The Hansen-Mullen Conjecture

Giorgos Kapetanakis

Sabanci University

October 11, 2016

1. Introduction
2. Wan's proof
   - Preliminaries
   - Weighted sums
   - Completion of the proof
3. The HMC for self-reciprocal irreducible polynomials
   - Motivation
   - Preliminaries
   - Weighted sum
   - Completion of the proof
   - The restriction $k \leq n/2$
   - Further research
4. Other extensions of the HMC
5. Different approaches

- Let q be a prime power. We denote by $\mathbb{F}_q$ the finite field of q elements.
- A generator of the multiplicative group $\mathbb{F}_q^*$ is called primitive.
- A polynomial of degree n of $\mathbb{F}_q[X]$ is called primitive if one (hence all) of its roots is a primitive element of $\mathbb{F}_{q^n}$.
- Primitive polynomials are irreducible, but not vice versa.

The properties of irreducible polynomials over $\mathbb{F}_q$ have proved to be of great theoretical and practical interest. Such properties, that have been investigated, include

- primitivity,
- normality,
- having certain coefficients fixed to given values and
- combinations of those properties with other interesting ones.

One such result is the following.

Theorem (Cohen (1990))

Let $n \geq 2$ and $t \in \mathbb{F}_q$ with $t \neq 0$ if $n = 2$ or if $n = 3$ and $q = 4$. Then there exists a primitive polynomial of degree n over $\mathbb{F}_q$ with trace t.

Based on the above and on computational evidence, Hansen and Mullen (1992) stated two important conjectures.

Conjecture (Hansen-Mullen (1992))

Let $a \in \mathbb{F}_q$, *let* $n \geq 2$ *and* $0 \leq j < n$. *Then there exists an irreducible polynomial* $f(X) = X^n + \sum_{k=0}^{n-1} a_k X^k \in \mathbb{F}_q[X]$ *with* $a_j = a$ *except when*

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

Conjecture (Hansen-Mullen (1992))

Let $a \in \mathbb{F}_q$, let $n \geq 2$ and $0 \leq j < n$. Then there exists a primitive polynomial $f(X) = X^n + \sum_{k=0}^{n-1} a_k X^k \in \mathbb{F}_q[X]$ with $a_j = a$ except when

- *$j = 0$ and $a \neq (-1)^n \alpha$, where $\alpha \in \mathbb{F}_q$ is a primitive element;*
- *$n = 2$, $j = 1$, and $a = 0$;*
- *$q = 4$, $n = 3$, $j = 2$, and $a = 0$;*
- *$q = 4$, $n = 3$, $j = 1$, and $a = 0$;*
- *$q = 2$, $n = 4$, $j = 2$, and $a = 1$.*

- The exceptions are genuine.
- Both conjectures are established.

- Cohen (1990) proved the HMC (Hansen-Mullen Conjecture) for $j = n - 1$.
- In order to further support their claim, Hansen and Mullen (1992) proved their conjecture for $j = 0$.
- Wan (1997) proved the HMC for irreducible polynomials if $n \geq 36$ or $q > 19$ with the help of character sums.
- Soon, Ham and Mullen (1998) completed the proof, by providing examples for the remaining cases with the help of computers.

- Cohen (1990) proved the HMC for $j = n - 1$.
- In order to further support their claim, Hansen and Mullen (1992) proved their conjecture for $j = 0$.
- The work of Cohen (2000) and Cohen and Huczynska (2003) prove the HMC for $j = 1$.
- Han (1996) and Cohen and Mills (2003) proved the HMC for $j = n - 2$ and $n \geq 5$.
- The work of Fan and Han (2004), Mills (2004) and Cohen and King (2004), established the HMC for $j = n - 3$ and $n \geq 7$.

- Fan and Han (2003) used p-adic methods to asymptotically prove the HMC for primitive polynomials for fixed n and q large enough, except when $n/2 \leq j \leq n/2+1$.
- Fan and Han (2004) proved the HMC for primitive polynomials for even q and odd $n \geq 7$, by using character sums, p-adic methods, sieving techniques and computer searches.
- Cohen (2006) proved the HMC for primitive polynomials for $n \geq 9$, by using character sums, p-adic methods, sieving techniques and computer searches.
- Two years later, Cohen and Prešern (2008) completed the proof of the Hansen-Mullen conjecture for primitive polynomials.

The main idea behind the techniques of most authors dates back to the work of Carlitz (1952) and still remains popular. Roughly, this method is:

1. Express the characteristic or a characteristic-like function for a polynomial with the desired properties with help of characters.
2. With the the help of character sum estimates or calculations, this leads to a lower bound of the number of polynomials with the desired properties.
3. This implies sufficient asymptotic conditions for the existence of the desired polynomial.
4. These conditions could be relaxed (i.e. with sieving) and/or give rise to effective results.
5. If desirable, one can we deal with the remaining cases with a case-by-case approach.

Nonetheless, there are also other approaches of the HMC.

Now, we will present Wan's proof for the HMC for irreducible polynomials.

D. Wan.
Generators and irreducible polynomials over finite fields.
Math. Comp., 66(219):1195–1212, 1997.

Definition

Let $\mathfrak{G}$ be a finite abelian group. A character of $\mathfrak{G}$ is a group homomorphism $\mathfrak{G} \to \mathbb{C}^*$, where $\mathbb{C}^*$ stands for the multiplicative group of $\mathbb{C}$. The characters of $\mathfrak{G}$ form a group under multiplication, which is isomorphic to $\mathfrak{G}$. This group is called the dual of $\mathfrak{G}$ and denoted by $\widehat{\mathfrak{G}}$. Furthermore, the character $\chi_0 : \mathfrak{G} \to \mathbb{C}^*$, where $\chi_0(g) = 1$ for all $g \in \mathfrak{G}$, is called the trivial character of $\mathfrak{G}$. Finally, by $\bar{\chi}$ we denote the inverse of χ.

A character or exponential sum is a sum that involves characters.

The simplest, albeit very important, form of character sum is the following.

Lemma (Orthogonality relations)

Let χ be a non-trivial character of a group $\mathfrak{G}$ and g a non-trivial element of $\mathfrak{G}$. Then

$$\sum_{x\in\mathfrak{G}}\chi(x)=0 \quad \textit{and} \quad \sum_{\chi\in\widehat{\mathfrak{G}}}\chi(g)=0.$$

- The orthogonality relations are true for arbitrary group $\mathfrak{G}$.

Definition

Given some $F \in \mathbb{F}_q[X]$, a Dirichlet character modulo F is a function $\chi : \mathbb{F}_q[X] \to \mathbb{C}^*$, such that

1. $\chi(G + FH) = \chi(G)$,
2. $\chi(GH) = \chi(G)\chi(H)$ and
3. $\chi(G) \neq 0 \iff (G, F) = 1$,

for every $G, H \in \mathbb{F}_q[X]$.

- Dirichlet characters were originally defined over $\mathbb{Z}$,
- Dirichlet characters modulo F are essentially the characters of $(\mathbb{F}_q[X]/F\,\mathbb{F}_q[X])^*$, extended to zero.

For χ a Dirichlet character modulo $M \in \mathbb{F}_q[X]$ and $n \in \mathbb{N}$ set

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

In particular the logarithmic derivative of the Dirichlet L-function of χ (multiplied by u) is $\sum_{n=0}^{\infty} c_n(\chi)u^n$. It follows from the Riemann Hypothesis from function fields, proven by Weil (1948), that:

Theorem (Weil)

Let χ be a Dirichlet character modulo M. Then

1. *If $\chi \neq \chi_0$ then*
$$|c_n(\chi)| \leq (\deg(M) - 1)q^{\frac{n}{2}}.$$
2. *If $\chi \neq \chi_0$ and $\chi(\mathbb{F}_q^*) = 1$, then*
$$|1 + c_n(\chi)| \leq (\deg(M) - 2)q^{\frac{n}{2}}.$$

For $H \in \mathbb{F}_q[X]$, we define the von Mangoldt function as

$$\Lambda(H) = \begin{cases} \deg(P), & \text{if } H \text{ is a power of the irreducible } P, \\ 1, & \text{if } H = 1, \\ 0, & \text{otherwise.} \end{cases}$$

It follows directly from the definition of Λ, that

$$c_n(\chi) = \sum_{\substack{H \text{ monic} \\ \deg(H)=n}} \Lambda(H)\chi(H).$$

By using Weil's theorem and this characterization for $c_n(\chi)$, one can see that the following character sum estimates hold.

Corollary

Let χ be a Dirichlet character modulo M. Then

1. *If $\chi \neq \chi_0$ then*

$$\left| \sum_{\substack{P \text{ monic irreducible} \\ \deg(P)=d}} \chi(P) \right| \leq \frac{1}{d}(\deg(M)+1)q^{d/2}.$$

2. *If $\chi \neq \chi_0$ and $\chi(\mathbb{F}_q^*) = 1$, then*

$$\left| \frac{1}{d} + \sum_{\substack{P \text{ monic irreducible} \\ \deg(P)=d}} \chi(P) \right| \leq \frac{1}{d}\deg(M)q^{d/2}.$$

Similarly, we can estimate character sums that run through irreducible polynomials with constant term 1 (not necessarily monic).

Corollary

Let χ be a non-trivial Dirichlet character modulo M, such that $\chi(\mathbb{F}_q^*) = 1$, then

$$\left| \sum_{\substack{P \text{ irreducible with constant term } 1 \\ \deg(P)=d}} \chi(P) \right| \leq \frac{1}{d} \deg(M) q^{d/2}.$$

From now on, fix n, $1 \leq j < n$ and $a \in \mathbb{F}_q$ and define the following weighted sum

$$w_a(n,j) := \sum_{H \text{ monic of degree } j} \Lambda(aH) \sum_{\substack{P \equiv aH \pmod{X^{j+1}} \\ P \text{ monic irreducible of degree } n}} 1.$$

If $w_a(n,j) \neq 0$, then there exists a monic irreducible of degree n with its j-th coefficient prescribed to a.

From the orthogonality relations, we have that

$$\begin{aligned} w_a(n,j) &= \sum_H \Lambda(aH) \sum_P \frac{1}{q^j(q-1)} \sum_\chi \chi(P)\bar{\chi}(aH) \\ &= \frac{1}{q^j(q-1)} \sum_\chi \left(\sum_P \chi(P) \right) \left(\sum_H \Lambda(aH)\bar{\chi}(aH) \right), \end{aligned}$$

where we note that for $a \neq 0$,

$$\left| \sum_H \Lambda(aH)\bar{\chi}(aH) \right| = \left| \sum_H \Lambda(H)\bar{\chi}(H) \right|,$$

while the case $a = 0$ requires special, but similar, treatment.

We then separate the term of χ_0 and apply the previous results and we eventually get.

Proposition

We have

$$\left| w_a(n,j) - \frac{\pi_n}{q-1} \right| < \frac{1}{n}(j^2+2j)q^{(n+j)/2}.$$

The above, combined with known lower bounds for π_n, implies.

Corollary

Let $a \in \mathbb{F}_q$, $n \geq 3$ and $1 \leq j < n$. If

$$q^{n-j} \geq (q-1)^2(j+1)^4,$$

then there exists an irreducible $P \in \mathbb{F}_q[X]$, with $\deg(P) = n$ and $P_j = a$, where P_j is the coefficient of X^j.

The latter is effective for $j \leq n/2$. For larger values of j, we consider the reciprocal of a monic irreducible, i.e. an irreducible with constant term equal to 1. Let G_{j-1} be the set of polynomials of $\mathbb{F}_q[X]$ of degree $j-1$ with constant term equal to 1 and fix $a \in \mathbb{F}_q$, n and $1 \leq j < n$ and define

$$W_a(n,j) := \sum_{H \in G_{j-1}} \Lambda(H) \sum_{\substack{P \text{ irreducible of degree } n \\ \text{and constant term equal to } 1 \\ P \equiv H + aX^j \pmod{X^{j+1}}}} 1.$$

If $W_a(n,j) \neq 0$, then there exists an irreducible $P \in \mathbb{F}_q[X]$ of degree n with constant term equal to 1 and $P_j = a$. This means that its reciprocal, i.e. $P^R := X^n P(1/X)$, is a monic irreducible of degree n with $P^R_{n-j} = a$.

With a similar treatment as with $w_a(n,j)$, we show that

Proposition

If $j>1$*, then*

$$\left|W_a(n,j)-\frac{\pi_n}{q}\right|<\frac{1}{n}j^2q^{(n+j-1)/2}.$$

Again, by using known bounds for π_n, the above implies the following.

Corollary

Let $a\in\mathbb{F}_q$ *and* $1\le j<n$*. If*

$$q^{n-j-1}\ge(j+1)^4,$$

then there exists an irreducible $P\in\mathbb{F}_q[X]$ *with constant term equal to* 1 *and its* j*-th coefficient fixed to* a*.*

The latter is effective for $j \leq n/2$, but since this implies the existence of a monic irreducible polynomial of degree n with the coefficient of X^{n-j} prescribed, it is actually effective for $j \geq n/2$.

By putting everything together, we end up with the following

Corollary

Let $a \in \mathbb{F}_q$, $n \geq 3$ and $1 \leq j < n$. If either

$$q^{n-j} \geq (q-1)^2 (j+1)^4 \quad \textit{or} \quad q^{j-1} \geq (n-j+1)^4,$$

then there exists a monic irreducible $P \in \mathbb{F}_q[X]$ of degree n with the coefficient of X^j equal to a.

A few computations verify that at least one of the requirements of the above is true for any value of j if $q > 19$ or $m \geq 36$, thus.

Theorem (Wan)

If $q > 19$ or $m \geq 36$, then the HMC for irreducible polynomials is true.

Next, we will present the work of Garefalakis and K. on the HMC for self-reciprocal irreducible polynomials.

T. Garefalakis and G. Kapetanakis.
On the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials.
Finite Fields Appl., 18(4):832–841, 2012.

T. Garefalakis and G. Kapetanakis.
A note on the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials.
Finite Fields Appl., 35(C):61–63, 2015.

Given a polynomial $Q \in \mathbb{F}_q[X]$, its reciprocal Q^R is defined as

$$Q^R(X) = X^{\deg(Q)} Q(1/X).$$

One class of polynomials that has been intensively investigated is that of self-reciprocal irreducible polynomials, that is, irreducible polynomials that satisfy $Q^R(X) = Q(X)$. Besides their theoretical interest, self-reciprocal irreducible polynomials have been useful in applications, and in particular in the construction of error-correcting codes.

- It is natural to expect that self-reciprocal monic irreducible polynomials over finite fields, with some coefficient fixed, exist. Here, we restrict ourselves to the case where q is odd and prove that there exists a self-reciprocal irreducible monic polynomial over $\mathbb{F}_q$, of degree $2n$ with its k-th coefficient prescribed, provided that

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

- With this result in mind, we show that we can prescribe the k-th coefficient of a self-reciprocal irreducible polynomial of degree $2n$, provided that $k \leq \lfloor n/2 \rfloor$, with a small number of genuine exceptions.
- Our proof is based on an estimate of a weighted sum, similar to the one that Wan considers, character sums and Carlitz's (1967) characterization of self-reciprocal irreducible monic polynomials.

- Carlitz (1967) characterized self-reciprocal irreducible monic polynomials over $\mathbb{F}_q$ (srimp): Q is a srimp iff

$$Q(X) = X^n \hat{P}(X + X^{-1})$$

for some monic irreducible $\hat{P}$ of degree n, such that $\psi(\hat{P}) = -1$, where $\psi(\hat{P}) = (\hat{P}|X^2 - 4)$, the Jacobi symbol of $\hat{P}$ modulo $X^2 - 4$.

- We compute

$$Q(X) = \sum_{i=0}^{n} \sum_{j=0}^{i} \binom{i}{j} \hat{P}_i X^{n-i+2j},$$

which imples

$$Q_k = \sum_{\substack{0 \le j \le k \\ k-j \in 2\mathbb{Z}}} \binom{n-j}{\frac{k-j}{2}} \hat{P}_{n-j}.$$

- In the last expression, Q_k is written in terms of the large degree coefficients of $\hat{P}$. In order to express in terms of the low degree coefficients of a polynomial, we define.

$$\hat{P} = X^n P(4X^{-1})$$

and prove that $\hat{P}_i = 4^{n-i} P_{n-i}$ and $\psi(P) = -\varepsilon\psi(\hat{P})$, where $\varepsilon = \pm 1$, depending on q and n.

- It follows that

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

where

$$\delta_j = \begin{cases} \binom{n-j}{\frac{k-j}{2}} 4^j, & \text{if } k-j \equiv 0 \pmod 2, \\ 0, & \text{if } k-j \equiv 1 \pmod 2. \end{cases}$$

We define $\tau_{n,k} : G_k \to \mathbb{F}_q,\ H \mapsto \sum_{j=0}^{k} \delta_j H_j$, where $G_k := \{H \in \mathbb{F}_q[X] \ : \ \deg(H) \le k \text{ and } H_0 = 1\}$. We have proved:

Proposition

Let $n \ge 2$, $1 \le k \le n$, and $a \in \mathbb{F}_q$. Suppose there exists an irreducible $P \in \mathbb{F}_q[X]$ with $P_0 = 1$, such that $\psi(P) = \varepsilon$ and $P \equiv H \pmod{X^{k+1}}$ for some $H \in G_k$ with $\tau_{n,k}(H) = a$. Then there exists a srimp Q, of degree $2n$, with $Q_k = a$.

Next, we need to correlate the inverse image of $\tau_{n,k}$ with G_{k-1}. In this direction, we prove.

Proposition

Let $a \in \mathbb{F}_q$, $n \ge 2$ and $1 \le k \le n$. Let $F = \sum_{i=0}^{k} F_i X^i \in \mathbb{F}_q[X]$, with $F_0 = 1$ and $F_i = \delta_{k-i}\delta_k^{-1}$, $1 \le i \le k-1$, and $F_k = \delta_k^{-1}(\delta_0 - a)$. Then the map $\tau_{n,k}^{-1}(a) \to G_{k-1} \ : \ H \mapsto HF \pmod{X^{k+1}}$ is a bijection.

Let $n \geq 2$, $1 \leq k \leq n$ and $a \in \mathbb{F}_q$. Inspired by Wan's work (1997) we introduce the following weighted sum.

$$w_a(n,k) = \sum_{H \in \tau_{n,k}^{-1}(a)} \Lambda(FH) \sum_{\psi(P)=\varepsilon,\ P \equiv H \pmod{X^{k+1}}} 1.$$

It is clear that if $w_a(n,k) > 0$, then there exists some P such that $P \equiv H \pmod{X^{k+1}}$ for some $H \in G_k$, with $\tau_{n,k}(H) = a$ and $\psi(P) = \varepsilon$. Then there exists a srimp 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 G_{k-1} is a set of representatives of U. Further, the group of characters of U consists exactly of those characters of $(\mathbb{F}_q[X]/X^{k+1}\mathbb{F}_q[X])^*$ that are trivial on $\mathbb{F}_q$, that is, $\widehat{U} = \{\chi \in (\mathbb{F}_q[X]/\widehat{X^{k+1}}\mathbb{F}_q[X])^* \ : \ \chi(\mathbb{F}_q^*) = 1\}$. Using these observations and the orthogonality relations, we get that

$$\begin{aligned} w_a(n,k) &= \frac{1}{q^k} \sum_{\chi \in \widehat{U}} \sum_{\substack{P \in J_n \\ \psi(P)=\varepsilon}} \chi(P) \sum_{H \in \tau_{n,k}^{-1}(a)} \Lambda(FH)\bar{\chi}(H) \\ &= \frac{1}{q^k} \sum_{\chi \in \widehat{U}} \sum_{\substack{P \in J_n \\ \psi(P)=\varepsilon}} \chi(P)\bar{\chi}(G) \sum_{H \in G_{k-1}} \Lambda(H)\bar{\chi}(H), \end{aligned}$$

where G is the inverse of F modulo X^{k+1} and J_n stands for the set of irreducible polynomials of degree n and constant term equal to 1.

We separate the term that corresponds to χ_0 and we get

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

$$\frac{1}{q^k} \sum_{\chi \neq \chi_o} \left| \sum_{P \in J_n,\ \psi(P)=\varepsilon} \chi(P) \right| \left| \sum_{H \in G_{k-1}} \Lambda(H) \bar{\chi}(H) \right|,$$

where $\pi_q(n,\varepsilon) = |\{P \text{ irreducible of degree } n : \psi(P) = \varepsilon\}|$.

We will also use the following result.

Theorem (Garefalakis (2011))

Let $\psi(P) = (P|X^2-4)$ *be the Jacobi symbol of* P *modulo* X^2-4 *and* χ *be a non-trivial Dirichlet character modulo* X^{k+1}, *where* $k \geq 1$. *The following bounds hold:*

1. *For every* $n \in \mathbb{N}$, $n \geq 2$,
$$\left| \sum_{P \text{ monic irreducible}, \ \psi(P)=-1} \chi(P) \right| \leq \frac{k+5}{n} q^{\frac{n}{2}}.$$
2. *For every* $n \in \mathbb{N}$, $n \geq 2$, n *odd*,
$$\left| \sum_{P \text{ monic irreducible}, \ \psi(P)=1} \chi(P) \right| \leq \frac{k+5}{n} q^{\frac{n}{2}}.$$

The latter, along with other results we have already seen yield:

- $$\sum_{H \in G_{k-1}} \Lambda(H) = \frac{q^k - 1}{q - 1},$$
- $$\left| \sum_{\substack{\deg(H)=n \\ H_0=1}} \Lambda(H)\chi(H) \right| \leq 1 + kq^{\frac{n}{2}}, \quad \text{for } n \geq 1.$$
- $$\left| \sum_{\substack{P \text{ irreducible} \\ P_0=1, \psi(P)=\varepsilon}} \chi(P) \right| \leq \tfrac{k+5}{n} q^{\frac{n}{2}}, \quad \text{for } n \geq 2,$$

where χ is a non-trivial Dirichlet character modulo X^{k+1}, such that $\chi(\mathbb{F}_q^*) = 1$ and either $\varepsilon = -1$, or $\varepsilon = 1$ and n is odd.

All of the above combined give:

Theorem

Let $n \geq 2$, $1 \leq k \leq n$, and $a \in \mathbb{F}_q$. There exists a srimp $Q \in \mathbb{F}_q[X]$, of degree $2n$ with $Q_k = a$ if the following bound holds.

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

Further, Carlitz (1967) computed $\pi_q(n, \varepsilon)$ and those computations imply

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

hence:

Theorem

Let $n \geq 2$, $1 \leq k \leq n$, and $a \in \mathbb{F}_q$. There exists a srimp $Q \in \mathbb{F}_q[X]$, of degree $2n$ with $Q_k = a$ if the following bound holds.

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

Our final step is to content ourselves for $k \leq n/2$ and solve the resulting problem. Using the theory developed earlier, we conclude that there exists a srimp over $\mathbb{F}_q$ of degree $2n$ with its k-th coefficient prescribed, if

$$\pi_q(n,-1) > \frac{\lfloor n/2 \rfloor (\lfloor n/2 \rfloor + 5)}{n} (\sqrt{q}+1)(q^{\lfloor n/2 \rfloor /2} - 1) q^{n/2}.$$

This bound is always true for $n \geq 27$. For $n < 27$ this bound is satisfied for the pairs (q,n) described below

n	3	4	5	6	7	8	9	10
q	≥ 149	≥ 839	≥ 37	≥ 59	≥ 17	≥ 23	≥ 11	≥ 13
n	11	12	13	14	15	16	17	18
q	≥ 9	≥ 9	≥ 7	≥ 7	≥ 5	≥ 7	≥ 5	≥ 5
n	19	20	21	22	23	24	25	26
q	≥ 5	≥ 5	≥ 5	≥ 5	≥ 5	≥ 5	≥ 3	≥ 5

Summing up, we have theoretically proved that:

Corollary

If $n \geq 3$ an integer and q a power of an odd prime, then there exists a srimp of degree $2n$ such that any of its $\lfloor n/2 \rfloor$ low degree coefficients is prescribed, if either $n \geq 27$ or $q \geq 839$.

For the remaining cases, computers searches have been employed. The computer results, combined with the above imply the following.

Theorem

Let $n \geq 3$ an integer and q a power of an odd prime. If $k \leq n/2$ and $a \in \mathbb{F}_q$, then there exists a srimp of degree $2n$ such that any of its k-th coefficient is prescribed to a, unless

1. $q = 3$, $n = 3$, $a = 0$ *and* $k = 1$ *or*
2. $q = 3$, $n = 4$, $a = 0$ *and* $k = 2$.

1. Can we extend this to $k \geq n/2$?
2. What about even q?

Now, we present some of the extensions of the HMC for irreducible polynomials that various authors have considered.

- Many authors have considered prescribing the norn and the trace of an irreducible polynomial (Wan (1997), Car (1999), Moisio (2008) and Omidi Koma, Panario and Wang (2010)).
- Cohen (2005) proved that there exists an irreducible polynomial of degree n with its first k and last m coefficients prescribed whenever $2 \leq k + m \leq n/3$.
- Garefalakis (2008) considered consecutive zero coefficients and he proved that for any c with $0 < c < 1$ and any positive integer n such that $(1 - 3c)n \geq 2 + 8 \log_q n$, there exists an irreducible polynomial of degree n over $\mathbb{F}_q$ with any $\lfloor cn \rfloor$ consecutive coefficients (other than the first or last) equal to 0.
- Panario and Tzanakis (2012), Pollack (2013) and Ha (2016) considered prescribing multiple coefficients of an irreducible polynomial.

Similarly, much effort has been given in extending the HMC for primitive polynomials.

- Many authors have considerd prescribing the norm and trace of a primitive polynomial (Cohen and Hachenberger (1999, 2000), Cohen (2000, 2012), Cohen and Huczynska (2003), Fan and Wang (2009)).
- Chou and Cohen (2001) fixed the coefficient of X and the trace to 0, given that $n \geq 5$.
- There are several results about prescribing the first two (Han (1996, 2009), Bao (1997), Cohen and Mills (2003), Cohen and King (2004) and Shuqin and Wenbao (2004)) and the first three (Cohen and King (2004), Fan and Han (2004) and Mills (2004)) coefficients of a primitive polynomial.
- Cohen and King (2004) and Fan and Han (2004) provided asymptotic results about the existence of primitives with their first $\lfloor (n-1)/2 \rfloor$ coefficients prescribed.
- Cohen (2004) proved that the first m, where $m \leq n/3$, coefficients of a primitive polynomial can be prescribed.

Another setting that has been investigated is prescribing coefficients of primitive and normal polynomials, where normal polynomials are those whose roots constitute a normal basis, that is a basis of the form $\{x, x^q, \ldots, x^{q^{n-1}}\}$.

- Fan and Wang (2009) proved that there exists a primitive normal polynomial with a prescribed coefficient when $n \geq 15$.
- Several efforts have been made in fixing the norm and trace of a primitive normal polynomial (Cohen (2000), Cohen and Hachenberger (2000) and Cohen and Huczynska (2003)).
- Fan and Wang (2009) proved the existence of a primitive normal polynomial with its first two coefficients prescribed if $n \geq 5$.
- Asymptotic results about prescribing the last $\lfloor n/2 \rfloor$ (Fan and Han (2007)) and the first $\lfloor n/2 \rfloor$ (Fan (2009)) have also been established.

Finally, it is worth mentioning that recently several different approaches have emerged.

- Ha [*Finite Fields Appl.* 40:10–25, 2016] introduced number-theoretic methods of Bourgain (2015) that enabled him to prescribe r coefficients, given that $r \leq (1/4 - \epsilon)n$, for any $\epsilon > 0$. This work improved previous work of Pollack (2013), where $r \leq (1/4 - \epsilon)\sqrt{n}$.
- Tuxanidy and Wang (A new proof of the Hansen-Mullen irreducibility conjecture, arXiv:1604.0423 [math.NT], unpublished. Irreducible polynomials with prescribed sums of coefficients, unpublished) have also introduced a new promising method to the area.

Thank You!