On the Enumeration of Irreducible Polynomials over $\mathbb{F}_q$ with Prescribed Coefficients

Robert Granger

`robert.granger@epfl.ch`

Laboratory for Cryptologic Algorithms
School of Computer and Communication Sciences
École polytechnique fédérale de Lausanne
Switzerland

Fq13, Gaeta
6th June 2017

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Overview

The problem

New results over $\mathbb{F}_2$

The main algorithm

Summary & open problems

Overview

The problem

New results over $\mathbb{F}_2$

The main algorithm

Summary & open problems

Irreducible polynomials with prescribed coefficients

"The long-term goal here is to provide existence and counting results for irreducibles with any number of prescribed coefficients to any given values. This goal is completely out of reach at this time. Incremental steps seem doable, but it would be most interesting if new techniques were introduced to attack these problems."

– Daniel Panario (2015)

Irreducible polynomials with prescribed coefficients

"The long-term goal here is to provide existence and counting results for irreducibles with any number of prescribed coefficients to any given values. This goal is completely out of reach at this time. Incremental steps seem doable, but it would be most interesting if new techniques were introduced to attack these problems."

– Daniel Panario (2015)

On the problem of existence the best result to date is:

Theorem (*Ha 2016*)

For any $0 < \epsilon < 1/4$ and $q \geq q_0(\epsilon)$ for some large q_0, there exists a monic irreducible of degree n in $\mathbb{F}_q[x]$ with r prescribed coefficients in any positions, provided that $r \leq \lfloor (1/4 - \epsilon)n \rfloor$ (unless the constant term is 0).

Counting results

A subproblem of the long-term goal is to determine the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n for which the first l coefficients have the prescribed values $t_1, \ldots, t_l$, which we denote by $I_q(n, t_1, \ldots, t_l)$.

- In 1952 Carlitz gave formulae for $I_q(n, t_1)$
- In 1990 Kuz'min gave formulae for $I_q(n, t_1, t_2)$
- In 1999 Cattell *et al.* reproduced Kuz'min's results for the base field $\mathbb{F}_2$
- In 2001 formulae for $I_2(n, t_1, t_2, t_3)$ were given by Fitzgerald and Yucas for n odd, and by Yucas and Mullen for n even
- In 2007 Moisio-Ranto gave formulae for $I_{2^r}(n, 0, *, t_3)$ for all $r \geq 1$
- In 2013 Ri *et al.* gave formulae for $I_{2^r}(n, t_1, t_2)$ for all $r \geq 1$
- In 2016 Ahmadi *et al.* gave formulae for $I_{2^r}(n, 0, 0, 0)$ for all $r \geq 1$

Note: Over $\mathbb{F}_q$, in 2004 Yucas obtained formulae for prescribed norm, while in 2007 Moisio obtained some results for prescribed trace and norm.

An equivalent formulation

For $a \in \mathbb{F}_{q^n}$ the characteristic polynomial of a w.r.t. the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is

$$\prod_{i=0}^{n-1}(x - a^{q^i}) = x^n - T_1(a)x^{n-1} + T_2(a)x^{n-2} - \cdots + (-1)^{n-1}T_{n-1}(a)x + (-1)^n T_n(a),$$

with $T_l : \mathbb{F}_{q^n} \to \mathbb{F}_q$, $1 \leq l \leq n$ the successive trace functions

$$T_l(a) = \sum_{0 \leq i_1 < \cdots < i_l \leq n-1} a^{q^{i_1} + \cdots + q^{i_l}}.$$

For any $n \geq l$ and $t_1, \ldots, t_l \in \mathbb{F}_q$, let $F_q(n, t_1, \ldots, t_l)$ be the number of elements $a \in \mathbb{F}_{q^n}$ for which $T_1(a) = t_1$, ..., $T_l(a) = t_l$.

The $F_q(n, t_1, \ldots, t_l)$ can be expressed in terms of the $I_q(n, t_1, \ldots, t_l)$, and vice versa using an elementary Möbius inversion-type argument.

$\Longrightarrow$ *The problem of computing the $I_q(n, t_1, \ldots, t_l)$ reduces to the problem of computing the $F_q(n, t_1, \ldots, t_l)$.*

Overview

The problem

New results over $\mathbb{F}_2$

The main algorithm

Summary & open problems

Preliminary remarks

For $t_1, \ldots, t_l \in \mathbb{F}_2$ we would like to compute a formula as a function of n for

$$F_2(n, t_1, \ldots, t_l) = \#\{a \in \mathbb{F}_{2^n} \mid T_1(a) = t_1, \ldots, T_l(a) = t_l\} \qquad (1)$$

Preliminary remarks

For $t_1, \ldots, t_l \in \mathbb{F}_2$ we would like to compute a formula as a function of n for

$$F_2(n, t_1, \ldots, t_l) = \#\{a \in \mathbb{F}_{2^n} \mid T_1(a) = t_1, \ldots, T_l(a) = t_l\} \qquad (1)$$

This appears to be non-trivial in general, since the degree of each $T_j(a)$ in a and its conjugates is j, while a priori we only know how to solve $T_1(a) = t_1$:

Preliminary remarks

For $t_1, \ldots, t_l \in \mathbb{F}_2$ we would like to compute a formula as a function of n for

$$F_2(n, t_1, \ldots, t_l) = \#\{a \in \mathbb{F}_{2^n} \mid T_1(a) = t_1, \ldots, T_l(a) = t_l\} \qquad (1)$$

This appears to be non-trivial in general, since the degree of each $T_j(a)$ in a and its conjugates is j, while a priori we only know how to solve $T_1(a) = t_1$:

Lemma (*Thm. 2.25, Lidl & Niederreiter*)

1. *For $a \in \mathbb{F}_{2^n}$, $T_1(a) = 0 \Longleftrightarrow a = a_0^2 + a_0$ for two $a_0 \in \mathbb{F}_{2^n}$.*
2. *For $a \in \mathbb{F}_{2^n}$, n odd, $T_1(a) = 1 \Longleftrightarrow a = a_0^2 + a_0 + 1$ for two $a_0 \in \mathbb{F}_{2^n}$.*

Preliminary remarks

For $t_1, \ldots, t_l \in \mathbb{F}_2$ we would like to compute a formula as a function of n for

$$F_2(n, t_1, \ldots, t_l) = \#\{a \in \mathbb{F}_{2^n} \mid T_1(a) = t_1, \ldots, T_l(a) = t_l\} \tag{1}$$

This appears to be non-trivial in general, since the degree of each $T_j(a)$ in a and its conjugates is j, while a priori we only know how to solve $T_1(a) = t_1$:

Lemma (*Thm. 2.25, Lidl & Niederreiter*)

1. *For $a \in \mathbb{F}_{2^n}$, $T_1(a) = 0 \iff a = a_0^2 + a_0$ for two $a_0 \in \mathbb{F}_{2^n}$.*
2. *For $a \in \mathbb{F}_{2^n}$, n odd, $T_1(a) = 1 \iff a = a_0^2 + a_0 + 1$ for two $a_0 \in \mathbb{F}_{2^n}$.*

We shall use (for n odd) a degree-lowering idea and the parameterisation of the count by an associated affine algebraic set.

Preliminary remarks

For $t_1, \ldots, t_l \in \mathbb{F}_2$ we would like to compute a formula as a function of n for

$$F_2(n, t_1, \ldots, t_l) = \#\{a \in \mathbb{F}_{2^n} \mid T_1(a) = t_1, \ldots, T_l(a) = t_l\} \tag{1}$$

This appears to be non-trivial in general, since the degree of each $T_j(a)$ in a and its conjugates is j, while a priori we only know how to solve $T_1(a) = t_1$:

Lemma (*Thm. 2.25, Lidl & Niederreiter*)

1. *For $a \in \mathbb{F}_{2^n}$, $T_1(a) = 0 \iff a = a_0^2 + a_0$ for two $a_0 \in \mathbb{F}_{2^n}$.*
2. *For $a \in \mathbb{F}_{2^n}$, n odd, $T_1(a) = 1 \iff a = a_0^2 + a_0 + 1$ for two $a_0 \in \mathbb{F}_{2^n}$.*

We shall use (for n odd) a degree-lowering idea and the parameterisation of the count by an associated affine algebraic set.

The technique is a natural extension of *“Fibre Products of Supersingular Curves and the Enumeration of Irreducible Polynomials with Prescribed Coefficients”* by Ahmadi, Göloğlu, G., McGuire, Yilmaz, F.F.A., Vol. 42, 2016.

Preliminary remarks

For $t_1, \ldots, t_l \in \mathbb{F}_2$ we would like to compute a formula as a function of n for

$$F_2(n, t_1, \ldots, t_l) = \#\{a \in \mathbb{F}_{2^n} \mid T_1(a) = t_1, \ldots, T_l(a) = t_l\} \qquad (1)$$

This appears to be non-trivial in general, since the degree of each $T_j(a)$ in a and its conjugates is j, while a priori we only know how to solve $T_1(a) = t_1$:

Lemma (*Thm. 2.25, Lidl & Niederreiter*)

1. *For $a \in \mathbb{F}_{2^n}$, $T_1(a) = 0 \iff a = a_0^2 + a_0$ for two $a_0 \in \mathbb{F}_{2^n}$.*
2. *For $a \in \mathbb{F}_{2^n}$, n odd, $T_1(a) = 1 \iff a = a_0^2 + a_0 + 1$ for two $a_0 \in \mathbb{F}_{2^n}$.*

We shall use (for n odd) a degree-lowering idea and the parameterisation of the count by an associated affine algebraic set.

The technique is a natural extension of *"Fibre Products of Supersingular Curves and the Enumeration of Irreducible Polynomials with Prescribed Coefficients"* by Ahmadi, Göloğlu, G., McGuire, Yilmaz, F.F.A., Vol. 42, 2016.

Assume for $2 \leq j \leq l$ that $T_j(x^2 + x)$ is expressible as a multivariate polynomial in traces of lower degree whose arguments are polynomials in x.

Example: $F_2(n, t_1, t_2, t_3, t_4)$

Suppose $t_1 = 0$. Write $a = a_0^2 + a_0$ and for n odd $F_2(n, 0, t_2, t_3, t_4) =$

$$\frac{1}{2}\#\{a_0 \in \mathbb{F}_{2^n} \mid T_2(a_0^2 + a_0) = t_2, T_3(a_0^2 + a_0) = t_3, T_4(a_0^2 + a_0) = t_4\}$$

Example: $F_2(n, t_1, t_2, t_3, t_4)$

Suppose $t_1 = 0$. Write $a = a_0^2 + a_0$ and for n odd $F_2(n, 0, t_2, t_3, t_4) =$

$$
\begin{aligned}
& \frac{1}{2}\#\{a_0 \in \mathbb{F}_{2^n} \mid T_2(a_0^2 + a_0) = t_2, T_3(a_0^2 + a_0) = t_3, T_4(a_0^2 + a_0) = t_4\} \\
= \quad & \frac{1}{2}\#\{a_0 \in \mathbb{F}_{2^n} \mid T_1(a_0^3 + a_0) = t_2, T_1(a_0^5 + a_0) = t_3, \\
& T_2(a_0^3) + T_2(a_0) + T_1(a_0^3)T_1(a_0) + T_1(a_0^7 + a_0^5 + a_0^3) = t_4\}
\end{aligned}
$$

Example: $F_2(n, t_1, t_2, t_3, t_4)$

Suppose $t_1 = 0$. Write $a = a_0^2 + a_0$ and for n odd $F_2(n, 0, t_2, t_3, t_4) =$

$$\begin{aligned}
& \frac{1}{2}\#\{a_0 \in \mathbb{F}_{2^n} \mid T_2(a_0^2 + a_0) = t_2, T_3(a_0^2 + a_0) = t_3, T_4(a_0^2 + a_0) = t_4\} \\
= \quad & \frac{1}{2}\#\{a_0 \in \mathbb{F}_{2^n} \mid T_1(a_0^3 + a_0) = t_2, T_1(a_0^5 + a_0) = t_3, \\
& T_2(a_0^3) + T_2(a_0) + T_1(a_0^3)T_1(a_0) + T_1(a_0^7 + a_0^5 + a_0^3) = t_4\} \\
= \quad & \frac{1}{8}\sum_{r_1, r_2 \in \mathbb{F}_2} \#\{(a_0, a_1, a_2) \in (\mathbb{F}_{2^n})^3 \mid T_1(a_0^3 + a_0) = t_2, T_1(a_0^5 + a_0) = t_3, \\
& a_1^2 + a_1 + r_1 = a_0,\ a_2^2 + a_2 + r_2 = a_0^3, \\
& T_1\left(a_2^3 + a_2 + a_1^3 + a_1 + a_0^7 + a_0^5 + r_1 r_2 + r_2 + (r_1 + r_2)\binom{n}{2}\right) = t_4\}
\end{aligned}$$

Example: $F_2(n, t_1, t_2, t_3, t_4)$

Suppose $t_1 = 0$. Write $a = a_0^2 + a_0$ and for n odd $F_2(n, 0, t_2, t_3, t_4) =$

$$
\begin{aligned}
& \frac{1}{2}\#\{a_0 \in \mathbb{F}_{2^n} \mid T_2(a_0^2 + a_0) = t_2,\, T_3(a_0^2 + a_0) = t_3,\, T_4(a_0^2 + a_0) = t_4\} \\
= \quad & \frac{1}{2}\#\{a_0 \in \mathbb{F}_{2^n} \mid T_1(a_0^3 + a_0) = t_2,\, T_1(a_0^5 + a_0) = t_3, \\
& T_2(a_0^3) + T_2(a_0) + T_1(a_0^3)T_1(a_0) + T_1(a_0^7 + a_0^5 + a_0^3) = t_4\} \\
= \quad & \frac{1}{8}\sum_{r_1, r_2 \in \mathbb{F}_2} \#\{(a_0, a_1, a_2) \in (\mathbb{F}_{2^n})^3 \mid T_1(a_0^3 + a_0) = t_2,\, T_1(a_0^5 + a_0) = t_3, \\
& a_1^2 + a_1 + r_1 = a_0,\ a_2^2 + a_2 + r_2 = a_0^3, \\
& T_1\left(a_2^3 + a_2 + a_1^3 + a_1 + a_0^7 + a_0^5 + r_1 r_2 + r_2 + (r_1 + r_2)\binom{n}{2}\right) = t_4\} \\
= \quad & \frac{1}{64}\sum_{r_1, r_2 \in \mathbb{F}_2} \#\{(a_0, a_1, a_2, a_3, a_4, a_5) \in (\mathbb{F}_{2^n})^6 \mid a_3^2 + a_3 + t_2 = a_0^3 + a_0, \\
& a_4^2 + a_4 + t_3 = a_0^5 + a_0,\ a_1^2 + a_1 + r_1 = a_0,\ a_2^2 + a_2 + r_2 = a_0^3, \\
& a_5^2 + a_5 + t_4 = a_2^3 + a_2 + a_1^3 + a_1 + a_0^7 + a_0^5 + r_1 r_2 + r_2 + (r_1 + r_2)\binom{n}{2}\}
\end{aligned}
$$

General strategy

For each $2 \leq j \leq l$ do the following:

- Expand $T_j(a_{j,0}^2 + a_{j,0} + r_{j,0})$ in terms of lower degree trace functions.
- If not of the form $T_1(\cdot)$ then pick an argument of a trace function featuring in a non-linear term, say $f(a_{j,0})$, and introduce $a_{j,1}$ and its linear trace $r_{j,1}$ and write $a_{j,1}^2 + a_{j,1} + r_{j,1} = f(a_{j,0})$ and expand.
- Introduce new variables $a_{j,2}, \ldots, a_{j,s_j-1}$ and their traces $r_{j,2}, \ldots, r_{j,s_j-1}$ as required until the original expression has been linearised, i.e., is of the form $T_1(f_{j,\mathbf{r}_j}(a_{j,0}, \ldots, a_{j,s_j-1})) = t_j$.

General strategy

For each $2 \leq j \leq l$ do the following:

- Expand $T_j(a_{j,0}^2 + a_{j,0} + r_{j,0})$ in terms of lower degree trace functions.
- If not of the form $T_1(\cdot)$ then pick an argument of a trace function featuring in a non-linear term, say $f(a_{j,0})$, and introduce $a_{j,1}$ and its linear trace $r_{j,1}$ and write $a_{j,1}^2 + a_{j,1} + r_{j,1} = f(a_{j,0})$ and expand.
- Introduce new variables $a_{j,2}, \ldots, a_{j,s_j-1}$ and their traces $r_{j,2}, \ldots, r_{j,s_j-1}$ as required until the original expression has been linearised, i.e., is of the form $T_1(f_{j,\mathbf{r}_j}(a_{j,0}, \ldots, a_{j,s_j-1})) = t_j$.

Let U be the union of all auxiliary variable equations, $s = \#U \leq \sum_{j=2}^{l} s_j$, $a_0, \ldots, a_{s-1}$ be the variables & $\mathbf{r} = (r_0, \ldots, r_{s-1})$ their possible linear traces.

General strategy

For each $2 \leq j \leq l$ do the following:

- Expand $T_j(a_{j,0}^2 + a_{j,0} + r_{j,0})$ in terms of lower degree trace functions.
- If not of the form $T_1(\cdot)$ then pick an argument of a trace function featuring in a non-linear term, say $f(a_{j,0})$, and introduce $a_{j,1}$ and its linear trace $r_{j,1}$ and write $a_{j,1}^2 + a_{j,1} + r_{j,1} = f(a_{j,0})$ and expand.
- Introduce new variables $a_{j,2}, \ldots, a_{j,s_j-1}$ and their traces $r_{j,2}, \ldots, r_{j,s_j-1}$ as required until the original expression has been linearised, i.e., is of the form $T_1(f_{j,\mathbf{r}_j}(a_{j,0}, \ldots, a_{j,s_j-1})) = t_j$.

Let U be the union of all auxiliary variable equations, $s = \#U \leq \sum_{j=2}^{l} s_j$, $a_0, \ldots, a_{s-1}$ be the variables & $\mathbf{r} = (r_0, \ldots, r_{s-1})$ their possible linear traces.

The l trace equations are parameterised by introducing a final variable a_{s_j} and writing $a_{s_j}^2 + a_{s_j} + t_j = f_{j,\mathbf{r}}(a_0, \ldots, a_{s-1})$, giving a system of $l + s - 1$ equations in $l + s$ variables.

General strategy

For each $2 \leq j \leq l$ do the following:

- Expand $T_j(a_{j,0}^2 + a_{j,0} + r_{j,0})$ in terms of lower degree trace functions.
- If not of the form $T_1(\cdot)$ then pick an argument of a trace function featuring in a non-linear term, say $f(a_{j,0})$, and introduce $a_{j,1}$ and its linear trace $r_{j,1}$ and write $a_{j,1}^2 + a_{j,1} + r_{j,1} = f(a_{j,0})$ and expand.
- Introduce new variables $a_{j,2}, \ldots, a_{j,s_j-1}$ and their traces $r_{j,2}, \ldots, r_{j,s_j-1}$ as required until the original expression has been linearised, i.e., is of the form $T_1(f_{j,\mathbf{r}_j}(a_{j,0}, \ldots, a_{j,s_j-1})) = t_j$.

Let U be the union of all auxiliary variable equations, $s = \#U \leq \sum_{j=2}^{l} s_j$, $a_0, \ldots, a_{s-1}$ be the variables & $\mathbf{r} = (r_0, \ldots, r_{s-1})$ their possible linear traces.

The l trace equations are parameterised by introducing a final variable a_{s_j} and writing $a_{s_j}^2 + a_{s_j} + t_j = f_{j,\mathbf{r}}(a_0, \ldots, a_{s-1})$, giving a system of $l + s - 1$ equations in $l + s$ variables.

Equations may feature $\binom{n}{j}$ of period $2^{1+\lfloor \log_2 j \rfloor}$ mod n, so let $\overline{n} \in \{1, 3, 5, \ldots, 2^{1+\lfloor \log_2 l \rfloor} - 1\}$. $\forall n \equiv \overline{n} \pmod{2^{1+\lfloor \log_2 l \rfloor}}$ with $n \geq l$ we have:

$$F_2(n, t_1, \ldots, t_l) = \frac{1}{2^{l+s}} \sum_{\mathbf{r} \in (\mathbb{F}_2)^s} \#U_{\mathbf{r},\overline{n}}(\mathbb{F}_{2^n}).$$

Example: $F_2(n, t_1, t_2, t_3, t_4)$

For $p \in \mathbb{Z}[X]$ let $\rho_n(p)$ denote the sum of the n-th powers of the roots of p, and let

$$\begin{aligned}
p_{2,1} &= X^2 + 2X + 2, \\
p_{2,2} &= X^2 + 2, \\
p_{4,1} &= X^4 + 2X^3 + 2X^2 + 4X + 4, \\
p_{8,1} &= X^8 + 4X^7 + 6X^6 + 4X^5 + 2X^4 + 8X^3 + 24X^2 + 32X + 16, \\
p_{8,2} &= X^8 + 2X^6 + 4X^5 + 2X^4 + 8X^3 + 8X^2 + 16.
\end{aligned}$$

Example: $F_2(n, t_1, t_2, t_3, t_4)$

For $p \in \mathbb{Z}[X]$ let $\rho_n(p)$ denote the sum of the n-th powers of the roots of p, and let

$$\begin{aligned}
p_{2,1} &= X^2 + 2X + 2,\\
p_{2,2} &= X^2 + 2,\\
p_{4,1} &= X^4 + 2X^3 + 2X^2 + 4X + 4,\\
p_{8,1} &= X^8 + 4X^7 + 6X^6 + 4X^5 + 2X^4 + 8X^3 + 24X^2 + 32X + 16,\\
p_{8,2} &= X^8 + 2X^6 + 4X^5 + 2X^4 + 8X^3 + 8X^2 + 16.
\end{aligned}$$

Theorem (*G. 2017*)

For $n \geq 4$ we have:

$$\begin{aligned}
F_2(n,0,0,0,0) &= 2^{n-4} - \frac{1}{16}\big(4\rho_n(p_{2,1}) + 3\rho_n(p_{2,2}) + \rho_n(p_{4,1}) + \rho_n(p_{8,1}) + \rho_n(p_{8,2})\big),\\
F_2(n,0,0,0,1) &= 2^{n-4} - \frac{1}{16}\big(-\rho_n(p_{2,2}) + \rho_n(p_{4,1}) - \rho_n(p_{8,1}) - \rho_n(p_{8,2})\big),\\
F_2(n,0,0,1,0) &= 2^{n-4} - \frac{1}{16}\big(-2\rho_n(p_{2,1}) + \rho_n(p_{2,2}) - \rho_n(p_{4,1}) + \rho_n(p_{8,1}) - \rho_n(p_{8,2})\big),\\
F_2(n,0,0,1,1) &= 2^{n-4} - \frac{1}{16}\big(2\rho_n(p_{2,1}) - 3\rho_n(p_{2,2}) - \rho_n(p_{4,1}) - \rho_n(p_{8,1}) + \rho_n(p_{8,2})\big).
\end{aligned}$$

Example: $F_2(n, t_1, t_2, t_3, t_4, t_5)$

Let

$$
\begin{aligned}
\overline{p}_{2,1} &= p_{2,1}(-X), \\
p_{4,2} &= X^4 + 2X^2 + 4, \\
\overline{p}_{8,2} &= p_{8,2}(-X), \\
p_{8,3} &= X^8 + 2X^7 + 2X^6 - 4X^4 + 8X^2 + 16X + 16.
\end{aligned}
$$

Example: $F_2(n, t_1, t_2, t_3, t_4, t_5)$

Let

$$\begin{aligned}
\overline{p}_{2,1} &= p_{2,1}(-X),\\
p_{4,2} &= X^4 + 2X^2 + 4,\\
\overline{p}_{8,2} &= p_{8,2}(-X),\\
p_{8,3} &= X^8 + 2X^7 + 2X^6 - 4X^4 + 8X^2 + 16X + 16.
\end{aligned}$$

Theorem (*G. 2017*)

For $n \geq 5$ we have:

$$\begin{aligned}
F_2(n,0,0,0,0,0) &= 2^{n-5} - \frac{1}{32}\big(7\rho_n(p_{2,1}) + 2\rho_n(\overline{p}_{2,1}) + 4\rho_n(p_{2,2}) + 5\rho_n(p_{4,1})\\
&\quad +3\rho_n(p_{4,2}) + 2\rho_n(p_{8,1}) + \rho_n(p_{8,2}) + \rho_n(\overline{p}_{8,2}) + \rho_n(p_{8,3})\big),\\
F_2(n,0,0,0,1,0) &= 2^{n-5} - \frac{1}{32}\big(3\rho_n(p_{2,1}) + 2\rho_n(\overline{p}_{2,1}) + \rho_n(p_{4,1}) - \rho_n(p_{4,2})\\
&\quad -2\rho_n(p_{8,1}) - \rho_n(p_{8,2}) - \rho_n(\overline{p}_{8,2}) + \rho_n(p_{8,3})\big),\\
F_2(n,0,0,0,0,1) &= 2^{n-5} - \frac{1}{32}\big(\rho_n(p_{2,1}) - 2\rho_n(\overline{p}_{2,1}) + 2\rho_n(p_{2,2}) - 3\rho_n(p_{4,1})\\
&\quad -3\rho_n(p_{4,2}) + \rho_n(p_{8,2}) - \rho_n(\overline{p}_{8,2}) - \rho_n(p_{8,3})\big),\\
F_2(n,0,0,0,1,1) &= 2^{n-5} - \frac{1}{32}\big(-3\rho_n(p_{2,1}) - 2\rho_n(\overline{p}_{2,1}) - 2\rho_n(p_{2,2}) + \rho_n(p_{4,1})\\
&\quad +\rho_n(p_{4,2}) - \rho_n(p_{8,2}) + \rho_n(\overline{p}_{8,2}) - \rho_n(p_{8,3})\big).
\end{aligned}$$

Computing $T_l(\alpha - \beta)$

We recall Newton's identities over $\mathbb{Z}$ with indeterminates $\alpha_1, \ldots, \alpha_n$. Working in the ring of symmetric functions, for all $l \geq 1$ and $n \geq l$ we have

$$l\, T_l(\alpha) = \sum_{k=1}^{l} (-1)^{k-1} T_{l-k}(\alpha) T_1(\alpha^k).$$

In order to use the argument $\alpha - \beta$ we need to work instead in the ring $\mathbb{Z}[\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n]$ and with the ring of multisymmetric functions in two variables. Abusing notation slightly, we have:

$$l\, T_l(\alpha - \beta) = \sum_{k=1}^{l} (-1)^{k-1} T_{l-k}(\alpha - \beta) T_1((\alpha - \beta)^k).$$

- Want r.h.s. to have all coefficients divisible by l so that expression for $T_l(\alpha - \beta)$ is over $\mathbb{Z}$, and thus valid in positive characteristic.
- Rewriting any trace occurring to a power higher than 1 using Newton's identities leads to such a r.h.s. for $2 \leq l \leq 7$, but not $l \geq 8$.
- If it worked then could compute algebraic sets for *any number of coefficients prescribed in any positions*.

Open problems for $F_2(n, t_1, \ldots, t_l)$

For $F_2(n, t_1, \ldots, t_6)$ and n odd we obtained ab. irred. curves, all of genus 50.

For $F_2(n, t_1, \ldots, t_7)$ and n odd we obtained ab. irred. curves, all of genus 58.

Problems:

- What are their zeta functions?
- Is there a method/formulae for all $l \leq 7$ cases for n even?
- Can one compute $T_l(\alpha + \beta) \bmod 2$ for any (or all) $l \geq 8$?

Overview

The problem

New results over $\mathbb{F}_2$

The main algorithm

Summary & open problems

The main algorithm

Let $q = p^r$, $l < p$ and $n \geq l$ coprime to p. Degree lowering easy since

$$T_l(\alpha - \beta) = \frac{1}{l} \sum_{k=1}^{l} (-1)^{k-1} T_{l-k}(\alpha - \beta) T_1((\alpha - \beta)^k),$$

so all are expressible in terms of T_1's only whose arguments are $\alpha^c \beta^d$.

The method is the same as before, except need only consider $\overline{n} \in \{1, \ldots, p-1\}$ and final equations are

$$a_{s_j}^q - a_{s_j} + t_j/\overline{n} = f_{j,\mathbf{r}}(a_0, \ldots, a_{s-1}),$$

and we have

$$F_q(n, t_1, \ldots, t_l) = \frac{1}{q^{l+s}} \sum_{\mathbf{r} \in (\mathbb{F}_q)^s} \#U_{\mathbf{r},\overline{n}}(\mathbb{F}_{q^n}).$$

The same approach works for $F_q(n, t_{l_0}, \ldots, t_{l_{m-1}})$, *for which any subset of coefficients are prescribed.*

The main algorithm

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ & let $\overline{\mathbb{Z}}$ be the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$.

Theorem (*G. 2017*)

For every $q = p^r$, $1 \leq l_0 < \cdots < l_{m-1} < p$, $(t_{l_0}, \ldots, t_{l_{m-1}}) \in (\mathbb{F}_q)^m$ and $\overline{n} \in \{1, \ldots, p-1\}$ there exists $\alpha_1, \ldots, \alpha_N \in \overline{\mathbb{Z}}$ and $c_1, \ldots, c_N \in \mathbb{Q}$ such that for all $n \equiv \overline{n} \pmod{p}$ with $n \geq l_{m-1}$ one has

$$F_q(n, t_{l_0}, \ldots, t_{l_{m-1}}) = \frac{1}{q^m} \sum_{i=1}^{N} c_i \alpha_i^n.$$

The main algorithm

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ & let $\overline{\mathbb{Z}}$ be the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$.

Theorem (*G. 2017*)

For every $q = p^r$, $1 \leq l_0 < \cdots < l_{m-1} < p$, $(t_{l_0}, \ldots, t_{l_{m-1}}) \in (\mathbb{F}_q)^m$ and $\overline{n} \in \{1, \ldots, p-1\}$ there exists $\alpha_1, \ldots, \alpha_N \in \overline{\mathbb{Z}}$ and $c_1, \ldots, c_N \in \mathbb{Q}$ such that for all $n \equiv \overline{n} \pmod{p}$ with $n \geq l_{m-1}$ one has

$$F_q(n, t_{l_0}, \ldots, t_{l_{m-1}}) = \frac{1}{q^m} \sum_{i=1}^{N} c_i \alpha_i^n.$$

Conjecture

For every $q = p^r$, $1 \leq l_0 < \cdots < l_{m-1} < p$, $(t_{l_0}, \ldots, t_{l_{m-1}}) \in (\mathbb{F}_q)^m$ and $\overline{n} \in \{1, \ldots, p-1\}$ there exists $\alpha_1, \ldots, \alpha_N \in \overline{\mathbb{Z}}$, all of norm $\sqrt{q}$, $d_1, \ldots, d_N \in \mathbb{Z}$ and an integer $s \geq 0$ such that for all $n \equiv \overline{n} \pmod{p}$ with $n \geq l_{m-1}$ one has

$$F_q(n, t_{l_0}, \ldots, t_{l_{m-1}}) = \frac{1}{q^m}\left(q^n + \frac{1}{q^s} \sum_{i=1}^{N} d_i \alpha_i^n\right) = q^{n-m} + O(q^{n/2-m}).$$

Overview

The problem

New results over $\mathbb{F}_2$

The main algorithm

Summary & open problems

Summary and open problems

- The prescribed traces enumeration problem should be regarded as an algorithmic problem.
- Proposed algorithms which parameterise such sets by associating to them certain affine algebraic sets.
- Although computing these algebraic sets is easy, computing their characteristic values is in general non-trivial.

Summary and open problems

- The prescribed traces enumeration problem should be regarded as an algorithmic problem.
- Proposed algorithms which parameterise such sets by associating to them certain affine algebraic sets.
- Although computing these algebraic sets is easy, computing their characteristic values is in general non-trivial.

Open problems (10 proposed in the paper):

- Can one obviate the failure of Newton's identities by working p-adically and in Galois rings, circumventing the $l < p$ constraint and allowing exact counts for *any number of coefficients prescribed in any positions*?
- By analysing properties of these algebraic sets can one prove interesting existence results?

Preprint and code

“On the Enumeration of Irreducible Polynomials over $\mathbb{F}_q$ with Prescribed Coefficients”

- Preprint is available from `https://arxiv.org/abs/1610.06878`
- All interesting Maple and Magma code is available from `https://github.com/robertgranger/CountingIrreducibles`