.

On the cryptographic applications of Gröbner bases and Lattice Theory

University of Maria Curie-Sklodowska

Faculty of Mathematics, Physics and Computer Science

Lublin, 2-14 December 2012

Jaime Gutierrez
University of Cantabria
Santander

This course will give a general introduction to the Gröbner basis and Lattice Theory, and cover the main applications to both cryptography and cryptanalysis. The main goal of this course is to show interactions between Cryptology and Symbolic Computation; the two important tools are lattices and Gröbner bases.

- The most famous example of such an interaction is probably the so called Lenstra, Lenstra, and Lovász (LLL) lattice basis reduction algorithm, it was a key ingredient to solve a computer algebra problem (factoring polynomials over the rational numbers); since then, it was used in numerous attacks in cryptology. Informally speaking a lattice is a set of points in n-dimensional space with a periodic structure. Historically, lattices were investigated since the late 18th century by mathematicians such as Lagrange, Gauss, and later Minkowski. More recently, lattices have become an active topic of research in computer science. At the beginning lattice reduction techniques were were used in cryptography principally to prove cryptographic insecurity. We will cover several of these negative results in particular:

  - breaking of knapsack-based cryptosystems
  - breaking the linear congruential pseudorandom generator.
  - breaking the security of padded RSA

  The lectures will be primarily focused on the algorithmic aspects of the lattice theory, which lattice problem can be solved in polynomial time, and which problems seems to be intractable. And also, presenting applications to predicting pseudorandom number generators and integer factoring.

- The second important symbolic computation tool is the theory of Gröbner basis. A Gröbner basis is a set of multivariate polynomials that has desirable algorithmic properties. Every set of polynomials can be transformed into a Gröbner basis. This process generalizes three familiar techniques: Gaussian elimination for solving linear systems of equations, the Euclidean algorithm for computing the greatest common divisor of two univariate polynomials, and the Simplex Algorithm for linear programming. It is a powerful technique for solving problems in algebraic geometry that was introduced by Bruno Buchberger, who named them after his advisor Wolfgang Gröbner. Gröbner bases provide a uniform approach for solving problems that can be expressed in terms of systems of multivariate polynomial equations. It happens that many practical problems, can be transformed into sets of polynomials, thus solved using Gröbner bases method. For instance, in cryptology the ciphers are rewritten to systems of multivariate equations that are solved for variables representing, for example, key bits. Algebraic attacks apply to a variety of ciphers, ranging from

  - blockciphers, like AES and Serpent,
  - streamciphers, like Toyocrypt and Bluetoot,
  - Asymmetric cryptosystems, like Hidden Field Equation (HHE),
  - hash functions, like multivariate polynomial for hashing.

  The course will give a short theoretical and algorithmic background on Gröbner bases, including the Buchberger's algorithm for computing a such basis, and then shows several applications to cryptology, including the asymmetric cryptographic primitives based on multivariate polynomials over finite fields. Those schemes are often considered to be good candidates for post-quantum cryptography, once quantum computers can break the current schemes.

On the cryptographic applications of Gröbner bases and Lattice Theory

University of Maria Curie-Sklodowska.
Faculty of Mathematics, Physics and Computer Science.
Lublin, 2-14 December 2012

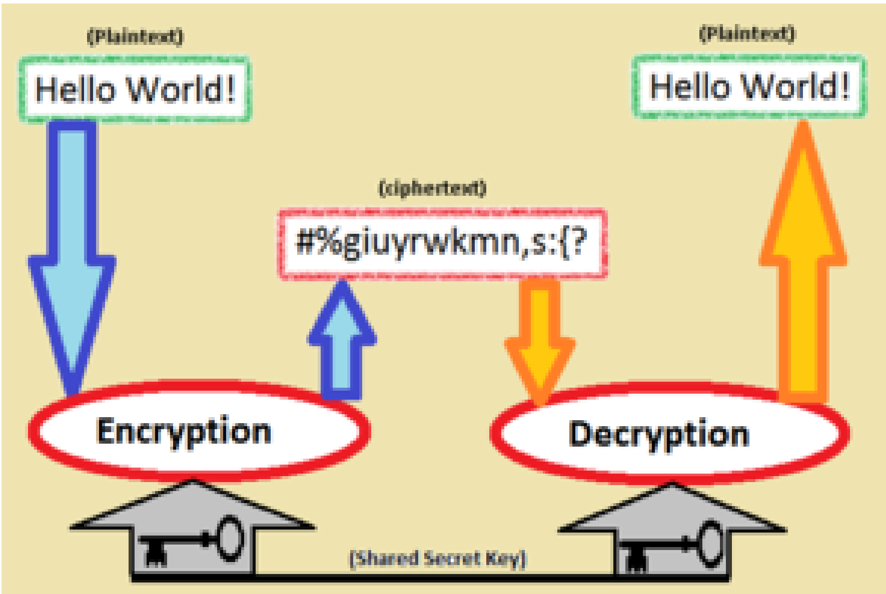
Jaime Gutierrez (University of Cantabria)

- GRÖBNER BASES:
  - Affine varieties and ideals
  - Division algorithm
  - Buchberger's Algorithm. Extensions F4 and F5
  - Elimination theory: How to solve system of equations
  - Common cryptosystems and Algebraic cryptanalysis
  - AES (Advanced Encryption Standard)
  - HFE (Hidden Field Equations)
  - Stream Ciphers: Trivium, Bivium
- LATTICES:
  - Definitions
  - Minkowski theorem.
  - Computational problems: SVP, CVP
  - LLL Reduced Lattice Basis
  - Knapsack-based cryptosystems and Lattice-based cryptanalysis.
  - Small roots of integers polynomials:
    - Predicting pseudorandom number generators
    - Security of RSA with small decryption exponent

- Douglas Stinson, *Cryprography: theory and practice*. Chapman and Hall/CRC 2006.
- D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms: An introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer-Verlag, 1996.
- M. Grötschel, L. Lovász and A. Schrijver, *Geometric algorithms and combinatorial optimization*, Springer-Verlag, Berlin, 1993.
- Antoine Joux, *Algorithmic Cryptanalysis*. Chapman and Hall/CRC 2009.

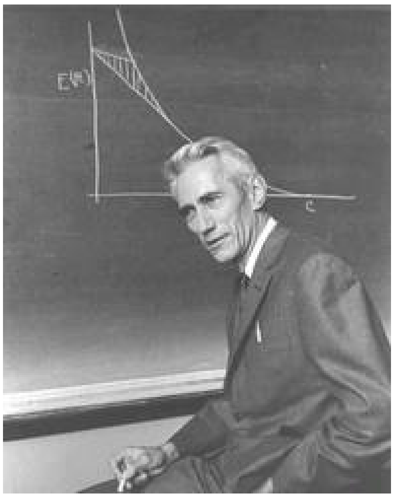
Sage: Open Source Mathematics Software

- Cryptography
  - Private Key
  - Public key
- Cryptanalysis



C.E. Shannon (1916 – 2001)

Communication Theory of Secrecy Systems, Bell System Technical Journal (1949).



"AS MUCH WORK AS SOLVING A SYSTEM OF SIMULTANEOUS EQUATIONS IN A LARGE NUMBER OF UNKNOWNS OF A COMPLEX TYPE."

Gröbner bases in public key cryptography

University of Maria Curie-Sklodowska.
Faculty of Mathematics, Physics and Computer Science.
Lublin, 2-14 December 2012

Jaime Gutierrez (University of Cantabria)

The public key is a set of polynomial equations over a finite field $\mathbb{K}$

$$\begin{cases} y_1 = f_1(x_1, \ldots, x_n), \\ y_2 = f_2(x_1, \ldots, x_n), \\ \quad\vdots \\ y_n = f_n(x_1, \ldots, x_n). \end{cases}$$

- **Encryption:** Evaluating the polynomials f_i in: plaintext $x = (x_1, \ldots, x_n) \in \mathbb{K}^n$, $\rightarrow$ ciphertext $y = (y_1, \ldots, y_n) \in \mathbb{K}^n$
- **Attacking:** Solving the system of equations.

Theorem

Deciding if an arbitrary system of multivariate, quadratic equations over a finite field is solvable is NP-complete.

- $\mathbb{K} = \mathbb{F}_q$ a finite field of characteristic a prime number p.
- HFE polynomial:

$$f(x) = \sum_{i,j} \beta_{i,j} x^{q^{\theta_{i,j}} + q^{\phi_{i,j}}} + \sum_{l} \alpha_l x^{q^{\epsilon_l}} + \mu \in \mathbb{F}_{q^n}[x]$$

  $\beta_{i,j}, \alpha_l, \mu \in \mathbb{F}_{q^n}$ and $\theta_{i,j}, \phi_{i,j}, \epsilon_l \in \mathbb{N}$
- For an irreducible polynomial $g(x) \in \mathbb{K}[x]$:

$$K[x]/ < g(x) > \quad \cong \quad \mathbb{F}_{q^n}$$

  The elements of $\mathbb{F}_{q^n}$ are represented as n-tuples over K.

  $f(x_1, \ldots, x_n) = (p'_1(x_1, \ldots, x_n), p'_2(x_1, \ldots, x_n \ldots, p'_n(x_1, \ldots, x_n))$

  $p'_i(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$ are quadratic polynomials.
- Two affine bijections s and t as vector spaces: $\mathbb{K}^n \to \mathbb{K}^n$.

$$t(f(s(x_1, \ldots, x_n))) = (p_1(x_1, \ldots, p_n(x_1, \ldots, x_n))$$

- **Public key:** $\mathbb{K}$, n and $p_i(x_1, \ldots, x_n)$.
- **Private key:** f, s, t and the representation of $\mathbb{F}_{q^n}$ over $\mathbb{K}$.

- **Encrypt:** Plaintext $x = (x_1, \ldots, x_n)$ compute the ciphertext $y = (y_1, \ldots, y_n)$:

$$y = p_1(x_1, \ldots, p_n(x_1, \ldots, x_n))$$

- **Decrypt:** Find all solutions to the equation

$$f(z) = t^{-1}(y)$$

and $x' = s^{-1}(z)$

Matsumoto-Imai (1988), J. Patarin, H (1996), N. Koblitz, 1997.

- Encryption and Decryption can be computed efficiently:
  - Public transformation: $O(n^5)$
  - Private: $O(n^4(n + \log n)$
- The inverse quadratic polynomial map may have a much higher degree.
- Algebraic Cryptanalysis

SK :

- Three affine bijections $r, s, t : \mathbb{K}^n \to \mathbb{K}^n$
- Two applications $\psi, \phi : \mathbb{K}^n \to \mathbb{K}^n$

PK : $h_1, \ldots, h_u, \ldots, h_n \in \mathbb{K}[x_1, \ldots, x_n]$ describing :

$$\mathbf{h} = \underbrace{t \circ \psi \circ s}_{\mathbf{f}} \circ \underbrace{\phi \circ r}_{\mathbf{g}}, \mathbb{K}^n \to \mathbb{K}^n.$$

$2R^-$ schemes : some polynomials of the PK are removed

Input : $\mathbf{h} = (h_1, \ldots, h_u) \in \mathbb{K}[x_1, \ldots, x_n]^u$.

Find :

- $\mathbf{f} = (f_1, \ldots, f_u) \neq h \in \mathbb{K}[x_1, \ldots, x_n]^u$, and
- $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbb{K}[x_1, \ldots, x_n]^n$,

such that :

$$\mathbf{h} = (\mathbf{f} \circ \mathbf{g}) = \big(f_1(g_1, \ldots, g_n), \ldots, f_u(g_1, \ldots, g_n)\big).$$

- J. von zur Gathen, J. Gutierrez, R. Rubio Multivariate Polynomial Decomposition. Applicable Algebra in Engineering, Communication and Computing, 2004.
- D.F. Ye, Z.D. Dai, K.Y. Lam. (u = n) Decomposing Attacks on Asymmetric Cryptography Based on Mapping Compositions. Journal of Cryptology, 2001.
- E. Biham. Cryptanalysis of Patarin's 2-Round Public Key System with S-Boxes (2R). CRYPTO 2000.
- J.C Faugère, L. Perret An Efficient Algorithm for Decomposing Multivariate Polynomials and its Applications to Cryptography. 2010.

Lattices in Algorithmic and Cryptography

Jaime Gutierrez

ALGORITHMIC MATHEMATICS AND CRYPTOGRAPHY

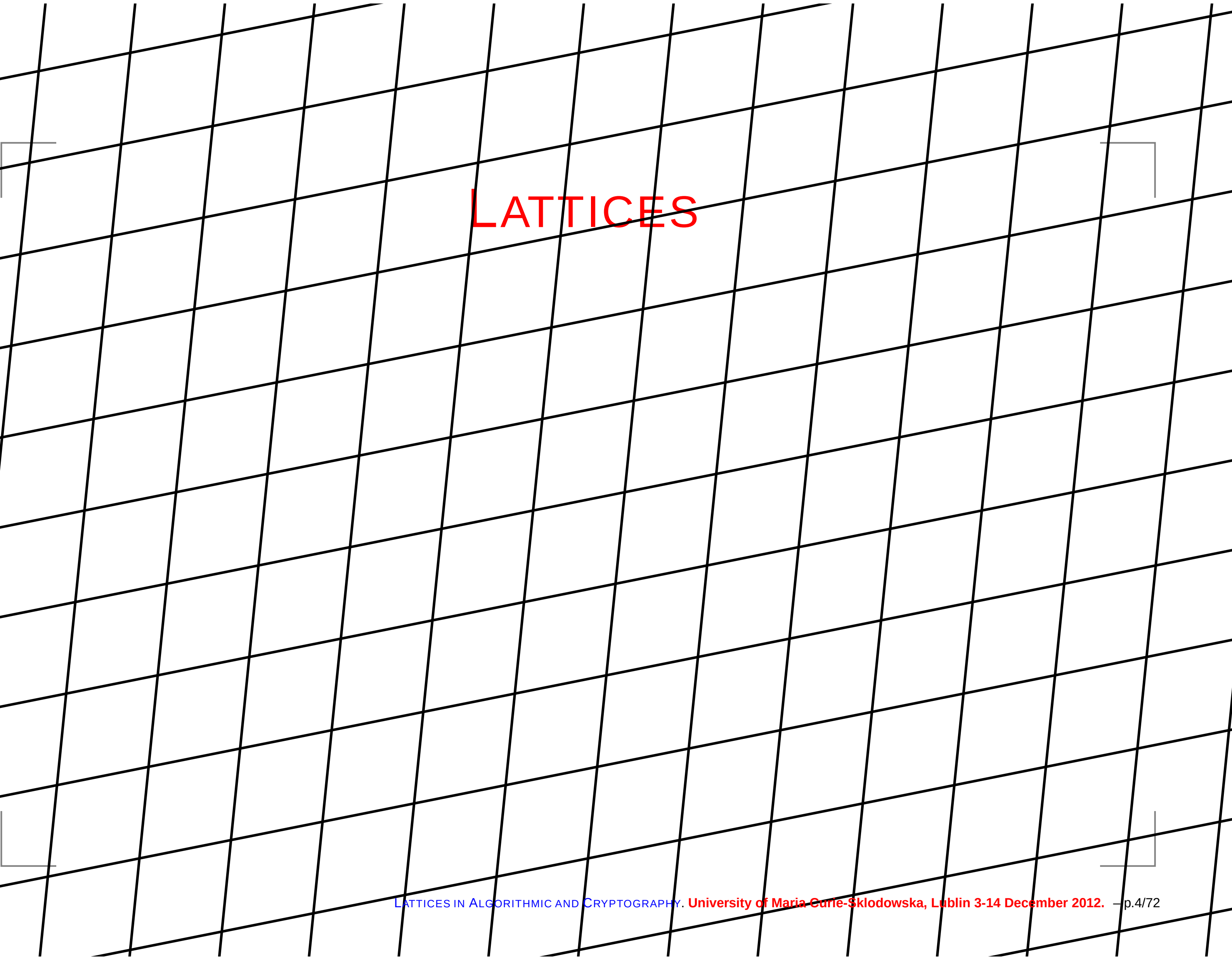
University of Cantabria

ORGANIZATION

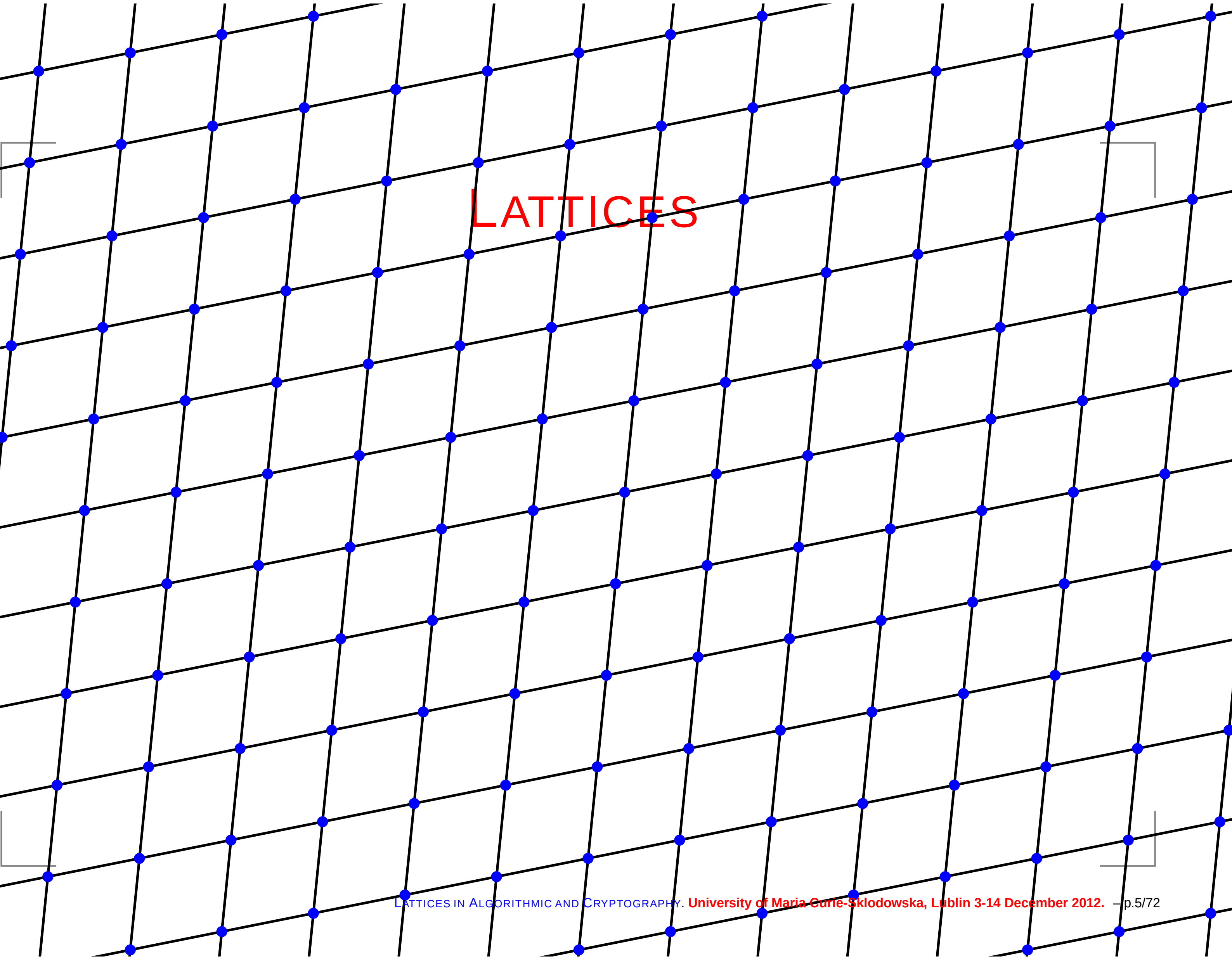
- Lattices.
- Cryptographic Knapsack Scheme
- RSA and integer factoring with extra information.
- Pseudorandom number generators over Elliptic curves.
- Ideal decomposition and intermediate subfields.
- Cayley graphs of cyclic groups.

LATTICES

LATTICES



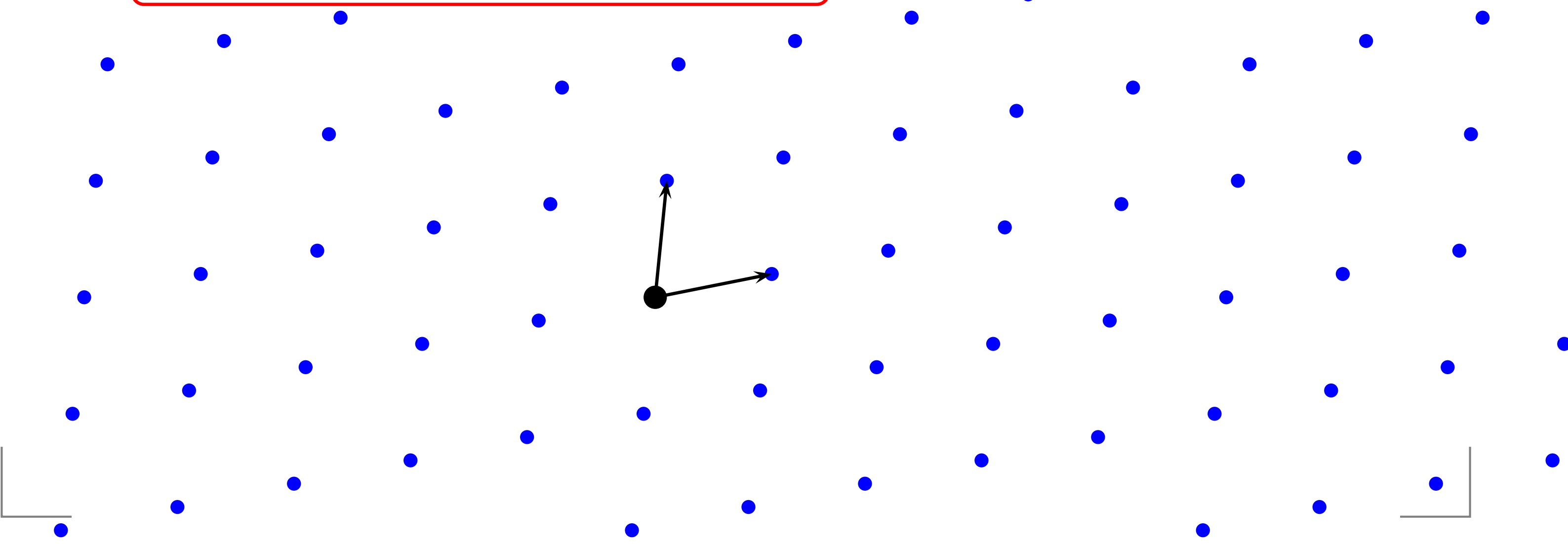
LATTICES



LATTICES

$$B = [\mathbf{b}_1|\cdots|\mathbf{b}_n], \text{ l.i.}$$

$$\mathcal{L}(B) := \{B\mathbf{x} \ / \ \mathbf{x} \in \mathbb{Z}^n\}$$



$$\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m, \text{ l.i.}$$

$$\mathcal{L} = \mathcal{L}([\mathbf{b}_1 | \cdots | \mathbf{b}_n]) =$$

$$= \left\{ \sum_{i=1}^{n} \lambda_i \mathbf{b}_i \;\middle|\; \lambda_i \in \mathbb{Z} \right\}.$$

$B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ is a **basis** of $\mathcal{L}$.

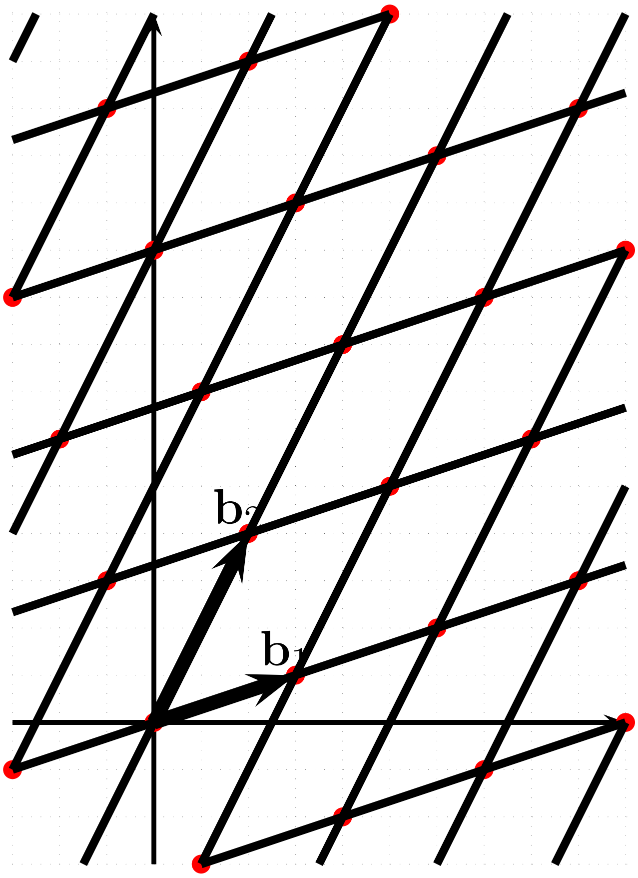
$$\mathcal{L}([(1,0),(0,1)] =$$

$$\mathcal{L}([(2006,1),(2007,1)]) = \mathbb{Z}^2$$

$$\mathcal{L}([(3,1),(2,4)]) =$$

$$\{(x,y) \in \mathbb{Z}^2 : 3x + y \equiv 0 \bmod 10\}$$

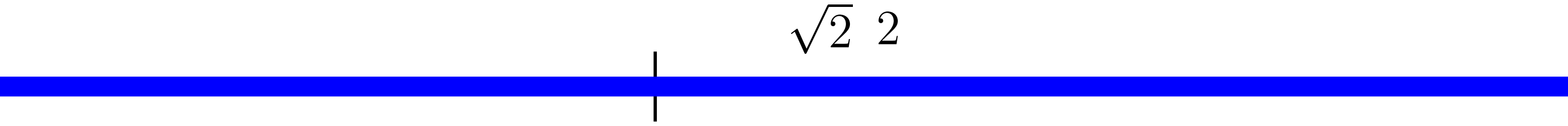
[LAGRANGE, GAUSS, MINSKOWSKI]



DISCRETE SUBGROUPS

In general, $\mathcal{L}(B)$ is not a lattice:

$$B := (2, \sqrt{2})$$



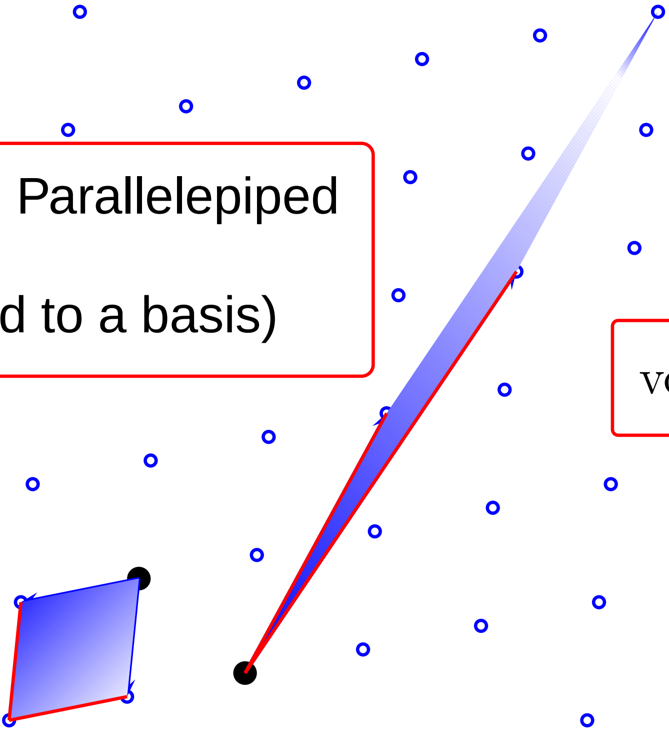
Lattices are **discrete** subgroups.

$$\lambda_1 := \min\{\|\mathbf{v}\| \ / \ \mathbf{v} \in \mathcal{L}\backslash\{0\}\}$$

The volume of a Lattice

Fundamental Parallelepiped

(associated to a basis)



$$\mathrm{vol}\,\mathcal{L} = \sqrt{|B^t B|}$$

Main bounds

- Norm ℓ_∞:

$$\lambda_1 \leq (\mathrm{vol}\,\mathcal{L})^{1/n}$$

- Norm ℓ_1:

$$\lambda_1 \leq (n!\,\mathrm{vol}\,\mathcal{L})^{1/n}$$

- Norm ℓ_2:

$$\lambda_1 \leq \sqrt{\gamma_n}(\mathrm{vol}\,\mathcal{L})^{1/n}$$

$$\frac{n}{2e\pi} + o(n) \leq \gamma_n \leq \frac{1'744}{e\pi} n + o(n)$$

Gauss Heuristic

MAIN PROBLEMS

- SVP

$$\min\{\|\mathbf{v}\| \ / \ \mathbf{v} \in \mathcal{L}\backslash\{0\}\}$$

NP hard ??

- CVP

$$\min\{\|\mathbf{v} - \mathbf{t}\| \ / \ \mathbf{v} \in \mathcal{L}\}$$

NP hard

Fixed n is polynomial: [KANNAN (1987)]

Approximation: [LLL = A. LENSTRA, H. LENSTRA, L. LOVÁCS (1982)], [T. BABAI (1986)], [M. AJTAI (1998)]

LLL-REDUCTION

$B = [\mathbf{b}_1|\cdots|\mathbf{b}_n]$ is a δ-LLL reduced basis of $\mathcal{L}$ if

- $|\mu_{i,j}| \leq 1/2$
- $\delta\|\mathbf{b}_i^*\| \geq \|\mu_{i+1,i}\mathbf{b}_i^* + \mathbf{b}_{i+1}^*\|$,

where $1/4 < \delta < 1$ y $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ is the Gram-Schmidt orthogonal basis : $\mathbf{b}_i^* := \mathbf{b}_i - \sum_{j<i} \mu_{ij}\mathbf{b}_j, \mu_{i,j} := \frac{<\mathbf{b}_i, \mathbf{b}_j^*>}{<\mathbf{b}_j^*, \mathbf{b}_j^*>}$.

$$\boxed{\|\mathbf{b}_1\| \leq \left(\frac{1}{\delta - 1/4}\right)^{\frac{n-1}{2}} \lambda_1}$$

LLL-algorithm is polynomial in $M = \max\{n, \log(\max_i \|\mathbf{b}_i\|)\}$.

Our lattices

$\mathcal{L}$ consist of integer solutions $\mathbf{x} = (x_0, \ldots, x_{s-1}) \in \mathbb{Z}^s$ of a system of congruences

$$\sum_{i=0}^{s-1} a_{ij} x_i \equiv 0 \bmod q_j, \qquad j = 1, \ldots, m,$$

modulo the intergers $q_1, \ldots, q_m$.

- Typically, $\mathrm{vol}(\mathcal{L}) = Q = q_1 \ldots q_m$.
- SVP and CVP are polynomials in $\log Q$.

CRYPTOGRAPHIC KNAPSACK SCHEME

The Knapsack Problem

- $(a_1, a_2, \ldots, a_n)$ a finite sequence of positive integers (the weights)
- Given a natural s compute, if it exists, $x_1, x_2, \ldots, x_n$, where $x_i\{0, 1\}$ such that

$$s = x_1a_1 + x_2a_2 + \cdots + x_na_n$$

NP-complete problem

SUPER-INCREASING SEQUENCES

The sequence $(a_1, a_2, \ldots, a_n)$ is super-increasing if satisfies:

$$a_i > a_1 + a_2 + \cdots + a_{i-1}$$

Example:

$$a_i := k^i$$

In this case it is simple

THE MERKLE-HELLMAN CRYPTOSYSTEM

- A $(b_1, b_2, \ldots, b_n)$ super-increasing sequence
- Two co-prime positive integers U and V such that

$$U > \sum_{i=1}^{n} b_i, \quad V < U.$$

- $a_i = b_i V \mod U.$

- PUBLIC KEY: $(a_1, a_2, \ldots, a_n)$
- PRIVATE KEY: $(b_1, b_2, \ldots, b_n), U, V)$

THE MERKLE-HELLMAN CRYPTOSYSTEM

- ENCRYPTION:
  The plaintext $x, 0 \leq x < 2^n$
  - $x = [x_1, \ldots, x_n]$ binary representation
  - The cipher text is $y = \sum_i^n x_i a_i$
- DECRYPTION.
  The ciphertext $y, 0 \leq y < 2^n$
  - Compute $s = yV^{-1} \mod U = \sum x_i b_i$
  - $x = \sum_{i=1}^n x_i 2^{i-1}$

The Merkle-Hellman Cryptosystem

- Several variations of this scheme.
- It is easy to implement.
- It is faster than RSA
- Broken by Shamir in 1982
- Chor-Rivest Scheme

LLL and Merkle-Hellman Cryptosystem

Given a knapsack problem with coefficients $(c_1, c_2, \ldots, c_n)$ and s. Let $\mathcal{L}$ be the lattice generated by A:

$$A = \begin{pmatrix} -a_1 & a_2 & \ldots & -a_n & s \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \cdots & \cdots & \ldots & \cdots & \cdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix} \in \mathbb{Z}^{(n+1)\times(n+1)},$$

If $x = (x_1, \ldots, x_n) : \sum_i^n x_i c_i = s \to$ vector $v \in \mathcal{L}$ is small:

$$v = (0, x_1, \ldots, x_n).$$

RSA and INTEGERS FACTORIZATION

THE PROBLEM

INPUT : $N = PQ$ and the high-order h bits of P.

THE PROBLEM

INPUT : $N = PQ$ and the high-order h bits of P.

OUTPUT: The factorization of N, i.e, P and Q.

WHY STUDY THIS PROBLEM ?

WHY TO STUDY THIS PROBLEM ?

- because I like it,

WHY TO STUDY THIS PROBLEM ?

- because I like it,
- RSA
  - loss of the equipment that generated P and Q,
  - explicit release of partial extra information as part of a protocol, for instance exchange of secret,
  - timing measurements,
  - routine usage of P and Q to decrypt mail, sign messages, etc.,
  - poor physical security to guard P and Q,
  - any other heuristic attack . . .

[RIVEST AND SHAMIR (1986)], [COPPERSMITH (1995-1998)], [BONEH AND HOWGRAVE-GRAHAM (1999)], [MAY AND CORON (2005)]

FORMALIZATION AND NOTATION

DEFINITION. *We say that an integer w is a Δ-approximation to the integer u when $|w-u| \leq \Delta$.*
We can build a Δ-approximation P_0 to P, by taking the h high-order bits of P and $\lfloor \log P \rfloor + 1 - h$ zeroes. In this case, $\Delta = 2^{\lfloor \log P \rfloor + 1 - h} - 1$, that is,

$$P - P_0 \leq \Delta \cong \frac{P}{2^h}.$$

By dividing N into P_0, we obtain a Δ_1-approximation Q_0 to Q:

$$|Q - Q_0| \leq \Delta_1 \cong \frac{Q\Delta}{P}.$$

FORMALIZATION AND NOTATION

Let $\varepsilon_0 = P - P_0$ and $\varepsilon_1 = Q - Q_0$. From $N = PQ$ we obtain:

$$f(\varepsilon_0, \varepsilon_1) = 0,$$

where

$$f(\varepsilon_0, \varepsilon_1) = (P_0 + \varepsilon_0)(Q_0 + \varepsilon_1) - N.$$

And with

$$|\varepsilon_0| \leq \Delta, \quad |\varepsilon_1| \leq \Delta_1.$$

The main objective is to find small roots of this innocent polynomial $f(\varepsilon_0, \varepsilon_1)$.

THE COPPERSMITH'S RESULT

THEOREM. [D. COPPERSMITH (1997)]
Let $p(\varepsilon_0, \varepsilon_1)$ *be an irreducible polynomial in two variables over* $\mathbb{Z}$*, of maximum degree* δ *in each variable separately. Let* Δ, Δ_1 *be bounds on the desired solutions* x_0, y_0*. Define* $p^*(\varepsilon_0, \varepsilon_1) = p(\varepsilon_0 \Delta, \varepsilon_1 \Delta_1)$ *and let W be the absolute value of the largest coefficient of* $p^*(\varepsilon_0, \varepsilon_1)$*. If*

$$\Delta\Delta_1 \leq W^{2/(3\delta)-\epsilon} 2^{-14\delta/3},$$

then in polynomial time in $(\log W, \delta, 1/\epsilon)$ *we can find all integer pairs* (x_0, y_0) *with* $p(x_0, y_0) = 0$ *bounded by* $|x_0| \leq \Delta, |y_0| \leq \Delta_1$*.*

ADAPTING COPPERSMITH'S RESULT

We suppose that we know $N = PQ$ and the high-order $h = \frac{1}{4}\log_2 N$ bits of P. We apply the previous result to polynomial $f(\varepsilon_0, \varepsilon_1)$ and take:

$$|\varepsilon_0| < P_0 N^{-1/4} = \Delta,$$
$$|\varepsilon_1| < Q_0 N^{-1/4} = \Delta_1,$$
$$\delta = 1, \quad W = N^{3/4}.$$

Corollary. [D. COPPERSMITH (1997)]
In polynomial time we can find the factorization of $N = PQ$ if we know the high-order $(\frac{1}{4}\log_2 N)$ bits of P

TWO ITERATION TECHNIQUE

- $(P_0 + \varepsilon_0)(Q_0 + \varepsilon_1) = N,$
- $|\varepsilon_0| \le \Delta$, $|\varepsilon_1| \le \Delta_1$
-

$$\begin{aligned}(P_0Q_0 - N)\Delta_1\Delta + Q_0\Delta x_1 + P_0\Delta_1 x_2 + x_3 &= 0,\\ x_1 &\equiv 0 \mod \Delta,\\ x_2 &\equiv 0 \mod \Delta_1.\end{aligned}$$

Two iterations technique

- $\mathbf{e} = (\Delta_1\varepsilon_0, \Delta\varepsilon_1, \varepsilon_0\varepsilon_1)$.
- $\mathbf{f}$ solution of the CVP. Check if $\mathbf{e} = \mathbf{f}$, otherwise:
- $\mathbf{u}, \mathbf{v}$ LLL reduced basis of lattice:

$$\begin{aligned} Q_0\Delta x_1 + P_0\Delta_1 x_2 + x_3 &= 0, \\ x_1 &\equiv 0 \mod \Delta, \\ x_2 &\equiv 0 \mod \Delta_1. \end{aligned}$$

- $$\begin{aligned} \mathbf{f} &= (\Delta_1 f_1, \Delta f_2, f_3), \\ \mathbf{u} &= (\Delta_1 u_1, \Delta u_2, u_3), \\ \mathbf{v} &= (\Delta_1 v_1, \Delta v_2, v_3), \end{aligned}$$

TWO ITERATIONS TECHNIQUE

$$\mathbf{e} = \mathbf{f} + \alpha\mathbf{u} + \beta\mathbf{v}$$

$$\Downarrow$$

$$\begin{aligned} \varepsilon_0 &= f_1 + \alpha u_1 + \beta v_1, \\ \varepsilon_1 &= f_2 + \alpha u_2 + \beta v_2, \\ \varepsilon_0\varepsilon_1 &= f_3 + \alpha u_3 + \beta v_3, \end{aligned}$$

$$\Downarrow$$

$$(f_1 + \alpha u_1 + \beta v_1)(f_2 + \alpha u_2 + \beta v_2) = f_3 + \alpha u_3 + \beta v_3$$

This is a new equation in α, β

TWO ITERATIONS RESULT

THEOREM. [D. GÓMEZ AND J. G. AND A. IBEAS (2006)]

For a prime P and natural numbers $\Delta,\ \Delta_1$, there is a set $\mathcal{V}(\Delta, \Delta_1) \subset \mathbb{Z}_P$ of cardinality

$$\#\mathcal{V}(\Delta, \Delta_1) = O\left(\frac{(\Delta^7 \Delta_1^4)}{P^3}\right)$$

with the following property. Given $N,\ P_0,\ Q_0,\ \Delta_1$ and Δ, where $N = PQ$, P_0 is a Δ-approximation of P and Q_0 a Δ_1-approximation of Q then if $Q \notin \mathcal{V}(\Delta, \Delta_1)$ there is an algorithm such that recover P and Q in polynomial time in the size of N.

PRACTICAL APPLICATION: TWO ITERATIONS

$P \equiv Q \equiv \sqrt{N}$, then $O\left(\frac{(\Delta^7 \Delta_1^4)}{P^3}\right) < P$ implies $3/10 \log N < h$

$$P, Q \equiv 2^{1000}$$

- This method requires :636 bits of P.
- The dimension of the lattice is 8.
- For the same known bits, Coppersmith method requires a lattice of dimension 199.

NUMERICAL RESULTS

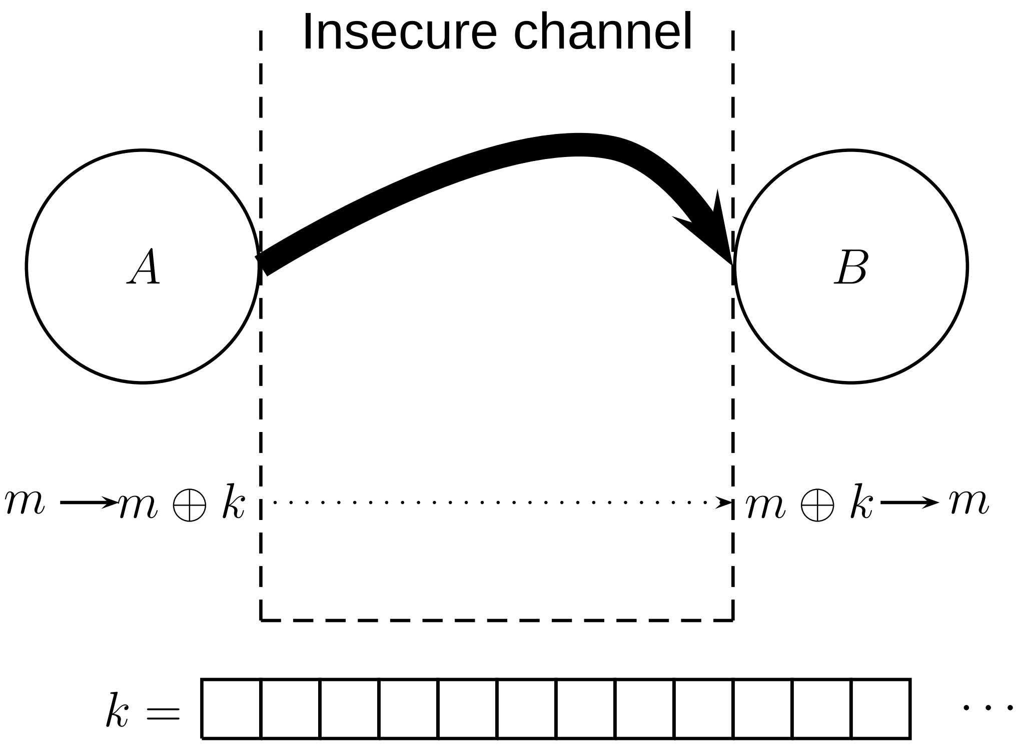
Bits of P	Bits of Q	Bits known	Iterations	Time
100	100	66	1	3.675 sec
100	100	60	2	10.271 sec
512	512	306	2	11.392 sec
512	512	300	3	14.025 sec
512	512	292	3	15.339 sec
1024	1024	624	2	7.240 sec
1024	1024	600	3	29. 357 sec
1024	1024	580	3	1 m. 35 sec

LINEAR GENERATOR

over

ELLIPTIC CURVES

STREAM CIPHERS

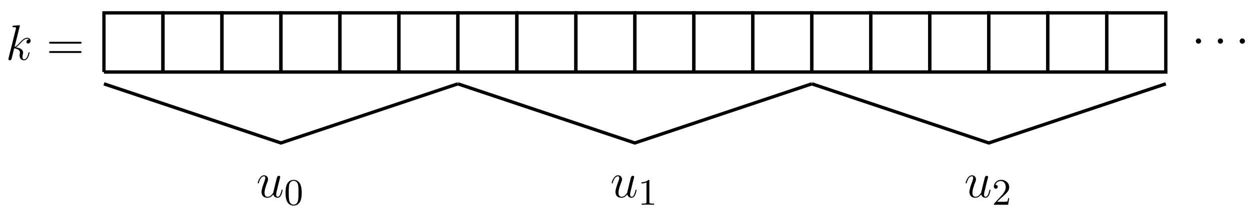


LINEAR CONGRUENTIAL GENERATOR

$$a \in \mathbb{F}_p^*, \quad c \in \mathbb{F}_p$$

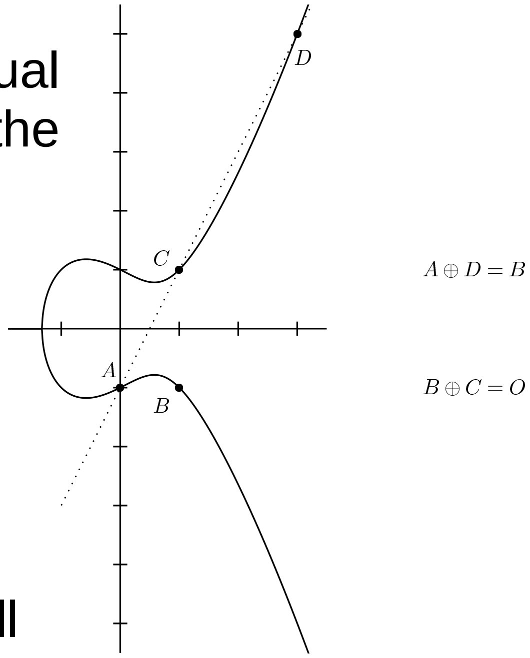
$$u_0 \in \mathbb{F}_p \text{ (seed)}$$

$$u_{n+1} \equiv_p a u_n + c$$



LINEAR GENERATOR ON ELLIPTIC CURVES

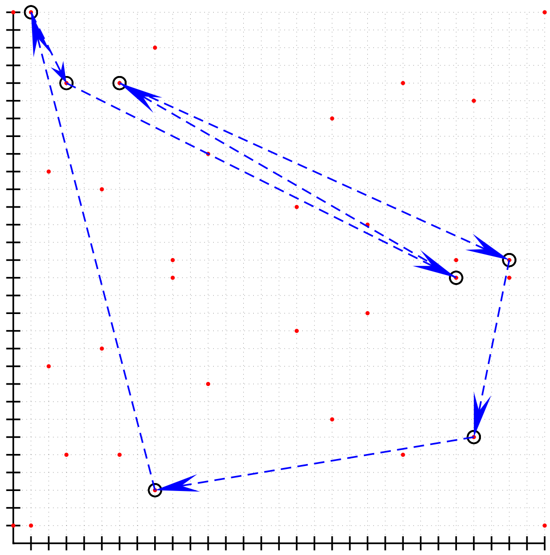
This generator employs the usual abelian group operation $(\oplus)$ on the set of points of an elliptic curve:



- A prime p.
- An elliptic curve $\mathbb{E} : Y^2 = X^3 + AX^2 + B$ over $\mathbb{F}_p$.
- The seed $U_0 \in \mathbb{E}$.
- The parameter $G \in \mathbb{E}$, which we call **composer**.

$$\boxed{U_{n+1} = U_n \oplus G, \forall n \geq 0.}$$

LINEAR GENERATOR ON ELLIPTIC CURVES



Toy example with a 7-periodic generator in an elliptic curve with 35 points over $\mathbb{F}_{31}$.

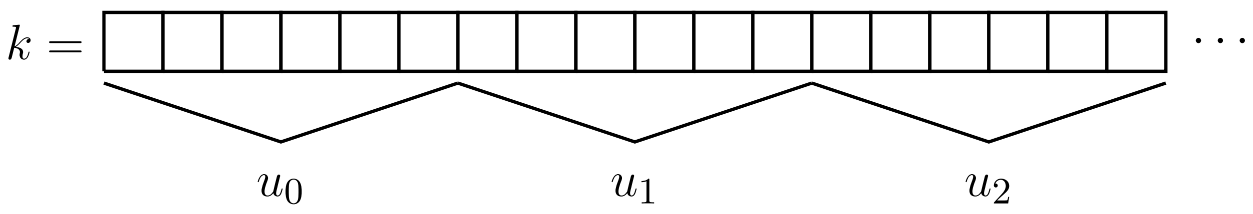
$$\mathbb{E} : Y^2 = X^3 - X^2 + 1$$

$$U_{n+1} = n(5, 11) \oplus (8, 3)$$

CRYPTOGRAPHICALLY SECURE GENERATOR

A **PRBG** *is cryptographically secure if there is no polynomial time algorithm which on input of the first l bits of an output sequence s can predict the $(l+1)^{st}$ bit of s with probability significant greater than $1/2$.*

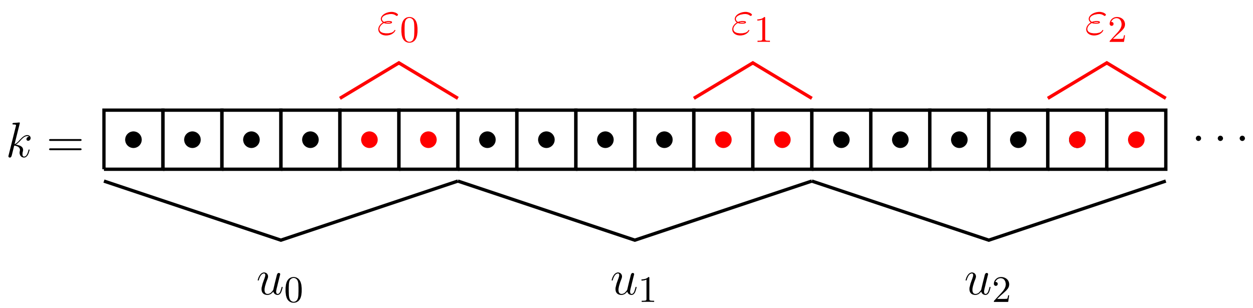
[YAO (1982)], [BLUM AND BLUM AND SHUB (1998)]



Cryptographically secure generator

A **PRBG** *is cryptographically secure if there is no polynomial time algorithm which on input of the first l bits of an output sequence s can predict the $(l+1)^{st}$ bit of s with probability significant greater than $1/2$.*

[Yao (1982)], [Blum and Blum and Shub (1998)]



[S. Blackburn and D. Gómez and J. G. and I. Shparlinski (2005)]

[D. Gómez and J. G. and A. Ibeas (2006)], [Knuth (1985)]

METHOD SKETCH

We assume access to:

- Approximations W_0, W_1 to the first two values U_0, U_1:
  - $U_i = (x_i, y_i), W_i = (\alpha_i, \beta_i)$,
  - $x_i = \alpha_i + e_i,\ y_i = \beta_i + f_i,\ |e_i|, |f_i| \le \Delta.$
- The composer $G = (x_G, y_G)$.

From $U_0 \oplus G = U_1$ when $U_0 \notin \{G, -G\}$, we obtain (over $\mathbb{F}_p$):

$$x_G^3 + x_1 x_G^2 - x_0 x_G^2 - 2x_1 x_G x_0 - x_G x_0^2 + x_0^3 + 2y_G y_0 + x_1 = 0,$$

$$y_1 x_G - y_1 x_0 - y_G x_0 + y_G x_1 - y_0 x_1 + y_0 x_G = 0.$$

METHOD SKETCH

- Translate previous equations into a linear system in the approximation errors e_0, e_1, f_0, f_1.
- Find the smaller integer solution to the system (CVP)
- Check if the obtained solution is valid.

THEOREM. [J. G. AND A. IBEAS (2007)]

If the algorithm outputs a wrong solution, the first coordinate x_0 of the first value must satisfy a certain equation. This leads to the bound $O(\Delta^6)$ for the possibilities for x_0 in a failure example. So, when $\Delta < p^{1/6}$ we can expect with high probability the success of the guessing algorithm.

UNKNOWN COMPOSER

We take three approximations $W_i = (\alpha_i, \beta_i)$ to any three values (consecutive or not): $U_i = (x_i, y_i)$

$$y_i^2 = x_i^3 + Ax_i + B, i = 0, 1, 2.$$

Eliminating the curve parameters A, B and assuming that $U_0 \notin \{U_1, -U_1\}$ (that is, $x_0 \neq x_1$), we obtain the following equation:

$$-y_2^2x_1+y_2^2x_0+x_2^3x_1-x_2^3x_0-x_2y_0^2+x_2x_0^3+x_2y_1^2-x_2x_1^3-y_1^2x_0+x_1^3x_0+x_1y_0^2-$$

Substituting $x_i = \alpha_i + e_i$, $y_i = \beta_i + f_i$ for $i = 0, 1, 2$, we obtain a threshold of $p^{1/46}$ for the tolerance below wich we can expect successful guessing.

SMALL ROOTS OF MODULAR POLYNOMIALS

THEOREM. [J. G. (2007)]

There exists an algorithm with the following properties. Let p be a prime number and Δ a positive integer such that $p > \Delta \geq 1$. Let $f(X,Y) = \sum_{i=0,j=0}^{m_1,m_2} a_{i,j} X^i Y^j \in \mathbb{F}_p[X,Y]$ be an irreducible polynomial of degree $m_1 \geq 2$ in X and degree $m_2 \geq 2$ in Y over $\mathbb{F}_p$. The algorithm, when given f and Δ-approximations w_0, w_1 to v_0, v_1 where $f(v_0, v_1) \equiv 0 \mod p$, recovers v_0, v_1 in time polynomial in m_1, m_2 and $\log q$ provided that v_0 does not lie in a certain set $\mathcal{V}(f) \subseteq \mathbb{F}_p$ of cardinality:

$$\mathcal{V}(f) = (2\sqrt{(m_1+1)(m_2+1)}\lambda_{(m_1+1)(m_2+1)})^{(m_1+1)(m_2+1)} \Delta^{\omega_{m_1,m_2}}$$

$$\omega_{m_1,m_2} = \frac{m_1^2}{2}(2m_2+1) + \frac{m_2^2}{2}(2m_1+1) + m_1 m_2.$$

IDEAL DECOMPOSITION

and

INTERMEDIATE FIELDS

THE PROBLEM

Given:

$f(x)$ *polynomial in* $\mathbb{Q}[x]$

Find:

$g(x), h(x), \bar{f}(x) \in \mathbb{Q}[x]$ *verifying*

$$f(x)\bar{f}(x) = g(h(x)),$$

$$1 < \deg g, \deg h < \deg f.$$

POLYNOMIAL DECOMPOSITION AND RATIONAL SUBFIELDS

If $\deg \bar{f} = 0$, then

$$f(x) = g(h(x)).$$

Lüroth's Theorem. [A. SCHINZEL (1982)]

Let $\mathbb{F}$ *be a field such that* $\mathbb{K} \subset \mathbb{F} \subset \mathbb{K}(x_1, \ldots, x_n)$ *and* $\mathrm{tr.deg.}(\mathbb{F}/\mathbb{K}) = 1$*. Then there exists* $h \in \mathbb{K}(x_1, \ldots, x_n)$ *such that* $\mathbb{F} = \mathbb{K}(h)$*. Also, if the field contains a polynomial, then a polynomial generator exists.*

$$\boxed{\begin{array}{ccc} \{[(g,h)] : f = g(h)\} & \longleftrightarrow & \{\mathbb{F} : \mathbb{K}(f) \subset \mathbb{F} \subset \mathbb{K}(x)\} \\ [(g,h)] & \longleftrightarrow & \mathbb{F} = \mathbb{K}(h). \end{array}}$$

[LANDAU-KOZEN-VON ZUR GATHEN (19889)], [GIESBRECHT (1990)], [J. G. AND R. RUBIO AND D. SEVILLA (98-2005)]

ALGEBRAIC SUBFIELDS

If $f(x)$ is irreducible and $f(\alpha)=0$, then the following statements are equivalent:

- f is an ideal decomposable.
- $Gal_{\mathbb{Q}}(f)$ acts imprimitively on the roots of f.
- A proper subfield, $\mathbb{Q}(\beta)$, exists with

$$\mathbb{Q} \subset \mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha).$$

$$\boxed{\begin{array}{ccc} \{[(\bar{f},g,h)] : f\bar{f} = g(h)\} & \longleftrightarrow & \{\mathbb{F} : \mathbb{Q} \subset \mathbb{F} \subset \mathbb{Q}(\alpha)\} \\ \big[(\bar{f},g,h)\big] & \longleftrightarrow & \mathbb{F} = \mathbb{Q}(h(\alpha)). \end{array}}$$

[S. LANDAU AND G. MILLER (1985)], [J. KLÜNERS AND M. POHST (1997)]
[J. G. AND D. SEVILLA (2006)]

THE ALGORITHM

We divide the problem into two parts:

1. Compute candidates polynomial $h(x)$.
2. Given $f(x)$ and $h(x)$, compute (if it exists) $\bar{f}(x), g(x)$:

$$f(x)\bar{f}(x) = g(h(x))$$

- Compute $\bar{f}(x), g(x)$ from $f(x)$ and $h(x)$ is solving a linear system of equations.
- The hard part is compute $h(x)$.

THE BASIC IDEA

From

$$f(x)\bar{f}(x) = g(h(x)),$$

There are two distintict roots of $f(x)$, say α_i and α_j for which

$$h(\alpha_i) = h(\alpha_j)$$

$h(x) = \sum_{k=1}^{s} h_k x^k \in \mathbb{Z}[x]$ for some s with: $1 < s < \deg f$

Find the coefficients $h_1, h_2, \ldots, h_s$ in $\mathbb{Z}$ satisfying

$$h_1(\alpha_i - \alpha_j) + h_2(\alpha_i^2 - \alpha_j^2) + \cdots + h_s(\alpha_i^s - \alpha_j^s).$$

INTEGER RELATIONS

A nonzero vector $\mathbf{h} = (h_1, \ldots, h_s) \in \mathbb{Z}^s$ is called an INTEGER RELATION for the real numbers $\gamma_1, \ldots, \gamma_s$ if

$$h_1\gamma_1 + \cdots + h_s\gamma_s = 0.$$

Given $\bar{\gamma}_1, \ldots, \bar{\gamma}_s$ complex numbers approximating to the algebraic numbers $\gamma_1, \ldots, \gamma_s$, and a parameter ϵ

- either finds an integer relation for $\gamma_1, \ldots, \gamma_s$ or
- proves that no relation of Euclidean length shorter than $1/\epsilon$ exists.

INTEGER RELATIONS AMONG ALGEBRAIC NUMBERS

$\mathcal{L}([\mathbf{b}_1|\cdots|\mathbf{b}_s]) \subset \mathbb{Q}^{s+2}$ the lattice spanned

$$\begin{cases} \mathbf{b}_1 = (1, 0, \ldots, 0, C \cdot Re(\bar{\gamma}_1), C \cdot Im(\bar{\gamma}_1)) \\ \quad \vdots \\ \mathbf{b}_s = (0, \ldots, 0, 1, C \cdot Re(\bar{\gamma}_s), C \cdot Im(\bar{\gamma}_s)) \end{cases}$$

C is a large integer depend on ϵ, the height of $(\gamma_1, \ldots, \gamma_s)$ and $[\mathbb{Q}(\gamma_1, \ldots, \gamma_s) : \mathbb{Q}]$.

- Let $\mathbf{b}$ be the first vector of the LLL-basis:
  $$\mathbf{b} = (m_1, \ldots, m_s, C \cdot \textstyle\sum_{i=1}^{s} m_i Re(\bar{\gamma}_i), C \cdot \sum_{i=1}^{s} m_i Im(\bar{\gamma}_i)).$$
- If $\|\mathbf{b}\| < 2^n/\epsilon^2$, then $(m_1, \ldots, m_s)$ is a solution. Otherwise, no solution shorter than $1/\epsilon$ exists.

[J. HÄSTAD AND B. JUST AND J. LAGARIAS AND C. SCHNORR (1989)]

Bounds on the coefficients of $h(x)$

Given a non-trivial ideal decomposition of polynomial $f \in \mathbb{Z}[x]$, i.e

$$f(x)\bar{f}(x) = g(h(x))$$

find an upper bound on the height $Ht(h(x))$ of $h(x)$.

- Polynomial Decomposition, i.e., $\bar{f}(x) = 1$, then
  $$Ht(h(x)) < CHt(f(x)).$$
- If $f(x)$ is irreducible: [J. Dixon (1990)], [J. McKay (1996)],
  $$Ht(h(x)) < CHt(f(x))^{\deg f},$$
  where C is a constant
- In general, ???

CAYLEY GRAPHS

of

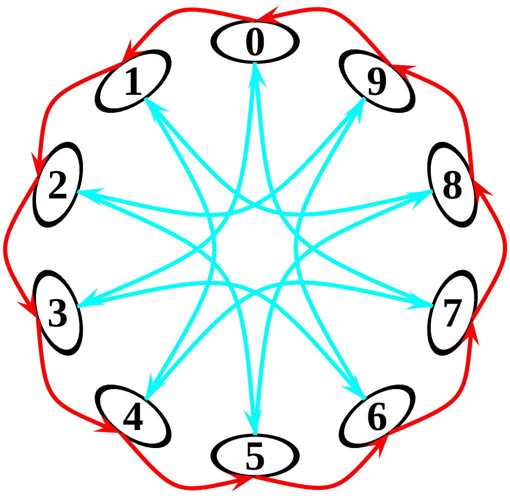
CYCLIC GROUPS

CIRCULANT DI-GRAPHS

- Vertices : $G = (\mathbb{Z}_N, +)$
- Edges - Set of jumps $H = \{j_1, \ldots, j_r\}$

$(x, x + j_i \bmod N),$

$x \in \mathbb{Z}_N,\ 1 \leq i \leq r$



$N = 10$

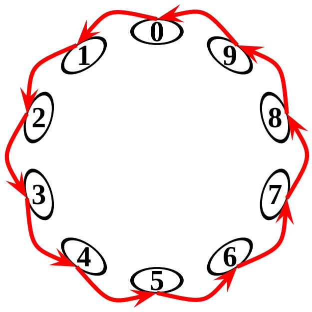
$H = \{1, 3\}$

Connected graph : $\gcd(j_1, \ldots, j_r, N) = 1$

ADJANCENCY MATRIX

Circulant Matrix :

$$R_N = \left(\begin{array}{ccc|c} & 0 & & 1 \\ \hline 1 & & & \\ & \ddots & & 0 \\ & & 1 & \end{array}\right)$$



$$\mathcal{C}_N(j_1, \ldots, j_r), \qquad \sum_{i=1}^{r} R_N^{j_i}$$

Undirected : $\mathcal{C}_N(\pm j_1, \ldots, \pm j_r)$

Distributed Loop Computer Networks

- Application to distributing an parallel computation.
- A extremely simple description.

$$O\left(r\log N\right)$$

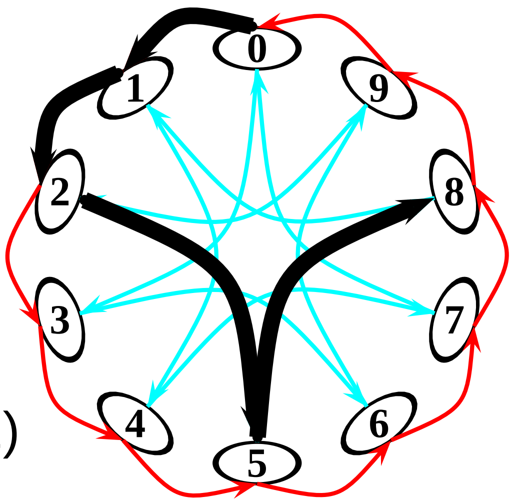
- small diameter.
- Routing algorithms and fault tolerance.
- The two jump case is widely studied.

[C. K. Wong and D. Coppersmith (1974)]

[J.C. Bermond and F. Comellas and D. F. Hsu (1995)]

PATHS IN A CIRCULANT

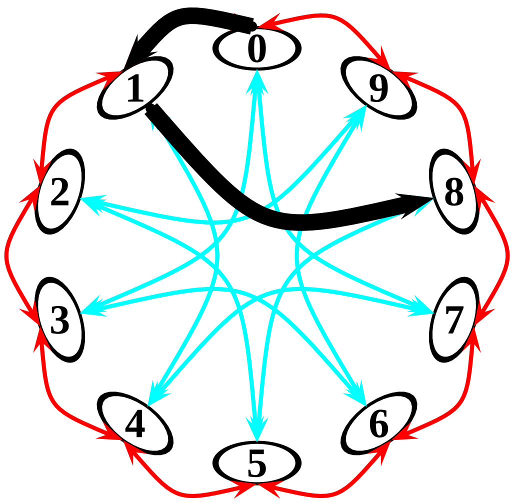
Directed



(2,2)

$$\mathbf{x} = (x_1, \ldots, x_r) \in \mathbb{N}^r$$

Undirected



(1,-1)

$$\mathbf{x} = (x_1, \ldots, x_r) \in \mathbb{Z}^r$$

THE LATTICE OF A CIRCULANT GRAPH

Given the jumps $j_1, \ldots, j_r$ and the number of nodes N:

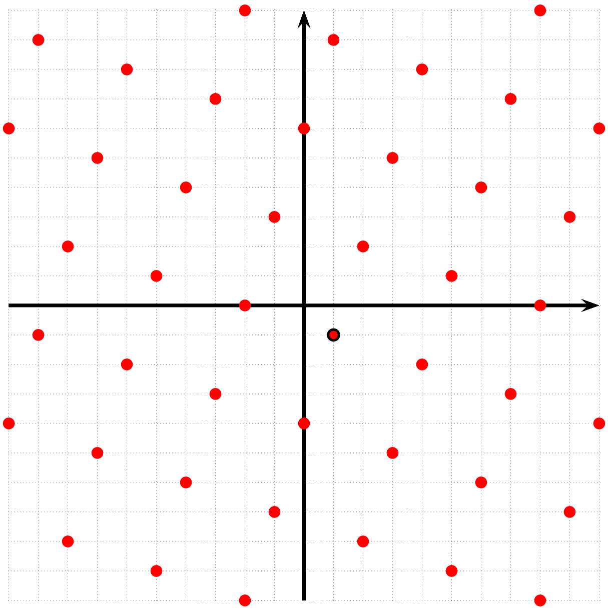
$$\mathcal{L}_{\mathcal{C}} = \{(x_1, \ldots, x_r) \in \mathbb{Z}^r : j_1 x_1 + \cdots + j_r x_r \equiv 0 \bmod N.\}$$

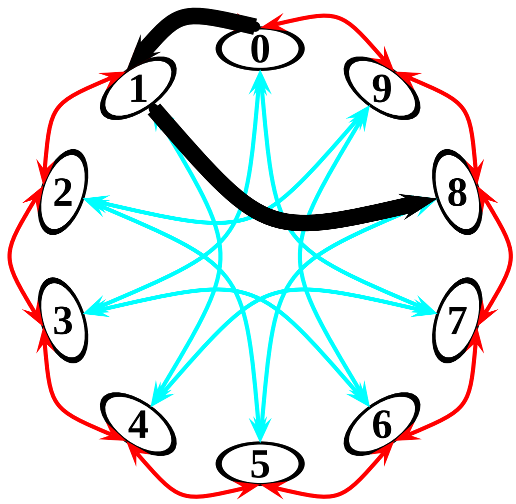
A shortest path from node α to node β:

- Undirected : $\mathbf{x} = (x_1, \ldots, x_r) \in \mathcal{L}_{\mathcal{C}}$ (with minimal $\|\mathbf{x}\|_1$).
- Directed: $\mathbf{x} = (x_1, \ldots, x_r) \in \mathcal{L}_{\mathcal{C}} \bigcap \mathbb{N}^r$ (with minimal $\|\mathbf{x}\|_1$)

$$\sum_{i=1}^{r} x_i j_i \equiv \alpha - \beta \bmod N.$$

SHORTEST PATH FOR TWO JUMPS





PATH DESCRIPTION

$$\mathcal{C}_N(a,b)$$

$$\mathbf{w} = (x_1, x_2) \;/\; ax_1 + bx_2 \equiv c \bmod N$$

$$\mathcal{L} := \{\mathbf{x} \in \mathbb{Z}^2 \;/\; ax_1 + bx_2 \equiv 0 \bmod N\}$$

$$\mathcal{CA}(c) = \mathbf{w} + \mathcal{L}$$

The total amount of jumps of the path $\mathbf{w}$ is $\|\mathbf{w}\|_1$.

THE COMPLEXITY

THEOREM. [D. GÓMEZ AND J. G. AND A. IBEAS (2005)]

- INPUT: a, b, N, c
- Description of the set of paths $\mathcal{CA}(c)$.
  $\mathbf{w} + \mathbb{Z} < \mathbf{u}, \mathbf{v} >$ $\mathcal{O}(\log N)$
- Recduction of the basis $\mathcal{L}$.
  $\mathbf{w} + \mathbb{Z} < \mathbf{u}, \mathbf{v} >$ $\mathcal{O}(\log N)$
- Iterative reduction.
  $\mathbf{w}'$ $\mathcal{O}(\log N)$
- Discrete searching.
  $\mathbf{w}''$ $\mathcal{O}(1)$

$$\mathcal{O}(\log^2 N \log\log N \log\log\log N))$$

THE POLYNOMIAL IDEAL OF A LATTICE

$$I_{\mathcal{L}} := (\quad \mathbf{x}^{\mathbf{a}^+} - \mathbf{x}^{\mathbf{a}^-} : \mathbf{a} \in \mathcal{L} \quad) \quad \subset \quad \mathbb{K}[X_1, \ldots, X_r].$$

$\mathbf{a} = \mathbf{a}^+ - \mathbf{a}^- = (a_1, \ldots, a_r) \in \mathbb{Z}^r$, $\mathbf{a}^+ = (a_1^+, \ldots, a_r^+)$,
$a_i^+ = \max\{a_i, 0\}$, $\mathbf{a}^- = (a_1^-, \ldots, a_r^-)$, $a_i^- = \max\{-a_i, 0\}$.

[B. STURMFELS AND R. WEISMANTEL AND G. M. ZIEGLER (1995)]

THEOREM. [J. G. AND A. IBEAS (2006)]

$$I_{\mathcal{L}_C} = (\quad x_1^N x_2^N \cdots x_r^N - 1, \quad \mathbf{x}^{\mathbf{a}^+} - \mathbf{x}^{\mathbf{a}^-}, (\mathbf{a} \in S) \quad),$$

$$\boxed{\begin{gathered} S = \{(N\alpha_1, \ldots, N\alpha_r), (\alpha_1 j_1 - 1, \alpha_2 j_2, \ldots, \alpha_r j_r), \\ (\alpha_1 j_1, \alpha_2 j_2 - 1, \ldots, \alpha_r j_r), \ldots, (\alpha_1 j_1, \ldots, \alpha_{r-1} j_{r-1} \alpha_r j_r - 1)\}. \\ \alpha_i \in \mathbb{Z}, (i = 1, \ldots, r), \quad 1 = \alpha_1 j_1 + \cdots + \alpha_r j_r + \beta N \end{gathered}}$$

GROEBNER BASES AND ROUTING

THEOREM. [J. G. AND A. IBEAS (2006)]

Fixed any grade monomial ordering $\prec$:
Let G be a Gröbner basis of $I_{\mathcal{L}_C}$ with respcet $\prec$ and $\mathbf{c}$ a path from 0 to $j \in \mathbb{Z}_N$.

The normal form of

$$\mathbf{x}^{\mathbf{c}} - 1$$

with respect G is

$$\mathbf{x}^{\mathbf{d}} - 1,$$

where $\mathbf{d}$ is a shortest path.

GROEBNER BASES

and

LLL-REDUCED BASES

GROEBNER BASIS VERSUS LLL-REDUCED BASIS

Definition Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$.
$G = \{g_1, \ldots, g_s\} \subset I$ is a Groebner Basis if and only if $\forall f \in I$

$f = \sum_{i=1}^{s} f_i g_i$ with $f_i \in \mathbb{K}[x_1, \ldots, x_n], g_i \in G$ and
$lm(f) \geq lm(f_i g_i)$

GROEBNER BASIS VERSUS LLL-REDUCED BASIS

Definition Let I be an ideal of $\mathbb{K}[x_1,\ldots,x_n]$.
$G=\{g_1,\ldots,g_s\}\subset I$ is a Groebner Basis if and only if $\forall f\in I$

$$\boxed{\begin{array}{c} f=\sum_{i=1}^{s} f_i g_i \text{ with } f_i\in\mathbb{K}[x_1,\ldots,x_n], g_i\in G \text{ and} \\ lm(f)\geq lm(f_i g_i)\end{array}}$$

Definition Let $\mathcal{L}$ be a lattice of $\mathbb{Z}^n$. $G=\{\mathbf{b}_1,\ldots,\mathbf{b}_s\}\subset\mathcal{L}$ is a G-Reduced Basis if and only if $\forall\mathbf{v}\in\mathcal{L}$

$$\boxed{\mathbf{x}=\sum_{i=1}^{s}\alpha_i\mathbf{b}_i \text{ with } \alpha_i\in\mathbb{Z}, b_i\in G \text{ and } \|\mathbf{x}\|\geq\|\alpha_i\mathbf{b}_i\|}$$

GROEBNER BASIS VERSUS LLL-REDUCED BASIS

Definition Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$.
$G = \{g_1, \ldots, g_s\} \subset I$ is a Groebner Basis if and only if $\forall f \in I$

$$\boxed{\begin{array}{c} f = \sum_{i=1}^{s} f_i g_i \text{ with } f_i \in \mathbb{K}[x_1, \ldots, x_n], g_i \in G \text{ and} \\ lm(f) \geq lm(f_i g_i) \end{array}}$$

Definition Let $\mathcal{L}$ be a lattice of $\mathbb{Z}^n$. $G = \{\mathbf{b}_1, \ldots, \mathbf{b}_s\} \subset \mathcal{L}$ is a G-Reduced Basis if and only if $\forall \mathbf{v} \in \mathcal{L}$

$$\boxed{\mathbf{x} = \sum_{i=1}^{s} \alpha_i \mathbf{b}_i \text{ with } \alpha_i \in \mathbb{Z}, b_i \in G \text{ and } \|\mathbf{x}\| \geq \|\alpha_i \mathbf{b}_i\|}$$

LLL-Reduced $\not\Rightarrow$ G-reduced

GROEBNER BASIS VERSUS LLL-REDUCED BASIS

THEOREM [D. GÓMEZ (2005)]
Let $\{\mathbf{b}_1, \ldots, \mathbf{b}_s\}$ *be a LLL reduced basis of a lattice* $\mathcal{L}$ *with repect to* δ*,* $1/4 < \delta < 1$*. Let* $\mathbf{x} \in \mathcal{L}$ *such that:*

$$\mathbf{x} = \alpha_1 \mathbf{b}_1 + \cdots + \alpha_s \mathbf{b}_s,$$

then we have the following inequality:

$$\|\alpha_i \mathbf{b}_i\| \leq 2^{3s} \|\mathbf{x}\|,$$

for all $i = 1, ..., s$*.*