A new proof of the Hansen-Mullen irreducibility conjecture

Aleksandr Tuxanidy

School of Mathematics and Statistics
Carleton University

September 29, 2017

Outline

Outline

Origins

Let q be a prime power, let $\mathbb{F}_q$ be the finite field with q elements, and let $n \geq 2$.

Conjecture, Hansen-Mullen (1992)

- Let $c \in \mathbb{F}_q$ and let $1 \leq w \leq n$
- Then there exists a monic irreducible $P(x) \in \mathbb{F}_q[x]$ with $\deg(P) = n$ and $[x^{n-w}]P(x) = c$, except when:
- $(w, c) = (n, 0)$, and $(n, w, c) = (2, 1, 0)$ with q odd .

Now a theorem

- Proved by Wan (1997) for $q > 19$ or $n \geq 36$
- Analytic techniques: Dirichlet characters on $\mathbb{F}_q[x]$, character sums, von Mangoldt function, Weil's bound
- Remaining cases computationally checked by Ham-Mullen (1998)

Generalizations and goals

Irreducibles with several prescribed digits

- Garefalakis (2008), Panario-Tzanakis (2012), Pollack (2013)
- Ha (2016): roughly up to $n/4$ arbitrary coefficients to any values!
- Adapts ideas of Bourgain (2015) on prime numbers with prescribed digits

Techniques

Overall techniques

- Wan (1997) used Dirichlet characters on $\mathbb{F}_q[x]$
- Cohen (2006) and Cohen-Prešern (2006, 2008): Newton identities + sieving lemma + Vinogradov's characteristic function.
- Newton's identities "break" when $p > 0$ is small $\implies$ work taken to p-adic fields and rings.
- Pollack (2013) and Ha (2016) adapt ideas of Harman-Katai (2008) and Bourgain (2015) on rational primes with prescribed digits. Use circle method

Goals and new techniques

Panario (2014):

"*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*"

Outline

Why a new proof?

Pros

- Completely different ideas
- A sufficient condition for a polynomial to have an irreducible factor (or be irreducible) of degree n
- The proof is elementary (no character sums, Weil's bound, etc)
- All cases of the conjecture are *theoretically explained (no computers needed)*

Cons

- No estimates for the number of such irreducibles

A sufficient condition

Definition (Least period)

- Let $a = a_0 a_1 \cdots a_{N-1}$ be cyclic sequence
- Let r be smallest positive number with $a_i = a_{(i+r) \bmod N}$ for all $0 \leq i \leq N-1$
- r is called the *least period* of a

Lemma, Tuxanidy-Wang (2016)

Let $h(x) \in \mathbb{F}_q[x]$ and let L be any subfield of $\mathbb{F}_{q^n}$ containing $h(\mathbb{F}_{q^n}^{\times})$. Define

$$S_h(x) = \left(1 - h(x)^{|L^{\times}|}\right) \bmod \left(x^{q^n-1} - 1\right) \in \mathbb{F}_q[x].$$

If the least period of the cyclic sequence $([x^m]S_h(x))_{m=0}^{q^n-2}$ does not divide $(q^n-1)/\Phi_n(q)$, then $h(x)$ has an irreducible factor of degree n over $\mathbb{F}_q$.

Corollary

If $\deg(h) = n$ and $S_h(x)$ satisfies the condition, then $h(x)$ is irreducible

Outline

Hansen-Mullen revisited

- A typical irreducible polynomial $P(x) \in \mathbb{F}_q[x]$ of degree n is

$$P(x) = \prod_{k=0}^{n-1} \left(x - \xi^{q^k} \right) = x^n + \sum_{w=1}^{n} (-1)^w \sigma_w(\xi) x^{n-w}$$

  where $\deg_{\mathbb{F}_q}(\xi) = n$ and

$$\sigma_w(\xi) = \sum_{0 \le i_1 < \cdots < i_w \le n-1} \xi^{q^{i_1} + \cdots + q^{i_w}} \in \mathbb{F}_q$$

- If $(-1)^w \sigma_w(x) - c \in \mathbb{F}_q[x]$ has a irreducible factor $P(x)$ of degree n, then any root ξ of $P(x)$ satisfies $(-1)^w \sigma_w(\xi) = c$ and so $[x^{n-w}]P(x) = c$
- Thus for HM we need to show $(-1)^w \sigma_w(x) - c$ has an irreducible factor of degree n

Hansen-Mullen revisited

- Let $w < n$. If the least period of the sequence

$$s_m = [x^m]\left(1 - ((-1)^w \sigma_w(x) - c)^{q-1}\right),$$

$0 \le m \le q^n - 2$, is not a divisor of $(q^n - 1)/\Phi_n(q)$, then there exists a monic irreducible polynomial $P(x)$ of degree n over $\mathbb{F}_q$ with $[x^{n-w}]P(x) = c$

Notations

- For $k \in \mathbb{Z}_{q^n-1}$, let $(k)_q \in [0, q-1]^n$ be the q-adic representation of the canonical representative of k in $\mathbb{Z}$. Let $s_q(k)$ be the sum of the q-digits of $(k)_q$
- For $0 \le w \le n$, let

$$\Omega(w) = \left\{k \in \mathbb{Z}_{q^n-1} \ : \ (k)_q \in \{0,1\}^n, \ s_q(k) = w\right\}$$

- Let $\delta_w : \mathbb{Z}_{q^n-1} \to \mathbb{F}_p$ be defined by

$$\delta_w(k) = \begin{cases} 1 & \text{if } k \in \Omega(w); \\ 0 & \text{otherwise.} \end{cases}$$

Hansen-Mullen revisited

For functions $f_1, \ldots, f_s$ on $\mathbb{Z}_{q^n-1}$, let

$$(f_1 \otimes \cdots \otimes f_s)(m) = \sum_{\substack{j_1+\cdots+j_s=m \\ j_1,\ldots,j_s \in \mathbb{Z}_{q^n-1}}} f_1(j_1)\cdots f_s(j_s)$$

be the convolution of $f_1, \ldots, f_s$. Let $f^{\otimes s}$ denote the convolution of f with itself s times.

Lemma, Tuxanidy-Wang (2016)

If the least period of $\Delta_{w,c} : \mathbb{Z}_{q^n-1} \to \mathbb{F}_q$ given by

$$\Delta_{w,c} = \delta_0 - ((-1)^w \delta_w - c\delta_0)^{\otimes(q-1)}$$

does not divide $(q^n-1)/\Phi_n(q)$, then there exists an irreducible polynomial $P(x)$ of degree n over $\mathbb{F}_q$ with $[x^{n-w}]P(x) = c$.

Hansen-Mullen revisited

Observation

- The functions $\delta_w : \mathbb{Z}_{q^n-1} \to \mathbb{F}_p$ are q-symmetric, i.e., $\delta_w((a_0, \ldots, a_{n-1})_q) = \delta_w((a_{\sigma(0)}, \ldots, a_{\sigma(n-1)})_q)$ for any $\sigma \in \mathcal{S}_{[0,n-1]}$ and $(a_0, \ldots, a_{n-1})_q \in \mathbb{Z}_{q^n-1}$
- Question: Is

$$\Delta_{w,c} = \delta_0 - ((-1)^w \delta_w - c\delta_0)^{\otimes(q-1)}$$

q-symmetric?.... Yes! Because:

Lemma

Let $f_1, \ldots f_s$ be q-symmetric functions such that for every $a_k \in \mathrm{supp}(f_k)$, $1 \le k \le s$, there occurs no “carry” in the q-adic addition $a_1 + \cdots + a_s$. Then $f_1 \otimes \cdots \otimes f_s$ is q-symmetric.

HM revisted

Definition

- A set $A \subseteq \mathbb{Z}_{q^n-1}$ is q-symmetric if for all $(a_0, \ldots, a_{n-1})_q \in A$, we have $(a_{\sigma(0)}, \ldots, a_{\sigma(n-1)})_q \in A$ for all $\sigma \in \mathcal{S}_{[0,n-1]}$, i.e., A is a union of orbits on $\mathbb{Z}_{q^n-1}$ under the action of digit permutation
- A set $A \subseteq \mathbb{Z}_{q^n-1}$ is *r-periodic* if

$$A = \bigcup_{g \in \mathcal{G}} \{g + br \;:\; 0 \leq b < (q^n - 1)/r\}$$

for some $\mathcal{G} \subseteq [0, r-1]$

Observation

- The support of a q-symmetric function is a q-symmetric set
- The support of an r-periodic function is r-periodic.

HM revisited

Idea of proof

- q-symmetric sets should not be r-periodic: Repeated addition by r should lead to carries which destroy q-symmetric structure
- We show that the q-symmetric set $\mathrm{supp}(\Delta_{w,c})$ is not r-periodic.

Acknowledgments

Acknowledgments

After submitting the article we noticed "*Irreducible coefficient relations*" by Dorsey-Hales, SETA (2012). One of their lemmas shows that if r is not too large, then essentially no q-symmetric sets are r-periodic.

Is there an analytic proof that q-symmetric sets are not r-periodic (for adequate sets)

Lemma: Let $q, n \geq 2$ be integers and set $N = q^n - 1$. Assume $A \subset \mathbb{Z}_N$ is an r-periodic set, where $r > 1$ divides N. Let $\tau \in \mathcal{S}_{[0,n-1]}$ be the transposition $(0, 1)$. Set

$$S_\tau(A) := \#\{a \in A \ : \ \tau((a)_q) \in A\}$$
$$B = \{(q-1)c \ : \ 0 \leq c \leq q-1\} \subset \mathbb{Z}_N$$

and let

$$E(A, B) = \#\{(a, b, a', b') \in A \times B \times A \times B \ : \ a + b = a' + b'\}.$$

Then

$$\left| S_\tau(A) + A(0) - \frac{q^{n-2}}{N} E(A, B) \right| \leq \frac{q^2(r-1)|A|}{N}.$$

Is there an analytic proof that q-symmetric sets are not r-periodic (for adequate sets)

If $r > q^{n-2}$,

$$S_\tau(A) \leq \frac{q^{n-2}}{N} E(A,B) + \frac{q^2(r - q^{n-2})|A|}{N}.$$

If $r = q - 1 > 1$, then

$$S_\tau(A) = \frac{q^{n-2}}{N} E(A,B) - \frac{|A|}{N}.$$

A special case

Proof sketch for $c = 0$ with $0 < w < n$ s.t. $w \neq n/2$: Here $\Delta_{w,0} = \delta_0 - \delta_w^{\otimes(q-1)}$. First note

$$\delta_w^{\otimes(q-1)}(m) = \#\left\{(j_1, \ldots, j_{q-1}) \in \Omega(w)^{q-1} \ : \ j_1 + \cdots + j_{q-1} = m\right\} \bmod p,$$

where $\Omega(w) = \{k \in \mathbb{Z}_{q^n-1} \ : \ (k)_q \in \{0,1\}^n, \ s_q(k) = w\}$.

- If $\delta_w^{\otimes(q-1)}(m) \neq 0$, then $s_q(m) = (q-1)w$
- Note $\Delta_{w,0}(0) = 1$. If $0 < r < q^n - 1$ is a period of $\Delta_{w,0}$, then $\Delta_{w,0}(r) = 1$ and $\delta_w^{\otimes(q-1)}(r) = -1 \neq 0$. Hence $s_q(r) = (q-1)w$
- Note $r' = q^n - 1 - r$, $0 < r' < q^n - 1$, is a period of $\Delta_{w,0}$. By the previous arguments, $s_q(r') = (q-1)w$
- Since $s_q(r') = (q-1)n - s_q(r)$, we get $w = n/2$, contradiction

Outline

Multiple prescribed coefficients? Stay tuned

Proposition

Let $W \subset [n]$, fix $c_w \in \mathbb{F}_q$, $w \in W$. If the least period of the cyclic sequence $([x^m]S_W(x))_{m=0}^{q^n-2}$ is not a divisor of $(q^n-1)/\Phi_n(q)$, where

$$S_W(x) = \left(\prod_{w \in W} \left(1 - ((-1)^w \sigma_w(x) - c_w)^{q-1}\right) \right) \bmod \left(x^{q^n-1} - 1\right),$$

then there exists an irreducible polynomial $P(x)$ of degree n over $\mathbb{F}_q$ such that $[x^{n-w}]P(x) = c_w$, $w \in W$.