Building Algebraic-Geometric Codes with Magma

Lancelot Pecquet
INRIA-Rocquencourt, Project CODES
Lancelot.Pecquet@inria.fr

joint work with

Paweł Wocjan
Universität Karlsruhe
Institut für Algorithmen und Kognitive Systeme
wocjan@ira.uka.de

Magma?

- What? Magma is a non-commercial computer algebra system.
- Who? Direction: Dr. John CANNON. Many contributors worldwide.
- When? Developed since 1993, successor of *Cayley* (1975).
- Purpose? Unified environment for algebra (group theory, linear algebra, rings, fields, number theory, modules, algebraic geometry, lattices, graphs, designs, coding theory, *etc.*)
- Why?
  - Simple (flexible and expressive language).
  - Clean (strong typing based on category theory and universal algebra).
  - Fast (state-of-the-art algorithms, optimization at machine level).

Sample of contributors

- Integer primality: Francois MORAIN (LIX, France).
- Integer factorization: Arjen LENSTRA (Bellcore, USA).
- Number Theory: *Pari* group (Henri COHEN, Bordeaux, France), *Kant* group (Michael POHST, Berlin, Germany), Wieb BOSMA (Nijmegen, Netherlands).
- Elliptic Curves: John CREMONA (Nottingham, UK).
- Modular Forms: David KOHEL (Sydney, Australia), William STEIN (Berkeley, USA).
- Function Fields: Florian HESS (Sydney, Australia).
- Coding Theory: Project CODES, INRIA (Le Chesnay, France).
- Permutation groups: Jeff LEON (UIC, USA).
- Invariant Theory: Gregor KEMPER (Heidelberg, Germany).

Sample algorithms

- Integer primality: Atkin-Morain Elliptic Curves Primality Proving (ECPP), Miller-Rabin.
- Integer factorization: Elliptic Curve Method (ECM), Multiple Polynomial Quadratic Sieve (MPQS).
- Gröbner bases: grevlex Gröbner basis + Gröbner walk.
- Integer rings of number fields: *Round 2*, *Round 4*.
- Rewrite groups: Knuth-Bendix Algorithm
- Lattices reduction: FP-LLL (Schnorr & Euchner), Exact Integral Algorithm (de Weger).
- Finite field factorization: Berlakamp, Shoup.
- Mordell-Weil rank: Cremona's mwrank.
- Decoding of alternant codes: Euclidean decoding, Sudan's algorithm.

Reliable communications and linear codes (SHANNON, HAMMING, ... , 1948)

Problem: Send a message $x = (x_1, \ldots, x_k) \in \mathbb{F}_q^k$ through a noisy channel in a way that allows to reconstruct x from the noisy data.

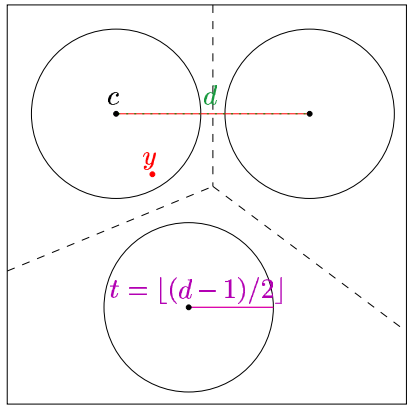
Idea: Embed the message space $\mathbb{F}_q^k$ into a linear code *i.e.* a k-dimensional vector subspace C of $\mathbb{F}_q^n$, equipped with the HAMMING metric:

$$\mathrm{d}(u, v) = \left|\left\{i \in \{1, \ldots, n\} \mid u_i \neq v_i\right\}\right| .$$

When a noisy message $y \in \mathbb{F}_q^n$ is received, the corresponding codeword will be the closest $c \in C$.

The minimum distance of C measures its correction capability:

$$\mathrm{d}(C) = \min_{\substack{c, c' \in C \\ c \neq c'}} \mathrm{d}(c, c') .$$



One says it is an $[n, k, d]_q$-code.

Representation of linear codes

It is characterized by a generator matrix

$$G = \begin{pmatrix} c_{1,1} & \cdots & c_{1,n} \\ \vdots & \ddots & \vdots \\ c_{k,1} & \cdots & c_{k,n} \end{pmatrix} \quad \text{where} \quad C = \langle c_1, \ldots, c_k \rangle \, .$$

Algebraic Geometric Codes (Goppa, 1975): informal description

Let X be a curve over $\mathbb{F}_q$, $p_1, \ldots, p_n$ be distinct points of X and $L = \langle f_1, \ldots, f_k \rangle$ be a vector space of functions such that for $1 \leq i \leq k$, $f_i(p_j) \in \mathbb{F}_q$, the corresponding Alebraic-Geometric code is:

$$C = \{(f(p_1), \ldots, f(p_n)) \ , \ f \in L\} \ .$$

A generator matric of C is:

$$G = \begin{pmatrix} f_1(p_1) & \cdots & f_1(p_n) \\ \vdots & \ddots & \vdots \\ f_k(p_1) & \cdots & f_k(p_n) \end{pmatrix} \ .$$

Ex (Reed-Solomon codes): Let X be the affine line $\mathbb{F}_q^1$, $p_1, \ldots, p_n$, be all nonzero elements of $\mathbb{F}_q$ and $L = \{f(x) \in \mathbb{F}_q[x] \mid \deg f < k\} = \langle 1, x, \cdots, x^{k-1} \rangle$, the associated Reed-Solomon code is

$$C = \{(f(p_1), \ldots, f(p_n)) \ , \ f \in L\} \ .$$

Goal of code builders: the GILBERT-VARSHAMOV bound (and beyond!)

We want families of $[n, k_n, d_n]_q$-codes such that

1. k_n/n is large: low cost.
2. d_n/n is large: high correction capability.

Th (GILBERT-VARSHAMOV bound, 1952) For any $\delta \in [0, (q-1)/q]$, there exists a sequence $(C_n)_{n\in\mathbb{N}}$ of $[n, k_n, d_n]_q$-codes such that

$$\limsup_{n\longrightarrow\infty} \frac{d_n}{n} \geq \delta \quad \text{and} \quad \limsup_{n\longrightarrow\infty} \frac{k_n}{n} \geq 1 - \mathrm{H}_q(\delta) \ ,$$

where H_q is the q-ary entropy function defined by $\mathrm{H}_q(0) = 0$ and for $0 < \delta < (q-1)/q$, by

$$\mathrm{H}_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta) \log_q(1-\delta) \ .$$

Random codes reach this bound but they are not deterministically constructible in polynomial time, nor decodable in polynomial time, unless P=NP.

How good Algebraic Geometric Codes can be?

Th (Drinfeld-Vlăduţ bound, 1993) For any geometically irreducible projective curve X over $\mathbb{F}_q$ with n rational points, and geometric genus g, $n/g \leq \sqrt{q} - 1$.

Th (Ihara/Tsfasman-Vlăduţ-Zink bound, 1981) If q is a square, there exists a sequence $(X_n)_{n\in\mathbb{N}}$ of geometrically irreducible projective curves over $\mathbb{F}_q$ with $n+1$ rational points and geometric genus g_n, asymptotically achieving the Drinfeld-Vlăduţ bound. Therefore for any $\delta \in [0, (q-1)/q]$, there exists a sequence $(C_n)_{n\in\mathbb{N}}$ of $[n, k_n, d_n]_q$-codes that can be built in deterministic polynomial time, and such that:

$$\limsup_{n\longrightarrow\infty} \frac{d_n}{n} \geq \delta \quad \text{and} \quad \limsup_{n\longrightarrow\infty} \frac{k_n}{n} \geq 1 - \frac{1}{\sqrt{q}-1} - \delta \ .$$

This exceeds the Gilbert-Varshamov bound for q square ≥ 49.

Garcia and Stichtenoth have given (1995) a simpler and equivalent (Elkies, 1997) construction.

Plane curves *vs.* space curves

Two geometrically irreducible curves X and Y over $\mathbb{F}_q$ are birationally equivalent iff the function fields $\mathrm{K}(X)$ and $\mathrm{K}(Y)$ are isomorphic $\mathbb{F}_q$-algebras.

Prop: Any geometrically irreducible curve over $\mathbb{F}_q$ is equivalent to a plane curve.

Prop: Any geometrically irreducible curve over $\mathbb{F}_q$ is equivalent its normalization X^{nor} (*i.e.* all local rings $\mathscr{O}_{X,p}$ are normal). Moreover, X^{nor} is nonsingular (*i.e.* all local rings $\mathscr{O}_{X,p}$ are regular and, as $\dim X = 1$, DVRs).

	Good	Bad
Space curves (nonsingular)	Easier theory, $\lvert X(\mathbb{F}_q)\rvert$ unbounded	GRÖBNER bases $\Longrightarrow$ exponentially bounded complexity
Plane curves (singular)	2 or 3 variables $\Longrightarrow$ polynomially bounded complexity	Harder theory, $\lvert X(\mathbb{F}_q)\rvert \leq \lvert \mathbb{P}^2(\mathbb{F}_q) = q^2+q+1\rvert$

Curves over non-algebraically closed fields

In real life, curves are over non-algebraically closed fields.

Given an affine point $p \in X$ of degree $d > 1$, we will "locally extend" X to $X \times_{\mathbb{F}_q} \mathbb{F}_{q^d}$ in order to represent p by a pair $(a, b) \in \mathbb{F}_{q^d}^2$, and allow translation $(a, b) \longrightarrow (0, 0)$. However we keep only one "distinguished" representative under Gal $\left(\mathbb{F}_{q^d}/\mathbb{F}_q\right)$.

There is no canonical "$\overline{\mathbb{F}_q}$" but Magma provides default finite fields with compatible embeddings using Conway polynomials. (D^5 pseudo-algebraic closure is currently being adapted for finite fields)

Rational points, singular points

Prop: If $X = \operatorname{Spec} \mathbb{F}_q[x,y]/\langle F(x,y)\rangle$ and $Y = \operatorname{Spec} \mathbb{F}_q[x,y]/\langle G(x,y)\rangle$ are affine reduced plane curves with $\gcd(F,G) = 1$. Let $R = \{a \in \overline{\mathbb{F}_q} \mid \exists b \in \overline{\mathbb{F}_q} \mid F(a,b) = G(a,b) = 0\}$, the projection $X \cap Y$ on the first coordinate. For any $a \in \overline{\mathbb{F}_q}$, if $\mathrm{lc}_y(F(x,y))$ and $\mathrm{lc}_y(G(x,y))$ do not both vanish at $x = a$.

$$a \in R \quad \Longleftrightarrow \quad \big(\operatorname{res}_y(F(x,y),G(x,y))\big)(a) = 0\,.$$

We therefore find the intersections $(a,b) \in X \cap Y$ by finding the roots a of $\operatorname{res}_y(F(x,y),G(x,y))$, then by finding the roots b of $\gcd(F(a,y),G(a,y))$.

Th (Jacobian criterion): If $X = \operatorname{Spec} \mathbb{F}_q[x,y]/\langle F(x,y)\rangle$ is an affine reduced plane curve the jacobian ideal

$$J = \langle \partial F/\partial x, \partial F/\partial y\rangle;,$$

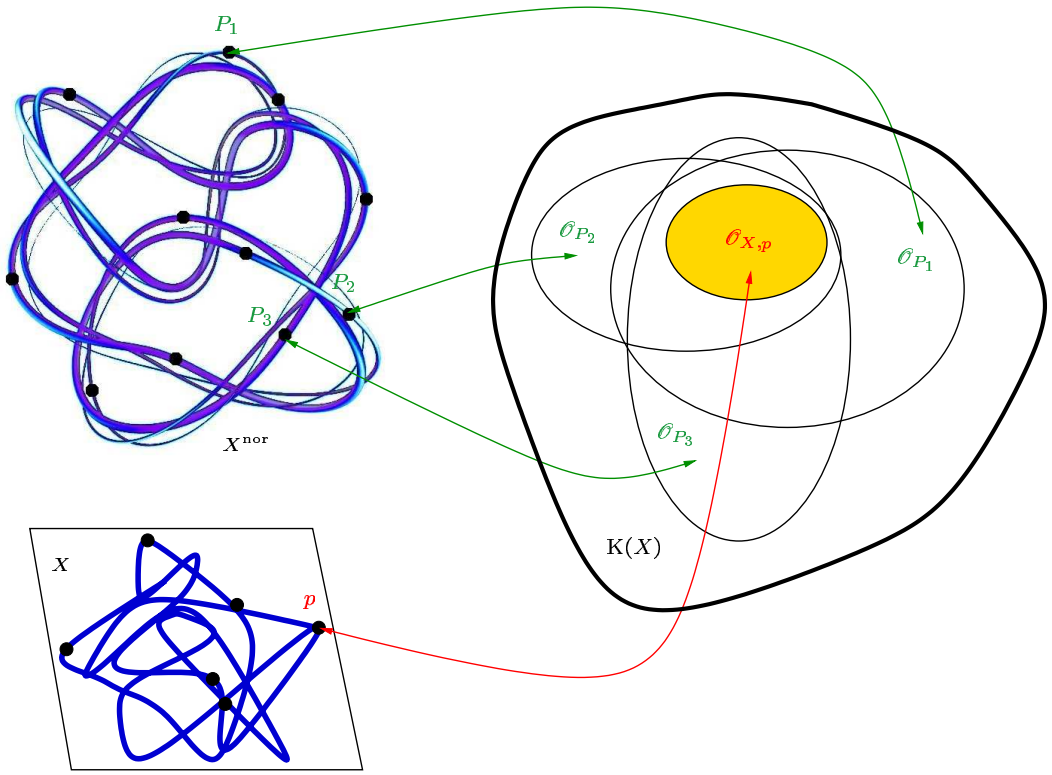
defines the singular locus $\operatorname{Sing}(X)$ of X. It is a finite closed set of X.

Places over points

For each point $p \in X$, the local ring $\mathscr{O}_{X,p}$ is included in finitely many DVRs $\mathscr{O}_P \subset \mathrm{K}(X)$.

The maximal ideal P of $\mathscr{O}_P$ is called a place of X over p (one denote $P|p$).

Places of X are in bijections with the points of X^{nor}.



Geometric normalization *via* adjoint divisors and geometric genus

If $f \in \mathrm{K}(X)$, we define the local divisor at $p \in X$:

$$(f)_p = \sum_{P|p} \mathrm{v}_P(f) \cdot P \ .$$

The local adjoint divisor at $p \in X$ is:

$$(\mathscr{O}_{X,p}^{\mathrm{nor}} : \mathscr{O}_{X,p}) = \{f \in \mathrm{K}(X) \mid (f)_p \geq \mathrm{adj}_p(X)\} \ ,$$

and the adjoint divisor is

$$\mathrm{adj}(X) = \sum_{p \in \mathrm{Sing}(X)} \mathrm{adj}_p(X) \ .$$

Th (Gorenstein, 1952) If X is a geometrically irreducible projective plane curve of degree d,

$$\mathrm{p_g}(X) = \mathrm{p_a}(X) - \frac{1}{2} \deg \mathrm{adj}(X) = \frac{1}{2}\big((d-1)(d-2) - \deg \mathrm{adj}(X)\big);.$$

Algorithmics of the desingularization using blowups

Let $k = \mathbb{F}_q$ and $X = \operatorname{Spec} k[x,y]/\langle F(x,y)\rangle$ be a geometrically irreducible affine plane curve and $p \in X$ a non-smooth point, using quadratic transforms and translations (extension fields required!), we build a sequence of curves $X_{p'_1}, \ldots, X_{p'_s}$, such that for all i,

1. $0 = p'_i \in X_{p'_i}$.
2. $X_{p'_i}$ is defined over some extension k_i of k.
3. $X_{p'_i}$ is birationally equivalent to $X \times_k k_i$.
4. The isomorphic image of $\mathscr{O}_{X_i,p'_i}$ contains $\mathscr{O}_{X,p}$.

Each p'_i is said to be infinitely close to p and one denote by $\operatorname{Icp}(p)$ the set of such points.
The process is recursively repeated on the $X_{p'_i}$ as long as they are not smooth. It stops after finitely many steps and the leaves of the corresponding desingularization tree are labeled by curves $\widetilde{X}_j = \operatorname{Spec} \widetilde{k}_j[\tilde{x},\tilde{y}]/\langle \widetilde{F}_j(\tilde{x},\tilde{y})\rangle$ such that the $\mathscr{O}_{\widetilde{X}_j,0}$ are the DVRs whose isomorphic image contain $\mathscr{O}_{X,p}$. W.l.o.g., we can suppose $\tilde{x}$ is a local parameter of $\mathscr{O}_{\widetilde{X}_j,0}$ and use NEWTON's method to write $\tilde{y}$ as a power series in $\tilde{x}$ in the completion of the ring.

Algorithmics of the computation of adjoint divisors

Once the desingularization tree is built, one recursively build the exceptional divisors

$$\mathrm{exc}_p(X) = \sum_{P|p} m_P(p) \cdot P \ , \quad \text{where} \quad m_P(p) = \min\{\mathrm{v}_P(f) \ , \ f \in \mathfrak{m}_{X,p}\} \ ,$$

and to compute the local adjoint divisor, we use the recursive formula:

$$\mathrm{adj}_p(X) = (\mathrm{m}_p(X) - 1) \cdot \mathrm{exc}_p(X) + \sum_{q \in \mathrm{Icp}(p)} \mathrm{adj}_q(X_q) \ ,$$

where $\mathrm{m}_p(X)$ is the multiplicity of $X = \mathrm{Spec}\, k[x,y]/\langle F(x,y)\rangle$ at p, *i.e.* the degree of the initial form of $F(x,y)$.

Implementation of the desingularization

Desingularization

Theoretical step	Algorithmic tools
Build X.	Multivariate polynomial rings, multivariate gcd, scheme structure.
Find singularities of X.	Multivariate resultants, univariate factorization, tower of extension of finite fields.
Build desingularization trees at each singularity.	Labeled tree structure, polynomial ring homomorphisms. NEWTON's method
Compute adjoint divisor adj(X), deduce the geometric genus $p_g(X)$.	Places structure, divisor structure, recursive parsing of the desingularization tree.

A basis of $\mathscr{L}(D)$ using Brill-Noether theorem

Let $X = \operatorname{Proj} S$, be a geometrically irreducible projective plane curve over $\mathbb{F}_q$ of degree d, and a divisor $D = \sum_{P \in \mathrm{Pl}(X)} n_P \cdot P$, we want to compute a basis of the finite-dimensional $\mathbb{F}_q$-vector space:

$$\mathscr{L}(D) = \left\{ f \in \mathrm{K}(X) \setminus \{0\} \;\middle|\; (f) + D \geq 0 \right\} \sqcup \{0\} \; .$$

We use the space of interpolating forms of degree δ for an effective divisor $B \geq 0$:

$$S_\delta(B) = \{ f \in S_\delta \mid (f) \geq B \} \; .$$

Th (Brill-Noether) Let $B = (D + \mathrm{adj}(X))_+ = v_1 P_1 + \cdots + v_r P_r \geq 0$. For all integer δ such that $\delta > \max\left(d-1, \frac{d-3}{2} + \frac{v}{d}\right)$, there exists $g_0 \in S_\delta(B) \setminus \{0\}$, such that

$$\mathscr{L}(D) = \left\{ \frac{g}{g_0} \; , \; g_i \in S_\delta\big((g_0) - D\big) \setminus \{0\} \right\} \sqcup \{0\} \; .$$

Interpolating forms

Let $\Sigma = \mathbb{F}_q[x, y, z]$ and Σ_δ the $\mathbb{F}_q$-vector space of homomogeneous polynomials of degree δ. The basis $(x^i y^j z^k \ , \ i + j + k = \delta)$ has $(\delta + 1)(\delta + 2)/2$ elements.

Let $B = v_1 P_1 + \cdots v_r P_r \geq 0$ be an effective divisor. For $1 \leq i \leq r$, the fact an element $f \in S_\delta \backslash \{0\}$ satisfies $\mathrm{v}_{P_i}(f) \geq v_i$ signifies that the P_i-adic series of f has zero coefficients up to order $v_i - 1$.

Let p_i be the point of X below P_i, the map $\mathscr{O}_p \longrightarrow \mathscr{O}_{P_i}$ induces a map

$$\mathbb{F}_q[x, y, z] \hookrightarrow \mathfrak{k}_{P_i}[u, v] \hookrightarrow \mathfrak{k}_{P_i}[[\pi]] \ .$$

We compute a generator system of the interpolating forms of $v_i P_i$ by computing the $\mathbb{F}_q$-kernel of the matrix of images of the $x^i y^j z^k$, using a generalization of DELSARTE's Theorem.

A vector space complement removes multiples of H.

We take the intersection of all spaces for $1 \leq i \leq r$ to get $S_\delta(B)$.

Implementation of Brill-Noether algorithm

Brill-Noether algorithm

Theoretical step	Algorithmic tools
Compute the Brill-Noether bound δ	Divisor structure
Compute the space of interpolating forms of degree δ of $\big(D + \mathrm{adj}(X)\big)_+$ and take a nonzero element g_0	Homomorphism $\mathbb{F}_q[x,y,z] \longrightarrow \mathbb{F}_{q^r}[[\pi]]$ to compute P-adic series, linear algebra over finite fields
Compute a basis $(g_1, \ldots, g_\kappa)$ of the space of interpolating forms of degree δ of $\big((g_0) - D\big)_+$ and return the basis $(g_1/g_0, \ldots, g_\kappa/g_0)$	Idem + vector space complement.

Building an Algebraic-Geometric Code

Let $P = (P_1, \ldots, P_n)$ be an n-tuple of distinct places of degree 1, and define the evaluation map:

$$\begin{aligned} \mathrm{ev}_P : \bigcap_{i=1}^{n} \mathscr{O}_P &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)) \end{aligned}$$

Let $D \in \mathrm{Div}(X)$, such that $P_i \notin \mathrm{Supp}\, D$ for all i, the $[n, k \leq \ell(D), d]_q$-weakly-algebraic-geometric (WAG) code is: $C \stackrel{\text{def}}{=} \mathrm{im}\left(\mathrm{ev}_{P|\mathscr{L}(D)}\right) = \{(f(P_1), \ldots, f(P_n)) \ , \ f \in \mathscr{L}(D)\}$.
If $\deg D < n$, $\mathrm{ev}_{P|\mathscr{L}(D)}$ is injective and C is an algebraic-geometric (AG) and according to Riemann inequality:

$$k = \ell(D) \geq \deg D + 1 - \mathrm{p_g}(X) \quad \text{and} \quad d \geq n - \deg D \ .$$

If $2g - 2 < \deg D < n$, C is a strongly-algebraic-geometric (SAG) code and according to Riemann-Roch theorem $k = \ell(D) = \deg D + 1 - \mathrm{p_g}(X)$.

Conclusion

It works! Even for reduced curves that are not geometrically irreducible: it allows absolute factorization.

There is something very frustrating: all objects we want to build have a definition over $\mathbb{F}_q$ and algorithms involve field extensions, non-canonical choices, and therefore an exasperating additional cost of equality tests. Please help!

One can derive from algorithms to build the ring of integers of a number field K (*i.e.* the normalization of $\mathbb{Z}$ in K), a purely algebraic normalization of affine plane curves working with their function field (both are global fields). (*Round 2*, Florian HESS, Magma V.2.7, *Round 4*, Emmanuel HALLOIN). Benchmarks suggest that our implementation and the *Round 2* implementation are equally competitive, depending on the situation.

Decoding algorithms for AG-codes ("SUDAN-like") are being implemented.