On the Hansen-Mullen Conjecture for Self-Reciprocal Irreducible Polynomials

Giorgos N. Kapetanakis

(joint work with T. Garefalakis)

University of Crete

Fq10 – July 14, 2011

Conjecture (Hansen-Mullen, 1992)

Let $a \in \mathbb{F}_q$, let $n \geq 2$ and fix $0 \leq j < n$. Then there exists an irreducible polynomial $F = X^n + \sum_{k=0}^{n-1} F_k X^k$ over $\mathbb{F}_q$ with $F_j = a$ except when

- *q arbitary and $j = a = 0$;*
- *$q = 2^m$, $n = 2$, $j = 1$ and $a = 0$.*

Theorem (Wan)

If either $q > 19$ or $n \geq 36$, then the Hansen-Mullen conjecture is true.

Theorem (Ham-Mullen)

The Hansen-Mullen conjecture is true.

What can we say about self-reciprocal polynomials?

Let q be a power of an odd prime p. Carlitz characterized self-reciprocal polynomials over $\mathbb{F}_q$.

Theorem (Carlitz)

If Q is a self-reciprocal monic irreducible polynomial over $\mathbb{F}_q$, then $\deg Q$ is even and $Q = X^n P(X + X^{-1})$ for some monic irreducible P, such that $\psi(P) = -1$, where $\psi(P) = (P|X^2 - 4)$, the Jacobi symbol of P modulo $X^2 - 4$. The converse also holds.

We denote $P = \sum_{i=0}^{n} P_i X^i$ and $Q = \sum_{i=0}^{2n} Q_i X^i$, and we compute

$$Q = X^n P(X + X^{-1}) = \sum_{i=0}^{n} P_i X^{n-i}(X^2+1)^i = \sum_{i=0}^{n} \sum_{j=0}^{i} \binom{i}{j} P_i X^{n-i+2j}.$$

For $1 \le k \le n$ the last equation implies that

$$Q_k = \sum_{\substack{0 \le j \le i \le n \\ n-i+2j=k}} \binom{i}{j} P_i = \sum_{\substack{n-k \le i \le n \\ k-n+i \in 2\mathbb{Z}}} \binom{i}{\frac{k-n+i}{2}} P_i \overset{j=n-i}{=} \sum_{\substack{0 \le j \le k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} P_{n-j}.$$

In order to express Q_k in terms of the low degree coefficients of some polynomial we define $\hat{P} = X^n P(4/X)$ and we prove.

Lemma

Let P be an irreducible polynomial of debree $n \geq 2$ and constant term 1. Then $\hat{P}$ is a monic irreducible of degree n and $\hat{P}_i = 4^{n-i} P_{n-i}$. Further, $\psi(P) = -\varepsilon\psi(\hat{P})$, where

$$\varepsilon := \begin{cases} -1 & \text{, if } q \equiv 1 \pmod 4 \text{ or } n \text{ is even.} \\ 1 & \text{, otherwise.} \end{cases}$$

Using this result, if we let $Q = X^n \hat{P}(X + X^{-1})$, we have

$$Q_k = \sum_{\substack{0 \leq j \leq k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} \hat{P}_{n-j} = \sum_{\substack{0 \leq j \leq k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} 4^j P_j = \sum_{j=0}^{k} \delta_j h_j,$$

where $\delta_j := \begin{cases} \binom{n-j}{\frac{k-j}{2}} 4^j & \text{, if } k-j \equiv 0 \pmod 2, \\ 0 & \text{, if } k-j \equiv 1 \pmod 2) \end{cases}$ and h a polynomial of degree at most k such that $P \equiv h \bmod X^{k+1}$.

Set $\mathbb{G}_k := \{h \in \mathbb{F}_q[X] \ : \ \deg(h) \leq k$ and $h_0 = 1\}$. For $1 \leq k \leq n$ we define

$$\tau_{n,k} : \ \mathbb{G}_k \to \mathbb{F}_q$$
$$h \mapsto \textstyle\sum_{j=0}^{k} \delta_j h_j .$$

The following proposition summarizes our observations.

Proposition

Let $n \geq 2$, $1 \leq k \leq n$, and $a \in \mathbb{F}_q$. Suppose that there exist an irreducible polynomial P, with constant term 1, such that $\psi(P) = \varepsilon$ and $P \equiv h \pmod{X^{k+1}}$ for some $h \in \mathbb{G}_k$ with $\tau_{n,k}(h) = a$. Then there exists a self-reciprocal monic irreducible polynomial Q, of degree $2n$, with $Q_k = a$.

We prove a correlation of the inverse image of $\tau_{n,k}$ with $\mathbb{G}_{k-1}$.

Proposition

Let a, n, k as above and $f = \sum_{i=0}^{k} f_i X^i \in \mathbb{F}_q[X]$, with $f_0 = 1$ and $f_i = \delta_{k-i}\delta_k^{-1}$, $1 \leq i \leq k-1$, and $f_k = \delta_k^{-1}(\delta_0 - a)$. Then the map $\sigma_{n,k,a} : \tau_{n,k}^{-1}(a) \to \mathbb{G}_{k-1}$ defined by $\sigma_{n,k,a}(h) = hf \mod X^{k+1}$ is a bijection.

Let $M \in \mathbb{F}_q[X]$ be a polynomial of degree at least 1 and χ a non-trivial Dirichlet character modulo M. The Dirichlet L-function associated with χ is defined to be

$$L(u,\chi) = \sum_{n=0}^{\infty} \left(\sum_{\substack{F \text{ monic} \\ \deg(F)=n}} \chi(F) \right) u^n.$$

It turns out that $L(u,\chi)$ is a polynomial in u of degree at most $\deg(M) - 1$. Further, $L(u,\chi)$ has an Euler product,

$$L(u,\chi) = \prod_{d=1}^{\infty} \prod_{\substack{P \text{ monic irreducible} \\ \deg(P)=d}} \left(1 - \chi(P) u^d\right)^{-1}.$$

Taking the logarithmic derivative of $L(u,\chi)$ and multiplying by u, we obtain a series $\sum_{n=1}^{\infty} c_n(\chi) u^n$, with

$$c_n(\chi) = \sum_{d|n} \frac{n}{d} \sum_{\substack{P \text{ monic irreducible} \\ \deg(P)=n/d}} \chi(P)^d = \sum_{\substack{h \text{ monic} \\ \deg(h)=n}} \Lambda(h)\chi(h),$$

where Λ stands for the von Mangoldt function.

Weil's theorem of the Riemann Hypothesis for function fields implies the following.

Theorem (Weil)

Let $M \in \mathbb{F}_q[X]$ be non-constant and let χ be a non-trivial Dirichlet character modulo M.

1. *Then*
$$|c_n(\chi)| \leq (\deg(M) - 1)q^{\frac{n}{2}}.$$
2. *If $\chi(\mathbb{F}_q^*) = 1$, then*
$$|1 + c_n(\chi)| \leq (\deg(M) - 2)q^{\frac{n}{2}}.$$

Theorem (Garefalakis)

Let χ be a non-trivial Dirichlet character modulo X^{k+1}. Then the following bounds hold:

1. *For every $n \in \mathbb{N}$, $n \geq 2$,*

$$\left| \sum_{\substack{P \text{ monic of degree } n \\ \psi(P)=-1}} \chi(P) \right| \leq \frac{k+5}{n} q^{\frac{n}{2}}.$$

2. *For every $n \in \mathbb{N}$, $n \geq 2$, n odd,*

$$\left| \sum_{\substack{P \text{ monic of degree } n \\ \psi(P)=1}} \chi(P) \right| \leq \frac{k+5}{n} q^{\frac{n}{2}}.$$

Based on the two previous theorems we prove.

Proposition

Let $n, k \in \mathbb{N}$, $1 \leq k \leq n$ and let χ be a non-trivial Dirichlet character modulo X^{k+1}, such that $\chi(\mathbb{F}_q^*) = 1$, then

$$\left| \sum_{\substack{\deg(h)=n \\ h_0=1}} \Lambda(h)\chi(h) \right| \leq 1 + kq^{\frac{n}{2}}, \quad \text{for } n \geq 1$$

and

$$\left| \sum_{\substack{P \text{ irreducible of degree } n \\ P_0=1,\ \psi(P)=\varepsilon}} \chi(P) \right| \leq \frac{k+5}{n} q^{\frac{n}{2}}, \quad \text{for } n \geq 2,$$

where either $\varepsilon = -1$, or $\varepsilon = 1$ and n is odd.

Definition

Let n, k, a be as usual. Inspired by Wan's work we introduce the following weighted sum.

$$w_a(n,k) = \sum_{h \in \tau_{n,k}^{-1}(a)} \Lambda(\sigma_{n,k,a}(h)) \sum_{\substack{P \text{ irreducible of degree } n \\ \psi(P)=\varepsilon,\ P_0=1,\ P\equiv h \pmod{X^{k+1}}}} 1.$$

It is clear that if $w_a(n,k) > 0$, then there exists some self-reciprocal, monic irreducible polynomial Q, of degree $2n$ with $Q_k = a$.

Let U be the subgroup of $(\mathbb{F}_q[X]/X^{k+1}\mathbb{F}_q[X])^*$ that contains classes of polynomials with constant term equal to 1.

- The set $\mathbb{G}_{k-1}$ is a set of representatives of U.
- The group of characters of U consists of those characters that are trivial on $\mathbb{F}_q^*$.

Using these and with the help of the orthogonality relations we get that

$$w_a(n,k) = \frac{1}{q^k} \sum_{\chi \in \widehat{U}} \sum_{\substack{P \text{ irreducible of degree } n \\ \psi(P)=\varepsilon,\ P_0=1}} \chi(P) \sum_{h \in \tau_{n,k}^{-1}(a)} \Lambda(\sigma_{n,k,a}(h))\bar{\chi}(h).$$

We denote by g the inverse of f modulo X^{k+1} and we obtain

$$\begin{aligned} w_a(n,k) &= \frac{1}{q^k} \sum_{\chi \in \widehat{U}} \sum_{\substack{P \text{ irreducible of degree } n \\ \psi(P)=\varepsilon,\ P_0=1}} \chi(P) \sum_{h \in \tau_{n,k}^{-1}(a)} \Lambda(\sigma_{n,k,a}(h))\bar{\chi}(\sigma_{n,k,a}(h)g) \\ &= \frac{1}{q^k} \sum_{\chi \in \widehat{U}} \sum_{\substack{P \text{ irreducible of degree } n \\ \psi(P)=\varepsilon,\ P_0=1}} \chi(P)\bar{\chi}(g) \sum_{h \in \mathbb{G}_{k-1}} \Lambda(h)\bar{\chi}(h). \end{aligned}$$

Separating the term that corresponds to χ_o, we have

$$\left| w_a(n,k) - \frac{\pi_q(n,\varepsilon)}{q^k} \sum_{h \in \mathbb{G}_{k-1}} \Lambda(h) \right| \leq$$

$$\frac{1}{q^k} \sum_{\chi \neq \chi_o} \left| \sum_{\substack{P \text{ irreducible of degree } n \\ \psi(P)=\varepsilon,\ P_0=1}} \chi(P) \right| \left| \sum_{h \in \mathbb{G}_{k-1}} \Lambda(h) \bar{\chi}(h) \right|,$$

where $\pi_q(n,\varepsilon) = \#\{P \in \mathbb{F}_q[X] : P \text{ monic irreducible of degree } n,\ \psi(P) = \varepsilon\}$.

We have that

$$\sum_{h\in\mathbb{G}_{k-1}} \Lambda(h) = \sum_{m=0}^{k-1} \sum_{\substack{\deg(h)=m \\ h_0=1}} \Lambda(h) = \sum_{m=0}^{k-1} q^m = \frac{q^k-1}{q-1}$$

and (for $\chi \neq \chi_o$)

$$\left| \sum_{h\in\mathbb{G}_{k-1}} \Lambda(h)\bar{\chi}(h) \right| \leq 1 + \sum_{m=1}^{k-1} (1 + kq^{\frac{m}{2}}) = k\frac{q^{\frac{k}{2}}-1}{\sqrt{q}-1}.$$

Putting everything together, our inequality becomes

$$\left| w_a(n,k) - \frac{q^k-1}{q^k(q-1)}\pi_q(n,\varepsilon) \right| \leq \frac{k(k+5)}{n} \frac{(q^k-1)(q^{\frac{k}{2}}-1)q^{\frac{n}{2}}}{q^k(\sqrt{q}-1)}.$$

As mentioned before, if $w_a(n,k) > 0$, then there exists some self-reciprocal, monic irreducible polynomial Q, of degree $2n$, with $Q_k = a$. This fact and the last relation are enough to prove the following.

Theorem

Let $n,k \in \mathbb{N}$, $n \geq 2$, $1 \leq k \leq n$ and $a \in \mathbb{F}_q$. There exists a monic, self-reciprocal irreducible polynomial Q, of degree $2n$ with $Q_k = a$, if the following bound holds.

$$\pi_q(n,\varepsilon) \geq \frac{k(k+5)}{n}(\sqrt{q}+1)q^{\frac{n+k}{2}}.$$

Carlitz computed

$$\pi_q(n,-1) = \begin{cases} \frac{1}{2n}(q^n - 1) & \text{, if } n = 2^s, \\ \frac{1}{2n}\sum_{\substack{d \mid n \\ d \text{ odd}}} \mu(d) q^{\frac{n}{d}} & \text{, otherwise.} \end{cases}$$

From this it is clear that

- if n is even, then $\varepsilon = -1$, thus $\pi_q(n,\varepsilon) = \pi_q(n,-1)$ and
- if n is odd, then $\pi_q(n,-1) = \frac{1}{2n}\sum_{\substack{d \mid n \\ d \text{ odd}}} \mu(d) q^{\frac{n}{d}} = \frac{1}{2}\pi_q(n)$, thus $\pi_q(n,-1) = \pi_q(n,1)$,

so, in any case $\pi_q(n,\varepsilon) = \pi_q(n,-1)$. Furthermore Carlitz's computation implies

$$\left| \pi_q(n,-1) - \frac{q^n}{2n} \right| \leq \frac{1}{2n}\frac{q}{q-1} q^{\frac{n}{3}}.$$

This result, combined with the last Theorem, are enough to prove the following.

Theorem

Let $n, k \in \mathbb{N}$, $n \geq 2$, $1 \leq k \leq n$, and $a \in \mathbb{F}_q$. There exists a monic, self-reciprocal irreducible polynomial Q, of degree $2n$ with $Q_k = a$ if the following bound holds.

$$q^{\frac{n-k-1}{2}} \geq \frac{16}{5} k(k+5) + \frac{1}{2}.$$

- Can we get a better result?
- What can we say when q is even?
- Can we extend this method, in order to examine similar questions for other types of irreducible polynomials?

L. Carlitz.
Some theorems on irreducible polynomials over a finite field.
Journal für die Reine und Angewandte Mathematik, 1967(227):212–220, 1967.

T. Garefalakis.
Self-reciprocal irreducible polynomials with prescribed coefficients.
Finite Fields and Their Applications, 17(2):183–193, 2010.

K. H. Ham and G. L. Mullen.
Distribution of irreducible polynomials of small degrees over finite fields.
Mathematics of Computation, 67(221):337–341, 1998.

T. Hansen and G. L. Mullen.
Primitive polynomials over finite fields.
Mathematics of Computation, 59(200):639–643, 1992.

M. Rosen.
Number Theory in Function Fields.
Springer-Verlag, New York, 2002.

D. Wan.
Generators and irreducible polnomials over finite fields.
Mathematics of Computation, 66(219):1195–1212, 1997.