

On a generalization of the Hansen-Mullen conjecture for irreducible polynomials with a fixed coefficient

Georgios Tzanakis

Carleton University

July 21, 2010



Questions about irreducible polynomials with fixed coefficients:

- Estimate their number
- Examine their existence

Introduction

Fixed coefficients

Dirichlet's Theorem

Background

A generalization of the
H-M conjecture

Wan's method

Variation

The generalization

Other results

Open questions



Questions about irreducible polynomials with fixed coefficients:

- Estimate their number
- Examine their existence

Two interesting cases:

- Hansen-Mullen conjecture
- Consecutive zero coefficients

Introduction

Fixed coefficients

Dirichlet's Theorem

Background

A generalization of the
H-M conjecture

Wan's method

Variation

The generalization

Other results

Open questions



Questions about irreducible polynomials with fixed coefficients:

- Estimate their number
- Examine their existence

Two interesting cases:

- Hansen-Mullen conjecture
- Consecutive zero coefficients

Hansen-Mullen conjecture (proven by Wan)

Let m and n integers with $n \geq 3$, $n \geq m \geq 1$, and $\alpha \in \mathbb{F}_q$. There exists a monic irreducible polynomial of degree n over \mathbb{F}_q with the coefficient of x^{m-1} being α .

Introduction

Fixed coefficients

Dirichlet's Theorem

Background

A generalization of the
H-M conjecture

Wan's method

Variation

The generalization

Other results

Open questions



Questions about irreducible polynomials with fixed coefficients:

- Estimate their number
- Examine their existence

Two interesting cases:

- Hansen-Mullen conjecture
- Consecutive zero coefficients

Hansen-Mullen conjecture (proven by Wan)

Let m and n integers with $n \geq 3$, $n \geq m \geq 1$, and $\alpha \in \mathbb{F}_q$. There exists a monic irreducible polynomial of degree n over \mathbb{F}_q with the coefficient of x^{m-1} being α .

Generalization of the Hansen-Mullen conjecture

Do irreducible polynomials exist with any 2 or more coefficients fixed to any elements of \mathbb{F}_q ?



Let $f, g \in \mathbb{F}_q[x]$ be coprime, and $\pi(n, f, g)$ be the number of monic irreducible polynomials of degree n which are congruent to g modulo f .

On a generalization of the H-M conjecture

Georgios Tzanakis

Introduction

Fixed coefficients

Dirichlet's Theorem

Background

A generalization of the H-M conjecture

Wan's method

Variation

The generalization

Other results

Open questions



Let $f, g \in \mathbb{F}_q[x]$ be coprime, and $\pi(n, f, g)$ be the number of monic irreducible polynomials of degree n which are congruent to g modulo f .

Bounds for $\pi(n, f, g)$ give the analogue of Dirichlet's theorem for primes in arithmetic progressions.

On a generalization of the H-M conjecture

Georgios Tzanakis

Introduction

Fixed coefficients

Dirichlet's Theorem

Background

A generalization of the H-M conjecture

Wan's method

Variation

The generalization

Other results

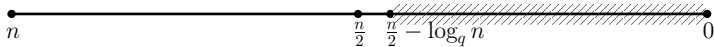
Open questions




Let $f, g \in \mathbb{F}_q[x]$ be coprime, and $\pi(n, f, g)$ be the number of monic irreducible polynomials of degree n which are congruent to g modulo f .

Bounds for $\pi(n, f, g)$ give the analogue of Dirichlet's theorem for primes in arithmetic progressions.

For suitable choice of g and f , we get the following:



 = coefficients that can be prescribed to any value

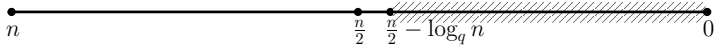
and



Let $f, g \in \mathbb{F}_q[x]$ be coprime, and $\pi(n, f, g)$ be the number of monic irreducible polynomials of degree n which are congruent to g modulo f .

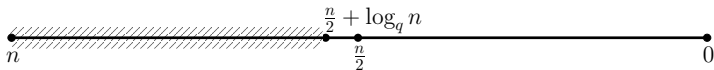
Bounds for $\pi(n, f, g)$ give the analogue of Dirichlet's theorem for primes in arithmetic progressions.

For suitable choice of g and f , we get the following:



= coefficients that can be prescribed to any value

and



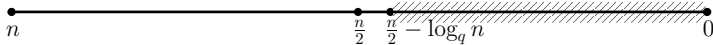
= coefficients that can be prescribed to any value




Let $f, g \in \mathbb{F}_q[x]$ be coprime, and $\pi(n, f, g)$ be the number of monic irreducible polynomials of degree n which are congruent to g modulo f .

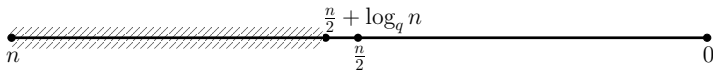
Bounds for $\pi(n, f, g)$ give the analogue of Dirichlet's theorem for primes in arithmetic progressions.


For suitable choice of g and f , we get the following:



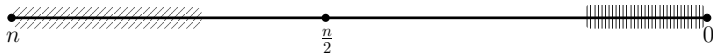
 = coefficients that can be prescribed to any value



and



 = coefficients that can be prescribed to any value

More generally,



,  = coefficients that can be prescribed to any value

$$\text{diagonal lines} + \text{vertical lines} \leq \frac{n}{2} - \log_q n$$



Introduction

Fixed coefficients
Dirichlet's Theorem

Background

A generalization of the
H-M conjecture

Wan's method
Variation

The generalization
Other results

Open questions

Definition

Let $f \in \mathbb{F}_q[x]$. A Dirichlet character modulo f , is a map χ from $\mathbb{F}_q[x]$ to \mathbb{C} such that for all $a, b \in \mathbb{F}_q[x]$ we have

- 1 $\chi(a + bf) = \chi(a)$
- 2 $\chi(a)\chi(b) = \chi(ab)$
- 3 $\chi(a) = 0 \Leftrightarrow (a, f) \neq 1$



Definition

Let $f \in \mathbb{F}_q[x]$. A Dirichlet character modulo f , is a map χ from $\mathbb{F}_q[x]$ to \mathbb{C} such that for all $a, b \in \mathbb{F}_q[x]$ we have

- 1 $\chi(a + bf) = \chi(a)$
- 2 $\chi(a)\chi(b) = \chi(ab)$
- 3 $\chi(a) = 0 \Leftrightarrow (a, f) \neq 1$

Consider the sums:

$$c_n(\chi) = \sum_{g \in \mathbb{M}_n} \Lambda(g)\chi(g)$$

$$c_n'(\chi) = \sum_{P \in \mathbb{I}_n} \chi(P)$$



Introduction

Fixed coefficients

Dirichlet's Theorem

Background

A generalization of the
H-M conjecture

Wan's method

Variation

The generalization

Other results

Open questions

Bounds (Weil)

Let $f \in \mathbb{F}_q[x]$ and χ a Dirichlet character modulo f . We have

$$|c_n(\chi)| \leq (\deg(f) - 1)q^{n/2},$$

$$c_n(\chi_0) = q^n,$$

and

$$|c_n'(\chi)| \leq \frac{\deg(f)}{n} q^{n/2},$$

$$|c_n'(\chi_0)| \leq |\mathbb{I}_n|.$$



Let $\alpha \in \mathbb{F}_q^*$, $n \geq m \geq 1$. Consider

$$\begin{aligned}
 W &= \sum_{h \in \alpha \mathbb{H}_{m-1}} \Lambda(h) \sum_{\substack{P \in \mathbb{I}_n \\ P \equiv h \pmod{x^m}}} 1 \\
 &= \sum_{h \in \alpha \mathbb{H}_{m-1}} \Lambda(h) \left(\sum_{P \in \mathbb{I}_n} \frac{1}{\Phi(x^m)} \sum_{\chi \in X_{x^m}} \chi(P) \overline{\chi(h)} \right) \\
 &= \frac{1}{\Phi(x^m)} \sum_{\chi \in X_{x^m}} \chi(\alpha) \sum_{h \in \mathbb{H}_{m-1}} \Lambda(h) \overline{\chi(h)} \sum_{P \in \mathbb{I}_n} \chi(P) \\
 &= \frac{1}{\Phi(x^m)} \sum_{\chi \in X_{x^m}} \chi(\alpha) c_{m-1}(\overline{\chi}) c_n'(\chi).
 \end{aligned}$$

Introduction

Fixed coefficients

Dirichlet's Theorem

Background

A generalization of the
H-M conjecture

Wan's method

Variation

The generalization

Other results

Open questions



Let $\alpha \in \mathbb{F}_q^*$, $n \geq m \geq 1$. Consider

$$\begin{aligned}
 W &= \sum_{h \in \alpha \mathbb{H}_{m-1}} \Lambda(h) \sum_{\substack{P \in \mathbb{I}_n \\ P \equiv h \pmod{x^m}}} 1 \\
 &= \sum_{h \in \alpha \mathbb{H}_{m-1}} \Lambda(h) \left(\sum_{P \in \mathbb{I}_n} \frac{1}{\Phi(x^m)} \sum_{\chi \in X_{x^m}} \chi(P) \overline{\chi(h)} \right) \\
 &= \frac{1}{\Phi(x^m)} \sum_{\chi \in X_{x^m}} \chi(\alpha) \sum_{h \in \mathbb{H}_{m-1}} \Lambda(h) \overline{\chi(h)} \sum_{P \in \mathbb{I}_n} \chi(P) \\
 &= \frac{1}{\Phi(x^m)} \sum_{\chi \in X_{x^m}} \chi(\alpha) c_{m-1}(\overline{\chi}) c_n'(\chi).
 \end{aligned}$$

With the help of the Weil bound, we obtain a lower bound for W .

Introduction

Fixed coefficients

Dirichlet's Theorem

Background

A generalization of the
H-M conjecture

Wan's method

Variation

The generalization

Other results

Open questions



Let $\alpha \in \mathbb{F}_q^*$, $n \geq m \geq 1$. Consider

$$\begin{aligned}
 W &= \sum_{h \in \alpha \mathbb{H}_{m-1}} \Lambda(h) \sum_{\substack{P \in \mathbb{I}_n \\ P \equiv h \pmod{x^m}}} 1 \\
 &= \sum_{h \in \alpha \mathbb{H}_{m-1}} \Lambda(h) \left(\sum_{P \in \mathbb{I}_n} \frac{1}{\Phi(x^m)} \sum_{\chi \in X_{x^m}} \chi(P) \overline{\chi(h)} \right) \\
 &= \frac{1}{\Phi(x^m)} \sum_{\chi \in X_{x^m}} \chi(\alpha) \sum_{h \in \mathbb{H}_{m-1}} \Lambda(h) \overline{\chi(h)} \sum_{P \in \mathbb{I}_n} \chi(P) \\
 &= \frac{1}{\Phi(x^m)} \sum_{\chi \in X_{x^m}} \chi(\alpha) c_{m-1}(\overline{\chi}) c_n'(\chi).
 \end{aligned}$$

With the help of the Weil bound, we obtain a lower bound for W .
When $q^{n-m+1} \geq (q-1)^2 m^4$, W is positive.

Introduction

Fixed coefficients

Dirichlet's Theorem

Background

A generalization of the
H-M conjecture

Wan's method

Variation

The generalization

Other results

Open questions



Let $n \geq m_1 \geq l_1 > m_2 \geq l_2 \cdots > m_r \geq l_r \geq 1$ and $\alpha_1, \dots, \alpha_r \in \mathbb{F}_q^*$.
Set $m = \sum_i m_i$, $l = \sum_i l_i$.

Consider

$$W' = \sum_{h_1 \in \alpha_1 \mathbb{H}_{l_1-1}} \Lambda(h_1) \sum_{h_2 \in \alpha_2 \mathbb{H}_{l_2-1}} \Lambda(h_2) \cdots \sum_{h_r \in \alpha_r \mathbb{H}_{l_r-1}} \Lambda(h_r) \sum_P 1$$

where the last sum is taken over all $P \in \mathbb{I}_n$ such that $P \equiv h_i \pmod{x_i^{m_i}}$.

[Introduction](#)[Fixed coefficients](#)[Dirichlet's Theorem](#)[Background](#)[A generalization of the
H-M conjecture](#)[Wan's method](#)**Variation**[The generalization](#)[Other results](#)[Open questions](#)

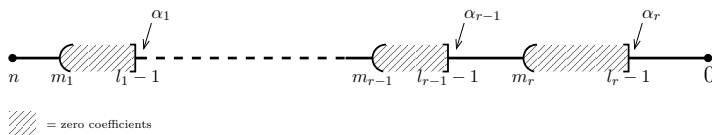
Variation of Wan's method

Let $n \geq m_1 \geq l_1 > m_2 \geq l_2 \cdots > m_r \geq l_r \geq 1$ and $\alpha_1, \dots, \alpha_r \in \mathbb{F}_q^*$.
Set $m = \sum_i m_i$, $l = \sum_i l_i$.

Consider

$$W' = \sum_{h_1 \in \alpha_1 \mathbb{H}_{l_1-1}} \Lambda(h_1) \sum_{h_2 \in \alpha_2 \mathbb{H}_{l_2-1}} \Lambda(h_2) \cdots \sum_{h_r \in \alpha_r \mathbb{H}_{l_r-1}} \Lambda(h_r) \sum_P 1$$

where the last sum is taken over all $P \in \mathbb{I}_n$ such that $P \equiv h_i \pmod{x_i^{m_i}}$.



Introduction

Fixed coefficients
Dirichlet's Theorem

Background

A generalization of the
H-M conjecture

Wan's method

Variation

The generalization
Other results

Open questions



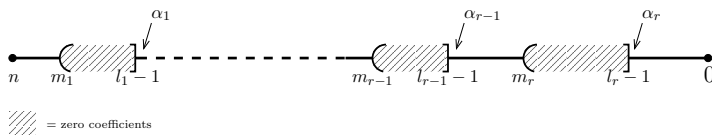
Variation of Wan's method

Let $n \geq m_1 \geq l_1 > m_2 \geq l_2 \cdots > m_r \geq l_r \geq 1$ and $\alpha_1, \dots, \alpha_r \in \mathbb{F}_q^*$.
Set $m = \sum_i m_i$, $l = \sum_i l_i$.

Consider

$$W' = \sum_{h_1 \in \alpha_1 \mathbb{H}_{l_1-1}} \Lambda(h_1) \sum_{h_2 \in \alpha_2 \mathbb{H}_{l_2-1}} \Lambda(h_2) \cdots \sum_{h_r \in \alpha_r \mathbb{H}_{l_r-1}} \Lambda(h_r) \sum_P 1$$

where the last sum is taken over all $P \in \mathbb{I}_n$ such that $P \equiv h_i \pmod{x_i^{m_i}}$.



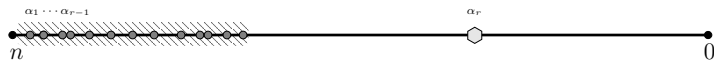
When $2m - l$ is less than roughly n , then $W' > 0$



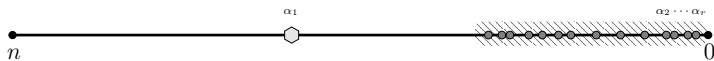
The generalization

Using this result we get the following:

There exists an irreducible polynomial of degree n with r coefficients fixed to any element of \mathbb{F}_q , if at least $r - 1$ of them are among roughly the $n/2r$ most or least significant ones.



OR




= roughly $\frac{n}{2r}$ = one prescribed coefficient anywhere = $r - 1$ prescribed coefficients in



When $2m - l$ is roughly less than n , then irreducible polynomials of the form below exist.



 = zero coefficients



When $2m - l$ is roughly less than n , then irreducible polynomials of the form below exist.



= zero coefficients

Let $\alpha \in \mathbb{F}_q$ and c be a real number such that $0 < c < 1/4$. Then there exists an integer n and an irreducible polynomial over \mathbb{F}_q with trace α and a sequence of $\lfloor cn \rfloor$ consecutive zero coefficients.



= roughly $\frac{n}{4}$ zero coefficients



- Can the Hansen-Mullen conjecture be generalized in two (or more) coefficients without restrictions?



- Can the Hansen-Mullen conjecture be generalized in two (or more) coefficients without restrictions?
- Can we estimate the number of the polynomials whose existence we examined?

