Irreducibility of curves over finite fields

Felipe Voloch

NZMS-AMS-AusMS meeting

December 2024

Abstract

We discuss some problems on algebraic curves over finite fields motivated by list decoding algorithms for Reed-Solomon codes. We look at certain linear systems of curves and bound how many of these are reducible over the finite field. We also consider a sufficient condition for irreducibility for those curves and bound the number of curves failing it. Preliminary report.

Reed-Solomon codes

$\mathbb{F}_q$ finite field of q elements

$V = \{g : \mathbb{F}_q \to \mathbb{F}_q\}$, vector space of dimension q.

$d(g_1, g_2) = \#\{\alpha \in \mathbb{F}_q \mid g_1(\alpha) \neq g_2(\alpha)\}$ is a metric on V.

$RS_k = \{f \in \mathbb{F}_q[x], \deg f < k\}$, $k < q$, viewed as a subspace of V.

Problem: Recognize when $g \in V$ is close to an element of RS_k and obtain said element(s).

Reed-Solomon codes II

For $g \in V$:

If $d(g, f) < q - (q + k)/2, f \in RS_k$, then f is unique.

The set of $f \in RS_k$ with $d(g, f) < q - \sqrt{qk}$ has small cardinality (Johnson) and, for most g for which it is non-empty, it has only one element (McEliece).

Sudan's algorithm

Theorem 1

(Sudan) For given q, k, let d be an integer satisfying

$$q < \frac{d(d+1)}{2}(k-1) + d + 1. \tag{1}$$

For $g \in V$, there exists $G(x,y) = \sum_{i=0}^{d} a_i(x)y^i \in \mathbb{F}_q[x,y]$ with $\deg a_i \leq (d-i)(k-1), i = 0, \ldots, d$ such that $\forall \alpha \in \mathbb{F}_q, G(\alpha, g(\alpha)) = 0$. Moreover, if $f(x) \in RS_k(q)$ satisfies $d(f,g) < q - (k-1)d$ then $G(x, f(x))$ is identically zero.

G can be found by linear algebra and the f with $G(x, f(x)) \equiv 0$ can be found using a polynomial factoring algorithm.

Main result

The theorem ensures that if f is close to g, then f is a root of G.

The converse is not always true. But is often true.

Theorem 2

Let $\varepsilon > 0$ be fixed. If $k \geq \varepsilon q$ and

$$\frac{\log(q)}{\log(q-1)}\left(k + d(\frac{(d-1)(k-1)}{2} + 1)\right) < t < q - (k-1)d.$$

Given $f \in RS_k$, for most functions $g : \mathbb{F}_q \to \mathbb{F}_q$, $d(f,g) = t$, no associated G from Theorem 1 have a factor of the form $y - f_1(x), f_1 \neq f, \deg f_1 < k$.

Open questions

If the inequality (1) is close to sharp, then for most g, any associated G has no root in RS_k. How do we refine theorem 1 so the conclusion holds even if (1) is not close to sharp?

Sudan's algorithm was extended by Guruswami and Sudan, by requiring G to vanish at $(\alpha, g(\alpha))$ with multiplicities. Does the above result extend?

Does the condition $D_x^{(k)}(y) = 0$ characterize f among the roots of G in $\overline{\mathbb{F}_q(x)}$, for most g?

THANK YOU