Methods for primitive and normal polynomials

Stephen D Cohen

University of Glasgow

Fields-Carleton Finite Fields Workshop
Ottawa, 21 July, 2010

Preliminaries

Throughout $\mathbb{F}_q$ is the finite field of cardinality q

- q is a power of the characteristic, the prime p

$\mathbb{F}_{q^n}$ is the extension of $\mathbb{F}_q$ of degree n

Denote the $\mathbb{F}_q$-trace and norm of elements γ in $\mathbb{F}_{q^n}$ by
$\mathrm{Tr}(\gamma), \ \mathrm{Nm}(\gamma)$

The trace of $\gamma \in \mathbb{F}_{q^n}$ over the ground field $\mathbb{F}_p$ is denoted by $\mathrm{Tr}_0(\gamma)$

Polynomials are monic:
$f(x) = x^n + a_1x^{n-1} + \cdots a_mx^{n-m} + \cdots + a_n \in \mathbb{F}_q[x]$
$a_m = m\text{th coefficient}$

For $K \in \mathbb{F}_q[x]$, $|K| = q^{\deg(K)}$

$W(m) = 2^{\omega(m)} =$ no. of square-free divisors of m
($\omega(m)$ is the number of distinct prime factors of m)

Primitive elements and polynomials

Definitions 1

A primitive element of $\mathbb{F}_{q^n}$ is a generator of the multiplicative cyclic group $\mathbb{F}_{q^n}^*$ (of cardinality $q^n - 1$)

A primitive polynomial of degree n over $\mathbb{F}_q$ is a (monic irreducible) polynomial whose roots are all primitive elements of $\mathbb{F}_{q^n}$

- The number of primitive elements in $\mathbb{F}_{q^n}$ is $\phi(q^n - 1)$, where ϕ is Euler's function
- For $k \in \mathbb{N}$, set $\theta(k) = \frac{\phi(k)}{k} = \prod_{\text{prime } l | k} (1 - \frac{1}{l})$
- The proportion of primitive elements in $\mathbb{F}_{q^n}^*$ is $\theta(q^n - 1)$

Normal/free elements and polynomials

Definitions 2

A normal polynomial of degree n over $\mathbb{F}_q$ is an irreducible polynomial whose roots $\{\alpha, \alpha^q, \dots \alpha^{q^{n-1}}\}$ form a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$
A root of such a normal polynomial is a free element of $\mathbb{F}_{q^n}$

- For a polynomial $K \in \mathbb{F}_q[x]$ the polynomial Euler's function is

$$\phi(K) = |K| \prod_{\text{irred } P|K} (1 - \frac{1}{|P|})$$

- The number of free elements is $\phi(x^n - 1)$
- For $K \in \mathbb{F}_q[x]$, define $\theta(K) = \dfrac{\phi(K)}{|K|}$
- The proportion of free elements in $\mathbb{F}_{q^n}$ is $\theta(x^n - 1)$

Formal products

For notational convenience (only), for some divisor k of $q^n - 1$ and some polynomial factor of $x^n - 1 \in \mathbb{F}_q[x]$ we consider a formal product kK Later this may be a contracted to a single symbol k

In this spirit, for such a formal product kK, write

- $\phi(kK) = \phi(k)\phi(K)$
- $\theta(kK) = \frac{\phi(kK)}{k|K|}$
- $W(kK) = W(k)W(K)$

- These may be contracted simply to $\phi(k)$, $\theta(k)$ and $W(k)$, respectively

Existence problems to be discussed

Problem 1 (PFNT)

Primitive normal polynomials with specified trace and norm

Given $n \geq 3$, does there exist an element $\alpha \in \mathbb{F}_{q^n}$ that is simultaneously primitive and free over $\mathbb{F}_q$ with specified $\mathbb{F}_q$-trace and norm (necessarily a primitive element of $\mathbb{F}_q$)?

See: Cohen (2000), $n \geq 5$; Cohen-Huczynska (2003), $n = 4, 3$

Problem 2 (SPNBT)

The strong primitive normal basis problem

Does there exist a primitive element $\alpha \in \mathbb{F}_{q^n}$ such that both α and $1/\alpha$ are free over $\mathbb{F}_q$?

See: Cohen-Huczynska (2010)

Problem 3 (Pm)

Primitive polynomials with prescribed coefficient

Given $1 \leq m < n$ and $a \in \mathbb{F}_q$, does there exist a primitive polynomial over $\mathbb{F}_q$ with m-th coefficient a?

See: Cohen (2006), $n \geq 9$ and $n \leq 4$; Cohen-Prešern (2006, 2008), $5 \leq n \leq 8$

Problem 4 (PFm)

Primitive normal polynomials with prescribed coefficient

Given $1 \leq m < n$ and $a \in \mathbb{F}_q$, does there exist a primitive normal polynomial over $\mathbb{F}_q$ with m-th coefficient a?

See:
Fan-Wang (2009), $n \geq 15$, Wang-Fan-Wang (2010), $9 \leq n \leq 14$

Definition 3
For any divisor k of $q^n - 1$, a k-free element γ of $\mathbb{F}_{q^n}^*$ is such that $\gamma = \beta^d$ $(\beta \in \mathbb{F}_{q^n},\ d \mid k)$ implies $d = 1$

- A primitive element of $\mathbb{F}_{q^n}$ is $(q^n - 1)$-free

Application to irreducibility
Given any pair $(q, n) \neq (2, 6)$, there exists a prime divisor l_n of $q^n - 1$ that does not divide $q^d - 1$ for any $d < n$ Zsigmondy

Hence: if $\gamma \in \mathbb{F}_{q^n}$ is l_n-free then its minimal polynomial is irreducible of degree n **Zsigmondy criterion**

Can be used to resolve Problem Im (= irreducible analogue of Problem Pm) Any other applications?

Characteristic function for $\gamma \in \mathbb{F}_{q^n}$ to be k-free

$$\Lambda(k) := \theta(k) \sum_{d|k} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi_d(\gamma) = \begin{cases} 1, & \gamma \ k\text{-free} \\ 0, & \text{otherwise} \end{cases}$$

- χ_d: multiplicative character of $\mathbb{F}_{q^n}$ of order d
- $\sum_{\chi_d}$: sum over all such characters
- $\theta(k) := \frac{\phi(k)}{k}$

Write $\Lambda(k)$ as $\theta(k) \int_{d|k} \chi_d(\gamma)$

K-free elements of $\mathbb{F}_{q^n}$

Given a polynomial $H = \sum H_i x^i \in \mathbb{F}_q[x]$, $H^\sigma = \sum H_i x^{q^i}$

The Order of $\gamma \in \mathbb{F}_{q^n}$ is the "least" factor K of $x^n - 1$ such that $K^\sigma(\gamma) = 0$. If γ has Order K then $\gamma = H^\sigma(\beta)$ for some $\beta \in \mathbb{F}_{q^n}$, where $H = (x^n - 1)/K$

Definition 4

For any factor K of $x^n - 1$, $\gamma \in \mathbb{F}_{q^n}^*$ is K-free if

$\gamma = H^\sigma(\beta)$ $(\beta \in \mathbb{F}_{q^n},\ H \mid K)$ $\implies$ $H = 1$

- $\gamma \in \mathbb{F}_{q^n}$ is free $\iff$ it is $x^n - 1$-free

Characteristic function for $\gamma \in \mathbb{F}_{q^n}$ to be K-free

$$\Lambda(K) := \theta(K) \sum_{D|K} \frac{\mu(D)}{\phi(D)} \sum_{\delta_D \in \Delta_D} \psi(\delta_D \gamma) = \begin{cases} 1, & \gamma \ K\text{-free} \\ 0, & \text{otherwise} \end{cases}$$

- $\psi = \psi_n =$ canonical additive character of $\mathbb{F}_{q^n}$, i.e.

$$\psi(\alpha) = \exp\left(\frac{2\pi \mathrm{Tr}_0(\alpha)}{p}\right)$$

- $\Delta_D \subseteq \mathbb{F}_{q^n}$ is such that
  $\{\psi(\delta_D \gamma) : \delta_D \in \Delta_D\} =$ set of all characters of Order D

Write $\Lambda(K)$ as $\theta(K) \int_{D|K} \psi(\delta_D \gamma)$

Basic character sum estimate

ψ = canonical additive character on $\mathbb{F}_{q^n}$
χ = a multiplicative character on $\mathbb{F}_{q^n}$ of order $d > 1$

Lemma

Let $h(x) \in \mathbb{F}_{q^n}$ be a polynomial (rational function) of degree D. Then

$$\left| \sum_{\alpha \in \mathbb{F}_{q^n}} \psi(h(\alpha))\chi(\alpha) \right| \leq Dq^{n/2}$$

- Referred to as the Weil bound

Definitive reference?

Character sum expression in Problem 1 (PFTN)

Given $k|q^n - 1, K|x^n - 1,\ a, b \in \mathbb{F}_q$

$N_{k,K}(a,b) :=$ no. of kK-free $\gamma \in \mathbb{F}_{q^n}$ with norm a, trace b.

Then $q(q-1)N_{k,K}(a,b) = \theta(kK)(q^n + S)$ where $S =$

$$\int_{d|k} \int_{D|K} \sum_{\nu \in \mathbb{F}_q^*} \sum_{c \in \mathbb{F}_q} \bar{\nu}(b)\bar{\lambda}(ac) \sum_{\alpha \in \mathbb{F}_{q^n}} (\chi_d \nu)(\alpha)\psi((\delta_D + c)\alpha)$$

Here

- $\nu =$ multiplicative character on $\mathbb{F}_q$
- $\lambda =$ canonical additive character on $\mathbb{F}_q$

Thus

$q(q-1)N_{k,K}(a,b) = \theta(kK)(q^n + S)$ where

$$S = \int_{d|k} \int_{D|K} \sum_{\nu \in \mathbb{F}_q^*} \sum_{c \in \mathbb{F}_q} C(c,\nu)(\nu) G_n(\chi\nu) + \cdots$$

Here

- $G_n(\chi) = \sum_{\alpha \in \mathbb{F}_{q^n}} \psi(\alpha)\chi(\alpha) =$ Gauss Sum over $\mathbb{F}_{q^n}$
- $|C(c,\nu)| \leq 1$
- $|G_n(\chi_d) \leq q^{n/2} \qquad (d > 1)$

- Easily $S \leq W(kK)q^{\frac{n}{2}+2}$
- Recall $S = \int_{d|k}\int_{D|K}\sum_{\nu\in\mathbb{F}_q^*}\sum_{c\in\mathbb{F}_q}\bar{\nu}(b)\bar{\lambda}(ac)\sum_{\alpha\in\mathbb{F}_{q^n}}(\chi_d\nu)(\alpha)\psi((\delta_D+c)\alpha)$

  Typically, replace δ_D by $c\delta_D$ and α by $\alpha/(c(\delta_D+1))$ to yield $C(\nu,c) = C_1(\nu)G_1(\nu)$, $|C_1(\nu)| \leq 1$:

  so $|S| \leq W(kK)q^{\frac{n+3}{2}}$

- Use $\left|\sum_{\substack{\alpha\in\mathbb{F}_{q^n}\\ \mathrm{Tr}(\alpha)=\mathrm{Nm}(\alpha)=1}}\chi(\alpha)\right| \leq nq^{(n-2)/2}$ Katz, 1993

  to yield

$$|S| \leq nW(k)q^{\frac{n}{2}+1}; \quad K=1, a=b=1$$

Katz result (+ special considerations) vital for $n=3,4$.
Improvement by Moisio and Wan (2010) ...

Character sum expression in Problem 2 (SPNBT)

Let $Q_n = \frac{q^n-1}{(q-1)\gcd(n,q-1)}$. It suffices to show that the existence of $\alpha \in \mathbb{F}_{q^n}$ which is Q_n-free such that both α and $1/\alpha$ are free

Given $k|Q_n, K_1|x^n-1, K_2|y^n-1$, let $N(k, K_1, K_2)$ be the number of $\alpha \in \mathbb{F}_{q^n}$ with α k-free and K_1-free and $1/\alpha$ K_2-free.

$$N(k, K_1, K_2) = \theta(kK_1K_2) \int_{d|k} \int_{D_1|K_1} \int_{D_2|K_2} K(\delta_{D_1}, \delta_{D_2}; \chi_d)$$

where

$$K(\alpha, \beta; \chi) = \sum_{\gamma \in \mathbb{F}_{q^n}^*} \psi(\alpha\gamma + \beta\gamma^{-1})\chi(\gamma)$$ **generalized Kloosterman sum**

Since

$$N(k, K_1, K_2) = \theta(kK_1K_2) \int_{d|k} \int_{D_1|K_1} \int_{D_2|K_2} K(\delta_{D_1}, \delta_{D_2}; \chi_d)$$

then

$$\left| \frac{N(k, K_1, K_2)}{\theta(kK_1K_2)} - q^n \right| \leq 2W(kK_1K_2)q^{n/2}$$

- In this problem, the further ingredient required is not an improvement in the character sum estimate but skill in handling the "sieving techniques" available (see later)

Prescribing the mth coefficient $(m < p)$

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_m x^{n-m} + \cdots + a_n \in \mathbb{F}_q[x]$$

$a_m = (-1)^m \sigma_m$ is the mth coefficient $(1 \leq m \leq n)$

Write $s_m = \sum_{\gamma \text{ a root of } f} \gamma^m$; $\sigma_m = m$th symmetric fn of roots

Lemma (Newton's identities)

$$ra_r + a_{r-1}s_1 + a_{r-2}s_2 + \cdots + s_r = 0, \; r \leq n$$

- **Specifying the first m coefficients $(m < p)$**
  $\{a_1, \ldots, a_m\}$ can be specified by specifying $\{s_1, \ldots s_m\}$
- **zero criterion for specifying $a_m = a$ $(m < p)$**
  Set $s_t = 0$ $(t \leq m^* := \lfloor m/2 \rfloor)$, $s_m = -ma$. Then $a_m = a$.
- **z criterion for specifying $a_m = a$, $m(< p)$ even**
  Set $s_t = 0$, $t < m^*$, $s_{m^*} = z(\in \mathbb{F}_q)$, $s_m = z^2 - ma$.
  Then $a_m = a$.

Character sum expression in Problem 3 (Pm), $m < p$

$N_m(k) :=$ No. of k-free $\gamma \in \mathbb{F}_{q^n}$ with $a_m = a$

By the **zero criterion**

$$q^{m^*+1} N_m(k) = \theta(k) \int_{d|k} \sum_{\substack{c_t \in \mathbb{F}_q \\ t \leq m^* \text{ or } t=m}} \psi(-c_m a) S_n(c_t \gamma^t, \chi_d),$$

where, for $h(x) \in \mathbb{F}_{q^n}[x]$, $S_n(h, \chi) = \sum_{\alpha \in \mathbb{F}_{q^n}} \psi(h(\alpha))\chi(\alpha)$

- Generally $|S_n(c_t \gamma^t, \chi)| \leq t q^{n/2}$
- So $\left| \dfrac{N_m(k)}{q^{n/2}\theta(k)} - q^{\frac{n}{2} - m^* - 1} \right| \leq mW(k)$

- When $a \neq 0$, squeezing $S_1(-cax^m, \hat{\chi_d})$ into the expression for $N_m(k)$ yields

$$\left| \frac{N_m(k)}{q^{(n+1)/2}\theta(k)} - q^{\frac{n}{2}-m^*-\frac{1}{2}} \right| \leq m' m W(k), \quad m' = (m, q-1) \; (a \neq 0)$$

Useful when $n = 5, m = 3; n/2 - m^* - 1/2 = 1$

- Alternatively, when m is even, using z-criterion and averaging over $z \in \mathbb{F}_q$

$$\left| \frac{N_m(k)}{q^{(n+1)/2}\theta(k)} - q^{\frac{n-m-1}{2}} \right| \leq m W(k)$$

Useful when $n = 8, m = 4; (n - m - 1)/2 = 3/2$

All these estimates for $N_m(k)$ are less useful (even useless!) as m approaches n (even assuming $n < p$)

- In practice, use them for $m \leq (n+1)/2$
- If $m > (n+1)/2$ fix constant term as primitive $b \in \mathbb{F}_q$ and look for a (monic) primitive polynomial of the reciprocal form $b^{-1}x^n f(1/x)$ with prescribed $(n-m)$th coefficient a/b. If now $N_m(k) :=$ No. of k-free $\gamma \in \mathbb{F}_{q^n}$ with $a_m = a$ and $a_0 = b$ then

$$\left| \frac{N_m(k)}{q^{n/2}\theta(k)} - q^{\frac{n}{2}-m^*-2} \right| \leq mW(k)$$

......

Sieving

In any problem let $N(k)$ denote the number of relevant k-free $\alpha \in \mathbb{F}_{q^n}$. Here k is a formal divisor of the relevant formal product $q^n - 1$ or $(q^n - 1)(x^n - 1)$, etc.

- $N(k)$ is unaffected if k is replaced by its "square-free" radical

Take a set of complementary divisors, i.e. a set $\{k_1, \ldots, k_r\}$ of formal divisors of k such that, for $i \neq j$, $\gcd(k_i, k_j) = k_0$ (the core) and (the radical of) the lcm of $\{k_1, \ldots, k_r\}$ is (the radical of) k

Lemma (Sieving Lemma)

$$N(k) \geq \sum_{i=1}^{r} N(k_i) - (r-1)N(k_0)$$

- In practice, usually $k_i = k_0 p_i$ where p_i is a prime dividing k; thus a prime number or irreducible polynomial $\{p_1, \ldots, p_r\}$ can be a mixture of both types of prime
- k_0 is the core; $p_1, \ldots, p_r$ are the sieving primes

The Sieving Lemma can be written

Lemma (Sieving Lemma)

$$N(k) \geq \sum_{i=1}^{r} N(k_0 p_i) - (r-1) N(k_0)$$

$$N(k) \geq \delta N(k_0) + \sum_{i=1}^{r} \left(N(k_0 p_i) - \left(1 - \frac{1}{|p_i|}\right) N(k_0) \right),$$

where $\delta = 1 - \sum_{i=1}^{r} \frac{1}{|p_i|}$ ($|p_i| = p_i$ *for* p_i *a prime number*)

- In applications, k may be $q^n - 1$ or $Q_n(x^n - 1)$, etc.
- Because estimates for $N(k)$ have factor $\theta(k)$ and $\theta(k_0 p_i) = (1 - 1/|p_i|)\theta(k_0)$, differences in Sieving Lemma can be efficiently estimated
- Essential to choose complementary divisors so that $\delta > 0$

Focusing on the additive sieve: SPBNT problem

For theoretical arguments, the more regular pattern of the irreducible factors of $x^n - 1$ over the prime factorisation of $q^n - 1$ favours additive sieving wherever possible

SPBNT $$\left| \frac{N(k, K_1, K_2)}{\theta(kK_1K_2)} - q^n \right| \leq 2W(kK_1K_2)q^{n/2}$$

Key strategy $(p \nmid n)$

- Define s minimal such that $n | q^s - 1$
  $s =$ maximal degree of irreducible factors of $x^n - 1$
- $x^n - 1 = g(x)G(x)$ $\quad$ G prod. of irred. factors $l_i(x)$ of deg s
- Core: $k_0 = Q_n g(x) g(y)$
- Sieving primes p_i: all $l_i(x)$ and $l_i(y)$
- $\delta = 1 - \frac{2(n-d)}{sq^s}$ $\quad$ $d = \deg g$

Then $$\frac{N(k)}{q^{n/2}\theta(Q_n g^2)} > q^{n/2} - 2W(Q_n g^2)\left(\frac{q^s 2((n-d)-s)}{sq^s - 2(n-d)} + 2\right)$$

The multiplicative sieve for the Pm problem

$$\left| \frac{N_m(k)}{q^{(n+1)/2}\theta(k)} - q^{\frac{n-m-1}{2}} \right| \leq mW(k) \qquad \text{(e.g. } a \neq 0,\ m \text{ even)}$$

- Worst case: $q,\ n \equiv 3 \bmod 4, m = (n+1)/2$
  For set of r compl. divisors of $q^n - 1$ with core k_0, $N(q^n - 1)$ positive whenever

$$q^{(n-3)/4} > \left(\frac{n+1}{2}\right) W(k_0) \left(\frac{r-1}{\delta} + 2\right)$$

Outline strategy $\omega := \omega(q^n - 1)$

(1) Assume $\omega \geq 1547$. Then $W(q^n - 1) < q^{n/12}$ and $q^{\frac{n}{6}-1} > n/2$ suffices without sieving

(2) Assume $\omega \leq 1546$ with $n \geq 16, q \geq 5$. Take $k_0 =$ product of 10 least primes in $q^n - 1$: then $r \leq 1536$, $\delta > 0.00267$ and OK unless $q \leq 821$ and $\omega \leq 79$

(3) Assume $\omega \leq 79, q \leq 821$: $k_0 =$ prod. of least 4 primes

(4) … …

Further tool

Fan and Wang (inherited from Lenstra-Schoof PNBT)

Lemma

Let $\mathcal{S}_h$ be the set of primes $< h$ such that each prime divisor of $q^n - 1 \in \mathcal{S}_h$. Set $H = \prod_{h \in \mathcal{S}_h} h$. Then

$$\omega(q^n - 1) \leq \frac{\log(q^n - 1) - \log H}{\log h} + |\mathcal{S}_h|$$

p-adic method

For $r = 1, n$:

- R_r: ring of integers in splitting field of $x^{q^r} - x$ over the p-adic field $\mathcal{Q}_p$, i.e. the completion of $\mathbb{Q}$ w.r.t. p-adic metric
  - R_r has characteristic zero
  - $R_1 \subseteq R_n$
- Γ_r: roots of $x^{q^r} - x$ Teichmüller points
  - Γ_r may be identified with $\mathbb{F}_{q^r}$ $r = 1, n$
  - Γ_r^* is cyclic of order $q^r - 1$
  - $R_r = \sum_{i=0}^{\infty} \gamma_i p^i, \ \gamma_i \in \Gamma_n$
- Lift primitive $f[x] \in \mathbb{F}_q[x]$ to unique primitive $\hat{f}(x) \in R_1[x]$
  If f is normal over $\mathbb{F}_q$, then $\hat{f}$ is normal over R_1
- $f \equiv \hat{f} \pmod{p}$; $\sigma_i \equiv \hat{\sigma}_i \pmod{p}$; roots $\hat{\gamma}$ of $\hat{f} \in \Gamma_n$

The Galois ring $R_{n,e}$

Define $\Gamma_{n,e} = \Gamma_n \pmod{p^e}$ (e positive integer)

- $\Gamma_{r,e}$ (like Γ_r) can be identified with $\mathbb{F}_{q^r}$

Define $R_{n,e} = \sum_{i=0}^{e-1} \gamma_i p^i, \; \gamma_i \in \Gamma_{n,e}$

- $R_{n,e}$ has cardinality q^{ne} and characteristic p^e
  - $R(n,1)$ is effectively $\mathbb{F}_{q^n}$
- Lift primitive or normal $f(x) \in \mathbb{F}_q(x)$ to primitive or normal $\hat{f}(x) \in R_{1,e}$
- Roots $\hat{\gamma} \in R_{n,e}$

Traces

Consider roots of lifted irreducible pol. $\hat{f}(x) \in R_1(x)$ or $R_{1,e}[x]$

Definitions 5

$s_l =$ R_1-trace of the lth powers of roots (strictly $\hat{s}_l$)

In particular assume $p \nmid t$

$$s_t = \sum_{j=0}^{\infty} s_{t,j}\, p^j \qquad (s_{t,j} \in \Gamma_1 \cong \Gamma_{1,e} \cong \mathbb{F}_q)$$

$$s_t^{(i)} = \sum_{j=0}^{\infty} s_{t,j}^{p^i} p^j$$

- $s_{t,j} \longrightarrow tp^j$ yields a bijection $\mathbb{N} \longleftrightarrow \{s_{t,j};\ p \nmid t,\ j \geq 0\}$

Specifying coefficients up to the mth, even when $p \leq m$

Proposition (p-adic Identity)

With $\hat{f}(x) \in R_1[x]$ irreducible and p odd

$$f^*(x) := x^n \hat{f}\left(\frac{1}{x}\right) = 1 - \sigma_1 x + \sigma_2 x^2 + \cdots + (-1)^n \sigma_n x^n$$

$$\equiv \prod_{\substack{t=1 \\ p \nmid t}}^{\infty} \prod_{j=0}^{\infty} \prod_{\substack{r=1 \\ p \nmid r}}^{\infty} \left(1 - \left(-\frac{s_{t,j}^{p^j}}{t}\right)^r x^{rtp^j}\right)^{-\frac{\mu(r)}{r}} \pmod{p}$$

- There is an alternative expression for $p = 2$

Proof

$$f^*(x) = \prod_{i=0}^{n-1} (1 - \hat{\gamma}^{q^i} x), \quad \hat{f}(\hat{\gamma}) = 0$$

$$
\begin{aligned}
f^*(x) &= \exp(-\sum_{l=1}^{\infty} \frac{\mathrm{Tr}(\hat{\gamma})^l x^l}{l}) = \exp(-\sum_{l=1}^{\infty} \frac{s_l x^l}{l}) \\
&= \exp\left(-\sum_{\substack{t=1\\ p\nmid t}}^{\infty} \sum_{i=0}^{\infty} \frac{s_t^{(i)} x^{tp^i}}{tp^i}\right) = \prod_{\substack{t=1\\ p\nmid t}}^{\infty} \exp\left(-\sum_{i=0}^{\infty} \frac{s_t^{(i)} x^{tp^i}}{tp^i}\right) \\
&= \prod_{\substack{t=1\\ p\nmid t}}^{\infty} \prod_{j=0}^{\infty} \prod_{i=0}^{\infty} \exp\left(-\frac{s_{t,j}^{p^i} p^{j-i} x^{tp^i}}{t}\right)
\end{aligned}
$$

Next, for each t, $p \nmid t$, consider the contribution of the terms with $i \geq j$

$$\prod_{j=0}^{\infty}\prod_{i=j}^{\infty}\exp\left(-\frac{s_{t,j}^{p^i}p^{j-i}x^{tp^i}}{t}\right)$$

$$=\prod_{j=0}^{\infty}\prod_{k=0}^{\infty}\exp\left(-\frac{\left(s_{t,j}^{p^j}x^{tp^j}\right)^{p^k}}{tp^k}\right)$$

$$\equiv \prod_{j=0}^{\infty}\exp\left(\sum_{k=0}^{\infty}\left(\frac{-s_{t,j}^{p^j}x^{tp^j}}{t}\right)^{p^k}\left(\frac{1}{p^k}\right)\right) \pmod{p}$$

$$\equiv \prod_{j=0}^{\infty}E_p\left(-\frac{s_{t,j}^{p^j}x^{tp^j}}{t}\right) \pmod{p} \quad \text{Artin-Hasse exp. fn}$$

$$\equiv \prod_{j=0}^{\infty}\prod_{\substack{r=1\\ p\nmid r}}^{\infty}\left(1-\left(\frac{-s_{t,j}^{p^j}}{t}\right)^r x^{tp^j r}\right)^{-\frac{\mu(r)}{r}} \pmod{p}$$

Finally, when $i < j$,

$$\exp\left(-\frac{s_{t,j}^{p^i} p^{j-i} x^{tp^i}}{t}\right) \equiv 1 \pmod{p}, \quad i < j,$$

and so such terms contribute a multiplier of 1

This proves the p-adic Identity

Criteria for specifying mth coefficient

- $a_1, \ldots, a_m$ can be specified by specifying $s_{t,j}$ for all $tp^j \leq m$
  m conditions as before

- $a_m = (-1)^m \sigma_m$ can be specified (as a) by
  - $s_{t,j} = 0 \qquad tp^j \leq \frac{m}{2}$
  - $s_{T,J} = -(Ta)^{1/p^J} \qquad m = Tp^J,\ p \nmid T$ **zero criterion**

  $\left\lfloor \frac{m}{2} \right\rfloor + 1$ conditions as before

- When m is even and p is odd, a_m can be specified by
  - $s_{t,j} = 0 \qquad tp^j \leq \frac{m}{2} - 1$
  - $s_{T_0,J_0} = z \in \Gamma_1 \qquad \frac{m}{2} = T_0 p^{J_0},\ p \nmid T_0$
  - $s_{T,J} = \left(\frac{2}{T}\right)^{1/p^J} z^2 - (Ta)^{1/p^J}$ **z criterion**

  $\left\lfloor \frac{m}{2} \right\rfloor + 1$ conditions as before

Characters over Galois rings

Only multiplicative characters over $\Gamma_{n,e}^* \cong \mathbb{F}_{q^n}^*$ required:
derived from those on $\mathbb{F}_{q^n}$, again denoted by χ_d, $d | q^n - 1$

Additive characters are needed over $R_{n,e}$:

canonical additive character: ψ where $\psi(\alpha) = \exp\left(\frac{2\pi \mathrm{Tr}_0(\alpha)}{p^e}\right)$

- Let $\mathcal{T}$ be a set of positive integers indivisible by p
- For a polynomial $h(x) = \sum_{t \in \mathcal{T}} \alpha_t x^t$ $(\alpha_t \in R_{n,e}) \in R_{n,e}[x]$, write

  $h(x) = \sum_{j=0}^{e-1} h_j(x) p^j$ $\quad h_j(x) \in \Gamma_{n,e}[x]$

  The weighted degree of h is $d_h := \max_{0 \le j \le e-1} (\deg(h_j) p^{e-1-j})$
- Set $S_n(h, \chi) = \sum_{\alpha \in \Gamma_{n,e}} h(\alpha)\chi(\alpha)$

$$S_n(h,\chi) = \sum_{\alpha \in \Gamma_{n,e}} h(\alpha)\chi(\alpha)$$

Lemma (W Li)

Generally $\quad |S_n(h,\chi)| \leq d_h q^{n/2}$

Application to Problem 3 (Pm)

$N_m(k) :=$ No. of k-free $\gamma \in \mathbb{F}_{q^n}$ with $a_m = a$

Define

- $\mathcal{T} = \{t \le m^*, \; p \nmid t\} \cup \{T\}$, where $m = Tp^J = Tp^{e_T - 1}$
- e^t = smallest integer such that $tp^{e_t} > m^*$, $t \le m^*$, $p \nmid t$,
- $e = e_1 = \max_{t \in \mathcal{T}} e_t$

By the zero criterion, for $a \in \mathbb{F}_q$ interpreted as in $R_{1,1}$,

$$q^{m^*+1} N_m(k) = \theta(k) \int_{d|k} \sum_{\substack{\alpha_{t,j} \in \Gamma_{1,1} \\ t \in \mathcal{T}, \; 0 \le j \le e_t - 1}} \psi(-p^{e-1} \alpha_{T,0} a) S_n(h, \chi_d),$$

where $h(x) = \sum_{t \in \mathcal{T}} \left(\sum_{j=0}^{e_t - 1} \alpha_{t,j} p^{e - e_t + j} \right) x^t$

For comparison:

- From before, when $p > m$

$$q^{m^*+1} N_m(k) = \theta(k) \int_{d|k} \sum_{\substack{c_t \in \mathbb{F}_q \\ t \le m^* \text{ or } t = m}} \psi(-c_m a) S_n(c_t \gamma^t, \chi_d),$$

- Now, more generally,

$$q^{m^*+1} N_m(k) = \theta(k) \int_{d|k} \sum_{\substack{\alpha_{t,j} \in \Gamma_{1,1} \\ t \in \mathcal{T},\ 0 \le j \le e_t - 1}} \psi(-p^{e-1} \alpha_{T,0} a) S_n(h, \chi_d),$$

where $h(x) = \sum_{t \in \mathcal{T}} \left(\sum_{j=0}^{e_t - 1} \alpha_{t,j} p^{e - e_t + j} \right) x^t$

- Details proceed as before

PFm: Primitive, normal, mth coefficient problem

- zero criterion (specifies a_m with $m^* = \lfloor m/2 \rfloor + 1$ conditions) cannot be used: it can only produce a polynomial with $a_1 = 0$, so not-normal

Alternative approach (taking $p > m$ for simplicity)

(1) Specify $s_1 = 1, s_2 = \cdots = s_{m-1} = 0, s_m = a$ to force $a_m = a$: thereby find a primitive normal polynomial m **conditions**

(2) **reciprocal zero criterion** Use the zero criterion on the reciprocal polynomial $a_n^{-1} x^n f(1/x)$ to find a primitive normal polynomial with specified $n-m$th coefficient and constant term $\left\lfloor \frac{n-m}{2} \right\rfloor + 2$ **conditions**

So use (1) for $m \leq \frac{n+4}{3}$ and (2) for $m > \frac{n+4}{3}$

- For $m = \frac{n+4}{3}$, need $\frac{n}{2} + \frac{n+4}{3} < n$ to work, i.e. $n > 8$
  - e.g. Method must fail if $n = 8, m = 4$

In worst case use of (1) and (2) would lead to

$$\left| \frac{N_m(k)}{q^{n/2}\theta(k)} - q^{\frac{n-8}{6}} \right| \leq \binom{n}{3} W(k)$$

where k is a formal divisor of $(q^n - 1)(x^n - 1)$ (not just $q^n - 1$)

Use of improved character sum expressions/estimates could lead to

$$\left| \frac{N_m(k)}{q^{n/2}\theta(k)} - q^{\frac{n-5}{6}} \right| \leq nW(k)$$

which would offer hope down to $n = 6$

- Wang, Fan and Wang, 2010 use the z criterion in both strategies (1) and (2) for $9 \leq n \leq 14$

Additive sieving also needed: sometimes Fan and Wang use all the irreducible factors of $x^n - 1$ as sieving "primes".

Is there a superior strategy?

Hard cases

Small values of n: e.g. $n = 3, m = 2; \quad n = 4, m = 2, 3$

For these, special arguments to reduce the number of conditions might be tried!!

Conjecture (Fan-Wang, 2010)

For $n \geq 2$ $(a \neq 0 \text{ if } m = 1)$, $N_m(q^n - 1)$ *is positive, except when*

$$(q, n, m, a) = (2, 3, 2, 1), (2, 4, 2, 1), (2.4, 3, 1), (2, 6, 3, 1)$$

$$(3, 4, 2, 2), (5, 3, 4, 3), (4, 3, 2, 1 + c),$$

where $c \in \mathbb{F}_4$ *satisfies* $c^2 + c + 1 = 0$

For further work

(1) Resolve the Fan-Wang Conjecture
(2) Use the Zsigmondy criterion (or similar) to resolve questions on the distribution of irreducible polynomials
(3) Existence of strong primitive normal polynomials with specified trace, norm, etc.
(4) Formalise the p-adic method and character sum estimates over Galois rings
(5) Alternative criteria for specifying a_m with approx. $m/2$ conditions
(6) Specify (say) 2 coefficients ($\leq m$th) with εm conditions, where $\varepsilon < 1$. Hence resolve associated existence questions
(7) Investigate and apply further sieving strategies

S D Cohen
Gauss sums and a sieve for generators of finite fields
Publl. Math Debrecen, 56 (**2000**), 293–312

S D Cohen and S Huczynska
Primitive free quartics with specified norm and trace
Acta Arith., 109 (**2003**), 359–385

S D Cohen and S Huczynska
Primitive free cubics with specified norm and trace
Trans. Amer. Math. Soc., 355 (**2003**), 3099–3116

S D Cohen and S Huczynska
The strong primitive normal basis theorem
Acta Arith., 143 (**2010**), 299–332

S D Cohen
Primitive polynomials with a prescribed coefficient
Finite Fields Appl., 12 (**2006**), 425–491

S D Cohen and M Prešern
The Hansen-Mullen primitivity conjecture: completion of proof
LMS Lecture Notes, 352 (**2008**), 89–120

S Fan and X Wang
Primitive normal polynomials with a prescribed coefficient
Finite Fields Appl., 15 (**2009**), 682–730

X Wang, S Fan and Z Wang
Primitive normal polynomials of degree $\leq n \leq 14$ with a prescribed coefficient
Preprint **2010**

See also

M Moisio and D Wan
On Katz's bound for the number of elements with given trace and norm
J. Reine Angew. Math., 638 (**2010**), 69–74