THE JOINT DISTRIBUTION OF Q-ADDITIVE FUNCTIONS ON POLYNOMIALS OVER FINITE FIELDS

MICHAEL DRMOTA* AND GEORG GUTENBRUNNER*

ABSTRACT. Let K be a finite field and $Q \in K[T]$ a polynomial of positive degree. A function f on $K[T]$ is called (completely) Q-additive if $f(A + BQ) = f(A) + f(B)$, where $A, B \in K[T]$ and $\deg(A) < \deg(Q)$. We prove that the values $(f_1(A), ..., f_d(A))$ are asymptotically equidistributed on the (finite) image set $\{(f_1(A), ..., f_d(A)) : A \in K[T]\}$ if Q_j are pairwise coprime and $f_j : K[T] \to K[T]$ are Q_j-additive. Furthermore, it is shown that $(g_1(A), g_2(A))$ are asymptotically independent and Gaussian if $g_1, g_2 : K[T] \to \mathbb{R}$ are Q_1- resp. Q_2-additive.

1. INTRODUCTION

Let $g > 1$ be a given integer. A function $f : \mathbb{N} \to \mathbb{R}$ is called (completely) g-additive if

$$f(a + bg) = f(a) + f(b)$$

for $a, b \in \mathbb{N}$ and $0 \le a < g$. In particular, if $n \in \mathbb{N}$ is given in its g-ary expansion

$$n = \sum_{j \ge 0} \varepsilon_{g,j}(n) g^j$$

then

$$f(n) = \sum_{j \ge 0} f(\varepsilon_{g,j}(n)).$$

g-additive functions have been extensively discussed in the literature, in particular their asymptotic distribution, see [1, 3, 4, 5, 6, 7, 8, 9, 11, 12, 14, 15]. We cite three of these results (in a slightly modified form). We want to emphasise that Theorems A and C also say that different g-ary expansions are (asymtotically) independent if the bases are coprime.

Theorem A. (Kim [13]**)** *Suppose that $g_1, \dots, g_d \ge 2$ are pairwise coprime integers, $m_1, \dots, m_d$ positive integers, and let f_j, $1 \le j \le d$, be completely g_j-additive functions. Set*

$$H := \{(f_1(n) \bmod m_1, \dots, f_d(n) \bmod m_d) : n \ge 0\}.$$

Then H is a subgroup of $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}$ and for every $(a_1, \dots, a_d) \in H$ we have

$$\frac{1}{N} \#\{n < N : f_1(n) \bmod m_1 = a_1, \dots, f_d(n) \bmod m_d = a_d\} = \frac{1}{|H|} + O\left(N^{-\delta}\right),$$

where $\delta = 1/(120 d^2 \overline{g}^3 \overline{m}^2)$ with

$$\overline{g} = \max_{1 \le j \le d} g_j \quad \text{and} \quad \overline{m} = \max_{1 \le j \le d} m_j$$

and the O-constant depends only on d and $g_1, \dots, g_d$.

Date: May 8, 2004.

This research was supported by the Austrian Science Foundation FWF, grant S8302-MAT.

*Institute of Discrete Mathematics and Geometry, Technische Universität Wien, Wiedner Hauptstraße 8-10/104, A-1040 Wien, Austria.

Remark. In [13] the set H is explicitly determined. Set $F_j = f_j(1)$ and $d_j = \gcd\{m_j, (q_j-1)F_j, f_j(r) - rF_j \ (2 \le j \le q_j - 1)\}$. Then $(a_1, \dots, a_d) \in H$ if and only if the system of congruences $F_j n \equiv a_j \bmod d_j$, $1 \le j \le d$, has a solution.

Theorem B. (Bassily-Katai [1]**)** *Let f be a completely g-additive function and let $P(x)$ be a polynomial of degree r with non-negative integer coefficients. Then, as $N \to \infty$,*

$$\frac{1}{N}\#\left\{n < N : \frac{f(P(n)) - r\mu_f \log_g N}{\sqrt{r\sigma_f^2 \log_g N}} < x\right\} \to \Phi(x)$$

and

$$\frac{1}{\pi(N)}\#\left\{p < N : p \text{ prime }, \frac{f(P(p)) - r\mu_f \log_g N}{\sqrt{r\sigma_f^2 \log_g N}} < x\right\} \to \Phi(x),$$

where

$$\mu_f = \frac{1}{g}\sum_{r=0}^{g-1} f(r) \quad \text{and} \quad \sigma_f^2 = \frac{1}{g}\sum_{r=0}^{g-1} f(r)^2 - \mu^2,$$

and

$$\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}\,dt.$$

Remark. The result of [1] is more general. It also provides asymptotic normality if f is not strictly g-additive but the variance grows sufficiently fast.

Theorem C. (Drmota [6]**)** *Suppose that $g_1 \ge 2$ and $g_2 \ge 2$ are coprime integers and that f_1 and f_2 are completely g_1- resp. g_2-additive functions.*

Then, as $N \to \infty$,

$$\frac{1}{N}\#\left\{n < N : \frac{f_1(n) - \mu_{f_1}\log_{g_1} N}{\sqrt{\sigma_{f_1}^2 \log_{g_1} N}} \le x_1, \frac{f_2(n) - \mu_{f_2}\log_{g_2} N}{\sqrt{\sigma_{f_2}^2 \log_{g_2} N}} \le x_2\right\} \to \Phi(x_1)\Phi(x_2).$$

Remark. Here it is also possible to provide general versions (see Steiner [17]) but – up to now – it was not possible to prove a similar property for three or more bases g_j.

The purpose of this paper is to generalize these kinds of result to polynomials over finite fields.

Let $\mathbb{F}_q$ be a finite field of characteristic p (that is, $q = |\mathbb{F}_q|$ is a power of p) and let $\mathbb{F}_q[T]$ denotes the ring of polynomials over $\mathbb{F}_q$. The set of polynomials in $\mathbb{F}_q$ of degree $< k$ will be denoted by $P_k = \{A \in \mathbb{F}_q[T] : \deg A < k\}$. Fix some polynomial $Q \in \mathbb{F}_q[T]$ of positive degree. A function $f : \mathbb{F}_q[T] \to G$ (where G is any abelian group) is called (completely) Q-additive if $f(A + BQ) = f(A) + f(B)$, where $A, B \in \mathbb{F}_q[T]$ and $\deg(A) <\deg(Q)$. More precisely, if a polynomial $A \in \mathbb{F}_q[T]$ is represented in its *Q-ary digital expansion*

$$A = \sum_{j\ge 0} D_{Q,j}(A)\, Q^j,$$

where $D_{Q,j}(A) \in P_k$ are the *digits*, that is, polynomials of degree $\deg(D_{Q,j}(A)) < k = \deg Q$, then

$$f(A) = \sum_{j\ge 0} f(D_{Q,j}(A)).$$

For example, the *sum-of-digits function* $s_Q : \mathbb{F}_q[T] \to \mathbb{F}_q[T]$ is defined by

$$s_Q(A) = \sum_{j\ge 0} D_{Q,j}(A).$$

Note that the image set of a Q-additive function is always finite and that (in contrast to the integer case) the sum-of-digits function satisfies $s_Q(A+B) = s_Q(A)+s_Q(B)$.

2. Results

The first theorem is a direct generalization of Theorem A.

Theorem 1. *Let $Q_1, Q_2, \dots, Q_d$ and $M_1, M_2, \dots, M_d$ be non-zero polynomials in $\mathbb{F}_q[T]$ with $\deg Q_i = k_i, \deg M_i = m_i$ and $(Q_i, Q_j) = 1$ for $i \neq j$. Furthermore let $f_i : \mathbb{F}_q[T] \to \mathbb{F}_q[T]$ be Q_i-additive functions $(1 \leq i \leq d)$. Set*

$$H := \{(f_1(A) \bmod M_1, \dots, f_d(A) \bmod M_d) : A \in \mathbb{F}_q[T]\}.$$

Then H is a subgroup of $P_{m_1} \times \cdots \times P_{m_d}$ and for every $(R_1, \dots, R_d) \in H$ we have

$$\lim_{l\to\infty} \frac{1}{q^l} \#\{A \in P_l : f_1(A) \bmod M_1 = R_1, \dots, f_d(A) \bmod M_d = R_d\} = \frac{1}{|H|}.$$

Since the image sets of f_i are finite we can choose the degrees m_i of M_i sufficiently large and obtain

$$\lim_{l\to\infty} \frac{1}{q^l} \#\{A \in P_l : f_1(A) = R_1, \dots, f_d(A) = R_d\} = \frac{1}{|H'|},$$

where

$$H' := \{(f_1(A), \dots, f_d(A)) : A \in \mathbb{F}_q[T]\}.$$

In particular this theorem says that if there is $A \in \mathbb{F}_q[T]$ with $f_i(A) = R_i$ $(1 \leq i \leq d)$ then there are infinitely many $A \in \mathbb{F}_q[T]$ with that property.

The next theorem is a generalization of Theorem B.

Theorem 2. *Let $Q \in \mathbb{F}_q[T], k = \deg Q \geq 1$ be a given polynomial, $g : \mathbb{F}_q[T] \to \mathbb{R}$ be a Q-additive function, and set*

$$\mu_g := \frac{1}{q^k} \sum_{A\in P_k} g(A), \qquad \sigma_g^2 := \frac{1}{q^k} \sum_{A\in P_k} g(A)^2 - \mu^2. \tag{2.1}$$

Let $P(T) \in \mathbb{F}_q[T]$ with $r = \deg P$ and suppose that $\sigma_g^2 > 0$. Then, as $n \to \infty$,

$$\frac{1}{q^n} \#\Big\{A \in P_n : \frac{g(P(A)) - \frac{nr}{k}\mu_g}{\sqrt{\frac{nr}{k}\sigma_g^2}} \leq x\Big\} \to \Phi(x) \tag{2.2}$$

and

$$\frac{1}{|I_n|} \#\Big\{A \in I_n : \frac{g(P(A)) - \frac{nr}{k}\mu_g}{\sqrt{\frac{nr}{k}\sigma_g^2}} \leq x\Big\} \to \Phi(x), \tag{2.3}$$

where I_n denotes the set of monic irreducible polynomials of degree $< n$.

Finally we present a generalization of Theorem C.

Theorem 3. *Suppose that $Q_1 \in \mathbb{F}_q[T]$ and $Q_2 \in \mathbb{F}_q[T]$ are coprime polynomials of degrees $k_1 \geq 1$ resp. $k_2 \geq 1$ such that at least one of the derivatives Q_1', Q_2' is non-zero. Further suppose that $g_1 : \mathbb{F}_q[T] \to \mathbb{R}$ and $g_2 : \mathbb{F}_q[T] \to \mathbb{R}$ are completely Q_1- resp. Q_2-additive functions.*

Then, as $n \to \infty$,

$$\frac{1}{q^n} \#\left\{A \in P_n : \frac{g_1(A) - \frac{n}{k_1}\mu_{g_1}}{\sqrt{\frac{n}{k_1}\sigma_{g_1}^2}} \leq x_1, \frac{g_2(A) - \frac{n}{k_2}\mu_{g_2}}{\sqrt{\frac{n}{k_2}\sigma_{g_2}^2}} \leq x_2\right\} \to \Phi(x_1)\Phi(x_2).$$

Furthermore, Theorems 1 and 3 say that Q-ary digital expansions are (asymptotically) independent if the base polynomials are pairwise coprime.

3. Proof of Theorem 1

Throughout the paper we will use the additive character E defined by

$$E(A) := e^{2\pi i \operatorname{tr}(\operatorname{Res}(A))/p}, \tag{3.1}$$

that is defined for all formal Laurent series

$$A = \sum_{j \ge -k} a_j T^{-j}$$

with $k \in \mathbb{Z}$ and $a_j \in \mathbb{F}_q$. The residue $\operatorname{Res}(A)$ is given by $\operatorname{Res}(A) = a_1$ and tr is the usual trace $\operatorname{tr} : \mathbb{F}_q \to \mathbb{F}_p$.

Let $Q_1, Q_2, \dots, Q_d$ and $M_1, M_2, \dots, M_d$ be non-zero polynomials in $\mathbb{F}_q[T]$ with $\deg Q_i = k_i, \deg M_i = m_i$ and $(Q_i, Q_j) = 1$ for $i \neq j$. Furthermore let f_i be completely Q_i-additive functions. For every tuple $R = (R_1, \dots, R_d) \in P_{m_1} \times \cdots \times P_{m_d}$ set

$$g_{R_i}(A) := E\left(\frac{R_i}{M_i} f_i(A)\right) \tag{3.2}$$

and

$$g_R(A) := \prod_{i=1}^{d} g_{R_i}(A) = E\left(\sum_{i=1}^{d} \frac{R_i}{M_i} f_i(A)\right). \tag{3.3}$$

Proposition 1. *Let $Q_1, Q_2, \dots, Q_d$, $M_1, M_2, \dots, M_d$, and $R = (R_1, \dots, R_d)$ be as above. Then we either have*

$$g_R(A) = 1 \quad \textit{for all } A \in \mathbb{F}_q[T]$$

or

$$\lim_{l \to \infty} \frac{1}{q^l} \sum_{A \in P_l} g_R(A) = 0.$$

We will first prove Proposition 1 (following the lines of Kim [13]). Theorem 1 is then an easy corollary.

3.1. Preliminaries.

Lemma 1. *Let $H \neq 0, H, G \in \mathbb{F}_q[T]$, and let E be the character defined in (3.1), then:*

$$\sum_{\deg R < \deg H} E\left(\frac{G}{H} R\right) = \begin{cases} q^{\deg H} & \text{if } H \text{ divides } G \\ 0 & \text{otherwise.} \end{cases} \tag{3.4}$$

The next lemma is a version of the Weyl–van der Corput inequality.

Lemma 2. *For each $A \in \mathbb{F}_q[T]$ let u_A be a complex number, with $|u_A| = 1$, then*

$$\left|\frac{1}{q^l} \sum_{A \in P_l} u_A\right|^2 \le \frac{1}{q^r} + \frac{1}{q^r} \sum_{D \in P_r \setminus \{0\}} \left|\frac{1}{q^l} \sum_{A \in P_l} \overline{u_A} u_{A+D}\right|. \tag{3.5}$$

Proof. Since $\langle P_l, + \rangle$ is a group we have

$$\begin{aligned} q^r \sum_{A \in P_l} u_A &= \sum_{B \in P_r} \sum_{A \in P_l} u_{A-B} \\ &= \sum_{A \in P_l} 1 \left(\sum_{B \in P_r} u_{A-B}\right). \end{aligned}$$

Hence, using the Cauchy-Schwarz-inequality

$$\begin{aligned} q^{2r}\left|\sum_{A\in P_l} u_A\right|^2 &\leq \sum_{A\in P_l} 1^2 \sum_{A\in P_l}\left|\sum_{B\in P_r} u_{A-B}\right|^2 \\ &= q^l \sum_{A\in P_l}\sum_{B\in P_r}\sum_{C\in P_r} \overline{u}_{A-B}u_{A-C} \\ &= q^l \sum_{D\in P_r}\sum_{A\in P_l}\sum_{B\in P_r} \overline{u}_{A-B}u_{A-B+D} \\ &= q^l \sum_{D\in P_r}\sum_{B\in P_r}\sum_{A\in P_l} \overline{u}_{A-B}u_{A-B+D} \\ &= q^{l+r} \sum_{D\in P_r}\sum_{A\in P_l} \overline{u}_A u_{A+D} \\ &= q^{l+r}\sum_{A\in P_l}|u_A|^2 + q^{l+r}\sum_{D\in P_r\setminus\{0\}}\sum_{A\in P_l}\overline{u}_A u_{A+D}. \end{aligned}$$

The desired result follows from $|u_A| = 1$. □

Lemma 3. *Let f be a completely Q-additive function, and $t \in \mathbb{N}, K, R \in \mathbb{F}_q[T]$ with $\deg R, \deg K < \deg Q^t$. Then for all $N \in \mathbb{F}_q[T]$ satisfying $N \equiv R \bmod Q^t$ we have*

$$f(N+K) - f(N) = f(R+K) - f(R). \tag{3.6}$$

Proof. Due to the above conditions, $N = A\cdot Q^t + R$ for some $A \in \mathbb{F}_q[T]$. Since f is completely Q-additive, and $\deg(R+K) < \deg(Q^t)$, we have

$$\begin{aligned} f(N+K) - f(N) &= f(AQ^t + R + K) - f(AQ^t + R) \\ &= f(A) + f(R+K) - (f(A) + f(R)) \\ &= f(R+K) - f(R). \end{aligned} \tag{3.7}$$

□

3.2. **Correlation Estimates.** In this section we will first prove a correlation estimate (Lemma 4) which will be applied to prove a pre-version (Lemma 5) of Proposition 1.

Let $Q \in \mathbb{F}_q[T]$ of $\deg Q = k$, $M \in \mathbb{F}_q[T]$ of $\deg M = m$, and f be a (completely) Q-additive function. Furthermore for $R \in P_m$ set $g(A) := E\left(\frac{R}{M} f(A)\right)$.
Unless otherwise specified, n and l are arbitrary integers, and $D \in \mathbb{F}_q[T]$ arbitrary as well. We introduce the *correlation functions*

$$\Phi_n(D) = \frac{1}{q^n}\sum_{A\in P_n} \overline{g(A)} g(A+D)$$

and

$$\Phi_{l,n} = \frac{1}{q^l}\sum_{A\in P_l} \left|\Phi_n(A)\right|^2.$$

Lemma 4. *Suppose that $|\Phi_k(R)| < 1$. Then*

$$\frac{1}{q^l}\sum_{H\in P_l}\left|\frac{1}{q^n}\sum_{A\in P_n} E\left(\frac{R}{M}\left(f(A+H) - f(A)\right)\right)\right|^2 \ll \exp\left(-\min\{n,l\}\frac{1-|\Phi_k(R)|^2}{kq^k}\right).$$

Proof. We begin by establishing some recurrence relations for Φ_n and $\Phi_{l,n}$, namely

$$\Phi_{k+n}(QK+R) = \Phi_k(R)\Phi_n(K) \tag{3.8}$$

for polynomials K, R with $R \in P_k$. By using the relation $g(AQ+B) = g(A)g(B)$ and splitting the sum defining $\Phi_{k+n}(QK+R)$ according to the residue class of A modulo Q we obtain

$$\begin{aligned} q^{k+n}\Phi_{k+n}(QK+R) &= \sum_{I\in P_k}\sum_{A\in P_n} \overline{g(AQ+I)}g(AQ+I+QK+R) \\ &= \sum_{I\in P_k}\sum_{A\in P_n} \overline{g(A)g(I)}g(A+K)g(I+R) \\ &= \sum_{I\in P_k} \overline{g(I)}g(I+R) \sum_{A\in P_n} \overline{g(A)}g(A+K) \\ &= q^k\Phi_k(R)q^n\Phi_n(K). \end{aligned}$$

This proves (3.8).

Next observe that

$$\begin{aligned} q^{k+l}\Phi_{k+l,k+n} &= \sum_{I\in P_k}\sum_{A\in P_l} \overline{\Phi_{k+n}(QA+I)}\Phi_{k+n}(QA+I) \\ &= \sum_{I\in P_k}\sum_{A\in P_l} \overline{\Phi_k(I)\Phi_n(A)}\Phi_k(I)\Phi_n(A) \\ &= \sum_{I\in P_k} \overline{\Phi_k(I)}\Phi_k(I) \sum_{A\in P_l} \overline{\Phi_n(A)}\Phi_n(A) \\ &= q^k\Phi_{k,k}q^l\Phi_{l,n}. \end{aligned} \tag{3.9}$$

Thus

$$\Phi_{k+l,k+n} = \Phi_{k,k}\Phi_{l,n} \tag{3.10}$$

and consequently

$$\Phi_{ik+l,ik+n} = (\Phi_{k,k})^i\,\Phi_{l,n}. \tag{3.11}$$

Since $|\Phi_{l,n}| \le 1$ we also get $|\Phi_{ik+l,ik+n}| \le |\Phi_{k,k}|^i$.

Hence, if n and l are given then we can represent them as $n = ik+r, l = ik+s$ with $i = \min([n/k],[l/k])$ and $\min(r,s) < k$. By definition we have

$$\Phi_{k,k} = \frac{1}{q^k}\sum_{A\in P_k} |\Phi_k(A)|^2$$

with $|\Phi_k(A)| \le 1$ for all A. Since $|\Phi_k(R)| < 1$ we also have

$$\Phi_{k,k} \le 1 - \frac{1-|\Phi_k(R)|^2}{q^k} \le \exp\left(-\frac{1-|\Phi_k(R)|^2}{q^k}\right) < 1$$

and consequently

$$|\Phi_{l,n}| \le |\Phi_{k,k}|^i \ll \exp\left(-\min\{l,n\}\frac{1-|\Phi_k(R)|^2}{kq^k}\right).$$

□

Remark. We want to remark that $|\Phi_k(R)| = 1$ is a *rare* event. In particular, we have

$$\begin{aligned} \forall R : |\Phi_k(R)| = 1 \quad &\Leftrightarrow \quad \forall R\ \forall A \in P_k : \overline{g(A)}g(A+R) \text{ is constant} \\ &\Leftrightarrow \quad \forall R, \forall A, B \in P_k : \overline{g(A)}g(A+R) = \overline{g(B)}g(B+R) \\ &\Leftrightarrow \quad \forall A, B \in P_k : g(A+B) = g(A)g(B). \end{aligned}$$

Thus, there exists R with $|\Phi_k(R)| < 1$ if and only if there exist $A, B \in P_k$ with $g(A)g(B) \neq g(A+B)$.

Next we prove a pre-version of Proposition 1.

Lemma 5. *Let $Q_1, Q_2, \dots, Q_d \in \mathbb{F}_q[T]$ be pairwise coprime polynomials, $M_1, M_2, \dots, M_d \in \mathbb{F}_q[T]$, and $R = (R_1, R_2, \dots, R_d) \in P_{m_1} \times \cdots \times P_{m_d}$ such that $|\Phi_{k_j}(R_j)| < 1$ for at least one $j = 1, \dots, d$. Then*

$$\lim_{l\to\infty} \frac{1}{q^l} \sum_{A\in P_l} g_R(A) = 0, \tag{3.12}$$

where $g_R(A) = \prod_{j=1}^d g_{R_j}(A)$ with $g_{R_j}(A) = E\left(\frac{R_j}{M_j} f_j(A)\right)$.

Proof. Set $B_j = Q_j^{t_j}$, where $b_j = t_j \deg Q_j$ satisfies that $r \le b_j \le 2r$ with $r = \frac{l}{3d}$. Given $S = (S_1, S_2, \dots, S_d)$ and $B_1, B_2, \dots, B_d$, we define $N_S := \{A \in P_l : A \equiv S_1 \bmod B_1, \dots, A \equiv S_d \bmod B_d\}$. By the Chinese remainder theorem we have for $l \ge \sum_{j=1}^d b_j$

$$|N_S| = \frac{q^l}{\prod_{j=1}^d q^{b_j}} = q^{l-\sum_{j=1}^d b_j}$$

Furthermore set $\mathcal{S} := P_{b_1} \times \cdots \times P_{b_d}$. By Lemma 3 we obtain for $D \in P_r \setminus \{0\}$:

$$\begin{aligned}
\sum_{A\in P_l} \overline{g_R(A)} g_R(A+D) &= \sum_{S\in\mathcal{S}} \sum_{A\in N_S} \overline{g_R(A)} g_R(A+D) \\
&= \sum_{S\in\mathcal{S}} \sum_{A\in N_S} \prod_{j=1}^d \overline{g_{R_j}(S_j)} g_{R_j}(S_j+D) \\
&= \sum_{S\in\mathcal{S}} \prod_{j=1}^d \overline{g_{R_j}(S_j)} g_{R_j}(S_j+D) \sum_{A\in N_S} 1 \\
&= \prod_{j=1}^d \sum_{S_j\in P_{b_j}} \overline{g_{R_j}(S_j)} g_{R_j}(S_j+D) \frac{q^l}{\prod_{j=1}^d q^{b_j}} \\
&= q^l \prod_{j=1}^d \frac{1}{q^{b_j}} \sum_{S_j\in P_{b_j}} \overline{g_{R_j}(S_j)} g_{R_j}(S_j+D).
\end{aligned}$$

According to Lemma 2 we obtain for $r \le l$

$$\begin{aligned}
\left|\sum_{A\in P_l} g_R(A)\right|^2 &\le q^{2l-r} + q^{l-r} \sum_{D\in P_r\setminus\{0\}} \left|\sum_{A\in P_l} \overline{g_R(A)} g_R(A+D)\right| \\
&= q^{2l-r} \underbrace{\sum_{D\in P_r\setminus\{0\}} \left|\prod_{j=1}^d q^{-b_j} \sum_{S_j\in P_{b_j}} \overline{g_{R_j}(S_j)} g_{R_j}(S_j+D)\right|}_{\Sigma_1} + O(q^{2l-r}).
\end{aligned}$$

Hölder's inequality gives

$$\begin{aligned}
\Sigma_1 &\le q^{r/(d+1)} \prod_{j=1}^d \left(\sum_{D\in P_r\setminus\{0\}} \left| q^{-b_j} \sum_{S_j\in P_{b_j}} \overline{g_{R_j}(S_j)} g_{R_j}(S_j+D)\right|^{d+1}\right)^{1/(d+1)} \\
&\le q^r \prod_{j=1}^d \left(q^{-r} \sum_{D\in P_r\setminus\{0\}} \left| q^{-b_j} \sum_{S_j\in P_{b_j}} \overline{g_{R_j}(S_j)} g_{R_j}(S_j+D)\right|^2\right)^{1/(d+1)}.
\end{aligned}$$

For some j we have $|\Phi_{k_j}(R_j)| < 1$, so that Lemma 4 is applicable and thus

$$q^{-r} \sum_{D \in P_r \setminus \{0\}} \left| q^{-b_j} \sum_{S_j \in P_{b_j}} \overline{g_{R_j}(S_j)} g_{R_j}(S_j + D) \right|^2 \to 0$$

as $r = l/(3d) \to \infty$. For all other j we trivially estimate by ≤ 1 and obtain

$$\frac{1}{q^l} \left| \sum_{A \in P_l} g_R(A) \right| \to 0 \tag{3.13}$$

as $l \to \infty$. □

3.3. **Proof of Proposition 1.** As above we set $g_R(A) = \prod_{j=1}^d g_{R_j}(A) = E\left(\sum_{j=1}^d \frac{R_j}{M_j} f_j(A)\right)$. We split up the proof into several cases.

Case 1: There exist j and $A, B \in P_{k_j}$ with $g_j(A)g_j(B) \neq g_j(A+B)$.

This case is covered by by Lemma 5 (compare with the remark following Lemma 4).

Case 2: For all j and for all $A, B \in P_{k_j}$ we have $g_j(A)g_j(B) = g_j(A+B)$.

In this case we also have (due to the additivity property) $g_j(A)g_j(B) = g_j(A+B)$ for all $A, B \in \mathbb{F}_q[T]$ and consequently $g(A)g(B) = g(A+B)$ for all $A, B \in \mathbb{F}_q[T]$.

Case 2.1: In addition we have $g(A) = 1$ for all $A \in \mathbb{F}_q[T]$.

This case is the first alternative in Proposition 1.

Case 2.2: In addition there exists $A \in \mathbb{F}_q[T]$ with $g(A) \neq 1$.

For simplicity we assume that q is a prime number. Thus, if $A = \sum_{i \ge 0} a_i T^i$ then we have $g(A) = \prod_{i \ge 0} g(T^i)^{a_i}$. Consequently there exists $i \ge 0$ with $g(T^i) \neq 1$. Furthermore

$$\sum_{a=0}^{q-1} g(T^j)^a = \begin{cases} q & \text{if } g(T^j) = 1 \\ 0 & \text{if } g(T^j) \neq 1. \end{cases}$$

Hence, if $l > i$ we surely have

$$\begin{aligned} \sum_{A \in P_l} g(A) &= \sum_{a_0=0}^{q-1} \sum_{a_1=0}^{q-1} \cdots \sum_{a_{l-1}=0}^{q-1} g(T^0)^{a_0} g(T^1)^{a_1} \cdots g(T^{l-1})^{a_{l-1}} \\ &= \left(\sum_{a_0=0}^{q-1} g(T^0)^{a_0} \right) \cdots \left(\sum_{a_{l-1}=0}^{q-1} g(T^{l-1})^{a_{l-1}} \right) \\ &= 0 \end{aligned} \tag{3.14}$$

If q is a prime power the can argue in a similar way. This completes the proof of Proposition 1.

3.4. **Completion of the Proof of Theorem 1.** We define two (additive) groups

$$G := \{R = (R_1, R_2, \dots, R_d) \in P_{m_1} \times \cdots \times P_{m_d} : \forall\, A \in \mathbb{F}_q[T]\ g_R(A) = 1\}$$

and

$$H_0 := \left\{ S \in P_{m_1} \times \cdots \times P_{m_d} : \forall R \in G :\ E\left(\sum_{i=1}^d -\frac{S_i R_i}{M_i} \right) = 1 \right\}.$$

Furthermore, set

$$F(S) := \frac{1}{|G|} \sum_{R \in G} E\left(\sum_{i=1}^d -\frac{S_i R_i}{M_i} \right). \tag{3.15}$$

Now, by applying Proposition 1 we directly get

$$\begin{aligned}
&\frac{1}{q^l}\#\{A \in P_l : f_1(A) \equiv S_1 \bmod M_1, \dots, f_d(A) \equiv S_d \bmod M_d\} \\
&= \frac{1}{q^l} \sum_{A \in P_l} \frac{1}{q^{\sum_{j=1}^d m_j}} \sum_{R \in P_{m_1} \times \cdots \times P_{m_d}} E\left(\sum_{j=1}^d \frac{R_j}{M_j}(f_j(A) - S_j)\right) \\
&= \frac{1}{q^{\sum_{j=1}^d m_j}} \sum_{R \in P_{m_1} \times \cdots \times P_{m_d}} \left[E\left(\sum_{j=1}^d -\frac{S_j R_j}{M_j}\right) \cdot \frac{1}{q^l} \sum_{A \in P_l} g_R(A)\right] \\
&= \frac{1}{q^{\sum_{j=1}^d m_j}} \sum_{R \in G} E\left(\sum_{j=1}^d -\frac{S_j R_j}{M_j}\right) + o(1) \\
&= \frac{|G|}{q^{\sum_{j=1}^d m_j}} F(S) + o(1).
\end{aligned}$$

More precisely the coefficient $F(S)$ characterizes H_0.

Lemma 6. *We have*

1. $F(S) = 1$ *for* $S \in H_0$
2. $F(S) = 0$ *for* $S \notin H_0$.

Furthermore $|G| \cdot |H_0| = |P_{m_1} \times \cdots \times P_{m_d}| = q^{m_1 + \cdots + m_d}$.

Proof. It is clear that $F(S) = 1$ if $S \in H_0$.

Now suppose that $S \notin H_0$. Then there exists $R^0 = (R_1^0, R_2^0, \dots, R_d^0) \in G$ with $E\left(\sum_{i=1}^d -\frac{S_i R_i^0}{M_i}\right) \neq 1$. Since

$$\begin{aligned}
\sum_{R \in G} E\left(\sum_{i=1}^d -\frac{S_i R_i}{M_i}\right) &= \sum_{R \in G} E\left(\sum_{i=1}^d -\frac{S_i (R_i + R_i^0)}{M_i}\right) \\
&= E\left(\sum_{i=1}^d -\frac{S_i R_i^0}{M_i}\right) \sum_{R \in G} E\left(\sum_{i=1}^d -\frac{S_i R_i}{M_i}\right)
\end{aligned}$$

it follows that $F(S) = 0$.

Finally, by summing up over all $S \in P_{m_1} \times \cdots \times P_{m_d}$ it follows that $|G| \cdot |H_0| = |P_{m_1} \times \cdots \times P_{m_d}|$. □

In fact we have now shown that (as $l \to \infty$)

$$\frac{1}{q^l}\#\{A \in P_l : f_1(A) \equiv S_1 \bmod M_1, \dots, f_d(A) \equiv S_d \bmod M_d\} = \frac{1}{|H_0|} + o(1)$$

if $S = (S_1, \dots, S_d) \in H_0$ and (as $l \to \infty$)

$$\frac{1}{q^l}\#\{A \in P_l : f_1(A) \equiv S_1 \bmod M_1, \dots, f_d(A) \equiv S_d \bmod M_d\} = o(1)$$

if $S = (S_1, \dots, S_d) \notin H_0$. The final step of the proof of Theorem 1 is to show that

$$H = \{(f_1(A) \bmod M_1, \dots, f_d(A) \bmod M_d) : A \in \mathbb{F}_q[T]\} = H_0.$$

In fact, if $S \in H_0$ then we trivially have $S \in H$.

Conversely, if $S \in H$ then there exists $A \in \mathbb{F}_q[T]$ with $f_1(A) \equiv S_1 \bmod M_1, \dots, f_d(A) \equiv S_d \bmod M_d$. In particular, it follows that

$$g_R(A) = E\left(\sum_{j=1}^d \frac{R_j}{M_j} f_j(A)\right) = E\left(\sum_{j=1}^d \frac{R_j S_j}{M_j}\right).$$

Moreover, for all $R \in G$ we have

$$E\left(\sum_{j=1}^{d} \frac{R_j S_j}{M_j}\right) = 1.$$

Consequently, $S \in H_0$. This proves $H = H_0$ and also completes the proof of Theorem 1.

4. Proof of Theorem 2

4.1. **Preliminaries.** The first lemma shows how we can extract a digit $D_{Q,j}(A)$ with help of exponential sums.

Lemma 7. *Suppose that $Q \in \mathbb{F}_q[T]$ with $\deg Q = k \geq 1$. Set*

$$c_{H,D} = \frac{1}{q^k} E\left(-\frac{DH}{Q}\right).$$

Then

$$\sum_{H \in P_k} c_{H,D}\, E\left(\frac{AH}{Q^{j+1}}\right) = \begin{cases} 1 & \text{if } D_{Q,j}(A) = D \\ 0 & \text{if } D_{Q,j}(A) \neq D. \end{cases}$$

Proof. Consider the Q-ary expansion

$$A = \sum_{j \geq 0} D_{Q,j}(A)\, Q^j \quad \text{with} \quad D_{Q,j}(A) \in P_k. \tag{4.1}$$

Then it follows that for $H \in P_k$

$$E\left(\frac{AH}{Q^{j+1}}\right) = E\left(\frac{D_{Q,j}(A)H}{Q}\right).$$

Consequently, for every $D \in P_k$ we obtain

$$\begin{aligned} \sum_{H \in P_k} c_{H,D} E\left(\frac{AH}{Q^{j+1}}\right) &= \frac{1}{q^k} \sum_{H \in P_k} E\left(-\frac{DH}{Q}\right) E\left(\frac{AH}{Q^{j+1}}\right) \\ &= \frac{1}{q^k} \sum_{H \in P_k} E\left(\frac{H}{Q}(D_{Q,j}(A) - D)\right) \\ &= \begin{cases} 1 & \text{if } D_{Q,j}(A) = D, \\ 0 & \text{if } D_{Q,j}(A) \neq D. \end{cases} \end{aligned}$$

□

The next two lemmas are slight variations of estimates of [2].

Lemma 8. *Suppose that $Q \in \mathbb{F}_q[T]$ has degree $\deg Q = k \geq 1$ and that $P \in \mathbb{F}_q[T]$ is a polynomial of degree $\deg P = r \geq 1$. Then*

$$\begin{aligned} &\frac{1}{q^n} \left| \sum_{A \in P_n} E\left(\frac{H}{Q^{j+1}} P(A)\right) \right| \\ &\qquad \ll n^{2^{2-r}} \max\left(q^{-(j+1)k2^{-r}}, q^{-n2^{-r}}, q^{(j+1)k2^{-r} - nr2^{-r}}\right) \end{aligned} \tag{4.2}$$

Corollary 1. *Let $n^{1/3} \leq j+1 \leq \frac{rn}{k} - n^{1/3}$. Then there exists a constant $c > 0$ such that uniformly in that range*

$$\frac{1}{q^n} \left| \sum_{A \in P_n} E\left(\frac{H}{Q^{j+1}} P(A)\right) \right| \ll e^{-cn^{1/3}}.$$

A similar estimate holds for monic irreducible polynomials I_n of degree $< n$. Note that $|I_n| = q^n/((q-1)n) + O(q^{n/2}) \sim q^n/(q-1)n)$.

Lemma 9. *Let $\frac{2r}{k}n^{1/3} \le j+1 \le \frac{rn}{k} - \frac{2r}{k}n^{1/3}$, and H be a polynomial coprime to Q. Then*

$$\frac{1}{|I_n|}\left|\sum_{A\in I_n} E\left(\frac{H}{Q^{j+1}}P(A)\right)\right| \ll (\log n)\cdot n^{4/3+2^{-2-2r}} q^{-r2^{-2r}n^{1/3}}. \tag{4.3}$$

With help of theses estimates we can prove the following frequency estimates.

Lemma 10. *Let m be a fixed integer and $\frac{2r}{k}n^{1/3} \le j_1 < j_2 < \cdots < j_m \le \frac{nr}{k} - \frac{2r}{k}n^{1/3}$. Then*

$$\begin{aligned}\frac{1}{q^n}\cdot \#\{A\in P_n : D_{Q,j_1}(P(A)) = D_1,\dots, D_{Q,j_m}(P(A)) = D_m\}\\ = \frac{1}{q^{km}} + O\left(e^{-cn^{1/3}}\right)\end{aligned}$$

and

$$\begin{aligned}\frac{1}{|I_n|}\cdot \#\{A\in I_n : D_{Q,j_1}(P(A)) = D_1,\dots, D_{Q,j_m}(P(A)) = D_m\}\\ = \frac{1}{q^{km}} + O\left(e^{-cn^{1/3}}\right)\end{aligned}$$

uniformly for all $D_1,\dots,D_m \in P_k$ and for all $j_1,\dots,j_m$ in the mentioned range.

Proof. By Lemma 7 we have

$$\begin{aligned}&\frac{1}{q^n}\#\{A\in P_n : D_{Q,j_1}(P(A)) = D_1,\dots, D_{Q,j_m}(P(A)) = D_m\} =\\
&= \frac{1}{q^n}\sum_{A\in P_n}\left(\sum_{H_1\in P_k} c_{H_1,D_1} E\left(\frac{H_1}{Q^{j_1+1}}P(A)\right)\right)\cdots\left(\sum_{H_m\in P_k} c_{H_m,D_m} E\left(\frac{H_m}{Q^{j_m+1}}P(A)\right)\right)\\
&= \sum_{H_1,\dots,H_m\in P_k} c_{H_1,D_1}\cdots c_{H_m,D_m}\frac{1}{q^n}\sum_{A\in P_n} E\left(P(A)\left(\frac{H_1}{Q^{j_1+1}}+\cdots+\frac{H_m}{Q^{j_m+1}}\right)\right)\\
&= c_{0,D_1}\cdots c_{0,D_m}\\
&\quad + {\sum_{H_1,\dots,H_m\in P_k}}^{*} c_{H_1,D_1}\cdots c_{H_m,D_m}\frac{1}{q^n}\sum_{A\in P_n} E\left(P(A)\left(\frac{H_1}{Q^{j_1+1}}+\cdots+\frac{H_m}{Q^{j_m+1}}\right)\right)\\
&= \frac{1}{q^{km}} + S,\end{aligned}$$

where $\sum^*$ denotes that we sum just over all $(H_1,\dots,H_m)\neq(0,\dots,0)$. In order to complete the proof we just have to show that $S = O(e^{-cn^{1/3}})$.

Let l be the largest i with $H_i \neq 0$ then

$$\frac{1}{q^n}\sum_{A\in P_n} E\left(P(A)\left(\frac{H_1}{Q^{j_1+1}}+\cdots+\frac{H_m}{Q^{j_m+1}}\right)\right) = \frac{1}{q^n}\sum_{A\in P_n} E\left(P(A)\frac{H}{Q^{j_l+1}}\right)$$

where $H = H_l + H_{l-1}Q^{j_l-j_{l-1}} + \cdots + H_1 Q^{j_l-j_1}$. By our assumption we have $\frac{2r}{k}n^{1/3} \le j_l \le \frac{nr}{k} - \frac{2r}{k}n^{1/3}$. Hence by Lemma 8 the first result follows.

The proof for $A\in I_n$ is completely the same. □

4.2. **Weak Convergence.** The idea of the proof of Theorem 2 is to compare the distribution of $g(P(A))$ with the distribution of sums of independent identically distributed random variables. Let $Y_0, Y_1, \dots$ be independent identically distributed random variables on P_k with $\mathbb{P}[Y_j = D] = q^{-k}$ for all $D\in P_k$. Then Lemma 10 can

be rewritten as

$$\frac{1}{q^n}\#\left\{A\in P_n : D_{Q,j_1}(P(A))=D_1,\dots,D_{Q,j_m}(P(A))=D_m\right\}$$
$$=\mathbb{P}[Y_{j_1}=D_1,\dots,Y_{j_m}=D_m]+O\left(e^{-cn^{1/3}}\right).$$

Note further that this relation is also true if $j_1,\dots,j_m$ vary in the range $\frac{2r}{k}n^{1/3}\le j_1,j_2,\cdots,j_m\le\frac{nr}{k}-\frac{2r}{k}n^{1/3}$ and are not ordered. It is even true if some of them are equal.

In fact, we will use a moment method, that is, we will show that the moments of $g(P(A))$ can be compared with moments of the normal distribution. Finally this will show that the corresponding (normalized) distribution function of $g(P(A))$ converges to the normal distribution function $\Phi(x)$.

It turns out that we will have to cut off the first and last few digits, that is, we will work with

$$\widetilde{g}(P(A)):=\sum_{\frac{2r}{k}n^{1/3}\le j\le\frac{nr}{k}-\frac{2r}{k}n^{1/3}} g(D_{Q,j}(P(A))$$

instead of $g(P(A))$.

Lemma 11. *Set*

$$\mu=\frac{1}{q^k}\sum_{H\in P_k} g(H)=\mathbb{E}\,g(Y_j).$$

Then the m-th (central) moment of $\widetilde{g}(P(A))$ is given by

$$\frac{1}{q^n}\sum_{A\in P_n}\left(\widetilde{g}(P(A))-\left(\frac{nr}{k}-2\frac{2r}{k}n^{1/3}\right)\mu\right)^m=$$
$$=\mathbb{E}\left(\sum_{\frac{2r}{k}n^{1/3}\le j\le\frac{nr}{k}-\frac{2r}{k}n^{1/3}}(g(Y_j)-\mu)\right)^m+O\left(n^me^{-cn^{1/3}}\right).$$

Proof. For notational convenience we just consider the second moment:

$$\frac{1}{q^n}\sum_{A\in P_n}\left(\widetilde{g}(P(A))-\left(\frac{nr}{k}-\frac{2r}{k}n^{1/3}\right)\mu\right)^2=$$
$$=\sum_{j_1,j_2}\sum_{D_1,D_2} g(D_1)g(D_2)\frac{1}{q^n}\#\{A\in P_n : D_{Q,j_1}(P(A))=D_1, D_{Q,j_2}(P(A))=D_2\}$$
$$-\sum_{j_1}\sum_{D_1} g(D_1)\frac{1}{q^n}\#\{A\in P_n : D_{Qj_1}(P(A))=D_1\}\cdot\sum_{j_2}\mu$$
$$-\sum_{j_1}\mu\sum_{j_2}\sum_{D_2} g(D_2)\frac{1}{q^n}\#\{A\in P_n : D_{Q,j_2}(P(A))=D_2\}+\sum_{j_1,j_2}\mu^2$$
$$=\sum_{j_1,j_2}\sum_{D_1,D_2} g(D_1)g(D_2)\mathbb{P}[Y_{j_1}=D_1,Y_{j_2}=D_2]+O\left(n^2e^{-cn^{1/3}}\right)$$
$$-\sum_{j_1}\sum_{D_1} g(D_1)\mathbb{P}[Y_{j_1}=D_1]\sum_{j_2}\mu$$
$$-\sum_{j_1}\mu\sum_{j_2}\sum_{D_2} g(D_2)\mathbb{P}[Y_{j_2}=\varepsilon_2]+\sum_{j_1}\sum_{j_2}\mu^2$$
$$=\mathbb{E}\left(\sum_j(g(Y_j)-\mu)\right)^2+O\left(n^2e^{-cn^{1/3}}\right).$$

The very same procedure works in general and completes the proof of the lemma. □

Since the sum of independent identically distributed random variables converges (after normalization) to the normal distribution it follows from Lemma 11

$$\frac{1}{q^n}\#\left\{A\in P_n : \frac{\widetilde{g}(P(A))-(\frac{nr}{k}-\frac{2r}{k}n^{1/3})\mu}{\sqrt{(\frac{nr}{k}-\frac{2r}{k}n^{1/3})\sigma^2}}\le x\right\}=\Phi(x)+o(1)$$

Because of

$$|\widetilde{g}(P(A))-g(P(A))|\ll n^{1/3}$$

and $n^{1/3}/n^{1/2}=n^{-1/6}\to 0$ it also follows that

$$\frac{1}{q^n}\#\left\{A\in P_n : \frac{g(P(A))-\frac{nr}{k}\mu}{\sqrt{\frac{nr}{k}\sigma^2}}\le x\right\}=\Phi(x)+o(1).$$

This completes the proof of Theorem 2.

5. Proof of Theorem 3

5.1. **Preliminaries.** As usual, let $\nu\left(\frac{A}{B}\right)=\deg(B)-\deg(A)$ be the valuation on $\mathbb{F}_q(T)$.

Lemma 12. *For $a,b\in\mathbb{F}_q(T)$ we have*

$$\nu(a+b)\ge\min\{\nu(a),\nu(b)\}. \tag{5.1}$$

Moreover, if $\nu(a)\neq\nu(b)$, then

$$\nu(a+b)=\min\{\nu(a),\nu(b)\}. \tag{5.2}$$

Furthermore, we will use the following easy property (see [10]) that is closely related to Lemma 1.

Lemma 13. *Suppose that $\nu\left(\frac{B}{C}\right)>0$ and that $n\ge\nu\left(\frac{B}{C}\right)$, then*

$$\sum_{A\in P_n}E\left(\frac{B}{C}A\right)=0. \tag{5.3}$$

Another important tool is Mason's theorem (see [16]).

Lemma 14. *Let K be an arbitrary field and $A,B,C\in K[T]$ relatively prime polynomials with $A+B=C$. If the derivatives A',B',C' are not all zero then the degree $\deg C$ is smaller than the number of different zeros of ABC (in a proper algebraic closure of K).*

We will use Mason's theorem in order to prove the following property.

Lemma 15. *Let $Q_1,Q_2\in\mathbb{F}_q[T]$ be coprime polynomials with degrees $\deg(Q_i)=k_i\ge 1$ such that at least one of the derivatives Q_1',Q_2' is non-zero. Then there exists a constant c such that for all polynomials $H_1\in P_{k_1}$ and $H_2\in P_{k_2}$ with $(H_1,H_2)\neq(0,0)$ and for all integers $m_1,m_2\ge 1$ we have*

$$\deg(H_1Q_2^{m_2}+H_2Q_1^{m_1})\ge\max\{\deg(H_1Q_2^{m_2}),\deg(H_2Q_1^{m_1})\}-c.$$

Proof. Set $A=H_1Q_2^{m_2}$, $B=H_2Q_1^{m_1}$, and $C=A+B$. If A and B are coprime by Mason's theorem we have $\deg(A)\le n_0(ABC)-1$ and $\deg(B)\le n_0(ABC)-1$, where $n_0(F)$ is defined to be the number of distinct zeroes of F. Hence

$$\begin{aligned}\max\{\deg(A),\deg(B)\} &\le n_0(ABC)-1\\ &= n_0(H_1H_2Q_1Q_2C)-1\\ &\le \deg(H_1H_2Q_1Q_2)+\deg(C)-1\end{aligned}$$

and consequently

$$\deg(C) \geq \max\{\deg(A), \deg(B)\} - \deg(H_1H_2Q_1Q_2) + 1. \tag{5.4}$$

This shows that (in the present case) $c = 2k_1 + 2k_2$ is surely a proper choice.

If A and B are not coprime then by assumption the common factor D is surely a divisor of H_1H_2. Furthermore, there exists $m' \geq 0$ such that D^2 is a divisor of $H_1H_2(Q_1Q_2)^{m'}$. Consequently we have

$$(A/D)(B/D) = (H_1H_2(Q_1Q_2)^{m'}/D^2)Q_1^{m_1-m'}Q_2^{m_2-m'}$$

and by a reasoning as above we get

$$\deg(C/D) \geq \max\{\deg(A/D), \deg(B/D)\} - \deg((H_1H_2(Q_1Q_2)^{m'}/D^2)Q_1Q_2) + 1.$$

or

$$\deg(C) \geq \max\{\deg(A), \deg(B)\} - \deg((H_1H_2(Q_1Q_2)^{m'}/D^2)Q_1Q_2) + 1.$$

Since there are only finitely possibilities for H_1, H_2, and D the lemma follows. □

5.2. **Convergence of Moments.** The idea of the proof of Theorem 3 is completely the same as that of Theorem 2. We prove weak convergence by considering moments. The first step is to provide a generalization of Lemma 10.

Lemma 16. *Let m_1, m_2 be fixed integers. Then there exists a constant $c' > 0$ such that for all $0 \leq i_1 < i_2 < \cdots < i_{m_1} \leq \frac{n}{k_1} - c'$ and $0 \leq j_1 < j_2 < \cdots < j_{m_2} \leq \frac{n}{k_2} - c'$ we have*

$$\begin{aligned}\frac{1}{q^n}\#\Big\{A \in P_n : D_{Q_1,i_1}(A) = D_1, \dots, D_{Q_1,i_{m_1}}(A) = D_{m_1},\\ D_{Q_2,j_1}(A) = E_1, \dots, D_{Q_2,j_{m_2}}(A) = E_{m_2}\Big\}\\ = \frac{1}{q_1^{k_1m_1}q_2^{k_2m_2}}.\end{aligned}$$

Instead of giving a complete proof of this lemma we will concentrate on the cases $m_1 = m_2 = 1$ and $m_1 = m_2 = 2$. The general case runs along the same lines (but the notation will be terrible).

First let $m_1 = m_2 = 1$. Here we have

$$\begin{aligned}&\frac{1}{q^n}\#\Big\{A \in P_n : D_{Q_1,i}(A) = D, D_{Q_2,j}(A) = E\Big\}\\ =\ &\frac{1}{q^n}\sum_{A\in P_n}\sum_{H_1\in P_{k_1}} c_{H_1,Q_1,D}E\left(\frac{AH_1}{Q_1^{i+1}}\right)\sum_{H_2\in P_{k_2}} c_{H_2,Q_2,E}E\left(\frac{AH_2}{Q_2^{j+1}}\right)\\ &= \frac{1}{q^{k_1+k_2}} + \sum_{(H_1,H_2)\neq(0,0)} c_{H_1,Q_1,D}c_{H_2,Q_2,E}\frac{1}{q^n}\sum_{A\in P_n} E\left(A\left(\frac{H_1}{Q_1^{i+1}} + \frac{H_2}{Q_2^{j+1}}\right)\right).\end{aligned}$$

Now we can apply Lemma 15 and obtain

$$\begin{aligned}\nu\left(\frac{H_1}{Q_1^{i+1}} + \frac{H_2}{Q_2^{j+1}}\right) &= \nu\left(\frac{H_1Q_2^{j+1} + H_2Q_1^{i+1}}{Q_1^{i+1}Q_2^{j+1}}\right)\\ &\leq k_1(i+1) + k_2(j+1)\\ &\quad - \max\{\deg(H_1) + k_2(j+1), \deg(H_1) + k_1(i+1)\} + c\\ &\leq \min\{k_1(i+1), k_2(j+1)\} + c.\end{aligned}$$

Thus, there exists a constant $c' > 0$ such that

$$\min\{k_1(i+1), k_2(j+1)\} + c \leq n$$

for all i, j with $0 \le i \le \frac{n}{k_1} - c'$ and $0 \le j \le \frac{n}{k_2} - c'$. Hence, by Lemma 13

$$\sum_{A \in P_n} E\left(A\left(\frac{H_1}{Q_1^{i+1}} + \frac{H_2}{Q_2^{j+1}}\right)\right) = 0.$$

This completes the proof for the case $m_1 = m_2 = 1$.

Next suppose that $m_1 = m_2 = 2$. Here we have

$$\begin{aligned}
&\frac{1}{q^n}\#\Big\{A \in P_n : D_{Q_1,i_1}(A) = D_1, D_{Q_1,i_2}(A) = D_2, D_{Q_2,j_1}(A) = E_1, D_{Q_2,j_2}(A) = E_2\Big\} \\
&= \frac{1}{q^n} \sum_{A \in P_n} \left(\sum_{H_{11} \in P_{k_1}} c_{Q_1,H_{11},D_1} E\left(\frac{H_{11}}{Q_1^{i_1+1}}A\right)\right)\left(\sum_{H_{12} \in P_{k_1}} c_{Q_1,H_{12},D_2} E\left(\frac{H_{12}}{Q_1^{i_2+1}}A\right)\right) \times \\
&\qquad \times \left(\sum_{H_{21} \in P_{k_2}} c_{Q_2,H_{21},E_1} E\left(\frac{H_{21}}{Q_2^{j_1+1}}A\right)\right)\left(\sum_{H_{22} \in P_{k_2}} c_{Q_2,H_{22},E_2} E\left(\frac{H_{22}}{Q_2^{j_2+1}}A\right)\right) \\
&= \sum_{H_{11},H_{12} \in P_{k_1}, H_{21},H_{22} \in P_{k_2}} c_{Q_1,H_{11},D_1}\, c_{Q_1,H_{12},D_2}\, c_{Q_2,H_{21},E_1}\, c_{Q_2,H_{22},E_2} \\
&\qquad \times \frac{1}{q^n} \sum_{A \in P_n} E\left(A\left(\frac{H_{11}}{Q_1^{i_1+1}} + \frac{H_{12}}{Q_1^{i_2+1}} + \frac{H_{21}}{Q_2^{j_1+1}} + \frac{H_{22}}{Q_2^{j_2+1}}\right)\right)
\end{aligned}$$

Of course, if $H_{11} = H_{12} = H_{21} = H_{22} = 0$ then we obtain the *main term*

$$\frac{1}{q_1^{2k_1} q_2^{2k_2}}.$$

For the remaining cases we will distinguish between four cases. Note that we only consider the case where all polynomials $H_{11}, H_{12}, H_{21}, H_{22}$ are non-zero. If some (but not all) of them are zero the considerations are still easier.

Case 1. $i_2 - i_1 \le c_1, j_2 - j_1 \le c_2$ for properly chosen constants $c_1, c_2 > 0$.
In this case we proceed as in the case $m_1 = m_2 = 1$ and obtain

$$\begin{aligned}
&\nu\left(\frac{H_{11}}{Q_1^{i_1+1}} + \frac{H_{12}}{Q_1^{i_2+1}} + \frac{H_{21}}{Q_2^{j_1+1}} + \frac{H_{22}}{Q_2^{j_2+1}}\right) \\
&= \nu\left(\frac{(H_{11}Q_1^{i_2-i_1} + H_{12})Q_2^{j_2+1} + (H_{21}Q_2^{j_2-j_1} + H_{22})Q_1^{i_2+1}}{Q_1^{i_2+1}Q_2^{j_2+1}}\right) \\
&\le k_1(i_2+1) + k_2(j_2+1) \\
&\quad - \max\{\deg(H_{11}Q_1^{i_2-i_1} + H_{12}) + k_2(j_2+1), \\
&\qquad \deg(H_{21}Q_2^{j_2-j_1} + H_{22}) + k_1(i_2+1)\} + c(c_1,c_2) \\
&\le \min\{k_1(i_1+1), k_2(j_1+1)\} + \tilde{c}(c_1,c_2)
\end{aligned}$$

for some suitable constants $c(c_1, c_2)$ and $\tilde{c}(c_1, c_2)$.

Case 2. $i_2 - i_1 > c_1, j_2 - j_1 > c_2$ for properly chosen constants $c_1, c_2 > 0$
First we recall that

$$\nu\left(\frac{H_{11}}{Q_1^{i_1+1}} + \frac{H_{21}}{Q_2^{j_1+1}}\right) \le \min\{k_1(i_1+1), k_2(j_1+1)\} + c.$$

Furthermore

$$\begin{aligned}\nu\left(\frac{H_{12}}{Q_1^{i_2+1}}\right) &\geq k_1(i_2+1)-\deg H_{12}\\ &\geq k_1(i_2-i_1)+k_1i_1 > k_1(i_1+c_1)\\ \nu\left(\frac{H_{22}}{Q_2^{j_2+1}}\right) &> k_2(j_1+c_2)\end{aligned}$$

Thus, if c_1 and c_2 are chosen that $(c_1-1)k_1 > c$ and $(c_2-1)k_2 > c$ then

$$\nu\left(\frac{H_{11}}{Q_1^{i_1+1}}+\frac{H_{21}}{Q_2^{j_1+1}}\right) < \min\left\{\nu\left(\frac{H_{12}}{Q_1^{i_2+1}}\right),\nu\left(\frac{H_{22}}{Q_2^{j_2+1}}\right)\right\}$$

and consequently by Lemma 12

$$\begin{aligned}\nu\left(\frac{H_{11}}{Q_1^{i_1+1}}+\frac{H_{12}}{Q_1^{i_2+1}}+\frac{H_{21}}{Q_2^{j_1+1}}+\frac{H_{22}}{Q_2^{j_2+1}}\right) &= \nu\left(\frac{H_{11}}{Q_1^{i_1+1}}+\frac{H_{21}}{Q_2^{j_1+1}}\right)\\ &\leq \min(k_1(i_1+1),k_2(j_1+1))+c\end{aligned}$$

Case 3. $i_2-i_1 \leq c_1, j_2-j_1 > c_2$ for properly chosen constants $c_1, c_2 > 0$

First we have

$$\begin{aligned}&\nu\left(\frac{H_{11}}{Q_1^{i_1+1}}+\frac{H_{12}}{Q_1^{i_2+1}}+\frac{H_{21}}{Q_2^{j_1+1}}\right)\\ &= \nu\left(\frac{(H_{11}Q_1^{i_2-i_1}+H_{12})Q_2^{j_1+1}+H_{21}Q_1^{i_2+1}}{Q_1^{i_2+1}Q_2^{j_1+1}}\right)\\ &\leq k_1(i_2+1)+k_2(j_1+1)\\ &\quad -\max\{k_1(i_2-i_1)+k_2(j_1+1),k_1(i_2+1)\}+c(c_1)\\ &= \min\{k_1(i_1+1),k_2(j_1+1)\}+c(c_1).\end{aligned}$$

Furthermore,

$$\begin{aligned}\nu\left(\frac{H_{22}}{Q_2^{j_2+1}}\right) &\geq k_2(j_2+1)-\deg(H_{22})\\ &\geq k_2(j_2-j_1)+k_2j_1 > k_2(j_1+c_2).\end{aligned}$$

Hence, if c_2 is sufficiently large then

$$\begin{aligned}\nu\left(\frac{H_{11}}{Q_1^{i_1+1}}+\frac{H_{12}}{Q_1^{i_2+1}}+\frac{H_{21}}{Q_2^{j_1+1}}+\frac{H_{22}}{Q_2^{j_2+1}}\right) &= \nu\left(\frac{H_{11}}{Q_1^{i_1+1}}+\frac{H_{12}}{Q_1^{i_2+1}}+\frac{H_{21}}{Q_2^{j_1+1}}\right)\\ &< \min(k_1(i_1+1),k_2(j_1+1))+c(c_1)\end{aligned}$$

Case 4. $i_2-i_1 > c_1, j_2-j_1 \leq c_2$ for properly chosen constants $c_1, c_2 > 0$

This case is completely symmetric to case 3.

Putting these four cases together they show that (with suitably chosen constants c_1, c_2) there exists a constant $\tilde{c}$ such that for all polynomials $(H_{11}, H_{12}, H_{21}, H_{22}) \neq (0,0,0,0)$ we have

$$\nu\left(\frac{H_{11}}{Q_1^{i_1+1}}+\frac{H_{12}}{Q_1^{i_2+1}}+\frac{H_{21}}{Q_2^{j_1+1}}+\frac{H_{22}}{Q_2^{j_2+1}}\right) \leq \min(k_1(i_1+1),k_2(j_1+1))+\tilde{c}.$$

Thus, there exists a constant $c' > 0$ such that

$$\min\{k_1(i_1+1),k_2(j_1+1)\}+\tilde{c} \leq n$$

for all i_1, j_1 with $0 \le i_1 \le \frac{n}{k_1} - c'$ and $0 \le j_1 \le \frac{n}{k_2} - c'$. Hence, by Lemma 13

$$\sum_{A \in P_n} E\left(A\left(\frac{H_{11}}{Q_1^{i_1+1}} + \frac{H_{12}}{Q_1^{i_2+1}} + \frac{H_{21}}{Q_2^{j_1+1}} + \frac{H_{22}}{Q_2^{j_2+1}}\right)\right) = 0.$$

This completes the proof for the case $m_1 = m_2 = 2$.

As in the proof of Theorem 2 we can rewrite Lemma 16 as

$$\begin{aligned}\frac{1}{q^n}\#\big\{A \in P_n : D_{Q_1,i_1}(A) = D_1, \dots, D_{Q_1,i_{m_1}}(A) = D_{m_1},\\ D_{Q_2,j_1}(A) = E_1, \dots, D_{Q_2,j_{m_2}}(A) = E_{m_2}\big\}\\ = \mathbb{P}[Y_{i_1} = D_1, \dots, Y_{i_{m_1}} = D_{m_1}, Z_1 = E_{j_1}, \dots, Z_{j_{m_2}} = E_{m_2}],\end{aligned}$$

where Y_i and Z_j are independent random variables that are uniformly distributed on P_{k_1} resp. on P_{k_2}.

If we define

$$\widetilde{g_1}(A) := \sum_{j_1 \le \frac{n}{k_1} - c'} g_1(D_{Q_1,j_1}(A)),$$

$$\widetilde{g_2}(A) := \sum_{j_2 \le \frac{n}{k_2} - c'} g_2(D_{Q_2,j_2}(A))$$

then Lemma 16 immediately translates to

Lemma 17. *For all positive integers m_1, m_2 we have for sufficiently large n*

$$\begin{aligned}&\frac{1}{q^n}\sum_{A \in P_n}\left(\widetilde{g_1}(A) - \frac{n}{k_1}\mu_{g_1}\right)^{m_1}\left(\widetilde{g_2}(A) - \frac{n}{k_2}\mu_{g_2}\right)^{m_2}\\ &= \mathbb{E}\left(\sum_{j_1 \le \frac{n}{k_1} - c'}(g_1(Y_{j_1}) - \mu_{g_1})\right)^{m_1}\mathbb{E}\left(\sum_{j_2 \le \frac{n}{k_2} - c'}(g_2(Z_{j_2}) - \mu_{g_2})\right)^{m_2}.\end{aligned}$$

Of course this implies that the joint distribution of $\tilde{g}_1$ and $\tilde{g}_2$ is asymptotically Gaussian (after normalization). Since the differences $g_1(A) - \tilde{g}_1(A)$ and $g_2(A) - \tilde{g}_2(A)$ are bounded the same is true for the joint distribution of g_1 and g_2. This completes the proof of Theorem 3.

References

[1] N. L. Bassily and I. Kátai, Distribution of the values of q-additive functions on polynomial sequences, *Acta Math. Hung.* **68** (1995), 353–361.

[2] Mireille Car, Sommes de puissances et d'irréductibles dans $F_q[X]$, *Acta Arith.* **44** (1984), 7–34.

[3] J. Coquet, Corrélation de suites arithmétiques, *Sémin. Delange-Pisot-Poitou,* 20e Année 1978/79, Exp. 15, 12 p. (1980).

[4] H. Delange Sur les fonctions q-additives ou q-multiplicatives, *Acta Arith.* **21** (1972), 285-298.

[5] H. Delange Sur la fonction sommatoire de la fonction "Somme de Chiffres", *L'Enseignement math.* **21** (1975), 31–77.

[6] M. Drmota, The joint distribution of q-additive functions, *Acta Arith.* **100** (2001), 17–39.

[7] M. Drmota and J. Gajdosik, The distribution of the sum-of-digits function, *J. Theor. Nombres Bordx.* **10** (1998), 17–32.

[8] J. M. Dumont and A. Thomas, Gaussian asymptotic properties of the sum-of-digits functions, *J. Number Th.* **62** (1997), 19–38.

[9] P. J. Grabner, P. Kirschenhofer, H. Prodinger, and R. F. Tichy, On the moments of the sum-of-digits function, in: *Applications of Fibonacci Numbers* **5** (1993), 263–271

[10] G.W. Effinger and D. R. Hayes, *Additive number theory of polynomials over a finite field.* Oxford University Press, New York, 1991.

[11] I. Kátai, Distribution of q-additive function, Probability theory and applications, *Essays to the Mem. of J. Mogyorodi, Math. Appl.* **80**, Kluwer, Dortrecht, 309–318 (1992).

[12] R. E. Kennedy and C. N. Cooper, An extension of a theorem by Cheo and Yien concerning digital sums, *Fibonacci Q.* **29** (1991), 145–149.

[13] D.-H. Kim, On the joint distribution of q-additive functions in residue classes , *J. Number Theory* **74** (1999), 307 – 336.
[14] P. Kirschenhofer, On the variance of the sum of digits function, *Lecture Notes Math.* **1452** (1990), 112–116.
[15] E. Manstavičius, Probabilistic theory of additive functions related to systems of numerations, *Analytic and Probabilistic Methods in Number Theory,* VSP, Utrecht 1997, 413–430.
[16] R. C. Mason, Diophantine Equations over Function Fields, *London Math. Soc. Lecture Notes* **96**, Cambridge University Press, 1984.
[17] W. Steiner, On the joint distribution of q-additive functions on polynomial sequences, *Theory of Stochastic Processes* **8** (24) (2002), 336–357.