Canad. Math. Bull. Vol. 62 (2), 2019 pp. 429–439
http://dx.doi.org/10.4153/CMB-2018-027-x

Irreducible Polynomials Over a Finite Field with Restricted Coefficients

Sam Porritt

Abstract. We prove a function field analogue of Maynard's celebrated result about primes with restricted digits. That is, for certain ranges of parameters n and q, we prove an asymptotic formula for the number of irreducible polynomials of degree n over a finite field $\mathbb{F}_q$ whose coefficients are restricted to lie in a given subset of $\mathbb{F}_q$.

1 Introduction

Many theorems concerning the existence of irreducible polynomials over a finite field of a special form have been proved. A discussion of such results can be found in [8]. In this paper we will prove a function field analogue of a result of Maynard [5] concerning primes with missing digits. He proved that for large enough integers b, the primes have the expected asymptotic density inside those integers that can be written in base b using only certain specified digits. We will prove the following natural analogue for polynomials in $\mathbb{F}_q[t]$.

Theorem 1.1 *Let $\mathcal{R} \subset \mathbb{F}_q$ be a subset of size s and assume that s is less than $\sqrt{q}/2$. Suppose that $q \geqslant 500$ and $n \geqslant 100(\log q)^2$. 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*

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

where

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

Remark Beyond stipulating that $s \leqslant \sqrt{q}$, the constraints on the sizes of s, q, and n are somewhat artificial, and were chosen with the aim of producing a more presentable error term. A more complicated, but more widely applicable, error term, from which the next two examples follow, is presented at the end of Section 4.

Received by the editors February 12, 2018.
Published electronically August 22, 2018.
This work was supported by the Engineering and Physical Sciences Research Council EP/L015234/1 via the EPSRC Centre for Doctoral Training in Geometry and Number Theory (The London School of Geometry and Number Theory), University College London.
AMS subject classification: **11T55**.
Keywords: finite field, irreducible polynomial, restricted coefficients.

Example 1.2 In the special case of $s = 1$, we get an asymptotic formula for any $q \geqslant 17$. In particular, we show that the number of irreducible polynomials of degree n with a single coefficient from $\mathbb{F}_{17}$ forbidden is asymptotic to $\Lambda \frac{16}{17}(16)^n/n$ as $n \to \infty$.

Example 1.3 An asymptotic formula still holds in the case of fixed n and $q \to \infty$, provided that $s = o(q^{1/2})$.

As in the integer setting, we can take s to be larger when the set $\mathcal{R}$ has additional structure. For example, in Section 5 we will prove the following theorem.

Theorem 1.4 *Suppose $\delta > 0$ and p is a prime sufficiently large in terms of δ. Then for any subset $\mathcal{R} = \{r, r+1, \dots, r+s-1\} \subset \mathbb{F}_p$ of s consecutive coefficients with $p - s > p^{3/4+\delta}$, the number of irreducible monic polynomials of degree n with coefficients only from $\mathbb{F}_p \backslash \mathcal{R}$ (except possibly the leading 1) is given by*

$$\frac{p}{p-1}\frac{(p-s)^n}{n}\Big(\Lambda + O(e^{-cn^{1/2}})\Big),$$

for some positive constant c depending on p and δ.

The integer version of Theorem 1.1 was proved in [5] under the assumption that the number of restricted digits s satisfies $s \leqslant b^{1/4-\delta}$ and the base b is sufficiently large in terms of δ. An analogue of Theorem 1.4 was proved under the assumption that $\mathcal{R} = \{0, 1, \dots, s-1\}$ and $s \leqslant b - b^{3/4+\delta}$. The proofs of Theorems 1.1 and 1.4 will use the circle method over $\mathbb{F}_q[t]$ along the lines of [3] and [5]. Two features make our arguments substantially simpler. First, we can make use of Weil's Riemann hypothesis for curves over a finite field which gives very good control for exponential sums over irreducibles. Second, we do not have to deal with any technicalities that arise from the fact that sometimes digits are 'carried' when rational integers are added. This does not happen with polynomials over a finite field.

For an overview of digit related results in the integers, see the recent work of Dietmann, Elsholtz, and Shparlinski [2] which also contains a section on finite fields, improving an earlier result of Dartyge, Mauduit, and Sárközy [1]. See also [6], which contains an extensive list of references to related problems.

2 Definitions and Set Up

This section introduces some notation. Let q be a prime power and $\mathbb{F}_q$ be the field with q elements and characteristic p. Let $\mathcal{R} = \{r_1, \dots, r_s\} \subset \mathbb{F}_q$ be a subset of *forbidden* coefficients. We are interested in counting monic (sometimes called *positive*) irreducible polynomials in $\mathbb{F}_q[t]$ of degree n, all of whose coefficients, apart from possibly the leading 1, are in the set $\mathcal{R}^c := \mathbb{F}_q \backslash \mathcal{R}$. The function field analogue of the real numbers is the completion of the field of fractions of $\mathbb{F}_q[t]$ with respect to the norm defined by

$$|f/g| = \begin{cases} q^{\deg f - \deg g} & \text{if } f \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

https://doi.org/10.4153/CMB-2018-027-x Published online by Cambridge University Press

This completion is naturally identified with the ring of formal Laurent series

$$\mathbb{F}_q((1/t)) = \Big\{ \sum_{i \leqslant j} x_i t^i : x_i \in \mathbb{F}_q, j \in \mathbb{Z} \Big\}.$$

The norm defined above is extended to $x = \sum_{i \leqslant j} x_i t^i \in \mathbb{F}_q((1/t))$ by setting $|x| = q^j$ where j is the largest index with $x_j \neq 0$. The subscript notation x_i will be used again to refer to the coefficient of t^i in x. The analogue of the real unit interval is $\mathbb{T} := \{\sum_{i<0} x_i t^i : x_i \in \mathbb{F}_q\}$, and is a subring of $\mathbb{F}_q((1/t))$. Define $\psi\colon \mathbb{F}_q \to \mathbb{C}^\times$ by

$$\psi(a) = \exp(2\pi i \operatorname{tr}(a)/p)$$

where $\operatorname{tr}\colon \mathbb{F}_q \to \mathbb{F}_p$ is the usual trace map. Also define the additive character $\mathbf{e}_q\colon \mathbb{F}_q((1/t)) \to \mathbb{C}^\times$ by $\mathbf{e}_q(x) = \psi(x_{-1})$. Fix a Haar measure on the additive group $\mathbb{T}$ normalised so that $\int_{\mathbb{T}} dx = 1$. Then for all $a \in \mathbb{F}_q[t]$, we have

$$\int_{\mathbb{T}} \mathbf{e}_q(ax)dx = \begin{cases} 1 & \text{if } a = 0, \\ 0 & \text{if } a \neq 0. \end{cases}$$

For $x \in \mathbb{T}$, define the sum over monic irreducible polynomials of degree n

$$S(x) = \sum_{\deg \omega = n} \mathbf{e}_q(\omega x).$$

Let $\mathcal{M}_{\mathcal{R}}(n)$ be the set of monic polynomials of degree n with non-leading coefficients taken from $\mathcal{R}^c$ and define

$$S_{\mathcal{R}}(x) = \sum_{m \in \mathcal{M}_{\mathcal{R}}(n)} \mathbf{e}_q(mx).$$

So $S(x)$ and $S_{\mathcal{R}}(x)$ depend on n even though this is not apparent from the notation. The main quantity of interest, the number of irreducible polynomials in $\mathcal{M}_{\mathcal{R}}(n)$, is then given by

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

We will make use of the important fact that for each $x \in \mathbb{T}$, there exist unique $a, g \in \mathbb{F}_q[t]$ with g monic, a and g coprime, and $|a| < |g| \leqslant q^{n/2}$ such that

$$\Big| x - \frac{a}{g} \Big| < \frac{1}{q^{\deg g + n/2}}.$$

This fact is [7, Lemma 3]. It implies that we can partition $\mathbb{T}$ into the so-called Farey arcs as

$$\mathbb{T} = \bigcup_{\substack{|a|<|g|\leqslant q^{n/2} \\ (a,g)=1}} \mathcal{F}\Big(\frac{a}{g}, q^{\deg g + n/2}\Big)$$

where $\mathcal{F}(\frac{a}{g}, \lambda) = \{x \in \mathbb{T} : |\frac{a}{g} - x| < \frac{1}{\lambda}\}$.

As usual, we let $\mu(f)$ denote the Möbius function, defined as $(-1)^k$ if f is the product of k distinct irreducibles and 0 otherwise. Let $\phi(f)$ be the size of the unit group $(\mathbb{F}_q[t]/(f))^\times$, that is, $|f|\prod_{\omega | f}(1 - 1/|\omega|)$, where the product is over all monic irreducibles dividing f. Finally, let $\pi(n)$ be the number of monic irreducible polynomials of degree n and recall the prime number theorem in the form $\sum_{d|n} d\pi(d) = q^n$.

https://doi.org/10.4153/CMB-2018-027-x Published online by Cambridge University Press

3 Lemmas

The sum $S(x)$ was analysed in [4]. Our first lemma is [7, Lemma 5] and is a consequence of Weil's Riemann Hypothesis for curves over a finite field.

Lemma 3.1 *Let $a, g \in \mathbb{F}_q[t]$ be two polynomials with $(a,g) = 1$ and $\gamma \in \mathbb{T}$, satisfying $|a| < |g| \leqslant q^{n/2}$ and $|\gamma| < 1/q^{\deg g + n/2}$. We have*

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

with $|E| \leqslant q^{n - \frac{1}{2}[\frac{n}{2}]}$.

For a subset $A \subset \mathbb{F}_q$, define the Fourier coefficient $\widehat{\mathbf{1}_A}(r) := \sum_{n \in A} \psi(nr)$. It turns out that the average value of $|S_{\mathcal{R}}(x)|$ can be written quite neatly in terms of the Fourier coefficients of the set $\mathcal{R}^c$.

Lemma 3.2

$$\int_{\mathbb{T}} |S_{\mathcal{R}}(x)| dx = \Big(\frac{1}{q} \sum_{r \in \mathbb{F}_q} |\widehat{\mathbf{1}_{\mathcal{R}^c}}(r)| \Big)^n .$$

Proof First

$$S_{\mathcal{R}}(x) = \sum_{m \in \mathcal{M}_{\mathcal{R}}(n)} \mathbf{e}_q(mx) = \mathbf{e}_q(xt^n) \prod_{i=0}^{n-1} \Big(\sum_{n_i \in \mathcal{R}^c} \mathbf{e}_q(x n_i t^i) \Big)$$
$$= \mathbf{e}_q(xt^n) \prod_{i=0}^{n-1} \Big(\sum_{n_i \in \mathcal{R}^c} \psi(n_i x_{-i-1}) \Big).$$

Notice that $|S_{\mathcal{R}}(x)|$ only depends on the leading n coefficients $(x_{-1}, \dots, x_{-n})$ of x and so, for each $a \in \mathbb{F}_q[t]$, $|S_{\mathcal{R}}(a/t^n + \gamma)|$ is constant in the range $|\gamma| < 1/q^n$, a set of measure $1/q^n$. Therefore,

$$\int_{\mathbb{T}} \big| S_{\mathcal{R}}(x) \big| dx = \frac{1}{q^n} \sum_{\deg a < n} \Big| S_{\mathcal{R}}\Big(\frac{a}{t^n} \Big) \Big| = \frac{1}{q^n} \sum_{\deg a < n} \Big| \prod_{i=0}^{n-1} \sum_{n_i \in \mathcal{R}^c} \psi(n_i a_{n-i-1}) \Big|$$
$$= \frac{1}{q^n} \sum_{\deg a < n} \prod_{i=0}^{n-1} \big| \widehat{\mathbf{1}_{\mathcal{R}^c}}(a_{n-i-1}) \big| = \frac{1}{q^n} \Big(\sum_{r \in \mathbb{F}_q} \big| \widehat{\mathbf{1}_{\mathcal{R}^c}}(r) \big| \Big)^n ,$$

which completes the proof of the lemma. ■

Corollary 3.3

$$\int_{\mathbb{T}} |S_{\mathcal{R}}(x)| dx \leqslant (\sqrt{s} + 1 - 2s/q)^n ,$$

with equality in the case $s = 1$.

Proof Notice that

$$\widehat{\mathbf{1}_{\mathcal{R}^c}}(r) + \widehat{\mathbf{1}_{\mathcal{R}}}(r) = \sum_{n \in \mathbb{F}_q} \psi(rn) = \begin{cases} q & \text{if } r = 0, \\ 0 & \text{if } r \neq 0. \end{cases}$$

https://doi.org/10.4153/CMB-2018-027-x Published online by Cambridge University Press

And hence,

$$\sum_{r\in\mathbb{F}_q}|\widehat{1_{\mathcal{R}^c}}(r)| = \sum_{r\in\mathbb{F}_q\setminus 0}|\widehat{1_{\mathcal{R}}}(r)| + |q-\widehat{1_{\mathcal{R}}}(0)| = \sum_{r\in\mathbb{F}_q}|\widehat{1_{\mathcal{R}}}(r)| + q - 2s.$$

It therefore suffices to show that $\sum_{r\in\mathbb{F}_q}|\widehat{1_{\mathcal{R}}}(r)| \leqslant q\sqrt{s}$. By the Cauchy–Schwarz inequality,

$$\Big(\sum_{r\in\mathbb{F}_q}|\widehat{1_{\mathcal{R}}}(r)|\Big)^2 \leqslant \Big(\sum_{r\in\mathbb{F}_q}1\Big)\Big(\sum_{r\in\mathbb{F}_q}\Big|\sum_{n\in\mathcal{R}}\psi(rn)\Big|^2\Big) = q\sum_{r\in\mathbb{F}_q}\sum_{n_1,n_2\in\mathcal{R}}\psi(r(n_1-n_2)).$$

By swapping the order of summation we see that the total contribution from the terms with $n_1 \neq n_2$ is 0. The terms $n_1 = n_2$ contribute $q^2 s$, as required. ■

The next lemma is similar to [7, Lemma 7].

Lemma 3.4 *Let $a, g \in \mathbb{F}_q[t]$ be coprime polynomials with $|a| < |g|$ and g not a power of t and let $d = \deg g > 0$. Then*

$$\Big|S_{\mathcal{R}}\Big(\frac{a}{g}\Big)\Big| \leqslant (q-s)^{n-[\frac{n}{d}]}s^{[\frac{n}{d}]}.$$

Proof Write $a/g = \sum_{i<0}x_i t^i$ and let z be the number of non-zeros amongst the x_i in the range $-n \leqslant i \leqslant -1$. Then, by our expression for $S_{\mathcal{R}}(a/q)$ from the start of the proof of Lemma 3.2, we have that

$$|S_{\mathcal{R}}(a/g)| = (q-s)^{n-z}\prod_{\substack{i=0\\ x_{-i-1}\neq 0}}^{n-1}\Big|\sum_{n_i\in\mathcal{R}}\psi(n_i x_{-i-1})\Big| \leqslant (q-s)^{n-z}s^z$$

by the triangle inequality. Since $q-s \geqslant s$, it suffices to show that $z \geqslant [\frac{n}{d}]$. We use proof by contradiction. Suppose $z \leqslant [\frac{n}{d}]-1$. Then, by the pigeonhole principle, there is some string of at least d consecutive zeros in $(x_{-n},\dots,x_{-1})$. Hence, $|\{t^r a/g\}| \leqslant 1/q^{d+1}$ for some integer $r \geqslant 0$ where $\{x\} = \sum_{i<0}x_i t^i$ denotes the fractional part of x. But this is a contradiction, since g does not divide $t^r a$ so we must have $|\{t^r a/g\}| \geqslant 1/q^d$. ■

Lemma 3.5 *For $d \leqslant n/2$ we have*

$$\sum_{\substack{\deg a<\deg g\leqslant d\\ (a,g)=1}}\Big|S_{\mathcal{R}}\Big(\frac{a}{g}\Big)\Big| \leqslant (q-s)^{n-2d}(q(1+\sqrt{s})-2s)^{2d}.$$

Proof For any integer Y and $x \in \mathbb{T}$, define

$$S^Y_{\mathcal{R}}(x) = \sum_{m\in\mathcal{M}_{\mathcal{R}}(Y)}\mathbf{e}_q(mx)$$

so that $S_{\mathcal{R}}(x) = S^n_{\mathcal{R}}(x)$. Then

$$\begin{aligned}\big|S^n_{\mathcal{R}}(x)\big| &= \Big|\prod_{i=0}^{n-1}\sum_{n_i\in\mathcal{R}^c}\psi(n_i x_{-i-1})\Big| = \Big|\prod_{i=0}^{Y-1}\sum_{n_i\in\mathcal{R}^c}\psi(n_i x_{-i-1})\prod_{i=Y}^{n-1}\sum_{n_i\in\mathcal{R}^c}\psi(n_i x_{-i-1})\Big|\\ &= \big|S^Y_{\mathcal{R}}(x)S^{n-Y}_{\mathcal{R}}(xt^Y)\big|.\end{aligned}$$

https://doi.org/10.4153/CMB-2018-027-x Published online by Cambridge University Press

Applying this with $Y = 2d$ gives

$$\begin{aligned}\sum_{\substack{\deg a<\deg g\leqslant d\\(a,g)=1}}\left|S_{\mathcal{R}}\left(\frac{a}{g}\right)\right| &= \sum_{\substack{\deg a<\deg g\leqslant d\\(a,g)=1}}\left|S^{2d}_{\mathcal{R}}\left(\frac{a}{g}\right)S^{n-2d}_{\mathcal{R}}\left(\frac{t^{2d}a}{g}\right)\right|\\ &\leqslant \max_{\substack{\deg a<\deg g\leqslant d\\(a,g)=1}}\left|S^{n-2d}_{\mathcal{R}}\left(\frac{t^{2d}a}{g}\right)\right|\sum_{\substack{\deg a<\deg g\leqslant d\\(a,g)=1}}\left|S^{2d}_{\mathcal{R}}\left(\frac{a}{g}\right)\right|\\ &\leqslant (q-s)^{n-2d}\sum_{\substack{\deg a<\deg g\leqslant d\\(a,g)=1}}\left|S^{2d}_{\mathcal{R}}\left(\frac{a}{g}\right)\right|,\end{aligned}$$

where we have used the trivial bound $|S^{n-2d}_{\mathcal{R}}(x)| \leqslant (q-s)^{n-2d}$. Notice that $S^{2d}_{\mathcal{R}}(a/g+\gamma)$ is constant in the range $|\gamma| < 1/q^{2d}$ and recall that the Farey arcs $\mathcal{F}(a/g, q^{2d})$ are disjoint. Therefore,

$$\frac{1}{q^{2d}}\sum_{\substack{\deg a<\deg g\leqslant d\\(a,g)=1}}\left|S^{2d}_{\mathcal{R}}\left(\frac{a}{g}\right)\right| = \sum_{a,q}\int_{\mathcal{F}(a/g,q^{2d})}\left|S^{2d}_{\mathcal{R}}\left(\frac{a}{g}+\gamma\right)\right|d\gamma \leqslant (\sqrt{s}+1-2s/q)^{2d}$$

by Corollary 3.3, where the sum is over all distinct fractions a/q with $\deg g \leqslant d$. ■

Lemma 3.6 *Let $g \in \mathbb{F}_q[t]$. Then*

$$\frac{q^{\deg g}}{\phi(g)} = \prod_{\omega|g}\left(1-\frac{1}{q^{\deg\omega}}\right)^{-1} \leqslant \left(1+\log_q(\deg g)\right)e^2.$$

Proof Arrange the monic, irreducibles $\omega_1,\dots,\omega_r$ dividing g and the monic irreducibles $P_1,\dots$ in $\mathbb{F}_q[t]$ in order of degree (ordering those of the same degree arbitrarily). Then we must have that $\deg P_i \leqslant \deg\omega_i$. Now, for some N, we have that $\sum_{P:\deg P\leqslant N-1}\deg P < \deg g \leqslant \sum_{P:\deg P\leqslant N}\deg P$. This implies that g has at most $\pi(N)$ irreducible factors, and so, since $\deg P_i \leqslant \deg\omega_i$, we have

$$\prod_{\omega|g}(1-q^{-\deg\omega})^{-1} \leqslant \prod_{P:\deg P\leqslant N}(1-q^{-\deg P})^{-1}.$$

Taking the logarithm of the right-hand side, and using the fact that $-\log(1-\frac{1}{x}) \leqslant \frac{1}{x-1}$ for $x > 1$, and that $\sum_{d|r} d\pi(d) = q^r$ so $\pi(r)r \leqslant q^r - 1$ for $r > 1$, we get

$$\sum_{P:\deg P\leqslant N}-\log(1-q^{-\deg P}) \leqslant \sum_{r\leqslant N}\frac{\pi(r)}{q^r-1} \leqslant \frac{q}{q-1}+\sum_{2\leqslant r\leqslant N}\frac{1}{r} \leqslant 2+\log N.$$

Now N is bounded in terms of $\deg g$ as follows:

$$\deg g > \sum_{P:\deg P\leqslant N-1}\deg P = \sum_{r\leqslant N-1}\pi(r)r \geqslant \sum_{r|N-1}\pi(r)r = q^{N-1}.$$

Hence $N \leqslant 1+\log_q\deg g$. Combining these inequalities gives the result. ■

4 Proof of Theorem 1.1

Recall that our aim is to evaluate $N(\mathcal{R},n)=\int_{\mathbb{T}}S(x)\overline{S_{\mathcal{R}}(x)}dx$. Now each $x\in\mathbb{T}$ can be written as $a/g+\gamma$ for unique a,g,γ as in Lemma 3.1, which allows us to write

$$N(\mathcal{R},n)=\int_{\mathbb{T}}\overline{S_{\mathcal{R}}(x)}\Big(\frac{\mu(g)}{\phi(g)}\pi(n)\mathbf{e}_q(\gamma t^n)\mathbf{1}_{|\gamma|<1/q^n}+E\Big)dx,$$

where $|E|\leqslant q^{n-\frac{1}{2}[\frac{n}{2}]}$ uniformly. The error term is bounded by using Corollary 3.3 as

$$\Big|\int_{\mathbb{T}}\overline{S_{\mathcal{R}}(x)}Edx\Big|\leqslant q^{n-\frac{1}{2}[\frac{n}{2}]}(\sqrt{s}+1-2s/q)^n. \tag{4.1}$$

We can write what's left as

$$\int_{\mathbb{T}}\overline{S_{\mathcal{R}}(x)}\frac{\mu(g)}{\phi(g)}\pi(n)\mathbf{e}_q(\gamma t^n)\mathbf{1}_{|\gamma|<1/q^n}dx=\sum_{a,g}\int_{\mathcal{F}(a/g,q^n)}\overline{S_{\mathcal{R}}\Big(\frac{a}{g}+\gamma\Big)}\frac{\mu(g)}{\phi(g)}\pi(n)\mathbf{e}_q(\gamma t^n)d\gamma,$$

where the sum is over all distinct fractions a/g such that $\deg g\leqslant n/2$. These are the so-called major arcs.

Since $|\gamma|<1/q^n$, from the definition we get

$$S_{\mathcal{R}}\Big(\frac{a}{g}+\gamma\Big)=\sum_{m\in\mathcal{M}_{\mathcal{R}}(n)}\mathbf{e}_q(am/g)\mathbf{e}_q(m\gamma)=\mathbf{e}_q(\gamma t^n)S_{\mathcal{R}}\Big(\frac{a}{g}\Big),$$

and therefore, since the integrand is constant on each of these major arcs, which have measure $1/q^n$, the contribution becomes

$$\frac{\pi(n)}{q^n}\sum_{a,g}\overline{S_{\mathcal{R}}\Big(\frac{a}{g}\Big)}\frac{\mu(g)}{\phi(g)}. \tag{4.2}$$

Let us first analyse the terms with $g=1$ and $g=t$, that is, look at

$$M=\frac{\pi(n)}{q^n}\Big(S_{\mathcal{R}}(0)+\sum_{b\in\mathbb{F}_q\backslash 0}\overline{S_{\mathcal{R}}\Big(\frac{b}{t}\Big)}\frac{\mu(t)}{\phi(t)}\Big).$$

The $g=1$ term gives $S_{\mathcal{R}}(0)=(q-s)^n$. Using our expression for $S_{\mathcal{R}}(\frac{b}{t})$ from the start of the proof of Lemma 3.2, the terms $g=t$ are

$$\sum_{b\in\mathbb{F}_q\backslash 0}S_{\mathcal{R}}(\tfrac{b}{t})=(q-s)^{n-1}\sum_{b\in\mathbb{F}_q\backslash 0}\sum_{n\in\mathcal{R}^c}\mathbf{e}_q(\tfrac{nb}{t})=-(q-s)^{n-1}\sum_{b\in\mathbb{F}_q\backslash 0}\sum_{r\in\mathcal{R}}\psi(br).$$

Using

$$\sum_{b\in\mathbb{F}_q\backslash 0}\psi(br)=\begin{cases}q-1 & \text{if } r=0,\\ -1 & \text{if } r\neq 0,\end{cases}$$

this becomes

$$\begin{cases}-(q-s)^n & \text{if } 0\in\mathcal{R},\\ (q-s)^{n-1}s & \text{if } 0\notin\mathcal{R}.\end{cases}$$

https://doi.org/10.4153/CMB-2018-027-x Published online by Cambridge University Press

Hence, since $\mu(t) = -1$ and $\phi(t) = q-1$ we have

$$M = \frac{\pi(n)}{q^n}\Big((q-s)^n - \frac{1}{q-1}\sum_{b\in\mathbb{F}_q\setminus 0} S_{\mathcal{R}}(b/t)\Big) = \frac{q\Lambda}{q-1}\pi(n)(1-s/q)^n,$$

where

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

Using $\pi(n) \leqslant q^n/n$, the remaining terms in (4.2) are bounded by

$$\frac{1}{n}\sum_{\substack{1\leqslant \deg g\leqslant n/2 \\ g\neq t}} \frac{|\mu(g)|}{\phi(g)} \sum_{\substack{\deg a<\deg g \\ (a,g)=1}} \Big|S_{\mathcal{R}}\Big(\frac{a}{g}\Big)\Big|.$$

Let U be some parameter $1 \leqslant U \leqslant n/2$ to be specified shortly. Grouping the g according to their degree and using Lemma 3.4 for the terms with $d = \deg g \leqslant U$ and Lemmas 3.5 and 3.6 for the terms with $\deg g > U$ we get

$$\begin{aligned}
&\sum_{\substack{1\leqslant \deg g\leqslant n/2 \\ g\neq t}} \frac{|\mu(g)|}{\phi(g)} \sum_{\substack{\deg a<\deg g \\ (a,g)=1}} \Big|S_{\mathcal{R}}\Big(\frac{a}{g}\Big)\Big| \\
&\quad\leqslant \sum_{1\leqslant d\leqslant U} q^d (q-s)^{n-[\frac{n}{d}]} s^{[\frac{n}{d}]} \\
&\qquad + e^2 \sum_{U<d\leqslant n/2} q^{-d}(q-s)^{n-2d}(q(1+\sqrt{s})-2s)^{2d}(1+\log_q(d)) \\
&\quad= (q-s)^n\Bigg(\sum_{1\leqslant d\leqslant U} q^d\Big(\frac{s}{q-s}\Big)^{[\frac{n}{d}]} \\
&\qquad\qquad + e^2\sum_{U<d\leqslant n/2} q^d\Big(\frac{1+\sqrt{s}-2s/q}{q-s}\Big)^{2d}(1+\log_q(d))\Bigg) \\
&\quad\ll (q-s)^n\Bigg(n\Bigg(q^U\Big(\frac{s}{q-s}\Big)^{n/U} + q^{U/2}\Big(\frac{\sqrt{s}+1-2s/q}{q-s}\Big)^U\Bigg)\Bigg).
\end{aligned}$$

We have trivially bounded the first sum. The bound for the second sum follows after using $1+\log_q(d) \leqslant n$ and bounding the resulting geometric sum using $s \leqslant \sqrt{q}/2$ so that

$$\frac{\sqrt{q}(\sqrt{s}+1-2s/q)}{q-s} \leqslant \frac{q/2+\sqrt{q}}{q-\sqrt{q}/2} < 1$$

for $q \geqslant 11$. Taking $U = (2n/5)^{1/2}$ and using $s \leqslant \sqrt{q}/2$, the expression above is bounded by

$$\begin{aligned}
&(q-s)^n\Bigg(n\Bigg(q^{\sqrt{\frac{2}{5}n}}\Big(\frac{q^{1/2}}{2q-q^{1/2}}\Big)^{\sqrt{\frac{5}{2}n}} + q^{\sqrt{\frac{1}{10}n}}\Big(\frac{q^{1/4}/\sqrt{2}+1}{q-q^{1/2}/2}\Big)^{\sqrt{\frac{2}{5}n}}\Bigg)\Bigg) \\
&\ll n(q-s)^n q^{-n^{1/2}/(2\sqrt{10})},
\end{aligned}$$

since

$$\sqrt{\tfrac{2}{5}} - \tfrac{1}{2}\sqrt{\tfrac{5}{2}} = -\tfrac{1}{2\sqrt{10}} \quad\text{and}\quad \sqrt{\tfrac{1}{10}} - \tfrac{3}{4}\sqrt{\tfrac{2}{5}} = -\tfrac{1}{2\sqrt{10}}.$$

https://doi.org/10.4153/CMB-2018-027-x Published online by Cambridge University Press

Combining this with our expression for the main term M and error estimate (4.1) we get

$$N(\mathcal{R},n)=\frac{q}{q-1}\frac{(q-s)^n}{n}\big(\Lambda+O(n\mathcal{E})\big) \tag{4.3}$$

where

$$\mathcal{E}\ll q^{-n^{1/2}/(2\sqrt{10})}+\Big(\frac{q^{3/4}(s^{1/2}+1)}{q-s}\Big)^n. \tag{4.4}$$

Since $s\leqslant\sqrt{q}/2$, we then have

$$\mathcal{E}\ll q^{-n^{1/2}/(2\sqrt{10})}+\Big(\frac{q/\sqrt{2}+q^{3/4}}{q-\sqrt{q}/2}\Big)^n.$$

A calculation reveals that for $n\geqslant 100(\log q)^2$, the first expression is larger than the second when $q\geqslant 500$ and that both are $\ll q^{-n^{1/2}/7}/n$, which completes the proof of Theorem 1.1. ■

Remark The conditions on the sizes of s, q and n were made in order to simplify the statement of Theorem 1.1, but (4.4) is also interesting for other choices. For example, when n is fixed, we have that $\mathcal{E}\to 0$ as $q\to\infty$ provided $s=o(q^{1/2})$.

Recall that in the special case $s=1$, we have equality in Corollary 3.3. Feeding this through the rest of the proof gives

$$\mathcal{E}\ll q^{-n^{1/2}/(2\sqrt{10})}+\Big(\frac{q^{3/4}(2-2/q)}{q-1}\Big)^n.$$

For $q\geqslant 17$, the expression in the brackets is less than 1, which proves that $n\mathcal{E}\to 0$ as $n\to\infty$ in this case.

5 Proof of Theorem 1.4

Our proof of Theorem 1.4 is the same as Theorem 1.1 except that we use modified versions of Corollary 3.3 and Lemma 3.4, which we will now prove. In this section, we assume that p is a prime, $\mathcal{R}\subset\mathbb{F}_p$ is subset of consecutive coefficients and use the same notation already introduced.

Corollary 5.1

$$\int_{\mathbb{T}}|S_{\mathcal{R}}(x)|dx\leqslant(\log p+1-s/p)^n.$$

Proof Write $\mathcal{R}=\{d,d+1,\dots,d+s-1\}$. Then if $r=0$, $|\widehat{1_{\mathcal{R}^c}}(r)|=p-s$, and if $r\neq 0$,

$$|\widehat{1_{\mathcal{R}^c}}(r)|=\Big|\sum_{k=d}^{d+s-1}e^{2\pi ikr/p}\Big|=\Big|\frac{1-e^{2\pi isr/p}}{1-e^{2\pi ir/p}}\Big|\leqslant\frac{1}{|\sin\pi r/p|}.$$

Therefore,

$$\sum_{r\in\mathbb{F}_p}|\widehat{1_{\mathcal{R}^c}}(r)|\leqslant p-s+\sum_{r=1}^{p-1}\frac{1}{|\sin\pi r/p|}<p-s+2\sum_{r=1}^{\frac{p-1}{2}}\frac{p}{2r}<p-s+p\log p.$$

Now use Lemma 3.2. ■

Consequently, the bound in Lemma 3.5 is replaced by

$$(p-s)^{n-2d}\big(p(\log p+1)-s\big)^{2d}.$$

Lemma 5.2 *Let $a, g \in \mathbb{F}_p[t]$ be coprime polynomials with $|a| < |g|$ and g not a power of t and let $d = \deg g > 0$. Then*

$$\big|S_{\mathcal{R}}(a/g)\big| \leqslant (p-s)^n e^{-[\frac{n}{d}]\frac{1}{p^3}}.$$

Proof As in the proof of Lemma 3.4, we have

$$|S_{\mathcal{R}}(a/g)| = (p-s)^{n-z} \prod_{\substack{i=0\\ x_{-i-1}\neq 0}}^{n-1} \Big|\sum_{n_i\in\mathcal{R}} e^{2\pi i(n_i x_{-i-1})/p}\Big|.$$

For $x \in \mathbb{F}_p\backslash\{0\}$, we have

$$\big|e^{2\pi i\frac{x}{p}n} + e^{2\pi i\frac{x}{p}(n+1)}\big|^2 = 2+2\cos\Big(\frac{2\pi x}{p}\Big) < 4e^{-2/p^2},$$

and therefore

$$\Big|\sum_{n_i\in\mathcal{R}} e^{2\pi i(n_i x_{-i-1})/p}\Big| \leqslant p-s-2+2e^{-1/p^2} \leqslant (p-s)e^{-1/p^3}.$$

Recalling from the proof of Lemma 3.4 that $z \geqslant [n/d]$ completes the proof. ■

Provided p is large enough to ensure that $\frac{\sqrt{p}(\log p+1-s/p)}{p-s} < 1$ (so the resulting geometric sum we saw earlier converges), we can just insert these new bounds into the proof of Theorem 1.1 to get (4.3) with

$$\mathcal{E} \ll p^U e^{-[\frac{n}{U}]\frac{1}{p^3}} + \Big(\frac{\sqrt{p}(\log p+1-s/p)}{p-s}\Big)^U + \Big(\frac{p^{3/4}(\log p+1-s/p)}{p-s}\Big)^n$$

for some parameter U. Taking $U = cn^{1/2}$, and since we are assuming that $p-s > p^{3/4+\delta}$, this proves Theorem 1.4 for some $c > 0$ sufficiently small in terms of p and δ.

Acknowledgements The author would like to thank his supervisor, Andrew Granville, for his encouragement and suggestions and Simon Myerson for his helpful comments.

References

[1] C. Dartyge, C. Mauduit, and A. Sárközy, *Polynomial values and generators with missing digits in finite fields*. Funct. Approx. Comment. Math. **52**(2015), 65–74. http://dx.doi.org/10.7169/facm/2015.52.1.5

[2] R. Dietmann, C. Elsholtz, and I. Shparlinski, *Prescribing the binary digits of squarefree numbers and quadratic residues*. Trans. Amer. Math. Soc. **369**(2017), 8369–8388. http://dx.doi.org/10.1090/tran/6903

[3] J. Ha, *Irreducible polynomials with several prescribed coefficients*. Finite Field Appl. **40**(2016), 10–25. http://dx.doi.org/10.1016/j.ffa.2016.02.006

[4] D. R. Hayes, *The expression of a polynomial as a sum of three irreducibles*. Acta Arith. **11**(1966), 461–488. http://dx.doi.org/10.4064/aa-11-4-461-488

[5] J. Maynard, *Primes with restricted digits*. 2016. arxiv:1604.01041

[6] A. Oppenheim and M. Shusterman, *Squarefree polynomials with prescribed coefficients*. J. Number Theory **187**(2018), 189–197. http://dx.doi.org/10.1016/j.jnt.2017.10.025

[7] P. Pollack, *Irreducible polynomials with several prescribed coefficients*. Finite Fields Appl. **22**(2013), 70-78. http://dx.doi.org/10.1016/j.ffa.2013.03.001

[8] A. Tuxanidy and Q. Wang, *Irreducible polynomials with prescribed sums of coefficients*. 2016. arxiv:1605.00351

Department of Mathematics, University College London, London, England
e-mail: ucahspo@ucl.ac.uk

https://doi.org/10.4153/CMB-2018-027-x Published online by Cambridge University Press