Polynomials with Restricted Digits

Aarhus Automorphic Forms Conference – Lightning Talks

Naomi Bazlov

Technion – Institute of Technology

11 August 2025

Primes with restricted digits

- Primes: $2, 3, 5, 7, \ldots 41, \ldots 89, \ldots 601, \ldots$

Primes with restricted digits

- Primes: $2, 3, 5, 7, \ldots 41, \ldots 89, \ldots 601, \ldots$
- Dirichlet's theorem for Primes in APs: infinitely many primes containing 7

Primes with restricted digits

- Primes: $2, 3, 5, 7, \ldots 41, \ldots 89, \ldots 601, \ldots$
- Dirichlet's theorem for Primes in APs: infinitely many primes containing 7
- Study of restricted digits began at the end of the 20^{th} century

Primes with restricted digits

- Primes: $2, 3, 5, 7, \ldots 41, \ldots 89, \ldots 601, \ldots$
- Dirichlet's theorem for Primes in APs: infinitely many primes containing 7
- Study of restricted digits began at the end of the 20^{th} century
- Maynard's instrumental papers gave concrete results!

Primes with restricted digits

- Primes: $2, 3, 5, 7, \ldots 41, \ldots 89, \ldots 601, \ldots$
- Dirichlet's theorem for Primes in APs: infinitely many primes containing 7
- Study of restricted digits began at the end of the 20^{th} century
- Maynard's instrumental papers gave concrete results!

Theorem (Maynard, 2015-6)

Let $q > 2,000,000$, $a_0 \in \{0, \ldots, q-1\}$ *and* $\mathcal{A} = \{\sum_{i \geq 0} n_i q^i : n_i \in \{0, \ldots, q-1\} \backslash \{a_0\}\}$.
Then for any constant $A > 0$,

$$\sum_{n < q^k} \Lambda(n) \mathbf{1}_{\mathcal{A}}(n) = \kappa_q(a_0)(q-1)^k + O_A\Big(\frac{(q-1)^k}{(\log q^k)^A}\Big).$$

Primes with restricted digits

- Primes: $2, 3, 5, 7, \ldots 41, \ldots 89, \ldots 601, \ldots$
- Dirichlet's theorem for Primes in APs: infinitely many primes containing 7
- Study of restricted digits began at the end of the 20^{th} century
- Maynard's instrumental papers gave concrete results!

Theorem (Maynard, 2015-6)

Let $q > 2,000,000$, $a_0 \in \{0, \ldots, q-1\}$ *and* $\mathcal{A} = \{\sum_{i \geq 0} n_i q^i : n_i \in \{0, \ldots, q-1\} \backslash \{a_0\}\}$.
There are infinitely many primes with no digit a_0 *when written in base* q.

Primes with restricted digits

- Primes: $2, 3, 5, 7, \ldots 41, \ldots 89, \ldots 601, \ldots$
- Dirichlet's theorem for Primes in APs: infinitely many primes containing 7
- Study of restricted digits began at the end of the 20^{th} century
- Maynard's instrumental papers gave concrete results!

Theorem (Maynard, 2015-6)

Let $q = 10$, $a_0 \in \{0, \ldots, q-1\}$ *and*
$\mathcal{A} = \{\sum_{i \geq 0} n_i q^i : n_i \in \{0, \ldots, q-1\} \backslash \{a_0\}\}$.
There are infinitely many primes with no digit a_0 *when written in base* q.

The Function Field Analogue

$\mathbb{Z}$	$\mathbb{F}_q[t]$
Rational prime	Irreducible polynomial
Base b	q
Digit	Coefficient

The Function Field Analogue

$\mathbb{Z}$	$\mathbb{F}_q[t]$
Rational prime	Irreducible polynomial
Base b	q
Digit	Coefficient

- 1924, Artin: analogue of Prime Number Theorem for APs for $\mathbb{F}_q[t]$

The Function Field Analogue

$\mathbb{Z}$	$\mathbb{F}_q[t]$
Rational prime	Irreducible polynomial
Base b	q
Digit	Coefficient

- 1924, Artin: analogue of Prime Number Theorem for APs for $\mathbb{F}_q[t]$
- Cohen, Hayes' work in the 1960s onwards

The Function Field Analogue

$\mathbb{Z}$	$\mathbb{F}_q[t]$
Rational prime	Irreducible polynomial
Base b	q
Digit	Coefficient

- 1924, Artin: analogue of Prime Number Theorem for APs for $\mathbb{F}_q[t]$
- Cohen, Hayes' work in the 1960s onwards

THEOREM 5.3. *If* $t \in \mathscr{W}_H$, *then*

$$\left| f(t) - \frac{1}{q^s \Phi(H)} \cdot \frac{q^r}{r} \cdot T_H(t) \right| < 2q^{1/4} q^{(1/4+\Theta)r}, \tag{5.7}$$

where $\Phi(H)$ *is the number of polynomials in a reduced residue system modulo* H.

Hayes, D. "The expression of a polynomial as a sum of three irreducibles." *Acta Arithmetica* **11.4** (1966): 461-488.

Porritt's work on polynomials with restricted digits

- Circle method setup:
  - $\mathbb{F}_q((1/t)) = \{ \sum_{i \leq j} x_i t^i \ : \ x_i \in \mathbb{F}_q, \ j \in \mathbb{Z} \}$, polynomial norm

Porritt's work on polynomials with restricted digits

- Circle method setup:
  - $\mathbb{F}_q((1/t)) = \{ \sum_{i \leq j} x_i t^i \ : \ x_i \in \mathbb{F}_q, \ j \in \mathbb{Z} \}$, polynomial norm
  - 'Circle': $\mathbb{T} := \{\sum_{i<0} x_i t^i \ : \ x_i \in \mathbb{F}_q\}$, the maximal ideal of $\mathbb{F}_q[1/t]$

Porritt's work on polynomials with restricted digits

- Circle method setup:
  - $\mathbb{F}_q((1/t)) = \{ \sum_{i \leq j} x_i t^i \ : \ x_i \in \mathbb{F}_q, \ j \in \mathbb{Z} \}$, polynomial norm
  - 'Circle': $\mathbb{T} := \{\sum_{i<0} x_i t^i \ : \ x_i \in \mathbb{F}_q\}$, the maximal ideal of $\mathbb{F}_q[1/t]$
  - Additive character $\mathbf{e}_q : \mathbb{F}_q((1/t)) \to \mathbb{C}^\times$, Haar measure, $S_{\mathcal{R}}(x) = \sum_{m \in \mathcal{M}_{\mathcal{R}}(n)} \mathbf{e}_q(mx)$

Porritt's work on polynomials with restricted digits

- Circle method setup:
  - $\mathbb{F}_q((1/t)) = \{ \sum_{i \le j} x_i t^i \ : \ x_i \in \mathbb{F}_q,\ j \in \mathbb{Z} \}$, polynomial norm
  - 'Circle': $\mathbb{T} := \{\sum_{i<0} x_i t^i \ : \ x_i \in \mathbb{F}_q\}$, the maximal ideal of $\mathbb{F}_q[1/t]$
  - Additive character $\mathbf{e}_q : \mathbb{F}_q((1/t)) \to \mathbb{C}^\times$, Haar measure, $S_{\mathcal{R}}(x) = \sum_{m \in \mathcal{M}_{\mathcal{R}}(n)} \mathbf{e}_q(mx)$

$$N(\mathcal{R}, n) = \int_{\mathbb{T}} \sum_{\substack{\deg p = n \\ p \text{ monic irred.}}} \mathbf{e}_q(px) \cdot \overline{S_{\mathcal{R}}(x)} dx.$$

Porritt's work on polynomials with restricted digits

- Circle method setup:
  - $\mathbb{F}_q((1/t)) = \{ \sum_{i \leq j} x_i t^i \ : \ x_i \in \mathbb{F}_q, \ j \in \mathbb{Z} \}$, polynomial norm
  - 'Circle': $\mathbb{T} := \{\sum_{i<0} x_i t^i \ : \ x_i \in \mathbb{F}_q\}$, the maximal ideal of $\mathbb{F}_q[1/t]$
  - Additive character $\mathbf{e}_q : \mathbb{F}_q((1/t)) \to \mathbb{C}^\times$, Haar measure, $S_{\mathcal{R}}(x) = \sum_{m \in \mathcal{M}_{\mathcal{R}}(n)} \mathbf{e}_q(mx)$

$$N(\mathcal{R}, n) = \int_{\mathbb{T}} S(x) \cdot \overline{S_{\mathcal{R}}(x)} dx.$$

Porritt's work on polynomials with restricted digits

- Circle method setup:
  - $\mathbb{F}_q((1/t)) = \{ \sum_{i \le j} x_i t^i \ : \ x_i \in \mathbb{F}_q, \ j \in \mathbb{Z} \}$, polynomial norm
  - 'Circle': $\mathbb{T} := \{\sum_{i<0} x_i t^i \ : \ x_i \in \mathbb{F}_q\}$, the maximal ideal of $\mathbb{F}_q[1/t]$
  - Additive character $\mathbf{e}_q : \mathbb{F}_q((1/t)) \to \mathbb{C}^\times$, Haar measure, $S_{\mathcal{R}}(x) = \sum_{m \in \mathcal{M}_{\mathcal{R}}(n)} \mathbf{e}_q(mx)$

$$N(\mathcal{R}, n) = \int_{\mathbb{T}} S(x) \cdot \overline{S_{\mathcal{R}}(x)} dx.$$

Lemma (from Hayes, 1966)

$a, g \in \mathbb{F}_q[t]$ two coprime polynomials, $\gamma \in \mathbb{T}$ s.t. $|a| < |g| \le q^{n/2}$ and $|\gamma| < 1/q^{\deg g + n/2}$; $|E| \le q^{n - \frac{1}{2}[\frac{n}{2}]}$:

$$S\left(\frac{a}{g} + \gamma\right) = \frac{\mu(g)}{\phi(g)} \pi(n) \mathbf{e}_q(\gamma t^n) \mathbf{1}_{|\gamma| < 1/q^n} + E$$

Porritt's work on polynomials with restricted digits

- Circle method setup:
  - $\mathbb{F}_q((1/t)) = \{ \sum_{i \le j} x_i t^i \ : \ x_i \in \mathbb{F}_q, \ j \in \mathbb{Z} \}$, polynomial norm
  - 'Circle': $\mathbb{T} := \{\sum_{i<0} x_i t^i \ : \ x_i \in \mathbb{F}_q\}$, the maximal ideal of $\mathbb{F}_q[1/t]$
  - Additive character $\mathbf{e}_q : \mathbb{F}_q((1/t)) \to \mathbb{C}^\times$, Haar measure, $S_{\mathcal{R}}(x) = \sum_{m \in \mathcal{M}_{\mathcal{R}}(n)} \mathbf{e}_q(mx)$

$$N(\mathcal{R}, n) = \int_{\mathbb{T}} S(x) \cdot \overline{S_{\mathcal{R}}(x)} dx.$$

Lemma (Porritt, 2017)

Let $a, g \in \mathbb{F}_q[t]$ be coprime polynomials with $|a| < |g|$, g not a power of t and let $k = \deg g > 0$. Then

$$|S_{\mathcal{R}}(a/g)| \le (q-s)^{n-[\frac{n}{k}]} s^{[\frac{n}{k}]}.$$

A result of Porritt

Theorem

Let $\mathcal{R} \subset \mathbb{F}_q$ be a subset of size s and assume $s < \sqrt{q}/2$.
Suppose that $q \geq 500$ and $n \geq 100(\log q)^2$.
The number of irreducible, monic polynomials of degree n with coefficients only from $\mathbb{F}_q \backslash \mathcal{R}$ (except possibly the leading 1) is given by

$$\frac{q}{q-1}\frac{(q-s)^n}{n}\left(\Lambda + O\left(q^{-n^{1/2}/7}\right)\right),$$

where

$$\Lambda = \begin{cases} 1 & \text{if } 0 \in \mathcal{R} \\ 1 - \frac{1}{q-s} & \text{if } 0 \notin \mathcal{R}. \end{cases}$$

Squarefree polynomials

- Squarefree polynomials are not divisible by the square of any irreducible polynomial

Squarefree polynomials

- Squarefree polynomials are not divisible by the square of any irreducible polynomial
- Estimate $\#N' = \#\{f : P^2 \nmid f, \deg P \text{ small}\}$, then check that $\#N'' = \#\{f : \exists P, P^2 \mid f, \deg P \text{ large}\}$ gives a small contribution

Squarefree polynomials

- Squarefree polynomials are not divisible by the square of any irreducible polynomial
- Estimate $\#N' = \#\{f : P^2 \nmid f, \deg P \text{ small}\}$, then check that $\#N'' = \#\{f : \exists P, P^2 \mid f, \deg P \text{ large}\}$ gives a small contribution
- To exclude small primes, use the Brun sieve
- For the large primes, we make use of the function field:

Squarefree polynomials

- Squarefree polynomials are not divisible by the square of any irreducible polynomial
- Estimate $\#N' = \#\{f : P^2 \nmid f, \deg P \text{ small}\}$, then check that $\#N'' = \#\{f : \exists P, P^2 \mid f, \deg P \text{ large}\}$ gives a small contribution
- To exclude small primes, use the Brun sieve
- For the large primes, we make use of the function field:
  - Bound by a triple sum $\sum_{d \in T_n} \sum_{\substack{P \mid d \\ \deg P > m_2}} \sum_{\substack{f \in S_n \\ f' = d \\ P \mid f}} 1$
  - Inner sum is easy to crudely bound
  - Innermost sum depends on how the coefficients of f indexed by multiples of p, the characteristic of $\mathbb{F}_q$.

Small primes approach

The 'small' range will consist of primes of degree up to some m_1.

Small primes approach

The 'small' range will consist of primes of degree up to some m_1.

$$\#N' = \sum_{j=0}^{\infty}(-1)^j \sum_{\substack{D|\mathcal{P}(m_1) \\ \omega(D)=j}} \#\{m \in \mathcal{M}_{\mathcal{R}}^n : D^2 \mid m\}. \qquad (1)$$

Small primes approach

The 'small' range will consist of primes of degree up to some m_1.

$$\#N' = \sum_{j=0}^{\infty}(-1)^j \sum_{\substack{D|\mathcal{P}(m_1)\\ \omega(D)=j}} \#\{m \in \mathcal{M}_{\mathcal{R}}^n : D^2 \mid m\}. \qquad (1)$$

$$\sum_{m\in\mathcal{M}_{\mathcal{R}}} \mathbb{1}_{g|m} = \sum_{m\in\mathcal{M}_{\mathcal{R}}} \frac{1}{|g|} \sum_{\deg a<\deg g} \mathbf{e}_q\left(\frac{am}{g}\right) = \frac{1}{|g|} \sum_{\deg a<\deg g} S_{\mathcal{R}}\left(\frac{a}{g}\right)$$

Lemma (Porritt, 2017)

Let $a, g \in \mathbb{F}_q[t]$ be coprime polynomials with $|a| < |g|$, g not a power of t and let $k = \deg g > 0$. Then

$$|S_{\mathcal{R}}(a/g)| \leq (q-s)^{n-[\frac{n}{k}]}s^{[\frac{n}{k}]}.$$

Large primes approach

- S_n is the set of degree n polynomials with restricted coefficients, and T_n is the set of derivatives of elements of S_n

Large primes approach

- S_n is the set of degree n polynomials with restricted coefficients, and T_n is the set of derivatives of elements of S_n
- $\#S_n = (q-s)^n$

Large primes approach

- S_n is the set of degree n polynomials with restricted coefficients, and T_n is the set of derivatives of elements of S_n
- $\#S_n = (q-s)^n$

$$\sum_{d \in T_n} \sum_{\substack{P \mid d \\ \deg P > m_2}} \sum_{\substack{f \in S_n \\ f' = d \\ P \mid f}} 1$$

Large primes approach

- S_n is the set of degree n polynomials with restricted coefficients, and T_n is the set of derivatives of elements of S_n
- $\#S_n = (q-s)^n$

$$(q-s)^{n-1-\lceil \frac{n-1}{p} \rceil} \sum_{\substack{P|d \\ \deg P > m_2}} \sum_{\substack{f \in S_n \\ f'=d \\ P|f}} 1$$

Large primes approach

- S_n is the set of degree n polynomials with restricted coefficients, and T_n is the set of derivatives of elements of S_n
- $\#S_n = (q-s)^n$

$$(q-s)^{n-1-\lceil \frac{n-1}{p} \rceil} \cdot \frac{n-1}{m_2} \cdot \sum_{\substack{f \in S_n \\ f'=d \\ P|f}} 1$$

Large primes approach

$$(q-s)^{n-1-\lceil \frac{n-1}{p} \rceil} \cdot \frac{n-1}{m_2} \cdot \sum_{\substack{f \in S_n \\ f'=d \\ P|f}} 1$$

If $f' = d$ then $f = f_0 + \sum_{i \leq n/p} a_i t^{pi}$, where $f_0' = d$. Since $f \equiv 0 \pmod{P}$ and we are over the finite field $\mathbb{F}_q$ of characteristic p, we get $f_0 + (\sum_{i \leq n/p} a_i^{q/p} t^i)^p \equiv 0 \pmod{P}$ and hence $\sum_{i \leq n/p} a_i^{q/p} t^i \equiv -f_0^{q^{\deg P}/p} \pmod{P}$

Large primes approach

If $f' = d$ then $f = f_0 + \sum_{i \leq n/p} a_i t^{pi}$, where $f_0' = d$. Since $f \equiv 0 \pmod{P}$ and we are over the finite field $\mathbb{F}_q$ of characteristic p, we get $f_0 + (\sum_{i \leq n/p} a_i^{q/p} t^i)^p \equiv 0 \pmod{P}$ and hence $\sum_{i \leq n/p} a_i^{q/p} t^i \equiv -f_0^{q^{\deg P}/p} \pmod{P}$

Lemma (B. 2025, after He-Pham-Xu, 2022)

Let $f(t) = \sum_{0 \leq i \leq n-1} \varepsilon_i t^i + t^n$ a polynomial of degree n in $\mathbb{F}_q[t]$, with ε_i independent and chosen uniformly at random from their respective allowed set of coefficients, $\mathcal{R}_i^c$. Then given a prime polynomial P,

$$\mathbb{P}[P \mid f] \leq \left(\frac{q-1+C}{q}\right)^{\deg P - 1}.$$

The result

Theorem (B.–Gorodetsky, 2025)

Let $\overline{\mathcal{R}} = (\mathcal{R}_1, \dots, \mathcal{R}_n) \subset \mathbb{F}_q^n$ be an ordered collection of subsets of size s. The number of squarefree, monic polynomials of degree n with the coefficient of t^{n-i} only from $\mathbb{F}_q \backslash \mathcal{R}_i$ is given by

$$\zeta_q^{-1}(2)(q-s)^n(1+o(1)).$$

The result

Theorem (B.–Gorodetsky, 2025)

Let $\overline{\mathcal{R}} = (\mathcal{R}_1, \dots, \mathcal{R}_n) \subset \mathbb{F}_q^n$ be an ordered collection of subsets of size s. The number of squarefree, monic polynomials of degree n with the coefficient of t^{n-i} only from $\mathbb{F}_q \backslash \mathcal{R}_i$ is given by

$$\zeta_q^{-1}(2)(q-s)^n(1+o(1)).$$

Thank you for listening!