University of Warsaw
Faculty of Mathematics, Informatics and Mechanics

Aleksander Zabłocki

On some generalizations of Shamir's secret sharing scheme

PhD dissertation

Supervisors

prof. dr hab. Jerzy Urbanowicz

prof. dr hab. Stanisław Spież

Institute of Mathematics
Polish Academy of Sciences

October 2015

Author's declaration:

Aware of legal responsibility I hereby declare that I have written this dissertation myself and all the contents of the dissertation have been obtained by legal means.

October 27, 2015 .....
date *Aleksander Zabłocki*

Supervisor's declaration:

The dissertation is ready to be reviewed.

October 27, 2015 .....
date *prof. dr hab. Stanisław Spież*

Abstract

A *Lai-Ding's secret sharing scheme* $\Sigma_q^{LD}(\mathbf{c}, i)$ defined by parameters $\mathbf{c} = (c_0, \ldots, c_{k-1})$, i and q is a modification of a Shamir's k-threshold scheme in which the share given to a participant $x \in \mathbb{F}_q$ is computed as the value of $P(x) = \sum_{j=0}^{k-1} a_j \cdot x^{c_j}$, where a_j are confidential while c_j are publicly known, and a_i is the value of the secret. Following the prior research of Spież, Urbanowicz et al., we study access structures realized by such schemes, as well as the behaviour of their admissible sets, where a set of participants is called *admissible* if the scheme restricted to it is k-threshold.

Our main efforts focus on providing asymptotic estimates for the number of admissible (or non-admissible) sets of a given size n in a Lai-Ding's scheme $\Sigma_q^{LD}(\mathbf{c}, i)$; in these estimates, q is the variable and $\mathbf{c}$, i, n are parameters (which may influence the asymptotic constants). Generalizing prior results for the case $\mathbf{c} = (0, 1, \ldots, k-1)$, we show in general that the number of admissible sets of size n is $\Theta(q^n)$. As for non-admissible sets, we show that, for fixed $\mathbf{c}$ and i, the number of such sets of size $k-1$ may be 0 for all q, $\Theta(q^{k-2})$ for all q, or may periodically switch between those two patterns. Moreover, in many cases, we provide computationally tractable lower bounds for q (and for the characteristic of $\mathbb{F}_q$) for which those sets must exist. This takes place in particular when $\mathbf{c}$ is an arithmetic progression, or when $\hat{\mathbf{c}}_i$ (i.e. $\mathbf{c}$ with c_i removed) has the property that every two its consecutive increments are coprime.

As an internal step in the above considerations (required by our need to use Weil's theorem), we investigate absolute irreducibility of the classical Schur polynomials over finite fields. Using the arguments of Monge and Rajan, and (partially) translating the latter from $\mathbb{C}$ to finite fields, we obtain a new result on irreducibility of a large class of such polynomials. Moreover, by implementing another novel method based on Newton polytopes, we generalize our irreducibility criterion to a large class of perturbations of Schur polynomials.

Finally, we make several preliminary observations on Lai-Ding's access structures. First, we show that they are almost as general as in Brickell's schemes; however, our construction of an appropriate Lai-Ding's scheme leads to significantly complex results. Then, we analyze the cases when $\mathbf{c}$ or $\hat{\mathbf{c}}_i$ are arithmetic. While the former case essentially reduces to Shamir's type schemes, the latter exhibits new examples of access structures, including certain graphic structures; we provide a characterization of graphs which can appear in this context.

Keywords: secret sharing, Shamir's scheme, Brickell's scheme, access structure, finite field, Schur polynomial, absolute irreducibility, matroid

Classification (MSC 2010): 94A62, 11T71, 11C20, 05B35, 12E10

Streszczenie

Schematem Lai-Dinga współdzielenia sekretu (oznaczenie: $\Sigma_q^{LD}(\mathbf{c}, i)$) dla parametrów $\mathbf{c} = (c_0, \ldots, c_{k-1})$, i, q nazywamy modyfikację k-progowego schematu Shamira, w której udziałem uczestnika $x \in \mathbb{F}_q$ jest wartość wielomianu $P(x) = \sum_{j=0}^{k-1} a_j \cdot x^{c_j}$, przy czym współczynniki a_j są tajne, zaś wykładniki c_j jawne, zaś wartością sekretu jest współczynnik a_i. Kontynuując wcześniejsza badania Spieża, Urbanowicza i in., badamy struktury dostępu realizowane przez takie schematy, a także zachowanie tzw. zbiorów progowych, gdzie zbiór uczestników nazywamy *progowym*, jeśli schemat po obcięciu do niego staje się k-progowy.

Jednym z naszych ważniejszych celów jest podanie asymptotycznych oszacowań liczby zbiorów progowych (bądź nie-progowych) o danej wielkości n w schemacie Lai-Dinga $\Sigma_q^{LD}(\mathbf{c}, i)$, przy czym w oszacowaniach tych rolę zmiennej pełni q, zaś $\mathbf{c}$, i, n są parametrami (mogącymi wpływać na stałe w notacji asymptotycznej). Uogólniając wcześniejsze wyniki dla $\mathbf{c} = (0, 1, \ldots, k-1)$, wykazujemy w ogólności, że liczba zbiorów progowych wynosi $\Theta(q^n)$. Odnośnie zbiorów nie-progowych, wykazujemy, że dla ustalonych $\mathbf{c}$ oraz i liczba takich zbiorów o wielkości $k-1$ może wynosić 0 dla wszystkich q, $\Theta(q^{k-2})$ dla wszystkich q, lub w sposób okresowy przełączać się pomiędzy tymi dwoma wzorcami. Ponadto dla wielu przypadków podajemy rozsądne z obliczeniowego punktu widzenia ograniczenia dolne na q (a także na charakterystykę ciała $\mathbb{F}_q$), powyżej których takie zbiory muszą istnieć. Ma to miejsce w szczególności gdy ciąg $\mathbf{c}$ jest arytmetyczny, lub gdy w ciągu $\hat{\mathbf{c}}_i$ (powstającym z $\mathbf{c}$ przez usunięcie c_i) każde dwa kolejne przyrosty są względnie pierwsze.

W ramach powyższego rozumowania (na potrzeby wykorzystywanego w nim twierdzenia Weila) badamy absolutną nierozkładalność klasycznych wielomianów Schura nad ciałami skończonymi. Wykorzystując rozumowania Mongego i Rajana i przenosząc (częściowo) metody Rajana z $\mathbb{C}$ nad ciała skończone, otrzymujemy nowy wynik dotyczący nierozkładalności dużej klasy wielomianów Schura. Co więcej, wykorzystując inną, nową metodę, opartą na wielościanach Newtona, uogólniamy powyższe kryterium nierozkładalności na szeroką klasę zaburzeń wielomianów Schura.

W ostatnim rozdziale pracy gromadzimy kilka spostrzeżeń dotyczących struktur dostępu w schematach Lai-Dinga. Najpierw wykazujemy, że są one niemal równie ogólne jak w schematach Brickella, choć nasza konstrukcja odpowiedniego schematu Lai-Dinga ma znaczny stopień złożoności. Następnie analizujemy przypadki, gdy ciąg $\mathbf{c}$ lub $\hat{\mathbf{c}}_i$ jest arytmetyczny. O ile pierwszy z nich zasadniczo sprowadza się do schematów typu Shamira, o tyle w drugim można znaleźć nowe przykłady struktur dostępowych, w tym niektóre struktury grafowe; podajemy charakteryzację grafów uzyskiwalnych w powyższy sposób.

Słowa kluczowe: współdzielenie sekretu, schemat Shamira, schemat Brickella, struktura dostępu, ciało skończone, wielomian Schura, absolutna nierozkładalność, matroid

Klasyfikacja (MSC 2010): 94A62, 11T71, 11C20, 05B35, 12E10

Contents

Introduction

Secret sharing and our area of interest

Secret sharing means distributing the knowledge of a hidden value (the *secret*) among a set of parties (the *participants*) by equipping them with pieces of partial information on the secret (*shares*) in a way which allows to control the *access structure*, that is, to specify exactly which sets of participants shall be able to reconstruct the secret if they meet together and reveal their shares. Many deterministic elementary algorithms for this task have been proposed, and *secret sharing schemes* have become their standard abstract model. (For details, see Section 2.1).

A particularly known example is the family of *Shamir's schemes* [52], in which, given two integers $n \geqslant 0$, $k \geqslant 1$ and a prime power $q > n$, an external *dealer* shall randomly choose a *secret-hiding polynomial* P of degree $k-1$ over the finite field $\mathbb{F}_q$ such that $P(0)$ is the value of the secret, and equip each participant p with the value $P(x_p)$, for arbitrary pairwise distinct *participants' identities* $x_p \in \mathbb{F}_q \setminus \{0\}$. This is currently treated as the standard method of sharing a secret among n participants so that the secret can be recovered by *every* set of k participants, and by *no* smaller set. (Such access structure, as well as a scheme realizing it, is called *k-threshold*). Despite being one of the oldest in the area, Shamir's construction is still appreciated for its simplicity, efficiency, and good security properties. As a result, over the last 35 years it has been the starting point for many adjustments and generalizations, some of which are capable of realizing various non-threshold structures.

Our research concentrates on one of those generalizations, proposed by Lai and Ding in [28], which we will refer to as *Lai-Ding's schemes*. Comparing to the Shamir's procedure described above, they introduce three modifications:

(i) dispersion of monomial degrees: P shall be now chosen among polynomials of the form $\sum_{j=0}^{k-1} a_j x^{c_j}$, where $\mathbf{c} = (c_0, \ldots, c_{k-1})$ is a fixed increasing sequence of non-negative integers, treated as a new parameter of the scheme;

(ii) shift of the secret: it shall be the coefficient a_i, where $0 \leqslant i \leqslant k-1$ is a new parameter of the scheme;

(iii) allowing that one of participants may have its identity x_p set to $0 \in \mathbb{F}_q$.

Shamir's schemes correspond to the case $\mathbf{c} = (0, 1, \ldots, k-1)$ and $i = 0$ (with $x_p = 0$ forbidden).

Lai-Ding's schemes have been investigated in [28] and [54]; certain their special sub-cases are also studied in [27], [59], [45], [55] and [56]. In particular, the paper [54] shows that studying Lai-Ding's schemes essentially reduces to describing zeroes of *Schur polynomials*, best known from representation theory. (This connection will be described in Section 2.2.2 and additionally discussed in Section 4.1.1). However, most of the prior research involves only

a rather particular special subclass of Lai-Ding's schemes, called *Shamir's type schemes* in [56], in which $\mathbf{c} = (0, 1, \ldots, k-1)$ (that is, only modifications of types (ii) and (iii) are allowed).

Main goals

Our primary objective is to answer several questions which have been raised (and, sometimes partially, answered for Shamir's type schemes) in [54] and the last three of the papers mentioned above. Apart from the natural problem of describing possible access structures, these questions concentrate around the notion of an *admissible* set of participants (see Section 2.2), which is understood in the simplest setting as a set such that the restriction of the scheme to it (obtained by simply disregarding all other participants) is k-threshold. In particular, we will study existence and approximate number of admissible sets, as well as of non-admissible sets, of a given size n.

In doing it, we will focus on asymptotic estimates in which q is treated as varying and the other parameters $\mathbf{c}$, i, n as fixed; in particular, the latter parameters will be allowed to influence the asymptotic constants hidden in the Θ-notation. This is what takes place in [45] and [56].

We will also pay particular attention to practical tractability of various lower bounds in our existential results. To enhance discussion, we distinguish three classes of such bounds:

- *sufficiently large* (*SL*) shall mean any provably existing bound;
- *reasonably sufficiently large* (*RSL*) shall mean any concrete bound which depends polynomially on n and c_{k-1} but possibly exponentially on k;
- *polynomially sufficiently large* (*PSL*) shall indicate that the dependence on k is also polynomial.

A summary of the necessary knowledge on the area, results obtained so far, and the motivation for our selection of research topics can be found in Section 2.

Below, we briefly describe the main branches of our research, and report their results.

Admissible sets (Chapter 3)

Following [45], we study the behaviour of admissible sets of a given size $n \geqslant k-1$ in a given Lai-Ding's scheme over the field $\mathbb{F}_q$, where q is an arbitrary prime power treated as a parameter of the scheme. We also denote the characteristic of $\mathbb{F}_q$ by p.

Given such input, the main problems considered in [45] are:

(A) For which q are there any admissible sets of size n?

(B) What is the asymptotics, with respect to q, of the number of such sets?

(C) Is there a procedure to build (almost) all such sets?

Also, assuming that the parameter $\mathbf{c}$ is fixed but i is varying, it has been asked:

(D) Can we answer the above questions for $\mathbf{c}$-*admissible* sets, i.e. sets which are simultaneously admissible for the given $\mathbf{c}$ and *every* $0 \leqslant i \leqslant k-1$?

For Shamir's type schemes, [45] tells that (see Section 2.2.3 for details):

- Admissible sets of size n exist for q RSL, and their number is $\Theta(q^n)$;
- The same applies to $\mathbf{c}$-admissible sets.

In our Theorems 1 and 2 (stated on pages 45 and 46), we show that both above claims generalize rather straightforwardly to general Lai-Ding's schemes. In fact, the proofs share the main idea of [45], which is ensuring existence of many simultaneous non-zeroes of a system of Schur polynomials. This part of the thesis, already published as a stand-alone paper [67], seems to be the simplest one.

Non-admissible sets (Chapters 4 and 5)

In [56] and [45], non-admissible sets in Shamir's type schemes are considered with regard to the above questions (A-C). We generalize this to Lai-Ding's schemes, at the same time limiting ourselves to the case $n = k - 1$ (which does not seem to be a very substantial restriction; see Section 4.1.2).

The prior results for Shamir's type schemes (see Section 2.2.3) show that, even for arbitrary $n \geqslant k - 1$, the behaviour of the total number of non-admissible sets of size n (for fixed $\mathbf{c}, i, n$ and varying q) falls into one of two templates:

(T1) there are no non-admissible sets of size n;

(T2) non-admissible sets of size n exist for q RSL, and their number is $\Theta(q^{n-1})$.

However, the situation for general Lai-Ding's schemes is more complex, and involves at least two new templates. Actually, our results involve three new scenarios:

(T2′) non-admissible sets of size n exist if q is RSL and in addition p is PSL;
under these assumptions, their number is $\Theta(q^{n-1})$;

(this is a tractable generalization of (T2), and it cannot be avoided)

(T2*) non-admissible sets of size n exist if q and p are SL;
under these assumptions, their number is $\Theta(q^{n-1})$;

(an intractable generalization of (T2′); we do not know if it can be avoided)

(T3) the number of non-admissible sets of size n is either 0 or $\Theta(q^{n-1})$, depending on the residue of q modulo some positive integer, with both possibilities indeed taking place infinitely many times;

in particular, they exist if q is PSL *and in addition* yields a good residue.

(this is significantly different from all above, and cannot be ruled out).

Our main results (discussed in more detail in the introduction to Chapter 4) state that, under the assumption that $n = k - 1$:

(1) For all $\mathbf{c}$ and i, non-admissible sets adhere to (T1), (T2*) or (T3);

(2) Non-admissible sets adhere to (T1), (T2′) or (T3) in the following cases:
   (a) $\hat{\mathbf{c}}_i$ (i.e. $\mathbf{c}$ with its i-th entry removed) is an arithmetic progression;
   (b) $\mathbf{c}$ is an arithmetic progression;
   (c) $\hat{\mathbf{c}}_i$ is *step-coprime* (see Definition 4.1).

In Chapter 4, we prove (2a) by purely elementary methods, and (2b) by using a deep theorem of Weil (see Section 1.2.2), though in a relatively simple particular case. For (1) and (2c), we use Weil's theorem in its full strength, which results in a reduction of the initial problem to verifying absolute irreducibility (and some coprimality properties) of Schur polynomials over finite fields (see Lemma 4.28). However, this verification turns out to require a laborious excursion into pure algebra, which we place in a separate Chapter 5.

Irreducibility of Schur polynomials (Chapter 5)

To complete the proof of the above claims (1) and (2c), we need to understand how the corresponding Schur polynomials factor over the algebraic closure $\overline{\mathbb{F}_q}$. Our primary goal is to find sufficient conditions for their absolute irreducibility. This is a purely algebraic problem and, due to the general importance of Schur polynomials, it seems to deserve interest independently of our main topic. Actually, we also allow some non-absolutely-irreducible cases, in which we additionally need to verify a coprimality property (see Lemma 4.28).

Although Schur polynomials are classical and widely studied, surprisingly little has been known on them in this regard. Even over the field $\mathbb{C}$ of complex numbers, the question of their irreducibility has been solved only recently, in [14] and independently in [42]. As we show in Section 5.2, this knowledge can be projected to $\overline{\mathbb{F}_q}$ by standard means of elimination theory, which suffices to prove (1). However, the resulting bounds for q (and even for p) are far from being RSL, so (2c) requires another approach.

In this direction, we obtain two results. First, we show that a theorem of [37] regarding the case $k = 3$ can be combined with an adjustment of fragments of the proof for the $\mathbb{C}$-based case from [42]. This yields absolute irreducibility under certain assumptions on $\mathbf{c}$, and for p PSL (see Theorem 7). This is what we need to prove (2c).

Second, in Section 5.6 we show that, in the proof of Theorem 7, the (adjusted) arguments of [42] can be replaced with another, somewhat simpler reasoning, which enables proving absolute irreducibility for a broad class of perturbations of Schur polynomials (see Theorem 7'). This result is digressive, in that it does not tell anything new about Lai-Ding's schemes; nevertheless, it seems to be interesting from a purely algebraic viewpoint.

Access structures (Chapter 6)

Apart from investigating (non-)admissible sets, the prior papers, particularly [55], provide some insight into the possible range of access structures realized by Shamir's type schemes. However, their results (listed in Section 2.2.4) are far from giving a complete picture of such structures, which reflects the general difficulty of the problem. For general Lai-Ding's schemes, the task seems even more complex, and we have only obtained preliminary results in two directions.

First, in Theorem 9, we prove that Lai-Ding's schemes have almost the same expressive power (with respect to realizable access structures) as the more general class of Brickell's schemes (see Section 2.1.3), and consequently (by comparing with the results of [55]) substantially more general than the Shamir's type. Although this result might seem theoretically appealing, it

does not seem to have significant practical applications (see the introduction to Chapter 6).

Second, we investigate the access structures which may arise in the simplest two cases considered in Chapter 4, i.e. $\mathbf{c}$ or $\hat{\mathbf{c}}_i$ arithmetic. The first of these cases is similar to Shamir's type schemes, and we show that the results from [55] generalize there, with subtle modifications (see Theorem 10). The other case behaves significantly differently, and we construct a family of access structures which can be realized by Lai-Ding's scheme of this kind but not by any Shamir's type scheme (see Theorem 11).

Conclusions

Our main goal — to generalize prior results on Shamir's type schemes to the Lai-Ding's case — has been achieved, though with many limitations. We have obtained new results in several most important research directions initiated in the papers [54], [45], [55] and [56]; in particular, it seems that Lai-Ding's schemes are now understood much better than in the founding paper [28].

Many of our results are still far from providing a complete picture of the problems considered. In fact, some of them show that we shall expect a significant increase in complexity of the corresponding problems when passing from Shamir's type to Lai-Ding's case, which is demonstrated by the increase in diversity of achievable outputs. This applies to the asymptotics of non-admissible sets, and particularly to the possible range of access structures.

In a purely algebraic language, we have thus demonstrated that the algebraic geometry of Schur polynomials is much richer than that of elementary symmetric polynomials. While such rough claim is probably not surprising, our concrete estimates seem to be not easily available on the grounds of classical algebraic geometry, and we hope that they could possibly have some value from an algebraic viewpoint. In particular, our investigation from Chapter 5 seems to add a minor contribution to algebra rather than cryptology, within a research direction which has been active in recent years.

Acknowledgements

The author would like to express his gratitude to the first supervisor of this thesis, the late Prof. Jerzy Urbanowicz. Prof. Urbanowicz has proposed the general topic and several questions regarded in this thesis, provided the author with a number of relevant references, and read preliminary draft versions.

The author is also thankful to Prof. Stanisław Spież for his agreeing to take over the role of the supervisor of this thesis, reading its consecutive draft versions, spending his time on lengthy conversations, and providing many valuable remarks.

The two abovementioned persons, together with Dobromir Matusiewicz, have communicated to the author that they also had deduced Theorem 1 in a somewhat different way.

The author is grateful to Prof. Andrzej Schinzel, Piotr Achinger, Prof. Piotr Pragacz, Dominika Pawlik and C. S. Rajan for conversations in which they have extended his knowl-

edge or asked insightful and stimulating questions. The author would also like to acknowledge Maurizio Monge for informing the author about his paper [37].

Finally, the author would like to thank his parents, relatives, friends, colleagues and other people whose kind interest in the condition of the research presented here has additionally motivated this work. The list of those persons is too long to be placed here. Many thanks to all of you for your support.

Chapter 1

Technical preliminaries

This chapter contains a brief summary of necessary preliminaries which are not connected to secret sharing. The conventions described in Section 1.1 are elementary, and mostly standard. The other section gathers various facts connected to number theory; the most important of them is the Weil's theorem, stated in Section 1.2.2.

1.1 Basic conventions

Throughout the whole thesis, the symbols

$$\mathbb{Z}, \quad \mathbb{Z}_{\geqslant 0} = \mathbb{N}, \quad \mathbb{Z}_{>0}, \quad \mathbb{R}, \quad \mathbb{R}_{\geqslant 0}, \quad \mathbb{R}_{>0}$$

denote respectively the sets of all/non-negative/positive integers and all/non-negative/positive real numbers. For a prime power q, $\mathbb{F}_q$ denotes the finite field with q elements. By default, all variables introduced in the text belong either to $\mathbb{Z}$ or to some $\mathbb{F}_q$ (with the choice clear from the context); in the first case, they will be usually explicitly restricted to $\mathbb{N}$.

For $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{>0}$, the notation $a \mod b$ will denote the residue of a modulo b.

For a set X, we will denote by $|X|$ its cardinality, by 2^X the family of all its subsets, and by $\mathrm{id}_X : X \to X$ its identity function. For a function $f : A \to B$ and a subset $A' \subseteq A$, we will denote by $f\big|_{A'} : A' \to B$ the restriction of f to A'.

1.1.1 Empty collections

As generally practiced, we will allow sums (resp. products) in commutative unital rings indexed over the empty set, letting them take the value 0 (resp. 1).

We will occasionally consider the empty sequence, denoted by $()$, as well as the empty matrix, denoted by $\left[\right]$. We will consider this matrix as the result also in situations which, taking strictly, would lead to a result of size "$0 \times k$" or "$k \times 0$" (with $k > 0$), a notable example being Definition 1.1 for either $\mathbf{c} = ()$ or $\mathbf{x} = ()$.

Quite naturally, $[\,]$ will be assumed to have rank zero. Moreover, we will assume that its determinant is 1, which seems reasonable in that it is consistent with the Laplace expansion, as well as with the permutational formula for the determinant (as the empty set has a unique permutation, which is positive).

1.1.2 Sequences, tracks and related notation

We will generally adopt the convention of [54] and the subsequent papers to organize the participants of secret sharing schemes into sequences rather than sets. This is convenient as one often needs to build such sets in an iterative procedure of choosing consecutive elements, so that the result is naturally of sequential type.

To clarify the language, we use the term *track* for sequences of pairwise distinct elements of $\mathbb{F}_q$ (understood as coalitions of participants); by permuting, we see that every set of size n corresponds to exactly $n!$ tracks.

We will now fix a set of notational conventions, aimed at increasing convenience of manipulating tracks of participants. (Among them, the ones which we will use most frequently are borrowed from [56] and [45]).

We will use bold letters to denote sequences either in $\mathbb{Z}$ (in most cases, $\mathbb{N}$) or a field currently taken into consideration (in most cases, a finite field $\mathbb{F}_q$). We adopt the convention that the entries of sequences and matrices are numbered starting from zero.

For any sequences $\mathbf{x}$, $\mathbf{y}$ with elements in a ring R, we denote:

- by x_i the i-th entry of $\mathbf{x}$ (numbering from zero);
- by $|\mathbf{x}|$ the length of $\mathbf{x}$;
- by $C_{\mathbf{x}}$ the set of all entries of $\mathbf{x}$;
- by $\hat{\mathbf{x}}_{i_0,i_1,\ldots,i_s}$ the sequence obtained by removing x_{i_0}, x_{i_1}, …, x_{i_s} from $\mathbf{x}$;
- by $\hat{x}_{i_0,\ldots,i_s,j}$ the j-th element of $\hat{\mathbf{x}}_{i_0,\ldots,i_s}$;
- by $\mathbf{x}+a$ (for $a \in R$) the sequence $(x_0+a,\, x_1+a,\, \ldots,\, x_{|\mathbf{x}|-1}+a)$;
- by $\mathbf{x}-a$ (for $a \in R$) the sequence $\mathbf{x}+(-a)$;
- by $\mathbf{x}^n$ (for $n \in \mathbb{Z}$) the sequence $(x_0^n, x_1^n, \ldots, x_{|\mathbf{x}|-1}^n)$;
  (here, we assume that $n \geqslant 0$ or $\mathbf{x}$ does not contain $0 \in R$)
- by $\mathbf{x}^{\mathbf{s}}$ (for $\mathbf{s} \in \mathbb{Z}^{|\mathbf{x}|}$) the sequence $(x_0^{s_0}, x_1^{s_1}, \ldots, x_{|\mathbf{x}|-1}^{s_{|\mathbf{x}|-1}})$;
  (here, we assume that, for every $0 \leqslant i < |\mathbf{x}|$, we have $s_i \geqslant 0$ or $x_i \neq 0$)
- by $\mathbf{x}[r]$ the prefix of $\mathbf{x}$ of length r;
- by $\gcd(\mathbf{x})$ (if $R \subseteq \mathbb{Z}$) the greatest common divisor of all elements of $\mathbf{x}$;
- by $\mathbf{x} \,||\, \mathbf{y}$ the concatenation $(x_0, \ldots, x_{|\mathbf{x}|-1}, y_0, \ldots, y_{|\mathbf{y}|-1})$;
- by $\mathbf{x} \circ \mathbf{y}$ (if $|\mathbf{x}| = |\mathbf{y}|$) the "scalar product" $\sum_{i=0}^{k-1} x_i \cdot y_i$;
- by $\mathbf{y} \sqsubseteq \mathbf{x}$ the condition that $\mathbf{y} = (x_{i_0}, \ldots, x_{i_{k-1}})$ for some $i_0 < \ldots < i_{k-1}$.

We also denote:

- by $\mathbf{e}_n$ the integer sequence $(0, 1, \ldots, n-1)$;
- by $\hat{\mathbf{e}}_{n,i}$ the sequence obtained from $\mathbf{e}_n$ by removing i;
- by ε_i the standard basis vector $(0, \ldots, 0, 1, 0, \ldots, 0)$, with i leading zeroes, of total length assumed to be known from the context.

(Note the numeration shift: $(1,0,0)$ is ε_0, not ε_1. While rather non-standard by itself, this is compatible with the rest of our notation).

An increasing sequence of non-negative integers will be called a *sequence of exponents*.

As long as this does not lead to ambiguities, we will override the notation by using the set-theoretic symbols $\in$ and $\subseteq$ for sequences; this always means referring to the set of elements of a sequence. For example, if $\mathbf{x} = (1,2)$ and $\mathbf{y} = (2,1,3)$, then $\mathbf{x} \not\sqsubseteq \mathbf{y}$ but $\mathbf{x} \subseteq \mathbf{y}$.

1.1.3 General algebra

For any set X, we will denote by Σ_X the group of its permutations.

For any field K, $\operatorname{char} K$ will denote its characteristic, $\overline{K}$ its algebraic closure, and $K^\times$ its multiplicative group. In some places, we will use the (rather standard) fact that the group $\mathbb{F}_q^\times$ is cyclic [31, Theorem 2.8].

All considered *rings* will be commutative and unital. For an integral domain R, (R) will denote its field of fractions.

Following [54] and [59] (where this convention has been adopted implicitly), we assume that, in any ring,

$$0^0 = 1. \tag{1.1}$$

While this might be disputed from the viewpoint of real analysis, it seems reasonable in the algebraic context of this thesis. In particular, adopting (1.1) simplifies the definition of generalized Vandermonde matrices (Definition 1.1).

Let R be a unique factorization domain. An element $x \in R$ is:

- *irreducible* [29, p. 111] if it is not invertible, and, for every decomposition $x = y \cdot z$ in R, y or z is invertible;
- *square-free* if there is no irreducible $a \in R$ such that a^2 is a divisor of x.

For a subset A of a vector space V over K, we denote by $\operatorname{span} A$ its linear span (i.e. the set of all linear combinations of its elements).

In the matrix notation of the form

$$\left[a_{ij}\right]_{0 \leqslant i \leqslant I,\, 0 \leqslant j \leqslant J},$$

the index i (resp. j) will be assumed to indicate the row (resp. column). Vectors of length n over a field K will be identified with matrices over K of size $n \times 1$ (i.e. having n rows and one column). The transpose of a matrix A will be denoted by A^T.

1.1.4 Polynomials

General conventions

Let R be a ring. As usual, $R[x_0, \dots, x_{n-1}]$ denotes the ring of polynomials with indeterminates $x_0, \dots, x_{n-1}$ and coefficients in R; if the sequence $(x_0, \dots, x_{n-1})$ is denoted by $\mathbf{x}$, this ring will be denoted in short by $R[\mathbf{x}]$. We recall that this is a unique factorization domain if R also is.

For a polynomial $P \in R[\mathbf{x}]$, we will (rather self-explanatory) use the term "monomials *in* P" (or "monomials *of* P") to refer to all monomials which appear in the formula for P in its fully expanded and cancelled form; for example, the list of all monomials in $P = (x_0 - x_1)^2$ consists exactly of x_0^2, x_1^2, and also of $-2x_0x_1$ in the case when $2 \neq 0$ in R. For a permutation $\sigma \in \Sigma_{\mathbf{x}}$, we will denote by P^σ the image of P under the action of σ induced on $R[\mathbf{x}]$.

The *total degree* [29, p. 103] of a polynomial $P \in R[\mathbf{x}]$, which we will denote by $\operatorname{tot\,deg} P$, is understood as the maximum of total degrees of all its monomials, where the total degree of a monomial $a \cdot \prod_{i=0}^{n-1} x_i^{d_i}$ is the sum of its "partial" degrees with respect to each of the indeterminates, i.e. $\sum_{i=0}^{n-1} d_i$.

A polynomial $P \in R[\mathbf{x}]$ is *symmetric* [29, p. 190] if it is invariant under the action of $\Sigma_{\mathbf{x}}$; the subring of $R[\mathbf{x}]$ consisting of such polynomials will be denoted by $R[\mathbf{x}]^{\mathrm{sym}}$. In addition, we will call P *semi-symmetric* if, for every $\sigma \in \Sigma_{\mathbf{x}}$, there is $c(\sigma) \in R$ such that

$$P^\sigma = c(\sigma) \cdot P.$$

(This notion will be helpful in Sections 5.2 and 5.5; it reduces to being symmetric or skew-symmetric in the sense of [41, Section 3.1.2], as we will show in the proof Fact 5.9).

Below, let K be any field.

Rather classically, a polynomial $P \in K[\mathbf{x}]$ is called:

- *irreducible* if it is irreducible as an element of the ring $K[\mathbf{x}]$
  (that is: P is non-constant, and whenever $P = A \cdot B$ in $K[\mathbf{x}]$, one of A, B is constant);
- *absolutely irreducible* if it is irreducible as an element of $\overline{K}[\mathbf{x}]$.

Note that the first of these notions may depend on the choice of K; if not clear from the context, this choice will be indicated explicitly (by calling P irreducible "*in* $K[\mathbf{x}]$" or "over K").

In Sections 4.5 and 5.2, we will use the fact that two polynomials $P, Q \in K[\mathbf{x}]$ are coprime if and only if their *resultant* is not zero; for the definition of resultant and the proof of this fact, see [31, Definition 1.93 and below].

Generalized Vandermonde matrices and determinants

In the thesis, we will mainly focus on the following family of matrices, whose importance for our topic will become evident in Section 2.1.3. Below, K denotes any field (in practice, taken to be $\mathbb{F}_q$ or, less frequently, $\mathbb{C}$; the choice will be clear from the context).

Definition 1.1 (cf. [54, p. 6])**.** For two sequences $\mathbf{c} \in \mathbb{Z}^k$ and $\mathbf{x} \in K^r$ such that

$$\mathbf{c} \in \mathbb{N}^k \text{ and } \mathbf{x} \in K^r \qquad \text{or} \qquad \mathbf{c} \in \mathbb{Z}^k \text{ and } \mathbf{x} \in (K \setminus \{0\})^r,$$

we define the *generalized Vandermonde matrix* by the formula

$$VM_{\mathbf{c}}(\mathbf{x}) = \left[x_i^{c_j}\right]_{\substack{0 \leqslant i < r \\ 0 \leqslant j < k}}.$$

(In the case when $\mathbf{x}$ and $\mathbf{c}$ both contain zero, (1.1) shall be applied).

Remark 1.2. As aforementioned in Section 1.1.1, in Definition 1.1 we allow also the cases $\mathbf{c} = ()$ or $\mathbf{x} = ()$, in which the Vandermonde matrix $VM_{\mathbf{c}}(\mathbf{x})$ shall be treated as empty.

Definition 1.3 ([54, p. 6])**.** Let $\mathbf{c}$ be a sequence of exponents of length $k \geqslant 0$ and $\mathbf{x} \in K^k$ be a sequence of the same length. Then, the *generalized Vandermonde determinant* $V_{\mathbf{c}}(\mathbf{x})$ is defined by the formula

$$V_{\mathbf{c}}(\mathbf{x}) = \det VM_{\mathbf{c}}(\mathbf{x}),$$

where $VM_{\mathbf{c}}(\mathbf{x})$ is the generalized Vandermonde matrix (see Definition 1.1). For $\mathbf{c} = \mathbf{e}_k$, this coincides with the classical Vandermonde determinant, which we will denote by $V(\mathbf{x})$.

Schur polynomials

It is well known (see e.g. [18, equation (A.4)]) that $V_{\mathbf{c}}(\mathbf{x})$ is always divisible by $V(\mathbf{x})$ in the multivariate polynomial ring $\mathbb{Z}[\mathbf{x}]$; the quotients of this form are widely known as *Schur polynomials*. This fact can be clearly projected to an arbitrary field K, regardless of its characteristic. For our purposes, we find it most convenient to introduce the notation

$$S_{\mathbf{c}}(\mathbf{x}) = \frac{V_{\mathbf{c}}(\mathbf{x})}{V(\mathbf{x})} \in K[\mathbf{x}], \tag{1.2}$$

which, although natural in our context, is inconsistent with the probably most standard notation; namely, our $S_{\mathbf{c}}$ coincides with s_λ of [17] and with S_λ of [18] provided that

$$\lambda = \big(c_{k-1} - (k-1),\, c_{k-2} - (k-2),\, \ldots,\, c_1 - 1,\, c_0\big).$$

Note that, by the properties of the classical Vandermonde determinant, we have

$$V_{\mathbf{c}}(\mathbf{x}) = 0 \iff S_{\mathbf{c}}(\mathbf{x}) = 0 \qquad \text{if } \mathbf{x} \text{ is a track.} \tag{1.3}$$

The general structure of Schur polynomials will be investigated in Chapter 5. As for now, we will only recall a particular coincidence between Schur polynomials and elementary symmetric polynomials, which we will need on several occasions.

Definition 1.4. Let $\mathbf{x} = (x_0, \ldots, x_{n-1})$ and $j \in \mathbb{Z}$. We define the *j-th elementary symmetric polynomial* $\tau_j(\mathbf{x})$ by the formula

$$\tau_j(\mathbf{x}) = \sum_{\substack{A \subseteq \{0,\ldots,n-1\} \\ |A| = j}} \prod_{i \in A} x_i.$$

In particular, $\tau_j(\mathbf{x}) = 0$ unless $0 \leqslant j \leqslant n$, and $\tau_0(\mathbf{x}) = 1$.

The following equality can be deduced immediately from [54, Lemma 2] or [28, Lemma 4]; in fact, it is a special case of a general determinantal identity (cf. [38, Chapter IX, p. 333] or [18, equation (A.6)]), which is attributed in [18] to Giambelli. A self-contained proof is provided in [28].

Lemma 1.5 (Giambelli, Muir; cf. [28])**.** For every $0 \leqslant i < k$, we have

$$S_{\hat{\mathbf{e}}_{k,i}} = \tau_{k-1-i}.$$

1.1.5 Asymptotic notation

We will use the notations $O(\cdot), \Omega(\cdot), \Theta(\cdot), \sim$ in their standard asymptotic meaning (see [11, Chapter 3] and [21, Glossary of Symbols]). More precisely, for any two functions $f : A \to \mathbb{R}$ and $g : B \to \mathbb{R}_{\geqslant 0}$, where A, B are two subsets of $\mathbb{N}$ with an infinite intersection, we write in short

$$f(n) = O\big(g(n)\big) \qquad (\text{resp. } f(n) = \Omega\big(g(n)\big))$$

to express the fact that there exist constants $C \in \mathbb{R}_{>0}$ and $N \in \mathbb{N}$ such that $|f(n)| \leqslant C \cdot g(n)$ (resp. $|f(n)| \geqslant C \cdot g(n)$) for every $n \in A \cap B$ such that $n > N$. The notation

$$f(n) = \Theta\big(g(n)\big)$$

is a shorthand for the conjunction of $f(n) = O\big(g(n)\big)$ and $f(n) = \Omega\big(g(n)\big)$.

Following the customary extended usage of these notations, we will write for example

$$f(n) = h(n) + O\big(g(n)\big) \tag{1.4}$$

as a synonym of $f(n) - h(n) = O\big(g(n)\big)$, etc. Let us underline that (1.4) serves actually as an estimate for $f(n)$ from *both* sides, as we defined the O-symbol to bound from above the absolute value $|f(n) - h(n)|$.

Finally, $f(n) \sim g(n)$ means that both $f(n), g(n)$ tend to infinity as $n \to \infty$, and the quotient $\frac{f(n)}{g(n)}$ tends to 1 as the value of n (chosen so that $n \in A \cap B$ and $g(n) \neq 0$) tends to infinity. More precisely, this means that for every real $C > 1$ there is some natural N_C such that $C^{-1} \leqslant \frac{f(n)}{g(n)} \leqslant C$ whenever $n \in A \cap B$ and $n > N$.

In practice, we will often apply the above notation to functions which may depend also on other arguments than n (thought of as parameters), some of which might influence the values of the constants C, N and N_C in the above definitions. In such situations, we will sometimes explicitly list the influencing parameters in the subscript (with $\emptyset$ denoting no influencing parameters), for example:

$$\tfrac{1}{ab+1} \cdot n \ \sim_{a,b} \ n, \qquad a \cdot n + \tfrac{1}{b+1} = \Theta_a(n), \qquad (a^2+1) \cdot n + \tfrac{1}{b+1} = \Omega_\emptyset(n).$$

However, as this convention is not very common in the literature, we will tend to use it only when the choice of the influencing parameters may be not clear from the context (e.g. in statements of new claims but not in their proofs).

1.2 Number-theoretic issues

1.2.1 Primes and density

We denote by P the set of all primes, and by $\widetilde{P}$ the set of all *prime powers* (i.e. numbers of the form p^k for some $p \in P$ and $k \geqslant 1$). The symbol φ will denote the Euler's totient function.

Density of a set. The *(asymptotic) density* [21, Chapter E] of a subset $A \subseteq \mathbb{N}$ is defined as

$$\rho(A) = \lim_{n\to\infty} \frac{|A \cap \{0, \ldots, n-1\}|}{n},$$

or is left undefined when the above limit does not exist. Note that the density is a finitely additive normalized measure on a subfamily of $2^{\mathbb{N}}$.

If $A \subseteq B \subseteq \mathbb{N}$, we define the *relative density* of A in B as

$$\rho(A \,|\, B) = \lim_{n\to\infty} \frac{|A \cap \{0, \ldots, n-1\}|}{|B \cap \{0, \ldots, n-1\}|}$$

or leave it undefined when the above limit does not exist. Again, this may be viewed as a finitely additive normalized measure on a subfamily of 2^B. Note that $\rho(A) = \rho(A \,|\, \mathbb{N})$. Note also that

$$\rho(A \,|\, C) = \rho(A \,|\, B) \cdot \rho(B \,|\, C), \tag{1.5}$$

provided that both values on the right-hand side are well-defined.

Ultimately periodic sets. A subset $A \subseteq \mathbb{N}$ is called *ultimately periodic* [35, Definition 2.2] if there exist $N \in \mathbb{N}$, $k > 0$ and a set $B \subseteq \{0, 1, \ldots, k-1\}$ such that

$$\forall_{n>N} \qquad \big(n \in A \quad \Leftrightarrow \quad n \mod k \in B\big).$$

For every such set A, we clearly have the following equivalence:

$$0 < |B| < k \qquad \Leftrightarrow \qquad 0 < \rho(A) < 1 \qquad \Leftrightarrow \qquad |A| = |\mathbb{N} \setminus A| = \infty. \tag{1.6}$$

If these conditions indeed hold, we will call A *proper ultimately periodic*.

A special case is an ultimately periodic set is (the set of elements of) an arithmetic progression. We call an arithmetic progression *coprime* if any (equivalently, every) its element is coprime to its common difference.

Primes (and their powers) in coprime sequences. The following theorem states intuitively that, for every positive integer l, the primes are asymptotically evenly distributed among the (reasonably chosen) residue classes modulo l.

Theorem A ([49, Chapter VI, Section 4.5])**.** *Let X be the set of all elements of a coprime arithmetic progression with common difference l. Then, we have*

$$\rho(X \cap P \,|\, P) = \frac{1}{\varphi(l)},$$

where φ is the Euler totient function.

To translate this to prime powers, we first recall a well-known fact that they are practically as dense as primes:

Fact 1.6 ([22])**.** The relative density of P in $\widetilde{P}$ is 1.

Proof. This follows e.g. from [22]; namely, from (1.31) combined with an unnamed equality on page 27 preceding (2.4.5). For reader's convenience, we restate them below in our language:

$$|P \cap \{0, \dots, n-1\}| \sim \frac{n}{\ln n};$$
$$\left|(\widetilde{P} \setminus P) \cap \{0, \dots, n-1\}\right| = O(\sqrt{n} \cdot \ln n).$$

Since the quotient of the second value by the first tends to zero, the claim follows. □

Corollary 1.7. Under the assumptions of Theorem A, we have

$$\rho(X \cap \widetilde{P} \,|\, \widetilde{P}) = \frac{1}{\varphi(l)}.$$

Proof. This is rather clear: we have $\rho(X \cap P \,|\, \widetilde{P}) = \frac{1}{\varphi(l)}$ by Theorem A, Fact 1.6 and (1.5), and also $\rho(X \cap (\widetilde{P} \setminus P) \,|\, \widetilde{P}) = 0$ by Fact 1.6. Summing these equalities yields the claim. □

1.2.2 Weil's theorems for irreducible polynomials

In several places, we will need to use the deep results of Weil [61] regarding the number of solutions of absolutely irreducible polynomials over a finite field. (They are also commonly known as "Riemann Conjecture for Curves over Finite Fields", even though the proof has appeared more than 60 years ago). However, as we are interested in the asymptotic behaviour of these solutions as well as in possibly strong concrete estimates (which we will need for further existential results), we will use a combination of two flavours of this theorem, both provided by Schmidt ([47], [46]), somewhat reformulated for our convenience.

Theorem B (Weil, Schmidt)**.** *Let q be a prime power, and $A \in \mathbb{F}_q[\mathbf{x}]$ be an absolutely irreducible polynomial of total degree $d > 0$. Denote by n the length of $\mathbf{x}$, and by $N_A(q)$ the number of zeroes of A in $\mathbb{F}_q^n$. Then, we have,*

$$N_A(q) = q^{n-1} + \Theta_d(q^{n-\frac{3}{2}}),$$

and moreover, the following concrete estimate from below holds:

$$N_A(q) \geqslant q^{n-1} - (d-1)(d-2)q^{n-\frac{3}{2}} - 6d^2q^{n-2} \qquad \text{for} \quad q > 10^{10}n^3(d \ln d)^5.$$

The first claim in the above statement is a direct consequence of [47, Chapter V, Theorem 5A]. Notably, the formulation given there provides concrete estimates with explicit constants; however, these constants are much too large for our purposes. Namely, [47] guarantees that $N_A(q) > 0$ only if q exceeds a bound slightly greater than the number

$$4d^2\binom{d+1}{2}^{2^{\binom{d+1}{2}}};$$

in particular, taking a fairly moderate value of $d = 12$ leads to requiring $q > 2^{2^{80}}$, which means that storing a single random element of $\mathbb{F}_q$ in a computer would require more than 2^{80} bits, i.e. 4 million petabytes.

For this reason, we supply our statement of Theorem B with its second part, which is a slight weakening of the main result of [46]. (Just for comparison, the lower bound for q obtained here for $n = d = 12$ is below 2^{69}, so that a reasonable representation of $\mathbb{F}_q$ should occupy less than 20 bytes per element). In the original formulation of [46], the lower bound for q takes a somewhat more complex form

$$q > 10^4 n^3 d^5 P^3([4 \ln d]), \tag{1.7}$$

where $[\cdot]$ denotes the floor operation (also called "entier" or "integer part"), and P is the prime enumerating function:

$$P(1) = 2, \qquad P(2) = 3, \qquad P(3) = 5, \qquad \dots$$

For $d = 1$, we literally obtain $P(0)$ which has unclear meaning; however, in such case, we have $N_A = q^{n-1}$ by basic linear algebra, so Theorem B clearly holds with no assumptions on q. For $d > 1$, we have $[4 \ln d] \geqslant 2$, which allows us to use the following estimate [13, formula (4.2)]:

$$P(k) \leqslant e \cdot k \cdot \ln k \qquad \text{for} \quad k \geqslant 2$$

and deduce that

$$P^3([4 \ln d]) \leqslant \big(4e \cdot \ln d \cdot \ln(4 \ln d)\big)^3 \leqslant 10^4 (\ln d)^5,$$

since the inequality $\ln(4x) \leqslant \frac{3}{2} \cdot (4x)^{\frac{2}{3}} \leqslant 4x^{\frac{2}{3}}$ holds for all real $x > 0$, and $(16e \cdot \frac{3}{2})^3 \leqslant 10^6$. This allows us to replace (1.7) with the bound used in our formulation of Theorem B.

Chapter 2

Secret sharing

In this chapter, we try to gather a versatile background related to secret sharing which will be needed (or helpful) in the next chapters.

The first two sections are sufficient (and recommended) for understanding most of the thesis. Section 2.1 contains a number of standard definitions and facts, and defines particular classes of schemes which will be of further interest. In the next section, we gather basic knowledge on the non-standard classes classes of Shamir's type and Lai-Ding's schemes; these include auxiliary definitions and preliminary results, either taken from prior literature or derived quickly on our own.

In Section 2.3, we take a deeper look on access structures, and discuss their relation with graphs and matroids; this content will be used only in Chapter 6 and Section 2.4. The latter, closing this chapter, aims at explaining the choice of topics taken by us; it is not needed for understanding our results but does place them in a broader context.

2.1 Definitions

2.1.1 Secret sharing schemes

We start from recalling the basic abstract model of secret sharing from [57].

The model involves a finite set $\mathcal{P}$, whose elements are called *participants*, and an additional element $D \notin \mathcal{P}$ called the *dealer*. (In practice, the dealer may be represented by a non-human device, or even by another cryptographic protocol; the model does not concern that, and assumes only that D can be trusted).

We assume that D chooses the *secret* (or *key*) K from a publicly known domain $\mathcal{K}$. Then, D may distribute the knowledge about K among the participants by equipping them with their *shares* (or *shadows* [2]), taken from a domain $\mathcal{S}$ correspondingly to the choice of K. The relation between the secret and the shares is formalized by choosing a set $\mathcal{I}$ of allowed *distribution rules*, each being of the form

$$f : \mathcal{P} \cup \{D\} \to \mathcal{S} \cup \mathcal{K},$$

with an additional restriction that

$$f(D) \in \mathcal{K} \qquad \text{and} \qquad f(p) \in \mathcal{S} \quad \text{for } p \in \mathcal{P}.$$

The set $\mathcal{I}$ is assumed to be known to the participants, together with the assumption that all distribution rules $f \in \mathcal{I}$ are equally probable (which will be used only in Definition 2.35 in Section 2.4.1). What is not known to the participants is the particular rule f chosen by the dealer; the participants can then form coalitions $C \subseteq \mathcal{P}$ in order to reveal the secret $f(D)$ on the basis of their shares $f(p)$ for $p \in C$.

The set $\mathcal{I}$, which we will call a *rule-set*, is the central point in the definition of a secret sharing scheme; in [57], $\mathcal{I}$ is simply called a "secret sharing scheme". Somewhat more formally, we can state this definition as follows.

Definition 2.1 (cf. [57, Section 3.1])**.** A *secret sharing scheme* is an arbitrary quintuple

$$\Sigma = (D, \mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{I})$$

in which the entries are of the form described above.

By a *sub-scheme* of Σ we mean any secret sharing scheme Σ' of the form

$$\Sigma' = \big(D, \mathcal{P}', \mathcal{K}, \mathcal{S}, \{f|_{\mathcal{P}' \cup \{D\}} \mid f \in \mathcal{I}\}\big)$$

for some subset $\mathcal{P}' \subseteq \mathcal{P}$.

Let $C \subseteq \mathcal{P}$ be a coalition of participants. Then, it is easy to see that C is always able to reveal the secret (where "always" means "regardless of the dealer's choice of $f \in \mathcal{I}$") if and only if

$$\forall_{f_1, f_2 \in \mathcal{I}} \qquad f_1\big|_C = f_2\big|_C \quad \Rightarrow \quad f_1(D) = f_2(D). \tag{2.1}$$

In Section 2.1.2 below, such sets will be called Σ-*authorized* (see Definition 2.4). However, for later convenience, this will be preceded by an abstract definition of an access structure.

Remark 2.2. Due to its simplicity, Definition 2.1 is not perfectly suitable for many practical purposes. In particular, it does not concern any kind of "security", which is usually achieved either by restricting to the families $\mathcal{I}$ with additional desired properties (often including *perfectness* and *ideality*), or even by extending the above model in a suitable way. In the latter case, the basic model has still the advantage of being a convenient starting point for such modifications. These issues will be discussed in more detail in Section 2.4; however, they are not essential for the purposes of this thesis.

2.1.2 Access structures

Roughly speaking, the notion of an *access structure* serves as an abstraction of the family of sets satisfying the condition (2.1) in a secret sharing scheme. Analogously as in Section 2.1.1, our introduction essentially follows [57] but is a little bit more formal.

Definition 2.3 (cf. [57])**.** An *access structure* is a pair $\Gamma = (\mathcal{P}, \mathcal{A})$, where $\mathcal{P}$ is a finite set (whose elements will be called *participants*) and $\mathcal{A} \subseteq 2^{\mathcal{P}}$ is a family of its subsets satisfying the following *monotonicity* condition:

$$\forall_{B \subseteq C \subseteq \mathcal{P}} \qquad \big(B \in \mathcal{A} \quad \Rightarrow \quad C \in \mathcal{A}\big). \tag{2.2}$$

The subsets of $\mathcal{P}$ belonging to $\mathcal{A}$ are called *authorized in* Γ (or Γ-*authorized*).

Given an access structure Γ, its components (i.e. the set of participants and the family of Γ-authorized sets) will be denoted by $\mathcal{P}_\Gamma$ and $\mathcal{A}_\Gamma$.

Let Σ be a secret sharing scheme over a set of participants $\mathcal{P}_\Sigma$, and let $\mathcal{A}_\Sigma$ be the family of all subsets in $\mathcal{P}_\Sigma$ satisfying the condition (2.1). Then, it is easy too see that $\mathcal{A}_\Sigma$ satisfies (2.2), which allows the following definition.

Definition 2.4 (cf. [57], [6])**.** The *access structure realized* (or *induced*) *by* a secret sharing scheme Σ (notation: $\Gamma(\Sigma)$) is defined as $(\mathcal{P}_\Sigma, \mathcal{A}_\Sigma)$, where $\mathcal{P}_\Sigma$ and $\mathcal{A}_\Sigma$ are as described above.

A subset $C \subseteq \mathcal{P}_\Sigma$ will be called *authorized in* Σ (or Σ-*authorized*) if and only if it is $\Gamma(\Sigma)$-authorized.

It turns out that every access structure Γ has the form $\Gamma(\Sigma)$ for some secret sharing scheme Σ; this is a simplified form of the main result in [26]. This shows soundness of Definition 2.3.

The *basis* of an access structure $\Gamma = (\mathcal{P}_\Gamma, \mathcal{A}_\Gamma)$ is the family $\mathcal{B}_\Gamma$ of all minimal sets in $\mathcal{A}_\Gamma$ (with respect to set inclusion). Note that, due to the monotonicity property, Γ is uniquely determined by specifying $\mathcal{P}_\Gamma$ and $\mathcal{B}_\Gamma$, where the latter can be chosen as any sub-family of $2^{\mathcal{P}_\Gamma}$ in which every two distinct elements are incomparable (i.e. neither is a subset of the other).

For a subset $\mathcal{P}' \subseteq \mathcal{P}_\Gamma$, we define the *substructure of* Γ *induced on* $\mathcal{P}'$ as $(\mathcal{P}', \mathcal{A}')$, where

$$\mathcal{A}' = \big\{C \subseteq \mathcal{P}' \,|\, C \in \mathcal{A}\big\}.$$

Clearly, for a secret sharing scheme Σ, the access structures induced by sub-schemes of Σ coincide with the sub-structures of $\Gamma(\Sigma)$.

The following class of access structure serves as the most basic example.

Definition 2.5 ([57])**.** For a finite set $\mathcal{P}$ and $k \geqslant 0$, the *k-threshold access structure (over $\mathcal{P}$)* is the pair $(\mathcal{P}, \mathcal{A})$, where $\mathcal{A}$ is the family of all subsets of $\mathcal{P}$ which are of size $\geqslant k$.

For $k = 0$, the resulting access structure (in which every subset of $\mathcal{P}$ is authorized) will be also called *degenerate*. Correspondingly, every access structure Γ not of this form (i.e. in which $\emptyset$ is not authorized) will be called *non-degenerate*.

2.1.3 Special classes of schemes

In the following definitions, we use the term *identity-setting function* to refer to any function of the form

$$I \quad : \quad \mathcal{P} \quad \to \quad \mathbb{F}_q^l,$$

where $\mathcal{P}$ denotes the set of participants, and $l \geqslant 0$. For $p \in \mathcal{P}$, we call the value $I(p)$ the *identity* of p (cf. [59], [54]), and use it (instead of p itself) to define the shares $f(p)$ for all $f \in \mathcal{I}$.

Unless stated otherwise, I is assumed to be publicly known. It might seem reasonable to assume also that I is injective; however, in general we will not require this, following the spirit of [6]. On the other hand, following [52] and other authors, we will require it in particular situations (see Definitions 2.9 and 2.13, and Remark 2.11).

As long as it does not lead to confusion, we will treat I as an actual identity, i.e. identify $\mathcal{P}$ with a subset of $\mathbb{F}_q^l$, and assume that $I = \mathrm{id}_{\mathcal{P}}$.

Brickell's schemes

Definition 2.6 ([6, Section 2])**.** Let $\mathcal{P}$ be a finite set, D be an element not belonging to $\mathcal{P}$, $k \geqslant 0$, $v_D \in \mathbb{F}_q^k$, and $J : \mathcal{P} \to \mathbb{F}_q^k$ be an identity-setting function. Then, the *Brickell's secret sharing scheme (defined by J and v_D)*, denoted by $\Sigma^B(J, v_D)$, is the quintuple $(D, \mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{I})$, where

$$\mathcal{K} = \mathcal{S} = \mathbb{F}_q, \qquad \mathcal{I} = \{f_v \,|\, v \in \mathbb{F}_q^k\}, \qquad \text{with} \quad f_v(x) = \begin{cases} v \circ J(x) & \text{for } x \in \mathcal{P}, \\ v \circ v_D & \text{for } x = D. \end{cases}$$

We will call such scheme *non-degenerate* if $v_D \neq 0$ (see Corollary 2.8 below).

Given an enumeration of elements of $\mathcal{P}$ in the form $\mathcal{P} = \{P_0, \ldots, P_{n-1}\}$, it is customary to represent the Brickell's scheme $\Sigma^B(J, v_D)$ by its *associated matrix* of the form

$$\left[\begin{array}{c|c|c|c|c} & & & & \\ v_D & J(P_0) & J(P_1) & \cdots & J(P_{n-1}) \\ & & & & \end{array}\right]. \tag{2.3}$$

Our key tool for understanding Brickell's schemes will be the following criterion, stated first in [6, Proposition 1]; we choose a formulation closer to that of [57].

Lemma 2.7 (Brickell)**.** Let $C \subseteq \mathcal{P}$ be a coalition of participants in the Brickell's scheme $\Sigma = \Sigma^B(J, v_D)$. Then,

$$C \text{ is } \Sigma\text{-authorized} \qquad \Longleftrightarrow \qquad v_D \in \operatorname{span}\big\{J(p) \,\big|\, p \in C\big\}.$$

By applying this lemma for $C = \emptyset$, we obtain in particular:

Corollary 2.8. A Brickell's scheme induces a non-degenerate access structure (see Definition 2.5) if and only if it is non-degenerate. □

Lai-Ding's schemes

Lai-Ding's schemes form a special case of Brickell's schemes, mentioned for the first time at the end of [28] and then investigated in [54]. Its definition depends on a sequence of exponents $\mathbf{c} = (c_0, \ldots, c_{k-1})$ and a number $0 \leqslant i < k$. (Note that this implies $k \geqslant 1$).

Definition 2.9 ([28, Section 5], [54, p. 2])**.** Let $\mathcal{P}, D$ be as in Definition 2.6, $\mathbf{c}$ be a sequence of exponents of length $k \geqslant 1$, $0 \leqslant i < k$, and $I : \mathcal{P} \to \mathbb{F}_q$ be an injective identity-setting function. Then, the *Lai-Ding's secret sharing scheme* $\Sigma_q^{LD}(I, \mathbf{c}, i)$ is defined as the Brickell's scheme $\Sigma^B(J, v_D)$, where

$$J(p) = \big(I(p)^{c_0},\, I(p)^{c_1},\, \ldots,\, I(p)^{c_{k-1}}\big) \quad \text{for } p \in \mathcal{P}, \qquad v_D = (\underbrace{0, \ldots, 0}_{i}, 1, 0, \ldots, 0).$$

(If $I(p)$ and c_i are both 0, we apply (1.1)).

The symbol $\Sigma_q^{LD}(\mathbf{c}, i)$ will denote the scheme $\Sigma_q^{LD}(I, \mathbf{c}, i)$ with $\mathcal{P} = \mathbb{F}_q$ and $I = \mathrm{id}_{\mathcal{P}}$.

Remark 2.10. Note that, for $\mathcal{P} \subseteq \mathbb{F}_q$ and $I = \mathrm{id}_{\mathcal{P}}$, Definition 2.9 makes the sense also if $\mathbf{c}$ is an increasing sequence of (not necessarily non-negative) integers; see also Definition 1.1. We will use this fact for convenience in Sections 4.2 and 4.3.

Remark 2.11. The assumption that I is injective is consistent with [54]. In [28, Section 4], it is not stated explicitly, but seems to be implicitly used in the statement of Lemma 5. Note, however, that J does not have to be injective even when I is.

Note that, for every Lai-Ding's scheme, the associated matrix contains a standard basis vector in its first column, while its remaining columns form the transpose of a generalized Vandermonde matrix (see Definition 1.1).

Although we will be mainly interested in Lai-Ding's schemes as defined above, in Section 6.1 we will find it helpful to consider also their variation in which I does not have to be injective.

Definition 2.12. Let $\mathcal{P}$, D, $\mathbf{c}$, i be as in Definition 2.9, and $I : \mathcal{P} \to \mathbb{F}_q$ be an *arbitrary* identity-setting function. Then, the scheme defined analogously as in Definition 2.9 will be called a *Lai-Ding's scheme with repeated identities* and denoted by $\Gamma_q^{LD*}(I, \mathbf{c}, i)$.

Shamir's and Shamir's type schemes

The *Shamir's type* and *Shamir's* schemes are two different classes which are obtained from Lai-Ding's schemes by subsequent restriction:

Definition 2.13 (cf. [52], [28], [54], [56])**.** Let $k \geqslant 0$, q be a prime power, and $I : \mathcal{P} \to \mathbb{F}_q$ be an injective identity-setting function. Then:

- **(a)** For $0 \leqslant i < k$, the *Shamir's type secret sharing scheme* $\Sigma_q^{ST}(I, k, i)$ is defined as the Lai-Ding's scheme $\Sigma_q^{LD}(I, \mathbf{e}_k, i)$;
- **(b)** The *Shamir's secret sharing scheme* $\Sigma_q^{S}(I, k)$ is defined as $\Sigma_q^{ST}(I, k, 0)$.

Analogously as for Lai-Ding's schemes, the case when $\mathcal{P} = \mathbb{F}_q$ and $I = \mathrm{id}_{\mathcal{P}}$ will be marked by omitting I in the above notation.

Shamir's schemes have been defined by Shamir in his paper [52], which together with the work of Blakley [5] has initiated the research on secret sharing. General Shamir's type schemes have been first considered in [28] and independently in [59]; however, the first definition concerning exactly this class appears in [54, p. 2], and the name "Shamir's type scheme" comes from an even later paper [56].

Remark 2.14. Shamir's schemes, certainly the most widely discussed in the literature of all the classes defined above, are usually referred to in singular, as "Shamir's *scheme*", which suggests that the word "scheme" denotes there a general (for instance, the Shamir's one) *pattern* of building quintuples Σ (see Definition 2.1).

However, we find this convention misleading, as it tends to miss a clear distinction between such patterns and single "instances"; for instance, both Brickell [6] and Stinson [57] speak

of "Shamir's threshold scheme" (a pattern) as well as of "the access structure realized by a secret sharing scheme" (which makes sense only if "scheme" refers to a single Σ, as in our Definition 2.1). To clarify this, we decide to unambiguously follow the second convention; this is generally consistent with [57, Section 3]. As a natural consequence, we will speak of Brickell's (Lai-Ding's, Shamir's type, Shamir's) *schemes*.[1]

Induced access structures

The access structures realized by the secret sharing schemes described above will be one of our main topics of interest. Correspondingly to the considered types of secret sharing schemes, we define *Brickell* (resp. *Lai-Ding, Shamir's type, Shamir*) *access structures*.

The access structures induced by the schemes

$$\Sigma^B(J, v_D), \qquad \Sigma_q^{LD}(\mathbf{c}, i), \qquad \Sigma_q^{ST}(k, i)$$

will be denoted respectively by

$$\Gamma^B(J, v_D), \qquad \Gamma_q^{LD}(\mathbf{c}, i), \qquad \Gamma_q^{ST}(k, i).$$

For a Shamir's scheme $\Sigma_q^S(k)$, a well-known result of [52] states that the induced access structure is the k-threshold one, provided that all participants' identities are non-zero and pairwise distinct.

2.2 Prior results on Shamir's type and Lai-Ding's schemes

2.2.1 Special types of coalitions/tracks

Definition 2.15. Let q be a prime power (fixed in a local context). Let $\mathbf{c}$ be a sequence of exponents, $0 \leqslant i < |\mathbf{c}|$, $n \geqslant 0$ and $\mathbf{t} = (t_0, \ldots, t_{n-1}) \in \mathbb{F}_q^n$ be a track. Let $C_{\mathbf{t}}$ denote, accordingly to Section 1.1.2, the coalition of all participants appearing in $\mathbf{t}$. Then, we call either $\mathbf{t}$ or its associated coalition $C_{\mathbf{t}}$:

- $(\mathbf{c}, i)$-*authorized* (cf. [56]) if $C_{\mathbf{t}}$ is authorized in $\Gamma_q^{LD}(\mathbf{c}, i)$,
- $(\mathbf{c}, i)$-*privileged* (cf. [45]) if it is $(\mathbf{c}, i)$-authorized and such that $|\mathbf{t}| < |\mathbf{c}|$,
- *max-length* $(\mathbf{c}, i)$-*privileged* if it is $(\mathbf{c}, i)$-authorized and such that $|\mathbf{t}| = |\mathbf{c}| - 1$,
- $(\mathbf{c}, i)$-S-*admissible* (cf. [54]) if the substructure of $\Gamma_q^{LD}(\mathbf{c}, i)$ induced on $C_{\mathbf{t}}$ is $|\mathbf{c}|$-threshold,
- $\mathbf{c}$-S-*admissible* (cf. [54]) if it is $(\mathbf{c}, i)$-S-admissible for every $0 \leqslant i < |\mathbf{c}|$;
- *zero-free* if all its entries are distinct from 0.

The parameters $\mathbf{c}, i$ will be omitted in the notation when they are clear from the context.

In the case when $\mathbf{c} = \mathbf{e}_k$ for some $k \geqslant 0$ (that is, when the Lai-Ding's scheme under consideration is actually a Shamir's type scheme), we will simplify the above notations by replacing "$\mathbf{e}_k$" with "k". This is consistent with the language of [54], [45] and [55].

[1] After all, switching to plural in a number of places is less invasive for the terminology than the other natural option, which would be implementing a new and rather uncommon term to refer to a single object Σ, like "an instance of secret sharing scheme".

Remark 2.16. The notion of *S-admissibility* given by Definition 2.15 is a natural generalization of *admissibility* according to Definition 2 of [56] (which regards Shamir's type schemes). It also coincides with *admissibility* in the sense of Definition 2 in [54] (which assumes $n \geqslant k$) but may disagree with its generalization for $n = k - 1$ introduced in [54, remarks following Proposition 2 and Lemma 2] and then explicitly quoted in [45, Definition 1] and [55, below Proposition 1].

Therefore, to avoid any confusion, we have introduced above the letter "S" (standing for "secret sharing" or "access structure"); on the other hand, admissibility in the broader sense of [54] will be referred to as *M-admissibility* (with "M" standing for "matrix"). The plain word *admissible* will be used to cover both variants, primarily in situations in which they coincide. See Section 2.2.2 for details.

2.2.2 Admissibility in Lai-Ding's schemes

Our goal in this section is to recall a criterion for S-admissibility in Lai-Ding's schemes from [56], and also to compare the two variants of "admissibility" (see Remark 2.16).

Most of the statements in this section can be also translated to arbitrary schemes of the form $\Sigma^B(J, \varepsilon_i)$, where $J : \mathcal{P} \to \mathbb{F}_q^k$ and $0 \leqslant i < k$; in particular, this is the situation considered in [54, Proposition 2], cited below as Lemma 2.21. However, we will not need this, and it is technically convenient for us to restrict to Lai-Ding's schemes now.

Criteria for being authorized

In the case of Lai-Ding's schemes, the criterion provided by Lemma 2.7 can be straightforwardly expressed in the language of generalized Vandermonde matrices, and then transformed to a somewhat more convenient form.

Fact 2.17. A track $\mathbf{t} \in \mathbb{F}_q^r$ is $(\mathbf{c}, i)$-authorized if and only if the vector ε_i is spanned by the (transpositions of) rows of $VM_{\mathbf{c}}(\mathbf{t})$. □

Fact 2.18. A track $t \in \mathbb{F}_q^r$ is $(\mathbf{c}, i)$-authorized if and only if

$$\operatorname{rank} VM_{\mathbf{c}}(\mathbf{t}) > \operatorname{rank} VM_{\hat{\mathbf{c}}_i}(\mathbf{t}),$$

or equivalently, if and only if the column corresponding to c_i in $VM_{\mathbf{c}}(\mathbf{t})$ is not spanned by the other columns.

Proof. This follows from the fact that

$$\operatorname{rank} VM_{\hat{\mathbf{c}}_i}(\mathbf{t}) = \operatorname{rank} \left[\begin{array}{c} VM_{\mathbf{c}}(\mathbf{t}) \\ \hline \varepsilon_i^T \end{array}\right] - 1.$$

□

Fact 2.19. A zero-free track of length 0 or 1 cannot be authorized in any Lai-Ding's scheme.

Proof. This follows from Fact 2.18. The case of the empty track is clear. For a track (x) with $x \in \mathbb{F}_q \setminus \{0\}$, note that, for every $\mathbf{c}$, i, both matrices $VM_{\mathbf{c}}((x))$ and $VM_{\hat{\mathbf{c}}_i}((x))$ have non-zero entries and hence rank one, which means that (x) is not $(\mathbf{c}, i)$-authorized. □

M-admissible tracks

We will now recall the actual general meaning of "admissibility" in [54], which we will refer to as "M-admissibility" (a shorthand for "matrix admissibility"). In our context, it is useful mainly in the computational criterion for S-admissibility provided by Lemma 2.21.

Definition 2.20 ([45, Definition 1]; cf. [54, Proposition 2])**.** Let q be a prime power and $\mathbf{c}$ be a sequence of exponents of length k, and let $0 \leqslant i < k$. A track $\mathbf{t}$ over $\mathbb{F}_q$ of length $n \geqslant k-1$ will be called $(\mathbf{c}, i)$-*M-admissible* if, for all subsequences $\mathbf{u}, \mathbf{v} \sqsubseteq \mathbf{t}$ respectively of lengths k and $k-1$, we have

$$V_{\mathbf{c}}(\mathbf{u}) \neq 0 \qquad \text{and} \qquad V_{\hat{\mathbf{c}}_i}(\mathbf{v}) \neq 0, \tag{2.4a}$$

or, equivalently by virtue of (1.3),

$$S_{\mathbf{c}}(\mathbf{u}) \neq 0 \qquad \text{and} \qquad S_{\hat{\mathbf{c}}_i}(\mathbf{v}) \neq 0. \tag{2.4b}$$

([2])

Lemma 2.21 ([54, Proposition 2])**.** Let $q, \mathbf{c}, k, i, \mathbf{t}, n$ be as in Definition 2.20, and assume in addition that $n \geqslant k$. Then, $\mathbf{t}$ is $(\mathbf{c}, i)$-S-admissible if and only if it is $(\mathbf{c}, i)$-M-admissible.

Remark 2.22. In [54, Proposition 2], it is required that $k \geqslant 2$; however, it is easy to check (e.g. using Fact 2.18) that Lemma 2.21 holds as well for $k = 1$.

Remark 2.23. While [45, Definition 1] formally defines "admissible tracks" according to Definition 2.20, [54] and [55] both actually use Definition 2.15 for $n \geqslant k$, and then (not so explicitly) switch to Definition 2.20 in the case $n = k-1$. Anyway, all three papers openly equate S-admissibility with M-admissibility, though in two slightly different contexts:

- Usually, it is assumed that $n \geqslant k$; then, the identification is justified by Lemma 2.21;
- In the remaining case $n = k-1$, both meanings coincide in Shamir's type schemes, as stated in [45]. (See Fact 2.25b below).

These two observations ensure unambiguous meaning of "admissible" in all relevant places of [45] and [55]. Nevertheless, in general the two meanings differ; see Remark 2.24 below.

Remark 2.24. Lemma 2.21 does not generally hold for $n = k-1$. For example, taking

$$q = 3, \qquad \mathbf{c} = (0, 2, 4), \qquad k = 3, \qquad i = 1, \qquad \mathbf{t} = (1, 2), \qquad n = 2,$$

leads to

$$VM_{\mathbf{c}}(\mathbf{t}) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \qquad VM_{\hat{\mathbf{c}}_i}(\mathbf{t}) = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

Then, $V_{\hat{\mathbf{c}}_i}(\mathbf{t}) = 0$, so $\mathbf{t}$ is not $(\mathbf{c}, i)$-M-admissible. On the other hand, since ε_i is not spanned by the rows of $VM_{\mathbf{c}}(\mathbf{t})$, Fact 2.17 implies that $\mathbf{t}$ is not $(\mathbf{c}, i)$-authorized, so it must be $(\mathbf{c}, i)$-S-admissible.

[2] Proposition 2 of [54] asserts that the conditions (2.4) reduce to a somewhat nicer condition that every minor of size k in the associated matrix of the scheme $\Gamma_q^{LD}(\mathbf{c}, i)$ is non-singular. However, we will not need this.

The case $n = k - 1$

In view of Remarks 2.23 and 2.24, it seems natural to supplement Lemma 2.21 with analysing how much of it can be saved when $k = n - 1$.

Lemma 2.25. Under the assumptions of Lemma 2.21:

(a) If $n = k - 1$, then the "if" part in the claim of Lemma 2.21 holds;

(b) If $\mathbf{c} = \mathbf{e}_k$, then Lemma 2.21 holds also for $n = k - 1$.

Proof. Using Definition 2.20, and Fact 2.18, we obtain equivalences:

$$\text{(2.5a)} \qquad \mathbf{t} \text{ is } (\mathbf{c}, i)\text{-}M\text{-admissible} \iff \operatorname{rank} VM_{\hat{\mathbf{c}}_i}(\mathbf{t}) = k - 1,$$
$$\text{(2.5b)} \qquad \mathbf{t} \text{ is } (\mathbf{c}, i)\text{-}S\text{-admissible} \iff \operatorname{rank} VM_{\hat{\mathbf{c}}_i}(\mathbf{t}) = \operatorname{rank} VM_{\mathbf{c}}(\mathbf{t}).$$

Now, the rank of $VM_{\mathbf{c}}(\mathbf{t})$ cannot exceed $k - 1$ which is the number of its rows; therefore, the condition (2.5a) implies (2.5b), which proves **(a)**. On the other hand, if $\mathbf{c} = \mathbf{e}_k$, then $VM_{\mathbf{c}}(\mathbf{t})$ contains a classical Vandermonde matrix $VM_{\mathbf{e}_{k-1}}(\mathbf{t})$, which is non-singular since $\mathbf{t}$ is a track; therefore, the rank of $VM_{\mathbf{c}}(\mathbf{t})$ is $k-1$, which makes (2.5a) and (2.5b) equivalent. This proves **(b)**. □

By combining this with Lemma 2.25b, we immediately obtain the following result:

Corollary 2.26 (cf. [45, the second paragraph following Definition 1])**.** A track $\mathbf{t}$ of length $k-1$ is (k, i)-privileged if and only if it is not (k, i)-M-admissible. □

Finally, let us formalize the meaning which we attach to *admissibility*:

Definition 2.27. Under the assumptions of Definition 2.20, assume in addition that $n \geqslant k$ or $\mathbf{c} = \mathbf{e}_k$. Then, $\mathbf{t}$ is $(\mathbf{c}, i)$-*admissible* if and only if it is $(\mathbf{c}, i)$-M-admissible, or, equivalently by virtue of Lemmas 2.21 and 2.25, $(\mathbf{c}, i)$-S-admissible.

As in Section 2.2.1, this naturally extends to the notions of (k, i)-*admissible* and k-*admissible* tracks.

2.2.3 Quantitative results on tracks

In the case of Shamir's type schemes, the previous papers (including in particular [45] and [56]) provide several quantitative results on admissible and non-admissible tracks. Most of these results are stated in the form of a rather complicated estimate from below, which has the advantage of providing (sometimes implicitly) two distinct kinds of information which will be of our main interest:

- a guarantee of existence of admissible (or non-admissible) tracks under certain assumptions (more precisely, for q sufficiently large in terms of the other variables);
- an asymptotic estimate of the number of tracks under consideration.

In the below statements, we reformulate the main results of [45] and [56], underlining their consequences in both directions described above. Generalizing these consequences will be our main objective in Chapters 3 and 4.

Before stating the results, we introduce some useful notation.

Denotation 2.28. Let $\mathbf{c}$ be a sequence of exponents of length k, $0 \leqslant i < k$, Π be one of the properties of tracks considered in Sections 2.2.1 and 2.2.2 (represented by an abbreviation like "S-adm", "M-adm", "max-priv", "$\substack{\text{max-priv}\\\text{zero-free}}$", "auth" etc.), and $n \geqslant 0$ (with an appropriate value in a given context). Then, the number of all tracks of length n over $\mathbb{F}_q$ which have the property "$(\mathbf{c}, i)$-Π" will be denoted as

$$N^{\Pi}_{\mathbf{c},i}(q,n),$$

where the subscript i may be removed when appropriate (e.g. $N^{\text{adm}}_{\mathbf{c}}(q,n)$ refers to $\mathbf{c}$-admissible tracks), the argument n may be removed when its value is obvious (which takes place for max-length privileged tracks), and $\mathbf{c}$ may be replaced with k to indicate that $\mathbf{c} = \mathbf{e}_k$ (as in Section 2.2.1).

Remark 2.29. Replacing "tracks" by "subsets" in the above denotation would lead to dividing the resulting value of $N^{\Pi}_{\mathbf{c},i}(q,n)$ (or $N^{\Pi}_{\mathbf{c}}(q,n)$) by $n!$.

For admissible tracks, [45] provides detailed inequalities of the form discussed above, both for the (k,i)-admissible and k-admissible case (Theorems C and D below). Moreover, it also contains a self-contained asymptotic estimate for the number of (k,i)-admissible tracks (Theorem E), which is stronger than what could be deduced from Theorem C since it effectively estimates $N^{M\text{-adm}}_{k,i}(q,n)$ from both sides (rather than only from below).

Theorem C ([45, Theorems 5 and 2]). *If $0 < i < k-1$, $n \geqslant k-1$ and $q > n - 1 + \binom{n-1}{k-2}$, then*

$$N^{M\text{-adm}}_{k,i}(q,n) \quad \geqslant \quad \prod_{j=0}^{i-1}(q-j) \cdot \prod_{j=i}^{k-2}(q-j-1) \cdot \prod_{j=k-1}^{n-1}\left(q-j-\tbinom{j}{k-2}\right) \quad > \quad 0.$$

Theorem D ([45, Theorem 7]). *If $n \geqslant k-1$ and $q > n + (k-2)\binom{n-1}{k-2}$, then*

$$N^{M\text{-adm}}_{k}(q,n) \quad \geqslant \quad \prod_{j=0}^{k-2}(q-2j-1) \cdot \prod_{j=k-1}^{n-1}\left(q-(j+1)-(k-2)\tbinom{j}{k-2}\right) \quad > \quad 0.$$

Theorem E ([45, Theorem 2]). *Let $0 < i < k-1$ and $n \geqslant k-1$. Then, we have*

$$N^{M\text{-adm}}_{k,i}(q,n) \quad = \quad q^n - \left(\tbinom{n}{2} + \tbinom{n}{k-1}\right)q^{n-1} + O_{k,i,n}(q^{n-2}).$$

Privileged tracks, on the other hand, have been investigated in [56], resulting in the following inequality:

Theorem F ([56, Theorems 1 and 2, and Remark 2]). *Let $k \geqslant 4$ and $0 \leqslant i < k$. Then, if $i \in \{0, k-1\}$, there are no zero-free max-length privileged tracks. On the other hand, if $0 < i < k-1$ and $q > 2k-1$, then*

$$N^{\substack{\text{max-priv}\\\text{zero-free}}}_{k,i}(q) \quad \geqslant \quad \prod_{j=1}^{m}(q-j) \cdot \prod_{j=m+1}^{k-3}(q-l-3-\mu) \cdot (q-2k+1) \quad > \quad 0,$$

where m denotes $\max(i, k-1-i)-1$, and μ denotes 0 (resp. 1) if q is odd (resp. even).

Easily to check, Theorem F straightforwardly implies that, under its assumptions,

$$N_{k,i}^{\text{max-priv}}(q) \;=\; \Omega_{k,i}\big(q^{k-2}\big). \tag{2.6}$$

However, a stronger asymptotic result has been obtained in [45] on the basis of Theorem E. Namely, since the number of all tracks in $\mathbb{F}_q^n$ is clearly equal to

$$\prod_{j=0}^{n-1}(q-j) \;=\; q^n - \tbinom{n}{2}q^{n-1} + O_k(q^{n-2}),$$

by combining this with Theorem E we immediately obtain:

Corollary 2.30 ([45, Corollary 2])**.** If $0 < i < k-1 \leqslant n$, then

$$N_{k,i}^{\text{non-adm}}(q,n) \;=\; q^{n-1} + O_{k,i}(q^{n-2}). \qquad \square$$

In particular, by setting $n = k-1$ and applying an observation stated above as Corollary 2.26, we obtain a strengthening of (2.6):

Corollary 2.31 ([45, Corollary 3])**.** If $0 < i < k-1$, then

$$N_{k,i}^{\text{max-priv}}(q) \;=\; q^{k-2} + O_{k,i}(q^{k-3}). \qquad \square$$

2.2.4 Shamir's type access structures

Finally, we would like to summarize the existing knowledge on possible access structures realized by Shamir's type schemes; this topic has been researched primarily in [55].

Theorem G ([55], [45], [56])**.** *Let $0 \leqslant i < k-1$, and denote $\Gamma = \Gamma_q^{ST}(k,i)$. Then:*

- ***(a)*** *All Γ-authorized sets are of size $\geqslant i+1$;*
- ***(b)*** *All Γ-authorized sets not containing zero are of size $\geqslant k-i$;*
- ***(c)*** *If $i = k-1$, then all Γ-authorized sets are of size $\geqslant k$;*
- ***(d)*** *If $i = 0$, then all Γ-authorized sets not containing zero are of size $\geqslant k$;*
- ***(e)*** *If $0 < i < k-1$, $r \geqslant \max(i+1, k-i)$ and $q \equiv 1 \pmod r$, then there exist Γ-authorized sets of size r;*
- ***(f)*** *If $k \geqslant 3$, $i = \frac{k-1}{2}$, $r = \frac{k+1}{2}$ and $\gcd(q,r) = 1$, then Γ-authorized sets of size r exist if and only if $q \equiv 1 \pmod r$;*
- ***(g)*** *If $k \geqslant 4$, $0 < i < k-1$ and $q > 2k-1$, then $\mathcal{B}_\Gamma$ contains a set of size $r \leqslant k-1$;*
- ***(h)*** *If $k \geqslant 3$, $0 < i < k-1$, $0 \leqslant r \leqslant k-1 \leqslant n$, $q \geqslant n + r\binom{n-2}{k-2}$, and $\mathcal{B}_\Gamma$ contains a set A of size r, then Γ contains a substructure Δ defined over a set $B \subseteq \mathbb{F}_q$ of size n, in which the basis has the form*

$$\mathcal{B}_\Delta = \{A\} \cup \big\{C \subseteq B \;\big|\; |C| = k\big\}.$$

(Recall that $\mathcal{B}_\Gamma$ denotes the basis of an access structure Γ; see Section 2.1.2).

Parts **(a-b)** follow from [55, Corollary 2], **(c)** and **(d)** from the first paragraph on the fourth page of [45], while **(e)** and **(f)** respectively from Theorems 2 and 3 in [55]. Finally, **(g)** is a consequence of Theorem F (taken from [56]), and **(h)** is a reformulation of [56, Theorem 3].

Altogether, Theorem G can be thought of as a demonstration of diversity of Shamir's type access structures, forced by their dependence on the relations between k, i and q. In particular, parts **(g-h)** can be used to construct arbitrarily large non-threshold substructures of $\Gamma_q^{ST}(k,i)$; this result can be made even more concrete by a relatively easy strengthening **(g)** to ensure that $r = k - 1$.[3]

On the other hand, the limitations imposed by parts **(a-b)** clearly show that Shamir's type schemes fail to realize many interesting examples of Brickell's access structures.

2.3 Access structures, graphs and matroids

2.3.1 Graphs

By a *graph* we will mean a pair $G = (V, E)$ consisting of a finite set V of *vertices* and a set E of *edges*, each of which is a two-element subset of V. This setting (in particular, using sets instead of multisets) means that our graphs are undirected, without loops and multiple edges (see [66, p. 3], where such objects are called *simple graphs*).

The *disjoint union* cf. [66, p. 10] of graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is defined as

$$G_1 \amalg G_2 = (V_1 \amalg V_2,\ E_1 \amalg E_2),$$

where $\amalg$ on the right-hand side denotes set-theoretic disjoint union. The *difference* (cf. [62, p. 1230]) of two graphs $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ which share the same set of vertices V is defined as

$$G_1 \setminus G_2 = (V,\ E_1 \setminus E_2).$$

(This meaning of "$\setminus$" is different from that of [66]).

A *clique* [11, Section 34.5.1] in a graph $G = (V, E)$ is a subset $A \subseteq V$ in which every two distinct vertices are connected by an edge. It is also common to call G a *clique* if the whole V is a clique in the above sense; following this, we will call G a *disjoint union of cliques* [12, Section 1.1] if it is a disjoint union of such graphs.

The other notions of graph theory which we will use (*isomorphism*, *path*, *connected component*) are rather self-explanatory; for their definitions, see [66].

2.3.2 Access structures revisited

Access structures have been defined already in Definition 2.3 in Section 2.1.2. We will now describe additional notions related to them, including some standard terms (with references

[3] For the details on how to obtain that, we refer the reader to another footnote in Section 4.5, where this issue is discussed thoroughly in a more demanding context.

provided), as well as our auxiliary definitions, purposed only for convenience of the discussions in Section 2.4 and Chapter 6.

Graphic structures ([57]). The *graphic access structure* for a graph $G = (V, E)$, denoted by $\Gamma(G)$, is defined by taking V as its set of participants, and E as its basis.

Morphisms. We define a *homomorphism* between two access structures Γ_1, Γ_2 as a map $f : \mathcal{P}_{\Gamma_1} \to \mathcal{P}_{\Gamma_2}$ such that

$$\forall_{C \subseteq \mathcal{P}_{\Gamma_1}} \qquad \big(C \in \mathcal{A}_{\Gamma_1} \quad \Leftrightarrow \quad f(C) \in \mathcal{A}_{\Gamma_2}\big). \tag{2.7}$$

Such a homomorphism f will be called an *embedding* (resp. *isomorphism*, *epimorphism*) if it is injective (resp. bijective, surjective).

"Prefix-potent" participants. Let Γ be a fixed access structure. We auxiliarily define the *relevance* of a subset $X \subseteq \mathcal{P}_\Gamma$ as the family of all subsets $C \subseteq \mathcal{P}_\Gamma$ such that $C \cup X$ is Γ-authorized but C is not. The *relevance* of a participant $p \in \mathcal{P}_\Gamma$ is the relevance of $\{p\}$. Basing on this, we say that:

- a participant $p \in \mathcal{P}_\Gamma$ is *omnipotent* if it has the full possible relevance (i.e. $\{p\}$ is authorized);
- a participant $p \in \mathcal{P}_\Gamma$ is *nilpotent* if its relevance is empty (i.e. $C \cup \{p\}$ is authorized iff C is, for every $C \subseteq \mathcal{P}_\Gamma$);
- two participants $p_1, p_2 \in \mathcal{P}_\Gamma$ are *equipotent* if they have equal relevance (i.e. $C \cup \{p_1\}$ is authorized iff $C \cup \{p_2\}$ is, for every $C \subseteq \mathcal{P}_\Gamma$).

Clearly, equipotence is an equivalence relation. In fact, a set E of (pairwise) equipotent participants may be effectively treated as a set of clones of a single participant, since cooperating with any single participant of E has the same effect as cooperating with the whole E. This is made precise (and generalized) in the following fact.

Fact 2.32. Let E be subset of $\mathcal{P}_\Gamma$ in which every two participants are equipotent. Then, every two non-empty subsets $E_1, E_2 \subseteq E$ have the same relevance in Γ.

Proof. If $E_1 = E_2$, the claim is obvious. For other cases, the proof can be obtained in three steps.

1. Assume that $E_1 \subseteq E_2$ and $E_2 \setminus E_1 = \{p\}$. Fix an element p' of E_1. Let C be any subset of $\mathcal{P}_\Gamma$, and denote $D = C \cup E_1$. Then, since p and p' are equipotent, $D \cup \{p\} = C \cup E_2$ is authorized iff $D \cup \{p'\} = C \cup E_1$ is. Hence, E_1 and E_2 have equal relevance.

2. Now, whenever $E_1 \subseteq E_2$, the claim is either obvious (if $E_1 = E_2$) or follows by applying inductively step 1.

3. Finally, for any two non-empty subsets $E_1, E_2 \subseteq E$, step 2 shows that E_1, E_2 must both have the same relevance as $E_1 \cup E_2$. □

An access structure Γ will be called an *equipotential extension* of its substructure Δ if every $p \in \mathcal{P}_\Gamma$ is equipotent with some $p' \in \mathcal{P}_\Delta$. In such case, Γ can be essentially viewed as obtained from Δ by cloning each of its elements into appropriately many copies.

Morphisms and equipotence. Our definition of homomorphism is rather strict in that it concerns images rather than pre-images of sets. In particular, if f is a homomorphism from Γ_1 to Γ_2, then, for every $q \in \mathcal{P}_{\Gamma_2}$, the whole pre-image $f^{-1}(q)$ belongs to a single equipotence class in Γ_1. Hence, if we choose any $\Delta \subseteq \Gamma_1$ containing one representative of every such pre-image, then it turns out that:

- Γ_1 is an equipotential extension of Δ;
- f maps Δ isomorphically to the substructure of Γ_2 induced on $f(\mathcal{P}_\Delta) = f(\mathcal{P}_{\Gamma_1})$.

This means that every homomorphism of access structures (in our sense) represents a very close relationship between its domain and its image. In particular, if f is an epimorphism, then Γ_1 is isomorphic to an equipotential extension of Γ_2.

Connectivity. An access structure $\Gamma = (\mathcal{P}, \mathcal{A})$ is called *connected* ([53, Section 3.1]; cf. "connected scheme" in [7]) if every its element belongs to some set in its basis. In our language, this is easily checked to be equivalent to inexistence of nilpotent elements.

2.3.3 Matroids

Matroids have been defined by Whitney [64]; detailed treatment can be found in [63] and [39]. In the below discussion, we restrict to notions useful for our purposes, concentrating on the relationship between matroids and access structures.

The definition. Roughly, the notion of matroid captures the property of linear independence specified by Steinitz Lemma.

Definition 2.33 ([39, Section 1.1])**.** A *matroid* is a pair $\mathcal{M} = (M, \mathcal{I})$, where is M is a finite set, and $\mathcal{I} \subseteq 2^M$ is a family of its subsets which contains the empty set, is closed under taking subsets, and satisfies the following condition:

$$\text{if} \quad A, B \in \mathcal{I} \text{ and } |A| < |B|, \quad \text{then} \quad \exists_{x \in B \setminus A}\ A \cup \{x\} \in \mathcal{I}.$$

The subsets of M belonging to $\mathcal{I}$ are called *independent sets*. The remaining subsets of M are called *dependent*, and the minimal ones among them (with respect to inclusion) are called *circuits*.

For a fixed matroid $\mathcal{M} = (M, \mathcal{I})$, every subset M' defines the *induced sub-matroid* $\mathcal{M}' = (M', \mathcal{I}')$, where $\mathcal{I}'$ consists of elements of $\mathcal{I}$ contained in M'.

Isomorphisms [39, p. 12]**.** An *isomorphism* between two matroids $(M_1, \mathcal{I}_1)$, $(M_2, \mathcal{I}_2)$ is a bijective map $f : M_1 \to M_2$ preserving dependence and independence:

$$\forall_{X \subseteq M_1} \qquad \big(X \in \mathcal{I}_1 \quad \Leftrightarrow \quad f(X) \in \mathcal{I}_2\big).$$

Special classes of matroids. For a finite set M and $k \geqslant 0$, the family $\mathcal{I}$ consisting of subsets of M of size $\leqslant k$ defines a matroid over M, called *(k-)uniform* [39, Example 1.2.7].

Let A be a finite matrix over a field K of size $m \times n$. Then, we define the *column matroid* of A (cf. [39, p. 20]) as $(M, \mathcal{I})$, where $M = \{0, \ldots, n-1\}$, and $\mathcal{I}$ consists of exactly those subsets

$\{i_0, \ldots, i_{s-1}\} \subseteq \{0, \ldots, k-1\}$ for which the sequence

$$\big(i_j\text{-th column of } A\big)_{0 \leqslant j < s}$$

is linearly independent in K^m (here, we number the columns starting from zero). The resulting matroid will be denoted by $\mathcal{M}(A)$.[4] Generally, matroids of this form (or isomorphic to such) are called *representable (over K)* [63, Section 9.1].

Note that, for any field extension L of K and $n \geqslant 0$, any sequence of vectors in K^m is linearly independent over K if and only if it is linearly independent over L. This shows that the column matroid of a matrix does not depend on the choice of K. (However, representability of a given matroid may depend on the ground field, particularly on its characteristic).

Ports [34]**.** The *port* of a matroid $\mathcal{M} = (M, \mathcal{I})$ at an element $m_0 \in M$ is the access structure

$$\Gamma(\mathcal{M}, m_0) = (M \setminus \{m_0\}, \mathcal{A}),$$

where $\mathcal{A}$ consists of all subsets $A \subseteq M \setminus \{m_0\}$ for which there exists $B \subseteq A$ such that B is independent but $B \cup \{m_0\}$ is not.

In the case when $\mathcal{M}$ is the column matroid of a matrix A, it follows easily that a subset $\{i_0, \ldots, i_{s-1}\} \subseteq \{0, \ldots, k-1\}$ belongs to $\Gamma(\mathcal{M}, m_0)$ if and only if the m_0-th column of A belongs to the linear span of the columns with numbers $i_0, \ldots, i_{s-1}$. This in turn allows to reformulate Lemma 2.7 in the language of matroids, as follows:

Lemma 2.7'. Let $\mathcal{P} = \{P_0, \ldots, P_{n-1}\}$ be an enumeration of the participants in a Brickell's scheme Σ over $\mathbb{F}_q$, and let A be its associated matrix (defined by the above enumeration). Then, the bijective assignment $\phi : P_i \mapsto i+1$ (for $0 \leqslant i < n$) defines an isomorphism between the access structure realized by Σ and the "left-most" port of the column matroid of A:

$$\phi \;:\; \Gamma(\Sigma) \quad \simeq \quad \Gamma\big(\mathcal{M}(A), 0\big). \qquad \square$$

Connectivity and direct sum. The *connected components* of a matroid $\mathcal{M} = (M, \mathcal{I})$ [63, Section 5.2] are defined as the sub-matroids induced by equivalence classes of the relation R defined so that $x \,R\, y$ if and only if x and y are equal or both belong to some circuit of $\mathcal{M}$. A matroid is *connected* if it has a single connected component. It turns out that every matroid can be presented as the *direct sum* of its connected components; the details can be found in [63, Section 5.3].

Connectivity of matroids is related to that of access structures: for every $m \in M$, $\Gamma(\mathcal{M}, m_0)$ is a connected access structure if and only if $\mathcal{M}$ is connected [53, above Proposition 1].

Matroids and access structures. Every matroid determines a finite family of access structures which are its ports. It turns out that this correspondence is, in some sense, bidirectional:

Lemma 2.34 ([63, Section 5.4, Theorem 1])**.** A connected matroid $\mathcal{M} = (M, \mathcal{I})$ can be uniquely determined on the basis of its port $\Gamma(\mathcal{M}, m_0)$, where m_0 is some element of M.

[4] It might be tempting to simplify this definition by removing indices, and taking M to be simply the set of columns of A (with $\mathcal{I}$ still defined by linear independence). This would indeed yield a matroid isomorphic to $\mathcal{M}(A)$, provided that the columns of A are pairwise distinct. In the other case, the results may differ (see [63, Section 9.1]).

This means that taking ports defines an *injective* mapping Π between isomorphism-closed *classes* of connected matroids and connected access structures: given such a class $\mathcal{C}$ of matroids, $\Pi(\mathcal{C})$ is defined as the class of all ports of elements of $\mathcal{C}$. (We define Π at the level of classes because a connected matroid may have several ports which are not pairwise isomorphic).

Matroids and graphs. Matroids are strongly connected with graph theory (see [39, Chapter 5]); this explains in particular the name "circuit". However, despite their name, *graphic matroids* (see [39]) have no connection to graphic access structures (see Section 2.3.2), and will be out of our interest.

More generally (and roughly), the triangle of standard connections between graphs, access structures and matroids does not at all "commute", and the link between graphs and matroids, although probably best known of all the three, is the one which we will disregard.

2.4 Cryptological context and motivation

This section is meant as purely motivational, and can be skipped with no consequences for understanding further chapters. On the other hand, it may be of top interest for a reader who would like to understand the reasons behind the choice of problems considered in this thesis.

In Section 2.4.1, we discuss two crucial cryptological advantages exhibited by every Shamir's scheme, and actually also by every Brickell's (and hence, every Lai-Ding's) scheme. This is intended to convince the reader that restricting our attention to Brickell's schemes (as we do in this thesis), although certainly being not necessary, is a quite good decision.

Then, we consider differences between Brickell's schemes and their subclasses defined so far. Here, a crucial aspect is the diversity of realized access structures, in which Lai-Ding's schemes turn out to substantially prevail over those of Shamir's type; this is a key point in the discussion of Section 2.4.2, summarized in Table 2.1.

Finally, we come to the question whether Lai-Ding's schemes have important advantages over Brickell's, which is much subtler. Several observations related to it, as well as the motivation behind the notion of $\mathbf{c}$-admissible tracks, are gathered in Section 2.4.3.

2.4.1 Perfect security and ideal schemes

According to the commonly accepted informal definition (see [6, p. 1], [57, p. 5], [52]), a secret sharing scheme is called *perfect* if every coalition of participants is either authorized (see Section 2.1) or "unable" to obtain "any information" on the secret.

In such description, the two quoted expressions deserve a deeper explanation. First, the word "unable" refers to information-theoretical security, i.e. to the model in which all participants are assumed to have unlimited computational power. This is unlike e.g. the RSA encryption algorithm [58, Chapter 4], whose security relies on our inability (as of 2015) to efficiently factor large integers and take roots in modular arithmetic. In other words, while every particular instance of RSA is actually threatened by possibility of quick decryption — by inventing

breakthrough solutions to those computational problems, by using huge computational power, or simply by plain luck — the secret sharing schemes considered below will be safe from all these scenarios. On the other hand, we still assume that all the participants use solely logic, their own knowledge and honest communication. These restrictions may still lead to great divergence between security in theory and in practice (see Section 2.4.3, particularly the discussion of cheating).

Second, the phrase "any information" is usually given a strong information-theoretic meaning, set up on the assumption stated in Section 2.1.1 that all distribution rules are equally probable. (However, other interpretations also exist; see Remark 2.36).

Using the language of Section 2.1.1, this can be strictly formulated as follows.

Definition 2.35 (cf. [6, p. 1] and [57, p. 5])**.** Let $\Sigma = (D, \mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{I})$ be a secret sharing scheme and $\Gamma(\Sigma)$ denote its induced access structure. We say that Σ is *perfect* if, for every

$$C \in 2^{\mathcal{P}} \setminus \Gamma(\Sigma), \qquad g \in \mathcal{I},$$

and for f denoting a random (with uniform distribution) element of $\mathcal{I}$, the conditional distribution of $f(D)$ under the assumption that $f\big|_C = g\big|_C$ is uniform, i.e.

$$\frac{\left|\left\{f \in \mathcal{I} \;\middle|\; f(D) = k,\ f|_C = g|_C\right\}\right|}{\left|\left\{f \in \mathcal{I} \;\middle|\; f|_C = g|_C\right\}\right|} = \frac{1}{|\mathcal{K}|} \qquad \text{for } k \in \mathcal{K}. \tag{2.8}$$

All Shamir's schemes are perfect, as well as Brickell's; see [52] and [6, Proposition 1].

Perfectness serves as a natural basic security criterion for secret sharing schemes: some of the pioneering papers in the area ([52], [57], [60]) openly restrict their attention to perfect schemes, while Brickell [6] even includes perfectness in his definition of a secret sharing scheme.

However, "perfect" does not automatically mean "more secure than non-perfect": even in a perfect scheme with very small key space $\mathcal{K}$, every coalition has a high probability of simply guessing the secret, while a scheme with large $\mathcal{K}$ satisfying (2.8) up to some small error can be still thought of as practically secure. This idea stands in particular behind secret sharing based on Chinese Remainder Theorem ([2], [36]).

In general, one can define a numerical value describing "how perfect" a given scheme is, by analyzing its *access function* and, for instance, taking its *gap* in the sense of [16, Definitions 2.3 and 2.6]. Together with the key space size $|\mathcal{K}|$, this kind of "perfectness rate" can be used to estimate from above the probability of guessing the secret by a non-authorized coalition. Although minimizing this probability is a crucial goal of secret sharing, there are other security aspects which should be also taken into account, as we will discuss below.

Remark 2.36. In [7], the definition of "perfect" requires only that the left-hand side of (2.8) be positive for every $k \in \mathcal{K}$. This meaning is certainly weaker in general; however, Theorem 9 of [7] ensures that it coincides with Definition 2.35 for schemes considered in [7], i.e. ones which are ideal (see Definition 2.38 below) and induce a connected access structure (see Section 2.3.3). Accordingly, Definition 5 of [53] also coincides with Definition 2.35, at least in the connected case.

Remark 2.37. It is also common to consider whether a scheme Σ is "perfect *with respect to* Γ", for a given access structure Γ. However, such definitions require in particular that $\Gamma = \Gamma(\Sigma)$, thus practically coinciding with Definition 2.35.

Wishing to maximize $|\mathcal{K}|$ in order to prevent guessing the secret, we simultaneously would like to achieve possibly small size of the share space $\mathcal{S}$. This is because the shares are confidential, which may lead to additional costs or vulnerabilities in storing or transferring them, to the extent depending on their length, which is roughly the logarithm of $|\mathcal{S}|$. This motivates the following definition.

Definition 2.38 ([57, p. 14])**.** Let $\Sigma = (D, \mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{I})$ be a secret sharing scheme which is perfect. Then:

- The *information rate* of Σ is defined as $\log_{|\mathcal{S}|} |\mathcal{K}|$;
- Σ is called *ideal* if and only if its information rate is 1, i.e. $|\mathcal{K}| = |\mathcal{S}|$.

In a perfect scheme, we must have $|\mathcal{S}| \geqslant |\mathcal{K}|$ ([57, p. 14]); therefore, 1 is the maximal possible value for information rate, and ideal schemes are those which attain this bound. Such situation clearly happens for all Brickell's schemes.

2.4.2 Access structures

Perfect schemes	general			ideal	Brickell's	Lai-Ding's	Shamir's type	Shamir's
Access structures	general	$\supsetneq$	matroid ports	$\supsetneq$ ideal	$\supsetneq$ Brickell's	$\approx$ Lai-Ding's	$\supsetneq$ Shamir's type	$\supsetneq$ threshold
Matroids	(N/A)		general		representable			uniform

Table 2.1: A summary of relations between various classes of (perfect) secret sharing schemes, access structures and matroids, discussed in Section 2.4.2. Correspondences between schemes/structures/matroids apply strictly columnwise, and empty positions represent unnamed intermediate classes of little importance. "(N/A)" in the matroid row represents the fact that some access structures do not correspond to any matroid.

The correspondence between the top two rows is unidirectional: each class of schemes determines the class of all access structures realized by those schemes. Note that, while ideal/Brickell's/Lai-Ding's/Shamir's type schemes correspond trivially to the analogously named structures just by our definitions of the latter, the correspondence between general schemes and general access structures is *not* obvious and follows from [26] or [4].

The correspondence between the bottom two rows (when both entries are shown) is defined by taking ports (see the mapping Π defined in Section 2.3.3); it is unidirectional in general (matroids determine access structures) but bidirectional under restriction to the connected case.

On the level of access structures, we show strict containments. The symbol $\approx$ indicates that the relation between Lai-Ding's and Brickell's structures is almost an equality; this will be stated in detail as Theorem 9 in Chapter 6.

The whole figure has been already known, except from the containments involving Lai-Ding's structures, which follow from Theorem 9.

Shamir's schemes have been designed to realize arbitrary threshold access structures, and no other structures; this reflects the fact that threshold structures seem to have vastly prevailed in initial practical applications (see [33, Section 3.5]). Nevertheless, they form a very special case of a much broader picture, and it is certainly desirable to design secret sharing schemes also for other structures.

Ito, Saito and Nishizeki [26] gave a construction of a secret sharing scheme realizing any given access structure, which was later simplified by Benaloh and Leichter [4]; however, the results of these constructions tend to have low information rates. This shows the value of Brickell's

schemes, which are capable of realizing a vast diversity of access structures, at the same time being all ideal.

Nevertheless, Benaloh and Leichter showed that

- There are access structures which are not *ideal*, in the sense that they do not admit any ideal scheme [4, Theorem 3].

Such structures clearly cannot be Brickell's. This naturally leads to two questions, regarding how general among all (resp. ideal) access structures are the ideal (resp. Brickell's) ones.

It turns out that this topic can be better understood by referring to the theory of matroids, discussed in Section 2.3.3. Using the terms defined there, we may state the following facts:

- All ideal and connected access structures are ports of matroids [7, Theorem 1].

  However, there exist connected ports of matroids which are not ideal [51].
- Access structures induced by Brickell's schemes over $\mathbb{F}_q$ are exactly ports of matroids representable over $\mathbb{F}_q$ (Lemma 2.7).

  Moreover, if a matroid is representable over some field, it must be also representable over some finite field [23, Lemma 7]; hence, we may conclude in short that "Brickell's access structures are ports of matroids which are representable (over some field)".
- There exist connected matroids with ideal ports which are not representable over any field [53, Sections 2 and 3].
- There also exist connected access structures which are not ports of any matroid [33, Example 6.2.6].

Altogether, the above facts build up a large part of Table 2.1; namely, the region containing Brickell's structures and the more general ones. For completeness, let us preindicate that the remaining part of this table is based on the correspondence between Shamir's schemes, threshold structures and uniform matroids (well known), the results of [55] on Shamir's type access structures (see Section 2.2.4), and our results on Lai-Ding's access structures (see Theorem 9 in Chapter 6, and Remark 4.10).

Turning back to the question of how general Brickell's structures are, we remark that this has been partially answered by providing characterization of matroids representable over small fields in terms of excluded minor list (see [65]). Nevertheless, representable matroids are far from being completely understood, leading some authors to claim simply that "there does not exist a good characterization" of Brickell's structures [40, p. 77]. More precisely, Seymour has showed that representability over $\mathbb{F}_2$ of a matroid $\mathcal{M} = (M, \mathcal{I})$ *cannot* be checked in polynomial time in terms of $|M|$ (this is the finishing remark in [50]), and Whittle claims that this observation can be easily generalized to other fields [65, Section 2, paragraph 1]. Moreover, Seymour's construction involves connected matroids. As a result, there seems to be no efficient algorithm to decide whether a given access structure is Brickell's. The author is also not aware of any algorithm deciding if an access structure is ideal (see also Remark 6.2).

2.4.3 Motivation for our research directions

The considerations of Sections 2.4.1 and 2.4.2 make it clear that both Shamir's and Brickell's schemes are worth investigation. As for the intermediate classes of Shamir's type and Lai-

Ding's schemes, they both have obviously an advantage over Shamir's schemes, in that they can handle more general access structures. However, it is not so clear what their advantages over Brickell's schemes are, and, consequently, what is the motivation for studying them.

Unfortunately, we are unable provide a "hard" motivation by indicating a practically important property of Lai-Ding's schemes which general Brickell's schemes do not have. However, we underline that the research on secret sharing is still rapidly developing, and it generally seems to acknowledge that today's pure theory is likely to become a part of tomorrow's practice. Below, we list several remarks intended to show that this general slogan might apply in particular to our topic.

Diversity of needs and schemes. Even within the basic problem of sharing a secret according to a threshold access structure, one could wish to ensure additional properties: resistance to various kinds of cheating, detecting or correcting a small number of communication errors, implementability without a trusted dealer, ability to efficiently deprive a participant of any knowledge once the shares have been dealt, etc. (For more examples and references, see [57, Chapter 10], [33, Section 3.4], and also [9]). Moreover, this list is likely to expand, as non-standard applications of secret sharing schemes are being invented (some examples and references are listed in the first paragraph of [3]).

These various needs have led many authors to develop new threshold schemes, either by subtly modifying Shamir's construction or by designing a significantly different one (e.g. [2]). Some papers ([59], [28]) even propose new schemes without indicating any benefit of using them (compared to Shamir's scheme), possibly reflecting authors' assumption that such benefits are likely to become known in the future; for instance, they might turn out to be resistant to some new cheater's strategy or other kind of attack on previously known schemes. Hence, diversity of schemes, even among threshold ones, may be regarded as valuable by itself.

This motivates our investigations of the asymptotic number of admissible tracks, as every such track gives rise to a distinct threshold scheme. Likewise, non-admissible tracks are also interesting, as they lead to new non-threshold schemes.

Cheaters and hidden identities. Tompa and Woll [60] showed that the classical k-threshold Shamir's scheme is vulnerable to a simple cheating attack: a single participant may try to deceive $k-1$ others by announcing a false value of his share (resulting in his being the only person knowing the secret), which will succeed with high probability. On the other hand, they observed that *every* choice of a false share becomes very improbable to succeed once we simultaneously shrink the key space and treat participants' identities as their private data; using terminology of [40], this produces an approximately $\frac{k}{\sqrt{q}}$-secure[5] scheme with information rate $\frac{1}{4}$.

Easily to check, this construction generalizes to Lai-Ding's schemes: a Lai-Ding's scheme $\Sigma_q^{LD}(\mathbf{c}, i)$ can be modified to be made approximately $\frac{|\mathbf{c}|}{\sqrt{q}}$-secure with information rate $\frac{1}{4}$. On the other hand, protecting general Brickell's schemes against cheating leads to information rate $\frac{1}{4n}$ with a naively generalized Tompa-Woll's method, and even worse results for the scheme described in [8]. Only after about 10 years, Padró, Sáez and Villar [40] constructed a $\frac{1}{q}$-secure version of a general Brickell's scheme having information rate $\frac{1}{2}$ (and proved impossibility of a substantial improvement). Hence, we may conclude that Lai-Ding's schemes *had had*

[5]Here and in the next paragraph, we omit the symbol Γ in the notion "(Γ, δ)-secure" of [40].

a subjective advantage over Brickell's until the appearance of [40]; analogous situations might yet arise.

Efficiency of implementation. Kogan and Tassa [27] observed that Shamir's type schemes with $i = k-1$ have an advantage over classical Shamir's schemes, in that their implementation may utilize Newton interpolation rather than Lagrange method, allowing to compute the secret in time $O(k)$ rather than $O(k^2)$ (and also using less memory). This observation has led to investigating general Shamir's type schemes in [59], which in turn was a part of motivation for [54] and the subsequent papers.

Generally, Shamir's schemes are more efficient than Brickell's, as the latter seem to require matrix inversion which needs more time than $O(k^2)$. In the case of Lai-Ding's schemes, this leads to the question whether there is an efficient dedicated method for inverting generalized Vandermonde matrices, or at least for sparse polynomial interpolation over finite fields. If such method was to be ever found, it would translate to practical relevance of Lai-Ding's schemes. While we cannot give a positive answer, we would like to remark that both these topics appear in recent research independent of secret sharing (see [1] and its references, and also [15]); however, the results which we found are either insufficient or inapplicable for our purpose.

c-admissible sets/tracks. The concept of **c**-admissibility seems to originate from [54], where it is claimed to be motivated by [59], and thus indirectly by the results of [27] discussed just above. More precisely, a remark in [54, Section 6] indicates that **c**-admissible tracks allow to construct threshold modifications of Shamir's schemes by shifting the secret from the constant term of the secret-hiding polynomial P (see the introduction to this thesis) to an "appropriate non-trivial" function of all its coefficients. The practical implications of such construction, if any, probably depend heavily on the choice of that function, and have been not studied so far.

A different motivation for studying **c**-admissible tracks appears in the concluding remarks of [45], where it is proposed to share up to k secrets simultaneously by hiding them e.g. in distinct coefficients of P, and then distributing the shares as in the original Shamir's method. This might look strange from a purely theoretical viewpoint, as the resulting scheme is "over-ideal" (with information rate k) in exchange for being substantially non-perfect. However, all the knowledge available to a coalition of $\leqslant k-1$ participants is the relation between different secrets, while every single secret still remains *totally unknown* (in the sense of Section 2.4.1). One could think of potential settings where such level of security is acceptable, and then the just mentioned "over-ideality" might turn out to be an advantage.

Chapter 3

Admissible tracks in Lai-Ding's scheme

In this chapter, we aim at generalizing (to a possibly large extent) the results from Section 2.2.3 regarding admissible tracks to the general case of Lai-Ding's schemes.

Using our knowledge on admissibility (see Section 2.2.2), we will investigate M-admissible tracks and state Theorems 1 and 2 analogous to Theorems C and D. On the other hand, we will prove that, for general Lai-Ding's schemes, it is impossible to provide an asymptotic lower bound for $N_{k,i}^{\mathrm{adm}}(n)$ of the form $q^n + Cq^{n-1} + O_{k,i,n}(q^{n-2})$, which means that Theorem E does not have a straightforward analogue; this fact will be stated as Theorem 3.

The notations of Section 1.1.2 will be extensively used. In the below formulations (and in the rest of this chapter), we consider $\mathbf{c}$ to be a sequence of exponents, with $k = |\mathbf{c}|$ and $n \geqslant k-1$. Note that we allow the case $k = 0$, i.e. $\mathbf{c} = ()$, along the explanations given in Section 1.1.1 and Remarks 1.2.

The results

Theorems 1 and 2 are given a rather complicated form in order to generalize the full strength of results from [45]. Whenever it is not necessary to achieve that, the estimates provided below can be easily weakened to obtain simpler and more elegant statements.

Theorem 1 (a generalization of Theorem C)**.** *Assume that $k \geqslant 2$ and let $0 \leqslant i \leqslant k-1$. Denote*

$$A(l) = \hat{c}_{i,l}$$

for $0 \leqslant l \leqslant k-2$ and

$$C(l) = l + \tbinom{l}{k-1}(c_{k-1} - (k-1)) + \tbinom{l}{k-2}(\hat{c}_{i,\,k-2} - (k-2))$$

for $k-1 \leqslant l \leqslant n-1$. Then, if $q > C(n-1)$, we have

$$N_{\mathbf{c},i}^{M\text{-adm}}(q,n) \quad \geqslant \quad \prod_{l=0}^{k-2}\big(q - A(l)\big) \cdot \prod_{l=k-1}^{n-1}\big(q - C(l)\big) \quad > \quad 0.$$

Theorem 2 (a generalization of Theorem D)**.** *Assume that $k \geqslant 2$ and denote*

$$B(l) = 1 + (l+1)c_{l+1} + (k-l-1)c_l - c_1 - (k-1)c_0 - l(k-1)$$

for $0 \leqslant l \leqslant k-2$ and

$$\begin{aligned} D(l) = 1 + l &+ \tbinom{l}{k-1}\big(c_{k-1} - c_0 - (k-1)\big) \\ &+ \tbinom{l}{k-2}\big((k-1)(c_{k-1}-c_0) + (c_{k-2}-c_1) - k(k-2)\big) \end{aligned}$$

for $k-1 \leqslant l \leqslant n-1$. Then, if $q > D(n-1)$, we have

$$N_{\mathbf{c}}^{M\text{-adm}}(q,n) \quad \geqslant \quad \prod_{l=0}^{k-2}\big(q - B(l)\big) \cdot \prod_{l=k-1}^{n-1}\big(q - D(l)\big) \quad > \quad 0.$$

Finally, we will prove the following observation:

Theorem 3. *Assume that $k \geqslant 2$ and let $0 \leqslant i \leqslant k-1$. Then, for fixed $\mathbf{c}, i, n$ and varying q, there exists a constant $C > 0$ such that*

$$N_{\mathbf{c},i}^{M\text{-adm}}(q,n) \geqslant q^n - Cq^{n-1} + O_{k,i,n}(q^{n-2}).$$

On the other hand, there is a choice of $\mathbf{c}, i$ and n such that there is no constant $C \in \mathbb{R}$ satisfying

$$N_{\mathbf{c},i}^{M\text{-adm}}(q,n) = q^n - Cq^{n-1} + O_{k,i,n}(q^{n-2}).$$

M- versus S-admissibility

The results obtained in this chapter have been published in [67]. However, the author regretfully admits that the exposition of that paper does not properly differentiate between the two notions of admissibility introduced in Chapter 1. This has resulted in particular in an erroneous formulation of Theorem A in [67] (corresponding to Definition 2.20 and Lemma 2.21 in here), which for $n = k-1$ requires understanding "admissible" as "M-admissible", contrary to the S-interpretation set by Definition 1.1 in [67].

However, since Theorem A is used in [67] as an obligatory first step to deal with "admissibility", it follows that all contents of that paper remain valid once we switch to the M-interpretation (as we have explicitly done in this chapter). Moreover, it turns out that the statements of all three theorems of [67] (or, equivalently, of this chapter) remain valid also under the S-interpretation, even if this does not straightforwardly apply to their proofs. Indeed, the S-variants of all these statements, except for the second claim of Theorem 3, follow easily from their M-variants together with Lemma 2.25a; on the other hand, the proof of the second claim of Theorem 3 remains valid under both interpretations, as one can verify using Lemma 4.6a.

3.1 Preliminary facts

In this section, we prove several auxiliary facts which will be used later.

In the remaining part of this chapter, $\mathbf{c}$ will always denote an increasing sequence of non-negative integers of length k.

Fact 3.1. Let $k \geqslant 1$ and $\mathbf{x} = (x_0, \ldots, x_{k-1})$ be a sequence of indeterminates in $\mathbb{F}_q$. Then for every $x \in \mathbb{F}_q$ and every $0 \leqslant j < k$ we have

$$V_{\mathbf{c}}(\mathbf{x}) = \sum_{i=0}^{k-1} (-1)^{i+j} \cdot V_{\hat{\mathbf{c}}_i}(\hat{\mathbf{x}}_j) \cdot x_j^{c_i}. \tag{3.1}$$

Proof. This is a straightforward consequence of the Laplace expansion. □

Fact 3.2. Let $\mathbf{c}$ and $\mathbf{x}$ be as in Fact 3.1. Then the polynomial $V(\mathbf{x})$ divides $V_{\mathbf{c}}(\mathbf{x})$; moreover, the quotient is divisible by $x_{k-1}^{c_0}$.

Proof. The fact that the quotient of $V_{\mathbf{c}}(\mathbf{x})$ over $V(\mathbf{x})$ exists is well known ([18, equation (A.6)]); some sources define the Schur polynomials to be quotients of that form. By Fact 3.1, the lowest x_{k-1}-degrees of monomials appearing in the expansions of these two polynomials with respect to x_{k-1} are correspondingly c_0 and 0. Hence the quotient must be divisible by $x_{k-1}^{c_0}$. □

Fact 3.3. Let $\mathbf{x}$ be as in Fact 3.1 and $\mathbf{y} \sqsubseteq \mathbf{x}$. Then $V(\mathbf{y})$ divides $V(\mathbf{x})$.

Proof. Reasoning by induction, it is sufficient to consider the case when $\mathbf{y} = \hat{\mathbf{x}}_j$ for some $0 \leqslant j < |\mathbf{x}|$. In such case, consider the expansion of $V(\mathbf{x})$ with respect to x_j provided by Fact 3.1; it follows from Fact 3.2 that every summand in this expansion is divisible by $V(\mathbf{y})$. □

While working with polynomials of the form $V_{\mathbf{c}}(x_0, \ldots, x_{k-1})$ (or their quotients) in the next sections, we will usually treat the terms $x_0, \ldots, x_{k-2}$ as fixed, thus effectively considering $V_{\mathbf{c}}(\mathbf{x})$ as a polynomial in a single variable x_{k-1}. In this setting, the divisibility properties provided by Facts 3.2 and 3.3 still apply.

3.2 Tracks of length $k - 1$

In this section, we prove Theorems 1 and 2 in the case $n = k - 1$ by developing an iterative method of choosing consecutive terms t_l so that the resulting track $\mathbf{t}$ be $(\mathbf{c}, I)$-M-admissible (see Definition 3.4). This procedure and the proof of its correctness will resemble Algorithms 3.1.1 and 3.2.1 and Lemmas 2 and 3 in [45]. The details of this correspondence will be discussed in Section 3.4.

Definition 3.4. Let $I \subseteq \mathbf{e}_k$. A track $\mathbf{t}$ is called $(\mathbf{c}, I)$-M-*admissible* if it is $(\mathbf{c}, i)$-M-admissible for every $i \in I$.

In particular, $(\mathbf{c}, \{i\})$-M-admissibility is $(\mathbf{c}, i)$-M-admissibility and $(\mathbf{c}, \mathbf{e}_k)$-$M$-admissibility is $\mathbf{c}$-M-admissibility.

Denotation 3.5. For $l \geqslant 0$ and $I \subseteq \mathbf{e}_k$, we denote by $\mathcal{A}_l^I$ the set of all tracks $\mathbf{t}$ of length l such that

$$V_{\hat{\mathbf{c}}_i[l]}(\mathbf{t}) \neq 0 \qquad \text{for every } i \in I.$$

Denotation 3.6. For $a \in \mathbb{Z}$, we denote by a^+ the number $\max(a, 0)$.

Fact 3.7. For any $I \subseteq \mathbf{e}_k$, $\mathcal{A}_0^I$ consists of the empty track (), while $\mathcal{A}_{k-1}^I$ consists exactly of $(\mathbf{c}, I)$-M-admissible tracks of length $k-1$.

Proof. The first claim is obvious; the second follows from Definition 2.20. □

Lemma 3.8. For every $0 \leqslant l < k-1$ and $\emptyset \neq I \subseteq \mathbf{e}_k$, we have

$$|\mathcal{A}_{l+1}^I| \geqslant |\mathcal{A}_l^I| \cdot \big(q - N_l + (E-1)^+\big),$$

where

$$N_l = l + \sum_{i \in I} (\hat{c}_{i,l} - l) \qquad \text{and} \qquad E = \sum_{i \in I} \hat{c}_{i,0}. \tag{3.2}$$

Proof. Let $\mathbf{t} \in \mathcal{A}_l^I$. We will look for all $t_l \in \mathbb{F}_q$ for which $\mathbf{t}' = \mathbf{t} \mid\mid (t_l)$ is a track lying in $\mathcal{A}_{l+1}^I$.

Let $i \in I$. By Fact 3.1, we have $V_{\hat{\mathbf{c}}_i[l+1]}(\mathbf{t}') = P_i(t_l)$, where

$$P_i(x) = \sum_{j=0}^{l} (-1)^{j+l} \cdot V_{\mathbf{d}_{(j)}}(\mathbf{t}) \cdot x^{\hat{c}_{i,j}} \qquad \text{and} \qquad \mathbf{d}_{(j)} = \Big(\widehat{\hat{\mathbf{c}}_i[l+1]}\Big)_j.$$

In particular, the highest coefficient of P_i is

$$V_{\mathbf{d}_{(l)}}(\mathbf{t}) = V_{\hat{\mathbf{c}}_i[l]}(\mathbf{t})$$

which is non-zero because $\mathbf{t} \in \mathcal{A}_l^I$. Thus $P_i \neq 0$. Note that $\deg P_i = \hat{c}_{i,l}$.

Now, $\mathbf{t}'$ is a track belonging to $\mathcal{A}_{l+1}^I$ if and only if

$$V(\mathbf{t} \mid\mid (t_l)) \cdot \prod_{i \in I} P_i(t_l) \neq 0. \tag{3.3}$$

Clearly, removing some repeated factors of the above polynomial will lead to an equivalent condition on t_l. In particular, using Fact 3.2, we obtain that (3.3) is equivalent to $P(t_l) \neq 0$, where

$$P(x) = V(\mathbf{t} \mid\mid (x)) \cdot \prod_{i \in I} \frac{P_i(x)}{V(\mathbf{t} \mid\mid (x))}. \tag{3.4}$$

It also follows from Fact 3.2 that $P(x)$ is divisible by $\Pi_{i \in I} x^{\hat{c}_{i,0}} = x^E$. Therefore, (3.3) is equivalent to $Q(t_l) \neq 0$, where

$$Q(x) = \left\{ \begin{matrix} \frac{P(x)}{x^{E-1}} & \text{if } E > 0 \\ P(x) & \text{if } E = 0 \end{matrix} \right\} = x^{-(E-1)^+} \cdot P(x).$$

The number of roots of the above polynomial is at most its degree, which equals

$$M = l + \sum_{i \in I} (\hat{c}_{i,l} - l) - (E-1)^+ = N_l - (E-1)^+.$$

Therefore, for every choice of $\mathbf{t} \in \mathcal{A}_l^I$, there exist at least $q - M$ choices for t_l such that $\mathbf{t} \mid\mid (t_l) \in \mathcal{A}_{l+1}^I$. This finishes the proof. □

Corollary 3.9. Let $\emptyset \neq I \subseteq \mathbf{e}_k$. Then, if $q > N_{k-2} - (E-1)^+$, the number of $(\mathbf{c}, I)$-M-admissible tracks over $\mathbb{F}_q$ of length $k-1$ is at least

$$\prod_{l=0}^{k-2} \left(q - N_l + (E-1)^+\right) > 0.$$

Proof. Use Lemma 3.8, Fact 3.7 and the fact that $N_{k-2} \geqslant N_l$ for all $l \leqslant k-2$. □

Corollary 3.10. Theorem 1 holds for $n = k-1$.

Proof. This follows from Corollary 3.9 with $I = \{i\}$ since in this case we have

$$N_l - (E-1)^+ \leqslant N_l = A(l).$$ □

Corollary 3.11. Theorem 2 holds for $n = k-1$.

Proof. By Corollary 3.9 with $I = \mathbf{e}_k$, we have

$$N_{\mathbf{c}}^{M\text{-adm}}(k-1, q) \geqslant \prod_{l=0}^{k-2} \left(q - N_l + (E-1)^+\right) \qquad \text{if} \qquad q > N_{k-2} - (E-1)^+.$$

In our case, we have

$$E = \sum_{i=0}^{k-1} \hat{c}_{i,0} = c_1 + (k-1)c_0 > 0,$$

whence $(E-1)^+ = E-1$. Similarly, for every $0 \leqslant l \leqslant k-2$ we have

$$N_l = l + \sum_{i=0}^{k-1} (\hat{c}_{i,l} - l) = -l(k-1) + \sum_{i=0}^{k-1} \hat{c}_{i,l} = -l(k-1) + (l+1)c_{l+1} + (k-l-1)c_l.$$

This implies that $N_l - (E-1)^+ = B(l)$. This finishes the proof. □

3.3 Tracks of length $\geqslant k$

In this section, we develop a procedure of extending $(\mathbf{c}, I)$-M-admissible tracks by appending to them consecutive elements, which will result in proofs of Theorems 1 and 2. In fact, we perform a straightforward generalization of Algorithms 3.1.3 and 3.2.3 and Theorems 4 and 6 from [45] in the spirit of Section 3.2 (For a discussion of this connection, see Section 3.4).

Denotation 3.12. We denote by $\mathcal{B}_l^I$ the set of $(\mathbf{c}, I)$-M-admissible tracks of length $l \geqslant 0$.

Lemma 3.13 (generalizing Theorems 4 and 6 in [45])**.** Let $\emptyset \neq I \subseteq \mathbf{e}_k$, $l \geqslant k-1$ and $\mathbf{t} \in \mathcal{B}_l^I$. Suppose that $q > \overline{N}_l - (\overline{E}_l - 1)^+$ (see Denotation 3.6), where

$$\overline{N}_l = l + \tbinom{l}{k-1}\left(c_{k-1} - (k-1)\right) + \tbinom{l}{k-2} \sum_{i \in I} \left(\hat{c}_{i,k-2} - (k-2)\right)$$

and

$$\overline{E}_l = \tbinom{l}{k-1} c_0 + \tbinom{l}{k-2} \sum_{i \in I} \hat{c}_{i,0}.$$

Then there exists $t_l \in \mathbb{F}_q$ such that $\mathbf{t} \mid\mid (t_l) \in \mathcal{B}^I_{l+1}$. The number of such t_l is at least $q - \overline{N}_l + (\overline{E}_l - 1)^+$.

Proof. The proof is similar to that of Lemma 3.8.

By Definitions 2.20 and 3.4, a track $\mathbf{x}$ of length not less than $k-1$ is $(\mathbf{c}, I)$-admissible if and only if it satisfies the following conditions:

$$V_{\mathbf{c}}(\mathbf{u}) \neq 0 \qquad \text{for all } \mathbf{u} \sqsubseteq \mathbf{x} \text{ of length } k, \tag{3.5a}$$

$$V_{\hat{\mathbf{c}}_i}(\mathbf{v}) \neq 0 \qquad \text{for all } \mathbf{v} \sqsubseteq \mathbf{x} \text{ of length } k-1 \text{ and } i \in I. \tag{3.5b}$$

Hence our assumptions imply that the conditions (3.5) hold after substituting $\mathbf{x} = \mathbf{t}$ and, on the other hand, our goal is to find many values for t_l such that they hold for $\mathbf{x} = \mathbf{t} \mid\mid (t_l)$. While checking (3.5) for all $\mathbf{u}, \mathbf{v} \sqsubseteq \mathbf{t} \mid\mid (t_l)$ of the appropriate length, all cases when $\mathbf{u} \sqsubseteq \mathbf{t}$ or $\mathbf{v} \sqsubseteq \mathbf{t}$ are satisfied by the assumption, so we may restrict to these $\mathbf{u}$ and $\mathbf{v}$ which contain t_l.

Let then $\mathbf{u} = \mathbf{u}' \mid\mid (t_l)$, where $\mathbf{u}' \sqsubseteq \mathbf{t}$ is of length $k-1$. Then by Fact 3.1 we know that $V_{\mathbf{c}}(\mathbf{u}) = P_{\mathbf{u}'}(t_l)$, where $P_{\mathbf{u}'}(x)$ is the polynomial defined by the right-hand side of (3.1); its degree is at most c_{k-1}. Similarly, if $\mathbf{v} = \mathbf{v}' \mid\mid (t_l)$ with $\mathbf{v}' \sqsubseteq \mathbf{t}$ of length $k-2$, then given some $i \in I$ we obtain a polynomial $P_{\mathbf{v}',i}(x)$ of degree at most $\hat{c}_{i,\,k-2}$ such that $V_{\hat{\mathbf{c}}_i}(\mathbf{v}) = P_{\mathbf{v}',i}(t_l)$. We will now check that all the polynomials defined above are non-zero.

For $P_{\mathbf{u}'}$, this follows from its explicit expansion formula given in Fact 3.1:

$$P_{\mathbf{u}'}(x) = \sum_{j=0}^{k-1} (-1)^{j+k-1} \cdot V_{\hat{\mathbf{c}}_j}(\mathbf{u}') \cdot x^{c_j}$$

because, for any $i \in I$, the coefficient $V_{\hat{\mathbf{c}}_i}(\mathbf{u}')$ is not zero by (3.5b) applied to $\mathbf{x} = \mathbf{t}$ and $\mathbf{v} = \mathbf{u}'$.

For $P_{\mathbf{v}',i}$, the argument is different. Since $|\mathbf{v}'| = k-2 < k-1 \leqslant |\mathbf{t}|$, there exists $t_m \in \mathbf{t}$ not belonging to $\mathbf{v}'$. Then, by Fact 3.1 applied to $\mathbf{v}' \mid\mid (t_m)$, we have

$$V_{\hat{\mathbf{c}}_i}\big(\mathbf{v}' \mid\mid (t_m)\big) = P_{\mathbf{v}',i}(t_m) \qquad \text{for every } i \in I. \tag{3.6}$$

However, $\mathbf{v}' \mid\mid (t_m)$ is a permutation of some subsequence $\mathbf{w} \sqsubseteq \mathbf{t}$ of length $k-1$; hence by (3.5b) applied to $\mathbf{x} = \mathbf{t}$ and $\mathbf{v} = \mathbf{w}$ we have $V_{\hat{\mathbf{c}}_i}\big(\mathbf{v}' \mid\mid (t_m)\big) = \pm V_{\hat{\mathbf{c}}_i}(\mathbf{w}) \neq 0$, so, by (3.6), $P_{\mathbf{v}',i} \neq 0$.

Clearly, $\mathbf{t} \mid\mid (t_l)$ is a $(\mathbf{c}, I)$-M-admissible track if and only if

$$V(\mathbf{t} \mid\mid (t_l)) \cdot \prod_{\mathbf{u}'} P_{\mathbf{u}'}(t_l) \cdot \prod_{\mathbf{v}',i} P_{\mathbf{v}',i}(t_l) \neq 0, \tag{3.7}$$

where the range of $\mathbf{u}'$, $\mathbf{v}'$, i is as described before. In this condition, we may freely remove a number of repeated factors. First, by Facts 3.2 and 3.3, we get that (3.7) is equivalent to $P(t_l) \neq 0$, where

$$P(x) = V(\mathbf{t} \mid\mid (x)) \cdot \prod_{\mathbf{u}} \frac{P_{\mathbf{u}'}(x)}{V(\mathbf{u}' \mid\mid (x))} \cdot \prod_{\mathbf{v},i} \frac{P_{\mathbf{v},i}(x)}{V(\mathbf{v}' \mid\mid (x))}. \tag{3.8}$$

Then, we note by Fact 3.2 that every quotient $\frac{P_{\mathbf{u}'}(x)}{V(\mathbf{u}'||(x))}$ (resp. $\frac{P_{\mathbf{v}',i}(x)}{V(\mathbf{v}'||(x))}$) is divisible by x^{c_0} (resp. $x^{\hat{c}_{i,0}}$). Thus $P(x)$ is divisible by $x^{\overline{E}_l}$ and, just as in the proof of Lemma 3.8, we conclude that (3.8) is equivalent to $Q(t_l) \neq 0$, where

$$Q(x) = x^{-(\overline{E}_l - 1)^+} \cdot P(x).$$

Now, the number of roots of Q is not greater than its degree, which equals $\deg P - (\overline{E}_l - 1)^+$. Further, we have

$$\deg P \leqslant l + \tbinom{l}{k-1}\big(c_{k-1} - (k-1)\big) + \tbinom{l}{k-2} \sum_{i \in I} \big(\hat{c}_{i,\,k-2} - (k-2)\big) = \overline{N}_l.$$

Therefore, if $q > \overline{N}_l - (\overline{E}_l - 1)^+$, there exists a value for t_l as desired, and the number of such values is at least $q - \overline{N}_l + (\overline{E}_l - 1)^+$. □

Corollary 3.14. Let $\emptyset \neq I \subseteq \mathbf{e}_k$. Then, if $q > \overline{N}_{n-1} - (\overline{E}_{n-1} - 1)^+$, we have

$$|\mathcal{B}_n^I| \quad \geqslant \quad \prod_{l=0}^{k-2} \big(q - N_l + (E-1)^+\big) \cdot \prod_{l=k-1}^{n-1} \big(q - \overline{N}_l + (\overline{E}_l - 1)^+\big) \quad > \quad 0,$$

where N_l and E are defined by (3.2).

Proof. This will follow immediately from Corollary 3.9 and Lemma 3.13 once we check that the sequence

$$\big(N_{k-2} - (E-1)^+\big) \,||\, \big(\overline{N}_l - (\overline{E}_l - 1)^+\big)_{l=k-1}^{n-1}$$

is non-increasing. First, note that $\overline{N}_{k-2} = N_{k-2}$ and $\overline{E}_{k-2} = E$, so it suffices to consider the values $\overline{N}_l - (\overline{E}_l - 1)^+$ for $k-2 \leqslant l \leqslant n-1$. Then, note that either $\overline{E}_l = 0$ for all $l \geqslant k-2$ or $\overline{E}_l > 0$ all for all such l. In both cases, $\big(\overline{N}_l - \overline{E}_l\big)$ is clearly non-decreasing for all $l \geqslant k-2$, therefore so is $\big(\overline{N}_l - (\overline{E}_l - 1)^+\big)$. □

Proof of Theorem 1. The theorem follows immediately from Corollary 3.14 with $I = \{i\}$ and the obvious inequalities

$$N_l - (E-1)^+ \leqslant N_l = A(l), \qquad \overline{N}_l - (\overline{E}_l - 1)^+ \leqslant \overline{N}_l = C(l).$$ □

Proof of Theorem 2. The theorem will follow immediately from Corollary 3.14 with $I = \mathbf{e}_k$ once we check that

$$N_l - (E-1)^+ = B(l) \qquad \text{for } 0 \leqslant l \leqslant k-2, \tag{3.9a}$$

$$\overline{N}_l - (\overline{E}_l - 1)^+ = D(l) \qquad \text{for } k-1 \leqslant l \leqslant n-1. \tag{3.9b}$$

We have proved in Corollary 3.11 that (3.9a) holds and also that $E > 0$. Hence $\overline{E}_l \geqslant \binom{l}{k-2} E > 0$ for all $l \geqslant k-1$, which means that $(\overline{E}_l - 1)^+ = \overline{E}_l - 1$. Then (3.9b) follows from a simple calculation involving the identity

$$\sum_{i=0}^{k-1} \hat{c}_{i,\,k-2} - \hat{c}_{i,\,0} = (k-1)(c_{k-1} - c_0) + (c_{k-2} - c_1).$$

This finishes the proof. □

3.4 Further remarks

We finish this chapter with a few slightly digressive remarks. The first of them has been stated at the beginning of the chapter as Theorem 3 due to its correspondence to Theorem E; it will now be proved. In the next two subsections, we investigate the similarities and differences between our paper and the aforementioned content of [45]; in particular, we discuss the possibilities of generalizing the algorithms given there. Finally, we give some examples showing that neither our estimates nor building procedures are ultimately precise.

3.4.1 Proof of Theorem 3

The first claim is a straightforward consequence of Theorem 1. Indeed, for fixed $\mathbf{c}, i, k$ and varying q, the right-hand side in the lower bound for $N_{\mathbf{c},i}^{M\text{-adm}}(q,n)$ provided by the theorem is of the form $P(q)$, where $P(x)$ is a polynomial with expansion

$$P(x) = x^n - \Big(\sum_{l=0}^{k-2} A(l) + \sum_{l=k-1}^{n-1} C(l)\Big)x^{n-1} + \ldots = x^n - Cx^{n-1} + O(x^{n-2}),$$

with C denoting the sum in parentheses.

For the second part, we take $\mathbf{c} = (0,1,3)$, $i = 1$ and $n = 2$. Then, by definition, $\mathbf{t} \in \mathbb{F}_q^2$ is a $(\mathbf{c}, i)$-M-admissible track if and only if $t_0^3 \neq t_1^3$. We recall that the multiplicative group $\mathbb{F}_q^\times$ is cyclic of order $q-1$. Hence, for a given t_0, the number of $t_1 \in \mathbb{F}_q$ satisfying $t_0^3 \neq t_1^3$ is

$$\begin{cases} q-1 & \text{if } t_0 = 0 \text{ or } 3 \nmid (q-1), \\ q-3 & \text{otherwise,} \end{cases}$$

which implies that

$$N_{\mathbf{c},i}^{M\text{-adm}} = \begin{cases} q^2 - q & \text{if } 3 \nmid (q-1), \\ q^2 - 3q + 2 & \text{if } 3 \mid (q-1). \end{cases}$$

This cannot be expressed in the form $q^2 + Cq + O(1)$ for any constant C. (Here we use the fact that both conditions $3 \nmid (q-1)$ and $3 \mid (q-1)$ are satisfied by infinitely many prime powers, which is clearly true even when considering only the powers of two). □

3.4.2 Relation between [45] and Sections 3.2 and 3.3

The closest correspondence between [45] and our work occurs in Lemma 3.13. The key difference between it and Theorems 4 and 6 in [45] comes from the fact that, for Shamir's type schemes (i.e. for $\mathbf{c} = \mathbf{e}_k$), any quotient of the form $V_{\mathbf{c}}(\mathbf{t})/V(\mathbf{t})$ becomes just 1, while the quotients of the form $V_{\hat{\mathbf{c}}_i}/V$ can be described by the following formula (see [54, Lemma 3.2]):

$$\frac{V_{\hat{\mathbf{e}}_{k,i}}(\mathbf{t})}{V(\mathbf{t})} = \tau_{k-1-i}(\mathbf{t}), \tag{3.10}$$

where τ_j is the j-th elementary symmetric polynomial. The proof of Lemma 3.13 is an almost straightforward translation of the two proofs from [45], with τ_{k-1-i} replaced by $V_{\hat{\mathbf{c}}_i}/V$, and $V_{\mathbf{c}}/V$ taken into consideration.

The correspondence between Lemma 3.8 and [45] is not as close. Lemma 3.8 allows building tracks $\mathbf{t}$ so that $\mathbf{t}[l] \in \mathcal{A}_l^I$ for every l; on the other hand, the invariant of Algorithm 3.1.1 in [45] is that $\tau_{k-1-i}(\mathbf{t}[l]) \neq 0$ for $l \geqslant k-1-i$; this requires forcing $t_l \neq 0$ for $l < k-1-i$. These two invariants are not equivalent: putting $\mathbf{c} = \mathbf{e}_k$ and $I = \{i\}$ we obtain that $\mathcal{A}_l^{\{i\}}$ consists of all tracks for $l \leqslant i$ and of all tracks $\mathbf{t}$ satisfying $\tau_{l-i}(\mathbf{t}) \neq 0$ for $l > i$.

The difference originates from the expansion of $\tau_\alpha(\mathbf{t} \mid\mid (t_l))$ along t_l (for $l > 0$ and $\alpha \in \mathbb{Z}$):

$$\tau_\alpha(\mathbf{t} \mid\mid (t_l)) = t_l \cdot \tau_{\alpha-1}(\mathbf{t}) + \tau_\alpha(\mathbf{t}).$$

In both methods, the existence of t_l such that $\tau_\alpha(\mathbf{t} \mid\mid (t_l)) \neq 0$ is ensured by requiring the polynomial on the right-hand side to be non-zero. In the algorithms in [45], this is achieved by controlling the constant term; in Lemma 3.8, as well as in Lemma 2 in [45], the highest coefficient is traced.[1] This approach seems slightly better in that it does not require $t_l \neq 0$ for small l. For this reason, Lemma 2 in [45] provides a somehow stronger estimate than could be easily deduced from Algorithm 3.1.1 given there. Lemma 3.8 in the current paper generalizes this benefit.

3.4.3 Constructing admissible tracks

The fact that the right-hand side of (3.10) is linear with respect to every t_l allowed the authors in [45] to translate the procedures of building and extending $(\mathbf{e}_k, i)$-M-admissible and $\mathbf{e}_k$-M-admissible tracks into four algorithms of high efficiency. In their paper, the extending algorithms 3.1.3 and 3.2.3 are closely connected to Theorems 4 and 6 and their proofs; similarly, the building algorithms 3.1.1 and 3.2.1 are somehow related to Lemmas 2 and 3 but in this case the connection is not so straightforward, as we pointed out in Section 3.4.2.

In an analogous fashion, we can turn Lemmas 3.8 and 3.13 into two procedures of building and extending $(\mathbf{c}, I)$-M-admissible tracks for Lai-Ding's schemes, generalizing the algorithms from [45]. Their correctness follows immediately from the proofs of the corresponding lemmas. However, as the polynomials appearing in them (see the steps numbered 1.1 below) have unbounded degrees, determining the sets $\mathcal{S}_l$ is computationally much harder than it was in [45]. For this reason, we do not explicitly call our procedures algorithms.

Procedure 1. (building procedure; cf. Lemma 3.8)

IN: $\mathbf{c}$ and I as in Lemma 3.8
OUT: a $(\mathbf{c}, I)$-M-admissible track $\mathbf{t}$

1. For $l = 0$ to $k-2$, do the following:
   1.1. Set $\mathcal{S}_l \leftarrow$ the set of roots of any of P_i $(i \in I)$ defined in the proof of Lemma 3.8.
   1.2. Select t_{l+1} as an arbitrary element of $\mathbb{F}_q \setminus (\{t_0, \ldots, t_l\} \cup \mathcal{S}_l)$.
2. Return $\mathbf{t}$.

[1] Actually, in Lemma 3.8 we expand $V_{\hat{\mathbf{c}}_i}$ rather than $V_{\hat{\mathbf{c}}_i}/V$, but this is not an essential difference.

Procedure 2. (extending procedure; cf. Lemma 3.13)

IN: $r > 0$ and a $(\mathbf{c}, I)$-M-admissible track $\mathbf{t}$ of length $m \geqslant k-1$
OUT: $\mathbf{t}' = (t_m, \ldots, t_{m+r-1})$ such that $\mathbf{t} \mid\mid \mathbf{t}'$ is a $(\mathbf{c}, I)$-M-admissible track

1. For $l = m-1$ to $m+r-2$, do the following:
   1.1. Set $\mathcal{S}_l \leftarrow$ the roots of any of $P_{\mathbf{u}'}$ and $P_{\mathbf{v}',i}$ (for suitable $\mathbf{u}'$, $\mathbf{v}'$ and $i \in I$) defined in the proof of Lemma 3.13.
   1.2. Select t_{l+1} as an arbitrary element of $\mathbb{F}_q \setminus (\{t_0, \ldots, t_l\} \cup \mathcal{S}_l)$.
2. Return $\mathbf{t}'$.

Remark 3.15. There are at least two methods to compute efficiently the quotients of the form $S = V_{\mathbf{c}}/V$. If $\mathbf{c}$ is dense (i.e. $c_{k-1} \approx k$), it is profitable use the "Giambelli equality" already mentioned at the end of Section 1.1.4 ([18, equation (A.6)]; also [54, Lemma 3.1]), which expresses S as the determinant of a matrix of size $c_k - k$ filled with appropriate elementary symmetric polynomials in $t_0, t_1, \ldots$. For such determinants, an expansion formula analogous to Fact 3.1 can be proved, which makes them "reusable" during an iterative application of Lemma 3.8. On the other hand, if $\mathbf{c}$ is sparse (i.e. $c_{k-1} \gg k$), it could be more efficient to work directly with the generalized Vandermonde determinant $V_{\mathbf{c}}$ than with its factors.

3.4.4 (Im)precision of the results

The estimates provided in Theorems 1 and 2 are clearly not exhaustive since the factors of $P(x)$ listed in (3.4) could share some roots (apart from 0), which would reduce the overall number of roots of P. (The same applies also to (3.8)). For an easy example, take $q = 2$, $\mathbf{c} = \mathbf{e}_3$, $I = \{1\}$, $l = 1$ and $\mathbf{t} = (1)$; then we have

$$\frac{P_1(x)}{V(\mathbf{t} \mid\mid (x))} = \frac{V_{(0,2)}(\mathbf{t} \mid\mid (x))}{V(\mathbf{t} \mid\mid (x))} = x + 1 = V(\mathbf{t} \mid\mid (x)).$$

A more interesting question is whether Procedures 1 and 2 generate all $(\mathbf{c}, I)$-M-admissible tracks even though we cannot precisely count them. This is true for Procedure 2 because its invariant requires only that $\mathbf{t}[l]$ be $(\mathbf{c}, I)$-M-admissible tracks for $k \leqslant l \leqslant n$, which is clearly necessary for $\mathbf{t}$ to be such track. Therefore the procedure produces all M-admissible extensions of a given M-admissible track; the same applies to Algorithms 3.1.3 and 3.2.3 in [45] which it generalizes.

However, Procedure 1 rejects certain M-admissible tracks because its invariant $\mathbf{t}[l] \in \mathcal{A}_l^I$ (inspired by Lemma 2 in [45]) is too strong. The same applies to Algorithms 3.1.1 and 3.2.1 in [45] even though they use another invariant. For some examples, take $q = 5$, $\mathbf{c} = \mathbf{e}_5$ and $I = \{2\}$; then:

- $\mathbf{t} = (0, 1, 2, 3)$ is accepted by Procedure 1 but rejected by Algorithm 3.1.1 in [45] because $t_0 = 0$,
- $\mathbf{u} = (3, 2, 0, 1)$ is accepted by Algorithm 3.1.1 in [45] but rejected by Procedure 1 because $(3, 2, 0) \notin \mathcal{A}_3^{\{2\}}$,
- $\mathbf{v} = (0, 2, 3, 1)$ is rejected by Procedure 1 because $(0, 2, 3) \notin \mathcal{A}_3^{\{2\}}$ and rejected by Algorithm 3.1.1 in [45] because $v_0 = 0$, even though it is $(\mathbf{e}_5, 2)$-M-admissible.

The above examples demonstrate the general fact that permuting a track does not influence its admissibility, even if it matters for its acceptability in either of our building procedures.

For $I = \{i\}$, it turns out that both Algorithm 3.1.1 in [45] and Procedure 1 have the property that every $(\mathbf{c}, I)$-M-admissible track has an accepted permutation; this follows correspondingly from [56, Proposition 7] and from Lemma 3.16 stated below.

For $I = \mathbf{e}_k$, the question seems to be harder, especially in the case of Procedure 1.

Lemma 3.16. Let $0 \leqslant i < k$, $0 < l < k$ and $\mathbf{t} \in \mathcal{A}_l^{\{i\}}$. Then there exists $\mathbf{u} \sqsubseteq \mathbf{t}$ of length $l-1$ which belongs to $\mathcal{A}_{l-1}^{\{i\}}$.

Proof. By the assumption we have $V_{\hat{\mathbf{c}}_i[l]}(\mathbf{t}) = 0$, i.e. the matrix $\left[t_a^{\hat{c}_{i,b}}\right]_{0 \leqslant a,b < l}$ has rank l. Therefore its sub-matrix $\left[t_a^{\hat{c}_{i,b}}\right]_{0 \leqslant a < l,\ 0 \leqslant b < l-1}$ has rank $l-1$, whence it must contain a non-zero minor of size $l-1$. Thus there exists some $0 \leqslant j < l$ such that

$$V_{\hat{\mathbf{c}}_i[l-1]}(\hat{\mathbf{t}}_j) = \det\left[(\hat{t}_{j,a})^{\hat{c}_{i,b}}\right]_{0 \leqslant a,b < l-1} \neq 0.$$

Then $\mathbf{u} = \hat{\mathbf{t}}_j$ belongs to $\mathcal{A}_{l-1}^{\{i\}}$, which finishes the proof. □

Chapter 4

Asymptotics of max-length privileged tracks

Having discussed admissible tracks in Chapter 3, we now turn towards investigating non-admissibility (or, more precisely, non-S-admissibility) in Lai-Ding's schemes, with a general aim of extending the results obtained in prior publications for the case of Shamir's type schemes (which we discussed in Section 2.2.3). Within this topic, following the spirit of [56] and some of the other papers, we will focus on two aspects:

(i) asymptotic estimates for the number of non-admissible tracks, and

(ii) conditions sufficient for their existence (including lower bounds for q),

where in both aspects the parameters $\mathbf{c}, i$ are treated as fixed and q as varying (which matters particularly for the sense of "asymptotic"). However, we decided to restrict our attention exclusively to non-S-admissible tracks of length $|\mathbf{c}|-1$ (for reasons explained in Section 4.1.2), which in Section 2.2.1 have been called *max-length privileged*.

In several special cases, we also describe the asymptotic behaviour of *zero-free* max-length privileged tracks; this is intended to correspond to prior results, including Theorem F, and turns out to aid in formulating the classifications of our Theorems 4 and 5. However, in the more general treatment (in Section 4.5 and Chapter 5), restricting to zero-free tracks seems to be more laborious (in particular, to require finding upper bounds for the number of non-max-length privileged coalitions; cf. Fact 4.2a and Section 4.1.2) and, at the same time, rather unnatural. Hence, we will not consider it in the general case.

For convenient formulation of our results, we introduce the following definition.

Definition 4.1. A sequence of exponents $\mathbf{c}$ of length $k \geqslant 3$ will be called *step-coprime* if

$$\gcd(c_{l+1} - c_l,\ c_{l+2} - c_{l+1}) = 1 \qquad \text{for all } 0 \leqslant l \leqslant k-3. \tag{4.1}$$

A general classification. As already announced in the introduction, the problem (i) will be solved for all Lai-Ding's schemes by classifying them into the templates (T1), (T2*) and (T3) defined there. More precisely, the solution consists of four independent cases:

- $k = 1$: (T1);
  (max-length $(\mathbf{c}, i)$-privileged tracks cannot exist by Fact 2.18)

- $k = 2$: (T1) or (T2);
  (this is a special case of Theorem 5 in Section 4.4)
- $k \geqslant 3$ and $\hat{\mathbf{c}}_i$ is an arithmetic progression: (T1), (T2′) or (T3);
  (see Theorem 4 and Remark 4.11 in Section 4.3)
- the remaining case: (T2*); possibly reducing to (T2′) or even (T2).
  (see Theorem 6 in Chapter 5)

Precise bounds. As for (ii), due to the overall complexity of the problem (see Section 4.1.1), we have managed to exclude (T2*) by providing lower bounds for q of the "RSL" type (as defined in the introduction) only for three selected classes of pairs $(\mathbf{c}, i)$:

- when $k \geqslant 3$ and $\hat{\mathbf{c}}_i$ is an arithmetic progression;
  (see Theorem 4 in Section 4.3; note that this covers all pairs $(\mathbf{c}, i)$ for $k = 3$)
- when $k \geqslant 2$ and $\mathbf{c}$ is an arithmetic progression;
  (see Theorem 5 in Section 4.4; note that this covers all pairs $(\mathbf{c}, i)$ for $k = 2$)
- when $k \geqslant 4$, $\hat{\mathbf{c}}_i$ is not arithmetic, and it is step-coprime.
  (see Theorem 8 in Chapter 5)

This constitutes the partial classification into (T1), (T2′) and (T3), announced in the introduction to this thesis.

The first case is the only one which uses purely elementary methods; the remaining two rely on Weil's theorem (see Section 1.2.2). While the last class is far more general than the two preceding, dealing with it will require much more effort (Section 4.5 and the whole Chapter 5).

Organization of the chapter. Section 4.1 is intended mainly to explain our choice of topics taken; it may be read before as well as after the rest of the chapter. Section 4.2 contains auxiliary tools, used for slight technical simplifications of further proofs. In the two following sections, we deal correspondingly with the first two special cases of $(\mathbf{c}, i)$ listed above.

In the last section, we design a general roadmap (summarized in Lemma 4.28) of estimating $N_{\mathbf{c},i}^{\text{max-priv}}(q)$ with the help of Weil's Theorem B and Schmidt's Lemma 4.26, under a set of assumptions which seem to be fairly weak but turn out to be rather hard to verify in practice. This method will be used in Chapter 5 to handle the third case in the above list.

4.1 Introductory remarks

4.1.1 General complexity of the problem

As explained in Section 2.2.2, admissibility of a track $\mathbf{t}$ of length n is connected (or even equivalent, in the case $n \geqslant k$) to non-vanishing of a set of Schur polynomials on certain sub-tracks of $\mathbf{t}$; conversely, describing non-admissible tracks is connected to describing sets of zeroes of these polynomials.

This task is particularly simple for Shamir's type schemes, for which Lemma 1.5 ensures that all the polynomials under consideration are elementary symmetric polynomials τ_j, for some appropriate values of j. Compared to other Schur polynomials, the crucial advantage

of the symmetric polynomials τ_j is being of degree 1 with respect to every variable (not to be confused with their total degree, which may be higher). This property, expressed in the inductive formula

$$\tau_j(\mathbf{x}) = x_n \cdot \tau_{j-1}(\hat{\mathbf{x}}_n) + \tau_j(\hat{\mathbf{x}}_n) \qquad \text{for } j \in \mathbb{Z},\ \mathbf{x} \in \mathbb{F}_q^n, \tag{4.2}$$

remains in the center of all algorithms for constructing and extending admissible or non-admissible tracks in [45] and [56], as it allows choosing x_n to obtain any desired value of $\tau_j(\mathbf{x})$ (should it be either zero or non-zero), requiring only relatively mild additional assumptions, for example, that $\tau_{j-1}(\hat{\mathbf{x}}_n)$ is not zero.

For more complicated Schur polynomials, which are no longer linear in any of their variables, this strategy can be generalized as long as we want to construct *non-zeroes* of such polynomials; this has been successfully done in the previous chapter. However, there seems to be no easy way to construct inductively *zeroes* of $S_{\mathbf{c}}$. In the general case, we have not found a better method of describing these zeroes than using Weil's theorem (see Section 1.2.2), which yields just an asymptotic estimate of their number, without any output of a strictly constructive nature. Moreover, verifying the assumptions of this theorem is a laborious task by itself, as we will see in Section 4.4 and in Chapter 5.

4.1.2 Restricting to max-length privileged tracks

As the factors described above have added much complexity to our considerations, we decided to simplify them by restricting attention to max-length privileged tracks. This reflects an analogous restriction of the content of Section 3 of [56], including its results which we have quoted in Section 2.2.3 as Theorem F.

In the case of Shamir's type schemes, focusing on max-length privileged tracks seems particularly reasonable: they turn out to form the "basis" for all longer non-admissible tracks, in the sense that a track of length $\geqslant k$ is non-S-admissible if and only if it contains a max-length privileged sub-track (see [56, Proposition 2]). Hence, the bounds provided by Theorem F for the class of max-length privileged zero-free tracks can be actually translated to the class of non-admissible tracks of length $n \geqslant k$: for example, one may first restrict to tracks which are *minimal* in the sense of having no privileged proper sub-tracks (whose number must also satisfy the asymptotic estimate of Theorem F [1]) and then apply the extending procedure for such tracks described in [56, Section 4], whose "non-colliding" property allows to avoid the problem of counting a single extension many times, leading to the conclusion that (under the assumptions of Theorem F) $N_{k,i}^{\text{non-adm}}(q,n) = \Theta_{k,i}(q^{n-1})$ for $n \geqslant k-1$. (For Shamir's type schemes, this conclusion actually follows already from Corollary 2.30; however, the just described strategy of proof is somewhat more elementary, and should be easier to generalize).

[1] This can be deduced as follows. A privileged track $\mathbf{t}$ has a proper privileged sub-track if and only if $\hat{\mathbf{t}}_s$ is privileged for some $0 \leqslant s \leqslant k-2$, which by [55, Theorem 1] happens if and only if $\hat{\mathbf{t}}_s$ is a common zero of τ_j and τ_{j-1}, where $j = k-1-i \leqslant k-2$ (the case $i=0$ is excluded, as it admits no privileged tracks). If $j < k-2$, then both these polynomials are irreducible over $\mathbb{F}_q$ (and therefore coprime), as they have degree 1 in each of their variables, and are not divisible by any monomial. If $j = k-2$, then $\tau_j(\hat{\mathbf{x}}_s) = \prod_{s' \neq s} t_{s'}$ is clearly reducible, but it still must be coprime with $\tau_{j-1}(\hat{\mathbf{x}}_s)$. In either case, by a result which we will cite in Section 4.5 as Lemma 4.26, the number of possible choices for $\hat{\mathbf{t}}_s \in \mathbb{F}_q^{k-2}$ is bounded as $O_{k,i}(q^{k-4})$; since every such track can correspond to at most $(q-1)\cdot(k-1)$ choices of $\mathbf{t}$, the number of possible choices for a "bad" track $\mathbf{t}$ is $O_{k,i}(q^{k-3})$. This vanishes when subtracted from the bound $\Theta_{k,i}(q^{k-2})$ coming from Theorem F.

Translating the above strategy to general Lai-Ding's schemes is complicated by at least three issues. First, non-admissible tracks are in general not exhausted by super-tracks of the max-length privileged ones. (This is because general Lai-Ding's schemes, unlike those of Shamir's type, may feature non-authorized tracks of length $\geqslant k$). Second, the application of Lemma 4.26 mentioned in the footnote to the previous paragraph will now require that two general Schur polynomials be coprime, which can be hard to verify over a finite field (this will be partially dealt with in Sections 5.2.1, 5.3.4 and 5.5.4). Last, although the extending procedure of [56, Section 4] seems essentially portable to Lai-Ding's schemes, analogously to what we did in Chapter 3, its general variant would certainly require non-M-admissible (rather than non-S-admissible) tracks on its input; in general, this makes a difference, as we have shown in Remark 2.24.

We believe that, at least for a "generic" choice of $\mathbf{c}$ and i, all these issues are not important for the asymptotics, by which we mean that the corrections to the number $N^{\text{non-adm}}_{\mathbf{c},i}(q,n)$ induced by them are $O_{\mathbf{c},i}(q^{n-2})$, so that the estimate

$$N^{\text{non-adm}}_{\mathbf{c},i}(q,n) = \Theta_{\mathbf{c},i}(q^{n-1}) \qquad\qquad (n \geqslant k-1)$$

would still hold. Nevertheless, to avoid getting involved in too many technical details, we leave this topic without further discussion.

Finally, we should mention non-max-length privileged tracks, investigated in [55] and discussed in Section 2.2.4. Basically, such tracks are described by zeroes of *systems* of Schur polynomials: for Shamir's type schemes, it suffices to take one system of appropriate τ_j's (see [55, Theorem 1]), while in general we probably need to take a Boolean combination of many systems (as suggested by Fact 2.18). In either case, quantitative analysis of such systems seems not straightforward; a suitable analogue of Theorem B, known as Lang-Weil Theorem [30], requires irreducibility (over $\overline{\mathbb{F}_q}$) not only of all the polynomials considered, but also of the algebraic set defined by them (plus control over its dimension). By now, we do not know of any technique of verifying such condition for Schur polynomials, or even for the elementary symmetric polynomials τ_j. If we could do this, it would probably follow in "generic" cases that the number of $(\mathbf{c},i)$-privileged tracks of length $r < k-1$ over $\mathbb{F}_q$ is $\Theta_{\mathbf{c},i}(q^{2r-k})$. However, the non-existential results of [55], cited here as Theorem G(a-b), show that this program must fail in many cases even for Shamir's type schemes.

As a result, we are generally unable to provide any asymptotic estimates of the above form (even in the Shamir's type case); for analogous reasons, we will also refrain from the question of existence of non-max-length privileged tracks. The only exception is the simplest of our special cases (i.e. $\hat{\mathbf{c}}_i$ arithmetic), investigated in Section 4.3; the results obtained there will serve as the basis for the investigation of related access structures in Section 6.2.2. Notably, the behaviour of non-max-length privileged tracks in this case differs significantly from the behaviour predicted for Shamir's type schemes by Theorem G (see Remark 4.10).

4.2 Preliminary facts

In the sequel, we assume that $\mathbf{c}$ is a sequence of exponents of length $k \geqslant 0$, and q is a prime power.

4.2.1 Tracks containing zero

While describing authorized tracks in a particular scheme, we will often find it convenient to restrict our attention to zero-free tracks. The following fact explains how to classify the tracks which contain 0. (Every such track has the form $(0) \parallel \mathbf{u}$ up to a permutation, which is an insignificant modification).

Fact 4.2. Let $\mathbf{t} = (0) \parallel \mathbf{u}$ be a track over $\mathbb{F}_q$. Then the following holds in the access structure $\Gamma_q^{LD}(\mathbf{c}, i)$:

- **(a)** If $c_0 > 0$, then $\mathbf{t}$ is authorized if and only if $\mathbf{u}$ is;
- **(b)** If $c_0 = 0$ and $i > 0$, then $\mathbf{t}$ is authorized if and only if $\mathbf{u}$ is authorized in $\Gamma_q^{LD}(\mathbf{c}', i')$, where $\mathbf{c}' = \hat{\mathbf{c}}_0$ and $i' = i - 1$;
- **(c)** If $c_i = 0$, then $\mathbf{t}$ is authorized.

Proof. The fact follows from considering the matrix

$$VM_{\mathbf{c}}(\mathbf{t}) = \left[\begin{array}{c|c} 0^{c_0} \quad \dots \quad 0^{c_{k-1}} & \\ \hline & VM_{\mathbf{c}}(\mathbf{u}) \\ & \end{array}\right].$$

If $c_0 > 0$, then the first row is zero, and **(a)** follows by Fact 2.17. Otherwise, we have

$$VM_{\mathbf{c}}(\mathbf{t}) = \left[\begin{array}{c|c|c} 1 & 0 \quad \dots \quad 0 & \\ \hline 1 & & \\ \vdots & \multicolumn{2}{c}{VM_{\hat{\mathbf{c}}_0}(\mathbf{u})} \\ 1 & & \end{array}\right].$$

If $i = 0$, then $\mathbf{t}$ is authorized by Fact 2.17; this gives **(c)**. Otherwise we have

$$\operatorname{rank} VM_{\mathbf{d}}(\mathbf{t}) = 1 + \operatorname{rank} VM_{\hat{\mathbf{d}}_0}(\mathbf{u}) \qquad \text{for } \mathbf{d} \in \{\mathbf{c}, \hat{\mathbf{c}}_i\},$$

which by Fact 2.18 implies the claim of **(b)**. □

Corollary 4.3. If $c_i = 0$ and $q \geqslant k \geqslant 2$, then max-length $(\mathbf{c}, i)$-privileged tracks over $\mathbb{F}_q$ exist.

Proof. If $c_i = 0$, then, by Fact 4.2, every track of length $k - 1$ starting with zero is $(\mathbf{c}, i)$-privileged. If $q \leqslant k$, such tracks certainly exist. □

4.2.2 Negative exponents

We recall from Remark 2.10 that, by excluding 0 from the set of participants, it becomes eligible to allow negative entries in the sequence $\mathbf{c}$. It is easy to check that Facts 2.17 and 2.18 hold in this setting. This allows formulating the following fact.

Fact 4.4. Let $\mathbf{c}$ be a sequence of exponents, $0 \leqslant i < k$, $l \in \mathbb{Z}$, and let $\mathbf{t}$ be a zero-free track. Then $\mathbf{t}$ is $(\mathbf{c}, i)$-authorized if and only if it is $(\mathbf{c} + l, i)$-authorized.

Proof. Since $\mathbf{t}$ is zero-free, for any increasing sequence of integers $\mathbf{d}$, the matrices $VM_{\mathbf{d}+l}(\mathbf{t})$ and $VM_{\mathbf{d}}(\mathbf{t})$ differ only by elementary row operations, so they have equal rank. Since $\widehat{(\mathbf{c}+l)}_i = \hat{\mathbf{c}}_i + l$, the claim follows from (generalized) Fact 2.18. □

4.3 The case of $\hat{\mathbf{c}}_i$ arithmetic

In this section, we consider a Lai-Ding's scheme $\Sigma_q^{LD}(\mathbf{c}, i)$ in the case when $\hat{\mathbf{c}}_i$ is an arithmetic progression.

Throughout the whole section, we denote by l the common difference of $\hat{\mathbf{c}}_i$; we assume that $k \geqslant 3$ so that l is well defined. (The case $k = 2$ may be freely ignored now, as it will be completely covered by Section 4.4). Also, we denote

$$m = c_i - \hat{c}_{i,0}. \tag{4.3}$$

As it will turn out, the behaviour of privileged tracks will mostly depend on the residue of m modulo l, which might be thought of a measure to what extent (if at all) the whole sequence $\mathbf{c}$ fails to be arithmetic.

The auxiliary Section 4.3.1 develops criteria for being authorized which will be used in the next section to obtain our main result, Theorem 4. Meanwhile, we also investigate the existence and asymptotic number of non-max-length privileged tracks; this knowledge will be used in Chapter 6.

4.3.1 Criteria for being authorized

Fact 4.5. Let $k, r > 0$ and let $\mathbf{x}$ be any sequence in $\mathbb{F}_q^r$ (not necessarily a track). Then

$$\operatorname{rank} VM_{\mathbf{e}_k}(\mathbf{x}) = \min(k, s),$$

where s is the number of pairwise distinct elements appearing in $\mathbf{x}$.

Proof. Let $\mathbf{y} \sqsubseteq \mathbf{x}$ be a track of length s. Then, $VM_{\mathbf{e}_k}(\mathbf{x})$ has the same rank as $VM_{\mathbf{e}_k}(\mathbf{y})$ because both matrices have the same set of rows. Now, $VM_{\mathbf{e}_k}(\mathbf{y})$ is of size $k \times s$, and either contains or is contained in a non-singular matrix $VM_{\mathbf{e}_s}(\mathbf{y})$ of size $s \times s$. In either case, its rank is $\min(k, s)$, q.e.d. □

Lemma 4.6. Let $\mathbf{c}$ be a sequence of exponents of length $k \geqslant 3$ and suppose that $\hat{\mathbf{c}}_i$ is an arithmetic progression with common difference l. Denote $m = c_i - \hat{c}_{i,0}$. Then:

(a) A zero-free track $(t_0, t_1) \in \mathbb{F}_q^2$ is authorized if and only if

$$(t_0 t_1^{-1})^m \neq (t_0 t_1^{-1})^l = 1; \tag{4.4}$$

(b) A zero-free track $\mathbf{t}$ is authorized if and only if at least one of the following holds:
- (i) $\mathbf{t}$ contains an authorized track of length 2;
- (ii) $\mathbf{t}$ contains a track $\mathbf{u}$ of length k such that $V_{\mathbf{c}}(\mathbf{u}) \neq 0$.

(c) A track $\mathbf{t} = (0) \,||\, \mathbf{u}$ of length $1 \leqslant r < k$ is authorized if and only if $\mathbf{u}$ is authorized or $c_i = 0$.

Proof. By Fact 4.4, while considering parts **(a-b)** we may assume without loss of generality that $\hat{c}_{i,0} = 0$. (In the case when $i = 0$, this will make c_0 negative, which still makes sense since we consider only zero-free tracks; see Section 4.2.2). Then, for every zero-free track $\mathbf{t}$ over $\mathbb{F}_q$, we have

$$VM_{\hat{\mathbf{c}}_i}(\mathbf{t}) = VM_{l\cdot\mathbf{e}_{k-1}}(\mathbf{t}) = VM_{\mathbf{e}_{k-1}}(\mathbf{t}^l). \tag{4.5}$$

(a) By Fact 2.18, a zero-free track $\mathbf{t} = (t_0, t_1)$ is authorized if and only if

$$\operatorname{rank}\left[\begin{array}{cccc|c} 1 & t_0^l & \dots & t_0^{l(k-2)} & t_0^m \\ 1 & t_1^l & \dots & t_1^{l(k-2)} & t_1^m \end{array}\right] > \operatorname{rank}\left[\begin{array}{cccc} 1 & t_0^l & \dots & t_0^{l(k-2)} \\ 1 & t_1^l & \dots & t_1^{l(k-2)} \end{array}\right]$$

Since the matrix on the right-hand side is not zero, this is equivalent to

$$\operatorname{rank}\left[\begin{array}{cccc|c} 1 & t_0^l & \dots & t_0^{l(k-2)} & t_0^m \\ 1 & t_1^l & \dots & t_1^{l(k-2)} & t_1^m \end{array}\right] = 2, \qquad \operatorname{rank}\left[\begin{array}{cccc} 1 & t_0^l & \dots & t_0^{l(k-2)} \\ 1 & t_1^l & \dots & t_1^{l(k-2)} \end{array}\right] = 1,$$

which is clearly equivalent to (4.4).

(b) The condition (i) is clearly sufficient for $\mathbf{t}$ to be authorized. If $\mathbf{u}$ is a track of length k as in (ii), then we have

$$\operatorname{rank} VM_{\hat{\mathbf{c}}_i}(\mathbf{u}) \leqslant |\hat{\mathbf{c}}_i| < k = \operatorname{rank} VM_{\mathbf{c}}(\mathbf{u}),$$

whence $\mathbf{u}$ is authorized by Fact 2.18. This shows the "if" part of **(b)**.

Conversely, let $\mathbf{t}$ be a zero-free authorized track. Denote by s the number of pairwise distinct elements in $\mathbf{t}^l$. By Fact 4.5, (4.5) and Fact 2.18, we have

$$\min(k-1, s) = \operatorname{rank} VM_{\mathbf{e}_{k-1}}(\mathbf{t}^l) = \operatorname{rank} VM_{\hat{\mathbf{c}}_i}(\mathbf{t}) < \operatorname{rank} VM_{\mathbf{c}}(\mathbf{t}).$$

This means that at least one of the following holds:

- $VM_{\mathbf{c}}(\mathbf{t})$ contains $s+1$ pairwise distinct rows;
- $VM_{\mathbf{c}}(\mathbf{t})$ contains a non-singular sub-matrix of size $k \times k$.

The first possibility means that there are some $j \neq j'$ such that

$$\left[\begin{array}{cccc|c} 1 & t_j^l & \dots & t_j^{l(k-2)} & t_j^m \end{array}\right] \neq \left[\begin{array}{cccc|c} 1 & t_{j'}^l & \dots & t_{j'}^{l(k-2)} & t_{j'}^m \end{array}\right] \qquad \text{while} \qquad t_j^l = t_{j'}^l,$$

which implies that $t_j^m \neq t_{j'}^m$, and so (i) must hold by **(a)**. In the second case, (ii) must hold because any $(k \times k)$-submatrix of $VM_{\mathbf{c}}(\mathbf{t})$ is of the form $VM_{\mathbf{c}}(\mathbf{u})$ for some $\mathbf{u} \sqsubseteq \mathbf{t}$ of length k.

(c) The cases $c_0 > 0$ and $c_i = 0$ are clear, respectively, by parts (a) and (c) of Fact 4.2.

If $c_0 = 0$, $i > 0$, and $k \geqslant 4$, then, by Fact 4.2b, using its notation, $\mathbf{t}$ is $(\mathbf{c}, i)$-authorized if and only if $\mathbf{u}$ is $(\mathbf{c}', i')$-authorized. However, in this case, $\widehat{(\mathbf{c}')}_{i'} = \hat{\mathbf{c}}_{i,0}$ is an arithmetic progression of length $\geqslant 3$, in which the common difference and the value of m (understood as in (4.3)) are the same as in $\mathbf{c}$. Hence, applying **(b)** to $\mathbf{u}$ yields that $\mathbf{u}$ is $(\mathbf{c}', i')$-authorized if and only if it

is $(\mathbf{c}, i)$-authorized; this is because the condition $|\mathbf{u}| < k-1$ ensures that (ii) is void, while (i) has been characterized in **(a)** exclusively in terms of l and m. Altogether, we have obtained that $\mathbf{t}$ is $(\mathbf{c}, i)$-authorized if and only if $\mathbf{u}$ is, as desired.

Finally, if $c_0 = 0$, $i > 0$ and $k = 3$, we must have $r = 2$. Then, $\mathbf{u}$ is of length 1 and hence it is not authorized by **(b)**; on the other hand, combining Facts 4.2b and 2.19 yields that $\mathbf{t}$ cannot be authorized. This shows the desired equivalence. □

4.3.2 Asymptotics of max-length privileged tracks

Fact 4.7. Under the assumptions of Lemma 4.6, denote $l' = \gcd(l, q-1)$. Then:

(a) The number of zero-free privileged tracks of length 2 is

$$(q-1)\Big(l' - \gcd(l', m)\Big) = \begin{cases} 0 & \text{if } l' \mid m, \\ \Theta_{\mathbf{c},i}(q) & \text{if } l' \nmid m; \end{cases}$$

(b) The number of zero-free privileged tracks of length $2 \leqslant r \leqslant k-1$ is

$$\begin{cases} 0 & \text{if } l' \mid m, \\ \Theta_{\mathbf{c},i,r}(q^{r-1}) & \text{if } l' \nmid m, \end{cases}$$

and such tracks exist in the second case if and only if $q > r$;

(c) The number of all privileged tracks of length $2 \leqslant r \leqslant k-1$ is

$$\begin{cases} 0 & \text{if } l' \mid m \text{ and } c_i > 0, \\ \Theta_{\mathbf{c},i,r}(q^{r-1}) & \text{if } l' \nmid m \text{ or } c_i = 0, \end{cases}$$

and such tracks exist in the second case if and only if $q \geqslant r$.

Proof. **(a)** Every track (t_0, t_1) satisfying (4.4) is uniquely determined by choosing

$$t_0 \in \mathbb{F}_q \setminus \{0\}, \qquad t_0 t_1^{-1} \in R_l \setminus R_m,$$

where R_d denotes the set of the d-th roots of unity in $\mathbb{F}_q$. Since the multiplicative group $\mathbb{F}_q^\times$ is cyclic of order $q-1$, we have $|R_d| = \gcd(d, q-1)$ for every d. Also, it follows that $R_{d_1} \cap R_{d_2} = R_{\gcd(d_1,d_2)}$ for every d_1, d_2. Hence

$$|R_l \setminus R_m| = |R_l| - |R_{\gcd(l,m)}| = \gcd(l, q-1) - \gcd(l, m, q-1) = l' - \gcd(l', m),$$

which proves **(a)**.

(b-c) For $n \geqslant 0$ and $E \subseteq \mathbb{F}_q$, let T_n^E (resp. A_n^E) denote the set of all (resp. authorized) tracks in $(\mathbb{F}_q \setminus E)^n$, and let $\pi_{j,j'}^E : T_n^E \to T_2^E$ be defined by the formula $\pi_{j,j'}^E(\mathbf{t}) = (t_j, t_{j'})$.

We start from considering the case when either $E = \emptyset$ and $c_i > 0$ or $E = \{0\}$. Then, since $r \leqslant k-1$, and permuting tracks does not affect being authorized, Lemma 4.6 implies that

$$A_r^E = \bigcup_{0 \leqslant j < j' \leqslant r-1} \big(\pi_{j,j'}^E\big)^{-1}\big(A_2^{\{0\}}\big). \tag{4.6}$$

Note that, for every $0 \leqslant j < j' \leqslant r-1$ and every $\mathbf{u} \in T_2^{\{0\}}$, the preimage $(\pi^E_{j,j'})^{-1}(\mathbf{u})$ has the same size

$$S_E \;=\; \tbinom{q-2-|E|}{r-2} \cdot (r-2)! \quad \sim_{r,|E|} \quad q^{r-2}. \tag{4.7}$$

Therefore, (4.6) gives

$$S_E \cdot |A_2^{\{0\}}| \;\leqslant\; |A_r^E| \;\leqslant\; \tbinom{r}{2} \cdot S_E \cdot |A_2^{\{0\}}|. \tag{4.8}$$

In particular, $A_r^E \neq \emptyset$ if and only if $A_2^{\{0\}} \neq \emptyset$ and $S_E > 0$; the latter is clearly equivalent to $q \geqslant r + |E|$. On the other hand, (4.8) implies

$$|A_r^E| = \Theta_{r,|E|}\big(S_E \cdot |A_2^{\{0\}}|\big),$$

which, together with (4.7) and part **(a)**, gives the desired asymptotic formula.

The remaining case ($E = \emptyset$ and $c_i = 0$) is clear by Fact 4.2c, which shows that $A_r^{\emptyset} \setminus A_r^{\{0\}}$ consists of all tracks of length r containing zero. The number of such tracks is clearly

$$r \cdot \tbinom{q-1}{r-1} \cdot (r-1)! \;\sim_r\; q^{r-1},$$

and they exist if and only if $q \geqslant r$. By combining this with the results on $A_r^{\{0\}}$ obtained above, we obtain the claim. This finishes the proof. □

Remark 4.8. Although the above reasoning suffices to obtain the claim of Fact 4.7, the estimate from below in (4.8) can be easily strengthened: in fact, we have used there only the fact that the set-theoretical sum in (4.6) is not smaller than any of its summands. To achieve more, we can use the following approximating version of inclusion-exclusion formula, known as Bonferroni inequality:

Lemma 4.9 ([10, p. 194, formula 7d])**.** For any finite sets $A_1, \ldots, A_n$, we have

$$\left|\bigcup_{i=1}^{n} A_i\right| \geqslant \sum_{i=1}^{n} |A_i| - \sum_{1 \leqslant i < j \leqslant n} |A_i \cap A_j| = \sum_{i=1}^{n} |A_i| - \tfrac{1}{2} \sum_{\substack{1 \leqslant i,j \leqslant n \\ i \neq j}} |A_i \cap A_j|.$$

By applying Lemma 4.9 to (4.6), we obtain

$$\big|A_r^E\big| \geqslant \tbinom{r}{2} \cdot S_E \cdot \big|A_2^{\{0\}}\big| - \tfrac{1}{2} \sum_{\substack{0 \leqslant j < j' \leqslant r-1 \\ 0 \leqslant m < m' \leqslant r-1 \\ (j,j') \neq (m,m')}} \Big|\big(\pi^E_{j,j'}\big)^{-1}\big(A_2^{\{0\}}\big) \cap \big(\pi^E_{m,m'}\big)^{-1}\big(A_2^{\{0\}}\big)\Big|,$$

where the number of summands on the right-hand side is less than $\binom{r}{2}^2 = O(1)$, and each summand can be verified to be $O(q^{r-2})$ by a reasoning analogous to the proof of **(a)** in Fact 4.7. This leads to a precise value for the asymptotic constant:

$$\big|A_r^E\big| \;\sim_{r,|E|}\; \tbinom{r}{2} \cdot \Big(l' - \gcd(l', m)\Big) \cdot q^{r-1}.$$

Remark 4.10. By Fact 4.7, zero-free $(\mathbf{c}, i)$-privileged tracks of every length $\geqslant 2$ exist for q sufficiently large whenever $\hat{\mathbf{c}}_i$ is arithmetic and $l' \nmid m$. This clearly contrasts with the situation in Shamir's type schemes, for which Theorem G(a-b) asserts that zero-free (k, i)-privileged tracks must be of length at least

$$\max(k - i,\, i + 1).$$

Theorem 4. *Let* $\mathbf{c}$ *be a sequence of exponents of length* $k \geqslant 3$ *and let* $0 \leqslant i < k$. *Assume that* $\hat{\mathbf{c}}_i$ *is an arithmetic progression with common difference* l, *and denote* $m = c_i - \hat{c}_{i,0}$. *Let* Π *be either "*max-priv*" or "*zfmp*" (denoting respectively "max-length privileged" or "zero-free max-length privileged"), and let* B_Π *denote the set of all prime powers* $q \in \widetilde{P}$ *for which* $N^{\Pi}_{\mathbf{c},i}(q) > 0$ *(see Denotation 2.28). Then, we have*

$$N^{\Pi}_{\mathbf{c},i}(q) = \Theta_{\mathbf{c},i}(q^{k-2}) \qquad \text{for } \ q \in B_\Pi. \tag{4.9}$$

Moreover, the behaviour of B_{zfmp} *is described as follows:*

- ***(a)*** *If* $l \mid m$, *then* $B_{\text{zfmp}} = \emptyset$;
- ***(b)*** *If* $2 \mid l$ *and* $2 \nmid m$, *then* B_{zfmp} *contains all odd prime powers greater than* k; *nevertheless, we have* $P \setminus B_{\text{zfmp}} \supseteq \{2\}$ *and* $\left|\widetilde{P} \setminus B_{\text{zfmp}}\right| = \infty$;
- ***(c)*** *In all other cases,* $\rho\big(B_{\text{zfmp}} \,\big|\, \widetilde{P}\big) \in (0,1)$; *moreover,* B_{zfmp} *is the intersection of* $\widetilde{P}$ *with a proper ultimately periodic set.*

Finally, the behaviour of $B_{\text{max-priv}}$ *may be reduced to the above cases as follows:*

- ***(d)*** *If* $c_i = 0$, *then* $B_{\text{max-priv}}$ *contains all prime powers greater than* k;
- ***(e)*** *If* $c_i > 0$, *then* $B_{\text{max-priv}}$ *coincides with* B_{zfmp} *in the range of numbers greater than* k.

Remark 4.11. The statement of the theorem implies straightforwardly that $N_q^{\text{zfmp}}(\mathbf{c}, i)$ adheres to the template (T1), (T2′) or (T3) correspondingly in the case **(a)**, **(b)**, or **(c)**. Then, $N_q^{\text{max-priv}}(\mathbf{c}, i)$ adheres to the same template in the case **(e)**, and to (T2) in **(d)**.

Remark 4.12. The statement of **(b)** makes it evident that (T2′) cannot be always reduced to (T2).

Proof of Theorem 4. **1.** The statement (4.9) and parts **(d-e)** follow straightforwardly from Fact 4.7. It remains to argue for **(a-c)**. From now on, we denote for simplicity

$$B = B_{\text{zfmp}}.$$

2. By Fact 4.7, we have

$$B = \widetilde{P} \cap C, \qquad \text{where} \qquad C \subseteq C' = \big\{q \in \mathbb{N} \;\big|\; \gcd(l, q-1) \nmid m\big\}$$

and moreover C and C' coincide in the range of numbers exceeding k. Note that C' is periodic because, for fixed l, whether $\gcd(l, q-1)$ divides m depends only on the residue of q modulo l. Hence, C is ultimately periodic.

Moreover, let us observe that the condition $\rho(B \,|\, \widetilde{P}) \in (0,1)$ appearing in **(c)** implies that both sets $C \supseteq B$ and $\mathbb{N} \setminus C \supseteq \widetilde{P} \setminus B$ are infinite, so, by (1.6), C must be proper ultimately periodic. This means that the second claim in **(c)** follows from the first one.

We will now analyze which $q \in \widetilde{P}$ belong to B. For convenience, denote $l' = \gcd(l, q-1)$.

3. If $l \mid m$, then for every q we have $l' \mid m$ and hence $q \notin C'$. This proves **(a)**.

Suppose now that $l \nmid m$. Then, whenever $q \equiv 1 \pmod{l}$, we have $l' = l \nmid m$, so $q \in C'$. By Corollary 1.7, there are infinitely many such q; moreover, their relative density in $\widetilde{P}$ is $\frac{1}{\varphi(l)}$. Hence,

$$\rho(B \,|\, \widetilde{P}) > 0.$$

To finish the proof of **(b)** and the first claim of **(c)**, we consider three sub-cases:

- If $2 \mid l$ and $2 \nmid m$, then for every odd q we have $2 \mid l'$, whence $l' \nmid m$ and $q \in C'$. By Fact 4.7b, this implies that B contains all odd prime powers greater than k, as desired.

  On the other hand, let $l = 2^a \cdot b$ with $a \geqslant 0$ and $2 \nmid b$. For any $j \in \mathbb{N}$, let $q = 2^{j\varphi(b)+1}$; then clearly $\gcd(q-1, 2^a) = 1$, and $q - 1 \equiv 1 \pmod{b}$ by Fermat's Little Theorem. Hence $l' = \gcd(q-1, 2^a \cdot b) = 1$, so $q \notin C'$; since $j \in \mathbb{N}$ was arbitrary and $\varphi(b) > 0$, we conclude that $\widetilde{P} \setminus B$ is infinite. Also, for $j = 0$ we obtain that $2 \notin B$. This proves **(b)**.
- If $2 \nmid l$, then the set
$$D = \{q \in \widetilde{P} \mid q \equiv 2 \pmod{l}\}$$
has positive relative density in $\widetilde{P}$ (by Corollary 1.7), and is certainly disjoint with C'. This shows that $\rho(B \mid \widetilde{P}) < 1$, as desired.
- If both l and m are even, then we consider the set
$$E = \{q \in \widetilde{P} \mid q \equiv -1 \pmod{l}\}.$$
Again, by Corollary 1.7, $\rho(E \mid \widetilde{P}) > 0$. Also, $E \subseteq \widetilde{P} \setminus B$, because for every $q \in E$, we have
$$l' = \gcd(q-1, l) = \gcd(-2, l) = 2$$
which is a divisor of m, whence $q \notin C'$. This proves that $\rho(B \mid \widetilde{P}) < 1$.

In every sub-case, we have obtained either the claim of **(b)** of the first claim of **(c)**. This finishes the proof. □

Remark 4.13. The above proof together with the exact formulation of Corollary 1.7 implies that, given some fixed l and m, the value of $\rho(B \mid \widetilde{P})$ can be effectively computed as
$$1 - \frac{\left|\left\{0 \leqslant a < l \;\middle|\; \gcd(a+1, l) = 1,\, \gcd(a, l) \mid m\right\}\right|}{\varphi(l)}.$$
However, we are unable to simplify this formula. Hence, we reduce the statement of Theorem 4 essentially to inform under which circumstances the above quantity equals 0 or 1.

4.4 The case of c arithmetic

We will now aim at proving an analogue of Theorem 4 for the case when the whole sequence $\mathbf{c}$ is arithmetic progression; to avoid collisions with Section 4.3, we will denote its common difference by λ. (Again, to make λ well defined, we assume that $k \geqslant 2$). Our main result, Theorem 5, will be stated in Section 4.4.4. Even though its formulation looks similarly to that of Theorem 4, the proof will be now more complex.

The basic idea of Theorem 5 and its proof is to reduce Lai-Ding's schemes to Shamir's type schemes (with λ-th powers as participants), according to Fact 4.14 of Section 4.4.1. Hence, our problem reduces to showing that a given Shamir's type scheme admits many privileged tracks consisting solely of λ-th powers. For this, we will need to refer to the results on Shamir's type schemes from [56], in particular, to some details of the construction of privileged tracks. These facts will be presented in Section 4.4.2.

After these initial steps, we will be left with the task of finding many zeroes for a particular multivariate polynomial, for which we will find it suitable to use the powerful theorem of Weil, stated as Theorem B in Section 1.2.2. The main proof of Theorem 5 occupies Section 4.4.4, while the preceding Section 4.4.3 contains auxiliary facts needed for verifying the assumptions of Theorem B.

4.4.1 Authorized tracks

Fact 4.14. Let $\mathbf{c}$ be an arithmetic sequence of exponents of length $k \geqslant 2$ with common difference λ, and let $\mathbf{t}$ be a track. Then:

(a) If $c_0 = 0$, then $\mathbf{t}$ is $(\mathbf{c}, i)$-authorized if and only if it contains a subtrack $\mathbf{u}$ such that

(4.10a) $\qquad \mathbf{u}^\lambda$ is a track which is (k, i)-authorized;

(b) If $c_0 > 0$, then $\mathbf{t}$ is $(\mathbf{c}, i)$-authorized if and only if it contains a subtrack $\mathbf{u}$ such that

(4.10b) $\qquad \mathbf{u}^\lambda$ is a zero-free track which is (k, i)-authorized.

Proof. **(a)** Let $c_0 = 0$, i.e. $\mathbf{c} = \lambda \cdot \mathbf{e}_k$. By Fact 2.18, $\mathbf{t}$ is $(\lambda \cdot \mathbf{e}_k, i)$-authorized if and only if

$$\operatorname{rank} VM_{\mathbf{e}_k}(\mathbf{t}^\lambda) = \operatorname{rank} VM_{\lambda \cdot \mathbf{e}_k}(\mathbf{t}) > \operatorname{rank} VM_{\widehat{(\lambda \cdot \mathbf{e}_k)_i}}(\mathbf{t}) = \operatorname{rank} VM_{\hat{\mathbf{e}}_{k,i}}(\mathbf{t}^\lambda). \tag{4.11}$$

Clearly, if $t_i^\lambda = t_j^\lambda$ for some $i \neq j$, then removing the j-th row from all the above matrices will not affect their rank. By repeating this reasoning, we obtain that if $\mathbf{t}$ is (k, i)-authorized, then there is some $\mathbf{u}$ satisfying (4.10a). Conversely, if such $\mathbf{u}$ exists, then it is $(\mathbf{c}, i)$-authorized by (4.11), whence $\mathbf{t}$ also is. This proves **(a)**.

(b) We consider two cases. If $\mathbf{t}$ is zero-free, conditions (4.10a) and (4.10b) coincide, whence the claim follows immediately from **(a)** by using Fact 4.4.

Otherwise, we may assume without losing generality that $\mathbf{t} = \mathbf{t}' \mid\mid (0)$ for some $\mathbf{t}'$. By Fact 4.2a, $\mathbf{t}$ is $(\mathbf{c}, i)$-authorized if and only if $\mathbf{t}'$ is. Since $0 \notin \mathbf{t}'$, we apply again the first case to see that this happens if and only if there is $\mathbf{u} \sqsubseteq \mathbf{t}'$ satisfying any of the conditions (4.10). This is equivalent to existence of $\mathbf{u} \sqsubseteq \mathbf{t}$ satisfying (4.10b). □

4.4.2 Privileged tracks in Shamir's type schemes

In this section, we state a number of properties of the main construction of [56] which we will need in the proof of Theorem 5.

Before that, we recall two simple properties of Shamir's schemes, essentially given in [55]. For completeness, we will show how to derive them easily from the knowledge presented so far.

Fact 4.15 ([55, Corollary 1])**.** Let q be a prime power, $1 \leqslant i \leqslant k - 2 \leqslant q - 2$ and denote $j = k - 1 - i$. Then, a track $\mathbf{t} \in \mathbb{F}_q^{k-1}$ is (k, i)-privileged if and only if $\tau_j(\mathbf{t}) = 0$.

Proof. This follows from Corollary 2.26, Definition 2.20 and Lemma 1.5. □

Lemma 4.16 (resulting primarily from [45, Corollary 3])**.** Let q be a prime power and $1 \leqslant j \leqslant k-2 \leqslant q-2$. Then the number of tracks $\mathbf{t} \in \mathbb{F}_q^{k-1}$ satisfying $\tau_j(\mathbf{t}) = 0$ is $\Theta_{k,i}(q^{k-2})$. Also, this asymptotic estimate remains unchanged if we restrict to zero-free tracks.

Proof. By Fact 4.15, a track $\mathbf{t}$ of length $k-1$ satisfies $\tau_j(\mathbf{t}) = 0$ if and only if $\mathbf{t}$ is (k,i)-privileged, where $i = k-1-j$. The number of such tracks over $\mathbb{F}_q$ is $\Theta(q^{k-2})$ by Corollary 2.31.

For zero-free solutions, Theorem F ensures that the number of zero-free (k,i)-privileged tracks of length $k-1$ is $\Omega(q^{k-2})$. On the other hand, it must be $O(q^{k-2})$ by the estimate for all privileged tracks. This gives the claim. □

Lemma 4.17 (extracted from [56, proof of Theorem 1])**.** Let q be a prime power with $2 \nmid q$ and let $1 \leqslant j \leqslant k-2$. Then there exist sets of tracks $\mathcal{A}_s \subseteq (\mathbb{F}_q \setminus \{0\})^s$ for $0 \leqslant s \leqslant k-3$ satisfying the following conditions:

- **(a)** The empty track () belongs to $\mathcal{A}_0$.
- **(b)** For every $0 \leqslant s \leqslant k-4$ and $\mathbf{t} \in \mathcal{A}_s$, there exists a subset $A \subseteq \mathbb{F}_q$ of size $q-k$ such that $\mathbf{t} \mid\mid (a) \in \mathcal{A}_{s+1}$ for every $a \in A$.
- **(c)** For every $j-1 \leqslant s \leqslant k-3$ and $\mathbf{t} \in \mathcal{A}_s$, we have

$$\tau_{j-1}(\mathbf{t}) \neq 0, \qquad \tau_{j-1}(\mathbf{t})^2 \neq \tau_j(\mathbf{t}) \cdot \tau_{j-2}(\mathbf{t}). \tag{4.12}$$

Proof. Consider the algorithm appearing in the proof of Theorem 1 in [56]. For $0 \leqslant s \leqslant k-3$, define $\mathcal{A}_s$ to be the set of all tracks "generated in the s-th step", i.e. all tracks $(t_1, \ldots, t_s) \in \mathbb{F}_q^s$ such that, for every $1 \leqslant u \leqslant s$, the value of t_u has been allowed in the appropriate step of the algorithm (namely, step 1.1 if $u \leqslant j-1$ and step 1.2.3 otherwise) in the context of the preceding values $t_1, \ldots, t_{u-1}$.

Since the empty track () satisfies the above condition, it belongs to $\mathcal{A}_0$, which gives **(a)**. For **(b)**, we need to verify that, for $1 \leqslant s \leqslant k-3$, the value of t_s is always chosen in the algorithm among at least $q-k$ possible candidates. For the choices made in step 1.1, this is clear. For step 1.2.3, this follows straightforwardly from (9) in [56]. Finally, **(c)** is stated as (8) in [56] using the notation $c_{j,l} = \tau_j(t_1, \ldots, t_l)$ which is defined at the beginning of Section 3 in [56]. □

Remark 4.18. By referring to [56, Theorem 2], one can generalize Lemma 4.17 to the case when $2 \mid q$ and $k \geqslant 4$. However, this is not essential for our purposes.

4.4.3 An irreducibility lemma

The goal of this short section is to prove an auxiliary result (Lemma 4.21) which will be used for estimating the asymptotics of $N_{\mathbf{c},i}^{\text{max-priv}}(q)$ in Theorem 5.

To shorten the proof, we will use the following result of Guersenzvaig:

Lemma 4.19 (a weakening of [20, Theorem 1.1])**.** Let Z be a unique factorization domain and U be the group of units in Z. Let $n > 1$, $m \geqslant 1$ and f be any irreducible polynomial in $Z[x]$ of degree m with leading coefficient $\alpha \in Z$ and constant term $\beta \in Z \setminus \{0\}$. Suppose that at least one of the sets

$$\alpha \cdot U = \{\alpha u \,|\, u \in U\}, \qquad \beta \cdot U = \{\beta u \,|\, u \in U\}$$

does not contain any non-trivial powers of elements of Z. Then, $f(x^n)$ is an irreducible element of $Z[x]$.

Fact 4.20. Let $n > 1$, K be a field with $\operatorname{char} K \not| n$, and $a, b \in K \setminus \{0\}$. Let $P(x) = ax^n + b \in K[x]$. Then there do not exist $Q(x) \in K[x]$ and $k > 1$ such that $P = Q^k$.

Proof. Suppose that such Q and k exist. Let $Q = \sum_i a_i x^i$; note that $a_0 \neq 0$ because $b \neq 0$. Let i_0 be the lowest $i > 0$ for which $a_i \neq 0$. Then, the coefficient of x^{i_0} in $Q(x)^k$ is $k \cdot a_{i_0} \cdot a_0^{k-1}$ which cannot vanish because $k \mid n$ while $\operatorname{char} K \not| n$, whence $\operatorname{char} K \not| k$. On the other hand, $k > 1$ implies $0 < i_0 < n$, so the coefficient of x^{i_0} in $P(x)$ is zero. Thus, $P \neq Q^k$. □

Lemma 4.21. Let q be a prime power, $p = \operatorname{char} \mathbb{F}_q$ and $n \geqslant 1$, $p \not| n$. Let $a, b, c, d \in \mathbb{F}_q$ be such that at most one of them is zero and $ad - bc \neq 0$. Then

$$P(x, y) = ax^n y^n + bx^n + cy^n + d \in \mathbb{F}_q[x, y]$$

is absolutely irreducible.

Proof. Let

$$\alpha = ay^n + b, \qquad \beta = cy^n + d, \qquad f = \alpha x + \beta,$$

so that $f(x^n, y) = P$. We will first verify that f is absolutely irreducible. Suppose that $f = g \cdot h$ for some $g, h \in \overline{\mathbb{F}_q}[x, y]$ which are not constant. Since f has degree 1 wrt. x, we may assume that $g \in \overline{\mathbb{F}_q}[y]$. Then, g must divide both α and β. However, α and β must be coprime because

$$c \cdot \alpha - d \cdot \beta = bc - ad \in \mathbb{F}_q \setminus \{0\}. \tag{4.13}$$

This proves absolute irreducibility of f.

Now, if $n = 1$, then $P = f$ and the proof is finished. Otherwise, we will use Lemma 4.19 for

$$Z = \overline{\mathbb{F}_q}[y], \qquad f \in \overline{\mathbb{F}_q}[x, y] \simeq Z[x], \qquad U = \overline{\mathbb{F}_q}.$$

Since f is already known to be irreducible, it remains to check the other assumption of the Lemma. Since at most one of a, b, c, d is zero, we have $\alpha, \beta \neq 0$, and moreover, at least one of α, β must have degree n and non-zero constant term wrt. y; this property will be clearly preserved after multiplying by any $u \in U$. Hence, since $\operatorname{char} \overline{\mathbb{F}_q} = p \not| n$, Fact 4.20 ensures that $\alpha \cdot U$ or $\beta \cdot U$ does not contain non-trivial powers in Z. Hence, by Lemma 4.19, $P = f(x^n)$ is irreducible as an element of $\overline{\mathbb{F}_q}[x, y]$, which was to be proved. □

Remark 4.22. The assumption that $p \not| n$ in the above lemma is essential. Indeed, for every $P_1, P_2 \in \mathbb{F}_q[x, y]$, we have

$$(P_1 + P_2)^p = \sum_{i=0}^{p} \binom{p}{i} P_1^i P_2^{p-i} = P_1^p + P_2^p,$$

which means that the map $\phi : x \mapsto x^p$ defines not only an automorphism of $\mathbb{F}_q$, but also a ring endomorphism of $\mathbb{F}_q[x, y]$. Now, whenever $n = p \cdot k$, we have

$$P(x, y) = ax^n y^n + bx^n + cy^n + d = \left(\phi^{-1}(a)x^k y^k + \phi^{-1}(b)x^k + \phi^{-1}(c)y^k + \phi^{-1}(d)\right)^p,$$

which means that P is reducible even in $\mathbb{F}_q[x, y]$.

4.4.4 Main asymptotic result

Theorem 5. *Let* $\mathbf{c}$ *be a sequence of exponents of length* $k \geqslant 2$ *and* $0 \leqslant i < k$. *Assume that* $\mathbf{c}$ *is an arithmetic progression with common difference* λ. *Let* Π *be as in Theorem 4, and let* B_Π *denote the set of all prime powers* $q \in \widetilde{P}$ *for which* $N^{\Pi}_{\mathbf{c},i}(q) > 0$ *(see Denotation 2.28). Then, we have*

$$N^{\Pi}_{\mathbf{c},i}(q) = \Theta_{\mathbf{c},i}(q^{k-2}) \qquad \text{for } q \in B_\Pi. \tag{4.14}$$

Moreover, the behaviour of B_{zfmp} *is described as follows:*

- ***(a)*** *If* $i \in \{0, k-1\}$, *then* $B_{\text{zfmp}} = \emptyset$;
- ***(b)*** *If* $k = 3$, $i = 1$ *and* $2 \mid \lambda$, *then* $\rho\big(B_{\text{zfmp}} \,\big|\, \widetilde{P}\big) \in (0,1)$, *and* B_{zfmp} *is the intersection of* $\widetilde{P}$ *with a proper ultimately periodic set;*
- ***(c)*** *In all other cases,* $\rho\big(B_{\text{zfmp}} \,\big|\, \widetilde{P}\big) = 1$; *moreover,* B_{zfmp} *contains all odd prime powers greater than*

$$\max\Big(10^{13}\big(\lambda \ln(2\lambda)\big)^5,\quad 128\lambda^4 + \tfrac{1}{4}k^2\Big). \tag{4.15}$$

Finally, the behaviour of $B_{\text{max-priv}}$ *may be reduced to the above cases as follows:*

- ***(d)*** *If* $c_i = 0$, *then* $B_{\text{max-priv}}$ *contains all prime powers greater than* k;
- ***(e)*** *If* $c_i > 0$, *then* $B_{\text{max-priv}}$ *coincides with* B_{zfmp} *in the range of numbers greater than* k.

Remark 4.23. Analogously as in Remark 4.11, parts **(a-d)** of the above statement classify the behaviour of $N^{\Pi}_q(\mathbf{c}, i)$ respectively into the templates (T1), (T3), (T2′) and (T2).

Proof of Theorem 5. In the whole proof, the constants used in the asymptotic notation will depend on $\mathbf{c}$ and possibly i but not on q.

1. First, we note that, while proving **(c)**, as well as **(e)** under the assumptions of **(c)**, it suffices to consider only the tracks $\mathbf{t} \in \mathbb{F}_q^{k-1}$ such that

$$\mathbf{t}^\lambda \text{ is a zero-free track.} \tag{4.16}$$

(Here, "considering only tracks satisfying (4.16)" formally means estimating $N^{\Pi\wedge(4.16)}_q(\mathbf{c}, i)$ instead of $N^{\Pi}_q(\mathbf{c}, i)$, where "(4.16)" serves as a self-explanatory description of the above property, and $\wedge$ is logical conjunction).

Indeed, the equality $\rho(B_\Pi \,|\, \widetilde{P}) = 1$ and the existential bound (4.15), if proved under the restriction to such tracks, will clearly hold as well for all tracks. As for the asymptotics of $N^{\Pi}_q(\mathbf{c}, i)$, we note that every track $\mathbf{t}$ failing to satisfy (4.16) must contain $0 \in \mathbb{F}_q$ or a zero-free subtrack $(t_j, t_{j'})$ for some $0 \leqslant j < j' < k-1$ such that $t_j \cdot t_{j'}^{-1}$ is a λ-th root of unity in $\mathbb{F}_q$; hence, the number of all such tracks is at most

$$(k-1)\cdot q^{k-2} + \tbinom{k-1}{2} \cdot q \cdot \lambda \cdot q^{k-3} = O(q^{k-2}).$$

Therefore, if we prove that the number of tracks satisfying (4.16) with property Π is $\Theta(q^{k-2})$, then removing the condition (4.16) cannot invalidate this estimate.

2. We now use prior results to deal with certain sub-cases:

(i) If $k = 2$, then $B_{\text{zfmp}} = \emptyset$ by Fact 2.19.

(i') If in addition $c_i > 0$, then also $B_{\text{max-priv}} = \emptyset$ by Fact 2.19 and Fact 4.2ab.

(ii) If $k \geqslant 3$ and $i \in \{0, k-1\}$, then Theorem 4a with $l = m = \lambda$ gives $B_{\text{zfmp}} = \emptyset$.

(ii') If in addition $c_i > 0$, then Theorem 4e also yields $B_{\text{max-priv}} = \emptyset$.

(iii) If $k = 3$ and $i = 1$, Theorem 4 applied with $l = 2\lambda$ and $m = \lambda$ gives (4.14), and moreover:

(A) if $2 \mid \lambda$, then Theorem 4c gives the claim of **(b)**;

(B) otherwise, Theorem 4b implies that B_{zfmp} contains all odd prime powers greater than k.

Regardless of the above sub-cases (A-B), we again observe that:

(iii') If in addition $c_i > 0$, then Theorem 4e also yields the claim of **(e)**.

(iv) If $k \geqslant 3$, $i \notin \{0, k-1\}$ and $\lambda = 1$, then by Fact 4.4 zero-free $(\mathbf{c}, i)$-privileged tracks coincide with zero-free (k, i)-privileged tracks. By [56, Theorem 1], the number of such tracks of length $k-1$ is $\Theta(q^{k-2})$ for all $q \in \widetilde{P}$, and moreover it is positive if q is odd and greater than k.

(v) If $c_i = 0$, then all tracks of length $k-1$ containing 0 are privileged by Fact 4.2c. Hence, $N_q^{\text{max-priv}}(\mathbf{c}, i) = N_q^{\text{zfmp}}(\mathbf{c}, i) + \Theta(q^{k-2})$, and $B_{\text{max-priv}}$ contains all prime powers greater than k.

Now, **(a)** and **(b)** follow respectively from (i-ii) and (iii.A). Under the assumptions of **(a-b)**, **(e)** follows from (i'), (ii') and (iii'). Moreover, (v) implies that parts **(a-c)** imply **(d)**. Finally, step 1 ensures that proving **(e)** under the assumptions of **(c)** reduces to proving **(c)**.

Hence, what remains is to prove **(c)** in all situations not covered by (iii.B) and (iv), that is, when

$$k \geqslant 4, \qquad 0 < i < k-1, \qquad \lambda > 1.$$

In the remaining part of the proof, the design of steps 3–9 aims at obtaining the desired asymptotic estimate without persistent tracking of all the involved constants; then, in the last step, the constants will be gathered to obtain a concrete lower bound for q.

3. Before starting the main proof, we introduce some denotations. Let

$$j = k - 1 - i, \qquad \lambda' = \gcd(q-1, \lambda).$$

Note that, although λ' depends on q, we have $1 \leqslant \lambda' \leqslant \lambda$ and hence $\lambda' = \Theta(1)$.

For any $m \in \mathbb{N}$, let $\phi_m : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$ be the group homomorphism sending x to x^m, and let P_m denote its image. Note that, since $\mathbb{F}_q^\times$ is cyclic of order $q-1$, we have

$$\ker \phi_\lambda = \ker \phi_{\lambda'} \qquad \text{and} \qquad P_\lambda = P_{\lambda'}. \tag{4.17}$$

4. Let $\mathbf{t}$ be as in (4.16). By Fact 4.14, $\mathbf{t}$ is $(\mathbf{c}, i)$-privileged if and only if $\mathbf{t}^\lambda$ is a (k, i)-privileged track. By Fact 4.15, we obtain

$$\mathbf{t} \text{ is } (\mathbf{c}, i)\text{-privileged} \qquad \Leftrightarrow \qquad \mathbf{t}^\lambda \in \mathcal{U},$$

where

$$\mathcal{U} = \{\mathbf{u} \in P_\lambda^{k-1} \mid \mathbf{u} \text{ is a track and } \tau_j(\mathbf{u}) = 0\}.$$

Since ϕ_λ is a homomorphism, for every $\mathbf{u} \in \mathcal{U}$ there exist exactly $|\ker \phi_\lambda|^{k-1} = (\lambda')^{k-1}$ zero-free tracks $\mathbf{t} \in \mathbb{F}_q^{k-1}$ such that $\mathbf{t}^\lambda = \mathbf{u}$, whence it follows that

$$N_{\mathbf{c},i}^{\text{max-priv}\wedge(4.16)}(q) = (\lambda')^{k-1} \cdot |\mathcal{U}|. \tag{4.18}$$

By Lemma 4.16, we have $|\mathcal{U}| = O(q^{k-2})$. Since $(\lambda')^{k-1} = \Theta(1)$, it remains to verify that $|\mathcal{U}| = \Omega(q^{k-2})$.

5. Let $\mathcal{A}_s$ denote the set described in Lemma 4.17. For $0 \leqslant s \leqslant k-4$, define

$$\mathcal{B}_s = \mathcal{A}_s \cap P_\lambda^s,$$
$$\mathcal{C}_s = \{\mathbf{v} \in \mathcal{B}_s \,|\, \tau_j(\mathbf{v}) \neq 0\}, \qquad \mathcal{D}_s = \{\mathbf{v} \in \mathcal{B}_s \,|\, \tau_{j-2}(\mathbf{v}) \neq 0\}. \tag{4.19}$$

The goal of this step is to prove that

$$|\mathcal{C}_{k-3} \cup \mathcal{D}_{k-3}| \geqslant \left(\tfrac{q-1}{\lambda'} - (k+1)\right)^{k-3} = \Omega(q^{k-3}). \tag{4.20}$$

By definition, $() \in \mathcal{B}_0$. Let $0 \leqslant s \leqslant k-4$ and $\mathbf{v} \in \mathcal{B}_s$. Since $|P_\lambda| = \frac{q-1}{\lambda'}$, Lemma 4.17b implies that there is a subset $B \subseteq P_\lambda$ of size $\frac{q-1}{\lambda'} - k$ such that $\mathbf{v} \,||\, (b) \in \mathcal{B}_{s+1}$ for every $b \in B$. Using this argument inductively, we conclude that

$$|\mathcal{B}_s| \geqslant \left(\tfrac{q-1}{\lambda'} - k\right)^s \qquad \text{for } 1 \leqslant s \leqslant k-4. \tag{4.21}$$

Now, let $s = k-4$ and $\mathbf{v}$ be any element in $\mathcal{B}_s$, and let B be the subset of P_λ chosen above. Let $\eta \in \{j-2, j\}$. By (4.2), we have

$$\tau_\eta(\mathbf{v} \,||\, (b)) = \tau_\eta(\mathbf{v}) + b \cdot \tau_{\eta-1}(\mathbf{v}). \tag{4.22}$$

Now, we consider two cases:

- If $j \leqslant k-3$, we choose $\eta = j$ and observe that $\tau_{\eta-1}(\mathbf{v}) = \tau_{j-1}(\mathbf{v}) \neq 0$ by (4.12) and the inequality $s = k-4 \geqslant j-1$. Together with (4.22), this implies that $\tau_\eta(\mathbf{v} \,||\, (b)) \neq 0$ (and hence $\mathbf{v} \,||\, (b) \in \mathcal{C}_{k-3}$) for every $b \in B \setminus \{-\frac{\tau_j(\mathbf{v})}{\tau_{j-1}(\mathbf{v})}\}$.
- If $j > k-3$, we choose $\eta = j-2$ and observe that $i > 0$ implies $j = k-2$. Now, since $\mathbf{v}$ is zero-free and has length $k-4 = j-2$, it follows that $\tau_\eta(\mathbf{v}) = \tau_{j-2}(\mathbf{v}) = \prod_{l=0}^{j-3} v_j$ is not zero. Again, putting this into (4.22), we deduce that $\tau_\eta(\mathbf{v} \,||\, (b)) \neq 0$ (and hence $\mathbf{v} \,||\, (b) \in \mathcal{D}_{k-3}$) for every $b \in B$ except for possibly one element.

In either case, we have obtained that

$$|\mathcal{C}_{k-3} \cup \mathcal{D}_{k-3}| \geqslant |\mathcal{B}_{k-4}| \cdot (|B| - 1),$$

which together with (4.21) yields (4.20).

6. Now, fix an element $\mathbf{v} \in \mathcal{C}_{k-3} \cup \mathcal{D}_{k-3}$ and define

$$\mathcal{X}_\mathbf{v} = \left\{\mathbf{x} \in \mathbb{F}_q^2 \;\middle|\; \mathbf{v} \,||\, \mathbf{x} \in \mathcal{U}\right\}. \tag{4.23}$$

We will aim at estimating $|\mathcal{X}_\mathbf{v}|$ from below. By the definition of $\mathcal{U}$, and by (4.17), it is evident that $\mathcal{X}_\mathbf{v}$ is the set of all pairs $(a^{\lambda'}, b^{\lambda'})$ for $a, b \in \mathbb{F}_q$ satisfying the following conditions:

$$a, b \neq 0, \qquad a^{\lambda'} \neq b^{\lambda'}, \qquad a^{\lambda'}, b^{\lambda'} \notin \mathbf{v} \tag{4.24a}$$

and

$$\tau_j(\mathbf{v} \mid\mid (a^{\lambda'}, b^{\lambda'})) \neq 0. \tag{4.24b}$$

Denote by $\mathcal{Y}_{\mathbf{v}}$ and $\mathcal{Z}_{\mathbf{v}}$ the sets of pairs $a, b \in \mathbb{F}_q$ satisfying respectively (4.24a) and (4.24b). By (4.2), it is easy to see that (4.24b) is equivalent to

$$P_{\mathbf{v},\lambda'}(a,b) = 0, \qquad \text{where} \qquad P_{\mathbf{v},\lambda'}(x,y) = \tau_{j-2}(\mathbf{v})x^{\lambda'}y^{\lambda'} + \tau_{j-1}(\mathbf{v})(x^{\lambda'} + y^{\lambda'}) + \tau_j(\mathbf{v}).$$

Using this criterion, we will first argue that the set $\mathcal{Z}_{\mathbf{v}}$ is large, and then check that the difference $\mathcal{Z}_{\mathbf{v}} \setminus \mathcal{Y}_{\mathbf{v}}$ is small.

7. The polynomial $P_{\mathbf{v},\lambda'}$ meets the assumptions of Lemma 4.21, which follows from (4.12), (4.19), from the assumption that $\mathbf{v} \in \mathcal{C}_{k-3} \cup \mathcal{D}_{k-3}$, and from the fact that λ' is a divisor of $q-1$ which is coprime with $\operatorname{char} \mathbb{F}_q$. Therefore, by the lemma, it is absolutely irreducible.

By Theorem B, this implies that $|\mathcal{Z}_{\mathbf{v}}| = \Theta_{\lambda'}(q)$, since the total degree of $P_{\mathbf{v},\lambda'}$ is $2\lambda'$. However, λ' is a divisor of λ which is determined by $\mathbf{c}$, so it may take only finitely many values for a fixed choice of $\mathbf{c}$. Hence, we have

$$|\mathcal{Z}_{\mathbf{v}}| = \Omega(q). \tag{4.25}$$

8. We will now consider pairs (a, b) which satisfy (4.24b) but not (4.24a). Every such pair falls into at least one of the following cases:

- If $a = 0$, then b is a solution of $Q(y) = P_{\mathbf{v},\lambda'}(0, y)$; since $P_{\mathbf{v},\lambda'}$ has at least three non-zero coefficients, it follows that Q is non-zero, so it has at most λ' roots. This leads to at most λ' values of (a, b). The case $b = 0$ is analogous.
- If $a^{\lambda'} = b^{\lambda'}$, then (a, b) is uniquely determined by choosing $\alpha \in \ker \phi_{\lambda'}$ such that $b = a\alpha$ and by choosing a to be a root of $Q_\alpha(x) = P_{\mathbf{v},\lambda'}(x, \alpha x)$; again, this polynomial is certainly non-zero. This leads to λ' possible values for α and, for each of them, at most $2\lambda'$ values of a. Altogether, we can obtain at most $2(\lambda')^2$ possible values of (a, b).
- Finally, since $|\mathbf{v}| = k-3$, the condition $a^{\lambda'} \in \mathbf{v}$ leads to at most $|\ker \phi_{\lambda'}| \cdot (k-3) = \lambda'(k-3)$ values of a. The case $b^{\lambda'} \in \mathbf{v}$ is analogous.

Altogether, we obtain that

$$|\mathcal{Z}_{\mathbf{v}} \setminus \mathcal{Y}_{\mathbf{v}}| \leqslant 2\lambda' + 2(\lambda')^2 + 2\lambda'(k-3) \leqslant 2\lambda'(\lambda' + k) = O(1). \tag{4.26}$$

9. Since $|\ker \phi_{\lambda'}| = \lambda'$, every element $\mathbf{x} \in \mathcal{X}_{\mathbf{v}}$ corresponds to exactly $(\lambda')^2 = \Theta(1)$ pairs (a, b) belonging to $\mathcal{Y}_{\mathbf{v}} \cap \mathcal{Z}_{\mathbf{v}}$. Combining this with (4.18) and (4.23), we obtain

$$\begin{aligned} N_{\mathbf{c},i}^{\text{max-priv}}(q) &\geqslant (\lambda')^{k-1} \cdot |\mathcal{U}| = (\lambda')^{k-1} \cdot \sum_{\mathbf{v} \in \mathcal{C}_{k-3} \cup \mathcal{D}_{k-3}} |\mathcal{X}_{\mathbf{v}}| \\ &\geqslant (\lambda')^{k-1} \cdot \big|\mathcal{C}_{k-3} \cup \mathcal{D}_{k-3}\big| \cdot \frac{1}{(\lambda')^2} \cdot \min_{\mathbf{v} \in \mathcal{C}_{k-3} \cup \mathcal{D}_{k-3}} \big|\mathcal{Y}_{\mathbf{v}} \cap \mathcal{Z}_{\mathbf{v}}\big|. \end{aligned} \tag{4.27}$$

Now, we put this together with (4.20), (4.25), (4.26) and the fact that $\lambda' = \Theta(1)$. (In particular, we underline that the asymptotic estimates (4.25), (4.26) do not depend on $\mathbf{v}$). By doing so, we arrive at the conclusion that

$$N_{\mathbf{c},i}^{\text{max-priv}}(q) = \Omega(q^{k-2}).$$

As explained in step 4, it follows that

$$N_{\mathbf{c},i}^{\text{max-priv}}(q) = \Theta(q^{k-2}) \qquad \text{for } q \in B.$$

This finishes the proof of the asymptotic estimate in **(c)**; it remains to find a lower bound for q, beyond which the above expression becomes positive.

10. We will now combine (4.27) with the detailed versions of (4.20), (4.25) and (4.26); among these auxiliary equations, only (4.25) has not been stated in its detailed form.

Denote $D = 2\lambda$. Since the total degree of $P_{\mathbf{v},\lambda'}$ is $2\lambda' \leqslant D$, applying Theorem B gives that, under the assumption that q exceeds the number

$$10^{10} \cdot 2^3 \cdot (D \ln D)^5 \;=\; 10^{10} \cdot 2^8 \cdot \big(\lambda \ln(2\lambda)\big)^5, \tag{4.28}$$

the following concretization of (4.25) holds:

$$|\mathcal{Z}_{\mathbf{v}}| \geqslant q - D^2(\sqrt{q} + 6). \tag{4.25'}$$

Combining this with (4.27), (4.20) and (4.26) produces

$$N_{\mathbf{c},i}^{\text{max-priv}}(q) \geqslant \Big((q-1) - \lambda'(k+1)\Big)^{k-3} \cdot \Big(q - D^2(\sqrt{q}+6) - 2\lambda'(\lambda'+k)\Big);$$

by simplifying the result with auxiliary inequalities

$$\lambda'(k+1) + 1 \leqslant Dk, \qquad 2\lambda'(\lambda'+k) \leqslant D(D+k),$$

we finally obtain

$$N_{\mathbf{c},i}^{\text{max-priv}}(q) \geqslant \Big(q - Dk\Big)^{k-3} \cdot \Big(q - D^2\sqrt{q} - D(7D+k)\Big).$$

This expression is positive whenever

$$q > Dk \tag{4.29a}$$

and the second parenthesis is positive, which (as we deduce by analyzing it as a quadratic polynomial in $\sqrt{q}$) must happen whenever

$$\sqrt{q} > \frac{D^2 + \sqrt{D^4 + 28D^2 + 4Dk}}{2}\,. \tag{4.29b}$$

Since $D \geqslant 2$, using the inequalities

$$\sqrt{a^2+ab} \leqslant a + \tfrac{b}{2}, \qquad a+b \leqslant \sqrt{2(a^2+b^2)}, \qquad ab \leqslant \tfrac{1}{2}(a^2+b^2) \qquad \text{for} \quad a,b \in \mathbb{R}_{\geqslant 0}$$

it is easy to deduce that the lower bound obtained in (4.29b) does not exceed $D^2 \cdot \frac{1+\sqrt{8}}{2} + k \cdot \frac{\sqrt{2}}{4}$, which is less than

$$\sqrt{8D^4 + \tfrac{1}{4}k^2}, \tag{4.30}$$

and that the lower bound for $\sqrt{q}$ coming from (4.29a) (namely, $\sqrt{Dk}$) is also less than (4.30). Altogether, this shows that $N_{\mathbf{c},i}^{\text{max-priv}}(q) > 0$ whenever q exceeds the maximum of (4.28) and the square of (4.30), which is consistent with (4.15). This finishes the proof. □

4.5 A general roadmap

In the previous two sections, we have ensured existence of many privileged coalitions in Lai-Ding's schemes for certain "nice" choices of the sequences $\mathbf{c}$, which admitted particularly simple criteria for max-length privileged tracks (given in Lemma 4.6 and Fact 4.14). We have also observed in Section 4.4 that even such simple criterion does not necessarily lead to an elementary estimate of the number of tracks satisfying it.

Now, we switch to a general choice of $\mathbf{c}$. In this case, the simplest criterion for a track $\mathbf{t}$ of length $k-1$ to be privileged (or, equivalently, authorized) which we have is the one given by Fact 2.18:

$$\operatorname{rank} VM_{\mathbf{c}}(\mathbf{t}) > \operatorname{rank} VM_{\hat{\mathbf{c}}_i}(\mathbf{t}), \tag{4.31}$$

which is more complex than the previous ones. To estimate from below the number of tracks satisfying (4.31), we will restrict to a special case (intuitively, the most generic one):

$$\operatorname{rank} VM_{\hat{\mathbf{c}}_i}(\mathbf{t}) < k-1, \qquad \operatorname{rank} VM_{\mathbf{c}}(\mathbf{t}) = k-1. \tag{4.32}$$

This gives motivation for the following fact.

Fact 4.24. Let $\mathbf{c}$ be a sequence of exponents of length k, $0 \leqslant i < k$, and $\mathbf{t}$ be a track in $\mathbb{F}_q^{k-1}$. Then:

(a) A sufficient condition for $\mathbf{t}$ to be $(\mathbf{c}, i)$-privileged is that

$$S_{\hat{\mathbf{c}}_i}(\mathbf{t}) = 0 \qquad \text{and} \qquad S_{\hat{\mathbf{c}}_j}(\mathbf{t}) \neq 0 \quad \text{for some } 0 \leqslant j < k, \tag{4.33}$$

where $S_{\hat{\mathbf{c}}_i}(\mathbf{t})$ and $S_{\hat{\mathbf{c}}_j}(\mathbf{t})$ are the Schur polynomials (defined in Section 1.1.4);

(b) If $\mathbf{t}$ is $(\mathbf{c}, i)$-privileged and (4.33) does not hold, then

$$S_{\hat{\mathbf{c}}_j}(\mathbf{t}) = 0 \quad \text{for all } 0 \leqslant j < k. \tag{4.34}$$

In particular, a necessary condition for $\mathbf{t}$ to be $(\mathbf{c}, i)$-privileged is that $S_{\hat{\mathbf{c}}_i}(\mathbf{t}) = 0$.

Proof. **(a)** First, recall that, for every track $\mathbf{t}$ and sequence of exponents $\mathbf{d}$ of the same length, the conditions $S_{\mathbf{d}}(\mathbf{t}) \neq 0$ and $V_{\mathbf{d}}(\mathbf{t}) \neq 0$ are equivalent because the quotient $V_{\mathbf{d}}/S_{\mathbf{d}}$ is the classical Vandermonde determinant which does not vanish on $\mathbf{t}$. Therefore, both letters "S" in (4.33) can be equivalently replaced by "V".

After such replacement, the first part of (4.33) translates immediately to the first part of (4.32). On the other hand, the second part of (4.32) is equivalent to existence of a non-singular sub-matrix in $VM_{\mathbf{c}}(\mathbf{t})$ of size $(k-1)\times(k-1)$; such sub-matrix must then be of the form $VM_{\hat{\mathbf{c}}_j}(\mathbf{t})$ for some $0 \leqslant j < k$, and its non-singularity is equivalent to the condition $S_{\hat{\mathbf{c}}_j}(\mathbf{t}) \neq 0$ in the second part of (4.33). Altogether, we obtain that (4.33) is equivalent to (4.32), and hence sufficient for $\mathbf{t}$ to be $(\mathbf{c}, i)$-privileged by virtue of Fact 2.18.

(b) If $\mathbf{t}$ is a $(\mathbf{c}, i)$-privileged track failing to satisfy (4.33), then it must satisfy (4.31) (by Fact 2.18) but not (4.32) (by the equivalence proved just above). Hence, the rank of $VM_{\mathbf{c}}(\mathbf{t})$ must be less than $k-1$, so all its sub-matrices of size $(k-1)\times(k-1)$ must be singular. By what was said above, this means that $S_{\hat{\mathbf{c}}_j}(\mathbf{t}) = 0$ for every $0 \leqslant j < k$. □

Remark 4.25. In view of Fact 4.24, finding a lower bound for $N_{\mathbf{c},i}^{\text{max-priv}}(q)$ decomposes into three sub-goals:

(i) ensure a large number of zeroes of $S_{\hat{\mathbf{c}}_i}$;

(ii) find an upper bound for the number of common zeroes of $S_{\hat{\mathbf{c}}_i}$ and $S_{\hat{\mathbf{c}}_j}$, $j \neq i$;

(iii) find an upper bound for the number of zeroes of $S_{\hat{\mathbf{c}}_i}$ which are not tracks (equivalently: the number of common zeroes of $S_{\hat{\mathbf{c}}_i}$ and $V_{\mathbf{e}_{k-1}}$).

The sub-goal (i) seems to be generally problematic, and will be treated in Section 4.5.2 by applying Theorem B; checking the assumptions of the latter will occupy much of Chapter 5. Before, in Section 4.5.1, we prove auxiliary facts which provide a solution of (iii) as well as a preparation for (ii), which also will be treated in Chapter 5.

4.5.1 Estimates of common zeroes

To deal with the above sub-goals (ii) and (iii), we will utilize the following result (which has been also used in [45]).

Lemma 4.26 ([47, Chapter IV, Lemma 3C])**.** Let $\mathbf{x}$ be a sequence of indeterminates of length $n \geqslant 2$ and $P_1, P_2 \in \mathbb{F}_q[\mathbf{x}]$ be two polynomials of total degrees respectively d_1, d_2 which are coprime in $\mathbb{F}_q[\mathbf{x}]$. Then, the number of common zeroes of P_1 and P_2 in $\mathbb{F}_q^n$ is at most

$$q^{n-2} d_1 d_2 \min(d_1, d_2) \;=\; O_{d_1,d_2}(q^{n-2}).$$

The following lemma ensures that Lemma 4.26 can be applied to solve (iii). For this purpose, it suffices to apply Lemma 4.27 with $D = 1$; the case $D > 1$ will be used in Section 5.7.

Lemma 4.27. Let $\mathbf{d}$ be a sequence of exponents of length $l \geqslant 0$, and $\mathbf{x}$ be a sequence of indeterminates of length l. Let $D > 0$ be coprime to $\gcd(\mathbf{d} - d_0)$ and let q be a power of a prime p such that $p \nmid D \cdot \gcd(\mathbf{d} - d_0)$. Then, the polynomials $S_{\mathbf{d}}(\mathbf{x})$ and $V_{D\cdot\mathbf{e}_l}(\mathbf{x})$ are coprime in $\overline{\mathbb{F}_q}[\mathbf{x}]$.

Proof. **1.** Let α be a primitive D-th root of unity in $\overline{\mathbb{F}_q}$ (for $D = 1$, we take $\alpha = 1$); it exists by the assumption that $p \nmid D$ [29, Chapter VI, §3]. It is well-known that

$$V_{D\cdot\mathbf{e}_l}(\mathbf{x}) = \prod_{0\leqslant i<j<l} (x_i^D - x_j^D) = \prod_{0\leqslant i<j<l} \prod_{s=0}^{D-1} (x_i - \alpha^s x_j).$$

The factors $x_i - \alpha^s x_j$ are clearly irreducible (as they have total degree 1) and pairwise coprime; therefore, it suffices to prove that neither of them divides $S_{\mathbf{d}}$. Since

$$S_{\mathbf{d}} = \frac{V_{\mathbf{d}}}{V_{\mathbf{e}_l}} = \frac{V_{\mathbf{d}}}{\prod_{0\leqslant i<j<l}(x_i - x_j)},$$

our goal is equivalent to showing that $V_{\mathbf{d}}$ is not divisible by

$$(x_i - \alpha^s x_j)^{\mu_s}, \qquad \text{where} \qquad \mu_s = \begin{cases} 2 & \text{if } s = 0, \\ 1 & \text{if } s > 0. \end{cases}$$

2. By introducing a new variable $y = x_i - \alpha^s x_j$ and substituting $x_i = \alpha^s x_j + y$, we identify the polynomial ring $\overline{\mathbb{F}_q}[\mathbf{x}]$ with $\overline{\mathbb{F}_q}[\hat{\mathbf{x}}_i \mid\mid (y)]$; our task is now to verify that

$$V_{\mathbf{d}}(\mathbf{x}) = \det \left[\begin{array}{cccc} x_0^{d_0} & x_0^{d_1} & \cdots & x_0^{d_{l-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \hline (\alpha^s x_j + y)^{d_0} & (\alpha^s x_j + y)^{d_1} & \cdots & (\alpha^s x_j + y)^{d_{l-1}} \\ \hline \vdots & \vdots & \ddots & \vdots \\ x_j^{d_0} & x_j^{d_1} & \cdots & x_j^{d_{l-1}} \\ \vdots & \vdots & \ddots & \vdots \\ x_{l-1}^{d_0} & x_{l-1}^{d_1} & \cdots & x_{l-1}^{d_{l-1}} \end{array}\right] \tag{4.35}$$

(where the extraordinary row has index i) is not divisible by y^{μ_s}.

3. For $s > 0$, we have $\mu_s = 1$, and it suffices to check that the constant term C in the expansion of (4.35) with respect to y is non-zero. Note that C can be computed by substituting $y = 0$ into (4.35). Since, for every $m \neq i, j$, the resulting matrix contains x_m only in the m-th row, it follows that, for every permutation σ of the set $\{0, 1, \ldots, l-1\}$, the coefficient of $\prod_{m \neq i,j} x_m^{d_{\sigma(m)}}$ in C is

$$\pm \det \left[\begin{array}{cc} (\alpha^s \cdot x_j)^{d_{\sigma(i)}} & (\alpha^s \cdot x_j)^{d_{\sigma(j)}} \\ x_j^{d_{\sigma(i)}} & x_j^{d_{\sigma(j)}} \end{array}\right] = \pm\big(\alpha^{s \cdot d_{\sigma(i)}} - \alpha^{s \cdot d_{\sigma(j)}}\big) \cdot x_j^{d_{\sigma(i)} + d_{\sigma(j)}}.$$

Since α is a primitive D-th root of unity, this expression vanishes in $\overline{\mathbb{F}_q}[x_j]$ if and only if

$$s \cdot d_{\sigma(i)} \equiv s \cdot d_{\sigma(j)} \pmod{D}.$$

Now, for every $0 < a < l$, we can choose σ so that $\sigma(i) = 0$ and $\sigma(j) = a$. Then, the above condition can be rewritten in the form

$$D \mid s \cdot (d_a - d_0). \tag{4.36}$$

Therefore, if $C = 0$, then (4.36) must hold for every $0 < a < l$, which altogether gives

$$D \mid s \cdot \gcd(\mathbf{d} - d_0).$$

However, by assumption, D is coprime to $\gcd(\mathbf{d} - d_0)$. Hence, D must divide s which belongs to $\{1, \ldots, D-1\}$; this is impossible. Hence, $C \neq 0$, as desired.

4. It remains to consider the case $s = 0$, in which $V_{\mathbf{d}}(\mathbf{x})$ is divisible by y, while our goal is to show that it is not divisible by y^2. For this, we will expand the quotient $V_{\mathbf{d}}(\mathbf{x})/y$ with respect to y, analogously as we did with $V_{\mathbf{d}}(\mathbf{x})$ in step 3.

First, we expand each entry in the i-th row of (4.35) with the binomial formula, and then subtract the j-th row from the i-th row. After that, the m-th entry in the i-th row takes the form

$$(x_j + y)^{d_m} - x_j^{d_m} = y \cdot P_{d_m}(x_j, y),$$

where

$$P_d(x, y) = \sum_{t=0}^{d-1} \binom{d}{t+1} x^{d-t-1} y^t \qquad \text{for} \quad d \geqslant 0.$$

Putting this back into (4.35), we obtain

$$\frac{V_{\mathbf{d}}(\mathbf{x})}{y} = \det \begin{bmatrix} x_0^{d_0} & x_0^{d_1} & \cdots & x_0^{d_{l-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \hline P_{d_0}(x_j, y) & P_{d_1}(x_j, y) & \cdots & P_{d_m}(x_j, y) \\ \hline \vdots & \vdots & \ddots & \vdots \\ x_j^{d_0} & x_j^{d_1} & \cdots & x_j^{d_{l-1}} \\ \vdots & \vdots & \ddots & \vdots \\ x_{l-1}^{d_0} & x_{l-1}^{d_1} & \cdots & x_{l-1}^{d_{l-1}} \end{bmatrix}. \tag{4.37}$$

Analogously as in step 3, denote by C_1 the constant coefficient in the expansion of this polynomial with respect to y; then, C_1 can be obtained from (4.37) by substituting $y = 0$, which leads to

$$C_1 = \det \begin{bmatrix} x_0^{d_0} & x_0^{d_1} & \cdots & x_0^{d_{l-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \hline d_0 \cdot x_j^{d_0-1} & d_1 \cdot x_j^{d_1-1} & \cdots & d_m \cdot x_j^{d_m-1} \\ \hline \vdots & \vdots & \ddots & \vdots \\ x_j^{d_0} & x_j^{d_1} & \cdots & x_j^{d_{l-1}} \\ \vdots & \vdots & \ddots & \vdots \\ x_{l-1}^{d_0} & x_{l-1}^{d_1} & \cdots & x_{l-1}^{d_{l-1}} \end{bmatrix}.$$

Again, for every $m \notin i, j$, x_m appears only in the m-th row of the above matrix. Therefore, for every permutation σ of $\{0, 1, \ldots, l-1\}$, the coefficient of $\prod_{m \neq i,j} x_m^{d_{\sigma(m)}}$ in C_1 is

$$\pm \det \begin{bmatrix} d_{\sigma(i)} \cdot x_j^{d_{\sigma(i)}-1} & d_{\sigma(j)} \cdot x_j^{d_{\sigma(j)}-1} \\ x_j^{d_{\sigma(i)}} & x_j^{d_{\sigma(j)}} \end{bmatrix} = \pm (d_{\sigma(i)} - d_{\sigma(j)}) \cdot x_j^{d_{\sigma(i)}+d_{\sigma(j)}-1}.$$

Hence, if C_1 vanishes in $\overline{\mathbb{F}_q}[\hat{\mathbf{x}}_i]$, then p must divide $d_{\sigma(i)} - d_{\sigma(j)}$ for every σ. Analogously as in step 3, since the choice of σ is arbitrary, this implies $p \mid \gcd(\mathbf{d} - d_0)$. Therefore, our assumption that $p \nmid \gcd(\mathbf{d} - d_0)$ guarantees that $C_1 \neq 0$, and consequently $y^2 \nmid V_{\mathbf{d}}(\mathbf{x})$, which finishes the proof. □

4.5.2 Main lemma

The above considerations, together with Theorem B, lead to a procedure of estimating the number of max-length privileged tracks, summarized below.

Lemma 4.28. Let $\mathbf{c}$ be a sequence of exponents of length $k \geqslant 2$, $0 \leqslant i, j < k$, $i \neq j$, and $\mathbf{x}$ be a sequence of indeterminates of length $k-1$. Denote $D = \sum_{l=0}^{k-1}(c_l - c_0)$ and let q be a power of a prime p such that $p > c_{k-1} - c_0$. Assume that $S_{\hat{\mathbf{c}}_i - \hat{c}_{i,0}}(\mathbf{x})$ has a factor $A(\mathbf{x})$ which is irreducible in $\overline{\mathbb{F}_q}[\mathbf{x}]$ (in particular, it is non-constant) and coprime with $S_{\hat{\mathbf{c}}_j - \hat{c}_{j,0}}(\mathbf{x})$. Then:

(a) The following asymptotic estimate holds:

$$N_{\mathbf{c},i}^{\text{max-priv}}(q) \quad = \quad \Theta_{\mathbf{c},i}(q^{k-2});$$

(b) If in addition $q > 10^{10}k^3(D\ln D)^5$, then

$$N_{\mathbf{c},i}^{\text{max-priv}}(q) \quad \geqslant \quad q^{k-2} - q^{k-3}\cdot D^2\big(\sqrt{q}+2D+6\big) \quad > \quad 0. \tag{4.38}$$

Proof. For a polynomial $P \in \mathbb{F}_q[\mathbf{x}]$, denote by N_P the number of zeros of P in $\mathbb{F}_q^{k-1}$.

1. By applying the permutational formula to the generalized Vandermonde determinant, one obtains easily that, for every sequence of exponents $\mathbf{d}$, we have

$$\operatorname{tot\,deg} V_{\mathbf{d}} = \sum_{i=0}^{|\mathbf{d}|-1} d_i.$$

This implies in particular that the polynomials A, $S_{\hat{\mathbf{c}}_i-\hat{c}_{i,0}}$, $S_{\hat{\mathbf{c}}_j-\hat{c}_{j,0}}$, $V_{\mathbf{e}_{k-1}}$, being divisors of $V_{\hat{\mathbf{c}}_i-\hat{c}_{i,0}}$ or $V_{\hat{\mathbf{c}}_j-\hat{c}_{j,0}}$, are all of total degree at most D.

2. Note also that, for every sequence of exponents $\mathbf{d}$ of length l, we have

$$V_{\mathbf{d}}(\mathbf{x}) = \Big(\prod_{i=0}^{l-1} x_i\Big)^{d_0}\cdot V_{\mathbf{d}-d_0}(\mathbf{x});$$

moreover, the second factor on the right-hand side is not divisible by any non-trivial monomial. Applying this for $\mathbf{d} = \hat{\mathbf{c}}_i$ and $\mathbf{d} = \hat{\mathbf{c}}_j$, we deduce that A is a divisor of $S_{\hat{\mathbf{c}}_i}$, and it is coprime with $S_{\hat{\mathbf{c}}_j}$.

3. Now, we apply Theorem B for A, resulting in lower bounds of the form

$$N_{S_{\hat{\mathbf{c}}_i}} \geqslant N_A = \Omega_{\mathbf{c},i}(q^{k-2}) \tag{4.39a}$$

in the general case, and, more precisely,

$$N_{S_{\hat{\mathbf{c}}_i}} \geqslant N_A \geqslant q^{k-2} - q^{k-3}\cdot D^2\big(\sqrt{q}+6\big) \tag{4.39b}$$

under the assumptions of part **(b)**.

On the other hand, a simple reasoning known as Schwartz-Zippel Lemma (see [48, Lemma 1]) shows that

$$N_{S_{\hat{\mathbf{c}}_i}} \leqslant D\cdot q^{k-2} = O_{\mathbf{c},i}(q^{k-2}). \tag{4.40}$$

4. Now, we apply Lemma 4.26 for A and $S_{\hat{\mathbf{c}}_j}$ (coprime by step 2), as well as for A and $V_{\mathbf{e}_k}$ (coprime by Lemma 4.27, since $A \mid S_{\hat{\mathbf{c}}_i-\hat{c}_{i,0}}$, and $p > c_{k-1} - c_0 \geqslant \max(\hat{\mathbf{c}}_i - \hat{c}_{i,0})$). Since all these three polynomials have total degree at most D, both applications of Lemma 4.26 result in bounding (from above) the number of common zeroes by $D^3\cdot q^{(k-1)-2}$. Combining this with Remark 4.25 and both parts of Fact 4.24, we deduce that

$$N_A - 2D^3\cdot q^{k-3} \quad \leqslant \quad N_{\mathbf{c},i}^{\text{max-priv}}(q) \quad \leqslant \quad N_{S_{\hat{\mathbf{c}}_i}}.$$

Together with (4.39) and (4.40), this proves **(a)**, and also the first inequality in **(b)**.

5. It remains to verify that the bound obtained in part **(b)** is positive. For that, we reason analogously as in the last step of the proof of Theorem 5: after dividing by q^{k-2}, we obtain a quadratic expression in $\sqrt{q}$, which must be positive whenever

$$\sqrt{q} > \frac{D^2 + \sqrt{D^4 + 4\big(2D+6\big)}}{2}.$$

Since $D \geqslant 1$, we see that this lower bound does not exceed $D^2 \cdot \frac{1+\sqrt{33}}{2}$, which is less than $\sqrt{12D^4}$. On the other hand, the assumption of part **(b)** clearly ensures that $q > 12D^4$, which means that the central expression in (4.38) must be positive. This finishes the proof. □

Chapter 5

Irreducibility of certain Schur polynomials

This chapter is devoted to the algebraic properties of Schur polynomials in finite characteristic, particularly to the question of their absolute irreducibility. (Let us recall that Schur polynomials have been defined in Section 1.1.4 by the formula

$$S_{\mathbf{c}}(\mathbf{x}) = \frac{V_{\mathbf{c}}(\mathbf{x})}{V_{(0,1,\dots,k-1)}(\mathbf{x})},$$

where $V_{\mathbf{c}}(\mathbf{x})$ denotes the generalized Vandermonde determinant; see Definition 1.1). As we have shown in Section 4.5, this problem is of crucial importance for our general strategy of estimating the number of max-length privileged tracks in Lai-Ding's schemes (see Lemma 4.28). It may also be placed in a much broader mathematical context, as Schur polynomials are widely known and have been extensively studied for many other purposes, mainly due to the important role which they play in representation theory (see [17] and [32] for general reference).

Nevertheless, quite surprisingly, the question of their irreducibility has been essentially open for decades, with most significant research appearing only in the current century.

State of the art and its consequences

The results obtained so far generally fall into two categories, discussed correspondingly in Sections 5.1 and 5.2:

- statements explicitly regarding very particular cases of $\mathbf{c}$ over finite fields, with reasonable lower bounds for $\operatorname{char} \mathbb{F}_q$;
- projections to finite fields of the statements regarding all values of $\mathbf{c}$ over $\mathbb{C}$, with huge or unmanageable lower bounds for $\operatorname{char} \mathbb{F}_q$.

The latter branch will lead us to a result on Lai-Ding's schemes of an analogous nature, which will be proved in Section 5.2.1:

Theorem 6. *Let $\mathbf{c}$ be a sequence of exponents of length $k \geqslant 2$, and $0 \leqslant i < k$. Assume that $\hat{\mathbf{c}}_i$ is not an arithmetic progression. Then, there exists $n_{\mathbf{c},i} \in \mathbb{N}$ such that, for every prime $p > n_{\mathbf{c},i}$*

and every q being a power of p, the number of max-length $(\mathbf{c}, i)$-privileged tracks over $\mathbb{F}_q$ is $\Theta_{\mathbf{c},i}(q^{k-2})$.

Together with Theorem 4, this result suffices to complete a classification of Lai-Ding's schemes into the templates (T1), (T2*) and (T3), discussed in the introduction to this thesis. However, the lower bounds for p obtained in this method are not acceptable in practice, as we show in Section 5.2.2.

As a result, we desire a criterion for irreducibility of Schur polynomials which would be general with respect to $\mathbf{c}$, and at the same time generous with respect to p.

A better criterion

Sections 5.3–5.5 contain a proof of the following theorem:

Theorem 7 (essentially by Monge [37] and Rajan [42])**.** *Let $\mathbf{c}$ be a sequence of exponents of length $k \geqslant 3$. Denote $d_i = c_{i+1} - c_i$ for $0 \leqslant i \leqslant k-2$ and assume that*

$$c_0 = 0, \qquad \gcd(d_i, d_{i+1}) = 1 \quad \text{for} \quad 0 \leqslant i \leqslant k-3. \tag{5.1}$$

Let p be a prime such that

$$p \nmid d_i \quad \text{for} \quad 0 \leqslant i \leqslant k-2, \qquad p \nmid d_i + d_{i+1} \quad \text{for} \quad 0 \leqslant i \leqslant k-3. \tag{5.2}$$

and let K be a field of characteristic p. Then, the Schur polynomial $S_{\mathbf{c}}(\mathbf{x}) \in K[\mathbf{x}]$ is either constant (for $\mathbf{c} = \mathbf{e}_k$) or irreducible in $K[\mathbf{x}]$ (for $\mathbf{c} \neq \mathbf{e}_k$).

Although never stated so far in print to the best of our knowledge, this result essentially follows from the two articles cited above, in the sense that it can be proved (and possibly even generalized; see Section 5.4.1) by putting together the main lemma of [37] (for $k = 3$) and an appropriate adjustment of parts of the proof from [42] (as an inductive step for $k \geqslant 4$), of which, as personal communication suggests, both authors were unaware. This strategy of proving Theorem 7 will be discussed in detail in Section 5.5.

Let us explicitly state the consequences of Theorem 7 for Lai-Ding's schemes (which will be proved, mainly by using Lemma 4.28, in Section 5.7):

Theorem 8. *Let $\mathbf{c}$ be a sequence of exponents of length $k \geqslant 4$, $0 \leqslant i < k$, and q be a power of a prime p such that $p > c_{k-1} - c_0$. Assume that the sequence $\hat{\mathbf{c}}_i$ is step-coprime (see Definition 4.1), and that it is not an arithmetic progression. Then, the number of max-length $(\mathbf{c}, i)$-privileged tracks is $\Theta_{\mathbf{c},i}(q^{k-2})$, and such tracks exist for $q > 10^{10}k^3(D \ln D)^5$, where D is the sum of all elements of $\mathbf{c} - c_0$.*

Remark 5.1. In a broad range of cases, the statement of Theorem 8 can be deduced immediately from Theorem 7, possibly in combination with Lemma 4.28 and Fact 5.14 (see Section 5.3.4). This happens whenever $0 < i < k-1$, or when there is some $0 \leqslant j < k$ distinct from i such that $\hat{\mathbf{c}}_j$ is step-coprime (as it will be made evident in the proof). Nevertheless, certain special cases seem to require more care, which explains the length of our proof.

A generalization to non-Schur polynomials

Although Theorems 6 and 8 exhaust the content of this chapter with respect to its primary goal (that is, estimating the number of max-length privileged tracks in Lai-Ding's schemes), we decided to provide in addition another inductive argument for irreducibility. Its advantage over Rajan's method is that it can be applied to a broad class of perturbations of Schur polynomials; on the other hand, it requires stronger assumptions on $\mathbf{c}$. To obtain possibly broad generality, we combine both arguments within a unified inductive procedure; this leads to the following generalization of Theorem 7, which will be proved in Section 5.6.

Theorem 7'. *Let $\mathbf{c}$ be a sequence of exponents of length $k \geqslant 3$. Denote $d_i = c_{i+1} - c_i$ for $0 \leqslant i \leqslant k-2$ and assume that $\mathbf{c}$ satisfies (5.1). Let p be either 0 or a prime satisfying (5.2), and K be a field of characteristic p. Let P be a polynomial in $K[\mathbf{x}]$ which, using the language of Section 5.3, satisfies the following conditions:*

(i) P agrees with $S_{\mathbf{c}}$ upon Newton polytope;

(ii) For every $1 \leqslant a \leqslant b \leqslant k-2$ such that $\prod_{i=a}^{b-1} d_i = 1$, P agrees with $S_{\mathbf{c}}$ upon all iterated standard faces of signature $(k-2-b,\, a-1)$.

(In particular, P must agree with $S_{\mathbf{c}}$ upon all iterated standard faces of order $k-3$).

Then, P is either constant (for $\mathbf{c} = \mathbf{e}_k$) or irreducible in $K[\mathbf{x}]$ (for $\mathbf{c} \neq \mathbf{e}_k$).

Remark 5.2. The *faces* of P are polynomials, not polytopes (see Section 5.3.2).

Remark 5.3. If we set $a = b$ in (ii), then the product $\prod_{i=a}^{b-1} d_i$ ranges over the empty set and hence is equal to 1; therefore, (ii) requires that P agrees with $S_{\mathbf{c}}$ upon all iterated standard faces of signature $(k-2-a,\, a-1)$. Now, by letting a range over $\{1, \ldots, k-2\}$, we obtain that the agreement involves all iterated standard faces of order $k-3$ (see Section 5.3.2). This justifies the parenthesized remark following (ii) in the statement of the theorem.

To enhance understanding of the claim of Theorem 7', let us analyze two extremal cases covered by it:

- For every $\mathbf{c}, p, K$ satisfying the assumptions of Theorem 7, the assumptions of Theorem 7' are satisfied by $\mathbf{c}$, p, K and $P = S_{\mathbf{c}}$. Hence, Theorem 7 is a special case of Theorem 7'.
- If $\mathbf{c}, p, K$ satisfy the assumptions of Theorem 7, and in addition

$$d_i > 1 \qquad \text{for} \quad 1 \leqslant i \leqslant k-3,$$

  then (ii) trivializes for $a < b$ (but not for $a = b$), and consequently it requires exactly that P shall agree with $S_{\mathbf{c}}$ upon all iterated standard faces of order $k-3$ (see Remark 5.3). Consequently, all polynomials P satisfying this condition must be irreducible.

The general form of condition (ii) allows trading between generality of $\mathbf{c}$ and that of P, within the scope set by the above two extremal scenarios. As an interesting intermediate example, let us note that

- If $\mathbf{c}, p, K$ are as in Theorem 7, and at least one of $d_1, \ldots, d_{k-3}$ exceeds 1, then (ii) requires that P shall agree with $S_{\mathbf{c}}$ upon all standard faces (of order 1).

In other words, for a fairly generic scenario satisfying the assumptions of Theorem 7, we can point out a vast majority of coefficients in $S_{\mathbf{c}}$ which can be arbitrarily modified without losing irreducibility.

Unfortunately, Theorem 7' does not say anything new about Schur polynomials in comparison to Theorem 7, and in particular it does not lead to any extension of Theorem 8. However, we hope that it may be useful for other purposes, at least as a novel example of applying the Newton polytope method (described in its generality in Section 5.3.1) in combination with using additional knowledge (in our case, irreducibility of faces). We find such technique uncommon, and believe that it might turn out to be successful also for other interesting classes of multivariate polynomials.

5.1 Previous results over finite fields

5.1.1 Basic cases

For $k \geqslant 1$, the following conditions are well known to be necessary for $S_{\mathbf{c}}$ to be irreducible, regardless of the field K:

$$c_0 = 0 \quad \text{or} \quad \mathbf{c} = (1), \tag{5.3a}$$

$$\gcd(\mathbf{c}) = 1 \quad \text{or} \quad k < 3. \tag{5.3b}$$

Indeed, denoting $d = \gcd(\mathbf{c})$, we see that $V_{\mathbf{c}}(\mathbf{x})$ is always divisible by

$$\prod_{i=0}^{k-1} x_i^{c_0} \qquad \text{and} \qquad V_{d\cdot\mathbf{e}_k}(\mathbf{x}),$$

so $S_{\mathbf{c}} = V_{\mathbf{c}}/V_{\mathbf{e}_k}$ is divisible by

$$\prod_{i=0}^{k-1} x_i^{c_0} \qquad \text{and} \qquad \frac{V_{d\cdot\mathbf{e}_k}(\mathbf{x})}{V_{\mathbf{e}_k}(\mathbf{x})} = \prod_{0\leqslant i<j<k} \frac{x_i^d - x_j^d}{x_i - x_j}, \tag{5.4}$$

where in the first case we use the fact that $V_{\mathbf{e}_k}$ is coprime to every monomial.

Now, if (5.3a) does not hold, then $c_0 \cdot k \geqslant 2$, so the first expression in (5.4) is a product of more than one non-trivial polynomial; hence, $S_{\mathbf{c}}$ cannot be irreducible. Analogously, if $d > 1$, then the second product in (5.4) consists of $\binom{k}{2}$ non-trivial divisors, which contradicts irreducibility of $S_{\mathbf{c}}$ if $k \geqslant 3$; this shows the necessity of (5.3b).

As for the case $0 \leqslant k < 3$, the only values of $\mathbf{c}$ not excluded by (5.3a) are:

$$(), \qquad (0), \qquad (1), \qquad (0,1), \qquad (0,2), \qquad (0,d) \text{ for } d \geqslant 3.$$

In these six cases, computing $S_{\mathbf{c}}(\mathbf{x})$ leads, respectively, to:

$$1, \qquad 1, \qquad x_0, \qquad 1, \qquad x_0 + x_1, \qquad \frac{x_1^d - x_0^d}{x_1 - x_0}.$$

While the third and the fifth result are clearly irreducible over any field, the last one is a homogeneous polynomial, so it is irreducible over K if and only if $\frac{x^d-1}{x-1}$ is, which might happen for a suitable choice of K but is impossible for K algebraically closed. Hence, in

particular, for $\mathbf{c} = (0, d)$ with $d \geqslant 3$ there is no number p for which the claim of Theorem 7 would hold.

The above considerations lead to the conclusion that, apart from a few trivial cases found above, the assumptions

$$k \geqslant 3, \qquad \mathbf{c} \neq \mathbf{e}_k, \qquad c_0 = 0, \qquad \gcd(\mathbf{c}) = 1 \tag{5.5}$$

are necessary for $S_{\mathbf{c}}$ to be irreducible. This shows to what extent the assumptions (5.1) of Theorem 7 could be possibly weakened; see Section 5.4.1 for additional discussion.

5.1.2 Other special cases

As stated in [14], the question of absolute irreducibility of a given Schur polynomial has been generally open until 2000's, except for certain special cases. Among the partial results cited there, only those of [44] are applicable to fields of finite characteristic; however, they restrict to the case $k = 3$ and require some additional assumptions (in particular, $c_2 > 5$).

The case $k = 3$ has been thoroughly understood in a recent work of Monge [37]. Unlike [44], its main result regards exclusively Schur polynomials, which has allowed to provide a compact proof of the following claim:

Theorem H ([37]). *Let* $\mathbf{c}$ *be a sequence of exponents of length* 3, *with* $c_0 = 0$. *Denote* $d = \gcd(\mathbf{c})$ *and let* p *be a prime such that*

$$p \nmid c_1 c_2 (c_2 - c_1).$$

Let K *be a field of characteristic* p. *Then, the quotient* $V_{\mathbf{c}}(\mathbf{x})/V_{d\cdot\mathbf{e}_k}(\mathbf{x}) \in K[\mathbf{x}]$ *is either constant (for* $\mathbf{c} = d \cdot \mathbf{e}_k$*) or irreducible in* $K[\mathbf{x}]$ *(for* $\mathbf{c} \neq d \cdot \mathbf{e}_k$*).*

The proof of Theorem H appears in Section 4.2 of [37]. The paper provides also certain counterexamples which ensure that neither of the conditions $p \nmid c_1$, $p \nmid c_2$, $p \nmid c_2 - c_1$ can be removed from the above statement.

Although restricting to the case $k = 3$ is far from full generality, several ideas from [37] turn out to be effective also for higher values of k (see Section 5.2.3).

5.2 A solution over $\mathbb{C}$ and its consequences

Over the field $\mathbb{C}$, irreducibility of Schur polynomials has been essentially understood in the last ten years. Namely, Dvornicich and Zannier [14] and independently Rajan [42] have proved the following:

Theorem I ([14, Theorem 3.1], [42, Theorem 1.2]). *Let* $K = \mathbb{C}$ *and* $\mathbf{c}$ *be a sequence of exponents with* $c_0 = 0$. *Denote* $d = \gcd(\mathbf{c})$. *Then, the quotient* $V_{\mathbf{c}}(\mathbf{x})/V_{d\cdot\mathbf{e}_k}(\mathbf{x}) \in K[\mathbf{x}]$ *is either constant (for* $\mathbf{c} = d \cdot \mathbf{e}_k$*) or irreducible in* $K[\mathbf{x}]$ *(in the other case).*

There are at least two ways in which we may benefit from this.

First, the machinery of elimination theory shows that every polynomial in $\mathbb{Z}[\mathbf{x}]$ which is irreducible over $\mathbb{C}$ must be also irreducible over any field of sufficiently large characteristic. This can be easily deduced e.g. from [43, Theorem 32], and is also stated explicitly in [47, Chapter V, Corollary 2B]. Hence, we have:

Corollary 5.4. Let $\mathbf{c}$ be a sequence of exponents with $c_0 = 0$. Denote $d = \gcd(\mathbf{c})$, and assume that $\mathbf{c} \neq d \cdot \mathbf{e}_k$. Then, there exists $n_{\mathbf{c}} > 0$ such that, for every prime $p > n_{\mathbf{c}}$, the quotient $V_{\mathbf{c}}(\mathbf{x})/V_{d\cdot\mathbf{e}_k}(\mathbf{x})$ is irreducible in $\overline{\mathbb{F}_p}[\mathbf{x}]$. □

This result is certainly valuable from the theoretical viewpoint; in our context, it suffices to prove Theorem 6, as we will show below in Section 5.2.1. However, the bounds for p obtained in this way are intractable in practice (see Section 5.2.2), which motivates our efforts on Theorem 7.

Clearly, another possible way to benefit from Theorem I is to inspect its two existing proofs, which, noteworthy, seem to be significantly different from each other. In, [14] the claim is deduced from some algebraic-geometric properties of $\mathbb{C}$, which leaves little hope for an easy generalization to fields of finite characteristic. On the other hand, in [42] arguments specific to the field $\mathbb{C}$ are essentially used only in the case $k = 3$, which serves as the base for an inductive reasoning relying mostly on pure polynomial algebra (in particular, on an appropriate generalization of Eisenstein criterion). Therefore, many arguments from that paper are in fact usable also in our situation, as we will show in Section 5.5 (see also Section 5.2.3).

5.2.1 Proof of Theorem 6

To prove Theorem 6, we need two more results from [42], regarding Schur polynomials over $\mathbb{C}$. In the following two lemmas, we utilize the statements of [42] regarding an arbitrary "simple based root system" $\mathcal{R}$, applied in the case when $\mathcal{R}$ is of type A. (For definitions, see [42, Section 2] and its reference [25, Section 11.4]).

Lemma 5.5 ([42, Corollary 9.2], for $\mathcal{R}$ of type A)**.** Let $\mathbf{c}$ be a sequence of exponents such that $c_0 = 0$. Then, the polynomial $V_{\mathbf{c}}(\mathbf{x})$ is a square-free element in $\mathbb{C}[\mathbf{x}]^{\mathrm{sym}}$.

Remark 5.6. Instead of "square-free", [42] uses the term "separable", which does not have a standard meaning (in the multivariate context) and has not been defined in [42]. However, the sentence following (7.2) in [42] together with the proofs of its Corollaries 9.1 and 9.2 make it rather clear that Rajan's "separable" is exactly our "square-free", at least over $\mathbb{C}$.[1]

Lemma 5.7 ([42, Proposition 9.1], for $\mathcal{R}$ of type A)**.** Let $\mathbf{c}$, $\mathbf{d}$ be two sequences of exponents of length k such that $c_0 = d_0 = 0$ and $\mathbf{c} \neq \mathbf{d}$. Denote $d = \gcd(\mathbf{c} \mid\mid \mathbf{d})$, and let $\mathbf{x}$ be a sequence of indeterminates of length k. Then, the polynomials

$$\frac{V_{\mathbf{c}}}{V_{d\cdot\mathbf{e}_k}} \qquad \text{and} \qquad \frac{V_{\mathbf{d}}}{V_{d\cdot\mathbf{e}_k}} \tag{5.6}$$

are coprime in $\mathbb{C}[\mathbf{x}]^{\mathrm{sym}}$.

[1] This conclusion is also consistent with the fact that being square-free is equivalent to separability in the case of a univariate polynomial $P(x) \in \mathbb{C}[x]$.

Remark 5.8. Note that, whenever $\mathbf{c}$ is a sequence of exponents of length k, and d is a divisor of $\gcd(\mathbf{c})$, we have $\mathbf{c} = d \cdot \mathbf{c}'$ for some $\mathbf{c}'$ and

$$\frac{S_{\mathbf{c}}(\mathbf{x})}{S_{d\cdot\mathbf{e}_k}(\mathbf{x})} = \frac{V_{\mathbf{c}}(\mathbf{x})}{V_{d\cdot\mathbf{e}_k}(\mathbf{x})} = S_{\mathbf{c}'}(x_0^d, x_1^d, \ldots, x_{k-1}^d).$$

In particular, the right-hand side shows that this polynomial has integer coefficients, which makes projecting it to finite fields straightforward.

We now need to translate these results to finite fields. For this, we will use the following two facts; although both seem fairly standard, their rigorous proofs take some place, and we could not find any substantial part of them in print. Hence, we provide those proofs below.

Fact 5.9. Let K be a field, and $P, Q \in K[\mathbf{x}]^{\mathrm{sym}}$ be two polynomials coprime in $K[\mathbf{x}]^{\mathrm{sym}}$. Then, P and Q are coprime also in $K[\mathbf{x}]$.

Proof. Suppose that P and Q have a common non-constant and non-symmetric divisor A. By symmetry, for every $\sigma \in \Sigma_{\mathbf{x}}$, A^σ also divides P and Q. Let B be the least common multiple of all A^σ; since $K[\mathbf{x}]$ is factorial, B is well defined up to multiplication by a non-zero constant. Clearly, B divides P and Q; moreover, it must be semi-symmetric (see Section 1.1.4).

If B is symmetric, then we are done. Otherwise, let $c : \Sigma_{\mathbf{x}} \to K^\times$ be such that $B^\sigma = c(\sigma) \cdot B$ for all $\sigma \in \Sigma_{\mathbf{x}}$. For every $\sigma, \sigma' \in \Sigma_{\mathbf{c}}$, we have

$$B^{\sigma\circ\sigma'} = \left(B^{\sigma'}\right)^\sigma = \left(c(\sigma') \cdot B\right)^\sigma = c(\sigma') \cdot B^\sigma = c(\sigma) \cdot c(\sigma') \cdot B,$$

which implies that $c : \Sigma_{\mathbf{x}} \to K^\times$ is a group homomorphism; we have just assumed that it is not trivial. Since $K^\times$ is abelian, c must vanish on the commutator subgroup of $\Sigma_{\mathbf{x}}$, i.e. on all even permutations, and consequently it must return -1 on all odd permutations. This means that the polynomials

$$B, \qquad P/B, \qquad Q/B$$

are all skew-symmetric in the sense of [41, Section 3.1.2]. Then, they all must be divisible by the Vandermonde determinant $V(\mathbf{x})$ [41, Theorem 3.1.2], which means in particular that $V(\mathbf{x})^2$ is a common symmetric divisor of P and Q. □

Fact 5.10. Let $\mathbf{x}$ be a sequence of indeterminates, and A, B be two polynomials in $\mathbb{Z}[\mathbf{x}]$ which are coprime in $\mathbb{C}[\mathbf{x}]$. Then, there exists some $n_{A,B}$ such that, for every prime $p > n_{A,B}$ and every field K of characteristic p, the projections $\widetilde{A}$, $\widetilde{B}$ of A, B to $K[\mathbf{x}]$ are coprime.

We start with an auxiliary fact:

Fact 5.11. Let K be a field, and $\mathbf{x}$ be a sequence of indeterminates of length k. Then, two polynomials $A, B \in K[\mathbf{x}]$ are coprime in $K[\mathbf{x}]$ if and only if, for every $0 \leqslant i < k$, they are coprime in $(K[\hat{\mathbf{x}}_i])[x_i]$.

Proof. Suppose that A, B have a non-constant common factor C in $K[\mathbf{x}]$ but they are coprime in $K_i = (K[\hat{\mathbf{x}}_i])[x_i]$ for every $0 \leqslant i < k$. This means that C must be invertible as an element of K_i, i.e. its degree with respect to x_i must be zero. Since i is arbitrary, C must be constant in $K[\mathbf{x}]$, a contradiction.

Conversely, suppose that A, B are coprime in $K[\mathbf{x}]$ but they have a non-invertible common factor C in K_i for some $0 \leqslant i < k$. Let $\mathrm{cont}(P) \in (K[\hat{\mathbf{x}}_i])$ denote the content of a polynomial $P \in K_i$. Denote $d = \gcd(\mathrm{cont}(A), \mathrm{cont}(B))$, and let $C' = \frac{d}{\mathrm{cont}(C)} \cdot C$. Then, by the well-known Gauss Lemma [29, Chapter IV, Theorem 2.1], we have

$$\mathrm{cont}(C') = d, \qquad \mathrm{cont}(A/C') = \frac{\mathrm{cont}(A)}{d}, \qquad \mathrm{cont}(B/C') = \frac{\mathrm{cont}(B)}{d}.$$

By the definition of d, all these three values belong to $K[\hat{\mathbf{x}}_i]$, which implies that C', A/C' and B/C' belong to $K[\mathbf{x}]$. Hence, C' is a common factor of A and B in $K[\mathbf{x}]$, and it cannot be constant in $K[\mathbf{x}]$ because C is non-invertible in K_i. This gives a contradiction, and finishes the proof. □

Proof of Fact 5.10. For every $0 \leqslant i < k$, Fact 5.11 implies that A, B are coprime in $(\mathbb{C}[\hat{\mathbf{x}}_i])[x_i]$, so their resultant R_i computed in this setting must be a non-zero element in $\mathbb{Z}[\hat{\mathbf{x}}_i]$. Marking the projection from $\mathbb{Z}$ to K by a tilde, it is clear that the resultant of $\widetilde{A}$ and $\widetilde{B}$, treated as elements of $(K[\hat{\mathbf{x}}_i])[x_i]$, is exactly $\widetilde{R_i} \in K[\hat{\mathbf{x}}_i]$. Hence, $\widetilde{A}$ and $\widetilde{B}$ are coprime in $(K[\hat{\mathbf{x}}_i])[x_i]$ whenever p exceeds the number N_i defined as the minimum absolute value of all non-zero coefficients of $R_i \in \mathbb{Z}[\hat{\mathbf{x}}_i] \setminus \{0\}$.

Now, if $p > \max_{0 \leqslant i < k} N_i$, then the projections of A and B to $(K[\hat{\mathbf{x}}_i])[x_i])$ are coprime for every i. Then, by using Fact 5.11 in the other direction, we deduce that $\widetilde{A}$ and $\widetilde{B}$ are coprime in $K[\mathbf{x}]$, as desired. □

Proper proof of Theorem 6

1. Let $\mathbf{c}$ be a sequence of exponents of length $k \geqslant 2$ and $0 \leqslant i < k$ such that $\hat{\mathbf{c}}_i$ is not arithmetic. (Note that this implies $k \geqslant 3$). Let

$$j = \begin{cases} k-1 & \text{if } i = 0, \\ \text{any element of } \mathbf{e}_k \setminus \{0, i\} & \text{otherwise.} \end{cases}$$

Then, we have $j \neq i$; moreover, the sequences

$$\mathbf{a} = \hat{\mathbf{c}}_i - \hat{c}_{i,0}, \qquad \mathbf{b} = \hat{\mathbf{c}}_j - \hat{c}_{j,0}$$

must be distinct: this is clear when $i \neq 0$ (since then $\hat{c}_{i,0} = c_0 = \hat{c}_{j,0}$), while for $i = 0$ and $j = k-1$, $\mathbf{a} = \mathbf{b}$ would imply that $\mathbf{c}$ (and hence also $\hat{\mathbf{c}}_i$) is arithmetic.

2. Let $d = \gcd(\mathbf{a})$ and $d' = \gcd(\mathbf{a}||\mathbf{b})$. Let $\mathbf{y}$ be a sequence of indeterminates of length $k-1$. By Theorem I, the polynomial

$$Q = \frac{V_{\mathbf{a}}}{V_{d \cdot \mathbf{e}_{k-1}}} = \frac{S_{\mathbf{a}}}{S_{d \cdot \mathbf{e}_{k-1}}} \in \mathbb{C}[\mathbf{y}]^{\mathrm{sym}}$$

is irreducible (it is not constant since $\hat{\mathbf{c}}_i$ is not arithmetic). We also note that Q must be coprime (in $\mathbb{C}[\mathbf{y}]$):

- to $V_{\mathbf{a}}/Q = V_{d \cdot \mathbf{e}_{k-1}}$, by Lemma 5.5 and Fact 5.9;
- to $S_{d' \cdot \mathbf{e}_{k-1}}$, since $d' \mid d$ implies $S_{d' \cdot \mathbf{e}_{k-1}} \mid V_{d' \cdot \mathbf{e}_{k-1}} \mid V_{d \cdot \mathbf{e}_{k-1}}$;

- to $S_{\mathbf{b}}/S_{d'\cdot\mathbf{e}_{k-1}}$, by Lemma 5.7, Fact 5.9, and the fact that

$$d' \mid d \quad \Longrightarrow \quad V_{d'\cdot\mathbf{e}_{k-1}} \mid V_{d\cdot\mathbf{e}_{k-1}} \quad \Longrightarrow \quad S_{d'\cdot\mathbf{e}_{k-1}} \mid S_{d\cdot\mathbf{e}_{k-1}} \quad \Longrightarrow \quad Q = \frac{S_{\mathbf{a}}}{S_{d\cdot\mathbf{e}_{k-1}}} \;\Big|\; \frac{S_{\mathbf{a}}}{S_{d'\cdot\mathbf{e}_{k-1}}}.$$

Altogether, it follows that Q is coprime to the product $(S_{\mathbf{b}}/S_{d'\cdot\mathbf{e}_{k-1}}) \cdot S_{d'\cdot\mathbf{e}_{k-1}} = S_{\mathbf{b}}$.

3. By Remark 5.8, Q has integer coefficients; hence, for any field K of characteristic p, the projection $\widetilde{Q}$ of Q to K is well-defined. Moreover, $\widetilde{Q}$ is clearly a divisor of $S_{\mathbf{a}} \in K[\mathbf{y}]$. Now, Corollary 5.4 ensures that $\widetilde{Q}$ is irreducible for p sufficiently large, and step 2 together with Fact 5.10 implies that it is coprime to $S_{\mathbf{b}} \in K[\mathbf{y}]$, also if p is sufficiently large.

Altogether, this means that, for large p, the assumptions of Lemma 4.28 are satisfied for $\mathbf{c}$ with $A = \widetilde{Q}$. Hence, by Lemma 4.28, for any q which is a power of such p, the number of max-length $(\mathbf{c}, i)$-privileged tracks over $\mathbb{F}_q$ is $\Theta(q^{k-2})$, q.e.d. □

5.2.2 Bounds for the characteristic

The lower bound for p hidden in Theorem 6 depends in particular on the bound $n_{\mathbf{c}}$ in Corollary 5.4. Unfortunately, the computational complexity of the latter is hardly acceptable, at least if we utilize the statement from [47], or apply the consecutive steps described in [43] and its reference [24] without any kind of tricky optimization.

Here, the term "computational complexity" is used to cover two distinct issues. First, a straightforward computation leads to values of $n_{\mathbf{c}}$ which grow extremely rapidly, in particular, multiply exponentially in $k = |\mathbf{c}|$; for example, [47] provides an estimate of the form

$$n_{\mathbf{c}} \leqslant \big(4M\big)^{N^{2^N}}, \qquad \text{where} \quad N = \binom{c_{k-1} + k - 1}{k - 1},$$

and where M denotes the sum of all coefficients of $S_{\mathbf{c}}(\mathbf{x})$, usually far above $k!$.

Second, while such bounds can be strengthened by a more precise computation, any significant improvement seems to require an amount of computation even exceeding the resulting bound. (If this looks surprising, recall that computing the determinant of a random 0-1 matrix of size $n \times n$ will usually take $\Theta(n^3)$ arithmetical operations, even if the result itself happens to be much smaller). As a consequence, the author has so far failed to compute the value $n_{\mathbf{c}}$ (or find a reasonable estimate from above) even in the simplest non-trivial cases, e.g. for $\mathbf{c} = (0, 1, 4)$.

In other words, we know that $S_{(0,1,4)}$ must be irreducible over $\overline{\mathbb{F}_p}$ for p large, but we have very poor control on what "large" means. In particular, we have no idea how the currently described approach could be strengthened to obtain an estimate of the RSL type (see introduction to the thesis). This motivates the work performed in the rest of this chapter.

5.2.3 Common ideas of [37] and [42]

Interestingly, even though the papers [37] and [42] are unrelated in their origin, primary topic and citations, both authors use very similar techniques.

One of these is repeated, multi-directional use of what both authors call *generalized Eisenstein criterion*, roughly involving a "half-way" application of the original Eisenstein's trick. This approach will be presented in detail in Section 5.5.3.

Another useful trick is to perceive $S_{\mathbf{c}}(\mathbf{x})$ as the quotient $V_{\mathbf{c}}(\mathbf{x})/V_{\mathbf{e}_k}(\mathbf{x})$, and focus on the dividend $V_{\mathbf{c}}$ rather than on $S_{\mathbf{c}}$ itself. The point of this idea is that the generalized Eisenstein criterion can be used to limit the range of possible divisors of $V_{\mathbf{c}}$, while the advantage of this polynomial over $S_{\mathbf{c}}$ is that its coefficients are much sparser — and thus easier to operate with — than those of $S_{\mathbf{c}}$. (This will be used in Sections 5.5.5 and 5.5.6).

5.3 Preliminaries

This section gathers a number of auxiliary notations and facts, useful in the proofs of Theorems 7 and 7'. The majority of them will be used in both reasonings presented in Sections 5.5 and 5.6.

5.3.1 Newton polytope and polynomial shape

Let $\mathbf{x}$ be a sequence of indeterminates of length k, and let $P \in K[\mathbf{x}]$ have the following expansion:

$$P(\mathbf{x}) = \sum_{\mathbf{s}\in\mathbb{Z}^k} a_{\mathbf{s}} \cdot \mathbf{x}^{\mathbf{s}},$$

in which we assume $a_{\mathbf{s}}$ to be defined for every $\mathbf{s} \in \mathbb{Z}^k$, and equal to 0 for all but finitely many $\mathbf{s}$.

Following some authors (see [19] and its references), we introduce the following notion:

Definition 5.12. The *Newton polytope* (in short: *N-polytope*) of P, denoted $New(P)$, is the convex hull in $\mathbb{R}^k$ of the (finite) set $\operatorname{sh} P = \{\mathbf{s} \in \mathbb{Z}^k \mid a_{\mathbf{s}} \neq 0\} \subseteq \mathbb{N}^k$.

For the above set $\operatorname{sh} P$, we introduce the name "*shape* of P".

It is well known that, for $P, Q \in K[\mathbf{x}]$, the polytope $New(P \cdot Q)$ is obtained from $New(P)$, $New(Q)$ as their sum (sometimes called *Minkowski sum*), in the following natural sense:

$$A + B = \{a + b \mid a \in A,\, b \in B\} \qquad \text{for } A, B \subseteq \mathbb{R}^n \tag{5.7}$$

This leads to a (commonly known) sufficient criterion for irreducibility of a given polynomial $P \in K[\mathbf{x}]$: it is enough to show that $New(P)$ cannot be decomposed (in the sense of (5.7)) into two summands contained in $\mathbb{R}^k_{\geqslant 0}$ and distinct from the one-point set $\{(0, \ldots, 0)\}$. (In fact, weaker *integral decomposability* suffices; see [19, p. 6]). Although we will not use this fact directly, its general idea will be crucial in Section 5.6.

5.3.2 Gradations and faces

In this subsection, we assume that $P \in K[\mathbf{x}] \setminus \{0\}$.

In the following auxiliary definitions, vectors $\mathbf{s} \in \mathbb{Z}^k$ are in fact used to describe all (signed integral) gradations of the polynomial ring $K[\mathbf{x}]$. For any such vector $\mathbf{s}$, we define:

- the $\mathbf{s}$-*degree* of a monomial $a \cdot \mathbf{x}^{\mathbf{s}'}$ to be the scalar product $\mathbf{s} \circ \mathbf{s}' = \sum_{i=0}^{k-1} s_i s'_i$;
- the $\mathbf{s}$-*degree* of P (denoted $\deg_{\mathbf{s}} P$) as the maximal $\mathbf{s}$-degree of its monomials (which might be negative);
- the *maximal (resp. minimal)* $\mathbf{s}$-*face* of P (denoted $\max_{\mathbf{s}} P$, resp. $\min_{\mathbf{s}} P$) as the sum of all monomials in P with the maximal (resp. minimal) $\mathbf{s}$-degree;
- the j-*th maximal (resp. minimal)* $\mathbf{s}$-*degree in* P as the j-th maximal (resp. minimal) value in the set of $\mathbf{s}$-degrees of monomials in P, provided that this set has $\geqslant j$ elements; otherwise we leave this number undefined;
- the $\mathbf{s}$-*width* of P (denoted $\operatorname{wth}_{\mathbf{s}} P$) by the formula

$$\operatorname*{wth}_{\mathbf{s}} P \;=\; \operatorname*{deg}_{\mathbf{s}} \max_{\mathbf{s}} P - \operatorname*{deg}_{\mathbf{s}} \min_{\mathbf{s}} P \;=\; \operatorname*{deg}_{\mathbf{s}} P + \operatorname*{deg}_{-\mathbf{s}} P.$$

Clearly, the operators $\max_{\mathbf{s}}$, $\min_{\mathbf{s}}$ are multiplicative, while $\deg_{\mathbf{s}}$ and consequently $\operatorname{wth}_{\mathbf{s}}$ are additive under multiplication of non-zero polynomials.

We note that

$$New(P) \text{ and } \mathbf{s} \text{ determine } New(\max_{\mathbf{s}} P). \tag{5.8}$$

Indeed, we have

$$New(\max_{\mathbf{s}} P) = New(P) \cap \left\{ \mathbf{s}' \in \mathbb{R}^k \,\middle|\, \mathbf{s}' \circ \mathbf{s} = \deg_{\mathbf{s}} P \right\}, \tag{5.9}$$

since an analogous equality holds for shapes by the definition of $\max_{\mathbf{s}} P$, and the second argument of the intersection is either the whole $\mathbb{R}^k$ or a hyperplane supporting $New(P)$. In the latter case (i.e. for $\mathbf{s} \neq 0$), $New(\max_{\mathbf{s}} P)$ can be though of as a "face" of $New(P)$; however, their topological dimensions may differ by more than one.

Any vector $\mathbf{s} \in \mathbb{Z}^k$ of the form $\alpha \cdot \varepsilon_i$ with $\alpha = \pm 1$ and $0 \leqslant i \leqslant k-1$ will be called *standard*. For such $\mathbf{s}$, we simplify the above notation by replacing "$\mathbf{s}$" with "i" (if $\alpha = 1$) or "$-i$" (if $\alpha = -1$). In particular, the i-*degree* of P is just its degree as a polynomial in x_i.

A *standard face* of P is any face of the form $\max_{\mathbf{s}} P$ for a standard vector $\mathbf{s}$.

For $a, b \geqslant 0$, an *iterated standard face of signature* (a, b) of P is as any expression of the form

$$\max_{\mathbf{s}_0} \max_{\mathbf{s}_1} \ldots \max_{\mathbf{s}_{l-1}} P,$$

where $l = a + b$ and

$$\mathbf{s}_0 = \alpha_0 \cdot \varepsilon_{i_0}, \quad \ldots, \quad \mathbf{s}_{l-1} = \alpha_{l-1} \cdot \varepsilon_{i_{l-1}}$$

are arbitrary standard vectors which are pairwise non-parallel and such that exactly a of the numbers $\alpha_0, \ldots, \alpha_{l-1}$ are positive (and exactly b are negative). Note that this implies $l \leqslant k$.

For a fixed $0 \leqslant l \leqslant k$, we will also speak of *iterated standard faces of order* l of P; this will mean iterated standard faces of all signatures (a, b) such that $a + b = l$.

5.3.3 Monomial decomposition

Definition 5.13. For $Q \in K[\mathbf{x}]$, we define its *monomial* and *non-monomial part*, denoted respectively by $M(Q)$ and $\widetilde{Q}$, as follows:

$$M(Q) = \begin{cases} \prod_{l=0}^{k-1} x_l^{\deg_l \min_l Q} & \text{for } Q \neq 0, \\ 1 & \text{for } Q = 0, \end{cases} \qquad \widetilde{Q} = \frac{Q}{M(Q)}.$$

It is easy to see that $M(Q)$ divides Q (so that $\widetilde{Q} \in K[\mathbf{x}]$), and that $M(Q)$, $\widetilde{Q}$ both depend multiplicatively on Q.

As in general divisibility theory, we say that $P, Q \in K[\mathbf{x}]$ are *associated* (notation: $P \simeq Q$) if

$$P = a \cdot Q \qquad \text{for some } a \in K \setminus \{0\}.$$

We will call P, Q *monomially equivalent* (notation: $P \sim Q$) if $\widetilde{P}$ and $\widetilde{Q}$ are associated, i.e. if

$$P = a \cdot \mathbf{x}^{\mathbf{s}} \cdot Q \qquad \text{for some } a \in K \setminus \{0\},\ \mathbf{s} \in \mathbb{Z}^k.$$

Clearly, $\sim$ and $\simeq$ are equivalence relations, and $\simeq$ implies $\sim$. We also note that $P \sim Q$ implies $\max_{\mathbf{s}} P \sim \max_{\mathbf{s}} Q$ as well as $\mathrm{wth}_{\mathbf{s}} P = \mathrm{wth}_{\mathbf{s}} Q$ for every $\mathbf{s}$. It is also evident that association preserves shape, and that monomial equivalence preserves shape up to a vector translation.

5.3.4 Basic properties of $V_{\mathbf{c}}$ and $S_{\mathbf{c}}$

In our considerations, we will concentrate on the shapes of $V_{\mathbf{c}}$ and $S_{\mathbf{c}}$, particularly on their i-faces for $0 \leqslant i < k-1$. For convenience, we will precompute these data now. First, by Laplace expansion, we have (cf. [42, (4.1)]):

$$V_{\mathbf{c}}(\mathbf{x}) = \sum_{j=0}^{k-1} (-1)^{i+j} \cdot x_i^{c_j} \cdot V_{\hat{\mathbf{c}}_j}(\hat{\mathbf{x}}_i), \tag{5.10}$$

whence in particular

$$\begin{aligned} \max_i V_{\mathbf{c}}(\mathbf{x}) &\simeq x_i^{c_{k-1}} \cdot V_{\hat{\mathbf{c}}_{k-1}}(\hat{\mathbf{x}}_i), \\ \min_i V_{\mathbf{c}}(\mathbf{x}) &\simeq x_i^{c_0} \cdot V_{\hat{\mathbf{c}}_0}(\hat{\mathbf{x}}_i). \end{aligned} \tag{5.11}$$

Also, note that (5.10) implies

$$V_{\mathbf{c}+l}(\mathbf{x}) = \Big(\prod_{i=0}^{k-1} x_i\Big)^l \cdot V_{\mathbf{c}}(\mathbf{x}) \qquad \text{for } l \geqslant 0. \tag{5.12}$$

On the other hand, for $c_0 = 0$, (5.10) implies that $V_{\mathbf{c}}(\mathbf{x})$ is not divisible by any of the x_i. Together with (5.12), this means that

$$\widetilde{V_{\mathbf{c}}(\mathbf{x})} = V_{\mathbf{c}-c_0}(\mathbf{x}). \tag{5.13}$$

Now, since $S_{\mathbf{c}} = V_{\mathbf{c}}/V_{\mathbf{e}_k}$, (5.11) and (5.13) lead to

$$\max_i S_{\mathbf{c}}(\mathbf{x}) \simeq x_i^{c_{k-1}-(k-1)} \cdot S_{\hat{\mathbf{c}}_{k-1}}(\hat{\mathbf{x}}_i), \tag{5.14a}$$

$$\min_i S_{\mathbf{c}}(\mathbf{x}) \simeq x_i^{c_0} \cdot S_{\hat{\mathbf{c}}_0}(\hat{\mathbf{x}}_i), \tag{5.14b}$$

$$\operatorname*{wth}_i S_{\mathbf{c}}(\mathbf{x}) = c_{k-1} - c_0 - (k-1), \tag{5.14c}$$

$$\widetilde{S_{\mathbf{c}}(\mathbf{x})} = S_{\mathbf{c}-c_0}(\mathbf{x}). \tag{5.14d}$$

Finally, we state the following auxiliary fact, which will be useful in the proof of Fact 5.19 in Section 5.5, and in the proof Theorem 8 in Section 5.7.

Fact 5.14. Let $\mathbf{c}$ and $\mathbf{c}'$ be two distinct sequences of exponents of the same length $k \geqslant 0$. Let K be a field, and $\mathbf{x}$ be a sequence of indeterminates of length k. Assume that the Schur polynomials $S_{\mathbf{c}}, S_{\mathbf{c}'}$ are both either constant or irreducible in $K[\mathbf{x}]$. Then, they are coprime in $K[\mathbf{x}]$.

Proof. If either of the polynomials is constant, then we are done. Assume that both are irreducible; then, it suffices to ensure that they are not associated. Suppose the contrary. Then, multiplying both expressions by $V_{\mathbf{e}_k}(\mathbf{x})$ yields that $V_{\mathbf{c}}(\mathbf{x}) \simeq V_{\mathbf{c}'}(\mathbf{x})$; in particular, they agree upon shape. However, it is easy to verify by (5.10) that every sequence $\mathbf{s} \in \operatorname{sh} V_{\mathbf{c}}$ is a permutation of $\mathbf{c}$; hence, $\operatorname{sh} V_{\mathbf{c}} = \operatorname{sh} V_{\mathbf{c}'}$ is impossible. □

5.4 Structure of the induction

The proofs of Theorems 7 and 7' proceed by induction on $k \geqslant 3$.

The case $k = 3$ in Theorem 7 follows immediately from Monge's Theorem H. As for Theorem 7', for $k = 3$ it requires that $P = S_{\mathbf{c}}$, whence it also follows from Theorem H, provided that $p > 0$. The remaining case $k = 3$ and $p = 0$ follows from Theorem I in combination with [43, Theorem 32] (which ensures that irreducibility over $\mathbb{C}$ implies irreducibility over other algebraically closed fields of characteristic 0).

We will now present two different reasonings for the inductive step for higher values of k.

The first argument, essentially borrowed from Rajan [42] and leading to Theorem 7, will be discussed in Section 5.5. The second proof, presented in Section 5.6, will use similar techniques to those of Monge and Rajan, though in a novel way, to obtain Theorem 7'.

In both reasonings, the validity of the claim for a given sequence $\mathbf{c}$ is essentially established on the basis of its validity for $\hat{\mathbf{c}}_{k-1}$ and $\hat{\mathbf{c}}_0 - c_1$; the crucial observation is that the Schur polynomials defined by these sequences are closely related to the standard faces of $S_{\mathbf{c}}$. Notably, such strategy turns out to require $k \geqslant 4$; for $k = 3$, $S_{\mathbf{c}}$ fails to have absolutely irreducible standard faces whenever $c_2 > 4$ (which can be deduced from Section 5.1.1). Therefore it is essential to start the induction as late as at $k = 3$.

5.4.1 Scope of results

We are now ready to discuss our choice of assumptions (on $\mathbf{c}$) for Theorems 7 and 7'.

As long as we simply reduce, according to our inductive strategy, a given sequence $\mathbf{c}$ to its two sub-sequences $\hat{\mathbf{c}}_0 - c_1$ and $\hat{\mathbf{c}}_{k-1}$ — which arise from $\mathbf{c}$ simply by truncating the first/last element and shifting the result to make it begin with zero — it follows easily that we should ultimately restrict to sequences $\mathbf{c}$ such that $c_0 = 0$ and, for every consecutive subsequence $\mathbf{b} \sqsubseteq \mathbf{c}$ of length 3, the Schur polynomial $S_{\mathbf{b}-b_0}$ is known to be irreducible, i.e. the sequence $\mathbf{b} - b_0$ satisfies the assumptions of Theorem H with $d = 1$. Easily to check, this approach produces exactly the assumptions present in Theorem 7.

In fact, such assumptions are probably somewhat superfluous, as the inductive reasoning in [42] manages to prove irreducibility of $S_{\mathbf{c}}$ even if the faces $S_{\hat{\mathbf{c}}_{k-1}}$ and $S_{\hat{\mathbf{c}}_0 - c_1}$ are reducible, primarily by inductive usage of Theorem I in its full strength, including the case $d > 1$. Transferring that method to a general field, if fully successful, would lead to a generalization of Theorem 7 which would be fully analogous to the formulation of Theorem I.

Although [42] uses much Lie-algebraic language, it seems that the base field does not really matter in a vast majority of its proofs. Therefore, the above guidelines almost certainly lead to some generalization of Theorem 7. However, exploiting this idea would force us to analyze a much larger part of [42], including Proposition 5.1 and the proper proof of Theorem 2.3, which would make the whole argument much more complex. Hence, we decided to formulate Theorem 7 in the weaker version, which still seems to be significantly broader than the current state-of-the-art.

5.5 Rajan's proof of Theorem 7

In this section, we perform the inductive step within the proof of Theorem 7, using almost entirely the arguments extracted from [42]. Nevertheless, uncovering the proof from the exposition given in [42] requires some care, as we explain below.

While Rajan considers general simple Lie algebras, it suffices for us to restrict to what he calls "$GL(r)$ case" (by which he usually means taking root systems of type A, as defined in [25, Section 11.4]), and to the case $k \geqslant 4$. Also, as explained in Section 5.4.1, we have strengthened our assumptions on $\mathbf{c}$ according to the statement of Theorem 7. As a result, out of all 39 pages of [42], we will need to refer only to a few, omitting all specifically Lie-algebraic arguments.

Clearly, we need Rajan's results to be ported from $\mathbb{C}$ to an arbitrary base field (which will actually pose no difficulty, at least under our assumptions), and, before that, to be fully translated from the Lie-algebraic language of [42] to a purely polynomial-algebraic one. Such translation has been partially performed in [42]: only within our area of interest, Rajan's (4.1) and Proposition 8.1 are respectively "polynomialized" versions of (4.9) and Proposition 5.2.

However, as we will explain in Section 5.5.2, the "polynomialized" expansion (4.1) is inconsistent with its Lie-algebraic version (4.9). Moreover, (4.1) is formulated in a way which does not clearly indicate its "head-tail symmetry" (see Section 5.5.2), although it is used later in the

proof. Altogether, this introduces some confusion (made evident in Remark 5.17) regarding the proofs of Proposition 8.1 and Lemma 10.1, particularly about the usage of Lemma 4.4 in them, and about the phrase "similarly arguing with the constant term" following (8.4). To clarify these issues, in Section 5.5.2 we will reformulate Rajan's (4.1) to reveal its "head-tail symmetry" hidden in the original form. Then, in Section 5.5.3, we provide an explicitly symmetric version of Lemma 4.4, stated in the polynomial-algebraic language.

Having done that, the rest of the proof can be almost covered by referring the reader to Proposition 8.1 and Lemma 10.1 in [42]; in our setting, one needs to replace references to Lemma 4.4 with our Lemma 5.16, argue for analogues of Corollaries 9.2 and 9.4, and finally link the parts of the proof using our Corollaries 5.22 and 5.25.

However, since the original proof of Lemma 10.1 in [42] contains two more confusing steps (see Remark 5.24), we found it most convenient to slightly modify Rajan's reasoning; this includes in particular switching from "symmetric" to "semi-symmetric" throughout the proof, and yet another modification in the statement of his Lemma 10.1 (see our Fact 5.23).

Finally, we note that the fragments of [42] relevant for our purposes still use some Lie-algebraic terminology, and their notation differs greatly from ours. (In particular, Rajan's $S(\lambda)$ is our $V_{\mathbf{c}}$, rather than the Schur polynomial).

For all the above reasons, for reader's convenience, we decided to reproduce those fragments (somewhat clarified by restructuring and more comments) in Sections 5.5.4–5.5.7. By doing so, we also hope to allow an easy comparison of Rajan's method with that of Section 5.6.

5.5.1 Initial setup

Throughout Section 5.5, we assume that $k \geqslant 4$, and that Theorem 7 has been proved for all smaller values of k. Then, we let

$$\mathbf{c}, \quad p, \quad K$$

satisfy the assumptions of Theorem 7. If $\mathbf{c} = \mathbf{e}_k$, then $S_{\mathbf{c}}$ is clearly constant, and we are done. From now on, we assume that

$$\mathbf{c} \neq \mathbf{e}_k \tag{5.15}$$

and aim at proving that $S_{\mathbf{c}}$ is irreducible over K.

Clearly, in the above setting, each of the sequences $\hat{\mathbf{c}}_0 - c_1$, $\hat{\mathbf{c}}_{k-1}$ must also satisfy (5.1); hence, by the inductive assumption, using (5.14) and the equality $c_0 = 0$, we obtain that, for every $0 \leqslant i < k$,

(5.16)

$$\widetilde{\max_i} S_{\mathbf{c}}(\mathbf{x}) = S_{\hat{\mathbf{c}}_{k-1}}(\hat{\mathbf{x}}_i) \quad \text{is irreducible (for } \hat{\mathbf{c}}_{k-1} \neq \mathbf{e}_{k-1}\text{) or constant (for } \hat{\mathbf{c}}_{k-1} = \mathbf{e}_{k-1}\text{),}$$

$$\widetilde{\min_i} S_{\mathbf{c}}(\mathbf{x}) = S_{\hat{\mathbf{c}}_0 - c_1}(\hat{\mathbf{x}}_i) \quad \text{is irreducible (for } \hat{\mathbf{c}}_0 - c_1 \neq \mathbf{e}_{k-1}\text{) or constant (for } \hat{\mathbf{c}}_0 - c_1 = \mathbf{e}_{k-1}\text{).}$$

5.5.2 Cofactor expansion

Definition 5.15 (cf. [42, (4.1), (4.9)])**.** For a standard vector $\mathbf{s} = \alpha \cdot \varepsilon_i$ and $P \in K[\mathbf{x}] \setminus \{0\}$, we define the *cofactor expansions* of P by the formulae

$$P = \sum_{j=\deg_{\mathbf{s}} \min_{\mathbf{s}} P}^{\deg_{\mathbf{s}} \max_{\mathbf{s}} P} P_j^{(\mathbf{s})} \cdot x_i^{\alpha \cdot j} = \sum_{j=\deg_{\mathbf{s}} \min_{\mathbf{s}} P}^{\deg_{\mathbf{s}} \max_{\mathbf{s}} P} \widetilde{P_j^{(\mathbf{s})}} \cdot \Big(M\big(P_j^{(\mathbf{s})}\big) \cdot x_i^{\alpha \cdot j} \Big). \tag{5.17}$$

Here, the coefficients $P_j^{(\mathbf{s})}$ are defined in a unique way by the first equation, which is basically the expansion of P as a polynomial in x_i with coefficients in $K[\hat{\mathbf{x}}_i]$; then, the expressions $\widetilde{P_j^{(\mathbf{s})}}$ and $M(P_j^{(\mathbf{s})})$ represent the monomial decomposition of $P_j^{(\mathbf{s})}$ according to Definition 5.13.

For $\alpha = -1$, the coefficients remain the same as for $\alpha = 1$ but their numbering is (additively) inverted. This is what we call the *"head-tail" symmetry* of (5.17); it plays a role in the proof.

For $P = V_{\mathbf{c}}$ and $\alpha = 1$, the first expansion is consistent with [42, (4.9)] in the "$GL(r)$ case" (i.e. when $\mathcal{R}$ is of type A), while the second expansion coincides with [42, (4.1)].

In fact, for $P = V_{\mathbf{c}}$, the two expansions differ (i.e. $M(P_j^{(\mathbf{s})}) \neq 1$) only for a single value of j, namely, $j = \deg_i \min_i P$.

5.5.3 Generalized Eisenstein criterion

The term *generalized Eisenstein criterion* appears both in [42] and [37], in a very similar meaning. However, while Monge explicitly considers what he calls "lower and upper signatures", referring exactly to the "head-tail" symmetry in our sense, Rajan formulates his Eisenstein criterion only in one direction (that is, for $\alpha = 1$), despite needing to use both. The statement below explicitly allows the case $\alpha = -1$, in combination with the second flavour of the cofactor expansion (5.17).

Lemma 5.16 (cf. [42, Lemma 4.4] and [37, p. 6])**.** Let $\mathbf{s} \in \mathbb{Z}^k$ be standard and $A \in K[\mathbf{x}]$ be a divisor of $U \in K[\mathbf{x}] \setminus \{0\}$. Denote by u, u' the maximal and second-maximal $\mathbf{s}$-degrees in U (in particular, assume that the latter exists), and by a the maximal $\mathbf{s}$-degree in A. Suppose that $\widetilde{U_u^{(\mathbf{s})}}$ is square-free in $K[\mathbf{x}]$. Then:

$$\widetilde{A_a^{(\mathbf{s})}} \;\Big|\; \widetilde{A_{a-1}^{(\mathbf{s})}}, \widetilde{A_{a-2}^{(\mathbf{s})}}, \ldots, \widetilde{A_{a-(u-u')+1}^{(\mathbf{s})}}. \tag{5.18}$$

Proof. Let $\mathbf{s} = \alpha \cdot \varepsilon_i$. Denote

$$B = U/A, \qquad b = \deg_{\mathbf{s}} B = u - a, \qquad R = K[\hat{\mathbf{x}}_i].$$

Let P be any irreducible factor of $\widetilde{A_a^{(\mathbf{s})}}$. Since $\widetilde{A_a^{(\mathbf{s})}} \cdot \widetilde{B_b^{(\mathbf{s})}} = \widetilde{U_u^{(\mathbf{s})}}$ is square-free, P cannot divide $\widetilde{B_b^{(\mathbf{s})}}$. However, as P divides $\widetilde{A_a^{(\mathbf{s})}}$, it cannot be a monomial, whence

$$P \not| \, B_b^{(\mathbf{s})}. \tag{5.19}$$

Now, let $\mathfrak{p} \lhd R$ be the ideal generated by P, and let π denote the canonical projection $R \to R/\mathfrak{p}$, as well as the induced projection $R[x_i] \to (R/\mathfrak{p})[x_i]$. Since $\pi(U) = \pi(A) \cdot \pi(B)$, and $R/\mathfrak{p}$ is an integral domain, we deduce that

$$u' \geqslant \deg_{\mathbf{s}} \pi(U) = \deg_{\mathbf{s}} \pi(A) + \deg_{\mathbf{s}} \pi(B) \overset{(5.19)}{=} \deg_{\mathbf{s}} \pi(A) + b,$$

so

$$\deg_{\mathbf{s}} \pi(A) \leqslant u' - b = a - (u - u').$$

Therefore, for every $j > a - (u - u')$, we have $P \mid A_j^{(\mathbf{s})}$. Now, fix any such j and let P vary over all irreducible factors of $\widetilde{A_a^{(\mathbf{s})}}$. Then, $A_j^{(\mathbf{s})}$ must be divisible by the least common multiple of all such factors; this must be $\widetilde{A_a^{(\mathbf{s})}}$ (up to association) because it is square-free (as a divisor of $\widetilde{U_u^{(\mathbf{s})}}$). Hence, $\widetilde{A_a^{(\mathbf{s})}} \mid A_j^{(\mathbf{s})}$, q.e.d. □

Remark 5.17. An analogue of Lemma 5.16 with all tildes removed in (5.18) (but *not* removed in the assumption that $\widetilde{U_u^{(\mathbf{s})}}$ is square-free) does not hold. For example, taking $\mathbf{c} = (0, 2)$, $\mathbf{s} = -\varepsilon_0$, $U = V_{\mathbf{c}}$, $A = S_{\mathbf{c}}$ leads to

$$U = x_1^2 - x_0^2, \quad A = x_0 + x_1, \quad u = a = 0, \quad u' = -2, \quad A_a^{(\mathbf{s})} = x_1 \not\mid 1 = A_{a-1}^{(\mathbf{s})}.$$

On the other hand, Lemma 5.16 *would* hold (with an even simpler proof) once we remove *all* tildes from its formulation. However, the obtained result would be too weak for our purposes: for $U = V_{\mathbf{c}}$ (which is how we wish to use Lemma 5.16), $U_u^{(\mathbf{s})}$ without a tilde is not square-free whenever $\alpha = -1$ and $c_1 \geqslant 2$, so in these cases the lemma would not be applicable. (Adding the tilde over $U_u^{(\mathbf{s})}$ solves this problem, as we will show in Fact 5.18 in Section 5.5.4).

This shows that, although the formulation of Lemma 4.4 in [42] indicates interpreting "cofactor expansion" according to (4.9), some its applications rely essentially on replacing (4.9) with (4.1). This applies particularly to the phrase "similarly arguing with the constant term" following (8.4).

5.5.4 Replacements for coprimality properties

Fact 5.18 (replacing [42, Corollary 9.2])**.** For every standard $\mathbf{s} \in \mathbb{Z}^k$, $\widetilde{\max_{\mathbf{s}} V_{\mathbf{c}}}(\mathbf{x})$ is square-free in $K[\mathbf{x}]$.

Proof. Let $\mathbf{s} = \alpha \cdot \varepsilon_i$. By (5.11) and (5.13), the considered polynomial is associated with

$$V_{\mathbf{b}}(\hat{\mathbf{x}}_i) = V_{\mathbf{e}_{k-1}}(\hat{\mathbf{x}}_i) \cdot S_{\mathbf{b}}(\hat{\mathbf{x}}_i) = \prod_{\substack{0 \leqslant j_1 < j_2 < k, \\ j_1, j_2 \neq i}} (x_{j_1} - x_{j_2}) \cdot S_{\mathbf{b}}(\hat{\mathbf{x}}_i),$$

where $\mathbf{b}$ is either $\hat{\mathbf{c}}_{k-1}$ or $\hat{\mathbf{c}}_0 - c_1$. The binomials $x_{j_1} - x_{j_2}$ are clearly irreducible and pairwise coprime. As for $S_{\mathbf{b}}(\hat{\mathbf{x}}_i)$, it is either constant or irreducible by (5.16), and it is not associated with any of the binomials $x_{j_1} - x_{j_2}$ because neither of them lies in $K[\hat{\mathbf{x}}_i]^{\mathrm{sym}}$ while $S_{\mathbf{b}}$ does. Hence, $S_{\mathbf{b}}$ is coprime to each of them. This proves that the whole product is square-free. □

Fact 5.19 (replacing [42, Corollary 9.4])**.** For every $0 \leqslant i < k$, we have

$$\gcd\left(\max_i S_{\mathbf{c}}, \min_i S_{\mathbf{c}}\right) \sim 1.$$

Proof. It suffices to prove that the non-monomial parts of $\max_i S_{\mathbf{c}}$ and $\min_i S_{\mathbf{c}}$ are coprime. By (5.14), these are respectively associated with $S_{\hat{\mathbf{c}}_{k-1}}(\hat{\mathbf{x}}_i)$ and $S_{\hat{\mathbf{c}}_0 - c_1}(\hat{\mathbf{x}}_i)$, both constant or irreducible by virtue of (5.16). If at least one of them is constant, we are done. Otherwise, Fact 5.14 shows coprimality unless $\hat{\mathbf{c}}_{k-1} = \hat{\mathbf{c}}_0 - c_1$, which is impossible because it would imply that $\mathbf{c}$ is an arithmetic progression, contrary to (5.1) and (5.15). □

5.5.5 Wideness of factors

Fact 5.20 (parts of the proof of Proposition 8.1 of [42])**.** Let C be a factor of $S_{\mathbf{c}}(\mathbf{x})$, $\mathbf{s} \in \mathbb{Z}^k$ be standard and $0 \leqslant j < k$. Denote by $v_{\mathbf{s}}, v'_{\mathbf{s}}$ the maximal and second-maximal $\mathbf{s}$-degree in $V_{\mathbf{c}}(\mathbf{x})$ (the latter exists since $k \geqslant 2$). Then:

(a) If $\max_{\mathbf{s}} C \sim 1$ and C is semi-symmetric, then $\operatorname{wth}_{\mathbf{s}}(S_{\mathbf{c}}/C) \geqslant \operatorname{wth}_j \max_{\mathbf{s}} S_{\mathbf{c}}$;

(b) If $\max_{\mathbf{s}} C \not\sim 1$, then $\operatorname{wth}_{\mathbf{s}} C \geqslant v_{\mathbf{s}} - v'_{\mathbf{s}}$.

Proof. **(a)** Denote $D = S_{\mathbf{c}}/C$. Since $S_{\mathbf{c}}$ and C are semi-symmetric, so is D. Using this fact and multiplicativity of $\max_{\mathbf{s}}$, we obtain that $\max_{\mathbf{s}} C \sim 1$ implies that

$$\operatorname*{wth}_{\mathbf{s}} D = \operatorname*{wth}_j D \geqslant \operatorname*{wth}_j \max_{\mathbf{s}} D = \operatorname*{wth}_j \max_{\mathbf{s}} S_{\mathbf{c}} - \operatorname*{wth}_j \max_{\mathbf{s}} C = \operatorname*{wth}_j \max_{\mathbf{s}} S_{\mathbf{c}}.$$

(b) Suppose that C does not satisfy the implication claimed, and denote $c = \deg_{\mathbf{s}} C$. We wish to apply Lemma 5.16 for $U = V_{\mathbf{c}}$ and $A = C$. Since $\widetilde{U_u^{(\mathbf{s})}} = \widetilde{\max_{\mathbf{s}} U}$, its assumptions are satisfied by virtue of Fact 5.18.

Since we have assumed that $\operatorname{wth}_{\mathbf{s}} C < v_{\mathbf{s}} - v'_{\mathbf{s}}$, Lemma 5.16 implies that $\widetilde{C_c^{(\mathbf{s})}}$ divides the whole C, which in turn divides $S_{\mathbf{c}}(\mathbf{x})$. Since $\widetilde{C_c^{(\mathbf{s})}}$ does not depend on x_i, it must divide $\max_i S_{\mathbf{c}}$ and $\min_i S_{\mathbf{c}}$. Then, by Fact 5.19, it must be a monomial, which contradicts the assumption that $\max_{\mathbf{s}} C \not\sim 1$. This finishes the proof. □

5.5.6 Inexistence of semi-symmetric factorizations

Lemma 5.21 (cf. [42, Proposition 8.1])**.** Let $S_{\mathbf{c}} = A \cdot B$ for some $A, B \in K[\mathbf{x}]$ and suppose that A, B are non-constant and semi-symmetric. Then, for every $0 \leqslant i \leqslant k-1$, we have:

$$\max_i A, \max_i B \not\sim 1 \qquad \text{or} \qquad \min_i A, \min_i B \not\sim 1.$$

While the above formulation resembles that of Proposition 8.1 in [42], in our setting (5.16) implies that the non-monomial part of $\max_i A \cdot \max_i B = \max_i S_{\mathbf{c}}$ is constant or irreducible, so the conditions $\max_i A$, $\max_i B \not\sim 1$ lead to an immediate contradiction. The same happens on the minimum side. Therefore, Lemma 5.21 implies:

Corollary 5.22. If $S_{\mathbf{c}} = A \cdot B$ with A, B semi-symmetric, then A or B is a constant. □

Proof of Lemma 5.21. **1.** (Rajan's (8.1)) We claim that $\max_i B$, $\min_i B$ cannot be simultaneously monomials. Indeed, suppose that $\max_i B \sim 1$, and denote

$$S = S_{\mathbf{c}}, \qquad b = \deg_i B, \qquad s = \deg_i S.$$

Then, $B_b^{(i)}$ is a monomial which divides $S_s^{(i)}$; the latter is associated with $S_{\hat{\mathbf{c}}_{k-1}}(\hat{\mathbf{x}}_i)$ by (5.14a) and therefore is not divisible by any non-trivial monomial by (5.14d) and the assumption that $c_0 = 0$. Hence, $B_b^{(i)} \simeq 1$, so $\max_i B \simeq x_i^b$. Since B is semi-symmetric and non-constant, it follows that $b > 0$, and that $\min_i B$ contains a monomial associated with x_j^b for every $j \neq i$. Since $b > 0$, these monomials are not associated to each other; hence, $\min_i B \not\sim 1$, as desired.

Analogously, $\max_i A$ and $\min_i A$ cannot be simultaneously monomials.

2. Suppose now that the claim of the lemma does not hold. Then, at least one of $\max_i A$, $\max_i B$ is a monomial; without losing generality, let it be $\max_i A$. Further, at least one of $\min_i A$, $\min_i B$ is a monomial; by step 1 (for A), this may happen only for $\min_i B$. By applying step 1 again (now for B), we obtain that

$$\max_i A \sim 1, \qquad \min_i A \not\sim 1, \qquad \max_i B \not\sim 1, \qquad \min_i B \sim 1.$$

It remains to show that this situation is impossible.

3. Choose any $0 \leqslant j < k$ distinct from i. By a four-fold application of Fact 5.20 with $\mathbf{s} = \pm\varepsilon_i$ and $C \in \{A, B\}$, and then simplifying the right-hand sides with (5.10) and (5.14), we obtain (using the notations $v_{\mathbf{s}}$, $v'_{\mathbf{s}}$ of Fact 5.20):

$$\begin{aligned}
C = B,\ \mathbf{s} = -\varepsilon_i \quad &\rightsquigarrow \quad \operatorname*{wth}_i A = \operatorname*{wth}_{-\varepsilon_i}(S_{\mathbf{c}}/B) \geqslant \operatorname*{wth}_j \max_{-\varepsilon_i} S_{\mathbf{c}} = c_{k-1} - c_1 - (k-2),\\
C = B,\ \mathbf{s} = \varepsilon_i \quad &\rightsquigarrow \quad \operatorname*{wth}_i B = \operatorname*{wth}_{\varepsilon_i} B \geqslant v_{\varepsilon_i} - v'_{\varepsilon_i} = c_{k-1} - c_{k-2},\\
C = A,\ \mathbf{s} = -\varepsilon_i \quad &\rightsquigarrow \quad \operatorname*{wth}_i A = \operatorname*{wth}_{-\varepsilon_i} A \geqslant v_{-\varepsilon_i} - v'_{-\varepsilon_i} = 0 - (-c_1),\\
C = A,\ \mathbf{s} = \varepsilon_i \quad &\rightsquigarrow \quad \operatorname*{wth}_i B = \operatorname*{wth}_{\varepsilon_i}(S_{\mathbf{c}}/A) \geqslant \operatorname*{wth}_j \max_{\varepsilon_i} S_{\mathbf{c}} = c_{k-2} - 0 - (k-2).
\end{aligned}$$

(These inequalities are respectively Rajan's (8.2), (8.3), (8.5) and (8.8)). Summing all together, and using additivity of wth_i under polynomial multiplication, we obtain

$$2 \operatorname*{wth}_i S_{\mathbf{c}} \geqslant 2\big(c_{k-1} - (k-2)\big),$$

which contradicts (5.14c). This finishes the proof. □

5.5.7 Final steps of the proof

In Lemma 5.21, we have ensured that, under the assumptions of Theorem 7 and the additional assumption (5.15), $S_{\mathbf{c}}$ does not have non-trivial semi-symmetric factorizations. It remains to rule out other factorizations. We will first present an analogue of Rajan's Lemma 10.1 (Fact 5.23) as a key argument for that, and later verify that its assumptions can be always satisfied, deducing irreducibility of $S_{\mathbf{c}}$ (Corollary 5.25). This will finish the proof of Theorem 7.

Fact 5.23 (cf. [42, Lemma 10.1])**.** Let $S_{\mathbf{c}} = A \cdot B$ with A irreducible in $K[\mathbf{x}]$, and suppose that there exists a standard vector $\mathbf{s} \in \mathbb{Z}^k$ such that $\max_{\mathbf{s}} S_{\mathbf{c}} \not\sim 1$ but $\max_{\mathbf{s}} B \sim 1$. Then, A and B are semi-symmetric.

Proof. First, observe that

$$\max_{\mathbf{s}} A \sim \max_{\mathbf{s}} S_{\mathbf{c}} \not\sim 1. \tag{5.20}$$

Suppose that A is not semi-symmetric, and let $\sigma \in \Sigma_{\mathbf{x}}$ be such that $A^\sigma \not\asymp A$. Since A is irreducible, it follows that A^σ is coprime to A, and consequently $A^\sigma \mid B$. Let $\mathbf{s} = \alpha \cdot \varepsilon_i$, and let $0 \leqslant j < k$ be such that $x_i = x_j^\sigma$.

If $j = i$, then $(\max_{\mathbf{s}} A)^\sigma = \max_{\mathbf{s}} A^\sigma \mid \max_{\mathbf{s}} B \sim 1$, which is impossible by (5.20).

Hence, $j \neq i$, and we have

$$\operatorname*{wth}_i B \geqslant \operatorname*{wth}_i A^\sigma = \operatorname*{wth}_j A \geqslant \operatorname*{wth}_j \max_{\mathbf{s}} A = \operatorname*{wth}_j \max_{\mathbf{s}} S_{\mathbf{c}}. \tag{5.21}$$

On the other hand, by (5.20) and Fact 5.20b, using its notation, we have

$$\operatorname*{wth}_i A \geqslant v_{\mathbf{s}} - v'_{\mathbf{s}}.$$

Summing with (5.21) and simplifying the right-hand side with (5.10) and (5.14) gives:

$$\operatorname*{wth}_i S_{\mathbf{c}} \geqslant \operatorname*{wth}_j \max_{\mathbf{s}} S_{\mathbf{c}} + v_{\mathbf{s}} - v'_{\mathbf{s}} = \begin{cases} \big(c_{k-2} - (k-2)\big) + c_{k-1} - c_{k-2} & \text{if } \alpha = 1, \\ \big(c_{k-1} - c_1 - (k-2)\big) + 0 - (-c_1) & \text{if } \alpha = -1. \end{cases}$$

In both branches, we obtain that $\operatorname{wth}_i S_{\mathbf{c}} \geqslant c_{k-1} - (k-2)$, contradicting (5.14c). □

Remark 5.24. In the corresponding Lemma 10.1 in [42], it is initially assumed only that $\max_{\mathbf{s}} S_{\mathbf{c}}$ *or* $\min_{\mathbf{s}} S_{\mathbf{c}}$ is not monomial; then, the proof assumes that $\max_{\mathbf{s}} S_{\mathbf{c}} \not\sim 1$. This requires some implicit argument showing no loss of generality, since exchanging $\mathbf{s}$ with $-\mathbf{s}$ could *a priori* influence the initial assumptions on B.

Also, the claim is that A is symmetric (rather than semi-symmetric), which is achieved in the proof by stating that $A^\sigma \neq A$ implies $A^\sigma \mid B$; this also must rely on some additional implicit argument.

Corollary 5.25. Under the assumptions of Theorem 7 and (5.15), $S_{\mathbf{c}}$ is irreducible.

Proof. **1.** First, observe that $\max_0 S_{\mathbf{c}}$ and $\min_0 S_{\mathbf{c}}$ cannot be both monomials. Indeed, in such case (5.14c) would imply that

$$c_{k-1} - c_1 - (k-2) = c_{k-2} - 0 - (k-2) = 0,$$

which implies $\mathbf{c} = \mathbf{e}_k$, contrary to (5.15).

2. Now, choose $\mathbf{s} = \pm\varepsilon_0$ so that $\max_{\mathbf{s}} S_{\mathbf{c}} \not\sim 1$. Suppose that $S_{\mathbf{c}}$ factors as $\prod_{j=1}^{J} A_j$, where A_j are all irreducible and $J > 1$.

Then, the product of all the faces $\max_{\mathbf{s}} A_j$ is equal to $\max_{\mathbf{s}} S_{\mathbf{c}}(\mathbf{x})$, whose non-monomial part is irreducible by (5.16) (it cannot be constant since $\max_{\mathbf{s}} S_{\mathbf{c}} \not\sim 1$). Hence, there must be some $1 \leqslant j_0 \leqslant J$ such that

$$\max_{\mathbf{s}} A_{j_0} \not\sim 1, \qquad \max_{\mathbf{s}} A_j \sim 1 \quad \text{for } j \neq j_0.$$

Let $A = A_{j_0}$ and $B = S_{\mathbf{c}}/A$; then A is irreducible and $\max_{\mathbf{s}} B \sim 1$. By Fact 5.23, A and B must be semi-symmetric. Then, it follows from Corollary 5.22 that A or B must be constant. This proves that $S_{\mathbf{c}}$ is irreducible. □

5.6 Proof of Theorem 7'

We will now provide the second argument for the inductive step, allowing to strengthen Theorem 7 to Theorem 7'. In comparison to the Rajan's method presented in Section 5.5, the main difference is that we fully avoid using generalized Eisenstein criterion (see Section 5.5.3), and instead focus only on the N-polytope of the given polynomial P and irreducibility of its standard faces. By doing so, we also leave out the necessity of considering the Vandermonde polynomials $V_{\mathbf{c}}(\mathbf{x})$, which allows us to handle polynomials which are not their factors.

As a result, we obtain a proof featuring more "stability" in the sense that it applies also after changing the "inner" coefficients of the given polynomial (where "inner" means precisely "not in its standard faces"). It is also, at least in our opinion, a bit simpler.

However, this comes at the price of restricting the possible range of $\mathbf{c}$. Namely, for performing a single inductive step with the currently described method, it is essential that the standard faces of $S_{\mathbf{c}}$ shall be either constant or irreducible, and moreover that $\prod_{i=1}^{k-2} d_i > 1$ (both these conditions will be used in Section 5.6.4). This contrasts with Rajan's method, in which our exposition (Section 5.5) uses only the first of those assumptions, while the original version of [42] proceeds even without that (see the discussion in Section 5.4.1). Unfortunately, we have currently no idea how the approach described below could be significantly generalized.

Certain resemblance of the spirit between both reasonings can be easily seen; for instance, the "wideness of factors" considered in Section 5.6.3 might be perceived as an analogue of that of Section 5.5.6. Nevertheless, at the level of details, a different choice of basic tools results in a completely different reasoning. Hence, apart from what has been already done in Sections 5.3 and 5.4, these proofs seem not to admit unification at a deeper level.

5.6.1 Initial setup

Analogously as we did in Section 5.5.1 for the purposes of Section 5.5, we now assume throughout Section 5.6 that $k \geqslant 4$, and that Theorem 7' has been proved for all smaller k. We let

$$\mathbf{c}, \quad p, \quad K, \quad P$$

satisfy the assumptions of Theorem 7', and aim at proving its claim for these data.

By the assumption (ii) of Theorem 7' applied for $a = 1$ and $b = k - 2$, we are guaranteed that $\prod_{i=1}^{k-3} d_i > 1$ or that P agrees with $S_{\mathbf{c}}$ upon all iterated standard faces of signature $(0, 0)$. The

latter condition means that $P = S_{\mathbf{c}}$; in such case, the claim of Theorem 7' follows immediately from Theorem 7. In the sequel, we assume the other possibility; then, we must have $d_i > 1$ for some $1 \leqslant i \leqslant k-3$, and consequently,

$$c_{k-2} - c_1 > k - 3. \tag{5.22}$$

Choose any standard vector $\mathbf{s} = \alpha \cdot \varepsilon_i$, and denote

$$\beta_+ = \tfrac{1+\alpha}{2}, \qquad \beta_- = \tfrac{1-\alpha}{2},$$

so that $\max_{\mathbf{s}} P$ is an iterated standard face of P of signature (β_+, β_-). Since P satisfies the assumptions (i-ii) of Theorem 7', it follows that $\max_{\mathbf{s}} P$, when treated as polynomial in $K[\hat{\mathbf{x}}_i]$, agrees with $\max_{\mathbf{s}} S_{\mathbf{c}}$ upon:

- (i') N-polytope;
  (this follows from (i) by (5.8))
- (ii') all iterated standard faces of signature $(k-2-b-\beta_+,\ a-1-\beta_-)$, for every $1 \leqslant a < b \leqslant k-2$ such that $\prod_{i=a}^{b-1} d_i = 1$.
  (this follows from (ii) by the definition of iterated standard faces of a given signature)

In particular, (i') ensures that the monomial parts of these polynomials must coincide, which easily implies that $\widetilde{\max_{\mathbf{s}} P}$ and $\widetilde{\max_{\mathbf{s}} S_{\mathbf{c}}}$ also agree upon all the data indicated by (i'-ii').

By (5.14) and the assumption that $c_0 = 0$, we have $\widetilde{\max_{\mathbf{s}} S_{\mathbf{c}}} = \gamma \cdot S_{\mathbf{b}}$, where

$$\gamma \in K \setminus \{0\}, \qquad \mathbf{b} = \begin{cases} \hat{\mathbf{c}}_{k-1} & \text{if } \alpha = 1, \\ \hat{\mathbf{c}}_0 - c_1 & \text{if } \alpha = -1. \end{cases}$$

We claim that Theorem 7' can be applied to $Q = \gamma^{-1} \cdot \widetilde{\max_{\mathbf{s}} P}$. Indeed, it is easy to see that $\mathbf{b}$ and p satisfy the conditions (5.1) and (5.2). Also, Q and $S_{\mathbf{b}}$ must agree upon the data (i'-ii') because $\gamma \cdot Q = \widetilde{\max_{\mathbf{s}} P}$ and $\gamma \cdot S_{\mathbf{b}} = \widetilde{\max_{\mathbf{s}} S_{\mathbf{c}}}$ do. This ensures that Q satisfies the assumption (i) of Theorem 7'. To verify (ii), let $1 \leqslant a \leqslant b \leqslant k-3$ satisfy

$$\prod_{j=a}^{b-1} (b_{j+1} - b_j) = 1;$$

since $b_{j+1} - b_j = c_{j+1+\beta_-} - c_{j+\beta_-}$ for every $0 \leqslant j \leqslant k-3$, it follows that

$$\prod_{j=a+\beta_-}^{b+\beta_--1} d_j = 1.$$

Hence, by (ii'), we know that Q agrees with $S_{\mathbf{b}}$ upon all iterated standard faces of signature

$$\big(k-2-(b+\beta_-)-\beta_+,\ (a+\beta_-)-1-\beta_-\big) = \big((k-1)-2-b,\ a-1\big).$$

This shows that Q satisfies (ii), and hence Theorem 7' is applicable to Q. By the inductive assumption, we can indeed apply it to Q, obtaining that Q is irreducible in $K[\hat{\mathbf{x}}_i]$ (note that $\mathbf{b} \neq \mathbf{e}_{k-1}$ by (5.22)). Since $Q \simeq \widetilde{\max_{\mathbf{s}} P}$, we finally deduce that

$$\widetilde{\max_{\mathbf{s}} P(\mathbf{x})} \quad \text{is irreducible in } K[\hat{\mathbf{x}}_i]. \tag{5.23}$$

This finishes the initial setup. Below, for reader's convenience, we gather some basic observations which might be puzzling if stated without explanation in more complicated proofs.

Fact 5.26. Let $Q \in K[\mathbf{x}]$ be an arbitrary polynomial, and $\mathbf{s}, \mathbf{t} \in \mathbb{Z}^k$. Then:

(a) $\deg_{\mathbf{s}} \max_{\mathbf{t}} Q \leqslant \deg_{\mathbf{s}} Q$;

(b) $\mathrm{wth}_{\mathbf{s}} \max_{\mathbf{t}} Q \leqslant \mathrm{wth}_{\mathbf{s}} Q$;

(c) $\deg_{\mathbf{s}} \max_{\mathbf{t}} \max_{\mathbf{s}} Q = \deg_{\mathbf{s}} Q$.

Proof. A monomial appearing in Q cannot have greater $\mathbf{s}$-degree than the whole Q; this gives **(a)**. By applying **(a)** for $\mathbf{s}$ and $-\mathbf{s}$, and summing results, we obtain **(b)**. Finally, **(c)** follows from the fact that all monomials in $\max_{\mathbf{s}} Q$ (and thus also in its maximal $\mathbf{t}$-face) have the same $\mathbf{s}$-degree. □

5.6.2 Face adjacency

Definition 5.27. Two standard vectors $\mathbf{s} = \alpha \cdot e_i$, $\mathbf{t} = \beta \cdot e_j$ will be called *adjacent* if $\alpha \neq \beta$ and $i \neq j$.

While the above definition might look surprising, it is motivated by the fact (which we prove below) that, for every P considered in Theorem 7', every pair of standard vectors satisfying the above condition determines a pair of adjacent faces of P, in the very common sense that these faces share a common sub-face. (Moreover, the conditions from Definition 5.27 are generally necessary, in the sense that no other pair of vectors has this property for all P under our consideration; however, we will not need this).

Fact 5.28. Let $\mathbf{s}$, $\mathbf{t}$ be adjacent standard vectors (and let P be as in Section 5.6.1). Then:

(a) the face operators $\max_{\mathbf{s}}$, $\max_{\mathbf{t}}$ commute on P:

$$\max_{\mathbf{s}} \max_{\mathbf{t}} P = \max_{\mathbf{t}} \max_{\mathbf{s}} P; \tag{5.24}$$

(b) the face $\max_{\mathbf{s}} P$ achieves the $\mathbf{t}$-degree of the whole P:

$$\deg_{\mathbf{t}} \max_{\mathbf{s}} P = \deg_{\mathbf{t}} P.$$

Proof. **(a)** Without losing generality, let $\mathbf{s} = -\varepsilon_i$ and $\mathbf{t} = \varepsilon_j$, with $i \neq j$. Then, using (5.14), it is easy to check that

$$\min_i \max_j S_{\mathbf{c}}(\mathbf{x}) \simeq x_i^{c_0} \cdot x_j^{c_{k-1}-(k-1)} \cdot S_{\hat{\mathbf{c}}_{0,k-1}}(\hat{\mathbf{x}}_{i,j}) \simeq \max_j \min_i S_{\mathbf{c}}(\mathbf{x}),$$

and consequently

$$New(\min_i \max_j S_{\mathbf{c}}) = New(\max_j \min_i S_{\mathbf{c}}).$$

By the equality $New(P) = New(S_{\mathbf{c}})$, and the fact that the N-polytope of a polynomial determines N-polytopes of its faces (see (5.8)), we deduce that

$$New(\min_i \max_j P) = New(\max_j \min_i P), \tag{5.25}$$

which rather clearly leads to (5.24). (For a strict argument, note that (5.25) implies in particular that the polynomials appearing on both sides have the same i-degree and j-degree; denote

them, respectively, by D_i and D_j. Then, by unfolding definitions, $\max_{\mathbf{s}} \max_{\mathbf{t}} P = \min_i \max_j P$ turns out to be the sum of all monomials M in P such that $\deg_i M = D_i$ and $\deg_j M = D_j$, and exactly the same description is obtained when evaluating $\max_{\mathbf{t}} \max_{\mathbf{s}} P$).

(b) This follows easily from **(a)**, and Fact 5.26c:

$$\deg_{\mathbf{t}} \max_{\mathbf{s}} P = \deg_{\mathbf{t}} \max_{\mathbf{t}} \max_{\mathbf{s}} P = \deg_{\mathbf{t}} \max_{\mathbf{s}} \max_{\mathbf{t}} P = \deg_{\mathbf{t}} P. \qquad \square$$

5.6.3 Wideness of factors

We will now show that a factor of P which fully consumes (up to monomial equivalence) any its two adjacent faces must achieve the full width of P in all *other* standard directions. (This intuitive statement is made precise in Lemma 5.29).

As it will be visible in the proof, this multi-directional wideness follows primarily from an analogous wideness of the "union of two adjacent faces" of P, by which we mean the sum of all monomials appearing in either of the faces (which reduces to taking union at the level of shapes).

Lemma 5.29. Let $0 \leqslant i, j < k$ with $i \neq j$, and let $C \in K[\mathbf{x}]$ be a factor of P such that

$$\min_i C \sim \min_i P, \qquad \max_j C \sim \max_j P.$$

(Here, P is as in section 5.6.1). Then, for every $0 \leqslant l < k$ distinct from i, j, we have

$$\operatorname{wth}_l C = \operatorname{wth}_l P. \tag{5.26}$$

Proof. **1.** Let $\mathbf{u}, \mathbf{u}' \in \mathbb{Z}^k$ be such that

$$\min_i C \simeq \mathbf{x}^{\mathbf{u}} \cdot \min_i P, \qquad \max_j C \simeq \mathbf{x}^{\mathbf{u}'} \cdot \max_j P. \tag{5.27}$$

Let $\mathbf{r} = (r_0, \ldots, r_{k-1})$ denote the difference $\mathbf{u} - \mathbf{u}'$. In steps 2–5, we will show that all its entries r_l are non-positive, while their sum is zero. This will yield $\mathbf{r} = 0$, which will be shown in step 2 to imply (5.26).

2. Let $0 \leqslant l < k$ with $l \neq i, j$. Then, ε_l and $-\varepsilon_l$ are, respectively, adjacent to $-\varepsilon_i$ and ε_j. By applying consecutively Fact 5.26a, (5.27) and Fact 5.28b, we obtain:

$$\begin{aligned} \deg_l C &\geqslant \deg_l \min_i C = \deg_l \min_i P + \varepsilon_l \circ \mathbf{u} \;\; = \deg_l P + \varepsilon_l \circ \mathbf{u}, \\ \deg_{-l} C &\geqslant \deg_{-l} \max_j C = \deg_{-l} \max_j P - \varepsilon_l \circ \mathbf{u}' = \deg_{-l} P - \varepsilon_l \circ \mathbf{u}'. \end{aligned}$$

Summing these equations yields

$$\operatorname{wth}_l C \geqslant \operatorname{wth}_l P + \varepsilon_l \circ \mathbf{r} = \operatorname{wth}_l P + r_l.$$

On the other hand, we certainly have $\operatorname{wth}_l C \leqslant \operatorname{wth}_l P$ because $C \mid P$. Hence, showing that $\mathbf{r} = 0$ suffices to prove (5.26). At the same time, we obtain that $r_l \leqslant 0$ for all $l \neq i, j$.

3. Let $\mathbf{h}$ be any vector in $\mathbb{Z}^k$. By (5.27) and Fact 5.28a, we have

$$\deg_{\mathbf{h}} \max_j \min_i C - \mathbf{h} \circ \mathbf{u} = \deg_{\mathbf{h}} \max_j \min_i P = \deg_{\mathbf{h}} \min_i \max_j P = \deg_{\mathbf{h}} \min_i \max_j C - \mathbf{h} \circ \mathbf{u}'.$$

As a consequence, which will be used below twice, we obtain:

$$\deg_{\mathbf{h}} \max_j \min_i C = \deg_{\mathbf{h}} \min_i \max_j C + \mathbf{h} \circ \mathbf{r}. \tag{5.28}$$

4. Let now $\mathbf{h} = (1, \dots, 1) \in \mathbb{Z}^k$. Since P has the same N-polytope as $S_{\mathbf{c}}$, which is homogeneous, we have

$$\operatorname{wth}_{\mathbf{h}} C \leqslant \operatorname{wth}_{\mathbf{h}} P = \operatorname{wth}_{\mathbf{h}} S_{\mathbf{c}} = 0.$$

Hence, the $\mathbf{h}$-degree of every monomial in C is the same. By (5.28), this implies

$$0 = \mathbf{h} \circ \mathbf{r} = \sum_{l=0}^{k-1} r_l.$$

5. Finally, it remains to bound from above r_i and r_j. For this, note first that for every $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^k$ we have

$$\deg_{\mathbf{a}} \max_{\mathbf{a}} \max_{\mathbf{b}} C = \deg_{\mathbf{a}} \max_{\mathbf{b}} C \overset{(*)}{\leqslant} \deg_{\mathbf{a}} C \overset{(*)}{=} \deg_{\mathbf{a}} \max_{\mathbf{b}} \max_{\mathbf{a}} C, \tag{5.29}$$

where the starred relations follow from Fact 5.26, parts (a) and (c). Now, by letting $\{\mathbf{a}, \mathbf{b}\} = \{-\varepsilon_i, \varepsilon_j\}$ (in both ways), substituting into (5.29), and then applying (5.28) with $\mathbf{h} = \mathbf{a}$, we obtain

$$\begin{aligned}
\deg_{-i} \min_i \max_j C &\leqslant \deg_{-i} \max_j \min_i C = \deg_{-i} \min_i \max_j C + (-\varepsilon_i) \circ \mathbf{r}, \\
\deg_{j} \max_j \min_i C &\leqslant \deg_{j} \min_i \max_j C = \deg_{j} \max_j \min_i C - \varepsilon_j \circ \mathbf{r}.
\end{aligned}$$

These inequalities imply respectively that $\varepsilon_i \circ \mathbf{r} = r_i$ and $\varepsilon_j \circ \mathbf{r} = r_j$ are non-positive. Together with the results of steps 2 and 4, this gives all relations claimed in step 1, which finishes the proof. □

5.6.4 The main argument

The following completes the inductive step for the proof of Theorem 7'.

Lemma 5.30. Let P be as in Section 5.6.1; then, P is irreducible.

Proof. Let $P = A \cdot B$ for some $A, B \in K[\mathbf{x}]$; our goal is to prove that A or B is constant.

1. For every standard vector $\mathbf{s}$, we have $\widetilde{\max_{\mathbf{s}} A} \cdot \widetilde{\max_{\mathbf{s}} B} = \widetilde{\max_{\mathbf{s}} P}$, which is irreducible by (5.23). Therefore, one of $\max_{\mathbf{s}} A$, $\max_{\mathbf{s}} B$ must be a monomial, and the other one must be monomially equivalent to $\max_{\mathbf{s}} P$.

Let $\mathcal{A}$ (resp. $\mathcal{B}$) denote the set of those standard vectors $\mathbf{s}$ for which the maximal $\mathbf{s}$-face of P is monomially equivalent to that of A (resp. B). By what was just said, $\mathcal{A}$ and $\mathcal{B}$ cover all the standard vectors. (They are also disjoint, but we will not need this).

2. First, suppose that there exist $i, j \in \{0, \dots, k-1\}$, not necessarily distinct, such that one of the sets $\mathcal{A}$, $\mathcal{B}$ contains ε_i and the other contains $-\varepsilon_j$; without losing generality, let $\varepsilon_i \in \mathcal{A}$ and $-\varepsilon_j \in \mathcal{B}$. Let $0 \leqslant l < k$ be distinct from i, j (it exists since $k \geqslant 4$). Then, using Fact 5.26b, as well as the equality $New(P) = New(S_{\mathbf{c}})$ and its consequences following for the standard faces by (5.8), we have:

$$\begin{aligned} \operatorname*{wth}_l A &\geqslant \operatorname*{wth}_l \max_i A = \operatorname*{wth}_l \max_i P = \operatorname*{wth}_l \max_i S_{\mathbf{c}}, \\ \operatorname*{wth}_l B &\geqslant \operatorname*{wth}_l \max_{-j} B = \operatorname*{wth}_l \max_{-j} P = \operatorname*{wth}_l \max_{-j} S_{\mathbf{c}}. \end{aligned}$$

Summing these inequalities, and using (5.14), we obtain

$$\begin{aligned} \operatorname*{wth}_l P \geqslant \operatorname*{wth}_l \max_i S_{\mathbf{c}} + \operatorname*{wth}_l \max_{-j} S_{\mathbf{c}} = \operatorname*{wth}_{x_l} S_{\hat{\mathbf{c}}_{k-1}}(\hat{\mathbf{x}}_i) + \operatorname*{wth}_{x_l} S_{\hat{\mathbf{c}}_0}(\hat{\mathbf{x}}_j) = \\ \overset{(*)}{=} \big(c_{k-2} - c_0 - (k-2)\big) + \big(c_{k-1} - c_1 - (k-2)\big). \end{aligned} \tag{5.30}$$

(The starred equality, following from (5.14c), is the only place where we use the assumption that $l \neq i, j$; otherwise the corresponding width(s) would be zero).

On the other hand, by the equality of N-polytopes, we have

$$\operatorname*{wth}_l P = \operatorname*{wth}_l S_{\mathbf{c}} = c_{k-1} - c_0 - (k-1).$$

By comparing this with (5.30), we obtain $k - 3 \geqslant c_{k-2} - c_1$, which contradicts (5.22).

3. Now, suppose that $\mathcal{A}$ and $\mathcal{B}$ are such that step 2 does not apply. Without losing generality, assume that $\varepsilon_0 \in \mathcal{A}$. Then, it follows that $-\varepsilon_i$ must also lie in $\mathcal{A}$ for every $0 \leqslant i < k$, and this in turn implies that $\varepsilon_j \in \mathcal{A}$ for every $0 \leqslant j \leqslant k$. This means that $\mathcal{A}$ must contain all standard vectors.

In such case, the assumptions of Lemma 5.29 (with $C = A$) are satisfied for *every* pair $0 \leqslant i, j < k$ with $i \neq j$. Since $k \geqslant 4$, the Lemma implies that $\operatorname{wth}_l A = \operatorname{wth}_l P$ for every $0 \leqslant l < k$, and this gives $\operatorname{wth}_l B = 0$ for all l, so B is a monomial. If B is constant, then we are done. Otherwise, there must be some $0 \leqslant i < k$ for which

$$0 < \operatorname*{deg}_i \min_i B \leqslant \operatorname*{deg}_i \min_i P = \operatorname*{deg}_i \min_i S_{\mathbf{c}},$$

which contradicts (5.14b) since we have assumed $c_0 = 0$. This finishes the proof. □

5.7 Proof of Theorem 8

We will now prove Theorem 8, mainly by simply deriving it from Theorem 7 in combination with Lemma 4.28 and Fact 5.14. However, these facts seem to be too weak to handle certain special cases, in which we will additionally use Theorem H and Lemma 4.27 in their full strength.

Let $\mathbf{c}$, k, i, p, q satisfy the assumptions of Theorem 8. Throughout the proof, we will apply Theorem 7 to several sequences of the form $\mathbf{b}+a$ for $\mathbf{b} \sqsubseteq \mathbf{c}$ and $a \in \mathbb{Z}$. Let us observe in advance that the assumption $p > c_{k-1} - c_0$ of Theorem 8 implies that p satisfies the condition (5.2) for every sequence of this form. Hence, we will only check whether $\mathbf{b} + a$ satisfies (5.1).

We observe that the sequence $\hat{\mathbf{c}}_i - \hat{c}_{i,0}$ satisfies the conditions (5.1); hence, by Theorem 7, $S_{\hat{\mathbf{c}}_i - \hat{c}_{i,0}}$ is irreducible over $\overline{\mathbb{F}_q}$.

By Lemma 4.28, to finish the proof it suffices to choose $0 \leqslant j < k$ distinct from i so that $S_{\hat{\mathbf{c}}_i - \hat{c}_{i,0}}$ is coprime to $S_{\hat{\mathbf{c}}_j - \hat{c}_{j,0}}$ over $\mathbb{F}_q$. Since the former polynomial is irreducible, it suffices to ensure that

$$S_{\hat{\mathbf{c}}_i - \hat{c}_{i,0}} \nmid S_{\hat{\mathbf{c}}_j - \hat{c}_{j,0}}. \tag{5.31a}$$

On the other hand, note that, by Theorem 7 and Fact 5.14, it suffices to ensure that

$$\hat{\mathbf{c}}_j - \hat{c}_{j,0} \text{ is step-coprime and distinct from } \hat{\mathbf{c}}_i - \hat{c}_{i,0}. \tag{5.31b}$$

To finish the proof, we consider a number of cases.

- If $0 < i < k-1$, we choose $j = k-1$. Then, we have

  $$\hat{c}_{i,k-2} = c_{k-1} > c_{k-2} = \hat{c}_{j,k-2}, \qquad \hat{c}_{i,0} = c_0 = \hat{c}_{j,0},$$

  and consequently, by (5.14c),

  $$\operatorname*{wth}_0 S_{\hat{\mathbf{c}}_i - \hat{c}_{i,0}} \;=\; \hat{c}_{i,k-2} - \hat{c}_{i,0} - (k-2) \;>\; \hat{c}_{j,k-2} - \hat{c}_{j,0} - (k-2) \;=\; \operatorname*{wth}_0 S_{\hat{\mathbf{c}}_j - \hat{c}_{j,0}}.$$

  Since 0-width is additive under polynomial multiplication, (5.31a) follows.

It remains to consider the possibilities $i = 0$ and $i = k-1$. Since it turns out that they are symmetric, we will discuss them jointly; to enhance notation, we introduce a new symbol

$$\delta = \begin{cases} 1 & \text{if } i = 0, \\ -1 & \text{if } i = k-1. \end{cases}$$

From now on, we assume that $i \in \{0, k-1\}$. Before analyzing subsequent cases, let us observe that, under this assumption,

$$\hat{\mathbf{c}}_i - \hat{c}_{i,0} \neq \hat{\mathbf{c}}_j - \hat{c}_{j,0} \qquad \text{for } j = i + \delta. \tag{5.32}$$

Indeed, by extracting and comparing the maximal entries on both sides, we obtain $c_{k-1} - c_1 \neq c_{k-1} - c_0$ for $i = 0$, and $c_{k-2} - c_0 \neq c_{k-1} - c_0$ for $i = k-1$.

With the above preparation, we consider the remaining three cases:

- If $\hat{\mathbf{c}}_{i,i+\delta} - \hat{c}_{i,i+\delta,0} = \mathbf{e}_{k-2}$, we choose $j = i + \delta$. Then, if $i = 0$ (resp. $i = k-1$), the sequence $\hat{\mathbf{c}}_j - \hat{c}_{j,0}$ is step-coprime because removing its first (resp. last) element leads to a sequence of the form $\mathbf{e}_{k-2} + a$ for some $a \in \mathbb{Z}$, and this means that, in an application of the condition (4.1) to $\hat{\mathbf{c}}_j - \hat{c}_{j,0}$, the second (resp. first) argument of the "gcd" operator always takes value 1. Together with (5.32), this gives (5.31b).

- If $\hat{\mathbf{c}}_{i,\,i+\delta} - \hat{c}_{i,\,i+\delta,\,0} \neq \mathbf{e}_{k-2}$ and $k \geqslant 5$, we choose $j = k-1-i$. Suppose that $S_{\hat{\mathbf{c}}_i - \hat{c}_{i,0}}$ divides $S_{\hat{\mathbf{c}}_j - \hat{c}_{j,\,0}}$. Then, corresponding divisibility must take place on the level of maximal $(-\delta \cdot \varepsilon_0)$-faces; by (5.14), we obtain

$$S_{\mathbf{a}} \;\simeq\; \widetilde{\max_{-\delta\cdot\varepsilon_0} S_{\hat{\mathbf{c}}_i - \hat{c}_{i,\,0}}} \;\sim\; \max_{-\delta\cdot\varepsilon_0} S_{\hat{\mathbf{c}}_i - \hat{c}_{i,\,0}} \;\Big|\; \max_{-\delta\cdot\varepsilon_0} S_{\hat{\mathbf{c}}_j - \hat{c}_{j,\,0}} \;\sim\; \widetilde{\max_{-\delta\cdot\varepsilon_0} S_{\hat{\mathbf{c}}_j - \hat{c}_{j,\,0}}} \;\simeq\; S_{\mathbf{b}}, \tag{5.33}$$

where

$$\mathbf{a} = \hat{\mathbf{c}}_{i,\,i+\delta} - \hat{c}_{i,\,i+\delta,\,0}, \qquad \mathbf{b} = \hat{\mathbf{c}}_{i,\,j} - \hat{c}_{i,\,j,\,0} = \hat{\mathbf{c}}_{0,\,k-1} - c_1.$$

The sequences $\mathbf{a}$, $\mathbf{b}$ both have length at least 3, start with zero, and are step-coprime because each of them is obtained from a sequence of the form $\hat{\mathbf{c}}_i + a$ for some $a \in \mathbb{Z}$ (which is step-coprime by assumption) by removing either the first or the last element. Moreover, by assumption, $\mathbf{a}$ is distinct from $\mathbf{e}_{k-2}$. Hence, Theorem 7 implies that $S_{\mathbf{a}}$ is irreducible over $\overline{\mathbb{F}_q}$, and $S_{\mathbf{b}}$ is either constant or irreducible over $\overline{\mathbb{F}_q}$.

We claim that $\mathbf{a} \neq \mathbf{b}$; indeed, otherwise comparing the consecutive entries of $\mathbf{a}$ and $\mathbf{b}$ would yield

$$c_{l+1+\delta} - c_{1+\delta} = c_{l+1} - c_1 \qquad \text{for } 0 \leqslant l \leqslant k-3;$$

which after regrouping gives

$$c_{l+1+\delta} - c_{l+1} = c_{1+\delta} - c_1 \qquad \text{for } 0 \leqslant l \leqslant k-3.$$

This is trivial for $l = 0$; however, combining the subsequent equalities for $1 \leqslant l \leqslant k-3$ leads to the conclusion that all the differences between any two consecutive elements in $\hat{\mathbf{c}}_i$ are equal. This contradicts the assumption that $\hat{\mathbf{c}}_i$ is not arithmetic. Hence, $\mathbf{a} \neq \mathbf{b}$.

Now, Fact 5.14 implies that $S_{\mathbf{a}}$, $S_{\mathbf{b}}$ are coprime over $\mathbb{F}_q$. In view of (5.33), this means that $S_{\mathbf{a}}$ must be a monomial; however, the first equality of (5.33) implies that $S_{\mathbf{a}}$ is not divisible by non-trivial monomials; hence, it must be constant. This contradicts its irreducibility which we have established before. The obtained contradiction shows that (5.31a) must hold.

- If $k = 4$, we look for a suitable j, as follows. Suppose that, for every $j \in \{1, 2\}$, (5.31a) is violated. Then, the polynomial $S_{\hat{\mathbf{c}}_i} - \hat{c}_{i,0}$ is a divisor of

$$S_{\hat{\mathbf{c}}_j - \hat{c}_{j,\,0}} = \frac{S_{\hat{\mathbf{c}}_j - \hat{c}_{j,\,0}}}{S_{D_j \cdot \mathbf{e}_3}} \cdot S_{D_j \cdot \mathbf{e}_3}, \qquad \text{where } D_j = \gcd(\hat{\mathbf{c}}_j - \hat{c}_{j,\,0}).$$

However, the second factor in the above decomposition is coprime to $S_{\hat{\mathbf{c}}_i - \hat{c}_{i,\,0}}$, which follows from Lemma 4.27 because $p > D_j$ and $\gcd(\hat{\mathbf{c}}_i - \hat{c}_{i,\,0}) = 1$ (since $\hat{\mathbf{c}}_i$ is step-coprime). Hence, $S_{\hat{\mathbf{c}}_i - \hat{c}_{i,\,0}}$ must be a divisor of the first factor, which is irreducible by Theorem H; therefore, these two polynomials must be associated. By comparing widths, using (5.14c), we obtain

$$\hat{c}_{i,\,2} - \hat{c}_{i,\,0} - 2 \;=\; \operatorname*{wth}_0 S_{\hat{\mathbf{c}}_i - \hat{c}_{i,\,0}} \;=\; \operatorname*{wth}_0 \frac{S_{\hat{\mathbf{c}}_j - \hat{c}_{j,\,0}}}{S_{D_j \cdot \mathbf{e}_3}} \;=\; \hat{c}_{j,\,2} - \hat{c}_{j,\,0} - 2D_j \qquad \text{for } j = 1, 2.$$

Since the left-most expression does not depend on j, the right-most value must also be independent of j; this leads to

$$c_3 - c_0 - 2D_1 = c_3 - c_0 - 2D_2$$

and consequently

$$D_1 = D_2.$$

On the other hand, we have $\{1, 2\} = \{i + \delta, i + 2\delta\}$, and

$$D_{i+\delta} \mid c_{i+2\delta} - c_{i+3\delta}, \qquad D_{i+2\delta} \mid c_{i+\delta} - c_{i+3\delta},$$

which altogether leads to the conclusion that

$$D_1 = D_2 \;\Big|\; \gcd(c_{i+2\delta} - c_{i+3\delta},\, c_{i+\delta} - c_{i+3\delta}) = \gcd(c_{i+2\delta} - c_{i+3\delta},\, c_{i+\delta} - c_{i+2\delta}) = 1,$$

where the last equality follows from the assumption that $\hat{\mathbf{c}}_i$ is step-coprime. Hence, $D_1 = D_2 = 1$.

Now, taking $j = i + \delta$, we have $D_j = 1$ which means that $\hat{\mathbf{c}}_j$ is step-coprime; together with (5.32), this gives (5.31b).

We have now finished analyzing all possible cases. In each of them, we reached either a contradiction or the conclusion that there exists some j satisfying (5.31a) or (5.31b). This finishes the proof. □

Chapter 6

Remarks on access structures

In the last chapter of this thesis, we turn our attention to Lai-Ding's access structures. Hence, compared to Chapter 4, we are no longer interested in the asymptotic number of privileged tracks; instead, we focus on their possible combinations and criteria for their existence. This naturally leads to the following two questions, each representing one direction in the relation between Lai-Ding's schemes and their induced access structures:

(i) Given $\mathbf{c}$, i and q, can we describe the access structure $\Gamma_q^{LD}(\mathbf{c}, i)$?

(ii) Given an access structure Γ, can we decide whether it is embeddable into some $\Gamma_q^{LD}(\mathbf{c}, i)$? If it is, can we understand the possible range of $\mathbf{c}$, i and q?

Prior knowledge in this area in the case of Shamir's type schemes has been summarized in Theorem G (in Section 2.2.4). We are not aware of any further prior results in this topic regarding either Shamir's type or general Lai-Ding's schemes.

Just as explained in Section 4.1, both these directions reduce essentially to the difficult task of studying zeroes of Schur polynomials and their systems. Consequently, our results in this area will be far from giving a complete picture of either (i) or (ii); nevertheless, we will present some partial results, mainly concerning (ii).

In Section 6.1, we prove that the class of Lai-Dings's access structures is very close to the whole class of Brickell's structures (see Theorem 9). Namely, all Brickell's schemes except for the degenerate one (see Definition 2.5) admit realization by a Lai-Ding's scheme with repeated identities (see Definition 2.12), and such repetitions can be avoided under a rather mild assumption that the given structure has no equipotent pairs (see Section 2.3.2). (Nevertheless, they cannot be always avoided, as we show in Remark 6.1).

At the first glance, this might look as if we could simulate Brickell's schemes (defined in terms of a relatively large matrix) by simpler ones (depending just on a sequence of exponents $\mathbf{c}$ and an integer i). However, the proof of Theorem 9 in fact "encapsulates" a Brickell's scheme Σ over $\mathbb{F}_q$ into a Lai-Ding's scheme Σ' over $\mathbb{F}_{q'}$, where q' is so large that a single element of $\mathbb{F}_{q'}$ may store a whole column from the original matrix. Hence, Σ' is in fact *more* complex then Σ, both in the amount of computation needed to recover the secret and in the size of shares. On the other hand, Σ' is still ideal (see Definition 2.38), and its complexity might turn out to be

totally acceptable if q is chosen very small. Nevertheless, even when Σ' is not worse than Σ (from a practical viewpoint), it is rather unclear if, in any way, Σ' is better; this depends on the question of general advantages of Lai-Ding's schemes, discussed in Section 2.4.3. This shows that, unfortunately, Theorem 9 does not bring evident benefits for practical applications.

On the other hand, demonstrating the vastness of diversity of Lai-Ding's schemes has some (meta-)theoretical value. First, it strongly suggests that there is no efficient algorithm to decide whether a given access structure is Lai-Ding's, since there is no such method for the Brickell's class (as we explain in detail in Remark 6.2). More generally, Theorem 9 suggests that the general answer to the above questions (i) and (ii), if ever found, should be quite complex. (In particular, it should be much more sophisticated than for Shamir's type schemes, which are, by Theorem G, too weak for realizing many examples of Brickell's access structures).

In Section 6.2, we will once more focus on the two very special cases, distinguished in Chapter 4, for which we can tell something more about privileged tracks: $\mathbf{c}$ or $\hat{\mathbf{c}}_i$ arithmetic. The reversion of order between them (relatively to Chapter 4) reflects the fact that the latter case will now be the more laborious one.

The case of $\mathbf{c}$ arithmetic, discussed in Section 6.2.1, reduces essentially (i.e. up to a homomorphism in the sense of Section 2.3.2) to restricting Shamir's type schemes to λ-th powers in the multiplicative group $\mathbb{F}_q^\times$. This does not tell how much of the diversity of Shamir's type access structures we can preserve; however, we will show that the whole knowledge on such structures gathered in Theorem G is preserved completely up to slight adjustments (this will be Theorem 10).

The other special case, $\hat{\mathbf{c}}_i$ arithmetic, will be treated in Section 6.2.2. Here, as already noticed in Remark 4.10, Theorem G no longer holds due to existence of privileged *pairs* of participants; since such pairs essentially determine all privileged tracks (see Lemma 4.6), we will mainly investigate their possible layouts in the access structure. Representing such layouts as graphs (according to the notion of graphic access structure; see Section 2.3.2), we will indicate the class of *distinguished* graphs (Definition 6.15), containing all such possible layouts (see Lemma 6.17). As for the other direction, we will construct (with some more technical effort) Lai-Ding's access structures corresponding to arbitrary distinguished graphs; this will be Theorem 11.

The results just described are still only a partial realization of our main goal: they do *not* classify all structures of the form $\Gamma_q^{LD}(\mathbf{c}, i)$, since such structure is not fully determined by the graph of its privileged pairs. However, they provide explicit realization by a Lai-Ding's scheme for many access structures not realizable by any Shamir's type scheme.

6.1 Lai-Ding's schemes for Brickell's access structures

By definition (see Section 2.1.3), Lai-Ding's secret sharing schemes form a subclass of Brickell's schemes. Analogously, Lai-Ding's access structures form a subclass of Brickell's structures, which makes it natural to ask how general this subclass is. As we will show in this section, it turns out that both classes almost coincide.

Theorem 9. *Let Γ be a Brickell's access structure. Then:*

(a) *Γ admits realization by a Lai-Ding's secret sharing scheme with repeated identities (see*

Definition 2.12) if and only if it is non-degenerate (see Definition 2.5);

(b) *If Γ is non-degenerate and has no equipotent pairs of non-nilpotent participants (see Section 2.3.2), then it admits realization by a Lai-Ding's scheme.*

The proof of Theorem 9 will be given below in Section 6.1.2. Below, we state some comments.

Remark 6.1. The assumptions in part **(b)** in Theorem 9 are not strictly necessary for Γ to be Lai-Ding's; for example, in $\Gamma_3^{LD}\big((1),0\big)$ there are two non-nilpotent participants (1 and 2) which are equipotent. On the other hand, the following example shows it is not enough to assume only that Γ is non-degenerate, or even that the underlying Brickell's scheme has non-zero and pairwise distinct participants' identities.

Let Γ be the access structure realized by the Brickell's scheme (over $\mathbb{F}_3$) corresponding to the matrix

$$\left[\begin{array}{c|cccc} 1 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

By Lemma 2.7, Γ consists of two omnipotent and two nilpotent participants. Now, suppose that this Γ is a sub-structure induced by a Lai-Ding's structure $\Gamma_q^{LD}(\mathbf{c},i)$ on a track $(x_0,x_1,y_0,y_1)\in\mathbb{F}_q^3$, where x_0,x_1 are omnipotent and y_0,y_1 are nilpotent. Then, in the associated matrix

$$\left[\begin{array}{c|cccc} & x_0^{c_0} & x_1^{c_0} & y_0^{c_0} & y_1^{c_1} \\ \varepsilon_i & \vdots & \vdots & \vdots & \vdots \\ & x_0^{c_{k-1}} & x_1^{c_{k-1}} & y_0^{c_{k-1}} & y_1^{c_{k-1}} \end{array}\right],$$

the left-most column is spanned by each of the two following columns, but not by any of the right-most two. If $k=1$, this implies $y_0^{c_0}=y_1^{c_0}=0$ and hence $y_0=y_1$, which is forbidden. If $k>1$, then the fact that $(x_j^{c_0},\ldots,x_j^{c_{k-1}})$ is parallel to ε_i (for $j=0,1$) clearly implies that $x_j=0$ (with $c_0=0$ and $i=0$); hence, $x_0=x_1$ which cannot take place. This shows that Γ is not a Lai-Ding's access structure. On the other hand, it admits realization by a Lai-Ding's scheme with repeated identities, as follows from part **(a)** of the theorem.

Remark 6.2. As we already mentioned in Section 2.4.2, Seymour [50] and Whittle [65] showed that there is no polynomial algorithm deciding whether a given connected matroid is representable. This translates to the difficulty of deciding whether an access structure is Brickell's, and also (by Theorem 9a), Lai-Ding's with repeated identities.

Moreover, we note that the construction of [50] involves connected matroids without circuits of size $\leqslant 3$, which, by virtue of Fact 6.3 stated below, implies that their ports do not contain equipotent pairs. Therefore, in view of Theorem 9b, we expect the difficulty to remain also when repeated identities are forbidden.

Nevertheless, we do not *claim* that the property of being a Lai-Ding's access structure is not polynomially decidable. In order to formulate such claim, we would first need a formal model of decision problems for access structures (analogous to that of "independence oracle" for matroids; see [50]); then, a proof would require a polynomial reduction between the two models. This issue is quite far from our main topics, and we leave it without deeper discussion.

The following fact is fairly intuitive but seems not to follow obviously from [39] or [63].

Fact 6.3. Let $\mathcal{M} = (M, \mathcal{I})$ be a connected matroid and m_0, a, b be pairwise distinct elements of M. Assume that a and b are equipotent in the port $\Gamma(\mathcal{M}, m_0)$. Then, $\{a, b\}$ is dependent in $\mathcal{M}$.

Proof. **1.** Let $\Gamma = \Gamma(\mathcal{M}, m_0)$. Since $\mathcal{M}$ is connected, it has a circuit containing m_0 and a. Let $Y \cup \{m_0, a\}$, with $m_0, a \notin Y$, be any of such circuits. Then, the sets

$$Y \cup \{m_0\}, \qquad Y \cup \{a\} \tag{6.1}$$

must be independent; hence, by the definition of Γ, $Y \cup \{a\}$ is Γ-authorized while Y is not. Hence, Y belongs to the relevance of a (see Section 2.3.2). By equipotence, we deduce that $Y \cup \{b\}$ is Γ-authorized. By (6.1), it follows that $Y \cup \{m_0, b\}$ is dependent, and consequently $b \notin Y$.

2. We claim that every circuit C in $\mathcal{M}$ satisfies the implication

$$m_0 \in C \subseteq Y \cup \{m_0, a, b\} \quad \Longrightarrow \quad C = Y \cup \{m_0, a\} \text{ or } C = Y \cup \{m_0, b\}. \tag{6.2}$$

Suppose that there is some C violating this. Denote $Y' = C \setminus \{m_0, a, b\}$. We consider four cases, depending on whether C contains a and/or b:

- If $a, b \notin C$, then $C \subseteq Y \subseteq \{m_0\}$ which is independent, a contradiction.
- If C contains both a and b, then $Y' \cup \{m_0, a, b\}$ is dependent while $Y' \cup \{m_0, a\}$ and $Y' \cup \{a, b\}$ are not; it follows that $Y' \cup \{a, b\}$ is Γ-authorized while $Y' \cup \{a\}$ is not. This contradicts equipotence of a and b.
- If C contains a but not b, then it is contained in $Y \cup \{m_0, a\}$ which is also a circuit; this implies that they are equal.
- If C contains b but not a, we need to prove that it coincides with $Y \cup \{m_0, b\}$. Suppose the contrary. Then, by repeating step 1 with the roles of a, b swapped, and Y' playing the role of Y, we obtain that $Y' \cup \{m_0, a\}$ is dependent. Since this set is contained in $Y \cup \{m_0, a\}$ which is a circuit, they must coincide; in particular, $Y = Y'$, as desired.

3. Having proved (6.1), we will now utilize a statement appearing in the proof of [63, Section 5.4, Theorem 1]. Adjusted to our notation, it says:

> Let $\mathcal{C}$ be the family of circuits in a connected matroid $\mathcal{M} = (M, \mathcal{I})$ which contain a fixed element $e \in M$, and let
>
> $$D(X) = X \setminus \bigcap \{C \in \mathcal{C} \,\big|\, C \subseteq X\} \qquad \text{for } X \subseteq M.$$
>
> Then, the circuits of M not containing e are exactly the minimal sets of the form $D(C_1 \cup C_2)$, where C_1, C_2 are distinct members of $\mathcal{C}$.

Applying this to $e = m_0$, $C_1 = Y \cup \{m_0, a\}$ and $C_2 = Y \cup \{m_0, b\}$, we obtain that

$$D(C_1 \cup C_2) = \big(Y \cup \{m_0, a, b\}\big) \setminus \bigcap \big\{C \text{ a circuit in } \mathcal{M} \;\big|\, m_0 \in C \subseteq Y \cup \{m_0, a, b\}\big\}.$$

By (6.2), the above intersection is exactly $Y \cup \{m_0\}$, and consequently $D(C_1 \cup C_2) = \{a, b\}$. By the claim of [63], this set must contain a circuit, which gives our claim. □

6.1.1 Auxiliary facts

Recall that Brickell's schemes (defined for $\mathcal{P}$, D, k, q and ϕ) can be conveniently represented by their *associated matrices* (over $\mathbb{F}_q$, of size $k \times (|\mathcal{P}| + 1)$), as defined by the formula (2.3). For a fixed ordering of $\mathcal{P}$, this representation is a one-to-one correspondence: every matrix is associated to a unique Brickell's scheme.

Definition 6.4. Let K be a field and A, B be two matrices over K with the same number of columns. We call A, B *column-equivalent* (or shortly: *c-equivalent*) *over* K (notation: $A \overset{c}{\sim}_K B$) if they can be obtained from each other in a number of steps of the following kind:

- elementary operations on matrix rows;
- adding/removing a zero row;
- multiplying a column by a non-zero element of K.

The field K will be omitted when clear from the context.

Since all the above operations have no influence on the linear (in-)dependence over K of the columns in matrices, using Lemma 2.7 we immediately obtain the following.

Fact 6.5. Let A, B, be two c-equivalent matrices over K. Then:

(a) the column matroids $\mathcal{M}(A)$, $\mathcal{M}(B)$ (see Section 2.3.3) coincide;

(b) the Brickell's schemes (over K) associated to A, B realize the same access structure. □

Hence, to prove Theorem 9 it is sufficient to transform any given matrix A over a finite field $\mathbb{F}_q$ (associated to the Brickell's scheme which realizes the given access structure Γ) into a matrix B which is c-equivalent to A (possibly over an extension of $\mathbb{F}_q$, since the column matroid does not change under ground field extension) and is associated to a Lai-Ding's scheme (possibly with repeated identities).

The main part of the proof of Theorem 9 will indeed focus on realizing the above plan; however, we will need another argument for the case when A contains zero columns. (The same extending trick will be also used to ensure non-repeating identities in part **(b)**).

In the proof, we will also use the following two facts.

Fact 6.6 ([31, Corollary 2.38])**.** Let q be a prime power, $n \geqslant 1$ and $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{F}_{q^n}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, we have

$$\det \left[\alpha_j^{q^i}\right]_{0 \leqslant i,j < n} \neq 0. \tag{6.3}$$

Fact 6.7. Let $\mathcal{M}_i = (M, \mathcal{I}_i)$ (for $i = 1, 2$) be two matroids over the same finite set M, and $m_0 \in M$. Let N be a set of elements which are nilpotent in both ports $\Gamma(\mathcal{M}_1, m_0)$ and $\Gamma(\mathcal{M}_2, m_0)$, and suppose that the sub-matroids of $\mathcal{M}_1$ and $\mathcal{M}_2$ induced by $M \setminus N$ coincide. Then, the ports $\Gamma(\mathcal{M}_1, m_0)$ and $\Gamma(\mathcal{M}_2, m_0)$ coincide.

Proof. For $i = 1, 2$, the port $\Gamma(\mathcal{M}_i, m_0)$ is fully determined by its minimal authorized sets, which must be disjoint with N by the definition of a nilpotent element. Now, by the definition of port, a subset $B \subseteq M \setminus N$ is minimal authorized in $\Gamma(\mathcal{M}_i, m_0)$ if and only if B belongs to $\mathcal{I}_i$ while $B \cup \{m_0\}$ does not. This, however, depends only on the sub-matroid of $\mathcal{M}_i$ induced by $M \setminus N$ (by its definition). Since this submatroid does not depend on i, the claim follows. □

6.1.2 Proof of Theorem 9

1. Let $\Sigma = \Sigma^B(J, v_D)$ be any Brickell's scheme. By definition, the access structure realized by Σ is non-degenerate if and only if the empty subset $\emptyset \subseteq \mathcal{P}$ is not authorized; by Lemma (2.7), this is equivalent to $v_D \neq 0$.

Now, by Definitions 2.9 and 2.12, this condition is not satisfied by any Lai-Ding's scheme, even with repeated identities; this proves the "only if" direction in **(a)**.

The positive direction in **(a)** and **(b)** will be proved in steps 2-7 . The main idea appears in step 4; step 3 serves as a technical preparation for it, and step 2 is purposed to handle nilpotent participants.

2. Now, let Γ be a non-degenerate access structure realized by a Brickell's scheme $\Sigma = \Sigma_q^B(J, v_D)$. Let A be the associated matrix of this scheme (see (2.3)), and denote by n the number of its columns. Let z be the number of nilpotent elements in Γ, and

$$l = \dim \operatorname{span}\big(\{v_D\} \cup X\big), \qquad \text{where} \qquad X = \{J(p) \,|\, p \text{ is not nilpotent in } \Gamma\}.$$

In particular, we have $l + z \leqslant n$.

By step 1, the left-most column in A (equal to v_D) is non-zero; hence, it can be extended to a basis of $\operatorname{span}(\{v_D\} \cup X)$ by using $l - 1$ vectors from X. Hence, without losing generality, we may order the participants (i.e. permute the columns of A except for the left-most one) so that:

(i) the left-most l columns of A are linearly independent;

(ii) for $1 \leqslant i < l$, the i-th column of A corresponds to a non-nilpotent participant in Γ; (note that the 0-th column equals v_D and does not correspond to any participant)

(iii) the next z columns correspond to the nilpotent participants in Γ.

Let A' (resp.A'') denote the matrix formed by the left-most l (resp. rightmost $n - l - z$) columns of A, and

$$B = \left[\begin{array}{c|c|c} A' & 0 & A'' \\ \hline 0 & I_z & 0 \end{array}\right], \tag{6.4}$$

where I_z denotes the identity matrix of size $z \times z$, and "0" stands for a zero block of an appropriate size. While the column matroids $\mathcal{M}(A)$ and $\mathcal{M}(B)$ do not have to coincide, it is easy to see the equality of ports

$$\Gamma\big(\mathcal{M}(A),\, 0\big) = \Gamma\big(\mathcal{M}(B),\, 0\big). \tag{6.5}$$

(For a strict argument, note first that the sub-matroids of $\mathcal{M}(A)$ and $\mathcal{M}(B)$ induced by the set $\{0, \dots, l-1\} \cup \{l+z, \dots, n-1\}$ coincide, since the corresponding sub-matrices consisting of the left-most l and right-most $n - l - z$ columns differ only by addition of z zero rows. On the other hand, for every $l \leqslant j < l + z$, the j-th column of B lies outside the linear span of all other columns in B, so adding it to any collection of other columns does not affect linear independence. Hence, j is nilpotent in $\Gamma(\mathcal{M}(B), 0)$, and also in $\Gamma(\mathcal{M}(A), 0)$ by (i). Now, (6.5) follows by Fact 6.7 with $N = \{l, \dots, l + z - 1\}$).

In this way, we have in particular ruled out zero columns. In the next steps, we will c-equivalently transform B into an associated matrix of a Lai-Ding's scheme (possibly with repeated identities).

3. Let C be the reduced echelon form of B, and C' be the result of removing all zero rows from C. By Definition 6.4, C' is c-equivalent to B (over $\mathbb{F}_q$). We will now construct a matrix D c-equivalent to C' over some extension of $\mathbb{F}_q$ such that the sum of entries in each of its columns equals one.

Denote $k = l + z$. By (6.4), this is the rank of B; moreover, it follows from the property (i) of step 2 that the left-most k columns of B are linearly independent. Hence, we have

$$C' = \left[\begin{array}{ccc|c|c|c} 1 & & & & & \\ & \ddots & & \mathbf{v}_0 & \cdots & \mathbf{v}_{n-k-1} \\ & & 1 & & & \end{array}\right]$$

for some $\mathbf{v}_0, \ldots, \mathbf{v}_{n-k-1} \in \mathbb{F}_q^k$. Now, let q_1 be a power of q greater than $(n-k) \cdot (\frac{q}{q-1})^k$ and let $\mathbf{a}$ be any element of $(\mathbb{F}_{q_1} \setminus \{0\})^k$. By dividing the i-th column and multiplying the i-th row of A'_1 by a_i (for $0 \leqslant i < k$), we obtain a new matrix

$$D' = \left[\begin{array}{ccc|c|c|c} 1 & & & & & \\ & \ddots & & \mathbf{w}_0 & \cdots & \mathbf{w}_{n-k-1} \\ & & 1 & & & \end{array}\right],$$

where each $\mathbf{w}_i$ is obtained by multiplying $\mathbf{v}_i$ by $\mathbf{a}$ coordinatewise; in particular, the sum of its entries is the scalar product $\mathbf{v}_i \circ \mathbf{a}$. We would like to choose $\mathbf{a}$ so that all these products are non-zero. Since $\mathbf{v}_i$ are all non-zero (by the assumptions on A), each of the conditions $\mathbf{v}_i \circ \mathbf{a} \neq 0$ excludes at most q_1^{k-1} potential values for $\mathbf{a}$. This means that an appropriate $\mathbf{a}$ exists because

$$\frac{(n-k) \cdot q_1^{k-1}}{(q_1-1)^k} = \frac{(n-k) \cdot (\frac{q_1}{q_1-1})^k}{q_1} < 1.$$

Hence, we can choose $\mathbf{a} \in (\mathbb{F}_{q_1} \setminus \{0\})^k$ so that the sum of entries in every non-pivot column of D' is non-zero. By scaling every such column, we can make the sum of its entries equal to one; in this way, we obtain the desired matrix D. Altogether, we have

$$B \overset{c}{\sim}_{\mathbb{F}_q} C \overset{c}{\sim}_{\mathbb{F}_q} C' \overset{c}{\sim}_{\mathbb{F}_{q_1}} D' \overset{c}{\sim}_{\mathbb{F}_{q_1}} D.$$

4. Assume now that $k > 1$ (the case $k = 1$ is simpler, and will be handled in step 5). Let $r = q_1^{k-1}$ and $\alpha_1, \ldots, \alpha_{k-1}$ be a basis of $\mathbb{F}_r$ over $\mathbb{F}_{q_1}$. By Fact 6.6, we have

$$\det \left[\alpha_j^{q_1^i}\right]_{0 \leqslant i < k-1,\, 1 \leqslant j < k} \neq 0. \tag{6.6}$$

Now, set $\alpha_0 = 0$ and

$$c_0 = 0, \qquad c_i = q_1^{i-1} \quad \text{for } 1 \leqslant i < k. \tag{6.7}$$

Then, it follows from (6.6) that the matrix

$$Z = \left[\alpha_j^{c_i}\right]_{0 \leqslant i,j < k} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{k-1} \\ 0 & \alpha_1^{q_1} & \alpha_2^{q_1} & \cdots & \alpha_{k-1}^{q_1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \alpha_1^{q_1^{k-2}} & \alpha_2^{q_1^{k-2}} & \cdots & \alpha_{k-1}^{q_1^{k-2}} \end{bmatrix}$$

is also non-singular. This means that the matrix

$$E = Z \circ D$$

is c-equivalent to D over $\mathbb{F}_r$. Let $D = [d_{ij}]$ and $E = [e_{ij}]$ $(0 \leqslant i < k,\, 0 \leqslant j < n)$, and

$$x_j = e_{1j} \qquad \text{for } \ 0 \leqslant j < n. \tag{6.8}$$

We will now verify that

$$E = V M_{\mathbf{c}}(\mathbf{x})^T. \tag{6.9}$$

First, since taking the q_1-th power is an automorphism of $\mathbb{F}_r$ over $\mathbb{F}_{q_1}$, we have

$$e_{ij} = \sum_{s=0}^{k-1} \alpha_s^{q_1^{i-1}} \cdot d_{sj} = \left(\sum_{s=0}^{k-1} \alpha_s \cdot d_{sj} \right)^{q_1^{i-1}} = (e_{1j})^{c_i} = x_j^{c_i} \qquad \text{for all } 2 \leqslant i < k \text{ and } 0 \leqslant j < n.$$

For $i = 1$, the equality $e_{ij} = x_j^{c_i}$ follows immediately from (6.7) and (6.8). Finally, for $i = 0$, we have

$$e_{0j} = \sum_{s=0}^{k-1} 1 \cdot d_{sj} = 1 = x_j^{c_0} \qquad \text{for all } 0 \leqslant j < n$$

because D has been chosen so that the sum of entries in every its column is 1. Hence, (6.9) holds.

5. As a result of steps 3 and 4, we have obtained the following picture (for $k > 1$):

$$B \overset{c}{\sim}_{\mathbb{F}_{q_1}} D \overset{c}{\sim}_{\mathbb{F}_r} E = V M_{\mathbf{c}}(\mathbf{x})^T = \left[\begin{array}{c|c} \varepsilon_0 & V M_{\mathbf{c}}(\hat{\mathbf{x}}_0)^T \end{array}\right], \tag{6.10}$$

where the last equality follows from (6.7) and from the fact that

$$x_0 = e_{10} = \sum_{s=0}^{k-1} \alpha_s^1 \cdot d_{s0} = \alpha_0^1 \cdot 1 = \alpha_0 = 0,$$

where we have used the fact that the left-most k rows of D form the identity matrix.

For $k = 1$, D must be a single row in which all entries are equal to 1. In such case, we let $E = D$ and $r = q_1$, and observe that

$$E = \left[\begin{array}{c|ccc} 1 & 1 & \dots & 1 \end{array}\right] = \left[\begin{array}{c|c} 1 & V M_{\mathbf{c}}(\hat{\mathbf{x}}_0)^T \end{array}\right],$$

where $\mathbf{c} = (0)$ and $\mathbf{x}$ is any track in $\mathbb{F}_{q_1}^n$ (it exists since we assumed in step 3 that $q_1 \geqslant (n-k)+1 = n$). This means that such choice of E also satisfies (6.10).

6. Let $\mathcal{P} = \{p_0, \dots, p_{n-2}\}$, and define an identity-setting function $I : \mathcal{P} \to \mathbb{F}_r$ by the formula $I(p_i) = x_{i+1}$ for $0 \leqslant i < n-1$. Then, by definition, E is the matrix associated to the scheme $\Sigma_r^{LD*}(I, \mathbf{c}, 0)$.

By (6.10) and Fact 6.5, E has the same column matroid as B. Then, by (6.5), we deduce equality of ports

$$\Gamma\big(\mathcal{M}(A), 0\big) = \Gamma\big(\mathcal{M}(E), 0\big).$$

This gives, by Lemma 2.7', an isomorphism between the access structures induced by the Brickell's schemes associated to the matrices A and E. This means that Γ admits realization by a Lai-Ding's scheme, possibly with repeated identities. This finishes the proof of **(a)**.

7. Now, **(b)** can be also deduced from the above construction, as follows.

Suppose that the given access structure Γ does not contain equipotent pairs of non-nilpotent elements. Then, by Lemma 2.7, the left-most $n - z$ columns in A (which correspond to non-nilpotent participants) must be pairwise non-parallel. By the definition of B, it follows that *all* columns in B are pairwise non-parallel. Since such property is preserved by c-equivalence, it must hold as well for E. This means in particular that the columns of E are pairwise distinct. On the other, since $c_1 = 1$, the first row in E (i.e. the one below the top-most one) contains exactly the sequence $\mathbf{x}$. This ensures that the identity-setting function I defined in step 5 is injective. This proves **(b)**, and finishes the whole proof. □

6.2 Access structures in special cases

6.2.1 The case of c arithmetic

As we already observed in Section 4.4, the Lai-Ding's scheme defined by an arithmetic progression of exponents $\mathbf{c} = c_0 + \lambda \cdot \mathbf{e}_k$ essentially reduces to the Shamir's type scheme defined by k (see Fact 4.14). Hence, the corresponding access structures must also be closely related.

Fact 6.8. Under the assumptions of Fact 4.14, the access structure $\Gamma_q^{LD}(\mathbf{c}, i)$, with the nilpotent element 0 removed in the case when $c_0 > 0$, admits a homomorphism to the Shamir's type access structure $\Gamma_q^{ST}(k, i)$, defined by the formula

$$\phi(x) = x^\lambda \qquad \text{for} \quad x \in \mathbb{F}_q.$$

Proof. The fact that 0 is nilpotent when $c_0 > 0$ follows directly from Fact 4.14b.

Let

$$D = \begin{cases} \mathbb{F}_q & \text{if } c_0 = 0, \\ \mathbb{F}_q \setminus \{0\} & \text{if } c_0 > 0, \end{cases}$$

(this is the domain of ϕ), and $\mathbf{t}$ be any track with elements in D. By Fact 4.14 and the definition of D, we have:

$$\mathbf{t} \text{ is } (\mathbf{c}, i)\text{-authorized} \qquad \Leftrightarrow \qquad \text{there is } \mathbf{u} \sqsubseteq \mathbf{t} \text{ satisfying (4.10a)}.$$

The right-hand side clearly implies that that the set of elements of $\mathbf{t}^\lambda$ belongs to $\Gamma_q^{ST}(k, i)$. Conversely, if the set of elements of $\mathbf{t}^\lambda$ belongs to $\Gamma_q^{ST}(k, i)$, then (by removing repetitions) we may choose $\mathbf{u} \sqsubseteq \mathbf{t}$ such that $\mathbf{u}^\lambda$ is a track with the same set of elements as $\mathbf{t}^\lambda$; hence it satisfies (4.10a). This proves that ϕ is a homomorphism of access structures. □

As a consequence of Fact 6.8, we observe that our whole *negative* knowledge on Shamir's type access structures translates straightforwardly to the Lai-Ding's structures of the considered kind:

Corollary 6.9. Let $\mathbf{c}$ be an arithmetic progression of length $k \geqslant 2$. Then, all the non-existential statements of Theorem G, that is, parts (a-d) and the "only if" direction in (f), apply as well to the access structure $\Gamma = \Gamma_q^{LD}(\mathbf{c}, i)$. □

Moreover, the *positive* part of Theorem G is also preserved under some subtle modifications. This fact will be strictly formulated in Theorem 10 below, after some preparation.

Denotation 6.10. **(a)** For a finite group G and its element x, we denote by $\mathrm{ord}(x)$ the order of x in G.

(b) For a positive integer a and a prime p, we denote by $\nu_p(a)$ the greatest $l \in \mathbb{N}$ for which $p^l \mid a$.

(c) For two positive integers a, b, we denote

$$\gcd(a, b^\infty) = \prod_{\substack{p \in P \\ p \mid b}} p^{\nu_p(a)}.$$

(In other words, it is the quotient of a by its maximal divisor coprime to b).

Fact 6.11. Let G be a finite cyclic group and $a, b \in \mathbb{Z}_{>0}$. Then, the set

$$M = \big\{x \in G \;\big|\; \mathrm{ord}(x^a) = b\big\}$$

is non-empty if and only if $|G|$ is divisible by $\gcd(a, b^\infty) \cdot b$.

Proof. Let $n = |G|$. Since G is cyclic, the subgroup of a-th powers in it is cyclic of size $\frac{n}{\gcd(a,n)}$, and it contains elements of order b if and only if b divides its size. Hence, $M \neq \emptyset$ is equivalent to

$$b \;\Big|\; \frac{n}{\gcd(a, n)}, \tag{6.11}$$

which in turn happens if and only if for every $p \in P$ we have

$$\nu_p(b) \leqslant \nu_p(n) - \min\big(\nu_p(a),\, \nu_p(n)\big). \tag{6.12}$$

Now, treating $\nu_p(a), \nu_p(b)$ as parameters and $\nu_p(n)$ as the variable, we easily see that this is equivalent to

$$\nu_p(n) \geqslant \begin{cases} 0 & \text{if } \nu_p(b) = 0, \\ \nu_p(a) + \nu_p(b) & \text{if } \nu_p(b) > 0. \end{cases} \tag{6.13}$$

Finally, the conjunction of (6.13) for all $p \in P$ can be expressed in short as

$$\gcd(a, b^\infty) \cdot b \;\Big|\; n. \tag{6.14}$$

Hence, (6.11) and (6.14) are equivalent. This finishes the proof. □

Fact 6.12. Let $\varphi : \Gamma \to \Gamma'$ be a homomorphism of access structures, and $A \subseteq \mathcal{P}_\Gamma$. Then, we have

$$A \in \mathcal{B}_\Gamma \qquad \Longleftrightarrow \qquad \phi(A) \in \mathcal{B}_{\Gamma'} \text{ and } |\phi(A)| = |A|.$$

Proof. Suppose first that $\phi(A) \in \mathcal{B}_{\Gamma'}$ and $|\phi(A)| = |A|$. Then, A is clearly Γ-authorized, and for every $A' \subsetneq A$ we have $\phi(A') \subsetneq \phi(A)$, which implies that $\phi(A')$ is not Γ'-authorized, whence A' is not Γ-authorized. This proves the minimality of A in $\mathcal{A}_\Gamma$, as desired.

Conversely, let $A \in \mathcal{B}_\Gamma$. Then, $\phi(A)$ is Γ'-authorized. As for minimality, if there was some Γ'-authorized set $B \in \mathcal{A}_{\Gamma'}$, then $A \cap \phi^{-1}(B) \subsetneq A$ would be Γ-authorized since it maps to B under ϕ. This cannot hold since A is minimal Γ-authorized. Hence, $\phi(A) \in \mathcal{B}_{\Gamma'}$.

Also, if assuming $A \in \mathcal{B}_\Gamma$ we had $|\phi(A)| < |A|$, then there would exist $A' \subsetneq A$ such that $\phi(A') = \phi(A)$. In such case, A' would be also Γ-authorized, contradicting the minimality of A. This finishes the proof. □

Theorem 10. *Let* $\mathbf{c}$ *be an arithmetic progression of length* $k \geqslant 2$*, with common difference* λ*. Then, the access structure* $\Gamma = \Gamma_q^{LD}(\mathbf{c}, i)$ *satisfies all the statements of Theorem G, with the following modifications:*

- *both conditions "*$q \equiv 1 \pmod r$*" (in parts (e-f)) shall be replaced with*

$$\text{“}q \equiv 1 \pmod{\gcd(\lambda, r^\infty) \cdot r}\text{”}$$

  (see Denotation 6.10c);
- *the condition "*$q > 2k - 1$*" (in (g)) shall be replaced with*

$$\text{“}q \text{ is odd and exceeds the expression } (4.15)\text{”};$$

- *the condition "*$q \geqslant n + r\binom{n-2}{k-2}$*" (in (h)) shall be replaced with*

$$\text{“}q \geqslant \lambda\left(n + r\tbinom{n-2}{k-2}\right)\text{”}. \tag{6.15}$$

Proof. **1.** The claim for parts **(a-d)** follows from Corollary 6.9. The modified version of **(g)** follows straightforwardly from Theorem 5.

2. We will now argue for **(e)** and for the "only if" direction in **(f)**. (Note that the "if" direction in **(f)** is just a special case of **(e)**).

For this, we will recall Theorems 2 and 3 from [55] in more detail than we cited in Theorem G, namely:

(Th2) Under the assumptions of **(e)**, for every $a \in \mathbb{F}_q^\times$ and every $\zeta \in \mathbb{F}_q^\times$ with $\operatorname{ord}(\zeta) = r$, the track

$$\mathbf{x}_{a,\zeta} = (a, a\zeta, a\zeta^2, \ldots, a\zeta^{r-1})$$

is (k, i)-authorized;

(Th3) Under the assumptions of **(f)**, all (k, i)-authorized tracks of length r (if any) are of the form $\mathbf{x}_{a,\zeta}$ for some a, ζ as above.

Denote $R = \gcd(\lambda, r^\infty) \cdot r$ and

$$\mathcal{A} = \left\{ \mathbf{t} \in \mathbb{F}_q^r \;\middle|\; \begin{array}{l} \mathbf{t} \text{ is a zero-free } (k,i)\text{-authorized track} \\ \text{consisting solely of } \lambda\text{-th powers in } \mathbb{F}_q \end{array} \right\}$$

By Fact 4.14, $\Gamma_q^{LD}(\mathbf{c}, i)$ contains authorized sets of size r if and only if $\mathcal{A} \neq \emptyset$. On the other hand, using Fact 6.11 (with $a = \lambda$, $b = r$, and $G = \mathbb{F}_q^\times$), we deduce that:

- If $R \mid q-1$, then, by Fact 6.11, there exists $\zeta \in \mathbb{F}_q^\times$ of order r which is a λ-th power. Then, by (Th2), $\mathbf{x}_{1,\zeta}$ is an element of $\mathcal{A}$;
- If $\mathcal{A} \neq \emptyset$, then, by (Th3), we have $\mathcal{A} \ni \mathbf{x}_{a,\zeta}$ for some a, ζ as above. This implies that $a^{-1} \cdot a\zeta = \zeta$ is a λ-th power in $\mathbb{F}_q^\times$ of order r. Hence, by Fact 6.11, $R \mid q-1$.

Altogether, we obtain that $q \equiv 1 \pmod{R}$ is equivalent to $\mathcal{A} \neq \emptyset$, i.e. to existence of $(\mathbf{c}, i)$-authorized sets of size r. This proves the modified versions of both **(e)** and the "only if" direction in **(f)**, as desired.

3. It remains to prove the modified version of **(h)**. Suppose that its assumptions are satisfied; in particular, we assume that A is a set from $\mathcal{B}_\Gamma$ of size r. Let ϕ denote the homomorphism between Γ (possibly with zero removed) and $\Gamma' = \Gamma_q^{ST}(k,i)$ coming from Fact 6.8. By Fact 6.12, the set $\phi(A)$ must belong to $\mathcal{B}_{\overline{\Gamma}}$ and be of size r.

Recall that our goal is to find a substructure Δ in Γ induced by a subset $B \subseteq \mathbb{F}_q$ of size n such that

$$\mathcal{B}_\Delta = \{A\} \cup \big\{C \subseteq B \;\big|\; |C| = k\big\}. \tag{6.16}$$

Denote by $\mathbb{F}_q^\lambda$ the set of λ-th powers in $\mathbb{F}_q$. We claim that it is sufficient for this to find a substructure Δ' in Γ' induced by a subset $B' \subseteq \mathbb{F}_q^\lambda$ of size n such that

$$\mathcal{B}_{\Delta'} = \{\phi(A)\} \cup \big\{C \subseteq B' \;\big|\; |C| = k\big\}. \tag{6.17}$$

Indeed, once we find such Δ' (or equivalently, B'), we may define B to be any set which consists of A and of exactly one element of $\phi^{-1}(x')$, for every $x \in B' \setminus \phi(A)$. Then, ϕ induces a bijection between B and B'; in particular, $|B| = n$. Moreover, for every $C \subseteq B$, Fact 6.12 ensures that $C \in \mathcal{B}_\Delta$ if and only if $\phi(C) \in \mathcal{B}_{\Delta'}$, which allows to deduce (6.16) straightforwardly from (6.17).

To extend the set $\phi(A)$ to a suitable B', we follow the proof of the original version of **(h)**, with an additional restriction that $B' \subseteq \mathbb{F}_q^\lambda$. We recall that **(h)** has been cited from Theorem 3 in [56]; the proof given in [56] has the form of an inductive procedure of choosing consecutive elements of $B' \setminus \phi(A)$. An inspection of this procedure reveals that every of those choices is restricted only by a set of forbidden values which is of size at most $F = n + r\binom{n-2}{k-2} - 1$. (Here, we use once more that fact that $|\phi(A)| = |A| = r$). On the other hand, the size of $\mathbb{F}_q^\lambda$ is certainly at least $\frac{q-1}{\lambda}$, and the new assumption (6.15) guarantees exactly that this number exceeds F.

Altogether, we arrive at the conclusion that a subset $B' \subseteq \mathbb{F}_q^\lambda$ of size n satisfying (6.17). As described before, this implies the existence of B and Δ with the desired properties. □

6.2.2 The case of $\hat{\mathbf{c}}_i$ arithmetic

Finally, we will investigate access structures under the assumptions of Section 4.3, i.e. that $k \geqslant 3$ and $\hat{\mathbf{c}}_i$ is an arithmetic progression with common difference l. (Recall also that we have denoted $m = c_i - \hat{c}_{i,0}$). In particular, these are exactly the assumptions of Lemma 4.6 from that section, which will now serve as a starting point.

Fact 6.13. Under the assumptions of Lemma 4.6, let $\mathcal{M}$ denote the set of minimal $(\mathbf{c}, i)$-privileged tracks, and $\mathcal{N}$ denote the set of zero-free tracks of length 2 satisfying (4.4). Then:

(a) If $c_i = 0$, then $\mathcal{M} = \mathcal{N} \cup \{(0)\}$;

(b) Otherwise, $\mathcal{M} = \mathcal{N}$.

Proof. This follows straightforwardly from Lemma 4.6. □

Definition 6.14. Let Γ_1, Γ_2 be two access structures, and $k \geqslant 0$. A map $f : \mathcal{P}_{\Gamma_1} \to \mathcal{P}_{\Gamma_2}$ will be called an *isomorphism below size* k (between Γ_1 and Γ_2) if the condition (2.7) is satisfied for sets of size less than k, that is,

$$\forall_{\substack{C \subseteq \mathcal{P}_{\Gamma_1} \\ |C| < k}} \quad C \in \mathcal{A}_{\Gamma_1} \quad \Longleftrightarrow \quad f(C) \in \mathcal{A}_{\Gamma_2}.$$

Definition 6.15. A graph G will be called *distinguished* if it is a difference of two graphs H_1, H_2, each of which is a disjoint union of cliques. (See Section 2.3.1).

Definition 6.16. In a graph G, a subset $X \subseteq V(G)$ will be called *sparse* if all its elements belong to pairwise distinct connected components of G.

Lemma 6.17. Under the assumptions of Lemma 4.6, let Γ be any induced substructure of the access structure $\Gamma_q^{LD}(\mathbf{c}, i)$. Then:

(a) Γ has at most one omnipotent element;

(b) If Γ does not contain omnipotent elements, then there is a distinguished graph G_Γ, having $\mathcal{P}_\Gamma$ as its set of vertices, such that the map $\mathrm{id}_{\mathcal{P}_\Gamma}$ is an isomorphism below size k between Γ and the graphic access structure $\Gamma(G_\Gamma)$;

(c) In the situation of **(b)**, every minimal Γ-authorized set of size k is sparse in G_Γ.

Proof. **(a)** By Fact 6.13, Γ cannot have omnipotent elements other than 0.

(b) Again by Fact 6.13, the assumption of no omnipotent elements implies that the authorized sets in Γ of size less than k are exactly these which contain at least one pair $\{t_0, t_1\}$ satisfying (4.4). These are exactly the authorized sets in the graphic structure $\Gamma(G_\Gamma)$, where $V(G_\Gamma) = \mathcal{P}_\Gamma$ and

$$E(G_\Gamma) = \big\{\{u, v\} \;\big|\; u \neq v,\ uv \neq 0,\ 1 = (uv^{-1})^l \neq (uv^{-1})^m\big\} = E(C_l) \setminus E(C_m), \tag{6.18}$$

where, for any $d \in \mathbb{Z}_{>0}$, C_d denotes the graph defined by

$$V(C_d) = \mathcal{P}_\Gamma, \qquad E(C_d) = \big\{\{u, v\} \,\big|\, u \neq v,\ u^d = v^d\big\}. \tag{6.19}$$

It remains to notice that, for every $d \in \mathbb{Z}_{>0}$, $\mathcal{P}_\Gamma$ decomposes into a disjoint union of sets of the form $\{v \in \mathcal{P}_\Gamma \,|\, v^d = a\}$, for $a \in \mathbb{F}_q$, each of which is a clique in C_d. Hence, C_d is a disjoint union of cliques. Then, it follows that $G_\Gamma = C_l \setminus C_m$ is distinguished.

(c) Let $X \subseteq \mathcal{P}_\Gamma$ be of size k and suppose that X is not sparse in G_Γ, i.e. there are two distinct elements $x, y \in X$ connected by a path in G_Γ. From the proof of **(b)** we know that $G_\Gamma = C_l \setminus C_m$; hence x, y must be connected also in C_l, which implies that $\{x, y\} \in E(C_l)$ because C_l is a disjoint union of cliques.

We now consider two cases. If $\{x, y\}$ is not an edge in C_m, then it is an edge in G_Γ, whence it is authorized in $\Gamma(G_\Gamma)$ and therefore also in Γ. This means that X is not a minimal authorized subset. If, on the other hand, $\{x, y\}$ is an edge in C_m, then by (6.19) we have

$$x^l = y^l, \qquad x^m = y^m,$$

which implies that the matrix $VM_{l\cdot\mathbf{e}_{k-1}||(m)}((x,y))$ has two identical rows, and therefore, by Fact 4.4, $VM_{\mathbf{c}}((x,y))$ is of rank one. Now, let $\mathbf{t}$ be any track containing all the elements of X; then $VM_{\mathbf{c}}(\mathbf{t})$ cannot be non-singular as it contains $VM_{\mathbf{c}}((x,y))$. This means that $\mathbf{t}$ does not satisfy the condition (ii) of Lemma 4.6b. Then, depending on whether it satisfies (i), $\mathbf{t}$ can either be non-authorized or contain an authorized sub-track of length 2.

In either case, we conclude that X cannot be a minimal Γ-authorized set. □

The above lemma presents certain restrictions on the layout of privileged coalitions in Lai-Ding's schemes. We will now focus on proving the positive result, which might be understood as a partial converse for Lemma 6.17. Intuitively, we claim that Lai-Ding's access structures may be isomorphic, below their „expected threshold" size k, to graphic access structures determined by arbitrary distinguished graphs.

More precisely, for every G and k as above, there is a Lai-Ding's access structure Γ (for $\mathbf{c}, i$ as currently considered) isomorphic to $\Gamma(G)$ below size k; moreover, Γ can be chosen to be „optimally generous" in the sense that its basis $\mathcal{B}$ contains all the subsets of size k which are allowed by Lemma 6.17 to belong there. All these claims are summarized in the following theorem.

Theorem 11. *Let $k \geqslant 3$, G be a distinguished graph, and let $\mathcal{A}$ be the family of all sparse subsets of $V(G)$ of size k. Then, the access structure Γ defined by*

$$\mathcal{P}_\Gamma = V(G), \qquad \mathcal{B}_\Gamma = E(G) \cup \mathcal{A}$$

is embeddable into a Lai-Ding's access structure of the form $\Gamma_q^{LD}(\mathbf{c}, i)$, where $|\mathbf{c}| = k$ and $\hat{\mathbf{c}}_i$ is an arithmetic progression.

The proof will be preceded with two remarks.

Remark 6.18. Recall from Section 2.1.2 than an access structure can be defined by specifying its basis, provided that every two its distinct elements are incomparable; the above family $E(G) \cup \mathcal{A}$ clearly satisfies the condition because every element of $\mathcal{A}$ is a sparse subset of G.

Remark 6.19. We note that Theorem 11 implies in particular that every graphic access structure $\Gamma(G)$ for a distinguished graph G is Lai-Ding's. Indeed, it suffices to choose k exceeding $|G|$.

Proof of Theorem 11. **1.** Denote $M = |V(G)|$. Let H_1, H_2 be disjoint unions of cliques such that $G = H_1 \setminus H_2$. Let $X_1, \ldots, X_A$ (resp. $Y_1, \ldots, Y_B$) denote the (vertex sets of) connected components of G (resp. H_2); note that $A, B \leqslant M$. For every $1 \leqslant a \leqslant A$ and $1 \leqslant b \leqslant B$, let $S_{a,b}$ denote the size of the intersection $X_a \cap Y_b$, and let

$$v_{a,b,1}, \ \ldots, \ v_{a,b,S_{a,b}}$$

be an enumeration of all its elements.

Clearly, for every subset $X \subseteq V(G)$, we have

$$X \text{ is sparse in } G \quad \Leftrightarrow \quad \text{for every } v_{a,b,s} \neq v_{a',b',s'} \text{ in } X, \quad a \neq a'. \tag{6.20}$$

Also observe that, for any a, b, s and a', b', s', we have

$$\{v_{a,b,s}, v_{a',b',s'}\} \in E(G) \quad \Leftrightarrow \quad a = a' \text{ and } b \neq b'. \tag{6.21}$$

Indeed, „⇒" is clear, while „⇐" holds because $a = a'$ implies that $v_{a,b,s}, v_{a',b',s'}$ are connected by a path in G and thus also in H_1, which is a disjoint union of cliques, whence they must be neighbours in H_1; on the other hand, $b \neq b'$ means that they are not neighbours in H_2, which justifies the claim.

2. Define integers N, m, l by the formulas

$$N = 1 + M + \tbinom{M-1}{k-1}, \tag{6.22a}$$

$$m = N + 1, \tag{6.22b}$$

$$l = \big(2 + N\big) \cdot m \tag{6.22c}$$

and choose a prime q so that

$$q > A \cdot l + 1, \qquad q \equiv 1 \pmod{l}. \tag{6.22d}$$

(The existence of such q follows from Theorem A). Let

$$\mathbf{c} = \big(0,\, m,\, l,\, 2l,\, \ldots,\, (k-2)l\big), \qquad i = 1.$$

Then, $\hat{\mathbf{c}}_i$ is arithmetic with common difference l, and we have $m = c_i - \hat{c}_{i,0}$, which means that the symbols l, m as defined by (6.22) coincide with the denotations used generally throughout this section.

3. Let α be a fixed generator of the multiplicative group $\mathbb{F}_q^\times$. For any non-negative numbers $a < A$, $\mu < N$, $s < M$ define

$$\psi(a, \mu, s) = \alpha^{a + \frac{q-1}{l}\mu + \frac{q-1}{m}s}. \tag{6.23a}$$

Then, we have

$$\psi(a, \mu, s)^m = \alpha^{am + \frac{(q-1)m}{l}\mu}, \tag{6.23b}$$

$$\psi(a, \mu, s)^l = \alpha^{al}. \tag{6.23c}$$

Since the multiplicative order of α is $q - 1$, and we have

$$a + 1 \leqslant A < \tfrac{q-1}{l}, \qquad \mu + 1 \leqslant N < \tfrac{l}{m}, \qquad s + 1 \leqslant M < m$$

by the conditions (6.22), the formulas (6.23) visibly imply that

$$\psi(a, \mu, s) \text{ is injective as a function of } (a, \mu, s); \tag{6.24a}$$

$$\psi(a, \mu, s)^m \text{ does not depend on } s \text{ and is injective as a function of } (a, \mu); \tag{6.24b}$$

$$\psi(a, \mu, s)^l \text{ does not depend on } \mu, s \text{ and is injective as a function of } a. \tag{6.24c}$$

4. We will now choose elements $x_{a,b,s} \in \mathbb{F}_q \setminus \{0\}$ for all $a < A$, $b < B$, $s < S_{a,b}$ so that the assignment

$$\varphi : V(G) \to \mathbb{F}_q, \qquad \varphi(v_{a,b,s}) = x_{a,b,s} \quad \text{for } a < A,\ b < B,\ s < S_{a,b} \tag{6.25}$$

will induce an embedding from Γ to the access structure $\Gamma' = \Gamma_q^{LD}(\mathbf{c}, i)$.

The definition of $x_{a,b,s}$ is inductive with respect to pairs (a, b) belonging to the set

$$I = \big\{(a,b) \;\big|\; 0 \leqslant a < A,\ 0 \leqslant b < B,\ S_{a,b} > 0\big\}.$$

(Note that $|I| \leqslant M$, since the sets $X_a \cap Y_b$ are pairwise disjoint for $a < A$, $b < B$). We assume that I is equipped with a linear order denoted by $\preceq$. (How $\preceq$ is exactly defined is of no importance for the proof; one may take e.g. some lexicographical order).

For given $(a, b) \in I$, let

$$x_{a,b,s} = \psi(a, \mu_{a,b}, s) \qquad \text{for } 1 \leqslant s \leqslant S_{a,b}, \tag{6.26}$$

where $\mu_{a,b} \in \mathbb{N}$ is any element such that

$$0 \leqslant \mu_{a,b} < N, \tag{6.27a}$$

$$\mu_{a,b} \neq \mu_{a',b'} \qquad \text{for all } (a',b') \prec (a,b), \tag{6.27b}$$

and moreover, for every $1 \leqslant s \leqslant S_{a,b}$, we have

$$\begin{aligned} &\det VM_{\mathbf{c}}\big(\mathbf{u} \mid\mid (x_{a,b,s})\big) \neq 0 \quad \text{for all tracks} \quad \mathbf{u} = (x_{a_j,b_j,s_j})_{j=0}^{k-2} \quad \text{such that} \\ &\qquad (a_j, b_j) \prec (a, b) \quad \text{for} \quad 0 \leqslant j \leqslant k-2 \quad \text{and} \quad \{v_{a_j,b_j,s_j}\}_{j=0}^{k-2} \cup \{v_{a,b,s}\} \in \mathcal{A}. \end{aligned} \tag{6.27c}$$

In step 5, we will verify that choosing an appropriate $\mu_{a,b}$ is possible.

5. For sequence $\mathbf{u} = (u_j)_{j=0}^{k-2}$ considered in (6.27c), the condition $\det VM_{\mathbf{c}}\big(\mathbf{u} \mid\mid (x_{a,b,s})\big) \neq 0$ expressed there reduces by (6.23c) to the form

$$\left|\begin{array}{cccc|c} 1 & u_0^l & \dots & u_0^{(k-2)l} & u_0^m \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & u_{k-2}^l & \dots & u_{k-2}^{(k-2)l} & u_{k-2}^m \\ \hline 1 & \alpha^{al} & \dots & \alpha^{(k-2)al} & \psi(a,\mu_{a,b},s)^m \end{array}\right| \neq 0. \tag{6.28}$$

By performing Laplace expansion along the last column, we reduce it further to the form

$$C + V(\mathbf{u}^l) \cdot \psi(a, \mu_{a,b}, s)^m \neq 0, \tag{6.29}$$

where C is the sum of all resulting summands except for the last one. We observe that C does not depend on $\mu_{a,b}$ (though it may depend on $\mu_{a',b'}$ for $(a',b') \prec (a,b)$).

By the assumption of $\mathbf{u}$ stated in (6.27c), the set $\{v_{a_j,b_j,s_j}\}_{j=0}^{k-2}$ is sparse, whence a_j are all pairwise distinct by (6.20). By (6.26) and (6.24c), this means that $\mathbf{u}^l$ is a track. This implies $V(\mathbf{u}^l) \neq 0$, so (6.29) excludes exactly one value for $\psi(a, \mu_{a,b}, s)^m$, which means by (6.24b) that it excludes at most one value for $\mu_{a,b}$.

Now, note that the condition (6.28) does not depend on the order of elements in $\mathbf{u}$. Also, it does not depend on s, by virtue of (6.24b). Therefore, the total number of values for $\mu_{a,b}$ excluded by (6.27c) for given a, b and any $s, \mathbf{u}$ is at most the number of all $(k-1)$-element subsets of the set of values $x_{a',b',s'}$ chosen so far, which is at most $\binom{M-1}{k-1}$.

On the other hand, conditions (6.27a) and (6.27b) together allow at least $N - |I| \geqslant N - M$ values for $\mu_{a,b}$. Therefore, by (6.22a), there must be a value satisfying all the conditions (6.27).

We have now verified that the map φ between Γ and Γ' has been correctly defined by (6.25), (6.26) and (6.27). In the rest of the proof, we check that it is an embedding of access structures.

6. The injectivity of φ follows immediately from its definition and (6.24a); it remains to verify that φ is a homomorphism between Γ and Γ'. For this, it suffices to compare the bases of these structures; that is, to show that a set $C \subseteq V(G)$ belongs to $\mathcal{B}_\Gamma$ if and only if $\varphi(C)$ belongs to $\mathcal{B}_{\Gamma'}$.

Now, we observe that both $\mathcal{B}_\Gamma$ and $\mathcal{B}_{\Gamma'}$ contain only sets of size 2 or k: for Γ, this holds by definition; for Γ', we use Lemma 4.6b and the fact that φ takes non-zero values. These two kinds of minimal authorized sets will be considered in the two subsequent steps.

7. For every two distinct $v_{a,b,s}, v_{a',b',s'} \in V(G)$, we have

$$\begin{aligned} &\{v_{a,b,s}, v_{a',b',s'}\} \in \mathcal{A}_\Gamma \quad \Leftrightarrow \quad \{v_{a,b,s}, v_{a',b',s'}\} \in E(G) \quad \Leftrightarrow \\ &\overset{(6.21)}{\Longleftrightarrow} \quad a = a' \text{ and } b \neq b' \quad \overset{(6.24)}{\Longleftrightarrow} \quad \left(\tfrac{x_{a,b,s}}{x_{a',b',s'}}\right)^m \neq \left(\tfrac{x_{a,b,s}}{x_{a',b',s'}}\right)^l = 1 \quad \Leftrightarrow \\ &\overset{(*)}{\Longleftrightarrow} \quad \{x_{a,b,s}, x_{a',b',s'}\} \in \mathcal{A}'_\Gamma, \end{aligned} \tag{6.30}$$

where $(*)$ is an application of Lemma 4.6a.

8. Finally, let $X \subseteq V(G)$ be of size k, and let $\mathbf{t}$ be a track containing all elements of the image $\varphi(X) \subseteq \mathbb{F}_q \setminus \{0\}$. Then, we have a sequence of implications

$$X \in \mathcal{B}_\Gamma \quad \Rightarrow \quad X \in \mathcal{A} \quad \Rightarrow \quad V_{\mathbf{c}}(\mathbf{t}) \neq 0 \quad \Rightarrow \quad \varphi(X) \in \mathcal{A}_{\Gamma'}$$

following respectively from the definition of Γ, from (6.27c), and from Lemma 4.6b. Then, $\varphi(X)$ must be minimal Γ'-authorized, since it cannot contain a Γ'-authorized set of size 2 by the assumption that $X \in \mathcal{B}_\Gamma$ and by step 7.

For the opposite implication, we first note that (6.30) implies in particular that

$$\{v_{a,b,s}, v_{a',b',s'}\} \in E(G) \quad \Leftrightarrow \quad \left(\tfrac{\varphi(v_{a,b,s})}{\varphi(v_{a',b',s'})}\right)^m \neq \left(\tfrac{\varphi(v_{a,b,s})}{\varphi(v_{a',b',s'})}\right)^l = 1 \qquad \text{for } v_{a,b,s} \neq v_{a',b',s'} \in V(G),$$

which, by comparing with (6.18), shows that φ is an isomorphism between G and the graph $G_{\Gamma'}$ coming from Lemma 6.17. Now, if $\varphi(X) \in \mathcal{B}_{\Gamma'}$ has size k, then Lemma 6.17c ensures that $\varphi(X)$ is sparse in $G_{\Gamma'}$; since φ is an isomorphism, it follows that X is sparse in G. By the definition of Γ, this means that $X \in \mathcal{A} \subseteq \mathcal{B}_\Gamma$. This finishes the proof. □

Bibliography

[1] A. Arnold, M. Giesbrecht, and D. S. Roche. Sparse interpolation over finite fields via low-order roots of unity. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, pages 27–34, New York, NY, USA, 2014. ACM.

[2] C. Asmuth and J. Bloom. A modular approach to key safeguarding. *IEEE Transactions on Information Theory*, 29(2):208–210, 1983.

[3] A. Beimel. Secret-sharing schemes: A survey. In YeowMeng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology*, volume 6639 of *Lecture Notes in Computer Science*, pages 11–46. Springer Berlin Heidelberg, 2011.

[4] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *Proceedings on Advances in Cryptology*, CRYPTO '88, pages 27–35, New York, NY, USA, 1990. Springer-Verlag New York, Inc.

[5] G. R. Blakley. Safeguarding cryptographic keys. *International Workshop on Managing Requirements Knowledge*, pages 313–317, 1979.

[6] E. F. Brickell. Some ideal secret sharing schemes. In Jean-Jacques Quisquater and Joos Vandewalle, editors, *Advances in Cryptology — EUROCRYPT '89*, volume 434 of *Lecture Notes in Computer Science*, pages 468–475. Springer Berlin Heidelberg, 1990.

[7] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *Journal of Cryptology*, 4(2):123–134, 1991.

[8] E. F. Brickell and D. R. Stinson. The detection of cheaters in threshold schemes. *SIAM Journal on Discrete Mathematics*, 4(4):502–510, 1991.

[9] M. Carpentieri. Some democratic secret sharing schemes. *Discrete Applied Mathematics*, 59(3):293 – 298, 1995.

[10] L. Comtet. *Advanced Combinatorics: The Art of Finite and Infinite Expansions*. Springer Netherlands, 1974.

[11] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms*. The MIT Press, 3rd edition, 2009.

[12] P. Damaschke. Fixed-parameter enumerability of cluster editing and related problems. *Theory of Computing Systems*, 46(2):261–283, 2010.

[13] P. Dusart. Estimates of some functions over primes without R.H. arXiv ePrint. http://arxiv.org/abs/1002.0442v1.

[14] R. Dvornicich and U. Zannier. Newton functions generating symmetric fields and irreducibility of schur polynomials. *Advances in Mathematics*, 222(6):1982 – 2003, 2009.

[15] M. E. A. El-Mikkawy. Explicit inverse of a generalized Vandermonde matrix. *Applied Mathematics and Computation*, 146(2–3):643 – 651, 2003.

[16] O. Farràs, T. Hansen, T. Kaced, and C. Padró. On the information ratio of non-perfect secret sharing schemes. Cryptology ePrint Archive, Report 2014/124, 2014. https://eprint.iacr.org/2014/124.pdf.

[17] W. Fulton. *Young tableaux : with applications to representation theory and geometry.* London Mathematical Society student texts. Cambridge University Press, Cambridge, New York, 1997. Autres tirages : 1999.

[18] W. Fulton and J. Harris. *Representation Theory: A First Course.* Graduate Texts in Mathematics. Springer-Verlag, 1991.

[19] Sh. Gao. Absolute irreducibility of polynomials via Newton polytopes. *Journal of Algebra*, 237(2):501 – 520, 2001.

[20] N. H. Guersenzvaig. Elementary criteria for irreducibility of $f(x^n)$. arXiv ePrint. http://arxiv.org/abs/1303.5333v2.

[21] R. Guy. *Unsolved Problems in Number Theory.* Problem Books in Mathematics. Springer New York, 2004.

[22] G. H. Hardy. *Ramanujan: twelve lectures on subjects suggested by his life and work.* Cambridge University Press, 1940.

[23] C. Herrmann. *On forbidden minors for matroids representable in finite characteristic.* Preprint. Technische Hochschule, Fachbereich Mathematik, 1992.

[24] W. V. D. Hodge and D. Pedoe. *Methods of Algebraic Geometry*, volume 2. Cambridge University Press, 1994. Cambridge Books Online.

[25] J. E. Humphreys. *Introduction to Lie Algebras and Representation Theory.* Springer-Verlag, New York, 1972.

[26] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. *Electronics and Communication in Japan (Part III)*, 72(9):56–64, 1989.

[27] N. Kogan and T. Tassa. Improved efficiency for revocation schemes via Newton interpolation. *ACM Transactions on Information and System Security*, 9(4):461–486, 2006.

[28] C.-P. Lai and C. Ding. Several generalizations of Shamir's secret sharing scheme. *International Journal of Foundations of Computer Science*, 15(2):445–458, 2004.

[29] S. Lang. *Algebra.* Graduate Texts in Mathematics. Springer New York, 2002.

[30] S. Lang and A. Weil. Number of points of varieties in finite fields. *American Journal of Mathematics*, 76(4):pp. 819–827, 1954.

[31] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1997.

[32] I. G. Macdonald. *Symmetric Functions and Hall Polynomials*. Oxford mathematical monographs. Clarendon Press, 1998.

[33] K. M. Martin. *Discrete structures in the theory of secret sharing*. PhD thesis, University of London, 1991.

[34] J. Martí-Farré, C. Padró, and L. Vázquez. On the diameter of matroid ports. *Electr. J. Comb.*, 15(1), 2008.

[35] A. B. Matos. Periodic sets of integers. *Theoretical Computer Science*, 127(2):287 – 312, 1994.

[36] M. Mignotte. How to share a secret. In *Proceedings of the 1982 Conference on Cryptography*, pages 371–375, Berlin, Heidelberg, 1983. Springer-Verlag.

[37] M. Monge. Generation of the symmetric field by Newton polynomials in prime characteristic. *Rocky Mountain Journal of Mathematics*, 42(2):729–749, 2012.

[38] T. Muir and W. H. Metzler. *A Treatise on the Theory of Determinants*. Dover Phoenix Editions. Dover Publications, 1933.

[39] J. G. Oxley. *Matroid Theory*. Oxford graduate texts in mathematics. Oxford University Press, 2006.

[40] C. Padró, G. Sáez, and J. L. Villar. Detection of cheaters in vector space secret sharing schemes. *Designs, Codes and Cryptography*, 16(1):75–85, 1999.

[41] V. V. Prasolov. *Polynomials*. Springer Berlin Heidelberg, 2009.

[42] C. S. Rajan. On the irreducibility of irreducible characters of simple Lie algebras. *Transactions of the American Mathematical Society*, 366(12):6443–6481, 2014.

[43] A. Schinzel. *Polynomials with Special Regard to Reducibility*. Cambridge University Press, 2000. Cambridge Books Online.

[44] A. Schinzel. On reducible trinomials, III. *Periodica Mathematica Hungarica*, 43(1-2):43–69, 2002.

[45] A. Schinzel, S. Spież, and J. Urbanowicz. Admissible tracks in Shamir's scheme. *Finite Fields and Their Applications*, 16(6):449–462, 2010.

[46] W. M. Schmidt. A lower bound for the number of solutions of equations over finite fields. *Journal of Number Theory*, 6(6):448 – 480, 1974.

[47] W. M. Schmidt. *Equations Over Finite Fields: An Elementary Approach*. Springer Berlin Heidelberg, 1976.

[48] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.

[49] J. P. Serre. *A Course in Arithmetic*. Graduate Texts in Mathematics. Springer New York, 1996.

[50] P. D. Seymour. Recognizing graphic matroids. *Combinatorica*, 1(1):75–78, 1981.

[51] P. D. Seymour. On secret-sharing matroids. *Journal of Combinatorial Theory, Series B*, 56(1):69 – 73, 1992.

[52] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[53] J. Simonis and A. Ashikhmin. Almost affine codes. *Designs, Codes and Cryptography*, 14(2):179–197, 1998.

[54] S. Spież, M. Srebrny, and J. Urbanowicz. Remarks on the classical threshold secret sharing schemes. *Fundamenta Informaticae*, 114(3-4):345–357, 2012.

[55] S. Spież, A. Timofeev, and J. Urbanowicz. Non-admissible tracks in Shamir's scheme. *Finite Fields and Their Applications*, 17(4):329 – 342, 2011.

[56] S. Spież, J. Urbanowicz, and A. Zabłocki. On constructing privileged coalitions in Shamir's type scheme. *Finite Fields and Their Applications*, 19(1):73–85, 2013.

[57] D. R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, 2:357–390, 1992.

[58] D. R. Stinson. *Cryptography: Theory and Practice*. CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 1995.

[59] T. Tassa and J. L. Villar. On proper secrets, (t, k)-bases and linear codes. *Designs, Codes and Cryptography*, 52(2):129–154, 2009.

[60] M. Tompa and H. Woll. How to share a secret with cheaters. *Journal of Cryptology*, 1(3):133–138, 1989.

[61] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités scientifiques et industrielles. 1041. Hermann & Cie, 1948.

[62] E. W. Weisstein. *CRC Concise Encyclopedia of Mathematics, Second Edition*. CRC Press, 2002.

[63] D. J. A. Welsh. *Matroid Theory*. Dover books on mathematics. Dover Publications, 2010.

[64] H. Whitney. On the abstract properties of linear dependence. In Ira Gessel and Gian-Carlo Rota, editors, *Classic Papers in Combinatorics*, Modern Birkhäuser Classics, pages 63–87. Birkhäuser Boston, 1987.

[65] G. Whittle. Recent work in matroid representation theory. *Discrete Mathematics*, 302(1–3):285 – 296, 2005.

[66] R. J. Wilson. *Introduction to Graph Theory*. Longman, 1996.

[67] A. Zabłocki. Admissible tracks in Lai–Ding's secret sharing scheme. *Finite Fields and Their Applications*, 27:72 – 87, 2014.