
TECHNISCHE UNIVERSITÄT WIEN

VIENNA UNIVERSITY OF TECHNOLOGY

# DISSERTATION

# The Joint Distribution of Q-additive Functions on Polynomials over Finite Fields

ausgeführt zum Zwecke der Erlangung des akademischen Grades
eines Doktors der technischen Wissenschaften unter der Leitung von

Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Michael Drmota
Institut für Diskrete Mathematik und Geometrie, E104

eingereicht an der Technischen Universität Wien
Fakultät für Mathematik und Geoinformation

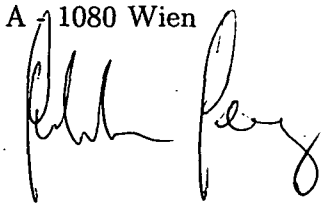
von

Dipl.-Ing. Georg Gutenbrunner
Matr.Nr.: 9725229

Greinerstraße 21
A - 4320 Perg

Breitenfeldergasse 9/17
A - 1080 Wien

Wien, am 1. Juni 2004



# Kurzfassung

In der zweiten Hälfte des vergangenen Jahrhunderts wurde der Begriff der $q$-additiven Funktionen geprägt. Damit im Zusammenhang stehen einerseits Michel Mendes-France und Hubert Delange sowie andere Vertreter der französischen Schule. Andererseits beschäftigte sich auch der russische Mathematiker Aleksandr Ossipovich Gelfond (1906-1968) damit. In einer seiner letzten Publikationen [15] hat er diese spezielle Art von Funktionen wie folgt definiert:

> Sei $q$ eine beliebige fest gewählte ganze Zahl größer als oder gleich zwei. Eine Funktion $f : \mathbb{N} \to \mathbb{R}$ heißt (vollständig) *$q$-additiv*, wenn für beliebige $a \geq 1$ und $0 \leq b < q$
>
> $$f(aq + b) = f(a) + f(b) \tag{1}$$
>
> gilt.

Seit den Anfängen in den späten 60er Jahren des 20. Jahrhunderts wurden viele Fortschritte erzielt, und so sind heute bereits zahlreiche Ergebnisse rund um $q$-additive Funktionen bekannt.

In der vorliegenden Arbeit beschreiten wir einen neuen Weg und führen die sogenannten $Q$-additiven Funktionen ein. Dabei handelt es sich um eine Verallgemeinerung der obigen $q$-additiven Funktionen, die folgendermaßen definiert ist:

> Sei $K$ ein endlicher Körper und $Q \in K[T]$ ein beliebiges Polynom mit positivem Grad. Eine Funktion $f$ auf $K[T]$ heißt (vollständig) *$Q$-additiv*, wenn für beliebige $A, B \in K[T]$ mit $\operatorname{grad}(B) < \operatorname{grad}(Q)$
>
> $$f(AQ + B) = f(A) + f(B) \tag{2}$$
>
> gilt.

Ziel dieser Dissertation ist es, das Verteilungsverhalten von $Q$-additiven Funktionen zu untersuchen. Genauer gesagt werden wir drei Resultate (von Kim, Bassily & Kátai bzw. Drmota) über $q$-additive Funktionen für den Polynomring über einem endlichen Körper adaptieren.

In Kapitel 1 wird zunächst ein kleiner Überblick über verschiedene Ergebnisse vorangegangener Untersuchungen zahlreicher Mathematiker gegeben. Besonderes Augenmerk wird dabei auf jene drei Resultate gelegt, die wir im Laufe der Dissertation in unserem Sinne verallgemeinern werden.
Weiters werden die wichtigsten Eigenschaften des additiven Charakters $E$ zusammengestellt.

In Kapitel 2 verallgemeinern wir ein Resultat von Dong-Hyun Kim [20] über die gemeinsame Verteilung von $q$-additiven Funktionen in Residuenklassen. Der Beweis unserer Verallgemeinerung (Theorem 4) stützt sich dabei teilweise auf Kims Methoden, es treten aber andere Schwierigkeiten auf.
In einem zweiten Unterkapitel (2.2) werden noch einige Fragen, die im Laufe unserer Betrachtungen im Zusammenhang mit oben genannten Theorem 4 auftauchen, behandelt.

In Kapitel 3 werden zwei zentrale Grenzwertsätze bewiesen. Zum einen verallgemeinern wir in 3.1 ein Resultat von Bassily und Kátai [1], einen zentralen Grenzwertsatz für die Verteilung der Folgen $f(P(n))$, $n \in \mathbb{N}$, und $f(P(p))$, $p \in \mathbb{P}$, wobei $f(n)$ eine $q$-additive Funktion und $P(n)$ ein Polynom mit ganzzahligen Koeffizienten ist. Mit Hilfe einer Abschätzung von $E$-Summen (siehe Lemma 24) sowie der Momentenmethode kann das entsprechende Resultat (Theorem 5) bewiesen werden.

Im letzten Abschnitt beschäftigen wir uns schließlich mit einem Ergebnis von Drmota [9]. Dieser hat Bassily und Kátais Ergebnisse auf die gemeinsame Verteilung von zwei Folgen $f_1(n)$ und $f_2(n)$ verallgemeinert, wobei $f_l(n)$ $q_l$-additive Funktionen und die Basen $q_1, q_2$ relativ prim sind. Für unsere Zwecke benötigen wir zusätzlich zu den Methoden aus 3.1 den Satz von Mason. Damit gelingt es uns, ein ensprechendes Resultat für die gemeinsame Verteilung von $Q_1$- bzw. $Q_2$-additiven Funktionen auf dem Polynomring über einem endlichen Körper zu beweisen, wobei $Q_1$ und $Q_2$ relativ prim sind.

# Abstract

The notion of $q$-additive functions was established in the second half of the last century. On the one hand, scientists like Michel Mendes-France and Hubert Delange as well as other members of the French school obtained first results on this concept. On the other hand, it was mainly the Russian mathematician Aleksandr Ossipovich Gelfond (1906-1968), who studied this matter. In one of his last publications [15] he defined this special kind of function as follows:

> Let $q$ be an arbitrary fixed integer, $q \geq 2$. A function $f : \mathbb{N} \to \mathbb{R}$ is called (completely) *$q$-additive* if
>
> $$f(aq + b) = f(a) + f(b) \tag{3}$$
>
> for arbitrary $a \geq 1$ and $0 \leq b < q$.

Since these beginnings in the late 60s of the $20^{th}$ century much progress has been achieved. Thus, various results concerning $q$-additive functions are known today.

In this thesis we work in the ring of polynomials over a finite field, and introduce the so-called $Q$-additive functions. They constitute a generalization of the above mentioned $q$-additive functions and are defined in the following way.

> Let $K$ be a finite field and $Q \in K[T]$ an arbitrary polynomial of positive degree. A function $f$ on $K[T]$ is called (completely) *$Q$-additive* if
>
> $$f(AQ + B) = f(A) + f(B) \tag{4}$$
>
> where $A, B \in K[T]$ and $\deg(B) < \deg(Q)$.

The aim of this thesis is to study the distribution of $Q$-additive functions. More precisely, we are going to adapt three results (by Kim, Bassily & Kátai and Drmota) about $q$-additive functions for the ring of polynomials over a finite field.

In Chapter 1 we will give a brief survey of different results of previous studies by various mathematicians. Our main focus will be on the above mentioned three results which we are going to generalize in the course of this thesis. Moreover, we will introduce the additive character $E$, on which all of our studies are based.

In Chapter 2 we are first going to concentrate on a work by Dong-Hyun Kim [20] about the joint distribution of $q$-additive functions in residue classes. The proof of our generalization (Theorem 4) will partly rely on Kim's original proof, but we have to face some difficulties that are different from that of Kim.
In a second section (2.2) we are going to deal with several questions which arise in the course of our study of Theorem 4.

In Chapter 3 we are going to prove two central limit theorems. On the one hand, we will generalize Bassily & Kátai's result in 3.1. They proved a central limit theorem for the distribution of sequences $f(P(n))$, $n \in \mathbb{N}$, and $f(P(p))$, $p \in \mathbb{P}$, where $f(n)$ is a $q$-additive function and $P(n)$ an arbitrary polynomial with integer coefficients. By the help of an estimate of $E$-sums (see Lemma 24) as well as the method of moments the corresponding result (Theorem 5) can be shown.

In our last section, we finally focus on Drmota's article [9]. In his work, Drmota generalized Bassily & Kátai's theorem for the joint distribution of two sequences $f_1(n), f_2(n)$ where $f_l(n)$ are $q_l$-additive functions, and $q_1$ and $q_2$ are coprime. For our purposes, we also need Mason's Theorem in addition to the methods used in 3.1. Thus, we succeed in proving the desired result for $Q_1$- and $Q_2$-additive functions on the ring of polynomials over a finite field, where $Q_1$ and $Q_2$ are coprime.

# Contents

# Chapter 1

# Introduction

The purpose of this chapter is to present basic preliminaries about $Q$-additive functions, on which our research in Chapters 2 and 3 is based.
We will start by defining $q$-additive functions which are concerned with integers. Of course, one cannot discuss $q$-additive functions without mentioning members of the French school like Mendes-France, Delange and Coquet, as well as the Russian mathematician A.O. Gelfond. The latter's basic ideas and definitions of $q$-additive functions will be given close attention.

While the early work on $q$-additive functions is still essential with respect to terminology, the findings themselves have long been extended. Therefore, we will give a brief survey about several works on $q$-additive functions. Of particular interest will be three more recent works, namely one by Kim ([20]), which is a generalization of Gelfond, one by Bassily and Kátai ([1]), who studied the distribution of $q$-additive functions on polynomial sequences, and one by Drmota ([9]), which is, in turn, a generalization of Bassily and Kátai. We will cite these results in a slightly modified form.
After that, we will introduce the new definition of $Q$-additive functions which are concerned with polynomials and which represent our actual focus.

The main aim of this thesis will be to generalize the results of the three above mentioned articles. Whereas they deal with $q$-additive functions defined on the non-negative integers, we try to translate these findings into $Q$-additive functions defined on the ring of polynomials over a finite field.

In the final section of this introduction we will deal with the properties of the additive character $E$ which is strongly related to the ordinary exponential function $\exp : \mathbb{R} \to \mathbb{R}$. As our proofs include the study of exponential sums, $E$ is a basic tool.

## 1.1 $q$-additive functions

The history of research concerning $q$-additive functions dates back to the 1960s. The first scientists who concerned themselves with this matter were members of the French school like Michel Mendes-France and Hubert Delange as well as the Russian mathematician Aleksandr Ossipovich Gelfond. They laid the foundation for the following definition.

Let $q > 1$ be a given integer. Then, every non-negative integer $n$ has a unique *$q$-ary expansion*

$$n = \sum_{j \geq 0} \varepsilon_{q,j}(n) q^j$$

with $\varepsilon_{q,j}(n) \in E_q := \{0, 1, \ldots, q-1\}$. The $\varepsilon_{q,j}(n)$ are called *digits* of $n$ in base $q$. If there is no risk of confusion, the index $q$ will be omitted.
$\{q, E_q\}$ is called a number system. There are generalizations of such number systems, however they are of no concern to the thesis in hand. For further reference see [22].
A function $f : \mathbb{N} \to \mathbb{R}$ is called *$q$-additive*, if $f(0) = 0$ and

$$f(n) = \sum_{j \geq 0} f(\varepsilon_{q,j}(n) q^j).$$

If $f$ even satisfies

$$f(n) = \sum_{j \geq 0} f(\varepsilon_{q,j}(n)),$$

it is said to be *completely $q$-additive*. An example of such a function is the *sum-of-digits function* $s_q : \mathbb{N} \to \mathbb{N}$ that denotes the sum of the digits of $n$ in base $q$:

$$s_q(n) = \sum_{j \geq 0} \varepsilon_{q,j}(n).$$

This particular example, as well as $q$-additive functions in general, has been very well studied by several authors.
Manstavičius [24], for example, extended an idea of Coquet [6]. He focused on the mean value of $q$-additive functions and formulated the most general result so far: Let

$$\mu_k = \frac{1}{q} \sum_{b=0}^{q-1} f(bq^k), \qquad \mu_{2;k}^2 = \frac{1}{q} \sum_{b=0}^{q-1} f(bq^k)^2$$

and

$$M(N) = \sum_{k=0}^{[\log_q N]} \mu_k, \qquad B(N)^2 = \sum_{k=0}^{[\log_q N]} \mu_{2,k}^2.$$

Then,

$$\frac{1}{N}\sum_{n<N}(f(n)-M(N))^2 \leq cB(N)^2,$$

which implies

$$\frac{1}{N}\sum_{n<N} f(n) = M(N) + O(B(N)).$$

For the sum-of-digits function $s_q(n)$ other much more precise results are known. For integral $N$, Delange [8] proved

$$\frac{1}{N}\sum_{n<N} s_q(n) = \frac{q-1}{2}\log_q N + \gamma(\log_q N),$$

where $\gamma$ is a continuous, nowhere differentiable and periodic function with period 1. Without mentioning their results in detail, we want to quote Kirschenhofer [21], Kennedy and Cooper [19] and Grabner, Kirschenhofer, Prodinger and Tichy [16] who studied higher moments of $s_q(n)$ in the given articles.

However, we want to present an interesting result by Gelfond [15]:

**Assertion 1** *Let $q > 1$, $p > 1$, $m > 1$, $l, a \in \mathbb{N}$ and $(p, q-1) = 1$. Then, the number of integers $n, n \leq N$, satisfying*

$$n \equiv l \ (m) \qquad \text{and} \qquad s_q(n) \equiv a \ (p),$$

*is given by*

$$\frac{N}{mp} + O(N^\lambda), \quad \lambda < 1.$$

Interestingly, one special case of Assertion 1 can even be found in an earlier work by Nathan Jacob Fine [14], which dates back to 1965. It deals with Stanislav Marcin Ulam's question whether the number of $n < N$ for which $s_{10}(n) \equiv n \equiv 0 \pmod{13}$ is asymptotically $N/13^2$.
This question was affirmatively answered by Fine's above mentioned article. Additionally, the latter showed

$$\lim_{N\to\infty}\frac{1}{N}\#\{n < N \mid n \equiv a \ (p) \text{ and } s_q(n) \equiv c \ (p)\} = \frac{1}{p^2}$$

for arbitrary $0 \leq a, c < p$ and for any prime $p$ which must, however, not be a divisor of $(q-1)$.

Gelfond was certainly not the first scientist to work on such questions. Nevertheless, he and the members of the French school were one of the first who contributed considerably to the notion of $q$-additive functions and who studied them in detail.

## 1.2 More recent findings on the distribution of $q$-additive functions

As we have learned in section 1.1, Gelfond's studies led to Assertion 1 about the sum-of-digits function $s_q(n)$. Now let us neglect the residue class which contains $n$. Then, due to Assertion 1, Gelfond actually proved the estimate

$$\frac{1}{N}\#\{0 \le n < N : s_q(n) \equiv a \bmod m\} = \frac{1}{m} + O(N^{1-\delta}) \qquad (1.1)$$

which is valid for any integer $a$ and positive $N$, where $\delta = \delta(q,m)$ is a positive constant depending only on $q$ and $m$.
In other words, he showed that the sum-of-digits function $s_q(n)$ is uniformly distributed in residue classes modulo $m$ for an arbitrary integer $m \ge 2$ provided that $m$ is coprime to $q-1$.

Since the beginnings of $q$-additive functions, they have been extensively discussed in the literature. One reason for this can be found in the fact that Gelfond, Mendes-France and Delange did not only create the pure concept of $q$-additive functions, but also made several conjectures concerning these functions. So, it was only a question of time until other scientists engaged in studying this field further in order to examine those conjectures and, if possible, to verify them.

For example, in [15] Gelfond made the following conjecture, which actually is a generalization of estimate (1.1).

**Conjecture 1** *Let $m_1, m_2, q_1$ and $q_2$ be integers $\ge 2$ satisfying $(q_1, q_2) = 1$ and $(m_1, q_1 - 1) = (m_2, q_2 - 1) = 1$. Then,*

$$\frac{1}{N}\#\{0 \le n < N : s_{q_1}(n) \equiv a_1 \bmod m_1, s_{q_2}(n) \equiv a_2 \bmod m_2\}$$
$$= \frac{1}{m_1 m_2} + O(N^{1-\delta}) \qquad (N \ge 1)$$

*holds for arbitrary integers $a_1, a_2$.*

Only a few years later, Bésineau [2] was able to take a decisive step towards Conjecture 1 in that his result was already valid for an arbitrary number of bases $q_i$. However, he did not fully succeed in attaining the error term which had originally been asserted. Actually, Bésineau showed that for any integers $a_1, a_2, \ldots, a_d$, as $N \to \infty$,

$$\frac{1}{N}\#\{0 \le n < N | s_{q_i}(n) \equiv a_i \bmod m_i, 1 \le i \le d\} \sim \frac{1}{m_1 m_2 \cdots m_d} \qquad (1.2)$$

holds under the condition that the bases $q_i$ are pairwise coprime and

$$(m_i, q_i - 1) = 1 \text{ for } 1 \leq i \leq d.$$

In 1998, Dong-Hyun Kim was able to sharpen Bésineau's estimate (1.2) to an estimate with the desired error term $O(N^{1-\delta})$. Moreover, Kim replaced the sum-of-digits function $s_{q_i}(n)$ by an arbitrary completely $q_i$-additive function $f_i$.

**Theorem 1 (Kim [20])** *Suppose that $q_1, \ldots, q_d \geq 2$ are pairwise coprime integers, $m_1, \ldots, m_d$ positive integers, and let $f_j$ be completely $q_j$-additive functions for $1 \leq j \leq d$. Set*

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

*Then, $H$ is a subgroup of $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}$ and we have*

$$\frac{1}{N}\#\{n < N : f_1(n) \bmod m_1 = a_1, \ldots, f_d(n) \bmod m_d = a_d\} = \begin{cases} 1/|H| + O\left(N^{1-\delta}\right) & (a_1, \ldots, a_d) \in H, \\ 0 & \text{otherwise,} \end{cases}$$

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

$$\overline{q} = \max_{1 \leq j \leq d} q_j \quad \text{and} \quad \overline{m} = \max_{1 \leq j \leq d} m_j;$$

*and the $O$-constant depends only on $d$ and $q_1, \ldots, q_d$.*

In [20] the set $H$ is explicitly determined. Set

$$\begin{aligned} F_j &= f_j(1), \\ d_j &= \gcd\{m_j, (q_j - 1)F_j, f_j(r) - rF_j \ (2 \leq r \leq q_j - 1)\}, \end{aligned}$$

for each $1 \leq j \leq d$. A $d$-tuple $(a_1, \ldots, a_d)$ of integers is called admissible with respect to the $d$-tuples $(q_1, \ldots, q_d), (m_1, \ldots, m_d)$ and $(f_1, \ldots, f_d)$, if the system of congruences

$$F_j n \equiv a_j \bmod d_j, 1 \leq j \leq d$$

has a solution.
Then, the elements of the set $H$ are exactly these admissible $d$-tuples in the above sense. Furthermore, Kim characterizes the admissible $d$-tuples $(a_1, \ldots, a_d)$ by congruence conditions in the following lemma.

**Lemma 1** *A d-tuple $(a_1, \ldots, a_d)$ of integers is admissible with respect to $(q_1, \ldots, q_d), (m_1, \ldots, m_d)$ and $(f_1, \ldots, f_d)$, if and only if the following conditions hold:*

$$\begin{aligned} (F_j, d_j) \mid a_j \qquad & (1 \leq j \leq d), \\ a_i^* F_j^* \equiv a_j^* F_i^* \bmod (d_i^*, d_j^*) \qquad & (i \neq j), \end{aligned}$$

*where $a_j^* = a_j/(F_j, d_j)$, $F_j^* = F_j/(F_j, d_j)$, and $d_j^* = d_j/(F_j, d_j)$. Moreover, if $(a_1, \ldots, a_d)$ is admissible, then*

$$\frac{1}{N}\#\{0 \leq n < N : F_j n \equiv a_j \bmod d_j (1 \leq j \leq d)\} = \begin{cases} 1/D + O(1) & \text{for all } N \geq 1, \\ 1/D & \text{if } D \mid N, \end{cases}$$

*where $D = [d_1^*, d_2^*, \ldots, d_d^*]$.*

The lemma follows directly from the definition of admissibility and the generalized version of the Chinese Remainder Theorem (see [28], Theorem 5.4.3 pp. 156–157).

**Remark 1** *In our next chapter we will generalize Theorem 1 and modify some of the ideas of Kim's proof for his theorem. Fortunately, in the case of polynomials over finite fields some aspects are easier to show than for integers, so some parts of Kim's original proof may be neglected. Some other difficulties appear instead.*

During the second half of the $20^{th}$ century other fields of research concerning these functions were explored as well. Thus, one can also find distributional results for $q$-additive functions in the literature. In this context we mention an analogue to the Erdös-Wintner Theorem by Delange [7]. There exists a distribution function $F(x)$ such that, as $N \to \infty$,

$$\frac{1}{N}\#\{n < N | f(n) < x\} \to F(x) \tag{1.3}$$

if and only if the two series $\sum_{k \geq 0} \mu_k$ and $\sum_{k \geq 0} \mu_{2;k}^2$ converge.
Later on, Imre Kátai [18] could generalize this result by proving that there exists a distribution function $F(x)$ such that, as $N \to \infty$,

$$\frac{1}{N}\#\{n < N | f(n) - M(N) < x\} \to F(x),$$

if and only if the series $\sum_{k \geq 0} \mu_{2;k}^2$ converges.

Once more, the most general result known concerning a central limit theorem is due to Manstavičius [24]. Suppose that, as $N \to \infty$,

$$\max_{bq^j<N} |f(bq^j)| = o(B(N))$$

and that $D(N) \to \infty$, where

$$D(N)^2 = \sum_{k=0}^{[\log_q N]} \sigma_k^2 \qquad \text{and} \qquad \sigma_k^2 = \frac{1}{q}\sum_{b=0}^{q-1} f(bq^k)^2 - m_k^2.$$

Then, as $N \to \infty$,

$$\frac{1}{N}\#\left\{n < N \Big| \frac{f(n) - M(N)}{D(N)} < x\right\} \to \Phi(x),$$

where $\Phi(x)$ is the ordinary normal distribution function.

Again, we content ourselves with just mentioning that similar distribution results can be found by Dumont and Thomas [12] resp. Drmota and Gajdosik [10].

Some years before Kim's work was published, Bassily and Kátai [1] studied the distribution of $q$-additive functions on polynomial sequences. They proved a central limit theorem for the distribution of sequences $f(P(n))$, $n \in \mathbb{N}$, and $f(P(p)), p \in \mathbb{P}$, where $f(n)$ is a $q$-additive function and $P(n)$ an arbitrary polynomial with non-negative integer coefficients.
This central limit theorem provides the second result which we are going to generalize at the beginning of Chapter 3.

**Theorem 2 (Bassily-Kátai [1])** *Let $f$ be a completely $q$-additive function and let $P(x)$ be a polynomial of degree $r$ with non-negative integer coefficients. Then, as $N \to \infty$,*

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

*and*

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

*where*

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

*and*

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

**Remark 2** *The result of [1] is more general. It even provides asymptotic normality, if $f$ is not strictly $q$-additive but the variance grows sufficiently fast.*

It seems to be a natural question to ask whether there are analogue results for the joint distribution of several $q_i$-additive functions $f_i(n)$, $1 \le i \le d$ (if $q_1, \ldots, q_d > 1$ are pairwise coprime integers). Drmota [9] quotes A.J. Hildebrand, who announced that one always has

$$\frac{1}{N}\#\{n < N | f_i(n) < x_i, 1 \le i \le d\} \to F_1(x)\cdots F_d(x)$$

if $f_i$ satisfies (1.3) for all $1 \le i \le d$ and that there is a joint central limit theorem of the form

$$\frac{1}{N}\#\left\{n < N \Big| \frac{f_i(n) - M_{q_i}(N)}{D_{q_i}(N)} < x_i, 1 \le i \le d\right\} \to \Phi(x_1)\Phi(x_2)\cdots\Phi(x_d)$$

if $B_{q_i}(N) \to \infty$ and $B_{q_i}(N^\eta) \sim B_{q_i}(N)$ for every $\eta > 0$ as $N \to \infty$.

Drmota [9] used a variation of Bassily and Kátai's proof; he combined it with a proper version of Baker's Theorem on linear forms of logarithms to generalize Theorem 2 on the joint distribution of sequences $f_i(P_i(n))$ (and $f_i(P_i(p))$ respectively) where $f_i$ are $q_i$-additive functions and $P_i(n)$ are polynomials of different degrees. For polynomials of equal degree Drmota could prove a central limit theorem only for two sequences $f_1(P_1(n)), f_2(P_2(n))$ with coprime $q_1, q_2$, and linear polynomials $P_1(n), P_2(n)$.
The result of his paper will be explained in the following theorem.

**Theorem 3 (Drmota [9])** *Suppose that $q_1 \ge 2$ and $q_2 \ge 2$ are coprime integers and that $f_1$ and $f_2$ are completely $q_1$- resp. $q_2$-additive functions. Then, as $N \to \infty$,*

$$\frac{1}{N}\#\left\{n < N : \frac{f_1(n) - \mu_{f_1}\log_{q_1} N}{\sqrt{\sigma_{f_1}^2 \log_{q_1} N}} \le x_1, \frac{f_2(n) - \mu_{f_2}\log_{q_2} N}{\sqrt{\sigma_{f_2}^2 \log_{q_2} N}} \le x_2\right\}$$
$$\to \Phi(x_1)\Phi(x_2).$$

**Remark 3** *By adapting Vinogradov's and Hua's results on exponential sums of polynomial sequences, Steiner [31] could extend Drmota's result to arbitrary polynomials $P_1(n), P_2(n)$ and sequences of primes. However, up to now it has not been possible to prove a similar property for three or more bases $q_j$.*

Theorem 3 constitutes the third result we are going to generalize in section 3.2.

## 1.3 $Q$-ary expansions and $Q$-additive functions

Contrary to $q$-additive functions, which deal with integers, $Q$-additive functions are concerned with polynomials.

Let $\mathbb{F}_q$ be a finite field of characteristic $p$ (that is, $q = |\mathbb{F}_q|$ is a power of $p \in \mathbb{P}$) and let $\mathbb{F}_q[T]$ denote the ring of polynomials over $\mathbb{F}_q$. The set of polynomials in $\mathbb{F}_q$ of degree $< k$ will be denoted by

$$P_k := \{A \in \mathbb{F}_q[T] : \deg A < k\}.$$

Sometimes we need a special subset of $P_k$:

$$\begin{aligned} P_k^* &:= \{A \in \mathbb{F}_q[T] : \deg A < k \ \wedge A \neq 0\} \\ &= P_k \setminus \{0\}. \end{aligned}$$

Analogously to the integer case, we can define the following: 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 $f(AQ + B) = f(A) + f(B)$, where $A, B \in \mathbb{F}_q[T]$ and $\deg(B) < \deg(Q)$. More precisely, if a polynomial $A \in \mathbb{F}_q[T]$ is represented in its *$Q$-ary digital expansion*

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

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

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

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

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

**Remark 4** *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* $s_Q(A+B) = s_Q(A) + s_Q(B)$.

This is based on the property that there is no carry over for the single digits when adding two polynomials, i.e. let

$$A = \sum_{j\geq 0} D_{Q,j}(A)Q^j, \qquad B = \sum_{j\geq 0} D_{Q,j}(B)Q^j,$$

and $C := A + B$, then

$$C = \sum_{j\geq 0} D_{Q,j}(C)Q^j \text{ with } D_{Q,j}(C) = D_{Q,j}(A) + D_{Q,j}(B).$$

Furthermore, $\deg(C) = \max\{\deg(A), \deg(B)\}$ if $\deg(A) \neq \deg(B)$.

In order to be able to analyze more complex results, we need the following notation introduced by Hayes [17], which we will just adopt.
Let $\mathbb{F}_q(T)$ denote the field of rational functions over the finite field $\mathbb{F}_q$:

$$\mathbb{F}_q(T) = \left\{ \frac{A}{B} \middle| A, B \in \mathbb{F}_q[T], B \neq 0 \right\}.$$

On $\mathbb{F}_q(T)$ one has the valuation $\nu$ associated with the „infinite prime“ of $\mathbb{F}_q(T)$ and defined by

$$\nu(0) = \infty, \tag{1.4}$$
$$\nu(A/B) = \deg(B) - \deg(A) \tag{1.5}$$

for every non-zero rational function $A/B$. The valuation has the following properties:

**Lemma 2** *Let* $a_1, \ldots, a_n \in \mathbb{F}_q(T)$, *then,*

1. $\nu\left(\prod_{i=1}^n a_i\right) = \sum_{i=1}^n \nu(a_i)$
2. $\nu(a_1 + a_2 + \cdots + a_n) \geq \min\{\nu(a_1), \nu(a_2), \ldots, \nu(a_n)\}$
3. $\nu(a_i) = \infty$ *if and only if* $a_i = 0$.

*Proof.*

1. Let $a_i = A_i/B_i$ for $i = 1, \ldots, n$. Then,

$$\begin{aligned}
\prod_{i=1}^{n} a_i &= \prod_{i=1}^{n} \frac{A_i}{B_i} \\
\nu\left(\prod_{i=1}^{n} a_i\right) &= \nu\left(\frac{\prod_{i=1}^{n} A_i}{\prod_{i=1}^{n} B_i}\right) = \deg\left(\prod_{i=1}^{n} B_i\right) - \deg\left(\prod_{i=1}^{n} A_i\right) \\
&= \sum_{i=1}^{n} \deg(B_i) - \sum_{i=1}^{n} \deg(A_i) = \sum_{i=1}^{n} \nu\left(\frac{A_i}{B_i}\right) \\
&= \sum_{i=1}^{n} \nu(a_i).
\end{aligned}$$

2. We only prove property 2 for $n = 2$. The general case follows by induction.

$$\begin{aligned}
\frac{A}{B} + \frac{C}{D} &= \frac{AD + BC}{BD} \\
\nu\left(\frac{A}{B} + \frac{C}{D}\right) &= \deg(B) + \deg(D) - \deg(AD + BC) \\
&\geq \min\{\deg(B) + \deg(D) - \deg(A) - \deg(D), \\
&\qquad \deg(B) + \deg(D) - \deg(B) - \deg(C)\} \\
&= \min\{\deg(B) - \deg(A), \deg(D) - \deg(C)\} \\
&= \min\left\{\nu\left(\frac{A}{B}\right), \nu\left(\frac{C}{D}\right)\right\}.
\end{aligned}$$

3. Property 3 follows directly from the definition of $\nu$.

□

The next lemma is an important extension of property 2.

**Lemma 3** *Let $a_1, \ldots, a_n \in \mathbb{F}_q(T)$ with pairwise different valuations (i.e. $\nu(a_i) \neq \nu(a_j)$ for $i \neq j$), then,*

$$\nu(a_1 + a_2 + \cdots + a_n) = \min\{\nu(a_1), \nu(a_2), \ldots, \nu(a_n)\}. \tag{1.6}$$

*Proof.* Again, we will concentrate on $n = 2$. The general case follows by induction.

$$\begin{aligned} \nu\left(\frac{A}{B}\right) \neq \nu\left(\frac{C}{D}\right) &\Leftrightarrow \deg(B) - \deg(A) \neq \deg(D) - \deg(C) \\ &\Leftrightarrow \deg(A) + \deg(D) \neq \deg(B) + \deg(C) \\ &\Leftrightarrow \deg(AD) \neq \deg(BC). \end{aligned}$$

If $\deg(AD) \neq \deg(BC)$, then $\deg(AD + BC) = \max\{\deg(AD), \deg(BC)\}$. Thus,

$$\begin{aligned} \nu\left(\frac{A}{B} + \frac{C}{D}\right) &= \deg(B) + \deg(D) - \deg(AD + BC) \\ &= \min\{\deg(B) + \deg(D) - \deg(A) - \deg(D), \\ &\qquad \deg(B) + \deg(D) - \deg(B) - \deg(C)\} \\ &= \min\{\deg(B) - \deg(A), \deg(D) - \deg(C)\} \\ &= \min\left\{\nu\left(\frac{A}{B}\right), \nu\left(\frac{C}{D}\right)\right\}. \end{aligned}$$

□

Let $\mathbb{F}_q((1/T))$ denote the set of formal Laurent series in $1/T$. It is well knwon that $\mathbb{F}_q((1/T))$ is the completion of $\mathbb{F}_q(T)$ with respect to the valuation $\nu$. More precisely, every $A \in \mathbb{F}_q((1/T))$ can be expanded in a unique way formal in an infinite series of the form

$$A = \sum_{j=-\infty}^{\infty} a_j \left(\frac{1}{T}\right)^j$$

with $a_j \in \mathbb{F}_q$. Thereby, all but a finite number of coefficients $a_j$ with $j < 0$ are zero. Thus, there exists $k \in \mathbb{N}$ with

$$A = \sum_{j \geq -k} a_j \left(\frac{1}{T}\right)^j. \tag{1.7}$$

The extension of the valuation $\nu$ to $\mathbb{F}_q((1/T))$ can also be determined in terms of the representation (1.7). If $A \neq 0$ and $A$ has the Laurent expansion (1.7), then,

$$\nu(A) = \text{ the smallest } j \text{ such that } a_j \neq 0.$$

Therefore, we can write (1.7) as

$$A = \sum_{j \geq \nu(A)} a_j \left(\frac{1}{T}\right)^j.$$

## 1.4 The character $E$

Throughout this thesis we will use the additive character $E$ defined for all formal Laurent series (1.7) by

$$E(A) := e^{2\pi i \,\mathrm{tr}(\mathrm{Res}(A))/p}. \tag{1.8}$$

The residue $\mathrm{Res}(A)$ is given by $\mathrm{Res}(A) = a_1$ and tr is the usual trace function $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$.

There are some simple properties, which we will resume in the following lemma.

**Lemma 4** *For the additive character $E : \mathbb{F}_q(T) \to \mathbb{R}$ defined as in (1.8), we have*

1. *For every $A, B \in \mathbb{F}_q((1/T))$,*
$$E(A+B) = E(A)E(B). \tag{1.9}$$
2. *For every $A \in \mathbb{F}_q[T]$ : $E(A) = 1$.*
3. *For $A \in \mathbb{F}_q((1/T))$,*
$$\nu(A) \geq 2 \Rightarrow E(A) = 1.$$
4. *Let $H$ be a non-zero polynomial and $A$, $B$ be arbitrary polynomials. If $A$ and $B$ are congruent modulo $H$, then,*
$$E\left(\frac{A}{H}\right) = E\left(\frac{B}{H}\right). \tag{1.10}$$

*Proof.* The first attribute is trivial and follows immediately from the definition of the character.
Since the coefficient of $1/T$ in the Laurent expansion of $A$ is zero in each of the next two cases, $E(A) = 1$.
If $A \equiv B \bmod H$, then $A = B + RH$ for some $R \in \mathbb{F}_q[T]$. Thus,

$$E\left(\frac{A}{H}\right) = E\left(\frac{B+RH}{H}\right) = E\left(\frac{B}{H} + R\right) = E\left(\frac{B}{H}\right) E(R) = E\left(\frac{B}{H}\right).$$

□

The character $E$ has, of course, many more features, see [17].
Due to their importance for the present thesis, we are going to mention two more properties of the character in the following lemmas. Both proofs pursue the very same concept.

**Lemma 5** *Let $H \neq 0, H, G \in \mathbb{F}_q[T]$, then:*

$$\sum_{\deg R<\deg H} E\left(\frac{G}{H}R\right) = \begin{cases} q^{\deg H} & \text{if } H \text{ divides } G, \\ 0 & \text{otherwise.} \end{cases} \tag{1.11}$$

*Proof.* If $H$ divides $G$, $G/H \in \mathbb{F}_q[T]$ and according to Lemma 4(2): $E\left(\frac{G}{H}R\right) = 1$. Hence,

$$\sum_{\deg R<\deg H} E\left(\frac{G}{H}R\right) = \sum_{\deg R<\deg H} 1 = |H| = q^{\deg H}.$$

Otherwise, $G = G_1H + G_2$ for some polynomials $G_1$ and $G_2$ with $\deg G_2 < \deg H$. Thus, by (1.10),

$$E\left(\frac{G}{H}R\right) = E\left(\frac{G_2}{H}R\right).$$

Moreover, there exists a polynomial $R_0$ with $\deg R_0 < \deg H$ such that

$$E\left(\frac{G_2}{H}R_0\right) \neq 1. \tag{1.12}$$

For example, set $R_0 := T^i$ with $i = \deg H - \deg G_2 - 1 < \deg H$. Then,

$$\begin{aligned} S &:= \sum_{\deg R<\deg H} E\left(\frac{G}{H}R\right) = \sum_{\deg R<\deg H} E\left(\frac{G_2}{H}R\right) \\ &= \sum_{\deg R<\deg H} E\left(\frac{G_2}{H}(R+R_0)\right) = S \cdot E\left(\frac{G_2}{H}R_0\right). \end{aligned}$$

By (1.12), it follows that $S = 0$. □

**Lemma 6** *Suppose that $\nu\left(\frac{B}{C}\right) > 0$ and that $n \geq \nu\left(\frac{B}{C}\right)$, then,*

$$\sum_{A\in P_n} E\left(\frac{B}{C}A\right) = 0. \tag{1.13}$$

*Proof.* Set $m := \nu\left(\frac{B}{C}\right)$, thus, $0 < m \leq n$. Set $A_0 = T^{m-1} \in P_n$. Again,

$$S := \sum_{A\in P_n} E\left(\frac{B}{C}A\right) = \sum_{A\in P_n} E\left(\frac{B}{C}(A+A_0)\right) = S \cdot E\left(\frac{B}{C}A_0\right).$$

Thus, the same argument as above holds. □

# Chapter 2

# Joint Distribution in Residue Classes

In this chapter, we will generalize Kim's result (Theorem 1) to the joint distribution of $Q$-additive functions on polynomials over a finite field. Therefore, we will inter alia use methods similar to those in Kim's article [20] but modified for the use of polynomials.
Afterwards, we will answer several questions which occur in the process of proving our first theorem.

**Theorem 4** *Let $Q_1, Q_2, \ldots, Q_d$ and $M_1, M_2, \ldots, M_d$ 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*

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

*Then, $H$ is a subgroup of $P_{m_1} \times \cdots \times P_{m_d}$ and we have*

$$\lim_{l\to\infty} \frac{1}{q^l} \#\{A \in P_l : f_1(A) \bmod M_1 = R_1, \ldots, f_d(A) \bmod M_d = R_d\}$$
$$= \begin{cases} 1/|H| & \text{if } (R_1, \ldots, R_d) \in H, \\ 0 & \text{if } (R_1, \ldots, R_d) \notin H. \end{cases}$$

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

**Corollary 1** *Let $Q_1, Q_2, \ldots, Q_d$ and $M_1, M_2, \ldots, M_d$ be non-zero polynomials in $\mathbb{F}_q[T]$ with $\deg Q_i = k_i, \deg M_i = m_i$, $m_i$ sufficiently large and*

*$(Q_i, Q_j) = 1$ for $i \neq j$. Moreover, let $f_i : \mathbb{F}_q[T] \to \mathbb{F}_q[T]$ be $Q_i$-additive functions $(1 \leq i \leq d)$. Set*

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

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

$$\lim_{l\to\infty} \frac{1}{q^l} \#\{A \in P_l : f_1(A) = R_1, \ldots, f_d(A) = R_d\}$$
$$= \begin{cases} 1/|H'| & \text{if } (R_1, \ldots, R_d) \in H, \\ 0 & \text{if } (R_1, \ldots, R_d) \notin H. \end{cases}$$

**Remark 5** *In particular, it follows that if there is $A \in \mathbb{F}_q[T]$ with $f_i(A) = R_i$ $(1 \leq i \leq d)$ ($f_i(A) \equiv R_i \bmod M_i$ resp.), then there are infinitely many $A \in \mathbb{F}_q[T]$ with that property.*

## 2.1 Proof of Theorem 4

Let $Q_1, Q_2, \ldots, Q_d$ and $M_1, M_2, \ldots, M_d$ 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 $R = (R_1, \ldots, R_d) \in P_{m_1} \times \cdots \times P_{m_d}$ set

$$g_{R_i}(A) := E\left(\frac{R_i}{M_i} f_i(A)\right) \tag{2.1}$$

and

$$g_R(A) := \prod_{i=1}^{d} g_{R_i}(A) = E\left(\sum_{i=1}^{d} \frac{R_i}{M_i} f_i(A)\right). \tag{2.2}$$

$E$ denotes the additive character defined in (1.8).

With these definitions we can state the following proposition.

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

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

*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 Kim [20]). Theorem 4 is then a simple corollary.

### 2.1.1 Preliminaries

We start with a version of the Weyl-van der Corput inequality.

**Lemma 7** *For each $A \in \mathbb{F}_q[T]$ let $u_A$ be a complex number with $|u_A| = 1$, then,*

$$\left|\frac{1}{q^l}\sum_{A\in P_l} u_A\right|^2 \le \frac{1}{q^r} + \frac{1}{q^r}\sum_{D\in P_r^*}\left|\frac{1}{q^l}\sum_{A\in P_l}\overline{u_A}u_{A+D}\right|. \tag{2.3}$$

*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

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

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

**Lemma 8** *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*

$$f(N+K) - f(N) = f(R+K) - f(R). \tag{2.4}$$

*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

$$\begin{aligned} f(N+K) - f(N) &= f(AQ^t + R + K) - f(AQ^t + R) \\ &= f(A) + f(R+K) - (f(A) + f(R)) \\ &= f(R+K) - f(R). \end{aligned} \tag{2.5}$$

□

### 2.1.2 Some Correlation Estimates

In the next step, we will first prove a correlation estimate (Lemma 9), which will be applied to prove a pre-version of Proposition 1 (Lemma 10).
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, set $g(A) := E\left(\frac{R}{M} f(A)\right)$ for $R \in P_m$.
Unless otherwise specified, $n$ and $l$ are arbitrary integers, and $D \in \mathbb{F}_q[T]$ is 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

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

**Lemma 9** *Suppose that* $|\Phi_k(R)| < 1$, *then,*

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

*Proof.* We start by establishing some recurrence relations for $\Phi_n$ and $\Phi_{l,n}$, namely

$$\Phi_{k+n}(KQ + R) = \Phi_k(R)\Phi_n(K) \tag{2.6}$$

for polynomials $K, R$ with $R \in P_k$. By using the relation $g(AQ + B) = g(A)g(B)$ and splitting the sum which defines $\Phi_{k+n}(KQ + R)$ according to

the residue class of $A$ modulo $Q$, we obtain

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

This proves (2.6). Next, observe that

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

Thus,

$$\Phi_{k+l,k+n} = \Phi_{k,k}\Phi_{l,n} \tag{2.7}$$

and consequently,

$$\Phi_{ik+l,ik+n} = (\Phi_{k,k})^i\,\Phi_{l,n}. \tag{2.8}$$

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, 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 6** *We want to remark that* $|\Phi_k(R)| = 1$ *occurs very rarely. In particular, we have* $|\Phi_k(R)| = 1$ $\forall R$

$\Leftrightarrow$ $\forall A \in P_k : \overline{g(A)}g(A+R)$ is constant (just depending on $R$)

$\Leftrightarrow$ $\forall R, \forall A, B \in P_k : \overline{g(A)}g(A+R) = \overline{g(B)}g(B+R)$

$\Leftrightarrow$ $\forall A, B \in P_k : g(A+B) = g(A)g(B)$.

*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 will prove a pre-version of Proposition 1.

**Lemma 10** *Let* $Q_1, Q_2, \ldots, Q_d \in \mathbb{F}_q[T]$ *be pairwise coprime polynomials,* $M_1, M_2, \ldots, M_d \in \mathbb{F}_q[T]$, *and* $R = (R_1, R_2, \ldots, R_d) \in P_{m_1} \times \cdots \times P_{m_d}$ *so that* $|\Phi_{k_j}(R_j)| < 1$ *for at least one* $j = 1, \ldots, d$. *Then,*

$$\lim_{l \to \infty} \frac{1}{q^l} \sum_{A \in P_l} g_R(A) = 0, \tag{2.9}$$

*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 $r \leq b_j \leq 2r$ with $r = \frac{l}{3d}$. For given $S = (S_1, S_2, \ldots, S_d)$ and $B_1, B_2, \ldots, B_d$, we define

$$N_S := \{A \in P_l : A \equiv S_1 \bmod B_1, \ldots, A \equiv S_d \bmod B_d\}.$$

By the Chinese Remainder Theorem we have for $l \geq \sum_{j=1}^d b_j$

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

Furthermore, set $\mathcal{S} := P_{b_1} \times \cdots \times P_{b_d}$. By Lemma 8 we obtain for $D \in P_r^*$:

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

According to Lemma 7, we obtain for $r \le l$

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

Hölder's inequality results in

$$\begin{aligned}\sum\nolimits_1 &\le q^{r/(d+1)}\prod_{j=1}^{d}\left(\sum_{D\in P_r^*}\left|q^{-b_j}\sum_{S_j\in P_{b_j}}\overline{g_{R_j}(S_j)}g_{R_j}(S_j+D)\right|^{d+1}\right)^{1/(d+1)} \\ &\le q^r\prod_{j=1}^{d}\left(q^{-r}\sum_{D\in P_r^*}\left|q^{-b_j}\sum_{S_j\in P_{b_j}}\overline{g_{R_j}(S_j)}g_{R_j}(S_j+D)\right|^2\right)^{1/(d+1)}.\end{aligned}$$

For some $j$ we have $|\Phi_{k_j}(R_j)| < 1$, so that Lemma 9 is applicable and thus,

$$q^{-r}\sum_{D\in P_r^*}\left|q^{-b_j}\sum_{S_j\in P_{b_j}}\overline{g_{R_j}(S_j)}g_{R_j}(S_j+D)\right|^2 \ll \exp\left(-r\frac{1-|\Phi_{k_j}(R_j)|}{k_j q^{k_j}}\right),$$

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

$$\left|\sum_{A\in P_l} g_R(A)\right|^2 \ll q^{2l-r} + q^{2l}\exp\left(-\frac{r}{d+1}\frac{1-|\Phi_{k_j}(R_j)|}{k_j q^{k_j}}\right)$$

resp.

$$\left|\sum_{A\in P_l} g_R(A)\right| \ll q^{l-\frac{r}{2}} + q^{l}\exp\left(-\frac{r}{2(d+1)}\frac{1-|\Phi_{k_j}(R_j)|}{k_j q^{k_j}}\right).$$

Thus,

$$\begin{aligned}\frac{1}{q^l}\left|\sum_{A\in P_l} g_R(A)\right| &\ll q^{-\frac{r}{2}} + \exp\left(-\frac{r}{2(d+1)}\frac{1-|\Phi_{k_j}(R_j)|}{k_j q^{k_j}}\right) \\ &\le q^{-\frac{r}{2}} + \exp\left(-\frac{l}{6d(d+1)}\frac{1-|\Phi_{k_j}(R_j)|}{k_j q^{k_j}}\right) \\ &\ll \exp(-\eta l) \qquad (2.10)\end{aligned}$$

with $\eta = \frac{1-|\Phi_{k_j}(R_j)|}{6d(d+1)k_j q^{k_j}}$. □

### 2.1.3 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 will divide the proof into several cases.

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

According to Remark 6, we have $|\Phi_{k_j}(R_j)| < 1$. Thus, this case is covered by Lemma 10:

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

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

Due to the additivity property, we also have $g_{R_j}(A)g_{R_j}(B) = g_{R_j}(A+B)$ for all $A, B \in \mathbb{F}_q[T]$ in this case, 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 $A \in \mathbb{F}_q[T]$.

Then,

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

This case is the first alternative in Proposition 1.

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

Let $A = \sum_{i\geq 0} a_i T^i$, then we have

$$g(A) = \prod_{i\geq 0} g(T^i)^{a_i} \neq 1.$$

Consequently, there exists $i \geq 0$ with $g(T^i) \neq 1$. Since $g(T^i)$ is a $p$-th root of unity and $q$ is a power of $p$, we have

$$\sum_{a=0}^{q-1} g(T^i)^a = \frac{1-g(T^i)^q}{1-g(T^i)} = \frac{1-(g(T^i)^p)^{q/p}}{1-g(T^i)} = 0,$$

if $g(T^i) \neq 1$. Otherwise, the sum equals $q$. Thus,

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

Hence, if $l > i$, we always have

$$\begin{aligned}\sum_{A\in P_l} g(A) &= \sum_{a_0=0}^{q-1}\sum_{a_1=0}^{q-1}\cdots\sum_{a_{l-1}=0}^{q-1} g(T^0)^{a_0} g(T^1)^{a_1}\cdots g(T^{l-1})^{a_{l-1}} \\ &= \left(\sum_{a_0=0}^{q-1} g(T^0)^{a_0}\right)\cdots\left(\sum_{a_i=0}^{q-1} g(T^i)^{a_i}\right)\cdots\left(\sum_{a_{l-1}=0}^{q-1} g(T^{l-1})^{a_{l-1}}\right) \\ &= 0. \end{aligned} \tag{2.11}$$

This completes the proof of Proposition 1. □

### 2.1.4 Completion of the Proof of Theorem 4

Before we start, we will define two (additive) groups:

$$G := \{R = (R_1, R_2, \ldots, R_d) \in \mathsf{X}_{i=1}^d P_{m_i} : \forall\ A \in \mathbb{F}_q[T]\ g_R(A) = 1\} \tag{2.12}$$

and

$$H_0 := \left\{S = (S_1, \ldots, S_d) \in \mathsf{X}_{i=1}^d P_{m_i} : \forall R \in G:\ E\left(\sum_{i=1}^d -\frac{S_i R_i}{M_i}\right) = 1\right\}.$$

**Lemma 11** *Let $G$ be defined as in (2.12), then, $G$ is a subgroup of $\mathsf{X}_{i=1}^d P_{m_i}$.*

*Proof.* Let $R = (R_1, R_2, \ldots, R_d) \in G, S = (S_1, S_2, \ldots, S_d) \in G$, then

$$\begin{aligned} g_R(A) = E\left(\frac{R_1}{M_1} f_1(A) + \frac{R_2}{M_2} f_2(A) + \cdots + \frac{R_d}{M_d} f_d(A)\right) &\equiv 1, \\ g_S(A) = E\left(\frac{S_1}{M_1} f_1(A) + \frac{S_2}{M_2} f_2(A) + \cdots + \frac{S_d}{M_d} f_d(A)\right) &\equiv 1. \end{aligned}$$

Thus,

$$E\left(\sum_{i=1}^d \frac{R_i}{M_i} f_i(A)\right) E\left(\sum_{i=1}^d \frac{S_i}{M_i} f_i(A)\right) = E\left(\sum_{i=1}^d \frac{R_i + S_i}{M_i} f_i(A)\right) \equiv 1,$$

and, $R + S = (R_1 + S_1, R_2 + S_2, \ldots, R_d + S_d) \in G$. □

For $S = (S_1, S_2, \ldots, S_d) \in \mathsf{X}_{i=1}^d P_{m_i}$, let the function $F(S)$ be defined as

$$F(S) := \frac{1}{|G|}\sum_{R\in G} E\left(\sum_{i=1}^d -\frac{S_i R_i}{M_i}\right). \tag{2.13}$$

By applying Proposition 1, we directly get

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

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

**Lemma 12** *We have*

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

*Furthermore,* $|G| \cdot |H_0| = |\mathsf{X}_{i=1}^d P_{m_i}| = q^{\sum_{j=1}^d m_j}$.

*Proof.* It is clear that $F(S) = 1$ if $S \in H_0$.
Now we suppose that $S \notin H_0$. Then, there exists $R^0 = (R_1^0, R_2^0, \ldots, R_d^0) \in G$ 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 $S \in \mathsf{X}_{i=1}^d P_{m_i}$, it follows that $|G| \cdot |H_0| = |\mathsf{X}_{i=1}^d P_{m_i}|$. □

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

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

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

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

if $S = (S_1, \ldots, S_d) \notin H_0$. The final step of the proof of Theorem 4 is to show that

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

In fact, if $S \in H_0$, then we trivially have $S \in H$.
Conversely, if $S \in H$, then there exists a polynomial $A \in \mathbb{F}_q[T]$ with $f_1(A) \equiv S_1 \bmod M_1, \ldots, f_d(A) \equiv S_d \bmod M_d$. 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 4.

**Remark 7** *Unfortunately, a finite characterization as Kim gave it in his article [20] was not possible in our case. We could find no way of defining an admissible d-tuple so that H turns out to be just the set of all admissible d-tuples. A reason for this fact is given in subsection 2.2.2.*

## 2.2 Further investigations

The investigations we have made so far raise some interesting questions, which we are going to study now. Actually, we will focus on several questions in connection with the sum-of-digits function $s_Q$. Note that we launch the following notation: instead of $s_{Q_i}$ we will simply write $s_i$.

At the beginning of subsection 2.2.1, we will tackle the question, when $g = g_R = g_{R_1} g_{R_2} = 1$. Trying to find a solution, we will make investigations concerning the additivity of the sum-of-digits function $s_i$, which turns out to be the actual focus of our first subsection.

In subsection 2.2.2 we are going to have a closer look at the group $H$ which appeared in the proof of Theorem 4. First, we will choose two bases $Q_1$ and $Q_2$, and determine the elements of $H$. Then, we will give a reason why Kim's finite characterization of $H$ does not work in our case.

### 2.2.1 Additivity of the sum-of-digits function

In the proof of Theorem 4 we applied Proposition 1, which played a decisive role in the whole proof. We can shorten this proposition to

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

However, no clue can be found anywhere as to which alternative – 0 or 1 – actually applies. For the sake of brevity we will focus on $d = 2$ and assume that

$$g = g_R = g_{R_1} g_{R_2} = 1. \tag{2.14}$$

Generally, there are two possible cases in which (2.14) is valid. First, $g_{R_1}$ as well as $g_{R_2}$ are identically 1 for all $A \in \mathbb{F}_q[T]$.

$$\begin{aligned} g_{R_1}(A) = E\left(\frac{R_1}{Q_1} s_1(A)\right) \equiv 1 \quad &\Leftrightarrow \quad \forall A \in P_{k_1} : g_{R_1}(A) = 1 \\ &\Leftrightarrow \quad \forall A \in P_{k_1} : \operatorname{Res}\left(\frac{R_1 s_1(A)}{Q_1}\right) = 0. \end{aligned}$$

If we want to examine whether $g_{R_1}(A)$ actually is identically 1, we only have to make a finite number of tests.

For the sum-of-digits function it is trivial that $s_1(A) = A$ for all $A \in P_{k_1}$ independent of the base $Q_1$. It turns out that for the sum-of-digits function $g(A)$ is not constant equal to 1.

**Lemma 13** *Let* $r_1 := \deg R_1$, $r_1 \geq 0$, *then*

$$\operatorname{Res}\left(\frac{R_1}{Q_1} T^{k_1 - r_1 - 1}\right) \neq 0.$$

*Proof.* Since $k_1 = \deg Q_1$, we have $Q_1^{-1} = a_0 T^{-k_1} + a_1 T^{-(k_1+1)} + \ldots$

$$\begin{aligned} \Rightarrow \quad & \frac{R_1}{Q_1} = b_0 \frac{T^{r_1}}{T^{k_1}} + \cdots \qquad (b_0 \in \mathbb{F}_q \setminus \{0\}) \\ \Rightarrow \quad & \frac{R_1}{Q_1} T^{k_1 - r_1 - 1} = b_0 \frac{T^{r_1} T^{k_1 - r_1 - 1}}{T^{k_1}} + \cdots = \frac{b_0}{T} + \cdots \end{aligned}$$

Thus, we obtain

$$\operatorname{Res}\left(\frac{R_1}{Q_1}T^{k_1-r_1-1}\right) \neq 0.$$

□

According to Lemma 13 we have

$$g_{R_1}(A) \neq 1 \text{ for all } A \in I,$$

$I = \{A \in \mathbb{F}_q[T] : s_1(A) = T^{k_1-r_1-1}\}$. Since $T^{k_1-r_1-1} \in P_{k_1}$, it follows that $T^{k_1-r_1-1} \in I$, which means $I \neq \emptyset$ and consequently, $g_{R_1} \not\equiv 1$.

Thus, our first possibility never occurs for the sum-of-digits function, and we can concentrate on the second scenario: $g_{R_1}(A) \neq 1$ but $g(A) \equiv 1$. So, $g_{R_2}(A) = \frac{1}{g_{R_1}(A)}$, i.e. $g_{R_1}(A)$ and $g_{R_2}(A)$ are $Q_1$- as well as $Q_2$-multiplicative:

$$\begin{aligned} g_{R_1}(AQ_1+B) &= g_{R_1}(A)g_{R_1}(B), \quad & g_{R_2}(EQ_1+F) &= g_{R_2}(E)g_{R_2}(F), \\ g_{R_1}(CQ_2+D) &= g_{R_1}(C)g_{R_1}(D), \quad & g_{R_2}(GQ_2+H) &= g_{R_2}(G)g_{R_2}(H), \end{aligned}$$

for $\deg B, \deg F < k_1$ and $\deg D, \deg H < k_2$.

**Lemma 14** *Let $f_1$ be a $Q_1$- and $Q_2$-additive function, and set $g_{R_1}(A) = E\left(\frac{R_1}{Q_1}f_1(A)\right)$. Then, $g_{R_1}$ is $Q_1$- and $Q_2$-multiplicative.*

*Proof.* Let $f_1$ be $Q_1$- and $Q_2$-additive. Thus,

$$\begin{aligned} f_1(AQ_1+B) &= f_1(A)+f_1(B), \\ f_1(CQ_2+D) &= f_1(C)+f_1(D). \end{aligned}$$

Since (1.9), the assertion holds for $g_{R_1}(A) = E\left(\frac{R_1}{Q_1}f_1(A)\right)$.

□

Hence, if we can show that $s_1$ and $s_2$ are both $Q_1$- and $Q_2$-additive, then we get by Lemma 14 that $g_{R_1}(A)$ and $g_{R_2}(A)$ are $Q_1$- resp. $Q_2$-multiplicative, a condition for the occurrence of our second scenario. This is exactly what we want to achieve by an appropriate choice of $Q_1$ and $Q_2$.
We assume w.l.o.g. that $\deg Q_2 \geq \deg Q_1$ and try to choose $Q_2$ in such a way that $s_1$ will be $Q_2$-additive ($s_1$ is always $Q_1$-additive by definition).

Before studying the general case, we will focus on a special case where $\deg Q_2 = \deg Q_1$. Therefore, we can state a base $Q_2$ independent of a specific base $Q_1$ so that $s_1$ is $Q_1$- and $Q_2$-additive.

**Lemma 15** *If $k_1 = k_2$, then there is just one possible choice of $Q_2$ so that $s_1$ can be $Q_2$-additive: $Q_2 = aQ_1 + (1-a)$ for some $a \in \mathbb{F}_q \setminus \{0,1\}$.*

*Proof.* Since $k_1 = k_2$, we can write $Q_2 = aQ_1 + B$ for some $a \in \mathbb{F}_q, B \in P_{k_1}$. Suppose that $s_1$ is $Q_2$-additive. $AQ_2 = aAQ_1 + AB$, thus,

$$s_1(AQ_2) = s_1(aAQ_1) + s_1(AB) = as_1(A) + s_1(AB)$$

equals $s_1(A)$ by assumption. Hence,

$$(a-1)s_1(A) + s_1(AB) = 0$$

for all $A \in \mathbb{F}_q[T]$.
If $\deg(B) = 0$, then $B = 1 - a \in \mathbb{F}_q$. Otherwise choose $A = c \in \mathbb{F}_q$, if $\deg(B) > 0$, thus, $\underbrace{(a-1)\cdot c}_{\in \mathbb{F}_q} = \underbrace{-c \cdot B}_{\notin \mathbb{F}_q}$, which contradicts our assumption. □

**Remark 8** *Actually, we have only proved the possibility of $Q_1$- and $Q_2$-additivity for the bases $Q_1$ and $Q_2$ as chosen in Lemma 15.*
*It will turn out later on, that for this special choice of $Q_1$ and $Q_2$ both sum-of-digits functions truly have the desired property (see Example 2).*

We will come across these two special bases again several times afterwards. Before we do so, we are going to focus on the general case, where there is no restriction concerning the degrees of the bases.

We assume w.l.o.g. that $\deg Q_2 \geq \deg Q_1$, and try to establish a criterion (Lemma 18) for $Q_1$ and $Q_2$ so that $s_1$ is definitely both $Q_1$- and $Q_2$-additive.

**Lemma 16** *Let $Q_1$ and $Q_2$ be arbitrary polynomials, w.l.o.g. $k_2 \geq k_1$. Then, we consider the $Q_1$-ary expansion of $Q_2$,*

$$Q_2 = \sum_{j=0}^{n} A_j Q_1^j, \tag{2.15}$$

*with $A_j \in P_{k_1}$, $A_n \neq 0$ and not all $A_j = 0$ for $0 \leq j < n$. Furthermore, we can write $Q_2$ as*

$$Q_2 = \sum_{j=0}^{n} B_j (Q_1 - 1)^j, \tag{2.16}$$

*with $B_j \in P_{k_1}$, $B_n \neq 0$ and not all $B_j = 0$ for $0 \leq j < n$. Then, we have the following correlations between $A_k$ and $B_j$:*

$$A_k = \sum_{j=k}^{n} (-1)^{j-k} \binom{j}{k} B_j, \tag{2.17}$$

$$B_k = \sum_{j=k}^{n} \binom{j}{k} A_j. \tag{2.18}$$

*In particular, we have $A_n = B_n$.*

*Proof.* We start with (2.16), and obtain

$$\begin{aligned}
\sum_{j=0}^{n} B_j (Q_1 - 1)^j &= \sum_{j=0}^{n} B_j \sum_{k=0}^{j} (-1)^{j-k} \binom{j}{k} Q_1^k \\
&= \sum_{j=0}^{n} B_j \sum_{k=0}^{n} (-1)^{j-k} \binom{j}{k} Q_1^k \\
&= \sum_{k=0}^{n} \sum_{j=0}^{n} (-1)^{j-k} \binom{j}{k} B_j Q_1^k \\
&= \sum_{k=0}^{n} \underbrace{\left( \sum_{j=k}^{n} (-1)^{j-k} \binom{j}{k} B_j \right)}_{=A_k} Q_1^k.
\end{aligned}$$

Thus, (2.17) is valid. Due to (2.15) we get

$$\begin{aligned}
\sum_{j=0}^{n} A_j Q_1^j &= \sum_{j=0}^{n} A_j (Q_1 - 1 + 1)^j \\
&= \sum_{j=0}^{n} A_j \sum_{k=0}^{j} \binom{j}{k} (Q_1 - 1)^k \\
&= \sum_{j=0}^{n} A_j \sum_{k=0}^{n} \binom{j}{k} (Q_1 - 1)^k \\
&= \sum_{k=0}^{n} \underbrace{\left( \sum_{j=k}^{n} \binom{j}{k} A_j \right)}_{=B_k} (Q_1 - 1)^k,
\end{aligned}$$

and therewith we have proved (2.18). Substituting $k = n$ in (2.17) resp. (2.18) we finally obtain $A_n = B_n$, as stated above. □

The following lemma is rather easy.

**Lemma 17** *Using the same notation as in the previous lemma we have*

$$B_0 = 1 \Leftrightarrow Q_1 - 1 \mid Q_2 - 1. \tag{2.19}$$

*Proof.* Due to (2.16), $Q_1 - 1 \mid Q_2 - B_0$. Thus, if $B_0 = 1$, then, $Q_1 - 1 \mid Q_2 - 1$. Accordingly, if $Q_2 \equiv 1 \bmod Q_1 - 1$, then it immediately follows that $B_0 \equiv 1 \bmod Q_1 - 1$. Since $B_0 \in P_{k_1}$, we have $B_0 = 1$. □

Finally, we can prove the following criterion:

**Lemma 18** *Let $Q_1$ and $Q_2$ be two arbitrary bases,* $\deg(Q_2) \geq \deg(Q_1)$, *with expansion (2.15). Then,*

$$Q_1 - 1 \mid Q_2 - 1 \Leftrightarrow s_1 \text{ is } Q_2\text{-additive.} \tag{2.20}$$

*Proof.* Let $s_1$ be $Q_2$-additive. Thus,

$$\begin{aligned} s_1(AQ_1 + B) &= s_1(A) + s_1(B), \\ s_1(CQ_2 + D) &= s_1(C) + s_1(D), \end{aligned}$$

for all $A, C \in \mathbb{F}_q[T]$, $B \in P_{k_1}$ and $D \in P_{k_2}$. Choose $C = 1, D = 0$. Hence, by (2.15),

$$s_1\left(\sum_{j=0}^{n} A_j Q_1^j\right) = \sum_{j=0}^{n} A_j = s_1(1) = 1.$$

Since $\sum_{j=0}^{n} A_j = B_0$ by (2.18), we get $B_0 = 1$, and thus, $Q_1 - 1 \mid Q_2 - 1$. Suppose $Q_1 - 1 \mid Q_2 - 1$. As is normal for $Q_2$-additivity, it suffices to show $s_1(BQ_2^l) = s_1(B)$.

$$s_1(BQ_2) = s_1\left(B\sum_{j=0}^{n} A_j Q_1^j\right) = s_1\left(B\sum_{j=0}^{n} A_j\right).$$

By Lemma 17 resp. by (2.18) we have

$$1 = B_0 = \sum_{j=0}^{n} A_j,$$

thus, $s_1(BQ_2) = s_1(B)$. Analogously,

$$s_1(BQ_2^2) = s_1\left(B\sum_{j=0}^{n} A_j Q_1^j Q_2\right) = s_1\left(B\sum_{j=0}^{n} A_j Q_1^j\right) = s_1(B).$$

Finally, by complete induction, we obtain that $s_1$ is $Q_2$-additive. □

Due to this criterion, we can give the following example of two polynomials $Q_1$ and $Q_2$, $\deg Q_2 > \deg Q_1$, so that $s_1$ is $Q_1$- and $Q_2$-additive.

**Example 1** *Let $Q_1 = x + 1$ and $Q_2 = x^2 + x + 1$ be polynomials in $\mathbb{F}_q[x]$. Then, we have $Q_1 - 1 = x \mid x(x+1) = x^2 + x = Q_2 - 1$, and thus, by Lemma 18 we obtain that $s_1$ is $Q_2$-additive.*

A very simple case where $s_1$ is $Q_2$-additive is, of course, if $s_1 \equiv s_2$. Due to Lemma 18 we get the following interesting equivalence:

**Lemma 19** *Let $Q_1$ and $Q_2$ be arbitrary bases, w.l.o.g. $k_2 \geq k_1$. Then, $s_1 \equiv s_2$ if and only if $Q_1 - 1 \mid Q_2 - 1$ and $Q_2 - 1 \mid Q_1 - 1$, i.e. $k_1 = k_2$ and $Q_1 - 1 = a(Q_2 - 1)$ for some $a \in \mathbb{F}_q \setminus \{0\}$.*

*Proof.* If $s_1 \equiv s_2$, then, $s_1$ is $Q_2$-additive and $s_2$ is $Q_1$-additive. Due to the above criterion we get $Q_1 - 1 \mid Q_2 - 1$ resp. $Q_2 - 1 \mid Q_1 - 1$. All in all we get $Q_1 - 1 = a(Q_2 - 1)$ for some constant $a \neq 0$, and especially $k_1 = k_2$, as stated above.
Conversely, let $Q_1 - 1 = a(Q_2 - 1)$ for some positive $a \in \mathbb{F}_q$. If $a = 1$, we have $Q_1 = Q_2$, and the result follows immediately. Thus, w.l.o.g. $Q_1 = aQ_2 + (1 - a)$, with $a \geq 2$, and

$$Q_1^j = (aQ_2 + (1-a))^j = \sum_{i=1}^{j} \binom{j}{i} a^i (1-a)^{j-i} Q_2^i.$$

For any arbitrary $B$ we have

$$B = \sum_{j=0}^{k} B_j Q_1^j = \sum_{j=0}^{k} B_j \sum_{i=1}^{j} \binom{j}{i} a^i (1-a)^{j-i} Q_2^i$$

for some polynomials $B_j \in P_{k_1}$. Hence, we get

$$s_2(B) = \sum_{j=0}^{k} s_2\left(B_j \sum_{i=0}^{j} \binom{j}{i} a^i (1-a)^{j-i}\right) = \sum_{j=0}^{k} s_2(B_j).$$

Since $B_j \in P_{k_2} = P_{k_1}$, we have

$$s_2(B) = \sum_{j=0}^{k} s_2(B_j) = \sum_{j=0}^{k} B_j = \sum_{j=0}^{k} s_1(B_j) = s_1(B).$$

Due to the arbitrary choice of $B$ we have $s_1(B) = s_2(B)$ for all $B \in \mathbb{F}_q[T]$, and thus, $s_1 \equiv s_2$. □

Due to the importance of these two bases $Q_1$ and $Q_2$, we want to mention them once more.

**Example 2** *Let $Q_2 = aQ_1 + (1-a)$ with $a \in \mathbb{F}_q \setminus \{0,1\}, Q_1 \in \mathbb{F}_q[T] \setminus \{0\}$. Then, we have $k_1 = k_2$ and $Q_1 - 1 \mid Q_2 - 1$ as well as $Q_2 - 1 \mid Q_1 - 1$. Therefore, by Lemma 19, $s_1 = s_2$ and thus, $s_1$ and $s_2$ are both $Q_1$- and $Q_2$-additive.*
*As already mentioned above, this is the only option if $Q_1$ and $Q_2$ are of equal degree so that the corresponding sum-of-digits functions are both $Q_1$- and $Q_2$-additive.*

### 2.2.2 The properties of the group $H$

After these extensive studies on the additivity of $s_i$, we turn to another interesting problem. In the proof of Theorem 1 two unnatural Groups $G$ and $H$ appeared, on which we want to focus now.

We take the previously studied example $Q_2 = aQ_1 + (1-a)$ up again and first have a look at $G$. More specifically, we ask if $G$ is trivial or not, and if there is $(R_1, R_2) \neq (0,0)$ so that

$$E\left(\frac{R_1}{Q_1}s_1(A) + \frac{R_2}{Q_2}s_2(A)\right) = E\left(\left(\frac{R_1}{Q_1} + \frac{R_2}{Q_2}\right)A\right) \equiv 1$$

for $A \in P_{k_1} = P_{k_2}$. Since $(Q_1, Q_2) = 1$ by assumption, there are $R_1, R_2 \in P_{k_1}$ satisfying $R_1Q_2 + R_2Q_1 \equiv 1$.

$$\begin{aligned}
\frac{R_1}{Q_1} + \frac{R_2}{Q_2} &= \frac{1}{Q_1Q_2} = \frac{c_0}{T^{2k_1}} + \frac{c_1}{T^{2k_1+1}} + \cdots \\
&\Rightarrow \frac{A}{Q_1Q_2} = \frac{c_1'}{T^{k_1+1}} + \frac{c_2'}{T^{k_1+2}} + \cdots \\
&\Rightarrow \operatorname{Res}\left(\frac{A}{Q_1Q_2}\right) \equiv 0 \text{ since } k_1 > 0 \\
&\Rightarrow E\left(\frac{A}{Q_1Q_2}\right) = g_{R_1,R_2}(A) \equiv 1.
\end{aligned}$$

This consideration implies that $G \neq \{(0,0)\}$, which means that $G$ is not trivial, and hence, $H \neq P_{k_1} \times P_{k_2}$.
We can become more explicit, if we consider Lemma 19. If $Q_1$ and $Q_2$ are chosen in this way, we have $s_1(A) = s_2(A)\ \forall A \in \mathbb{F}_q[T]$. Therefore, we obtain

$$H = \{(A, A) \mid A \in P_{k_1}\}. \tag{2.21}$$

Due to Lemma 12, we get $|H| = |P_{k_1}| = q^{k_1}$ and $|G| = q^{k_1}$.

Let us now turn back to Remark 7 and give a reason why Kim's characterization does not work in our case.
First, we repeat the two descriptions of $H$ which we already have, and transform Kim's group to polynomials.
As mentioned above, the two following groups are identical:

$$H = \left\{ S = (S_1, S_2, \ldots, S_d) \in \mathsf{X}_{i=1}^{d} P_{m_i} : \ \forall R \in G : \ E\left( \sum_{i=1}^{d} -\frac{S_i R_i}{M_i} \right) = 1 \right\},$$
$$H_0 = \{ (f_1(A) \bmod M_1, f_2(A) \bmod M_2, \ldots, f_d(A) \bmod M_d) : A \in \mathbb{F}_q[T] \}.$$

Analogy of Kim's description:

For $j = 1, \ldots, d$ define:

$$F_j := f_j(1), \tag{2.22}$$
$$D_j := \gcd\left(M_j, (Q_j - 1)F_j, f_j(R) - RF_j \ (R \in P_{k_j})\right), \tag{2.23}$$

where $f_j, M_j, Q_j$ and $R = (R_1, \ldots, R_d)$ are defined as usual. Furthermore, set $A = (A_1, \ldots, A_d) \in \mathbb{F}_q[T]^d$, $F = (F_1, \ldots, F_d)$ and $D = (D_1, \ldots, D_d)$. A $d$-tuple $A$ of polynomials is called „admissible" with respect to the $d$-tuples $Q, M$ and $f$, if the system of congruences

$$FN \equiv A \bmod D$$

has a solution $N \in \mathbb{F}_q[T]$. We write

$$\widetilde{H} := \{ A = (A_1, \ldots, A_d) : \deg A_j < m_j, A \text{ admissible} \}.$$

Before we study the relationship of $\widetilde{H}$ and $H$ resp. $H_0$, we have to prove the following Lemma according to an analogue to Kim.

**Lemma 20** *Let $Q$ and $M$ be polynomials with positive degrees $k := \deg Q$, $m := \deg M$, and let $f$ be a completely $Q$-additive function. Let $F$ and $D$ be defined in the same way as the quantities $F_j$ and $D_j$ in (2.22) and (2.23) with respect to $Q, M$ and $f$, which means that*

$$F := f(1),$$
$$D := \gcd\left(M, (Q-1)F, f(R) - RF(R \in P_k)\right).$$

*Then, for an arbitrary $N \in \mathbb{F}_q[T]$ we have*

$$f(N) \equiv NF \bmod D.$$

*Proof.* Let $N \in \mathbb{F}_q[T]$ be a polynomial with the $Q$-ary expansion $N = \sum_{i\geq 0} R_i Q^i$ where $R_i \in P_k$. The complete $Q$-additivity of $f$ implies

$$f(N) = \sum_{i=0}^{\infty} f(R_i). \tag{2.24}$$

On the one hand, we have

$$\sum_{i\geq 0} f(R_i) \equiv \sum_{i\geq 0} R_i F \bmod D \tag{2.25}$$

as $f(R) \equiv RF \bmod D$ for all $R \in P_k$ by definition of $D$. On the other hand, since $Q \equiv 1 \bmod Q-1$, we also obtain

$$N = \sum_{i\geq 0} R_i Q^i \equiv \sum_{i\geq 0} R_i \bmod Q-1,$$

and therefore,

$$N \cdot F \equiv \sum_{i\geq 0} R_i F \bmod D, \tag{2.26}$$

since $D \mid (Q-1)F$. Combining these congruences, we obtain

$$f(N) \overset{(2.24)}{=} \sum_{i\geq 0} f(R_i) \overset{(2.25)}{\equiv} \sum_{i\geq 0} R_i F \overset{(2.26)}{\equiv} N \cdot F \bmod D.$$

□

Thus, the following inclusion is trivial:

**Lemma 21** *With the common definitions of $H_0$ and $\widetilde{H}$ we have*

$$H_0 \subseteq \widetilde{H}.$$

*Proof.* Let $A \in H_0$. Then, by definition of $H_0$, we obtain the existence of a polynomial $N$ satisfying $f_j(N) \equiv A_j \bmod M_j$. Since $M_j \mid D_j$, it follows that $f_j(N) \equiv A_j \bmod D_j$, and therefore, by Lemma 20, we have: $FN \equiv A \bmod D$ $\Rightarrow A \in \widetilde{H}$. □

Unfortunately, the other inclusion is not generally true. We have already mentioned a counter-example where $\widetilde{H} \not\subseteq H_0$. It is our well-known Example 2. We consider the sum-of-digits functions with respect to the two bases, $M_j = Q_j$.

Determining $F_j$ and $D_j$, we obtain $F_j = D_j = 1$ for all $j = 1, \ldots, d$. Therefore, $\widetilde{H} = P_{k_1} \times P_{k_2}$.
However, this contradicts (2.21), whereby

$$H = \{(A, A) \mid A \in P_{k_1}\}.$$

So, $\widetilde{H}$ cannot generally be equal to or a subset of $H_0$ resp. $H$, and Kim's idea for a finite criterion to define $H$ does not work in our case.

# Chapter 3

# Two Central Limit Theorems

In this chapter, we successively generalize Theorem 2 by Bassily and Kátai (into Theorem 5) as well as Theorem 3 by Drmota (into Theorem 6) for $Q$-additive functions on polynomials over a finite field.
Whereas our Theorem 5 deals with only one $Q$-additive function $f$, Theorem 6 covers the joint distribution of two $Q_j$-additive functions $f_j$ for coprime bases $Q_j$. For both proofs we will use the same tool, namely again exponential sums; this time, however, in combination with a method of moments. The latter will be explained later on.

## 3.1 Generalization of Bassily and Kátai

We start with Bassily and Kátai's [1] central limit theorem, our Theorem 2. For polynomials over a finite field we obtain the following theorem.

**Theorem 5** *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*

$$\mu_g := \frac{1}{q^k} \sum_{A \in P_k} g(A), \qquad \sigma_g^2 := \frac{1}{q^k} \sum_{A \in P_k} g(A)^2 - \mu^2. \tag{3.1}$$

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

$$\frac{1}{q^n} \# \left\{ A \in P_n : \frac{g(P(A)) - \frac{nr}{k}\mu_g}{\sqrt{\frac{nr}{k}\sigma_g^2}} \leq x \right\} \to \Phi(x) \tag{3.2}$$

*and*

$$\frac{1}{|I_n|} \# \left\{ A \in I_n : \frac{g(P(A)) - \frac{nr}{k}\mu_g}{\sqrt{\frac{nr}{k}\sigma_g^2}} \leq x \right\} \to \Phi(x), \tag{3.3}$$

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

Before proving this Theorem, we need some preliminaries again, which we are going to introduce now.
First of all, we need a method to extract a digit $D_{Q,j}(A)$ of an arbitrary polynomial $A \in \mathbb{F}_q[T]$. The next lemma shows how we can do this with the help of exponential sums.

To begin with, consider the $Q$-ary expansion of an arbitrary polynomial $A \in \mathbb{F}_q[T]$ for any fixed polynomial $Q \in \mathbb{F}_q[T]$:

$$A = \sum_{j \geq 0} D_{Q,j} Q^j$$

with $D_{Q,j} \in P_k$. Furthermore, let $H \in P_k$ and

$$\frac{1}{Q} = \frac{c_0}{T^k} + \frac{c_1}{T^{k+1}} + \frac{c_2}{T^{k+2}} + \cdots$$

for some $c_i \in \mathbb{F}_q$. Therefore, we gradually get

$$\begin{aligned}
A &= D_{Q,0} + D_{Q,1}Q + \cdots + D_{Q,j-1}Q^{j-1} + D_{Q,j}Q^j + D_{Q,j+1}Q^{j+1} + \cdots, \\
\frac{A}{Q^{j+1}} &= \frac{D_{Q,0}}{Q^{j+1}} + \frac{D_{Q,1}}{Q^j} + \cdots + \frac{D_{Q,j-1}}{Q^2} + \frac{D_{Q,j}}{Q} + D_{Q,j+1} + \cdots, \\
\frac{AH}{Q^{j+1}} &= \frac{D_{Q,0}H}{Q^{j+1}} + \frac{D_{Q,1}H}{Q^j} + \cdots + \frac{D_{Q,j-1}H}{Q^2} + \frac{D_{Q,j}H}{Q} + D_{Q,j+1}H + \cdots.
\end{aligned}$$

Moreover, we have

$$\begin{aligned}
\deg D_{Q,i}H \leq 2(k-1) \quad &\Rightarrow \quad \operatorname{Res}\left(\frac{D_{Q,0}H}{Q^{j+1}}\right) = \cdots = \operatorname{Res}\left(\frac{D_{Q,j-1}H}{Q^2}\right) = 0 \\
&\Rightarrow \quad \operatorname{Res}\left(\frac{AH}{Q^{j+1}}\right) = \operatorname{Res}\left(\frac{D_{Q,j}H}{Q}\right) \\
&\Rightarrow \quad E\left(\frac{AH}{Q^{j+1}}\right) = E\left(\frac{D_{Q,j}H}{Q}\right).
\end{aligned}$$

Together with the ideas of the previous chapter on Kim's Theorem, the method is obvious:

**Lemma 22** *Suppose that $Q \in \mathbb{F}_q[T]$ with $\deg Q = k \geq 1$. For $D, H \in P_k$ 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

$$A = \sum_{j \geq 0} D_{Q,j}(A) Q^j \quad \text{with} \quad D_{Q,j}(A) \in P_k. \tag{3.4}$$

It follows that

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

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

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

□

What we have found is a very simple method for extracting the digit $D_{Q,j}(A)$. Therewith, it is possible to determine the number of polynomials whose $j$-th digit of $P(A)$ is equal to a given $\varepsilon \in P_k$. $P(A)$ is an arbitrary polynomial, $P(A) \in \mathbb{F}_q[T]$. The following studies will finally yield our first result concerning this topic, Lemma 26.

$$\begin{aligned}
&\frac{1}{q^n} \# \{A \in P_n | D_{Q,j}(P(A)) = \varepsilon\} \\
&= \frac{1}{q^n} \sum_{A \in P_n} \sum_{H \in P_k} c_{H,\varepsilon} E\left(\frac{P(A)}{Q^{j+1}} H\right) \\
&= \sum_{H \in P_k} c_{H,\varepsilon} \frac{1}{q^n} \sum_{A \in P_n} E\left(\frac{P(A)}{Q^{j+1}} H\right) \\
&= \frac{1}{q^k} + \underbrace{\sum_{H \in P_k^*} c_{H,\varepsilon} \frac{1}{q^n} \sum_{A \in P_n} E\left(\frac{P(A)}{Q^{j+1}} H\right)}_{\text{S:=}}.
\end{aligned} \tag{3.5}$$

**Remark 9** *For the constants $c_{H,D}$ we have*

$$c_{0,\varepsilon} = \frac{1}{q^k} \qquad \text{and} \qquad |c_{H,\varepsilon}| = \frac{1}{q^k}.$$

*In the next section, we will have to write $c_{Q,H,D}$ instead of $c_{H,D}$, because there is more than one base involved. As long as there is no risk of confusion, the parameter $Q$ will be omitted.*

Thus, it becomes necessary to study sums of the form $S$. So, we need the following estimate of [3], but slightly adapted for our purposes.

**Lemma 23** *Let $n \geq 0$ be an arbitrary integer, then,*

$$\frac{1}{q^n}\left|\sum_{A\in P_n} E\left(\frac{G}{H}A^k\right)\right| \ll n^{2^{k-2}} \max\left(|H|^{-2^{-k}}, q^{-n2^{-k}}, |H|^{2^{-k}} q^{-nk2^{-k}}\right).$$

*Proof.* For proof see [3]. □

Lemmas 24 and 33 are the variations we require. As an example, we are going to prove Lemma 24, which takes up Car's ideas.

**Lemma 24** *Suppose that $Q \in \mathbb{F}_q[T]$, $\deg Q = k \geq 1$ and that $P \in \mathbb{F}_q[T]$ is a polynomial with $\deg P = r \geq 1$. Then,*

$$\frac{1}{q^n}\left|\sum_{A\in P_n} E\left(\frac{H}{Q^{j+1}}P(A)\right)\right| \ll n^{2^{r-2}} \max\left(q^{-(j+1)k2^{-r}}, q^{-n2^{-r}}, q^{(j+1)k2^{-r}-nr2^{-r}}\right). \tag{3.6}$$

In order to prove this estimate we first need the following lemma.

**Lemma 25** *Let $\mathrm{d} : \mathbb{F}_q[T] \to \mathbb{N}$ denote the number of primary divisors of a polynomial, and set $\mathrm{d}(0) := 1$. Then, for $j \geq 0$ and $n > 0$ we have*

$$\sum_{A\in P_n} \mathrm{d}(A)^j \leq n^{2^j-1} q^n. \tag{3.7}$$

*Proof.* We will use the following easily shown property of the function d. Let $A, B$ be some arbitrary polynomials, then,

$$\mathrm{d}(AB) \leq \mathrm{d}(A)\,\mathrm{d}(B).$$

If $A$ and $B$ are coprime, we have $\mathrm{d}(AB) = \mathrm{d}(A)\,\mathrm{d}(B)$. Therewith, the lemma can be shown by complete induction.
Let $j = 0$, then,

$$\sum_{A\in P_n} 1 = q^n = n^0 q^n,$$

and therefore, (3.7) is true for $j = 0$.
Since there is a related idea to the below induction step, we will also study $j = 1$:

$$\sum_{A\in P_n} \mathrm{d}(A) \stackrel{?}{\leq} nq^n.$$

Thus, we will write the number of divisors of $A$ as the number of pairs $(B, C)$ with $BC = A$.

$$\begin{aligned}\sum_{A\in P_n} \mathrm{d}(A) &= \sum_{A\in P_n} \sum_{\substack{(B,C),\\ BC=A}} 1 = \sum_{B\in P_n'} \sum_{\substack{C\in\mathbb{F}_q[T]\\ \deg(BC)<n}} 1 \\ &= \sum_{B\in P_n'} q^{n-\deg(B)} = q^n \sum_{B\in P_n'} q^{-\deg(B)} \\ &= q^n(1\cdot q^0 + q\cdot q^{-1} + \cdots + q^{n-1}\cdot q^{1-n}) = nq^n,\end{aligned}$$

where $P_n'$ denotes the primary polynomials of a degree smaller than $n$.
Next, suppose (3.7) is valid for a fixed integer $j$. Let us study the case $j+1$:

$$\begin{aligned}\sum_{A\in P_n} \mathrm{d}(A)^{j+1} &= \sum_{A\in P_n} \mathrm{d}(A)^j \sum_{\substack{(B,C),\\ BC=A}} 1 \\ &= \sum_{B\in P_n'} \sum_{\substack{C\in\mathbb{F}_q[T],\\ \deg(BC)<n}} \mathrm{d}(BC)^j \\ &\leq \sum_{B\in P_n'} \sum_{\substack{C\in\mathbb{F}_q[T]\\ \deg(BC)<n}} (\mathrm{d}(B)\,\mathrm{d}(C))^j \\ &\leq \sum_{B\in P_n'} \mathrm{d}(B)^j \sum_{C\in P_{n-\deg(B)}} \mathrm{d}(C)^j.\end{aligned}$$

For the last sum we can use the induction hypothesis and get

$$\begin{aligned}\sum_{A\in P_n} \mathrm{d}(A)^{j+1} &\leq \sum_{B\in P_n'} \mathrm{d}(B)^j n^{2j-1} q^n q^{-\deg(B)} \\ &= n^{2j-1} q^n \sum_{B\in P_n'} \mathrm{d}(B)^j q^{-\deg(B)}.\end{aligned}$$

Finally, we consider

$$\begin{aligned}\sum_{B\in P_n'} \mathrm{d}(B)^j q^{-\deg(B)} &= \sum_{i\leq n} \sum_{\deg(B)=i-1} \mathrm{d}(B)^j q^{-i} \leq \sum_{i\leq n} i^{2j-1} q^i q^{-i} \\ &\leq \sum_{i\leq n} i^{2j-1} \leq n^{2j}.\end{aligned}$$

Consequently,

$$\sum_{A\in P_n} \mathrm{d}(A)^{j+1} \le n^{2^j-1} q^n n^{2^j} \le n^{2^{j+1}-1} q^n.$$

□

*Proof of Lemma 24.* Set

$$S := \sum_{A\in P_n} E\left(\frac{H}{Q^{j+1}} P(A)\right).$$

As in the proof of Webb's Lemma 3 (see [32]), we have

$$\begin{aligned} |S|^2 = S\overline{S} &= \sum_{B\in P_n}\sum_{A\in P_n} E\left(\frac{H}{Q^{j+1}}(P(B)-P(A))\right) \\ &= \sum_{M_1\in P_n}\sum_{A\in P_n} E\left(\frac{H}{Q^{j+1}}(P(A+M_1)-P(A))\right), \end{aligned}$$

since $A + M_1$ runs over all polynomials of degree smaller than $n$, while $M_1$ runs over all polynomials of degree smaller than $n$.
Let $P(A) = a_r A^r + a_{r-1}A^{r-1} + \cdots + a_1 A + a_0$, then,

$$\begin{aligned} P(A+M_1) - P(A) &= a_r(A+M_1)^r + a_{r-1}(A+M_1)^{r-1} + \cdots + a_0 \\ &\quad -(a_r A^r + a_{r-1}A^{r-1} + \cdots + a_1 A + a_0) \\ &= a_r r A^{r-1} M_1 + C_{r-2}A^{r-2} + \cdots + C_1 A + C_0, \end{aligned}$$

where $\deg(C_i A^i) < \deg(A^{r-1}M_1)$ and $M_1 \mid C_i$ for $0 \le i \le r-2$.
Therefore,

$$|S|^2 = \sum_{M_1\in P_n}\sum_{A\in P_n} E\left(\frac{H}{Q^{j+1}}(a_r r A^{r-1}M_1 + C_{r-2}A^{r-2} + \cdots + C_0)\right).$$

By Cauchy's inequality,

$$\begin{aligned} |S|^4 &\le \sum_{M_1\in P_n} 1^2 \sum_{M_1\in P_n} \left|\sum_{A\in P_n} E\left(\frac{H}{Q^{j+1}}(a_r r A^{r-1}M_1 + \cdots)\right)\right| \\ &= q^n \sum_{M_1\in P_n}\sum_{M_2\in P_n}\sum_{A\in P_n} E\Big(\frac{H}{Q^{j+1}}\Big(a_r r(A+M_2)^{r-1}M_1 + \cdots \\ &\qquad\qquad -(a_r r A^{r-1}M_1 + \cdots)\Big)\Big) \\ &= q^n \sum_{M_1\in P_n}\sum_{M_2\in P_n}\sum_{A\in P_n} E\left(\frac{H}{Q^{j+1}}(a_r r(r-1)A^{r-2}M_1M_2 + \cdots)\right). \end{aligned}$$

Continuing in this way, we get

$$\begin{aligned}|S|^{2^{r-1}} &\leq (q^n)^{2^{r-3}}(q^{2n})^{2^{r-4}}\cdots(q^{(r-2)n})^{2^0}\times\\ &\quad\times\sum_{M_1}\cdots\sum_{M_{r-1}}\sum_{A\in P_n}E\left(\frac{H}{Q^{j+1}}(a_r r!AM_1M_2\cdots M_{r-1}+\cdots)\right)\\ &\leq q^{n(2^{r-1}-r)}\sum_{M_1}\cdots\sum_{M_{r-1}}\sum_{A\in P_n}E\left(\frac{H}{Q^{j+1}}(a_r r!AM_1M_2\cdots M_{r-1})\right).\end{aligned}$$

Next, for an arbitrary polynomial $M$, set

$$V(M)=\begin{cases}1 & \text{if } \nu\left(\left\{\frac{H}{Q^{j+1}}M\right\}\right)>n,\\ 0 & \text{otherwise.}\end{cases}$$

So,

$$|S|^{2^{r-1}}\leq q^{n(2^{r-1}-r+1)}\sum_{(M_1,\ldots,M_{r-1})\in P_n^{r-1}}V(M_1\cdots M_{r-1}).$$

Set $t=(r-1)(n-1)+1=rn-r-n$, then, by using the function d for the number of primary divisors, we get

$$|S|^{2^{r-1}}\leq(q-1)^{r-2}q^{n(2^{r-1}-r+1)}\sum_{M\in P_t}V(M)d(M)^{r-1}.$$

One can easily show

$$\sum_{M\in P_t}V(M)\leq\begin{cases}q^{t-(j+1)k} & \text{if } (j+1)k<n,\\ q^{t-n} & \text{if } n<(j+1)k\leq t,\\ q^{(j+1)k-n} & \text{if } t<(j+1)k.\end{cases}$$

Once again, we use Cauchy's inequality as well as (3.7) and finally obtain

$$\begin{aligned}|S|^{2^r} &\leq (q-1)^{2r-4}q^{n(2^r-2r+2)}t^{2^{2r-2}}q^t\max\{q^{t-(j+1)k},q^{t-n},q^{(j+1)k-n}\}\\ &\leq q^{2r-4}q^{n(2^r-2r+2)}q^{2nr-2n-2r}t^{2^{2r-2}}\max\{q^{-(j+1)k},q^{-n},q^{(j+1)k-nr+r}\}\\ &\leq q^{r-4}q^{n2^r}t^{2^{2r-2}}\max\{q^{-(j+1)k},q^{-n},q^{(j+1)k-nr}\}\\ &\leq (rn)^{2^{2r-2}}q^{n2^r}\max\{q^{-(j+1)k},q^{-n},q^{(j+1)k-nr}\}.\end{aligned}$$

Thus, for $|S|$ we have

$$|S|\ll n^{2^{r-2}}q^n\max\{q^{-(j+1)k2^{-r}},q^{-n2^{-r}},q^{(j+1)k2^{-r}-nr2^{-r}}\}.$$

□

**Corollary 2** *Let* $n^{1/3} \leq j+1 \leq \frac{rn}{k} - n^{1/3}$. *Then, there exists a constant* $c > 0$ *such that*

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

*uniformly in this range.*

*Proof.* The maximum error in (3.6) occurs at the boundary of the range. The maximum degree is $\frac{rn}{k} - n^{1/3}$. Thus, by Lemma 24

$$\begin{aligned}&\frac{1}{q^n}\left|\sum_{A\in P_n} E\left(\frac{H}{Q^{j+1}}P(A)\right)\right| \\ &\quad\ll n^{2^{r-2}} \max\left(q^{-nr2^{-r}+n^{1/3}k2^{-r}}, q^{-n2^{-r}}, q^{nr2^{-r}-n^{1/3}k2^{-r}-nr2^{-r}}\right) \\ &\quad= e^{2^{r-2}\log n - n^{1/3}k2^{-r}\log q}.\end{aligned}$$

The minimum degree is just $n^{1/3}$. Therefore, we get

$$\frac{1}{q^n}\left|\sum_{A\in P_n} E\left(\frac{H}{Q^{j+1}}P(A)\right)\right| \ll n^{2^{r-2}} \max\left(q^{-n^{1/3}r2^{-r}}, q^{-n2^{-r}}, q^{n^{1/3}r2^{-r}-nr2^{-r}}\right).$$

Since $q^{-n^{1/3}r2^{-r}} > q^{n^{1/3}r2^{-r}-nr2^{-r}}$, we finally obtain a uniform estimation

$$\frac{1}{q^n}\left|\sum_{A\in P_n} E\left(\frac{H}{Q^{j+1}}P(A)\right)\right| \ll e^{2^{r-2}\log n - n^{1/3}k2^{-r}\log q} \ll e^{-cn^{1/3}}.$$

□

A similar estimate holds for monic irreducible polynomials of degree $< n$. However, we will first of all complete the proof of (3.2) and afterwards focus on (3.3). Since the proof of both parts of the theorem is very similar, the latter will be shortened.
Returning to $P_n$, we can use Corollary 2 to bring our thread concerning (3.5) to an end and forumlate our first extension.

**Lemma 26** *Let* $n^{1/3} \leq j+1 \leq \frac{nr}{k} - n^{1/3}$, *then,*

$$\frac{1}{q^n}\#\left\{A \in P_n | D_{Q,j}(P(A)) = \varepsilon\right\} = \frac{1}{q^k} + O\left(e^{-cn^{1/3}}\right)$$

*uniformly in this range.*

As a consequence for the mean value, we get the following lemma.

**Lemma 27** *Let $g : \mathbb{F}_q[T] \to \mathbb{R}$ be Q-additive. Then,*

$$\frac{1}{q^n} \sum_{A \in P_n} g(P(A)) = \frac{rn}{k}\mu + O\left(ne^{-cn^{1/3}}\right)$$

*with*

$$\mu := \frac{1}{q^k} \sum_{\varepsilon \in P_k} g(\varepsilon).$$

*Proof.* According to the range in Lemma 26, we split the whole sum into three parts.

$$\begin{aligned}\frac{1}{q^n} \sum_{A \in P_n} g(P(A)) &= \sum_{j \le \frac{nr}{k}} \sum_{\varepsilon \in P_k} g(\varepsilon) \frac{1}{q^n} \#\{A \in P_n | D_{Q,j}(P(A)) = \varepsilon\} \\ &= \underbrace{\sum_{j < n^{1/3}} \cdots}_{=:S_1} + \underbrace{\sum_{n^{1/3} \le j \le \frac{nr}{k} - n^{1/3}} \cdots}_{=:S_2} + \underbrace{\sum_{\frac{nr}{k} - n^{1/3} < j \le \frac{nr}{k}} \cdots}_{=:S_3}.\end{aligned}$$

Obviously, $S_1$ and $S_3$ can be estimated by $|S_1| \ll n^{1/3}$ resp. $|S_3| \ll n^{1/3}$.

$$\begin{aligned}S_2 &= \sum_{n^{1/3} \le j \le \frac{nr}{k} - n^{1/3}} \sum_{\varepsilon \in P_k} g(\varepsilon) \frac{1}{q^n} \#\{A \in P_n | D_{Q,j}(P(A)) = \varepsilon\} \\ &= \sum_{\varepsilon \in P_k} g(\varepsilon) \sum_j \left(\frac{1}{q^k} + O\left(e^{-cn^{1/3}}\right)\right) \\ &= \frac{1}{q^k}\left(\frac{nr}{k} - 2n^{1/3}\right) \sum_{\varepsilon \in P_k} g(\varepsilon) + O\left(ne^{-cn^{1/3}}\right) \\ &= \frac{nr}{k}\mu + O\left(ne^{-cn^{1/3}}\right).\end{aligned}$$

□

With the help of estimate (3.6), we can also prove the following frequency estimate.

**Lemma 28** *Let $m$ be a fixed integer and $n^{1/3} \le j_1 + 1 < j_2 + 1 < \cdots < j_m + 1 \le \frac{nr}{k} - n^{1/3}$. Then,*

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

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

*Proof.* By Lemma 22 we have

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

where $\sum^*$ denotes that we sum just over all $(H_1, \ldots, H_m) \neq (0, \ldots, 0)$. In order to complete the proof, we only 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 $n^{1/3} \leq j_l \leq \frac{nr}{k} - n^{1/3}$. Hence, by Corollary 2, the result follows. □

The idea of the proof of Theorem 5 is to compare the distribution of $g(P(A))$ with the distribution of sums of independent identically distributed random variables. Let $Y_0, Y_1, \ldots$ be independent identically distributed random variables on $P_k$ with $\mathbb{P}[Y_j = D] = \frac{1}{q^k}$ for all $D \in P_k$. Then, Lemma 28 can be rewritten as

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

Furthermore, note that this relation is also true if $j_1, \ldots, j_m$ vary in the range $n^{1/3} \leq j_1, j_2, \ldots, j_m \leq \frac{nr}{k} - n^{1/3}$ and are not in the correct order. It is even true if some of them are equal.
In fact, we will use a method of moments; that is, we will show that the moments of $g(P(A))$ can be compared with moments of the normal distribution. Therefore, we will make use of the following two results of the probability theory. The first one is well known and needs no further explanation.

**Lemma 29 (Central Limit Theorem)** *Let $(\xi_n)$ be a sequence of independent identically distributed random variables with mean $\mu$ and variance $\sigma^2$. Define*

$$\eta_n := \frac{\xi_1 + \cdots + \xi_n - n\mu}{\sqrt{n}\sigma},$$

*so that $\mathbb{E}(\eta_n) = 0$ and $\mathbb{V}(\eta_n) = 1$. Then, $\eta_n$ is asymptotically normal distributed, i.e.*

$$\lim_{n\to\infty} \mathbb{P}(\eta_n \leq t) = \Phi(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-u^2/2}\, du.$$

*Moreover, if the $m$-th moment $\mathbb{E}(\xi_n)^m$ exists for all $m \in \mathbb{N}$, then,*

$$\mathbb{E}(\eta_n)^m \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} t^m e^{-t^2/2}\, dt$$

*for all $m \in \mathbb{N}$.*

The second result is a variation of the Fréchet-Shohat Theorem (see for example [27]), which is used for the method of moments.

**Lemma 30** *Let $Z_n$ be a random variable, and*

$$\widetilde{Z_n} := \frac{Z_n - \mathbb{E}Z_n}{\sqrt{\mathbb{V}Z_n}}$$

*with $\mathbb{E}\widetilde{Z_n} = 0$ and $\mathbb{V}\widetilde{Z_n} = 1$. If*

$$\mathbb{E}\left(\frac{Z_n - \mathbb{E}Z_n}{\sqrt{\mathbb{V}Z_n}}\right)^m \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} t^m e^{-t^2/2}\, dt$$

*for every $m \in \mathbb{N}$, then,*

$$\widetilde{Z_n} \xrightarrow{w} \mathcal{N}(0,1).$$

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

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

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

**Lemma 31** *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*

$$\frac{1}{q^n} \sum_{A \in P_n} \left( \widetilde{g}(P(A)) - \left( \frac{nr}{k} - 2n^{1/3} \right) \mu \right)^m =$$

$$= \mathbb{E} \left( \sum_{n^{1/3} \le j \le \frac{nr}{k} - n^{1/3}} (g(Y_j) - \mu) \right)^m + O\left( n^m e^{-cn^{1/3}} \right).$$

*Proof.* For notational convenience we only consider the second moment in greater detail:

$$\frac{1}{q^n} \sum_{A \in P_n} \left( \widetilde{g}(P(A)) - \left( \frac{nr}{k} - 2n^{1/3} \right) \mu \right)^2 =$$

$$= \sum_{j_1, j_2} \sum_{D_1, D_2} g(D_1) g(D_2) \frac{1}{q^n} \#\{A \in P_n : D_{Q,j_1}(P(A)) = D_1, D_{Q,j_2}(P(A)) = D_2\}$$

$$- \sum_{j_1} \sum_{D_1} g(D_1) \frac{1}{q^n} \#\{A \in P_n : D_{Q,j_1}(P(A)) = D_1\} \cdot \sum_{j_2} \mu$$

$$- \sum_{j_1} \mu \sum_{j_2} \sum_{D_2} g(D_2) \frac{1}{q^n} \#\{A \in P_n : D_{Q,j_2}(P(A)) = D_2\} + \sum_{j_1, j_2} \mu^2$$

$$= \sum_{j_1, j_2} \sum_{D_1, D_2} g(D_1) g(D_2) \mathbb{P}[Y_{j_1} = D_1, Y_{j_2} = D_2] + O\left( n^2 e^{-cn^{1/3}} \right)$$

$$- \sum_{j_1} \sum_{D_1} g(D_1) \mathbb{P}[Y_{j_1} = D_1] \sum_{j_2} \mu$$

$$- \sum_{j_1} \mu \sum_{j_2} \sum_{D_2} g(D_2) \mathbb{P}[Y_{j_2} = \varepsilon_2] + \sum_{j_1} \sum_{j_2} \mu^2$$

$$= \mathbb{E} \left( \sum_j (g(Y_j) - \mu) \right)^2 + O\left( n^2 e^{-cn^{1/3}} \right).$$

The very same procedure also works in general:

$$\begin{aligned}
&\frac{1}{q^n}\sum_{A\in P_n}\left(\widetilde{g}(P(A))-\left(\frac{nr}{k}-2n^{1/3}\right)\mu\right)^m = \\
&= \sum_{j_1,\ldots,j_m}\sum_{\varepsilon_1,\ldots,\varepsilon_m} g(\varepsilon_1)\cdots g(\varepsilon_m) \\
&\qquad \frac{1}{q^n}\#\left\{A\in P_n | D_{Q,j_1}(P(A))=\varepsilon_1,\ldots,D_{Q,j_m}(P(A))=\varepsilon_m\right\} \\
&= \sum_{j_1,\ldots,j_m}\sum_{\varepsilon_1,\ldots,\varepsilon_m} g(\varepsilon_1)\cdots g(\varepsilon_m)\mathbb{P}[Y_{j_1}=\varepsilon_1,\ldots,Y_{j_m}=\varepsilon_m]+O\left(n^m e^{-cn^{1/3}}\right) \\
&\quad -\binom{m}{1}\sum_{j_1,\ldots,j_m}\mu\sum_{\varepsilon_1,\ldots,\varepsilon_{m-1}} g(\varepsilon_1)\cdots g(\varepsilon_{m-1}) \\
&\qquad \mathbb{P}[Y_{j_1}=\varepsilon_1,\ldots,Y_{j_{m-1}}=\varepsilon_{m-1}]+\cdots \\
&\quad +(-1)^i\binom{m}{i}\sum_{j_1,\ldots,j_m}\mu^{m-i}\sum_{\varepsilon_1,\ldots,\varepsilon_{m-i}} g(\varepsilon_1)\cdots g(\varepsilon_{m-i}) \\
&\qquad \mathbb{P}[Y_{j_1}=\varepsilon_1,\ldots,Y_{j_{m-i}}=\varepsilon_{m-i}]+\cdots \\
&\vdots \\
&= \mathbb{E}\left[\left(\sum_{n^{1/3}\le j\le \frac{nr}{k}-n^{1/3}}(g(Y_j)-\mu)\right)^m\right]+O\left(n^m e^{-cn^{1/3}}\right).
\end{aligned}$$

This completes the proof of the lemma. □

Since the sum of independent identically distributed random variables converges (after normalization) to the normal distribution (see Lemma 29), it follows from Lemma 31 that

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

Due to

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

we obtain

$$\begin{aligned}\frac{\widetilde{g}(P(A)) - (\frac{nr}{k} - 2n^{1/3})\mu}{\sqrt{(\frac{nr}{k} - 2n^{1/3})\sigma^2}} &= \frac{g(P(A)) + cn^{1/3} - (\frac{nr}{k} - 2n^{1/3})\mu}{\sqrt{(\frac{nr}{k} - 2n^{1/3})\sigma^2}} \\ &= \frac{g(P(A)) - \frac{nr}{k}\mu + c'n^{1/3}}{\sqrt{\frac{nr}{k}\sigma^2}} \cdot \underbrace{\frac{\sqrt{\frac{nr}{k}\sigma^2}}{\sqrt{(\frac{nr}{k} - 2n^{1/3})\sigma^2}}}_{\to 1} \\ &\to \frac{g(P(A)) - \frac{nr}{k}\mu}{\sqrt{\frac{nr}{k}\sigma^2}} + \underbrace{\frac{c'n^{1/3}}{\sqrt{\frac{nr}{k}\sigma^2}}}_{\to 0}.\end{aligned}$$

Thus,

$$\frac{\widetilde{g}(P(A)) - (\frac{nr}{k} - 2n^{1/3})\mu}{\sqrt{(\frac{nr}{k} - 2n^{1/3})\sigma^2}} \to \frac{g(P(A)) - \frac{nr}{k}\mu}{\sqrt{\frac{nr}{k}\sigma^2}}$$

and finally,

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

Following the same arguments, we will now complete the proof of Theorem 5 by proving (3.3) concerning monic irreducible polynomials. First, we want to determine the cardinality of $I_n$.

**Lemma 32** *The number $N_q(n)$ of monic irreducible polynomials in $\mathbb{F}_q[T]$ of degree $n$ is given by*

$$N_q(n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d},$$

*where $\mu$ is the Moebius function.*

*Proof.* For proof see [23] resp. [26]. □

Thus,

$$|I_n| = \sum_{k<n} N_q(k) = \sum_{k<n}\left(\frac{q^k}{k} + O(q^{k/2})\right) \sim \frac{q^n}{n(q-1)}.$$

Furthermore, we need the already mentioned second variation of Lemma 23, which can also be found in [3].

**Lemma 33** *Let* $\frac{2r}{k}n^{1/3} \leq j+1 \leq \frac{rn}{k} - \frac{2r}{k}n^{1/3}$, *and* $H$ *be a polynomial coprime to* $Q$. *Then,*

$$\frac{1}{|I_n|}\left|\sum_{A\in I_n} E\left(\frac{H}{Q^{j+1}}P(A)\right)\right| \ll (\log n)\cdot n^{7/3+2^{2r-2}}q^{-r2^{-2r}n^{1/3}}. \tag{3.8}$$

*Proof.* See Proposition VII.7 in [3]. □

**Corollary 3** *Let* $\frac{2r}{k}n^{1/3} \leq j+1 \leq \frac{rn}{k} - \frac{2r}{k}n^{1/3}$. *Then, there exists a constant* $c > 0$ *such that*

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

*uniformly in this range.*

*Proof.* By (3.8), we get the uniform estimation

$$\begin{aligned}\frac{1}{|I_n|}\left|\sum_{A\in I_n} E\left(\frac{H}{Q^{j+1}}P(A)\right)\right| &\ll (\log n)\cdot n^{7/3+2^{2r-2}}q^{-r2^{-2r}n^{1/3}}\\ &\ll e^{\log\log n+(7/3+2^{2r-2})\log n - r2^{-2r}n^{1/3}\log q}\\ &\ll e^{-cn^{1/3}}\end{aligned}$$

for some constant $c > 0$. □

**Lemma 34** *Let* $\frac{2r}{k}n^{1/3} \leq j+1 \leq \frac{nr}{k} - \frac{2r}{k}n^{1/3}$, *then,*

$$\frac{1}{|I_n|}\#\{A\in I_n | D_{Q,j}(P(A)) = \varepsilon\} = \frac{1}{q^k} + O\left(e^{-cn^{1/3}}\right)$$

*uniformly in this range.*

*Proof.*

$$\begin{aligned}\frac{1}{|I_n|}\#\{A\in I_n | D_{Q,j}(P(A)) = \varepsilon\} &= \frac{1}{|I_n|}\sum_{A\in I_n}\sum_{H\in P_k} c_{H,\varepsilon}E\left(\frac{P(A)}{Q^{j+1}}H\right)\\ &= \sum_{H\in P_k} c_{H,\varepsilon}\frac{1}{|I_n|}\sum_{A\in I_n} E\left(\frac{P(A)}{Q^{j+1}}H\right)\\ &= \frac{1}{q^k} + \underbrace{\sum_{H\in P_k^*} c_{H,\varepsilon}\frac{1}{|I_n|}\sum_{A\in I_n} E\left(\frac{P(A)}{Q^{j+1}}H\right)}_{\text{S:=}}.\end{aligned}$$

Due to Corollary 3 we have $S \ll e^{-cn^{1/3}}$, thus, the required result follows. □

As a consequence for the mean value, we get a similar lemma, as for $A \in P_n$:

**Lemma 35** *Let $g : \mathbb{F}_q[T] \to \mathbb{R}$ be Q-additive. Then,*

$$\frac{1}{|I_n|} \sum_{A \in I_n} g(P(A)) = \frac{rn}{k}\mu + O\left(ne^{-cn^{1/3}}\right)$$

*with*

$$\mu := \frac{1}{q^k} \sum_{\varepsilon \in P_k} g(\varepsilon).$$

*Proof.* According to the range in Lemma 34, we split the whole sum into three parts.

$$\begin{aligned}\frac{1}{|I_n|} \sum_{A \in I_n} g(P(A)) &= \sum_{j \le \frac{nr}{k}} \sum_{\varepsilon \in P_k} g(\varepsilon) \frac{1}{|I_n|} \#\left\{A \in I_n | D_{Q,j}(P(A)) = \varepsilon\right\} \\ &= \underbrace{\sum_{j < \frac{2r}{k} n^{1/3}} \cdots}_{=:S_1} + \underbrace{\sum_{\frac{2r}{k} n^{1/3} \le j \le \frac{nr}{k} - \frac{2r}{k} n^{1/3}} \cdots}_{=:S_2} + \underbrace{\sum_{\frac{nr}{k} - \frac{2r}{k} n^{1/3} < j \le \frac{nr}{k}} \cdots}_{=:S_3}.\end{aligned}$$

Obviously, $S_1$ and $S_3$ can be estimated by $|S_1| \ll n^{1/3}$ resp. $|S_3| \ll n^{1/3}$. Due to Lemma 34 we have

$$\begin{aligned}S_2 &= \sum_{n^{1/3} \le j \le \frac{nr}{k} - n^{1/3}} \sum_{\varepsilon \in P_k} g(\varepsilon) \frac{1}{|I_n|} \#\left\{A \in I_n | D_{Q,j}(P(A)) = \varepsilon\right\} \\ &= \sum_{\varepsilon \in P_k} g(\varepsilon) \sum_j \left(\frac{1}{q^k} + O\left(e^{-cn^{1/3}}\right)\right) \\ &= \frac{1}{q^k}\left(\frac{nr}{k} - \frac{4r}{k} n^{1/3}\right) \sum_{\varepsilon \in P_k} g(\varepsilon) + O\left(ne^{-cn^{1/3}}\right) \\ &= \frac{nr}{k}\mu + O\left(ne^{-cn^{1/3}}\right).\end{aligned}$$

□

With the help of estimate (3.8) we can prove the following frequency estimate.

**Lemma 36** *Let $m$ be a fixed integer and $\frac{2r}{k}n^{1/3} \le j_1 + 1 < j_2 + 1 < \cdots < j_m + 1 \le \frac{nr}{k} - \frac{2r}{k}n^{1/3}$. Then,*

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

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

*Proof.* By Lemma 22, we have

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

where $\sum^*$ once more denotes that we sum just over all $(H_1, \ldots, H_m) \neq (0, \ldots, 0)$.
Let $l$ be the largest $i$ with $H_i \neq 0$, then,

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

where $H = H_l + H_{l-1}Q^{j_l-j_{l-1}} + \cdots + H_1Q^{j_l-j_1}$. By our assumption, we have $\frac{2r}{k}n^{1/3} \le j_l + 1 \le \frac{nr}{k} - \frac{2r}{k}n^{1/3}$. Hence, by Corollary 3, we obtain $S = O(e^{-cn^{1/3}})$. □

Note that $Y_0, Y_1, \ldots$ are independent identically distributed random variables on $P_k$ with $\mathbb{P}[Y_j = D] = \frac{1}{q^k}$ for all $D \in P_k$. We rewrite Lemma 36 as

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

whereby this relation is also true if $j_1, \ldots, j_m$ vary in the range $\frac{2r}{k}n^{1/3} \leq j_1, j_2, \ldots, j_m \leq \frac{nr}{k} - \frac{2r}{k}n^{1/3}$ and are not in the correct order. It is even true if some of them are equal.

As already mentioned, our methods of proving Theorem 5 for $A \in I_n$ are absolutely the same as for $A \in P_n$. We will show that the moments of $g(P(A))$ can be compared with moments of the normal distribution. So, it will be shown that the corresponding (normalized) distribution function of $g(P(A))$ converges to the normal distribution function $\Phi(x)$, independent of whether $A \in P_n$ or $A \in I_n$.

Again, it turns out that we will have to cut off the first and last few digits. However, this time we will study another range, that is, we will work with

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

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

**Lemma 37** *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*

$$\frac{1}{|I_n|}\sum_{A \in I_n}\left(\widetilde{g}(P(A)) - \left(\frac{nr}{k} - \frac{4r}{k}n^{1/3}\right)\mu\right)^m =$$
$$= \mathbb{E}\left(\sum_{\frac{2r}{k}n^{1/3} \leq j \leq \frac{nr}{k} - \frac{2r}{k}n^{1/3}} (g(Y_j) - \mu)\right)^m + O\left(n^m e^{-cn^{1/3}}\right).$$

*Proof.* The procedure is identical to the proof of Lemma 31, thus, we content ourselves with the general case.

$$\begin{aligned}
&\frac{1}{|I_n|}\sum_{A\in I_n}\left(\widetilde{g}(P(A))-\left(\frac{nr}{k}-\frac{4r}{k}n^{1/3}\right)\mu\right)^m = \\
&= \sum_{j_1,\ldots,j_m}\sum_{\varepsilon_1,\ldots,\varepsilon_m} g(\varepsilon_1)\cdots g(\varepsilon_m) \\
&\qquad \frac{1}{|I_n|}\#\left\{A\in I_n | D_{Q,j_1}(P(A))=\varepsilon_1,\ldots,D_{Q,j_m}(P(A))=\varepsilon_m\right\} \\
&= \sum_{j_1,\ldots,j_m}\sum_{\varepsilon_1,\ldots,\varepsilon_m} g(\varepsilon_1)\cdots g(\varepsilon_m)\mathbb{P}[Y_{j_1}=\varepsilon_1,\ldots,Y_{j_m}=\varepsilon_m]+O\left(n^m e^{-cn^{1/3}}\right) \\
&\quad -\binom{m}{1}\sum_{j_1,\ldots,j_m}\mu\sum_{\varepsilon_1,\ldots,\varepsilon_{m-1}} g(\varepsilon_1)\cdots g(\varepsilon_{m-1}) \\
&\qquad \mathbb{P}[Y_{j_1}=\varepsilon_1,\ldots,Y_{j_{m-1}}=\varepsilon_{m-1}]+\cdots \\
&\quad +(-1)^i\binom{m}{i}\sum_{j_1,\ldots,j_m}\mu^{m-i}\sum_{\varepsilon_1,\ldots,\varepsilon_{m-i}} g(\varepsilon_1)\cdots g(\varepsilon_{m-i}) \\
&\qquad \mathbb{P}[Y_{j_1}=\varepsilon_1,\ldots,Y_{j_{m-i}}=\varepsilon_{m-i}]+\cdots \\
&\vdots \\
&= \mathbb{E}\left[\left(\sum_{\frac{2r}{k}n^{1/3}\le j\le \frac{nr}{k}-\frac{2r}{k}n^{1/3}}(g(Y_j)-\mu)\right)^m\right]+O\left(n^m e^{-cn^{1/3}}\right).
\end{aligned}$$

□

Since the sum of independent identically distributed random variables converges (after normalization) to the normal distribution, it follows from Lemma 37 that

$$\frac{1}{|I_n|}\#\left\{A\in I_n : \frac{\widetilde{g}(P(A))-(\frac{nr}{k}-\frac{4r}{k}n^{1/3})\mu}{\sqrt{(\frac{nr}{k}-\frac{4r}{k}n^{1/3})\sigma^2}}\le x\right\}=\Phi(x)+o(1).$$

Due to

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

and $n^{1/3}/n^{1/2}=n^{-1/6}\to 0$, we obtain

$$\frac{\widetilde{g}(P(A))-(\frac{nr}{k}-\frac{4r}{k}n^{1/3})\mu}{\sqrt{(\frac{nr}{k}-\frac{4r}{k}n^{1/3})\sigma^2}}\to\frac{g(P(A))-\frac{nr}{k}\mu}{\sqrt{\frac{nr}{k}\sigma^2}}$$

and finally,

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

This completes both the proof of Theorem 5 and this section on Bassily and Kátai's central limit theorem.

## 3.2 The joint distribution of two $Q_j$-additive functions

After studying the situation for one $Q$, we are now interested in the distribution with respect to several different basis-polynomials $Q_1, \ldots, Q_d$.
We are going to prove a generalization of Theorem 3 for two bases $Q_1, Q_2$.

First, our result:

**Theorem 6** *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. Furthermore, 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 $n \to \infty$,*

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

**Remark 10** *Theorems 4 and 6 assert that $Q$-ary digital expansions are (asymptotically) independent if the base polynomials are pairwise coprime.*

Apart from some properties of $\nu$ resp. the character $E$ (see Lemmas 2, 3 and 6 in Chapter 1), Mason's theorem (see [25]) is an important tool for proving Theorem 6.

**Lemma 38 (Mason's Theorem)** *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 present an alternate proof of this theorem which was found by Noah Snyder [29]. Therefore, we define $n_0(F)$ as the number of distinct zeros of a non-zero polynomial $F \in K[T]$.

**Lemma 39** *Let $F$ be a non-zero polynomial in $K[T]$. Then,*

$$\deg(F) \leq \deg(F, F') + n_0(F),$$

*where $(G, H)$ denotes the greatest common divisor (gcd) of $G, H$.*

*Proof.* Let $\alpha_1, \ldots, \alpha_m$ be the roots of $F$ with multiplicities $a_1, \ldots, a_m$, so that $F = c(T-\alpha_1)^{a_1} \cdots (T-\alpha_m)^{a_m}$. Then, due to the product rule,

$$\begin{aligned} F' &= ca_1(T-\alpha_1)^{a_1-1}(T-\alpha_2)^{a_2} \cdots (T-\alpha_m)^{a_m} \\ &\quad + c(T-\alpha_1)^{a_1} \frac{d}{dT}\left((T-\alpha_2)^{a_2} \cdots (T-\alpha_m)^{a_m}\right). \end{aligned}$$

Therefore, $(T-\alpha_1)^{a_1-1} \mid (F, F')$. Similarly, $(T-\alpha_i)^{a_i-1} \mid (F, F')$. So we see that $(T-\alpha_1)^{a_1-1} \cdots (T-\alpha_m)^{a_m-1} \mid (F, F')$. Therefore, since $F$ is non-zero, $\deg(F) - n_0(F) \leq \deg(F, F')$. The lemma follows immediately. □

Using this lemma, we can prove Mason's Theorem, Lemma 38.

*Proof of Lemma 38.* $A + B = C$. Therefore, $A' + B' = C'$. Multiplying the first equation by $A'$, the second by $A$, and subtracting, we find that $A'B - AB' = A'C - AC'$. Therefore, $(A, A'), (B, B')$, and $(C, C')$ all divide $A'B - AB'$. Since they are relatively prime,

$$(A, A')(B, B')(C, C') \mid (A'B - AB').$$

We claim that the right-hand side is non-zero. If $A'B - AB' = 0$, then, $A \mid A'B$. Since $A$ and $B$ are relatively prime, $A \mid A'$. Therefore, $A' = 0$. Similarly, $B'$ and $C'$ would also be zero, thus contradicting the assumption. Therefore, the right hand side is non-zero, and

$$\deg(A, A') + \deg(B, B') + \deg(C, C') \leq \deg(A) + \deg(B) - 1.$$

We move everything to the right-hand side and add $\deg(C)$ to both sides to find that

$$\deg(C) \leq \deg(A) - \deg(A, A') + \deg(B) - \deg(B, B') + \deg(C) - \deg(C, C') - 1.$$

The application of Lemma 39 yields the required result. □

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

**Lemma 40** *Let $Q_1, Q_2 \in \mathbb{F}_q[T]$ be coprime polynomials with degrees $\deg(Q_i) = k_i \geq 1$ such that at least one of the derivatives $Q_1', Q_2'$ is non-zero. Then, there exists a constant $c$ so that we have*

$$\deg(H_1 Q_2^{m_2} + H_2 Q_1^{m_1}) \geq \max\{\deg(H_1 Q_2^{m_2}), \deg(H_2 Q_1^{m_1})\} - c$$

*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 $m_1, m_2 \geq 1$.*

*Proof.* Set $A = H_1 Q_2^{m_2}$, $B = H_2 Q_1^{m_1}$, and $C = A + B$. If $A$ and $B$ are coprime by Mason's Theorem, we have $\deg(A) \leq n_0(ABC) - 1$ and $\deg(B) \leq n_0(ABC) - 1$, where $n_0(F)$ is defined as the number of distinct zeros of $F$, as above. Hence,

$$\begin{aligned} \max\{\deg(A), \deg(B)\} &\leq n_0(ABC) - 1 \\ &= n_0(H_1 H_2 Q_1 Q_2 C) - 1 \\ &\leq \deg(H_1 H_2 Q_1 Q_2) + \deg(C) - 1 \end{aligned}$$

and consequently,

$$\deg(C) \geq \max\{\deg(A), \deg(B)\} - \deg(H_1 H_2 Q_1 Q_2) + 1. \qquad (3.9)$$

This shows that (in the present case) $c = 2k_1 + 2k_2$ is an absolutely proper choice.
If $A$ and $B$ are not coprime, then we can write the common divisor $D$ in the following two ways:

$$D = D_{H_1} D_{Q_2} = D_{H_2} D_{Q_1},$$

where $D_{H_1}$ stands for the part of $D$ dividing $H_1$, and analogously $D_{H_2}$. $D_{Q_1}$ divides $Q_1^{m_1}$ and $D_{Q_2} \mid Q_2^{m_2}$. Since $(Q_1, Q_2) = 1$, we have $(D_{Q_1}, D_{Q_2}) = 1$, and thus,

$$\left.\begin{array}{c} D_{Q_2} \mid D_{H_2} \mid H_2 \\ D_{Q_1} \mid D_{H_1} \mid H_1 \end{array}\right\} \Rightarrow D \mid H_1 H_2.$$

Therefore, there are only finite possibilities for $D, D_{H_1}, D_{H_2}, D_{Q_1}$ and $D_{Q_2}$. Thus, $\exists\ m_2' : D_{Q_2} \mid Q_2^{m_2'}$ for all finitely possible $D_{Q_2}$. Analogously, $\exists\ m_1' : D_{Q_1} \mid Q_1^{m_1'}$ for all possibilities. Hence, there exists $m' \geq 0$, $m' := \max\{m_1', m_2'\}$ so that $D^2$ is a divisor of $H_1 H_2 (Q_1 Q_2)^{m'}$. Consequently, we have

$$(A/D)(B/D) = (H_1 H_2 (Q_1 Q_2)^{m'} / D^2) Q_1^{m_1 - m'} Q_2^{m_2 - m'},$$

and by the same reasoning as above we get

$$\deg(C/D) \geq \max\{\deg(A/D), \deg(B/D)\} - \deg((H_1 H_2 (Q_1 Q_2)^{m'} / D^2) Q_1 Q_2) + 1$$

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 finite possibilities for $H_1, H_2$, and $D$, the lemma follows. □

**Convergence of Moments** The idea of the proof of Theorem 6 is completely the same as the one of Theorem 5. We prove weak convergence by considering moments. The first step is to provide a generalization of Lemma 28.

**Lemma 41** *Let $m_1, m_2$ be fixed integers. Then, there exists a constant $c' > 0$ so 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*

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

Before giving the complete proof of this lemma we will concentrate on the cases $m_1 = m_2 = 1$ and $m_1 = m_2 = 2$. Thereafter, the main idea will have become clear, and the rather complex notation of the general proof will no longer disorient.

First, let $m_1 = m_2 = 1$. Thus, we have

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

Now, we can apply Lemma 40 and obtain

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

So, 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 $0\leq i\leq \frac{n}{k_1}-c'$ and $0\leq j\leq \frac{n}{k_2}-c'$. Hence, by Lemma 6

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

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

Next, suppose that $m_1=m_2=2$. Thus, we have

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

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

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

Otherwise, we will distinguish between four cases. Note that we assume w.l.o.g. that 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 even easier.

**Case 1** $i_2 - i_1 \leq c_1, j_2 - j_1 \leq c_2$ 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

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

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

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

Furthermore,

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

Thus, if $c_1$ and $c_2$ are chosen in a way that $c_1 k_1 > c + k_1$ and $c_2 k_2 > c + k_2$, 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 2,

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

**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 consider

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

Furthermore,

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

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. Let us consider

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

Furthermore,

$$\begin{aligned}
\nu\left(\frac{H_{12}}{Q_1^{i_2+1}}\right) &\geq k_1(i_2+1) - \deg(H_{12}) \\
&\geq k_1(i_2-i_1) + k_1 i_1 > k_1(i_1+c_1).
\end{aligned}$$

Hence, if $c_1$ is sufficiently large, then,

$$\nu\left(\frac{H_{11}}{Q_1^{i_1+1}}+\frac{H_{12}}{Q_1^{i_2+1}}+\frac{H_{21}}{Q_2^{j_1+1}}+\frac{H_{22}}{Q_2^{j_2+1}}\right) = \nu\left(\frac{H_{11}}{Q_1^{i_1+1}}+\frac{H_{21}}{Q_2^{j_1+1}}+\frac{H_{22}}{Q_2^{j_2+1}}\right)$$
$$< \min(k_1(i_1+1),k_2(j_1+1))+c(c_2).$$

Putting these four cases together, we show that (with suitably chosen constants $c_1, c_2$) there exists a constant $\tilde{c}$ so 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 $c' > 0$ such that

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

for all $i_1, j_1$ with $0 \leq i_1 \leq \frac{n}{k_1} - c'$ and $0 \leq j_1 \leq \frac{n}{k_2} - c'$. Hence, by Lemma 6,

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

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

Now, the general proof of Lemma 41 follows. Let $m_1, m_2 \geq 1$ be arbitrary positive integers, and consider

$$\frac{1}{q^n}\#\Big\{A \in P_n : D_{Q_1,i_1}(A) = D_1, \ldots, D_{Q_1,i_{m_1}}(A) = D_{m_1},$$
$$D_{Q_2,j_1}(A) = E_1, \ldots, D_{Q_2,j_{m_2}}(A) = E_{m_2}\Big\}$$
$$= \frac{1}{q^n}\sum_{A\in P_n}\prod_{s=1}^{m_1}\left(\sum_{H_{1s}\in P_{k_1}} c_{Q_1,H_{1s},D_s} E\left(\frac{H_{1s}}{Q_1^{i_s+1}}A\right)\right)\times$$
$$\times\prod_{t=1}^{m_2}\left(\sum_{H_{2t}\in P_{k_2}} c_{Q_2,H_{2t},E_t} E\left(\frac{H_{2t}}{Q_2^{j_t+1}}A\right)\right)$$
$$= \sum_{\substack{H_{11},\ldots,H_{1m_1}\in P_{k_1},\\ H_{21},\ldots,H_{2m_2}\in P_{k_2}}}\prod_{s=1}^{m_1} c_{Q_1,H_{1s},D_s}\prod_{t=1}^{m_2} c_{Q_2,H_{2t},E_t}$$
$$\times\frac{1}{q^n}\sum_{A\in P_n} E\left(A\left(\sum_{s=1}^{m_1}\frac{H_{1s}}{Q_1^{i_s+1}}+\sum_{t=1}^{m_2}\frac{H_{2t}}{Q_2^{j_t+1}}\right)\right).$$

For $H_{11} = \cdots = H_{1m_1} = H_{21} = \cdots = H_{2m_2} = 0$ we obtain the desired main term

$$\frac{1}{q_1^{k_1 m_1} q_2^{k_2 m_2}}.$$

Again, we only consider the case where all polynomials $H_{ij}$ are non-zero, and define integers $e_1$ and $e_2$ for properly chosen constants $c_1$ resp. $c_2$ by

$$i_2 - i_1 < \cdots < i_{e_1} - i_1 \leq c_1 < i_{e_1+1} - i_1 < \cdots < i_{m_1} - i_1, \quad (3.10)$$
$$j_2 - j_1 < \cdots < j_{e_2} - j_1 \leq c_2 < j_{e_2+1} - j_1 < \cdots < j_{m_2} - j_1. \quad (3.11)$$

Therewith, we look at

$$B := \sum_{s=1}^{e_1} \frac{H_{1s}}{Q_1^{i_s+1}} + \sum_{t=1}^{e_2} \frac{H_{2t}}{Q_2^{j_t+1}}$$

and determine the numerator of $B \in \mathbb{F}_q(T)$

$$\begin{aligned} \mathrm{num}(B) &= (H_{11}Q_1^{i_{e_1}-i_1} + H_{12}Q_1^{i_{e_1}-i_2} + \cdots + H_{1e_1})Q_2^{j_{e_2}+1} + \\ &\quad Q_1^{i_{e_1}+1}(H_{21}Q_2^{j_{e_2}-j_1} + H_{22}Q_2^{j_{e_2}-j_2} + \cdots + H_{2e_2}). \end{aligned}$$

By Lemma 40, we get

$$\begin{aligned} \deg(\mathrm{num}(B)) &\geq \max\left\{ \deg\left(\left(\sum_{s=1}^{e_1} H_{1s}Q_1^{i_{e_1}-i_s}\right)Q_2^{j_{e_2}+1}\right), \right. \\ &\qquad \left. \deg\left(Q_1^{i_{e_1}+1}\sum_{t=1}^{e_2} H_{2t}Q_2^{j_{e_2}-j_t}\right)\right\} - c' \\ &\geq \max\{k_1(i_{e_1} - i_1) + k_2(j_{e_2} + 1), k_2(j_{e_2} - j_1) + k_1(i_{e_1} + 1)\} - c'. \end{aligned}$$

Following the same principle as the example ($m_1 = m_2 = 2$) above,

$$\begin{aligned} \nu(B) &= \deg(\mathrm{den}(B)) - \deg(\mathrm{num}(B)) \\ &\leq k_1(i_{e_1} + 1) + k_2(j_{e_2} + 1) + c' \\ &\quad - \max\{k_1(i_{e_1} - i_1) + k_2(j_{e_2} + 1), k_1(i_{e_1} + 1) + k_2(j_{e_2} - j_1)\}. \quad (3.12) \end{aligned}$$

There are two possible cases:

**Case 1**

$$k_1(i_{e_1} - i_1) + k_2(j_{e_2} + 1) \geq k_1(i_{e_1} + 1) + k_2(j_{e_2} - j_1),$$

which is equivalent to $k_1(i_1 + 1) \leq k_2(j_1 + 1)$. Due to (3.12), we get

$$\nu(B) \leq k_1(i_1 + 1) + c'.$$

**Case 2**

$$k_1(i_{e_1} - i_1) + k_2(j_{e_2} + 1) \leq k_1(i_{e_1} + 1) + k_2(j_{e_2} - j_1),$$

which is equivalent to $k_1(i_1 + 1) \geq k_2(j_1 + 1)$. Due to (3.12), we get

$$\nu(B) \leq k_2(j_1 + 1) + c'.$$

Summing up, we have

$$\nu(B) \leq \min\{k_1(i_1 + 1), k_2(j_1 + 1)\} + c'.$$

Let $s$ be an arbitrary integer greater than $e_1$. We consider

$$\begin{aligned} \nu\left(\frac{H_{1s}}{Q_1^{i_s+1}}\right) &\geq k_1(i_s + 1) - \deg(H_{1s}) \\ &\geq k_1(i_s - i_1) + k_1 i_1. \end{aligned}$$

Since (3.10), we get

$$\nu\left(\frac{H_{1s}}{Q_1^{i_s+1}}\right) > k_1(i_1 + c_1).$$

Analogously, for $t > e_2$, $e_2$ defined by (3.11):

$$\nu\left(\frac{H_{2t}}{Q_2^{j_t+1}}\right) > k_2(j_1 + c_2).$$

Thus, if $c_1, c_2$ are chosen in a way that $c_1 k_1 \geq c' + k_1$ and $c_2 k_2 \geq c' + k_2$, then,

$$\nu\left(\sum_{s=1}^{e_1} \frac{H_{1s}}{Q_1^{i_s+1}} + \sum_{t=1}^{e_2} \frac{H_{2t}}{Q_2^{j_t+1}}\right) < \tag{3.13}$$

$$\min\left\{\nu\left(\frac{H_{1e_1+1}}{Q_1^{i_{e_1+1}+1}}\right), \ldots, \nu\left(\frac{H_{1m_1}}{Q_1^{i_{m_1}+1}}\right), \nu\left(\frac{H_{2e_2+1}}{Q_2^{j_{e_2+1}+1}}\right), \ldots, \nu\left(\frac{H_{2m_2}}{Q_2^{j_{m_2}+1}}\right)\right\}, \tag{3.14}$$

and consequently, by Lemma 2,

$$\begin{aligned} \nu\left(\sum_{s=1}^{m_1} \frac{H_{1s}}{Q_1^{i_s+1}} + \sum_{t=1}^{m_2} \frac{H_{2t}}{Q_2^{j_t+1}}\right) &= \nu\left(\sum_{s=1}^{e_1} \frac{H_{1s}}{Q_1^{i_s+1}} + \sum_{t=1}^{e_2} \frac{H_{2t}}{Q_2^{j_t+1}}\right) \\ &\leq \min\{k_1(i_1 + 1), k_2(j_1 + 1)\} + c'. \end{aligned}$$

Hence, there exists a constant $c'' > 0$ so that

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

for all $0 \le i_1 \le \frac{n}{k_1} - c'', 0 \le j_1 \le \frac{n}{k_2} - c''$. Hence, by Lemma 6

$$\sum_{A \in P_n} E\left(A\left(\sum_{s=1}^{m_1} \frac{H_{1s}}{Q_1^{i_s+1}} + \sum_{t=1}^{m_2} \frac{H_{2t}}{Q_2^{j_t+1}}\right)\right) = 0,$$

which completes the proof of Lemma 41.

As in the proof of Theorem 5 we can rewrite Lemma 41 as

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

where $Y_i$ and $Z_j$ are independent random variables that are uniformly distributed on $P_{k_1}$ resp. on $P_{k_2}$.
Moreover, we need a variation of the Central Limit Theorem, of Lemma 29 as well as a variation of Lemma 30.

**Lemma 42** *Let $(\xi_n)$ and $(\zeta_n)$ be sequences of independent identically distributed random variables, independent of each other, with mean values $\mu_\xi$ resp. $\mu_\zeta$ and variances $\sigma_\xi^2$ resp. $\sigma_\zeta^2$. Define*

$$\eta_n := \frac{\xi_1 + \cdots + \xi_n - n\mu_\xi}{\sqrt{n}\sigma_\xi} \text{ and } \vartheta_n := \frac{\zeta_1 + \cdots + \zeta_n - n\mu_\zeta}{\sqrt{n}\sigma_\zeta},$$

*so that $\mathbb{E}(\eta_n) = \mathbb{E}(\vartheta_n) = 0$ and $\mathbb{V}(\eta_n) = \mathbb{V}(\vartheta_n) = 1$. Then,*

$$\lim_{n\to\infty} \mathbb{P}(\eta_n \le s, \vartheta_n \le t) = \Phi(s)\Phi(t) = \frac{1}{2\pi}\int_{-\infty}^{s}\int_{-\infty}^{t} e^{-u^2/2}e^{-v^2/2}\,du\,dv.$$

*Moreover, if the moments $\mathbb{E}(\xi_n)^{m_1}$ and $\mathbb{E}(\zeta_n)^{m_2}$ exist for all $m_1, m_2 \in \mathbb{N}$, then, as $n \to \infty$,*

$$\mathbb{E}\left(\eta_n^{m_1}\vartheta_n^{m_2}\right) = \mathbb{E}(\eta_n)^{m_1}\mathbb{E}(\vartheta_n)^{m_2} \to \frac{1}{2\pi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} s^{m_1}t^{m_2}e^{-s^2/2}e^{-t^2/2}\,ds\,dt$$

*for all $m_1, m_2 \in \mathbb{N}$.*

**Lemma 43** *Let $Y_n$ and $Z_n$ be random variables, and*

$$\widetilde{Y_n} := \frac{Y_n - \mathbb{E}Y_n}{\sqrt{\mathbb{V}Y_n}} \text{ resp. } \widetilde{Z_n} := \frac{Z_n - \mathbb{E}Z_n}{\sqrt{\mathbb{V}Z_n}}$$

*with* $\mathbb{E}\widetilde{Y_n} = \mathbb{E}\widetilde{Z_n} = 0$ *and* $\mathbb{V}\widetilde{Y_n} = \mathbb{V}\widetilde{Z_n} = 1$. *If*

$$\mathbb{E}\left[\left(\frac{Y_n - \mathbb{E}Y_n}{\sqrt{\mathbb{V}Y_n}}\right)^{m_1}\left(\frac{Z_n - \mathbb{E}Z_n}{\sqrt{\mathbb{V}Z_n}}\right)^{m_2}\right] \to \frac{1}{2\pi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} s^{m_1}t^{m_2}e^{-s^2/2}e^{-t^2/2}\,ds\,dt$$

*for every* $m_1, m_2 \in \mathbb{N}$, *then,*

$$(\widetilde{Y_n}, \widetilde{Z_n}) \xrightarrow{w} (\mathcal{N}_1(0,1), \mathcal{N}_2(0,1)),$$

*where* $\mathcal{N}_1$ *and* $\mathcal{N}_2$ *are independent of each other.*

This will show that the corresponding (normalized) joint distribution of $g_1$ and $g_2$ is asymptotically Gaussian.
It turns out that we will have to cut off the last few digits, that is, we will work with

$$\widetilde{g_1}(A) := \sum_{j_1 \le \frac{n}{k_1} - c''} g_1(D_{Q_1,j_1}(A)),$$
$$\widetilde{g_2}(A) := \sum_{j_2 \le \frac{n}{k_2} - c''} g_2(D_{Q_2,j_2}(A)),$$

where $c''$ is the constant we have obtained above. Then, Lemma 41 immediately translates into

**Lemma 44** *For all positive integers* $m_1, m_2$ *we have*

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

*for sufficiently large* $n$.

Of course, this implies that the joint distribution of $\widetilde{g_1}$ and $\widetilde{g_2}$ is asymptotically Gaussian (after normalization). Since the differences $g_1(A) - \widetilde{g_1}(A)$ and $g_2(A) - \widetilde{g_2}(A)$ are smaller than a constant, the same is true for the joint distribution of $g_1$ and $g_2$. This completes the proof of Theorem 6.

# Acknowledgements

There are several people to whom I am thankful for supporting me during the last two years in which I was working on this thesis.

First of all, I would like to thank Prof. Michael Drmota very much. Not only did he give me the opportunity to write my thesis at the Institute of Discrete Mathematics and Geometry, but he also supervised my work and supported me continuously. Thanks to him, I have learned a lot about mathematical research in general, and of course about the topic of this thesis in particular. I am also grateful to the Austrian Science Foundation FWF, grant S8302-MAT, for the additional financial support.

Furthermore, I would like to thank my family. They supported me throughout my schooling, and especially during the last seven years of studying mathematics in Vienna. Besides the Austrian Science Foundation it was mainly their financial support which allowed me to concentrate on my studies unhurriedly and without worrying about money. Due to their help I could aspire to obtain an academic education. Moreover, they always had an open ear for my problems and gave me the necessary moral support.

Last but not least I would like to thank my friends for their assistance. Especially, I am very thankful to Angelika Friedrich for proof-reading and correcting my numerous mistakes. Due to her tireless activity, this thesis has become much more readable than I would ever have accomplished to make it.

Georg Gutenbrunner

# Bibliography


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

[2] J. Bésineau. Indépendence statistique d'esembles liés a la fonction „sommes des chiffres". *Acta Arith.*, 20:401–416, 1972.

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

[4] Mireille Car. Quadratic Forms on $F_q[T]$. *J. Number Th.*, 61:145–180, 1996.

[5] J. Coquet. Sur les fonctions q-multiplicatives pseudo-aléatoires. *C.R.Acad.Sci.Paris Sér. A-B*, 282:A175–A178, 1976.

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

[7] H. Delange. Sur les fonctions $q$-additives ou $q$-multiplicatives. *Acta Arith.*, 21:285–298, 1972.

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

[9] M. Drmota. The Joint Distribution of q-Additive Functions. *Acta Arith.*, 100:17–39, 2001.

[10] M. Drmota and J. Gajdosik. The Distribution of the Sum-of-Digits Function. *J. Theor. Nombres Bordx.*, 10:17–32, 1998.

[11] M. Drmota and G. Gutenbrunner. The Joint Distribution of $Q$-additive Functions on Polynomials over Finite Fields. *J. Th. Nombres Bordeaux*, to appear.

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

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

[14] N.J. Fine. The distribution of the sum of digits (mod $p$). *Bull. Amer. Math. Soc.*, 71:651–652, 1965.

[15] A. O. Gelfond. Sur les nombres qui ont des propriétés additives et multiplicatives données. *Acta Arith.*, 13:259–265, 1968.

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

[17] D.R. Hayes. The expression of a polynomial as a sum of three irreducibles. *Acta Arith.*, 11:461–488, 1966.

[18] I. Kátai. Distribution of $q$-additive function. *Probability theory and applications, Essays to the Mem. of J. Mogyorodi, Math. Appl.*, 80:309–318, 1992.

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

[20] D.-H. Kim. On the joint distribution of $q$-additive functions in residue classes. *J. Number Theory*, 74:307–336, 1999.

[21] P. Kirschenhofer. On the variance of the sum of digits function. *Lecture Notes Math.*, 1452:112–116, 1990.

[22] B. Kovács and A. Pethő. Number systems in integral domains, especially in orders of algebraic number fields. *Acta Sci. Math. (Szeged)*, 55(3-4):287–299, 1991.

[23] Rudolf Lidl and Harald Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Application.* Cambridge University Press, 1996.

[24] E. Manstavicius. Probabilistic theory of additive functions related to systems of numerations. *Analytic and Probabilistic Methods in Number Theory, VSP, Utrecht*, pages 413–430, 1997.

[25] R. C. Mason. Diophantine Equations over Function Fields. *London Math. Soc. Lecture Notes*, 96:Cambridge University Press, 1984.

[26] Michael Rosen. *Number Theory in Function Fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[27] Klaus Schürger. *Wahrscheinlichkeitstheorie*. Lehr- und Handbücher der Statistik. R. Oldenbourg Verlag, München, 1998.

[28] H. N. Shapiro. *Introduction to the Theory of Numbers*. Wiley, New York, 1983.

[29] N. Snyder. An Alternate Proof of Mason's Theorem. *Elem. Math.*, 55:93–94, 2000.

[30] J.A. Solinas. On the joint distribution of digital sums. *J. Number Th.*, 33:132–151, 1989.

[31] W. Steiner. On the joint distribution of q-additive functions on polynomial sequences. *Theory of Stochastic Processes*, 8(24):336–357, 2002.

[32] W. A. Webb. Waring's problem in GF$[q, x]$. *Acta Arith.*, 22:207–220, 1973.

# Lebenslauf

Ich wurde am 15. November 1978 als Sohn von Theresia Gutenbrunner, geb. Diesenreiter, und Otto Gutenbrunner in Linz geboren. In den Jahren 1985-1989 besuchte ich die Volksschule in Perg, in den anschließenden 4 Jahren die Hauptschule I, ebenfalls in Perg, und danach, zwischen 1993 und 1997, das Bundesoberstufenrealgymnasium Perg, naturwissenschaftlicher Zweig. Dort legte ich am 11. Juni 1997 mit der Fachbereichsarbeit in Mathematik („Zahlentheoretische Spielereien") die Matura mit Auszeichnung ab.

Im Oktober 1997 immatrikulierte ich an der Technischen Universität Wien und inskribierte das Studium der Technischen Mathematik, Studienzweig Mathematische Computerwissenschaften. Im Oktober 1999 inskripierte ich zusätzlich noch das Zweitstudium Wirtschaftsinformatik an der Universität Wien. Außerdem absolvierte ich in meiner Studienzeit ein Industriepraktikum bei der Firma Siemens AG (Juli und August 1999), sowie je ein weiteres Praktikum am Institut für Numerische und Angewandte Mathematik der TU Wien (März bis Juni 2000) und am Institut für Biomedizinische Technik und Physik des AKH Wien (Juli 2000 bis April 2001).
Weiters war ich in den Jahren 2000 bis 2003 am Institut für Angewandte und Numerische Mathematik der Technischen Universität Wien als Studienassistent tätig; darüber hinaus im Jahr 2001 auch als Studienassistent am Institut für Softwarewissenschaft der Universität Wien.

Am 18. März 2002 schloss ich mein Mathematik-Studium mit der Diplomarbeit „Anzahlsätze für Primzahlen und Primzahlkonstellationen", durchgeführt am Institut für Algebra und Computermathematik, ab. Noch im selben Monat begann ich mein Doktoratsstudium am damaligen Institut für Geometrie (seit 1.1.2004: Institut für Diskrete Mathematik und Geometrie) unter Anleitung von Prof. Michael Drmota. In der Zeit von November 2002 bis März 2004 war ich überdies am FWF-Projekt „Statistical Properties of Number Systems", S8302-MAT, beteiligt.

Wien, am 1. Juni 2004 Georg Gutenbrunner