Fast computation of a rational point of a variety over a finite field

Guillermo Matera

Universidad Nacional de General Sarmiento,
Buenos Aires

MAP Conference, 25-29.8.08

Let $\mathbb{F}_q$ be the finite field of q elements, $\overline{\mathbb{F}}_q$ its algebraic closure.

Given polynomials $f_1, \ldots, f_s \in \mathbb{F}_q[X_1, \ldots, X_n]$.

Multivariate Equation Problem (ME):

- find a solution $x \in \mathbb{F}_q^n$ of the polynomial system

$$f_1(X) = \cdots = f_s(X) = 0,$$

- find a point $x \in \mathbb{F}_q^n$ of the variety (defined over $\mathbb{F}_q$)

$$V(f_1, \ldots, f_s) := \{x \in \overline{\mathbb{F}}_q^n : f_1(x) = \cdots = f_s(x) = 0\}.$$

Motivation: coding theory, cryptography, polynomial system solving over $\mathbb{Q}$, etc.

Example: Public key schemes based on ME (Imai-Matsumoto, Patarin et al., Wolf-Preneel, ...).

- Given
  - ◇ a plaintext $x \in \mathbb{F}_q^n$,
  - ◇ a polynomial map $F := (f_1, \ldots, f_s) : \mathbb{F}_q^n \to \mathbb{F}_q^s$,
  - ◇ the cyphertext is $y := F(x)$.

Breaking such a cryptosystem "requires" solving the ME problem

$$f_1(X) - y_1 = 0, \ldots, f_s(X) - y_s = 0.$$

- ME is NP-complete, even for quadratic eqs. over $\mathbb{F}_2$.
- We are interested in probabilistic algorithms for ME.
- We shall assume that $q \gg$ degrees of equations.

First case: plane curves

Let $f \in \mathbb{F}_q[X,Y]$, $C := V(f) := \{(x,y) \in \overline{\mathbb{F}}_q^2 : f(x,y) = 0\}$, $C(\mathbb{F}_q) := C \cap \mathbb{F}_q^2$.

∘ Hardness of ME for C is related to $\#C(\mathbb{F}_q)$.

∘ Average number of points: $\#C(\mathbb{F}_q) \approx q$.

Estimates: Absolute irreducibility.

∘ $f \in \mathbb{F}_q[X,Y]$ is abs. irred. if it's irreducible in $\overline{\mathbb{F}}_q[X,Y]$.

Example: $f := X + Y^3$ is, $g := X^2 - 3Y^2$ is not in $\mathbb{F}_5$.

∘ $C := V(f) \subset \overline{\mathbb{F}}_q^2$ is abs. irred. if f is abs. irred.

[Weil, 1948] For $C := V(f)$ abs. irred. with $\deg(f) = d$

$$|\#C(\mathbb{F}_q) - q| \leq d^2 q^{1/2}.$$

Example (cont.): $\#V(f)(\mathbb{F}_5) = 5$, $\#V(g)(\mathbb{F}_5) = 1$.

Computation: search in a vertical strip (SVS).

Let $f \in \mathbb{F}_q[X, Y]$ be absolutely irreducible.

For $a \in \mathbb{F}_q$, let
$$C_a(\mathbb{F}_q) := C(\mathbb{F}_q) \cap \{X = a\} = \{b \in \mathbb{F}_q : f(a, b) = 0\}.$$

$\circ$ Weil $\Rightarrow$
$$\text{Prob}(a \in \mathbb{F}_q : C_a(\mathbb{F}_q) \neq \emptyset) \geq \frac{1}{dq}(q - d^2 q^{\frac{1}{2}}) = \frac{1}{d}\left(1 - \frac{d^2}{q^{1/2}}\right) \approx \frac{1}{d}.$$

Algorithm SVS

$\diamond$ find $a \in \mathbb{F}_q$ with $C_a(\mathbb{F}_q) \neq \emptyset$. [at most d trials]

$\diamond$ find $b \in C_a(\mathbb{F}_q)$. [find an $\mathbb{F}_q$-root of $f(a, Y)$]

[Gathen–Shparlinski, 1995] computes uniformly a point of $C(\mathbb{F}_q)$ in polynomial time.

What if $C = V(f)$ is not absolutely irreducible?

Decompose $C = \cup C_i$ over $\mathbb{F}_q$ (factor $f = \prod_i f_i$ over $\mathbb{F}_q$).

Easy case: If $\exists$ C_i absolutely irred., apply SVS to C_i.

Hard case: If C_i is not absolutely irreducible for all i
[C_i is relatively irreducible for all i], then

- ◇ Fact. $C(\mathbb{F}_q) \subset C \cap V(\partial f/\partial Y) = V(f, \partial f/\partial Y) =: W$.
  [observe that $\dim W = 0$, $\deg W \leq d(d-1)$]

- ◇ Algorithm SVS–RI
  - ▷ Compute the resultant $g(X) := \mathrm{res}_Y(f, \partial f/\partial Y)$.
  - ▷ find the set of $\mathbb{F}_q$–roots of g.
  - ▷ for each root $a \in \mathbb{F}_q$, find the $\mathbb{F}_q$–roots of $f(a, Y)$.

Cost of finding an $\mathbb{F}_q$-point in a plane curve

- If C has an absolutely irreducible $\mathbb{F}_q$-component then we perform $O\tilde{}(d^{\mathbf{2}} \log q)$ operations in $\mathbb{F}_q$.

- If C is a union of relatively irreducible $\mathbb{F}_q$-components then we perform $O\tilde{}(d^{\mathbf{3}} \log q)$ operations in $\mathbb{F}_q$.

- [von zur Gathen, 2007] Prob(f is rel. irred.)$\leq q^{-d^2/4}$.

Second case: hypersurfaces

Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ and let H be the hypersurface $H := V(f) := \{(x_1, \ldots, x_n) \in \overline{\mathbb{F}}_q^n : f(x_1, \ldots, x_n) = 0\}$.

Average number of points: $\#H(\mathbb{F}_q) \approx q^{n-1}$.

Estimates: Absolute irreducibility.

- $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ is absolutely irreducible if it is irreducible in $\overline{\mathbb{F}}_q[X_1, \ldots, X_n]$.
- $H := V(f) \subset \overline{\mathbb{F}}_q^n$ is absolutely irreducible if it is defined by an absolutely irreducible polynomial f.

[Lang–Weil, 1954] For $H := V(f) \subset \overline{\mathbb{F}}_q^n$ absolutely irreducible of degree $\delta > 0$, $\exists\ C = C(n, \delta)$ such that:

$$|\#H(\mathbb{F}_q) - q^{n-1}| \leq \delta^2 q^{n-3/2} + C q^{n-2}.$$

Computation: search in 1-dim. linear section (S1S).

For $H := V(f) \subset \overline{\mathbb{F}}_q^n$ abs. irred., we compute a point of $H(\mathbb{F}_q)$ in the plane curve $H \cap L$, with L an $\mathbb{F}_q$-plane.

Example: for $H : X - Y^2 - Z^2 = 0$ and a plane $L : \{X + bY + cZ = 0\}$, $H \cap L = \{Y^2 + Z^2 + bY + cZ = 0\} \cap L$.

Effective Bertini theorem [Kaltofen, 1995]: $H \cap L$ isn't abs. irreducible for a random L with probability $\leq 2\delta^4/q$.

Example (cont.): $H \cap L$ is abs. irred. for $b^2 + c^2 \neq 0$.

Explicit bounds

∘ Versions of the Effective Bertini theorem.

∘ "Statistics" on number of q-points on plane sections.

[Cafure-M., 2006]

⋄ For $q > 2\delta^4$, there exist q–rational points.

⋄ For $q > 15\delta^{13/3}$, $|\#H(\mathbb{F}_q) - q^{n-1}| \leq \delta^2 q^{n-3/2} + \mathbf{7} \cdot \boldsymbol{\delta}^{\mathbf{2}} q^{n-2}$.

Algorithm for searching in a 1-dim. section

∘ Algorithm S1S

⋄ choose an $\mathbb{F}_q$-plane L randomly. [$H \cap L$ is abs. irred.]

⋄ apply SVS to $H \cap L$. [factor gcd$(f(a, Y), Y^q - Y)$]

Cost: $\tilde{O}(\delta^2 \log q)$ operations in $\mathbb{F}_q$.

Case $H = V(f)$ not absolutely irreducible.

Decompose $H = \cup H_i$ over $\mathbb{F}_q$ (factor $f = \prod_i f_i$ over $\mathbb{F}_q$).

Easy case: If $\exists\ H_i$ absolutely irred., apply S1S to H_i.

Hard case: If H_i isn't absolutely irred. for all i, then

- ◇ Fact: $H(\mathbb{F}_q) \subset H \cap V(\partial f/\partial X_n) =: W^{(1)}$.
  [dim $W^{(1)} = n - 2$, deg $W^{(1)} \leq \delta^{\mathbf{2}}$]
- ◇ Decompose $W^{(1)} = \cup_i W_i^{(1)}$ over $\mathbb{F}_q$.
- ◇ If $\exists\ W_i^{(1)}$ absolutely irreducible, then Easy case.
- ◇ Else, Hard case: introduce $W^{(2)}$.
  [dim $W^{(2)} = n - 3$, deg $W^{(2)} \leq \delta^{\mathbf{4}}$].

⋮

Cost (worst-case): $O(\delta^{\mathbf{2^n}} \log q)$ operations in $\mathbb{F}_q$.

[von zur Gathen-Viola, 2007] Prob(f rel. irred.) $\rightarrow$0

Third case: arbitrary dimension

Let $V := V(f_1, ..., f_s) := \{x \in \overline{\mathbb{F}}_q^n : f_1(x) = \cdots = f_s(x) = 0\}$.

Two invariants: dimension and degree.

"Expected" number of points: $\#V(\mathbb{F}_q) \approx q^{\dim V}$.

[Lang–Weil, 1954] For $V \subset \overline{\mathbb{F}}_q^n$ absolutely irreducible of dimension $r > 0$ and degree δ, $\exists\ C = C(n, r, \delta)$ such that

$$|\#V(\mathbb{F}_q) - q^r| \le \delta^2 q^{r-1/2} + C q^{r-1}.$$

Reduction to hypersurfaces: birational projections.

Let $V \subset \overline{\mathbb{F}}_q^n$ abs. irred. of dimension r and degree δ.

Fact: For $q \geq \delta$, $\exists$ $\mathbb{F}_q$–linear $\pi : V \to \pi(V) \subset \overline{\mathbb{F}}_q^{r+1}$ with a rational inverse $\pi^{-1} : \pi(V) \to V$ defined in an open dense subset of $\pi(V)$.

Example: For $C := \{X = Z^2 + Z^4, Y = Z^2\}$, the projection onto the (X, Z)-plane is $\{X = Z^2 + Z^4\}$. The inverse is $\pi^{-1}(x, z) = (x, z^2, z)$.

[Cafure-M., 2006] For $q > 15\delta^{13/3}$, we have $C \leq 7 \cdot \delta^2$.

[Ghorpade-Lachaud, 2002] If $V := V(f_1, \ldots, f_s)$ and $d := \max \deg(f_i)$, then $C \leq 6 \cdot 2^s \cdot (sd + 1)^{n+1}$.

Bézout inequality $\Rightarrow \delta \leq d^r$.

Computation of a birational projection (BProj).

Input: $V := V(f_1, \ldots, f_{n-r})$ absolutely irreducible.

Algorithm BProj [Cafure-M, 2006b]

- ∘ Incremental elimination method.
- ∘ Global Newton–Hensel lifting.

Cost: $O\tilde{}(D^2 \log q)$ operations in $\mathbb{F}_q$, with $D \le \prod_i \deg(f_i)$.

Computation of an $\mathbb{F}_q$-point

- ∘ compute a birational projection π. [Algorithm BProj]
- ∘ find an $\mathbb{F}_q$-point in $\pi(V)$. [Algorithm S1S]

Cost: $O\tilde{}(D^2 \log q)$ operations in $\mathbb{F}_q$.

[Huang-Wong, 1999] $d^{O(n^2)} \log q$ ops. in $\mathbb{F}_q$, $d := \max \deg(f_i)$.

Extensions to non absolutely irreducible cases?

Easy case: $V = \cup_i V_i$ over $\mathbb{F}_q$ and $\exists\ V_i$ absolutely irreducible with $\dim(V_i) = \dim(V)$.

Hard case: $V = \cup_i V_i$ over $\mathbb{F}_q$ and all V_i with $\dim(V_i) =$ $= \dim(V)$ are relatively irreducible.

- $\diamond$ Each $x \in V(\mathbb{F}_q)$ belongs to all abs. irred. components.
- $\diamond$ Each $x \in V(\mathbb{F}_q)$ annihilates the discriminant of all linear birational projections.
- $\diamond$ Adding discriminants $\Rightarrow O(D^{\mathbf{2^r}} \log q)$ in worst case.

[Cesaratto-von zur Gathen-M.] Probability a curve C is relatively irreducible $\to 0$ as $q \to \infty$.

Conclusions

- Worst-case complexity of ME is doubly exponential.

- Complexity of ME $\approx$ complexity of the absolutely irreducible case.

- Finer analysis of the absolutely irred. case required.

  - [Knopfmacher–Knopfmacher, 90] Probability that a random polynomial $f \in \mathbb{F}_q[X]$ has a q-root is $1/e$.

  - This might imply that $\cong$ 3 trials suffice in SVS $\Rightarrow O\tilde{}(d \log q)$ operations in $\mathbb{F}_q$ in SVS and S1S.