On the Recursive Behaviour of the Number of Irreducible Polynomials with Certain Properties over Finite Fields

Max Schulz

University of Rostock, Institute of Mathematics
WCC 2024 Perugia

20.06.2024

How it started

Gohar Kyureghyan
Fr 24.02.2023, 11:29

irred_trace_2022.pdf
145 KB

Herunterladen

Lieber Max,

heute habe ich eine interessante Arbeit gesehen, sie ist im Anhang. Eventuell gibt sie dir neue Impulse.

Viele Grüße
Gohar

Omran Ahmadis Observation

$$x^5 + x^2 + 1$$
$$x^5 + x^3 + 1$$
$$x^5 + x^3 + x^2 + x + 1$$
$$x^5 + x^4 + x^2 + x + 1$$
$$x^5 + x^4 + x^3 + x + 1$$
$$x^5 + x^4 + x^3 + x^2 + 1$$

Omran Ahmadis Observation

$$x^5 + x^2 + 1$$
$$x^5 + x^3 + 1$$
$$x^5 + x^3 + x^2 + x + 1$$
$$x^5 + x^4 + x^2 + x + 1$$
$$x^5 + x^4 + x^3 + x + 1$$
$$x^5 + x^4 + x^3 + x^2 + 1$$

- Focus on the coefficients before x and x^{n-1} of a polynomial of degree n

Omran Ahmadis Observation

$$x^5 + x^2 + 1$$
$$x^5 + x^3 + 1$$
$$x^5 + x^3 + x^2 + x + 1$$
$$x^5 + x^4 + x^2 + x + 1$$
$$x^5 + x^4 + x^3 + x + 1$$
$$x^5 + x^4 + x^3 + x^2 + 1$$

- Focus on the coefficients before x and x^{n-1} of a polynomial of degree n

Omran Ahmadis Observation

$$x^5 + x^2 + 1$$
$$x^5 + x^3 + 1$$
$$x^5 + x^3 + x^2 + x + 1$$
$$x^5 + x^4 + x^2 + x + 1$$
$$x^5 + x^4 + x^3 + x + 1$$
$$x^5 + x^4 + x^3 + x^2 + 1$$

- Focus on the coefficients before x and x^{n-1} of a polynomial of degree n
- Always the case for n odd

n even

$$x^6 + x + 1$$
$$x^6 + x^3 + 1$$
$$x^6 + x^5 + 1$$
$$x^6 + x^4 + x^2 + x + 1$$
$$x^6 + x^4 + x^3 + x + 1$$
$$x^6 + x^5 + x^2 + x + 1$$
$$x^6 + x^5 + x^4 + x + 1$$
$$x^6 + x^5 + x^3 + x^2 + 1$$
$$x^6 + x^5 + x^4 + x^2 + 1$$

n even

$$x^6 + x + 1$$
$$x^6 + x^3 + 1$$
$$x^6 + x^5 + 1$$
$$x^6 + x^4 + x^2 + x + 1$$
$$x^6 + x^4 + x^3 + x + 1$$
$$x^6 + x^5 + x^2 + x + 1$$
$$x^6 + x^5 + x^4 + x + 1$$
$$x^6 + x^5 + x^3 + x^2 + 1$$
$$x^6 + x^5 + x^4 + x^2 + 1$$

Robert Grangers Result

Let $a_i(f)$ be the i-th coefficient of the polynomial f, then

$S_{a,b}(n) := \{f \in \mathbb{F}_2[x] \mid f \text{ irreducible and } a_{n-1}(f) = a,\ a_1(f) = b\}$.

Theorem (R. Granger)

$$|S_{1,1}(n)| - |S_{0,0}(n)| = \begin{cases} 0, & n \text{ is odd} \\ |S_{1,*}(n/2)|, & n \text{ is even.} \end{cases}$$

[1] Robert Granger. „Three proofs of an observation on irreducible polynomials over GF(2)“. In: *Finite Fields and Their Applications* 88 (2023).

Motivation

- Rewriting R. Grangers result gives

$$|S_{1,*}(n)| - |S_{0,*}(n)| = (|S_{1,1}(n)| + |S_{1,0}(n)|) - (|S_{0,1}(n)| + |S_{0,0}(n)|)$$
$$= |S_{1,1}(n)| - |S_{0,0}(n)|.$$

Motivation

- Rewriting R. Grangers result gives

$$\begin{aligned}|S_{1,*}(n)| - |S_{0,*}(n)| &= (|S_{1,1}(n)| + |S_{1,0}(n)|) - (|S_{0,1}(n)| + |S_{0,0}(n)|) \\ &= |S_{1,1}(n)| - |S_{0,0}(n)|.\end{aligned}$$

- Thus

$$|S_{1,*}(n)| - |S_{0,*}(n)| = \begin{cases} 0, & n \text{ is odd} \\ |S_{1,*}(n/2)|, & n \text{ is even} \end{cases}$$

Motivation

- Rewriting R. Grangers result gives

$$\begin{aligned}|S_{1,*}(n)| - |S_{0,*}(n)| &= (|S_{1,1}(n)| + |S_{1,0}(n)|) - (|S_{0,1}(n)| + |S_{0,0}(n)|)\\ &= |S_{1,1}(n)| - |S_{0,0}(n)|.\end{aligned}$$

- Thus

$$|S_{1,*}(n)| - |S_{0,*}(n)| = \begin{cases} 0, & n \text{ is odd} \\ |S_{1,*}(n/2)|, & n \text{ is even} \end{cases}$$

- We were familiar with that kind of behaviour but in another context, can we find a connection?

Rational Transformations

Let $F \in \mathbb{F}_q[x]$ and $Q = g/h \in \mathbb{F}_q(x)$, then

$$F^Q(x) := \lambda_{g,h,F} h(x)^{\deg(F)} \cdot F\left(\frac{g(x)}{h(x)}\right).$$

Rational Transformations

Let $F \in \mathbb{F}_q[x]$ and $Q = g/h \in \mathbb{F}_q(x)$, then

$$F^Q(x) := \lambda_{g,h,F} h(x)^{\deg(F)} \cdot F\left(\frac{g(x)}{h(x)}\right).$$

Lemma (Cohen)

Let $F \in \mathbb{F}_q[x]$ and $Q = g/h \in \mathbb{F}_q(x)$ with $\gcd(g,h) = 1$. Then F^Q is irreducible over $\mathbb{F}_q[x]$ if and only if $F \in \mathbb{F}_q[x]$ is irreducible and $g - \alpha h \in \mathbb{F}_q(\alpha)[x]$ is irreducible, where $\alpha \in \overline{\mathbb{F}}_q$ a root of F.

[2] Stephen D. Cohen. „On irreducible polynomials of certain types in finite fields“. In: *Mathematical Proceedings of the Cambridge Philosophical Society* 66.2 (1969), S. 335–344.

Yes/No

Fix a rational function $Q = g/h$.

Yes/No

Fix a rational function $Q = g/h$.

- We partition the set of irreducible monic polynomials $\mathcal{I}_q^n$ of degree n into

$$Yes(Q,n) := \{f \in \mathcal{I}_q^n \mid f^Q \text{ is irreducible}\}$$
$$No(Q,n) := \{f \in \mathcal{I}_q^n \mid f^Q \text{ is not irreducible}\}.$$

Yes/No

Fix a rational function $Q = g/h$.

- We partition the set of irreducible monic polynomials $\mathcal{I}_q^n$ of degree n into

$$Yes(Q,n) := \{f \in \mathcal{I}_q^n \mid f^Q \text{ is irreducible}\}$$
$$No(Q,n) := \{f \in \mathcal{I}_q^n \mid f^Q \text{ is not irreducible}\}.$$

- In general hard to describe, since deciding whether $g - \alpha h$ is irreducible can be difficult

A Change of (personal) Perspective

In the past:

- Only interested in the irreducible polynomials f^Q for f an irreducible polynomial of degree n
- ... because all invariant irreducible polynomials are special rational transformations

Now:

- Also interested in the irreducible polynomials f of degree n for which f^Q is irreducible

[3] Lucas Reis. „Möbius-like maps on irreducible polynomials and rational transformations“. In: *Journal of Pure and Applied Algebra* 224 (Mai 2019), S. 169–180.

A Theorem for Yes/No

A quotient map $Q_G \in \mathbb{F}_q(x)$ for a subgroup $G \leq \mathrm{PGL}_2(\mathbb{F}_q)$ is a rational function that generates the subfield

$$\mathbb{F}_q(x)^G := \left\{ Q \in \mathbb{F}_q(x) \mid Q\left(\frac{ax+b}{cx+d}\right) = Q(x) \text{ for all } \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \in G \right\}$$

Theorem (Sch.)

Let $G \leq \mathrm{PGL}_2(\mathbb{F}_q)$ be a cyclic subgroup of prime order s and Q_G a quotient map for G. For all $n > d(G)$ we have

$$|Yes(Q_G, n)| - (s-1)|No(Q_G, n)| = \begin{cases} 0, & \text{if } s \nmid n \\ |Yes(Q_G, n/s)|, & \text{if } s \mid n. \end{cases}$$

[4] Max Schulz. *On the Recursive Behaviour of the Number of Irreducible Polynomials with Certain Properties over Finite Fields*. 2023. arXiv: 2310.01872 [math.NT].

We have a recipe, so what now?

Are there particular instances of quotient maps Q_G for which $Yes(Q_G, n)$ and $No(Q_G, n)$ can be described in a "nice" arithmetical way?

Onto a Generalization of R. Grangers Result

Let p be prime and $q = p^t$. Let $f \in \mathbb{F}_q[x]$ be an irreducible monic polynomial of degree n, then we set

$$\mathrm{Tr}(f) := -\mathrm{Tr}_{q^n/p}(\alpha)$$

where $\alpha \in \mathbb{F}_{q^n}$.

Onto a Generalization of R. Grangers Result

Let p be prime and $q = p^t$. Let $f \in \mathbb{F}_q[x]$ be an irreducible monic polynomial of degree n, then we set

$$\mathrm{Tr}(f) := -\mathrm{Tr}_{q^n/p}(\alpha)$$

where $\alpha \in \mathbb{F}_{q^n}$.

- Be careful! It's the absolute trace!

Onto a Generalization of R. Grangers Result

Let p be prime and $q = p^t$. Let $f \in \mathbb{F}_q[x]$ be an irreducible monic polynomial of degree n, then we set

$$\mathrm{Tr}(f) := -\mathrm{Tr}_{q^n/p}(\alpha)$$

where $\alpha \in \mathbb{F}_{q^n}$.

- Be careful! It's the absolute trace!
- If $q = p$, then $\mathrm{Tr}(f) = a_{n-1}(f)$.

Onto a Generalization of R. Grangers Result

Let p be prime and $q = p^t$. Let $f \in \mathbb{F}_q[x]$ be an irreducible monic polynomial of degree n, then we set

$$\mathrm{Tr}(f) := -\,\mathrm{Tr}_{q^n/p}(\alpha)$$

where $\alpha \in \mathbb{F}_{q^n}$.

- Be careful! It's the absolute trace!
- If $q = p$, then $\mathrm{Tr}(f) = a_{n-1}(f)$.
- In general $\mathrm{Tr}(f) = \mathrm{Tr}_{q/p}(a_{n-1}(f))$.

Onto a Generalization of R. Grangers Result

Let $\mathcal{I}_q^n$ be the set of irreducible monic polynomials in $\mathbb{F}_q[x]$ of degree n. Define for $a \in \mathbb{F}_p$

$$S_a(n) := \{f \in \mathcal{I}_q^n \mid \mathrm{Tr}(f) = a\}.$$

Theorem (Sch.)

For all $n \in \mathbb{N} \setminus \{0\}$ and all finite fields $\mathbb{F}_q$ we have

$$\sum_{a \in \mathbb{F}_p^*} |S_a(n)| - (p-1)|S_0(n)| = \begin{cases} 0, & \text{if } p \nmid n \\ \sum_{a \in \mathbb{F}_p^*} |S_a(n/p)|, & \text{if } p \mid n. \end{cases}$$

Choosing the right Subgroups and Quotient Maps

The rational function $Q_G(x) = x^p - x$ is a quotient map for a cyclic subgroup of order $p = \mathrm{char}(\mathbb{F}_q)$ and

$$f(x^p - x) \text{ is irreducible } \Leftrightarrow$$
$$f \text{ is irreducible and } x^p - x - \alpha \text{ is irreducible in } \mathbb{F}_q(\alpha)$$

where $\alpha \in \overline{\mathbb{F}}_q$ is a root of f (Capelli/Cohens Lemma!). The polynomial $x^p - x - \alpha \in \mathbb{F}_{q^n}[x]$ is irreducible if and only if $\mathrm{Tr}_{q^n/p}(\alpha) \neq 0$ due to Varshamov. Thus

$$Yes(x^p - x, n) = \bigcup_{a \in \mathbb{F}_p^*} S_a(n)$$
$$No(x^p - x, n) = S_0(n).$$

And another one

Let q be odd and $u, v \in \mathbb{F}_q$ with $u \neq v$. Consider

$$C_{u,v}(n) := \{f \in \mathcal{I}_q^n \mid f(u) \cdot f(v) \text{ is a non-square in } \mathbb{F}_q\}$$
$$D_{u,v}(n) := \{f \in \mathcal{I}_q^n \mid f(u) \cdot f(v) \text{ is a square in } \mathbb{F}_q\}.$$

And another one

Let q be odd and $u, v \in \mathbb{F}_q$ with $u \neq v$. Consider

$$C_{u,v}(n) := \{f \in \mathcal{I}_q^n \mid f(u) \cdot f(v) \text{ is a non-square in } \mathbb{F}_q\}$$
$$D_{u,v}(n) := \{f \in \mathcal{I}_q^n \mid f(u) \cdot f(v) \text{ is a square in } \mathbb{F}_q\}.$$

Theorem (Sch.)

Let q be odd. For all $u, v \in \mathbb{F}_q$ with $u \neq v$ and $n > 1$ we have

$$|C_{u,v}(n)| - |D_{u,v}(n)| = \begin{cases} 0, & \text{if } 2 \nmid n \\ |C_{u,v}(n/2)|, & \text{if } 2 \mid n. \end{cases}$$

Choosing the right Subgroups and Quotient Maps

Theorem (Sch.)

Let q be odd. For all $u, v \in \mathbb{F}_q$ with $u \neq v$ and $n > 1$ we have

$$|C_{u,v}(n)| - |D_{u,v}(n)| = \begin{cases} 0, & \text{if } 2 \nmid n \\ |C_{u,v}(n/2)|, & \text{if } 2 \mid n. \end{cases}$$

The rational function

$$Q_G(x) = \frac{x^2 - uv}{2x - (u+v)}$$

is a quotient map for a subgroup of order 2 and it can be shown that

$$Yes(Q_G, n) = \{f \in \mathcal{I}_q^n \mid f(u) \cdot f(v) \text{ is a non-square in } \mathbb{F}_q\}$$
$$No(Q_G, n) = \{f \in \mathcal{I}_q^n \mid f(u) \cdot f(v) \text{ is a square in } \mathbb{F}_q\}.$$

Pros & Cons of our Approach

Pros:

- Gives a recipe for proving and finding recursive relations of irreducible polynomials
- Reveals that there's an underlying symmetry that forces these theorems to hold
- Shows that perspectives matter

Cons:

- A lot of theory and notations to digest
- There are easier proofs for both instances I showed you
- The defining arithmetical properties for $Yes(Q_G, n), No(Q_G, n)$ that we know of are not so diverse (trace, square/non-square or power/non-power conditions).