Polynomial Dynamics and Pseudorandomness

Dissertation

zur

Erlangung der naturwissenschaftlichen Doktorwürde (Dr. sc. nat.)

vorgelegt der

Mathematisch-naturwissenschaftlichen Fakultät

der

Universität Zürich

von

Alina Ostafe

aus

Rumänien

Promotionskomitee

Prof. Dr. Joachim Rosenthal (Leitung der Dissertation)

Prof. Dr. Markus Brodmann

Prof. Dr. Igor Shparlinski (Begutachter)

Prof. Dr. Arne Winterhof (Begutachter)

Zürich, 2010

To my parents, Paula and Dorel, to my sister Lavinia, to Daniel and to the one who is in my heart and soul...

... for a lot of support, patience and love.

Contents

Abstract

Dynamical systems generated by iterations of multivariate polynomials with slow degree growth have proved to have very interesting algebraic and number theoretic properties.

This project is concerned with the study of several aspects of dynamical systems generated by iterations of multivariate polynomials. This is a classical area of mathematics with a rich history and a variety of results, see [124, 127] and references therein. Recently, new links and applications have emerged in cryptography and Quasi–Monte Carlo methods, where such systems have been shown to provide very attractive alternatives to the classical pseudorandom number generators.

We study new classes of dynamical systems generated by iterations of multivariate polynomials which brings in new and favourable effects. We show a rather strong uniform distribution of elements of the orbits of these dynamical systems, provided these orbits are long enough. This property makes them a good building block for both pseudorandom number generation and cryptographic hash functions. Motivated by cryptographic applications, we show the absence of hidden low dimensional structures embedded in these orbits (the opposite would be detrimental for their cryptographic usability). Furthermore, [111] carries out a construction of a hash function from polynomial dynamical systems, which seems to be new and to have no close analogues in the literature. Our theoretic estimates of the distribution of elements in the orbits of polynomial iterations suggest that this construction should lead to efficient and secure hash functions. However, as is usual with cryptographic constructions, only time will tell whether this expectation is correct. In turn, the results and constructions of [107, 110, 111] motivated the work in [115], where we considered some classical number theoretic properties of our constructions, such as the patterns of quadratic residues and non–residues.

In addition, we are concerned with the algebraic properties of iterations of polynomials, such as irreducibility, which we show to have a direct effect on the quality of our constructions of pseudorandom sequences coming from polynomial dynamical systems. Unfortunately, questions of this type are notoriously hard, and the results known so far only apply to univariate quadratic polynomials, see [5, 9, 72, 73, 74]. Our main contribution to this area is a series of two papers [4, 112], which introduce to the field new tools such as the Weil bound of exponential sums and explicit bounds on the number of solutions of Diophantine equations. We are also able to characterise the irreducibility of iterates of even degree polynomials over finite fields which generalises all previous results.

Finally, we study the dynamical systems associated with Fermat quotients, which have

been introduced in our previous work, see [113], and obtain some theoretical and numerical results about various pseudorandom properties of the dynamical system naturally associated to Fermat quotients acting on the set $\{0, \ldots, p-1\}$. We also consider pseudorandom properties of Fermat quotients, such as uniform distribution, distribution with arbitrary lags and linear complexity. In the future, we plan to study the same problems for polynomial analogues of Fermat quotients.

Zusammenfassung

Für dynamische Systeme, die mit Hilfe von Iterationen von multivariaten Polynomen mit langsamem Gradwachstum erzeugt werden, liessen sich sehr interessante algebraische und zahlentheoretische Eigenschaften beweisen.

Dieses Projekt befasst sich mit dem Studium einiger Aspekte dynamischer Systeme, die mit Iterationen von multivariaten Polynomen erzeugt werden. Dieses ist ein klassisches Gebiet der Mathematik mit einer langen Geschichte und umfangreichen Resultaten, siehe [124, 127] und dort angegebenen Referenzen. Kürzlich wurden neue Verbindungen und Anwendungen zu Kryptographie und Quasi–Monte Carlo Methoden gefunden, bei denen solche Systeme sehr attraktive Alternativen zu klassischen Pseudozufallszahlengeneratoren liefern.

Wir studieren neue Klassen dynamischer Systeme, die mit Iterationen von multivariaten Polynomen erzeugt werden, was neue und positive Effekte hervorbringt. Wir beweisen ziemlich starke Gleichverteilungseigenschaften der Elemente auf den Orbits dieser dynamischen Systeme, vorausgesetzt, dass diese Orbits lang genug sind. Diese Eigenschaft macht sie zu einem guten Baustein, sowohl für die Pseudozufallszahlenerzeugung, als auch für kryptographische Hash Funktionen. Motiviert durch kryptographische Anwendungen, beweisen wir das Fehlen in diesen Orbits eingebetteter versteckter niedrig–dimensionaler Strukturen (das Gegenteil wäre schädlich für ihre kryptographische Anwendbarkeit). Weiterhin wird in [111] eine Konstruktion einer Hash Funktion aus Polynomiterationen vorgeschlagen, welche neu zu sein, und keine verwandten analogen Ergebnisse in der Literatur zu habe scheint. Unsere theoretischen Abschätzungen der Verteilung der Elemente in den Orbits von Polynomiterationen suggerieren, dass diese Konstruktion zu effizienten und sicheren Hash Funktionen führen sollte. Jedoch, wie üblich bei kryptographischen Konstruktionen, wird nur die Zeit zeigen, ob unsere Erwartung korrekt ist. Die Ergebnisse und Konstruktionen von [107, 110, 111] führten motivierten andererseits die Arbeit in [115], worin wir einige klassische zahlentheoretische Eigenschaften unserer Konstruktionen, wie z.B. das Muster quadratischer Reste und Nichtreste, betrachteten.

Des Weiteren beschäftigen wir uns ebenfalls mit den algebraischen Eigenschaften von Polynomiterationen, so wie Irreduzibilität, welche, wie wir zeigen, eine direkte Auswirkung auf die Qualität unserer Konstruktion hat. Leider sind Fragen dieser Art bekanntermassen sehr schwierig, und die einzig bis jetzt bekannten Ergebnisse beziehen sich auf quadratische univariate Polynome, siehe [5, 9, 72, 73, 74]. Unser Hauptbeitrag zu diesem Wissenschaftszweig ist eine Reihe von zwei Artikeln [4, 112], welche dem Gebiet neue Werkzeuge, wie

die Weil–Schranke für Exponentialsummen und explizite Schranken für die Lösungsanzahl Diophantischer Gleichungen, hinzufügen. Wir sind ebenfalls in der Lage, die Irreduzibilität von Iterationen von Polynomen von geradem Grad über endlichen Körpern zu charakterisieren, was alle früheren Resultate verallgemeinert.

Schliesslich studieren wir die dynamischen Systeme, die zu Fermatquotienten gehören, welche in unserer früheren Arbeit vorgestellt wurden, siehe [113], und erzielen theoretische und numerische Ergebnisse bezüglich einigen pseudozufälliger Eigenschaften der dynamischen Systeme, welche zu auf der Menge $\{0, \ldots, p-1\}$ agierenden Fermatquotienten natürlich assoziert sind. Wir betrachten auch pseudozufällige Eigenschaften von Fermatquotienten, so wie die Gleichverteilung, Verteilung mit beliebigen Abständen und lineare Komplexität. In Zukunft planen wir die gleichen Fragestellungen für die polynomialen Entsprechungen von Fermatquotienten zu studieren.

Introduction

Background and motivation

This work brings together several areas of mathematics, pure and applied, and cryptography. Namely, we combine ideas and constructions from the theory of *polynomial dynamical systems* with classical tools of *number theory* to construct, and give some quantitative estimates of their quality, various pseudorandom sequences and hash functions, which are of possible use in *quasi-Monte Carlo* methods and in *cryptography*.

More precisely, given a system of r polynomials $\mathcal{F} = \{f_1, \ldots, f_m\}$ in r variables over a ring $\mathcal{R}$ one can naturally define a dynamical system generated by its iterations:

$$f_i^{(0)} = f_i, \qquad f_i^{(k)} = f_i(f_1^{(k-1)}, \ldots, f_m^{(k-1)}), \qquad k = 1, 2, \ldots \ ,$$

for each $i = 1, \ldots, m$, see [6, 7, 8, 26, 31, 32, 48, 50, 73, 86, 124, 128, 129] and references therein for various aspects of such dynamical systems. It is also natural to consider the orbits obtained by such iterations evaluated at a certain initial value $(u_{k,1}, \ldots, u_{k,m})$.

In the special case of one linear univariate polynomial over a residue ring or a finite field such iterations, known as linear congruential generators, have been successfully used for decades in the theory of quasi-Monte Carlo methods, see [95, 96].

Unfortunately, in cryptographic settings, such linear generators have been successfully attacked [34, 53, 75, 79, 81] and thus deemed unusable for cryptographic purposes. It should be noted that nonlinear generators have also been attacked [12, 13, 55, 63], but the attacks are much weaker and do not rule out their use for cryptographic purposes (provided reasonable precautions are made). Although linear congruential generators have been used quite successfully for quasi-Monte Carlo methods, their linear structure shows in these applications too and often limits their applicability, see [95, 96].

Motivated by these potential applications, the statistical uniformity of the distribution (measured by the discrepancy) of one and multidimensional nonlinear polynomial generators have been studied in [61, 62, 99, 103, 105, 136]. However, all previously known results are nontrivial only for those polynomial generators that produce sequences of extremely large period, which could be hard to achieve in practice. The reason behind this is that typically the degree of iterated polynomial systems grows exponentially, and that in all previous results the saving over the trivial bound has been logarithmic. Furthermore, it is easy to see that in the one dimensional case (that is, for $m = 1$) the exponential growth of the degree of iterations of a nonlinear polynomial is unavoidable. One also expects the

same behaviour in the multidimensional case for "random" polynomials $f_1, \ldots, f_m$. However, for some specially selected polynomials $f_1, \ldots, f_m$ the degree may grow significantly slower, which is the underlying idea of this work.

Our results

The first chapter of the thesis is based on the series of papers [107, 108, 109, 110, 111, 114, 115]. Indeed, in Chapter 2 we describe a rather wide class of polynomial systems with polynomial growth of the degree of their iterations. Our construction resembles that of *triangular maps* of [86] but behaves quite differently; for example, triangular maps in [86] have the fastest possible degree growth.

In Section 2.2 we have considered multivariate polynomial systems $\mathcal{F} = \{f_1, \ldots, f_m\}$ of m polynomials in m variables over a finite field $\mathbb{F}_p$ having the "triangular" form

$$\begin{aligned} f_1(X_1, \ldots, X_m) &= X_1 g_1(X_2, \ldots, X_m) + h_1(X_2, \ldots, X_m), \\ f_2(X_1, \ldots, X_m) &= X_2 g_2(X_3, \ldots, X_m) + h_2(X_3, \ldots, X_m), \\ &\ldots \\ f_m(X_1, \ldots, X_m) &= g_m X_m + h_m, \end{aligned}$$

with $g_i, h_i \in \mathbb{F}_p[X_{i+1}, \ldots, X_m]$, $i = 1, \ldots, m-1$, and $g_m, h_m \in \mathbb{F}_p$, $g_m \neq 0$, and such that the polynomials g_i have the unique leading monomial which dominates the other terms in every variable. For this class of polynomials, it is shown in Section 2.2 that the degrees of the iterations of the polynomials f_i, $i = 1, \ldots, m$, grow significantly slower (polynomially) than it is usually expected (exponentially), which in turn leads to much better estimates of exponential sums, and thus of discrepancy, for vectors generated by these iterations, than in the general case, see Section 2.5.

Furthermore, it is shown in Section 2.5.3, that in the case when such a polynomial map generates a permutation of the corresponding vector space, one can get better results "on average" over all initial values. We exploit the linearity with respect to one variable and polynomial degree growth with respect to the other variables and achieve better estimates on exponential sums with a more elementary argument. We note that these results do not require any assumptions on the period length.

Although having a low discrepancy is a very important requirement on any pseudo-random number generator, this is not the only one. For example, the notion of *linear complexity* also plays an important role in this area, see [136]. Roughly speaking a high linear complexity indicates that the output sequence does not have any "hidden" linearities. Failing this properties is very undesirable for quasi-generalisedMonte Carlo applications of this generator and certainly detrimental for cryptographic purposes due to the series of attacks [34, 53, 75, 79, 81].

In Section 2.6 we study the (generalised) joint linear complexity of a class of nonlinear pseudorandom multisequences introduced in the previous sections as well as the linear complexity of its coordinate sequences. We prove lower bounds which are much stronger

than in the case of single sequences since the multidimensional case brings in new and favourable effects, see Section 2.6.2. Moreover, in Section 2.6.3 we improve the bound on the joint linear complexity in the case of permutation polynomials of maximal period over prime fields.

In Section 2.7 we continue our study of polynomial systems and we consider slightly more general polynomial dynamical systems, where at each step a different polynomial map can be used, thus extending those of Section 2.2. We use this generalisation to propose in Section 2.8 a construction of a hash function from polynomial maps.

We note that it is also very interesting to obtain bounds of character sums using our polynomial systems. In Section 2.9, we estimate multiplicative character sums along the orbits of a class of nonlinear recurrence vector sequences. In the 1-dimensional case only much weaker estimates are known and our results have no 1-dimensional analogues.

We conclude Chapter 2 with a new class of polynomial dynamical systems, see Section 2.10, and also a new approach, based on some combinatorial arguments which applies to arbitrary polynomial systems, such that their iterations on vectors in $\mathbb{F}_p^m$ generate sufficiently long trajectories, see Section 2.11.

In Chapter 3, motivated by possible applications to pseudorandom number generation, for example, see Section 2.12, we study some algebraic properties of polynomial iterations such as irreducibility. Questions of this type are notoriously hard and unfortunately at the moment there is a large gap between what is necessary for our application and what one can realistically hope to prove.

Chapter 4 is based on the series of papers [29, 113]. We consider dynamical systems generated by Fermat quotients. Fermat quotients are a celebrated number theoretic object, which appears in a surprising variety of applications, from the Fermat Last Theorem (A. Granville [58]), to the theory of algebraic number fields (Y. Ihara [68]), to algorithmic number theory and square-free testing (H. W. Lenstra [83]). In this chapter we introduce and study (theoretically and numerically) a completely new point of view on Fermat quotients, namely the dynamical system arising from iterations of Fermat quotients.

We obtain some theoretic and experimental results concerning various properties (the number of fixed points, image distribution, cycle lengths) of the dynamical system naturally associated with Fermat quotients acting on the set $\{0, \ldots, p-1\}$. In particular, we improve the lower bound of H. S. Vandiver on the image size of Fermat quotients on the above set (from $p^{1/2} - 1$ to $(1 + o(1))p(\log p)^{-2}$), see Section 4.6. We also consider pseudorandom properties of Fermat quotients such as joint distribution, distribution with arbitrary lags and linear complexity, see Sections 4.8, 4.9 and 4.10. Moreover, we analyse the lattice structure of Fermat quotients modulo p with arbitrary lags, see Section 4.11.

Future directions

There are several more projects in progress related to polynomial dynamical systems and their different applications. Some of them are ramifications of the ideas outlined in this thesis, some are principally new.

One ongoing project is based on the study of general multivariate polynomial systems and their behaviour under iterations. Intuitively, it is clear that a random polynomial under iterations has an exponential degree growth, but unfortunately no concrete results are proven in this direction. Some partial results are known for very special classes of polynomial systems which were considered in [61, 62]. In collaboration with E. Gorla, L. Ostafe and E. Pelican, we concentrate our efforts to extend the construction of [61, 62] to much more general polynomial systems. In this work, we consider systems $\mathcal{F} = \{F_1, \ldots, F_m\}$ of m polynomials in $\mathbb{F}[X_1, \ldots, X_m]$ over an arbitrary field $\mathbb{F}$ which, without loss of generality, we assume to be presented in the following "telescopic" form

$$F_i(X_1, \ldots, X_m) = \sum_{j=1}^{m} X_j G_{ij}(X_j, X_{j+1}, \ldots, X_m) + \alpha_i,$$

where

$$\alpha_i \in \mathbb{F}, \quad G_{ij} \in \mathbb{F}[X_1, \ldots, X_m], \quad i, j = 1, \ldots, m.$$

Under certain conditions on these general polynomial systems, we have been able to prove the "horizontal" degree growth, that is for any $k > l$, $\deg F_i^{(k)} > \deg F_i^{(l)}$, for any $i = 1, \ldots, m$. However, for applications to pseudorandom generators one also needs the following "vertical" degree growth: $\deg F_i^{(k)} > \deg F_j^{(k)}$, for any $m \geq j > i \geq 1$ and $k = 1, 2, \ldots$. Thus we are focusing on finding natural conditions that ensure both "horizontal" and "vertical" degree growth of the corresponding polynomial systems.

Another natural, but hard problem regarding iterations of polynomials is to be able to give a concise description of these iterations. In particular, it is natural to study the *additive complexity* of the polynomials $F_i^{(k)}$, for any $i = 1, \ldots, m$, $k = 1, 2, \ldots$, which is the smallest number of '+' signs in the formulas evaluating these polynomials. For example

$$f(x, y) = (x^2 + 2y)^{1000}(3x + y^3)^{1000} + (x^{100} + y^{200})^{10}$$

is of total degree 5000 and thus has a very long representation via the list of coefficients. However it is of additive complexity 4 and thus has a very concise representation as in the above (which also makes its evaluation at any point very efficient). It is clear that for the polynomial systems (2.1) this is easy to achieve as the degree grows polynomially, and thus the additive complexity also grows polynomially. The motivation for this work is a potential design of a new cryptographic primitive, a so-called *trap-door function*. We have been able to find some examples proving the existence of such polynomial systems. Let the polynomials $F_1, \ldots, F_m \in \mathbb{F}[X_1, \ldots, X_m]$ over an arbitrary field $\mathbb{F}$ be given by

$$F_1 = (a_1 X_1 + G(X_2, \ldots, X_m))^{s_1} + H(X_2, \ldots, X_m), \quad F_i = a_i X_2^{s_{i,2}} \ldots X_m^{s_{i,m}},$$

for $i = 2, \ldots, m$ with $G, H \in \mathbb{F}[X_2, \ldots, X_m]$, $s_1, s_{i,j} > 1$, $a_i \in \mathbb{F}^*$ for any $i = 1, \ldots, m$ and at least one $j = 2, \ldots, m$. It is very easy to see that the degree growth of the polynomials F_i is exponential, but the additive complexity is polynomial at every iteration. This example is very motivating and it is our belief that more general polynomial systems can be constructed achieving this very useful behaviour.

During our work on [107, 108, 110, 111, 114, 115] it has become clear that further progress here can only be achieved if more detailed information about the *algebraic structure* of polynomial iterates is available. Unfortunately questions of this type are notoriously hard, and the only known results apply only to univariate quadratic polynomials, see [5, 9, 72, 73, 74]. Our main contribution to this area is a series of two papers [4, 112], which introduce to the area such new tools as the Weil bound of exponential sums, and explicit bounds on the solutions of Diophantine equations. More precisely, we study the *stability* of quadratic polynomials under iterations, that is the property of polynomials to be irreducible at every iteration. In Section 3.3 we are able to prove that over $\mathbb{F}_2$ no quadratic polynomial has this property, and we extend our study to general finite fields $\mathbb{F}_q$ in Section 3.3 where we show that testing the stability can be done in finitely many steps. We conclude the chapter with Section 3.4 by showing that almost all quadratic polynomials over $\mathbb{Z}$ are stable under iterations.

Moreover, our results of [112] further motivated the authors of [57] to attack on one of the conjectures in [112] (along the lines outlined in [112]) and make a substantial step in its direction.

Standard heuristics, based on the density of irreducible polynomials suggests that one should expect that there are very few stable nonlinear polynomials over finite fields while almost all polynomials over $\mathbb{Z}$ should be stable. The result of [57] and Theorem 64 provide some theoretic evidences to these expectations, respectively. Overall, the situation is not well-understood both theoretically and heuristically. We plan to conduct an extensive series of numerical tests (at the computational facilities of Macquarie University) in order to gain better understanding, which in turn may lead to new theoretic advances.

As an independent project from this thesis, we have just started to study polynomial analogues of Fermat quotients. Let $f \in \mathbb{F}_q[X]$ be an irreducible polynomial. Then we can define the polynomial Fermat quotients of $A \in \mathbb{F}_q[X]$ modulo f as

$$Q_f(A) = (A^{q^{\deg f}-1} - 1)/f.$$

It is shown in [118] that many properties $Q_f(A)$ are similar to those of $q_p(a)$. However, as usual for function field analogues, one can get more results about $Q_f(A)$ than are currently known for $q_p(a)$. We plan to continue this line of research and the first step here is to try to obtain analogues of our results from Chapter 4. However, one of the most interesting questions is to see whether the function field scenario offers some advantages which can be exploited in order to get stronger results.

Acknowledgement

It is my pleasure to thank everyone without whom this work would not have been written.

I thank very much to my supervisors, Prof. Joachim Rosenthal and Prof. Markus Brodmann, for accepting me to the PhD program and their constant encouragement, support and advice.

I would like to thank very much Igor Shparlinski for introducing me to this beautiful subject of polynomial pseudorandom number generators, for his constant support, help and for many discussions which led to a series of papers that make the subject of this thesis. Second, I would like to thank Arne Winterhof for valuable stimulating discussions and for all the work we did in collaboration, and also for his hospitality during my visit to Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences.

I would also like to express my gratitude to all my other coauthors, Omran Ahmadi, Zhixiong Chen, Florian Luca and Elena Pelican without whom the work of my thesis would not have been possible.

I am obliged to Rafe Jones, Sergei Konyagin, Wilfried Meidl, Tauno Metsänkylä, Joseph Silverman and Daniel Sutantyo for many comments and suggestions on preliminary versions of several results. I also thank very much Daniel Perez for a careful reading of the thesis and his valuable suggestions on improving some parts of it.

I have been very lucky to meet these people (unfortunately some of them only electronically), I have learnt from them a lot.

During my doctoral studies I was supported in part by the Swiss National Science Foundation Grant 121874 and by the University of Zurich, which provided an inspiring work environment and the possibility to carry out all my work.

I am also grateful to the Fields Institute for the invitation to "Fields Cryptography Retrospective Meeting", Toronto, May 2009, its support and stimulating atmosphere which led to the initiation of some of this work. Thanks also go to the CRM, Université de Montréal, for the invitation to the "Workshop on Computer Security and Cryptography", Montréal, 12-16 April, 2010.

Chapter 1

Tools

1.1 General notation

Throughout the thesis p denotes a prime integer and $\mathbb{F}_p$ is the prime field with p elements, which we identify with the set $\{0, 1, \dots, p-1\}$. For a prime power q we use $\mathbb{F}_q$ to denote the finite field of q elements.

For a positive integer m we define

$$\mathbf{e}_m(z) = \exp(2\pi i z/m),$$

for every real z. In our results we work over finite fields, and m is chosen to be a prime p.

We recall that the notations $A = O(B)$, $B = \Omega(A)$, $A \ll B$ and $B \gg A$ are all equivalent to the assertion that the inequality $|A| \leq cB$ holds for some constant $c > 0$ (that may depend on some explicitly described parameters).

1.2 Zeros of polynomials

Let $\mathbb{F}_q$ be a finite field with q elements. We consider polynomial equations of the form

$$f(X_1, \dots, X_n) = 0,$$

where $f \in \mathbb{F}_q[X_1, \dots, X_n]$. By the number of solutions of this equation in $\mathbb{F}_q^n$ we mean the number of n-tuples $(c_1, \dots, c_n) \in \mathbb{F}_q^n$ for which $f(c_1, \dots, c_n) = 0$. In special cases one can give explicit formulas for the number of solutions, see [85], but in general one can't do better than finding estimates of this number.

We recall a well-known relation between the degree of a multivariate polynomial and the number of zeros, see [54, 85], which is an important tool in estimating exponential sums.

Lemma 1. *Let $F \in \mathbb{F}_q[X_1, \dots, X_n]$ be a polynomial in n variables of total degree at most d over a finite field $\mathbb{F}_q$. If F is not identical to zero, then the equation $f(X_1, \dots, X_n) = 0$ has at most dq^{n-1} solutions in $\mathbb{F}_q^n$.*

Proof. We follow the proof of [54, Lemma 6.44] and we prove the claim by induction on n. For $n = 1$ it is clear since a nonzero univariate polynomial of degree at most d over a field has at most d zeroes. For the induction step we write f as a polynomial in X_n with coefficients in $X_1, \ldots, X_{n-1}$:

$$f = \sum_{i=0}^{k} f_i X_n^i$$

with $f_i \in \mathbb{F}_q[X_1, \ldots, X_{n-1}]$ for $0 \leq i \leq k$ and $f_k \neq 0$. Then $\deg f_k \leq d - k$, and by the induction hypothesis, f_k has at most $(d-k)q^{n-2}$ zeros in $\mathbb{F}_q^{n-1}$, so there are at most $(d-k)q^{n-1}$ common zeros of f and f_k in $\mathbb{F}_q^n$. Moreover, for each $(c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^{n-1}$ with $f_k(c_1, \ldots, c_{n-1}) \neq 0$, the univariate polynomial

$$f(c_1, \ldots, c_{n-1}, X_n) = \sum_{i=0}^{k} f_i(c_1, \ldots, c_{n-1}) X_n^i \in \mathbb{F}_q[X_n]$$

of degree k has at most k zeros, so the total number of zeros of f in $\mathbb{F}_q^n$ is bounded by

$$(d-k)q^{n-1} + kq^{n-1} = dq^{n-1}.$$

□

1.3 Character sums and the Weil bound

1.3.1 Preliminaries

Let G be a finite abelian group (written multiplicatively) of order $|G|$ with identity element 1_G. A *character* χ of G is a homomorphism $\chi : G \to U$, where U is the multiplicative group of complex numbers of absolute value 1.

Since $\chi(1_G) = 1$, we note that for every $g \in G$, the values of χ are just $|G|$th roots of unity. Indeed, this is simple to see since

$$\chi(g)^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1,$$

for any $g \in G$.

We also note that $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_G) = 1$, and thus

$$\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)},$$

where the bar denotes complex conjugation. We denote by χ_0 the *trivial* character of G which is defined by $\chi_0(g) = 1$ for all $g \in G$. All the other characters of G are called *nontrivial* . For each character χ of G we can define the *conjugate* character $\overline{\chi}$ by $\overline{\chi}(g) = \overline{\chi(g)}$ for all $g \in G$.

It is easy to see that the set of characters of G forms an abelian group under the multiplication of characters given by

$$(\chi_1 \ldots \chi_n)(g) = \chi_1(g) \ldots \chi_n(g)$$

for any finitely many characters $\chi_1, \ldots, \chi_n$, and that this group is a finite group as it is given only by the $|G|$th roots of unity.

Example 2. *Let G be a finite cyclic group of order n, and let g be a generator of G. For a fixed integer j, $0 \leq j \leq n-1$, the function*

$$\chi_j(g^k) = \mathbf{e}_n(jk), \quad k = 0, 1, \ldots, n-1,$$

defines a character of G. On the other hand, if χ is any character of G, then $\chi(g)$ must be an nth root of unity, say $\chi(g) = \mathbf{e}_n(2\pi ij)$ for some j, $0 \leq j \leq n-1$, and it follows that $\chi = \chi_j$. Therefore, the group of characters of G consists exactly of the characters $\chi_0, \chi_1, \ldots, \chi_{n-1}$.

For a detailed presentation of character sums and their properties see [85, Chapter 5].

In a finite field $\mathbb{F}_q$ there are two finite abelian groups which are important: the additive group and the multiplicative group of the field. In this context, in Sections 1.3.2 and 1.3.3 we talk about *additive* and *multiplicative* characters, respectively.

1.3.2 Additive characters

Let p be a prime and $\mathbb{F}_q$ be a finite field of q elements of characteristic p. Here we concentrate on the additive group of $\mathbb{F}_q$.

We introduce first the following definition:

Definition 1. *Let $\mathbb{F}_{q^m}$ be a finite extension of the finite field $\mathbb{F}_q$ as a vector space over $\mathbb{F}_q$ and let $\alpha \in \mathbb{F}_{q^m}$. We define the trace $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ of α over $\mathbb{F}_q$ as*

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}.$$

If $q = p$, then $\mathrm{Tr}_{\mathbb{F}_{p^m}/\mathbb{F}_p}(\alpha)$ is called the absolute trace of α and simply denoted by $\mathrm{Tr}_{\mathbb{F}_{p^m}}(\alpha)$.

In other words, the trace of $\alpha \in \mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is the sum of the conjugates of α with respect to $\mathbb{F}_q$.

Remark 3. *It is very simple to note that the trace function $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ is a linear transformation, that is:*

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha + \beta) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) + \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta), \quad \forall \alpha \in \mathbb{F}_{q^m} \tag{1.1}$$

and

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c\alpha) = c\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha), \quad \forall c \in \mathbb{F}_q, \alpha \in \mathbb{F}_{q^m}.$$

We note that the function χ_1 defined by

$$\chi_1(c) = \mathbf{e}_p(\mathrm{Tr}(c)), \qquad \forall c \in \mathbb{F}_q \tag{1.2}$$

is a character of the additive group $\mathbb{F}_q$ due to the linearity of the trace function given by (1.1).

The characters of the additive group $\mathbb{F}_q$ are called *additive characters* of $\mathbb{F}_q$ and the character χ_1 in (1.2) is called the *canonical additive character* of $\mathbb{F}_q$. Moreover, all the additive characters of $\mathbb{F}_q$ can be expressed in terms of χ_1:

Theorem 4. *For $b \in \mathbb{F}_q$, the function χ_b with $\chi_b(c) = \chi_1(bc)$ for all $c \in \mathbb{F}_q$ is an additive character of $\mathbb{F}_q$, and every additive character of $\mathbb{F}_q$ is obtained in this way.*

For the proof of this theorem and more details about additive characters see [85, Chapter 5].

1.3.3 Multiplicative characters

Characters of the multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$ are called *multiplicative characters* of $\mathbb{F}_q$. Since $\mathbb{F}_q^*$ is a cyclic group of order $q-1$, we can determine easily its characters, see [85].

Definition 2. *A generator of the cyclic group $\mathbb{F}_q^*$ is called a primitive element of $\mathbb{F}_q$.*

Theorem 5. *Let ϑ be a fixed primitive element of $\mathbb{F}_q$. Then for each $j = 0, \ldots, q-2$, the function ψ_j with*

$$\psi_j(\vartheta^k) = \mathbf{e}_{q-1}(jk), \qquad k = 0, \ldots, q-2,$$

defines a multiplicative character of $\mathbb{F}_q$, and every multiplicative character of $\mathbb{F}_q$ is obtained in this way.

Proof. It follows from Example 2. □

Moreover, it is easy to note that the group of multiplicative characters of $\mathbb{F}_q^*$ is also a cyclic group of order $q-1$ where the identity element the trivial character ψ_0. Indeed, every character ψ_j in Theorem 5 with j relatively prime to $q-1$ is a generator of the group of multiplicative characters of $\mathbb{F}_q^*$.

We introduce the following well-known identity, see [84, Theorem 5.48].

Lemma 6. *For any elements $r, s \in \mathbb{F}_q$, and nonprincipal multiplicative character χ of $\mathbb{F}_q$, we have*

$$\sum_{a \in \mathbb{F}_q} \chi(a+r)\overline{\chi}(a+s) = \begin{cases} q-1, & \text{if } r = s, \\ -1, & \text{if } r \neq s. \end{cases}$$

1.3.4 Exponential sums

Basic facts

We now present a short introduction to exponential sums, by emphasizing the results and techniques we need in order to develop the theory of the next chapters. For this brief introduction we follow [123] which gives a very good insight into this subject; for more systematic approaches see [70, 78, 85].

It is well known that for many years number theory was the main area of applications of exponential sums. Such striking applications include (but are not limited to):

- Uniform distribution (H. Weyl);

- Additive problems with primes and integers such as the Goldbach and Waring problems (G. H. Hardy, J. E. Littlewood, R. Vaughan, I. M. Vinogradov);

- Riemann zeta function and distribution of prime numbers (J. E. Littlewood, N. M. Korobov, Yu. V. Linnik, E. C. Titchmarsh, I. M. Vinogradov).

However, it has turned out that exponential sums provide a valuable tool for a variety of problems of theoretical computer science, coding theory and cryptography, see [121, 122].

Exponential sums are objects of the form

$$S(\mathcal{X}, F) = \sum_{x \in \mathcal{X}} \mathbf{e}(F(x))$$

where

$$\mathbf{e}(z) = \exp(2\pi i z),$$

$\mathcal{X}$ is an arbitrary finite set, F is a real-valued function on $\mathcal{X}$.

If $\mathcal{X}$ is a set of vectors, we talk about *multiple sums*. In particular, in the two-dimensional case we talk about *double sums* which provides an invaluable tool in estimating one-dimensional sums.

In our case, very often $\mathcal{X}$ is a subset of the elements of a finite field $\mathbb{F}_q$ of q elements or vectors of $\mathbb{F}_q^m$ for some $m \geq 1$.

Certainly it would be very good to have a closed form expression for the sums $S(\mathcal{X}, F)$. Unfortunately, there are very few examples when we have such formulas. On the other hand, for main applications of exponential sums we do not need to know $S(\mathcal{X}, F)$ exactly. It is quite enough to have an *upper bound* on $S(\mathcal{X}, F)$, which is the main task of this area.

First of all we remark that because $|\mathbf{e}(z)| = 1$ for every real z,

$$|S(\mathcal{X}, F)| \leq \#\mathcal{X}.$$

This is the *trivial bound*.

We are interested in getting stronger bounds. Of course, to be able to prove such a bound we need some conditions on $\mathcal{X}$ and F. For example, if F is an integer-valued function, then $\mathbf{e}(F(x)) = 1$ and $S(\mathcal{X}, F) = \#\mathcal{X}$.

Accordingly, a very important class of exponential sums consists of *rational sums*. These are the sums with functions F of the form $F(x) = f(x)/m$ where $f : \mathcal{X} \to \mathbb{Z}$ is an integer-valued function on $\mathcal{X}$. The positive integer m is called the *denominator* of the exponential sum $S(\mathcal{X}, F)$.

Therefore we study sums of the form

$$S(\mathcal{X}, F) = \sum_{x \in \mathcal{X}} \mathbf{e}_m(f(x)).$$

In fact, we concentrate only on the case of prime denominators. Sometimes it is convenient to think that $f(x)$ is defined on elements of the finite field $\mathbb{F}_p$ of p elements.

Complete and Incomplete Exponential Sums

Very often the function $f(x)$ in $F(x) = f(x)/m$ is purely periodic modulo m with period T. Then the sum

$$S(f) = \sum_{x=1}^{T} \mathbf{e}_m(f(x))$$

is called a *complete sum*.

A shorter sum

$$S(f, N) = \sum_{x=1}^{N} \mathbf{e}_m(f(x))$$

with $1 \le N \le T$ is called an *incomplete sum*.

Linear sums

Certainly the simplest (and easiest) exponential sums one can think of are *linear exponential sums*, that is, exponential sums with

$$F(x) = ax/m.$$

The following simple result gives a complete description of such sums.

Theorem 7. *We have,*

$$\sum_{x=0}^{m-1} \mathbf{e}_m(ax) = \begin{cases} 0, & \text{if } a \not\equiv 0 \pmod m, \\ m, & \text{if } a \equiv 0 \pmod m. \end{cases}$$

Proof. The case $a \equiv 0 \pmod m$ is obvious because each term is equal to 1.

The case $a \not\equiv 0 \pmod m$ ... is obvious as well, because it is a sum of a geometric progression with quotient $q = \mathbf{e}_m(a) \ne 1$, thus

$$\sum_{x=0}^{m-1} \mathbf{e}_m(ax) = \sum_{x=0}^{m-1} q^x = \frac{q^m - 1}{q - 1} = \frac{\mathbf{e}_m(ma) - 1}{\mathbf{e}_m(a) - 1} = \frac{1 - 1}{\mathbf{e}_m(a) - 1} = 0.$$

□

Although this result is very simple, it has proved to be an invaluable tool for many applications of exponential sums. In particular, we repeatedly use it in our results. In fact, this fact is not so surprising if one thinks of the exponential sum of Theorem 7 as the characteristic function of the numbers which are divisible by m.

For other interesting results regarding exponential sums see [123].

Estimating double sums

Here we show that sometimes it is beneficial to *extend* our sum over a small set of arbitrary structure to a bigger set (just potentially increasing the size of the sum) with a nice well-studied structure. Certainly we cannot do this with the original sum because the terms are complex numbers, but this idea can be combined with some tricks, see [123]. Very often it is used together with the Cauchy inequality in the form

$$\left(\sum_{j=1}^{m} s_j\right)^2 \le m \sum_{j=1}^{m} s_j^2$$

which holds for any real $s_1, \dots, s_m$.

We demonstrate this principle on the following very important example. Let $\mathcal{X}$ and $\mathcal{Y}$ be arbitrary subsets of $\mathbb{F}_p$.

Define

$$W_c = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \mathbf{e}_p(cxy).$$

Trivially $|W_c| \le \#\mathcal{X}\#\mathcal{Y}$. We show that very simple arguments allow us to obtain a bound which is better than trivial for $\#\mathcal{X}\#\mathcal{Y} \ge p$, see [123, Theorem 4.1].

Theorem 8. *For any sets $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{F}_p$ and $1 \le c < p$,*

$$|W_c| \le \left(\#\mathcal{X}\#\mathcal{Y}p\right)^{1/2}.$$

Proof. We have

$$|W_c| = \left|\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \mathbf{e}_p(cxy)\right| \le \sum_{x \in \mathcal{X}} \left|\sum_{y \in \mathcal{Y}} \mathbf{e}_p(cxy)\right|.$$

From the Cauchy inequality,

$$|W_c|^2 \le \#\mathcal{X} \sum_{x \in \mathcal{X}} \left|\sum_{y \in \mathcal{Y}} \mathbf{e}_p(cxy)\right|^2.$$

We *extend* the sums over x to all $x \in \mathbb{F}_p$:

$$|W_c|^2 \le \#\mathcal{X} \sum_{x \in \mathbb{F}_p} \left|\sum_{y \in \mathcal{Y}} \mathbf{e}_p(cxy)\right|^2.$$

This is a very important step and seemingly wasteful step as we add many more terms to our sums (which we can do because each term is nonnegative). Of course we lose here, but our gain is that the sum over x (taken from some mysterious set we have no information about) is now extended to a very nice set.

Now we derive:

$$\begin{aligned}\sum_{x\in\mathbb{F}_p}\left|\sum_{y\in\mathcal{Y}}\mathbf{e}_p(cxy)\right|^2 &= \sum_{x\in\mathbb{F}_p}\sum_{y_1,y_2\in\mathcal{Y}}\mathbf{e}_p\left(cx\left(y_1-y_2\right)\right)\\ &= \sum_{y_1,y_2\in\mathcal{Y}}\sum_{x\in\mathbb{F}_p}\mathbf{e}_p\left(cx\left(y_1-y_2\right)\right)\\ &= p\sum_{\substack{y_1,y_2\in\mathcal{Y}\\ y_1=y_2}}1=\#\mathcal{Y}p,\end{aligned}$$

which concludes the proof. □

Without any assumptions on $\mathcal{X}$ and $\mathcal{Y}$ this bound remains the best possible.

The previous principle works for double sums. In the next chapters we show how we can create multiple *clones* of our exponential sums and thus reduce them to double sums which we can estimate by several well-known methods.

1.3.5 The Weil bound for additive and multiplicative characters

One of our main tools is also the Weil bound on exponential sums that we present in the following form given by [94, Theorem 2].

Lemma 9. *For any polynomials $f, g \in \mathbb{F}_p[X]$ over a field $\mathbb{F}_p$ of p elements, such that the rational function $F(X) = f(X)/g(X)$ is not constant on $\mathbb{F}_p$, we have the bound*

$$\left|\sum_{\substack{x\in\mathbb{F}_p\\ g(x)\neq 0}}\mathbf{e}_p(F(x))\right| \leq (\max\{\deg f, \deg g\} + r - 2)p^{1/2} + \delta,$$

where

$$(r,\delta) = \begin{cases}(s,1), & \text{if } \deg f \leq \deg g,\\ (s+1,0), & \text{if } \deg f > \deg g,\end{cases}$$

and s is the number of distinct zeros of $g(X)$ in the algebraic closure of $\mathbb{F}_p$.

In the special case when $f(X)$ is a nonconstant polynomial of degree $\deg f = n$, the bound takes its well-known form

$$\left|\sum_{x\in\mathbb{F}_p}\mathbf{e}_p\left(f(x)\right)\right| \leq (n-1)\,p^{1/2}.$$

Moreover, we have a similar bound for multiplicative character sums, see [85, Theorem 5.41].

Theorem 10. *Let ψ be a multiplicative character of $\mathbb{F}_q$ of order $m > 1$ and let $f \in \mathbb{F}_q[X]$ be a monic polynomial of positive degree that is not an mth power of a polynomial. Let d be the number of distinct roots of f in its splitting field over $\mathbb{F}_q$. Then for every $a \in \mathbb{F}_q$ we have*

$$\left|\sum_{x\in\mathbb{F}_q} \psi(af(x))\right| \le (d-1)q^{1/2}.$$

One tool that we need is the following result on character sums:

Lemma 11. *Let $g \in \mathbb{F}_q^*$ be an element of order t and $A, B \in \mathbb{F}_q^*$. Then for any nontrivial multiplicative character of $\mathbb{F}_q$, and integer a, we have*

$$\left|\sum_{n=0}^{t-1} \chi(Ag^n + B)\mathbf{e}_t(an)\right| \ll q^{1/2}.$$

Proof. Clearly there is a primitive root $\vartheta \in \mathbb{F}_q^*$ such that $g = \vartheta^s$ where $s = (q-1)/t$. Furthermore, for $x = g^n$ the function

$$\psi(x) = \mathbf{e}_{q-1}(an)$$

is obviously a multiplicative character of $\mathbb{F}_q^*$.

We now write

$$\begin{aligned}\sum_{n=0}^{t-1} \chi(Ag^n + B)e^{2\pi ian/t} &= \sum_{n=0}^{t-1} \chi(A\vartheta^{sn} + B)e^{2\pi iasn/(q-1)}\\ &= \frac{1}{s}\sum_{n=0}^{q-1} \chi(A\vartheta^{sn} + B)e^{2\pi iasn/(q-1)}\\ &= \frac{1}{s}\sum_{x\in\mathbb{F}_q^*} \chi(Ax^s + B)\psi(x^s).\end{aligned}$$

Since the polynomial $AX^s + B \in \mathbb{F}_q[X]$ has no multiple roots and $B \neq 0$ we see that

$$\sum_{x\in\mathbb{F}_q^*} \chi(Ax^s + B)\psi(x^s) \ll sq^{1/2}$$

by the Weil bound on multiplicative character sums, see Theorem 10. The result now follows. □

Using the standard technique of relating complete and incomplete sums, see [70], we now obtain the following generalisation of a result of [38] (which is formulated only for prime fields but certainly the proof extends to arbitrary finite fields without any changes).

Lemma 12. *Let $g \in \mathbb{F}_q^*$ be an element of order t and $A, B \in \mathbb{F}_q^*$. Then for any nontrivial multiplicative character of $\mathbb{F}_q$, and integer $N \le t$, we have*

$$\left|\sum_{n=0}^{N-1} \chi(Ag^n + B)\right| \ll q^{1/2} \log t.$$

We now combine Lemma 11 (with $a = 0$) and Lemma 12 in a convenient form for our applications.

Corollary 13. *Let $g \in \mathbb{F}_q^*$ be an element of order t and $A, B \in \mathbb{F}_q^*$. Then we have for any nontrivial multiplicative character of $\mathbb{F}_q$, and any integer N,*

$$\left|\sum_{n=0}^{N-1} \chi(Ag^n + B)\right| \ll Nt^{-1}q^{1/2} + q^{1/2} \log t.$$

1.4 Discrepancy and the Erdős-Turán-Koksma inequality

Given a sequence Γ of N points

$$\Gamma = \left\{(\gamma_{n,0}, \ldots, \gamma_{n,s-1})_{n=0}^{N-1}\right\} \tag{1.3}$$

in the s-dimensional unit cube $[0,1)^s$ it is natural to measure the level of its statistical uniformity in terms of the *discrepancy* $\Delta_N(\Gamma)$. More precisely,

$$\Delta_N(\Gamma) = \sup_{B \subseteq [0,1)^s} \left|\frac{T_\Gamma(B)}{N} - |B|\right|,$$

where $T_\Gamma(B)$ is the number of points of Γ inside the box

$$B = [\alpha_1, \beta_1) \times \ldots \times [\alpha_s, \beta_s) \subseteq [0,1)^s$$

and the supremum is taken over all such boxes, see [43, 80].

We recall that the discrepancy is a widely accepted quantitative measure of uniformity of distribution of sequences, and thus good pseudorandom sequences should (after an appropriate scaling) have a small discrepancy, see [95, 96].

For an integer vector $\mathbf{a} = (a_0, \ldots, a_{s-1}) \in \mathbb{Z}^s$ we put

$$|\mathbf{a}| = \max_{j=0,\ldots,s-1} |a_j|, \qquad r(\mathbf{a}) = \prod_{j=0}^{s-1} \max\{|a_j|, 1\}.$$

Typically the bounds on the discrepancy of a sequence are derived from bounds of exponential sums with elements of this sequence. The relation is made explicit in the celebrated *Erdős-Turán-Koksma inequality*, see [43, Theorem 1.21], which we present in the following form.

Lemma 14. *For any integer $L > 1$ and any sequence Γ of N points* (1.3) *the discrepancy $\Delta_N(\Gamma)$ satisfies the following bound:*

$$\Delta_N(\Gamma) \le \left(\frac{3}{2}\right)^s \left(\frac{2}{L+1} + \frac{1}{N} \sum_{0<|\mathbf{a}|\le L} \frac{1}{r(\mathbf{a})} \left| \sum_{n=0}^{N-1} \exp\left(2\pi i \sum_{j=0}^{s-1} a_j \gamma_{n,j}\right) \right| \right).$$

The law of the iterated logarithm, see [96, Equation (7.4)], asserts that the order of magnitude of the discrepancy of N points in $[0,1)^s$ should be around $N^{-1/2}(\log\log N)^{1/2}$. Accordingly, as a measure of randomness of a pseudorandom sequence, one investigates the discrepancy of s-tuples of consecutive terms, see [96, 43] and the references therein.

1.5 Linear complexity

In this section we follow [136, 140] to outline some basic facts regarding *linear complexity* and *linear complexity profile*, which are not only important measures of predictability of a given sequence, and thus suitable for cryptographic purposes, but also of interest for coding theory, information theory, Monte-Carlo simulations, etc.

Definition 3. *A sequence (s_n) of elements of the finite field $\mathbb{F}_q$ of q elements is called a linear recurring sequence of order k if there exist $c_0, \ldots, c_{k-1} \in \mathbb{F}_q$ satisfying the linear recurrence of order k over $\mathbb{F}_q$:*

$$s_{n+k} = c_{k-1}s_{n+k-1} + c_{k-2}s_{n+k-2} + \ldots + c_0 s_n, \quad n = 0, 1, \ldots.$$

Now let (s_n) be a sequence over $\mathbb{F}_q$. One can associate to it a non-decreasing sequence $\mathcal{L}(s_n, N)$ of non-negative integers as follows:

Definition 4. *The linear complexity profile of the sequence (s_n) over $\mathbb{F}_q$ is the sequence $\mathcal{L}(s_n, N)$, $N \ge 1$, where it's Nth term is defined to be the smallest L such that a linear recurrence of order L over $\mathbb{F}_q$ can generate the first N terms of (s_n).*

We use the convention that $\mathcal{L}(s_n, N) = 0$ if the first N elements of (s_n) are all zero and $\mathcal{L}(s_n, N) = N$ if the first $N-1$ elements of (s_n) are zero and $s_{N-1} \ne 0$.

Definition 5. *The value*

$$\mathcal{L}(s_n) = \sup_{N \ge 1} \mathcal{L}(s_n, N),$$

is called the linear complexity over $\mathbb{F}_q$ of the sequence (s_n).

If (s_n) is a periodic sequence of period t, then one can easily verify that

$$\mathcal{L}(s_n) = \mathcal{L}(s_n, 2t) \le t.$$

Mainly, the linear complexity (profile) is an important cryptographic characteristic of sequences (see the monographs and surveys [33, 92, 97, 98, 117, 136]). A low linear complexity profile has turned out to be undesirable for cryptographic applications as stream ciphers.

Example 15 (Stream Cipher)**.** *We consider a message $m_0, m_1, \ldots$ represented as a sequence over $\mathbb{F}_q$. In a* stream cipher *each message symbol m_j is enciphered with an element x_j of another sequence $x_0, x_1, \ldots$ over $\mathbb{F}_q$, the* key stream*, by*

$$c_j = m_j + x_j.$$

The cipher text $c_0, c_1, \ldots$ can be deciphered by subtracting the key stream

$$m_j = c_j - x_j.$$

The security of such a stream cipher depends on the unpredictability of the key stream. Since a sequence of small linear complexity is highly predictable, a high linear complexity of the sequence (x_n) is necessary (but not sufficient).

Linear complexity and linear complexity profile of a given sequence can be determined using the well-known Berlekamp-Massey algorithm, see [140, Theorem 1.1]. Unfortunately, the algorithm is efficient for sequences with low linear complexity and hence such sequences can easily be predicted. One typical example is the so-called *linear congruential generator*

$$s_{n+1} \equiv as_n + b \pmod{m},$$

for $a, b \in \mathbb{F}_q, a \neq 0$, and some initial value $s_0 \in \mathbb{F}_q$, which satisfies $L(s_n) \leq 2$. In fact the linear congruential generator is predictable even if only some parts of the sequence are exhibited, for example, only a short string of k most significant bits, see [53, 75, 79, 81]. Furthermore, this generator can be attacked and predicted even in the case when the modulus m is hidden too, see [34, 75].

Moreover, [140, Theorem 1.1] gives us the following relation between consecutive terms in the sequence $\mathcal{L}(s_n, N)$ for a sequence (s_n) in $\mathbb{F}_q$.

Theorem 16. *If $\mathcal{L}(s_n, N) > N/2$, then we have*

$$\mathcal{L}(s_n, N+1) = \mathcal{L}(s_n, N).$$

If $\mathcal{L}(s_n, N) \leq N/2$, then we have either

$$\mathcal{L}(s_n, N+1) = \mathcal{L}(s_n, N)$$

or

$$\mathcal{L}(s_n, N+1) = N + 1 - \mathcal{L}(s_n, N).$$

The expected values of linear complexity and linear complexity profile show that a 'random' sequence should have $\mathcal{L}(s_n, N)$ close to $\min\{N/2, t\}$ for all $N \geq 1$, see [140, Lemma 1.1].

Lemma 17. *If $\mathcal{L}(s_n, N) \leq N/2$ then there is a unique linear recurrence of shortest length for the first N sequence elements of (s_n), that is, for $L = \mathcal{L}(s_n, N)$ the coefficients $c_0, \ldots, c_{L-1} \in \mathbb{F}_q$ in the recurrence relation*

$$s_{n+L} = c_{L-1}s_{n+L-1} + c_{L-2}s_{n+L-2} + \cdots + c_0 s_n, \ n = 0, 1, \ldots \tag{1.4}$$

are uniquely defined.

Proof. Assume we have two different linear recurrences of the form (1.4) for the first N sequence elements of (s_n) with coefficients $c_0, \ldots, c_{L-1}$ respectively $d_0, \ldots, d_{L-1}$. Put

$$k = \max\{j \ : \ c_j \neq d_j\},$$

such that $0 \leq k \leq L-1$. Comparing the right hand sides in (1.4) yields

$$(c_0 - d_0)s_n + \cdots + (c_k - d_k)s_{n+k} = 0, \quad 0 \leq n \leq N - L - 1.$$

Since $c_k - d_k \neq 0$ this is a linear recurrence of order k for the first $N - (L-k)$ sequence elements of (s_n) and thus

$$\mathcal{L}(s_n, N - (L-k)) \leq k. \tag{1.5}$$

Hence, $\mathcal{L}(s_n, N-(L-k)) < \mathcal{L}(s_n, N)$ and there exists a smallest positive index $j \leq L-k$ with $\mathcal{L}(s_n, N-(L-k)+j) > \mathcal{L}(s_n, N-(L-k))$. Applying the second part of Theorem 16 gives

$$\mathcal{L}(s_n, N-(L-k)+j) = N-(L-k)+j-\mathcal{L}(s_n, N-(L-k)).$$

Form (1.5) and $L \leq N/2$ we get

$$\mathcal{L}(s_n, N-(L-k)+j) \geq N - L + j \geq N/2 + j.$$

Since $N-(L-k)+j \leq N$ we have $\mathcal{L}(s_n, N) = L \geq N/2 + j$ in contradiction to $L \leq N/2$. □

Chapter 2

On the degree growth of polynomial dynamical systems and their applications

2.1 Introduction

Let $\mathcal{F} = \{f_0, \ldots, f_m\}$ be a system of $m+1$ polynomials in $m+1$ variables over an arbitrary field. One can naturally define a dynamical system generated by its iterations, see [48, 128] and references therein for various aspects of such dynamical systems, and consider the orbits obtained by such iterations evaluated at a certain initial value $(v_0, \ldots, v_m)$. The statistical uniformity of the distribution (measured by the discrepancy) of one and multidimensional nonlinear polynomial generators over a finite field have been studied in [61, 62, 103, 105, 136]. However, almost all previously known results are nontrivial only for those polynomial generators that produce sequences of extremely large period, which could be hard to achieve in practice (the only known exceptions are generators from inversions [101], power functions [52], Dickson polynomials [56] and Redei functions [64]). The reason behind this is that typically the degree of iterated polynomial systems grows exponentially, and that in all previous results the saving over the trivial bound has been logarithmic. Furthermore, it is easy to see that in the one-dimensional case (that is, for $m = 0$) the exponential growth of the degree of iterations of a nonlinear polynomial is unavoidable. One also expects the same behaviour in the multidimensional case for "random" polynomials $f_0, \ldots, f_m$. However, as we saw in [110], for some specially selected polynomials $f_0, \ldots, f_m$ the degree may grow significantly slower.

Indeed, in this chapter we describe a rather wide class of polynomial systems with polynomial growth of the degree of their iterations (see Section 2.2). As a result, in Section 2.5 we obtain much better estimates of exponential sums, and thus of discrepancy, for vectors generated by these iterations, with a saving over the trivial bound being a power of p.

We remark that in the heart of all known approaches to estimate exponential sums

and discrepancy of sequences generated by polynomial iterations is the idea of [99] which requires to estimate exponential sums with polynomials $F_{\mathbf{a},k_1,\ell_1,\ldots,k_\nu,\ell_\nu}$ described in Corollary 20 below. In order to apply the Weil bound (see Lemma 9) one needs to show that the polynomial is not a constant, for most of the choices of the parameters $k_1, \ell_1, \ldots, k_\nu, \ell_\nu$. One of the ways to guarantee this is to ensure that degrees of the iterations $F_i^{(k)}$ grow doubly monotonically with respect to both i and k and thus after all obvious cancellations there is always a polynomial $F_i^{(h)}$ of degree higher than all other polynomials. However, if the degrees grow too fast, then the Weil bound gives a rather week result. So the challenge, solved in [110], has been to construct polynomials systems where the degrees grow at rather mild rate. On the other hand, we also note that in [109] we have developed an approach that does not use the degree argument, see Section 2.11.

Recently, multisequences have gained increasing interest for applications in cryptography and quasi-Monte Carlo methods. We study the (generalisfavourableed) joint linear complexity of a class of nonlinear pseudorandom multisequences generated by polynomial systems introduced in Section 2.2 as well as the linear complexity of its coordinate sequences. We prove lower bounds which are much stronger than in the case of single sequences since the multidimensional case brings in new and favourable effects.

Using our construction of dynamical systems, in Section 2.8 we design a new class of hash functions from iterations of polynomials and use our estimates to motivate their "mixing" properties.

We continue the study of these systems by estimating in Section 2.9 multiple multiplicative character sums along the orbits of multivariate polynomial recurrence sequences. Such estimates are known in the univariate case, however our results have no univariate analogues. Finally, we end this chapter by proposing in Sections 2.10, 2.12 other interesting constructions for pseudorandom vectors and pointing some open questions related to our study.

2.2 Construction and degree estimates

The construction of the following class of polynomial systems was first considered in [110]. Let $\mathbb{F}$ be an arbitrary field of characteristic p (or of zero characteristic) and let $\mathcal{F} = \{f_0, \ldots, f_m\}$ be a system of $m+1$ polynomials in $\mathbb{F}[X_0, \ldots, X_m]$ defined in the following way:

$$\begin{aligned} F_0(X_0, \ldots, X_m) &= X_0 G_0(X_1, \ldots, X_m) + H_0(X_1, \ldots, X_m), \\ F_1(X_0, \ldots, X_m) &= X_1 G_1(X_2, \ldots, X_m) + H_1(X_2, \ldots, X_m), \\ &\ldots \\ F_{m-1}(X_0, \ldots, X_m) &= X_{m-1} G_{m-1}(X_m) + H_{m-1}(X_m), \\ F_m(X_0, \ldots, X_m) &= g_m X_m + h_m, \end{aligned} \tag{2.1}$$

where

$$g_m, h_m \in \mathbb{F}, \quad g_m \neq 0, \quad G_i, H_i \in \mathbb{F}[X_{i+1}, \ldots, X_m], \quad i = 0, \ldots, m-1.$$

We also impose the condition that each polynomial G_i has *unique leading monomial* $X_{i+1}^{s_{i,i+1}} \dots X_m^{s_{i,m}}$, that is, for some $g_i \neq 0$,

$$G_i(X_{i+1}, \dots, X_m) = g_i X_{i+1}^{s_{i,i+1}} \dots X_m^{s_{i,m}} + \widetilde{G_i}(X_{i+1}, \dots, X_m), \tag{2.2}$$

where

$$g_i \in \mathbb{F}^*, \qquad \deg_{X_j} \widetilde{G_i} < s_{i,j}, \qquad \deg_{X_j} H_i \leq s_{i,j}, \tag{2.3}$$

for $i = 0, \dots, m-1$, $j = i+1, \dots, m$.

We define the degree of the polynomial system $\mathcal{F}$ to be the integer $\max\{\deg F_i \ : \ i = 0, \dots, m\}$, where $\deg F_i$ denotes the total degree of F_i.

For each $i = 0, \dots, m$ we define the k-th iteration of the polynomials F_i by the recurrence relation

$$F_i^{(0)} = X_i, \quad F_i^{(k)} = F_i(F_0^{(k-1)}, \dots, F_m^{(k-1)}), \quad k = 1, 2, \dots . \tag{2.4}$$

We denote by $d_{k,i}$ the degree of the polynomial $F_i^{(k)}$, $i = 0, \dots, m$. We also consider the vector of the degrees of the iterations

$$\mathbf{d}_k = (d_{k,0} \dots, d_{k,m}),$$

and the upper triangular matrix

$$S = \begin{pmatrix} 1 & s_{0,1} & s_{0,2} & \dots & s_{0,m} \\ 0 & 1 & s_{1,2} & \dots & s_{1,m} \\ & & \dots & & \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

given by the exponents of the leading monomials in f_i, $i = 0, \dots, m$. We observe that under iterations we have

$$\begin{aligned} F_i^{(k)} &= F_i^{(k-1)} G_i(F_{i+1}^{(k-1)}, \dots, F_m^{(k-1)}) + H_i(F_{i+1}^{(k-1)}, \dots, F_m^{(k-1)}), \\ & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad i = 0, \dots, m-1, \\ F_m^{(k)} &= a F_m^{(k-1)} + b, \end{aligned}$$

and using the conditions on the degrees of the polynomials G_i and H_i we get

$$\begin{aligned} d_{k,i} &= d_{k-1,i} + s_{i,i+1} d_{k-1,i+1} + \dots + s_{i,m} d_{k-1,m}, \qquad i = 0, \dots, m-1, \\ d_{k,m} &= 1. \end{aligned}$$

Using the above notations, the degrees of the iterations satisfy the relation

$$\mathbf{d}_k = S \mathbf{d}_{k-1}, \qquad k \geq 0 \qquad \text{and} \qquad \mathbf{d}_{-1} = (1, \dots, 1)^t$$

which is equivalent to writing

$$\mathbf{d}_k = S^{k+1} (1 \dots, 1)^t, \qquad k \geq 0. \tag{2.5}$$

We now show that the degrees of the iterations of $\mathcal{F}$ grow polynomially.

Lemma 18. *Let $F_0, \ldots, F_m \in \mathbb{F}[X_0, \ldots, X_m]$ be as in* (2.1)*, satisfying the conditions* (2.2) *and* (2.3)*. Then for $i = 0, \ldots, m$ and $k = 0, 1, \ldots$, for the polynomials $F_i^{(k)}$ given by* (2.4) *we have*

$$F_i^{(k)} = X_i G_{i,k}(X_{i+1}, \ldots, X_m) + H_{i,k}(X_{i+1}, \ldots, X_m),$$

where for $i = 0, 1, \ldots, m-1$, $G_{i,k}, H_{i,k} \in \mathbb{F}[X_{i+1}, \ldots, X_m]$ and

$$\deg G_{i,k} \;=\; \frac{1}{(m-i)!} k^{m-i} s_{i,i+1} \ldots s_{m-1,m} + \psi_i(k),$$

and $0 \neq G_{m,k} \in \mathbb{F}$, where $\psi_i(T) \in \mathbb{Q}[T]$ is a polynomial of degree $\deg \psi_i < m - i$, $i = 0, 1, \ldots, m-1$.

Proof. Using (2.5), an easy inductive argument implies that

$$F_i^{(k)} = X_i G_{i,k}(X_{i+1}, \ldots, X_m) + H_{i,k}(X_{i+1}, \ldots, X_m)$$

for some polynomials $G_{i,k}, H_{i,k} \in \mathbb{F}[X_{i+1}, \ldots, X_m]$, with $\deg G_{i,k} \geq \deg H_{i,k}$, where $i = 0, \ldots, m$, $k = 1, 2, \ldots$.

We use induction on m. For $m = 1$ one can easily see that we get

$$d_{k,0} = k s_{0,1} + s_{0,1} + 1 \qquad \text{and} \qquad d_{k,1} = 1.$$

We assume the result true for m indeterminates. Let S be the matrix of exponents of the leading monomials in $\mathcal{F}$ as above. We write S in the following way

$$S = \begin{pmatrix} R & \mathbf{s} \\ 0 & 1 \end{pmatrix},$$

where R is the matrix given by the exponents of the first m indeterminates in the leading monomials of f_i, $i = 0, \ldots, m-1$, and $\mathbf{s} = (s_{0,m}, \ldots, s_{m-1,m})$. For a vector $\mathbf{v} \in \mathbb{F}^m$ we use $\mathbf{v}^t$ and $\mathbf{v}_i$ to denote the transpose and the ith component of $\mathbf{v}$, respectively. We also denote by $\mathbf{e}$ the unit vector $\mathbf{e} = (1, \ldots, 1) \in \mathbb{F}^m$. Using these notations and recalling (2.5), we obtain

$$\mathbf{d}_k = S^{k+1}\mathbf{e}^t = \begin{pmatrix} R^{k+1} & (R^k + \ldots + R + I)\mathbf{s}^t \\ 0 & 1 \end{pmatrix} \mathbf{e}^t.$$

Componentwise, we have

$$\begin{aligned} d_{k,i} &= \left(R^{k+1}\mathbf{e}^t\right)_i + \left((R^k + \ldots + R + I)\mathbf{s}^t\right)_i, \qquad i = 0, \ldots, m-1, \\ d_{k,m} &= 1. \end{aligned}$$

It is easy to note that the maximal degree of the k^{th}-iteration of polynomials f_i for any i is given by the last position in each row of S^{k+1}. Using this remark and the induction hypothesis we get

$$(R^j \mathbf{s}^t)_i = \frac{1}{(m-1-i)!} j^{m-1-i} s_{i,i+1} \ldots s_{m-2,m-1} s_{m-1,m} + \varphi_i(j),$$

for some polynomials $\varphi_i(Z) \in \mathbb{Q}[Z]$ of degree $\deg \varphi_i < m-1-i$. Then

$$\sum_{j=0}^{k} (R^j \mathbf{s}^t)_i = \frac{1}{(m-1-i)!} s_{i,i+1} \dots s_{m-1,m} \sum_{j=0}^{k} j^{m-1-i} + \widetilde{\varphi}_i(k),$$

for some polynomials $\widetilde{\varphi}_i(Z) \in \mathbb{Q}[Z]$ of degree $\deg \widetilde{\varphi}_i < m-i$. As

$$\sum_{j=0}^{k} j^{m-1-i} = \frac{1}{m-i}(B_{m-i}(k+1) - B_{m-i}(0)),$$

where B_{m-i} is the Bernoulli polynomial of degree $m-i$ (which has the leading coefficient equal to 1), we finally obtain the desired result. □

Remark 19. *By straightforward computations it is easy to see that the polynomials $G_{i,k}$, $H_{i,k}$ in Lemma 18 are given by*

$$\begin{aligned} G_{i,k} =& G_i G_i^{(2)} \dots G_i^{(k)} \\ H_{i,k} =& H_i G_i^{(2)} \dots G_i^{(k)} + H_i^{(2)} G_i^{(3)} \dots G_i^{(k)} + \dots + H_i^{(k-1)} G_i^{(k)} + H_i^{(k)}, \end{aligned}$$

where $G_i^{(k)} = G_i(F_{i+1}^{(k-1)}, \dots, F_m^{(k-1)})$ and $H_i^{(k)} = H_i(F_{i+1}^{(k-1)}, \dots, F_m^{(k-1)})$.

Corollary 20. *Let $F_0, \dots, F_m \in \mathbb{F}[X_0, \dots, X_m]$ be as in (2.1), satisfying the conditions (2.2) and (2.3). If $s_{0,1} \dots s_{m-1,m} \neq 0$, then for any integer $\nu \geq 1$ there is a constant k_0 depending only on the matrix S and ν such that for any integers $k_1, \ell_1, \dots, k_\nu, \ell_\nu \geq k_0$ and any nonzero $\mathbf{a} = (a_0, \dots, a_{m-1}) \in \mathbb{F}^m$,*

$$F_{\mathbf{a},k_1,\ell_1,\dots,k_\nu,\ell_\nu} = \sum_{i=0}^{m-1} a_i \sum_{j=1}^{\nu} \left(F_i^{(k_j)} - F_i^{(\ell_j)} \right),$$

is a nonconstant polynomial of degree

$$\deg F_{\mathbf{a},k_1,\ell_1,\dots,k_\nu,\ell_\nu} = O(k^m),$$

where

$$k = \max\{k_1, \ell_1, \dots, k_\nu, \ell_\nu\}$$

unless the components of the vectors

$$(k_1 \dots, k_\nu) \qquad \text{and} \qquad (\ell_1 \dots, \ell_\nu)$$

are permutations of each other.

Proof. Let i_0 be the smallest integer with $a_{i_0} \neq 0$. Performing all trivial cancellations, without loss of generality we can also assume that the vectors $(k_1 \dots, k_\nu)$ and $(\ell_1 \dots, \ell_\nu)$ have no common elements. Thus the largest element amongst them k, is unique. It is now clear from Lemma 18 that the leading term of $F_{i_0}^{(k)}$ is present in $F_{\mathbf{a},k_1,\ell_1,\dots,k_\nu,\ell_\nu}$. □

2.3 Permutation polynomial systems

In order to be able to apply the technique introduced in [101] for inversive pseudorandom number generators to obtain a stronger bound on the discrepancy "on average" over all initial values, we need to work with systems of multivariate polynomials in $\mathbb{F}_q[X_0, \ldots, X_m]$ which induce maps that permute the elements of $\mathbb{F}_q^{m+1}$. Lidl and Niederreiter [84, 85] call such systems *orthogonal polynomial systems*, but we here refer to them as *permutation polynomial systems*.

Definition 6. *A system of polynomials*

$$F_0, \ldots, F_m \in \mathbb{F}_q[X_0, \ldots, X_m], \quad m \geq 1,$$

is said to be a permutation in $\mathbb{F}_q^{m+1}$ *if the system of equations*

$$F_0(X_0, \ldots, X_m) = a_0, \ldots, F_m(X_0, \ldots, X_m) = a_m$$

has one solution in $\mathbb{F}_q^{m+1}$ *for each* $(a_0, \ldots, a_m) \in \mathbb{F}_q^{m+1}$.

Let the polynomial system $\mathcal{F} = \{F_0, \ldots, F_m\}$, $m \geq 1$, be defined by (2.1) and satisfy the conditions (2.2) and (2.3). It is obvious that this system is a permutation system if and only if the polynomials g_i, $i = 0, \ldots, m$, do not have zeroes over $\mathbb{F}_q$.

We note that a "typical" absolute irreducible polynomial in $m \geq 2$ variables over $\mathbb{F}_q$ always has lots of zeros. By a special case of the Lang-Weil theorem [82] a polynomial F in $m \geq 2$ variables over $\mathbb{F}_q$ always has $rq^{m-1} + O(q^{m-3/2})$ zeros where r is the number of absolutely irreducible factors of F (with the implied constant depending only on $\deg F$), see also [119]. That is why we seek "atypical" polynomials, as the example below shows.

One of the attractive choices of polynomials which would lead to a fast PRNG is

$$G_i(X_{i+1}, \ldots, X_m) = \prod_{j=1}^{m-i} (X_{i+j}^2 - a_{i,j})$$

and

$$H_i(X_{i+1}, \ldots, X_m) = b_i$$

where $a_{i,j}$ are quadratic nonresidues and b_i are any constants in $\mathbb{F}_q$.

Even simpler, one can take

$$G_i(X_{i+1}, \ldots, X_m) = (X_{i+1}^2 - a_i)$$

where a_i are quadratic nonresidues.

2.4 Vector sequences

Let $\mathcal{F} = \{F_0, \ldots, F_m\}$ be a polynomial system in the ring $\mathbb{F}_q[X_0, \ldots, X_m]$ of the form (2.1), satisfying the conditions (2.2) and (2.3). We consider the $(m+1)$-dimensional multisequence

$$(\mathbf{w}_n) = ((u_{n,0}, \ldots, u_{n,m})) \tag{2.6}$$

defined by a recurrence relation of the form

$$u_{n+1,i} = F_i(u_{n,0}, \ldots, u_{n,m}), \qquad n = 0, 1, \ldots, \quad i = 0, 1, \ldots, m, \tag{2.7}$$

with some *initial vector* $\mathbf{w}_0 = (u_{0,0}, \ldots, u_{0,m}) \in \mathbb{F}_q^{m+1}$.

Using the following vector notation

$$\mathbf{F} = (F_0(X_0, \ldots, X_m), \ldots, F_m(X_0, \ldots, X_m)),$$

we have the recurrence relation

$$\mathbf{w}_{n+1} = \mathbf{F}(\mathbf{w}_n), \quad n = 0, 1, \ldots .$$

In particular, for any $n, k \geq 0$ and $i = 0, \ldots, m$ we have

$$u_{n+k,i} = F_i^{(k)}(\mathbf{w}_n) = F_i^{(k)}(u_{n,0}, \ldots, u_{n,m}) \tag{2.8}$$

or

$$\mathbf{w}_{n+k} = \mathbf{F}^{(k)}(\mathbf{w}_n).$$

Clearly, since $\mathbb{F} = \mathbb{F}_q$ is a finite field of q elements, then the sequence of vectors $(\mathbf{w}_n)$ is eventually periodic with some period $\tau \leq q^{m+1}$. We always assume that the sequence is purely periodic, that is,

$$\mathbf{w}_{n+\tau} = \mathbf{w}_n, \quad n = 0, 1, \ldots .$$

We sometimes discard the last component and define the truncated vectors

$$\mathbf{u}_n = (u_{n,0}, \ldots, u_{n,m-1}), \quad n = 0, 1, \ldots . \tag{2.9}$$

2.5 Discrepancy estimates for polynomial systems

2.5.1 Outline

In this section we study the distribution of vectors generated by the polynomial systems (2.1) over prime fields $\mathbb{F}_p$ and we exploit the special structure of their iterations that allows us to replace the use of the Weil bound (see [84, Chapter 5]) by a more elementary and stronger estimate on the corresponding exponential sums. This leads to better estimates on the discrepancy of the sequences generated by these systems, and thus to a

better final result and for more general systems of congruences. In fact, since our construction can easily be extended to polynomials over commutative rings, the new estimate can also be used to study polynomial maps over residue rings (while the Weil bound does not apply there). This estimate can also be used to improve and generalise the main result of [110].

Furthermore, as in [107], we also show that in the case when a polynomial map defined by (2.1) generates a permutation of the corresponding vector space, the same arguments introduced for the inversive generator in [101] allow us to obtain a stronger bound on the discrepancy "on average" over all initial values.

2.5.2 General polynomial systems

We follow the scheme previously introduced in [99, 100]. Furthermore, as it has been suggested in [105, 136], we work with higher moments of the corresponding exponential sums. However the polynomial growth of the degree allows us a much more favourable choice of parameters and thus leads to a better estimate than in previous works.

Assume that the sequence $\{\mathbf{u}_n\}$ generated by (2.7) is purely periodic with an arbitrary period τ. For integer vectors $\mathbf{a} = (a_0, \ldots, a_{m-1}) \in \mathbb{Z}^m$ and $\mathbf{b} = (b_0, \ldots, b_m) \in \mathbb{Z}^{m+1}$ we introduce the exponential sums

$$S_{\mathbf{a}}(N) = \sum_{n=0}^{N-1} \mathbf{e}_p\left(\sum_{i=0}^{m-1} a_i u_{n,i}\right) \quad \text{and} \quad T_{\mathbf{b}}(N) = \sum_{n=0}^{N-1} \mathbf{e}_p\left(\sum_{i=0}^{m} b_i u_{n,i}\right), \tag{2.10}$$

where

$$\mathbf{e}_p(z) = \exp(2\pi i z/p).$$

Clearly, if $\mathbf{b} = (a_0, \ldots, a_{m-1}, 0)$ then we simply have $S_{\mathbf{a}}(N) = T_{\mathbf{b}}(N)$, thus the sums $T_{\mathbf{b}}(N)$ are direct generalisations of the sums $S_{\mathbf{a}}(N)$ that have been treated in [107, 110]. Here we show that together with some additional arguments, one can obtain similar results for the sums $T_{\mathbf{b}}(N)$.

We need the following estimate on exponential sums which avoids using the Weil bound (see [84, Chapter 5]) and which is our main tool in improving the result of [110].

Lemma 21. *Let $\mathcal{F} = \{F_0, \ldots, F_m\}$ be a polynomial system in the ring $\mathbb{F}_p[X_0, \ldots, X_m]$ of the form (2.1), satisfying the conditions (2.2) and (2.3), with $s_{0,1} \ldots s_{m-1,m} \neq 0$. Then there is a positive integer k_0 depending only on S and m such that for any integer vectors*

$$\mathbf{k} = (k_1, \ldots, k_\nu), \quad \mathbf{l} = (l_1, \ldots, l_\nu), \quad \min\{k_1, \ldots, k_\nu, l_1, \ldots, l_\nu\} \geq k_0$$

with components that are not permutations of each other and integer vector $\mathbf{a} = (a_0, \ldots, a_{m-1})$ with

$$\gcd(a_0, \ldots, a_{m-1}, p) = 1,$$

for the polynomial

$$F_{\mathbf{a},\mathbf{k},\mathbf{l}} = \sum_{i=0}^{m-1} a_i \sum_{h=1}^{\nu} \left(F_i^{(k_h)} - F_i^{(l_h)}\right)$$

where the polynomials $F_i^{(k)}$ *are given by* (2.4)*, we have*

$$\sum_{x_0,\dots,x_m=1}^{p} \mathbf{e}_p\left(F_{\mathbf{a},\mathbf{k},\mathbf{l}}(x_0,\dots,x_m)\right) \ll K^m p^m,$$

where

$$K = \max\{k_1,\dots,k_\nu,l_1,\dots,l_\nu\}.$$

Proof. Let $s < m-1$ be the smallest integer such that $a_s \neq 0$. By Lemma 18 we have

$$\begin{aligned}
&F_{\mathbf{a},\mathbf{k},\mathbf{l}}(X_0,\dots,X_m)\\
&\quad= \sum_{i=s}^{m-1} a_i X_i \sum_{h=1}^{\nu} \left(\widetilde{G}_{k_h,i}(X_{i+1},\dots,X_m) - \widetilde{G}_{l_h,i}(X_{i+1},\dots,X_m)\right)\\
&\qquad\qquad + \sum_{i=s}^{m-1} a_i \sum_{h=1}^{\nu} \left(\widetilde{H}_{k_h,i}(X_{i+1},\dots,X_m) - \widetilde{H}_{l_h,i}(X_{i+1},\dots,X_m)\right)\\
&\quad= a_s X_s \sum_{h=1}^{\nu} \left(\widetilde{G}_{k_h,s}(X_{s+1},\dots,X_m) - \widetilde{G}_{l_h,s}(X_{s+1},\dots,X_m)\right)\\
&\qquad\qquad + \Psi_{\mathbf{a},\mathbf{k},\mathbf{l}}(X_{s+1},\dots,X_m)
\end{aligned}$$

for a certain polynomial $\Psi_{\mathbf{a},\mathbf{k},\mathbf{l}}(X_{s+1},\dots,X_m) \in \mathbb{F}_p[X_{s+1},\dots,X_m]$.

Therefore,

$$\begin{aligned}
&\sum_{x_0,\dots,x_m=1}^{p} \mathbf{e}_p\left(F_{\mathbf{a},\mathbf{k},\mathbf{l}}(x_0,\dots,x_m)\right)\\
&\quad= p^s \sum_{x_{s+1},\dots,x_m=1}^{p} \mathbf{e}_p\left(\Psi_{\mathbf{a},\mathbf{k},\mathbf{l}}(x_{s+1},\dots,x_m)\right)\\
&\qquad \sum_{x_s=1}^{p} \mathbf{e}_p\left(a_s x_s \sum_{h=1}^{\nu} \left(\widetilde{G}_{k_h,s}(x_{s+1},\dots,x_m) - \widetilde{G}_{l_h,s}(x_{s+1},\dots,x_m)\right)\right).
\end{aligned}$$

Recalling the identity of Theorem 7, we conclude that the sum over the variable x_s is nonzero only if the polynomial

$$\Phi_{s,\mathbf{k},\mathbf{l}} = \sum_{h=1}^{\nu} (\widetilde{G}_{k_h,s} - \widetilde{G}_{l_h,s}) \in \mathbb{F}_p[X_{s+1},\dots,X_m]$$

is zero modulo p at $(x_{s+1},\dots,x_m)$.

Performing all trivial cancelations, without loss of generality we can also assume that the vectors $\mathbf{k}$ and $\mathbf{l}$ have no common elements. Thus, by Lemma 18, we see that if $\min\{k_1,\dots,k_\nu,l_1,\dots,l_\nu\} \geq k_0$ for a sufficiently large k_0 then the polynomial $\Phi_{s,\mathbf{k},\mathbf{l}}$ is a nontrivial polynomial modulo p of degree $O(K^{m-s}) = O(K^m)$. Also, a simple inductive argument shows that a modulo p nontrivial polynomial in r variables of degree D may have only $O(Dp^{r-1})$ zeros modulo p, which concludes the proof. □

Theorem 22. *Let the sequence* $\{\mathbf{u}_n\}$ *be given by* (2.7) *where the polynomial system* $\mathcal{F} \in \mathbb{F}_p[X_0, \ldots, X_m]$ *is of the form* (2.1)*, of total degree* $d \geq 2$*, satisfying the conditions* (2.2) *and* (2.3)*, and such that* $s_{0,1} \ldots s_{m-1,m} \neq 0$*. Assume that* $\{\mathbf{w}_n\}$ *is purely periodic with period* τ*. Then for any fixed integer* $\nu \geq 1$*, positive integer* $N \leq \tau$ *and nonzero vector* $\mathbf{a} \in \mathbb{F}_p^m$ *the bound*

$$S_{\mathbf{a}}(N) \ll N^{1-\beta_{m,\nu}} p^{\alpha_{m,\nu}}$$

holds, where

$$\alpha_{m,\nu} = \frac{m^2 + m\nu + m}{2\nu(m+\nu)} \qquad \text{and} \qquad \beta_{m,\nu} = \frac{1}{2\nu}$$

and the implied constant depends only on d*,* m *and* ν*.*

Proof. We follow the same argument as in the proof of [110, Theorem 4] however instead of the Weil bound we use now Lemma 21 (and thus we optimise the parameters differently).

In particular, as in [110] we obtain that for any integer $K \geq k_0$,

$$(K - k_0 + 1)|S_{\mathbf{a}}(N)| \leq W + K^2, \tag{2.11}$$

where k_0 is the same as in Lemma 21 and

$$W = \left| \sum_{n=0}^{N-1} \sum_{k=k_0}^{K} \mathbf{e}\left(\sum_{i=0}^{m-1} a_i u_{n+k,i} \right) \right|.$$

Using the Hölder inequality we derive (again exactly the same way as in [110])

$$W^{2\nu} \leq N^{2\nu-1} \sum_{k_1,\ell_1,\ldots,k_\nu,\ell_\nu=k_0}^{K} \sum_{w_0,\ldots,w_m \in \mathbb{F}_p^{m+1}} \mathbf{e}(F_{\mathbf{a},\mathbf{k},\mathbf{l}}(w_0, \ldots, w_m)) \,.$$

For $O(K^\nu)$ vectors

$$(k_1 \ldots, k_\nu) \qquad \text{and} \qquad (\ell_1 \ldots, \ell_\nu)$$

which are permutations of each other, we estimate the inner sum trivially as p^{m+1}.

For the other $O(K^{2\nu})$ vectors, we apply Lemma 21 getting the upper bound $K^m p^m$ for the inner sum. Hence,

$$W^{2\nu} \leq K^\nu N^{2\nu-1} p^{m+1} + K^{m+2\nu} N^{2\nu-1} p^m.$$

Inserting this bound in (2.11), we derive

$$S_{\mathbf{a}}(N) \ll K^{-1/2} N^{1-1/2\nu} p^{(m+1)/2\nu} + K^{m/2\nu} N^{1-1/2\nu} p^{m/2\nu} + K.$$

Choosing

$$K = \left\lceil p^{1/(m+\nu)} \right\rceil$$

(and assuming that p is large enough, so $K \geq k_0$), after simple calculations we obtain the desired result. □

Using Lemma 14, we derive the following improvement of [110, Theorem 6].

Corollary 23. *Let the sequence* $\{\mathbf{u}_n\}$ *be given by* (2.7) *where the polynomial system* $\mathcal{F} \in \mathbb{F}_p[X_0, \ldots, X_m]$ *is of the form* (2.1)*, of total degree* $d \geq 2$*, satisfying the conditions* (2.2) *and* (2.3)*, and such that* $s_{0,1} \ldots s_{m-1,m} \neq 0$*. Assume that* $\{\mathbf{w}_n\}$ *is purely periodic with period* τ*. Then for any fixed integer* $\nu \geq 1$*, and any positive integer* $N \leq \tau$*, the discrepancy of the sequence*

$$\left(\frac{u_{n,0}}{p}, \ldots, \frac{u_{n,m-1}}{p}\right), \qquad n = 0, \ldots, N-1,$$

satisfies the bound $O\left(p^{\alpha_{m,\nu}} N^{-\beta_{m,\nu}} (\log p)^m\right)$*, where*

$$\alpha_{m,\nu} = \frac{m^2 + m\nu + m}{2\nu(m+\nu)} \qquad \text{and} \qquad \beta_{m,\nu} = \frac{1}{2\nu}$$

and the implied constant depends only on d*,* m *and* ν*.*

We note that both Theorem 22 and Corollary 23 are nontrivial for $\tau \geq N \geq p^{m+\varepsilon}$ for some $\varepsilon > 0$.

Next we obtain an estimate for exponential sums and discrepancy of sequences of the full vectors $(\mathbf{w}_n)$ defined by (2.7).

Theorem 24. *Let the sequence* $\{\mathbf{w}_n\}$ *be given by* (2.7) *where the polynomial system* $\mathcal{F} \in \mathbb{F}_p[X_0, \ldots, X_m]$ *is of the form* (2.1)*, of total degree* $d \geq 2$*, satisfying the conditions* (2.2) *and* (2.3)*, and such that* $s_{0,1} \ldots s_{m-1,m} \neq 0$*. Assume that* $\{\mathbf{w}_n\}$ *is purely periodic with period* τ*. Then for any fixed real* $\varepsilon > 0$*, there exist* $\delta > 0$ *such that for for any positive integer* N *with* $\tau \geq N \geq p^{m+\varepsilon}$ *and nonzero vector* $\mathbf{a} \in \mathbb{F}_p^{m+1}$ *the bound*

$$T_{\mathbf{b}}(N) \ll Np^{-\delta}$$

holds and the implied constant depends only on d*,* m *and* ε*.*

Proof. If $\gcd(a_0, \ldots, a_{m-1}, p) = 1$ then the same argument as in the proof of Theorem 24 leads to a fully analogous bound

$$T_{\mathbf{b}}(N) \ll N^{1-\beta_{m,\nu}} p^{\alpha_{m,\nu}}.$$

Thus for $\tau \geq N \geq p^{m+\varepsilon}$, taking a sufficiently large ν we obtain the desired estimate.

So it remains to consider the case

$$b_0 \equiv \ldots \equiv b_{m-1} \equiv 0 \pmod{p} \qquad \text{and} \qquad \gcd(b_m, p) = 1,$$

in which case we simply obtain

$$T_{\mathbf{b}}(N) = \sum_{n=0}^{N-1} \mathbf{e}_p\left(b_m u_{n,m}\right).$$

A trivial inductive argument shows that

$$u_{n,m} = g_m^n u_{0,m} + \frac{g_m^n - 1}{g_m - 1} h_m, \qquad n = 0, 1, \ldots, \tag{2.12}$$

if $g_m \neq 1$ and

$$u_{n,m} = n h_m, \qquad n = 0, 1, \ldots, \tag{2.13}$$

if $g_m = 1$ (where g_m and h_m are as in (2.1)).

We consider the case $g_m \neq 1$ first in which we obtain

$$T_{\mathbf{b}}(N) = \mathbf{e}_p(-b_m h_m (g_m - 1)^{-1}) \sum_{n=0}^{N-1} \mathbf{e}_p\left(b_m g_m^n \left(u_{0,m} + h_m (g_m - 1)^{-1}\right)\right).$$

Clearly, if t is the multiplicative order of g_m then we see from (2.12) that $u_{n,m}$, $n = 0, 1, \ldots$, takes exactly t distinct values. Since the truncated vector $\mathbf{u}_n$ takes at most p^m values we see that the full vector $\mathbf{w}_n$ takes at most tp^m values. Thus

$$\tau \leq p^m t.$$

Using the condition $\tau \geq N \geq p^{m+\varepsilon}$ we obtain

$$t \geq p^{\varepsilon}. \tag{2.14}$$

In particular (2.14) implies that

$$u_{0,m} + h_m (g_m - 1)^{-1} \not\equiv 0 \pmod{p}$$

as otherwise

$$u_{1,m} \equiv g_m u_{0,m} + h_m \equiv u_{0,m} \pmod{p}$$

and $t = 1$.

We now recall that by the result of [20], for any $\varepsilon > 0$ there exists $\eta > 0$ such that under the condition (2.14) we have

$$\sum_{n=1}^{t} \mathbf{e}_p(c g_m^n) \ll t p^{-\eta}$$

which concludes the proof in the case of $g_m > 1$.

For $g_m = 1$ we recall (2.13) and then using Theorem 7 we derive the result. □

Using again Lemma 14, we derive the following generalisation of [110, Theorem 6] (the bound is $\log p$ weaker as we work in the dimension $m + 1$ instead of m).

Corollary 25. *Let the sequence* $\{\mathbf{w}_n\}$ *be given by* (2.7) *where the polynomial system* $\mathcal{F} \in \mathbb{F}_p[X_0, \ldots, X_m]$ *is of the form* (2.1)*, of total degree* $d \geq 2$*, satisfying the conditions* (2.2) *and* (2.3)*, and such that* $s_{0,1} \ldots s_{m-1,m} \neq 0$*. Assume that* $\{\mathbf{w}_n\}$ *is purely periodic with period* τ*. Then for any fixed real* $\varepsilon > 0$*, there exist* $\gamma > 0$ *such that for any positive integer* N *with* $\tau \geq N \geq p^{m+\varepsilon}$ *the discrepancy of the sequence*

$$\left(\frac{u_{n,0}}{p}, \ldots, \frac{u_{n,m}}{p}\right), \qquad n = 0, \ldots, N-1,$$

satisfies the bound $O\left(p^{-\gamma}\right)$*, where the implied constant depends only on* d*,* m *and* ε*.*

Certainly one can get stronger and more explicit statements in both Theorem 24 and Corollary 25 if more information about the multiplicative order t modulo p is available. For example, if it is known that $t \geq p^{1/3+\varepsilon}$ then one can use the bound of Heath-Brown and Konyagin [67] (see also [78, Theorem 3.4])

$$\sum_{n=1}^{t} \mathbf{e}_p(cg_m^n) \ll \min\{p^{1/2}, p^{1/4}t^{3/8}, p^{1/8}t^{5/8}\}.$$

For smaller values of t, but with $t \geq p^{1/4}$ one can use the bound of Bourgain and Garaev [18], see also [77].

We remark that it is easy to see that a randomly chosen element $g \in \mathbb{F}_p^*$ is of order $t = p^{1+o(1)}$ with probability $1 + o(1)$ as $p \to \infty$.

Furthermore, it is also well-known that any fixed integer $g \neq 0, \pm 1$ is of multiplicative order

$$t \geq p^{1/2}, \tag{2.15}$$

for all but $o(x/\log x)$ primes $p \leq x$, see [45, 69, 116] for various improvements of this result.

2.5.3 Permutation polynomial systems

Obtaining stronger results "on average" over all initial values $\mathbf{v} \in \mathbb{F}_p^{m+1}$ is an interesting and challenging question. We remark that in the case of the so-called inversive generator rather stronger estimates "on average" are available (see [101]) and also estimates for the average distribution of powers and primitive elements of the inversive generators are considered in [25]. Here we study this problem by following the same arguments introduced for the inversive generator in [101]. For this we define a special family of multivariate polynomial systems (2.1), which beside the polynomial degree growth also leads to permutation polynomial systems. In turn this allows us to use the approach of [101] to obtain a stronger bound on the discrepancy "on average" over initial values.

We follow the scheme previously introduced in [101] for estimating the exponential sums introduced below, and thus the discrepancy of a sequence of points.

For a vector $\mathbf{a} = (a_0, \ldots, a_{m-1}) \in \mathbb{F}_p^m$ and integers c, M, N with $M \geq 1$ and $N \geq 1$, we introduce

$$V_{\mathbf{a},c}(M,N) = \sum_{v_0,\ldots,v_m \in \mathbb{F}_p} \left| \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j F_j^{(n)}(v_0,\ldots,v_m) \right) \mathbf{e}_M(cn) \right|^2. \tag{2.16}$$

Note that, as in Lemma 21, we do not include polynomials $F_m^{(n)}$ in the above exponential sum.

Theorem 26. *Let the permutation polynomial system of $m+1$ polynomials $\mathcal{F} = \{F_0, \ldots, F_m\} \in \mathbb{F}_p[X_0, \ldots, X_m]$ of total degree $d \geq 2$ of the form* (2.1)*, satisfying the conditions* (2.2) *and* (2.3) *and such that $s_{0,1} \ldots s_{m-1,m} \neq 0$. Then for any positive integers c, M, N and any nonzero vector $\mathbf{a} = (a_0, \ldots, a_{m-1}) \in \mathbb{F}_p^m$ we have*

$$V_{\mathbf{a},c}(M,N) \ll A(N,p),$$

where

$$A(N,p) = \begin{cases} Np^{m+1} & \text{if } N \leq p^{1/(m+1)}, \\ N^2 p^{m(m+2)/(m+1)} & \text{if } N > p^{1/(m+1)}. \end{cases}$$

Proof. We have

$$\begin{aligned} V_{\mathbf{a},c}(M,N) &= \sum_{k,l=0}^{N-1} \mathbf{e}_M(c(k-l)) \\ &\qquad \sum_{v_0,\ldots,v_m \in \mathbb{F}_p} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j \left(F_j^{(k)}(v_0,\ldots,v_m) - F_j^{(l)}(v_0,\ldots,v_m) \right) \right) \\ &\leq \sum_{k,l=0}^{N-1} \left| \sum_{v_0,\ldots,v_m \in \mathbb{F}_p} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j \left(F_j^{(k)}(v_0,\ldots,v_m) - F_j^{(l)}(v_0,\ldots,v_m) \right) \right) \right|. \end{aligned}$$

For $O(N)$ values of k and l which are equal, we estimate the inner sum trivially by p^{m+1}.

For the other values, by Lemma 21 we get the upper bound $O(N^m p^m)$ for the inner sum for at most N^2 sums. Hence,

$$V_{\mathbf{a},c}(M,N) \ll Np^{m+1} + N^{m+2}p^m. \tag{2.17}$$

Because $\mathcal{F}$ is a permutation polynomial system and using (2.8), for any integer L we obtain

$$\sum_{v_0,\ldots,v_m \in \mathbb{F}_p} \left| \sum_{n=L}^{L+N-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j F_j^{(n)}(v_0,\ldots,v_m) \right) \mathbf{e}_M(cn) \right|^2 = \sum_{v_0,\ldots,v_m \in \mathbb{F}_p}$$

$$\left|\sum_{n=0}^{N-1} \mathbf{e}_p\left(\sum_{j=0}^{m-1} a_j F_j^{(n)}\left(F_0^{(L)}(v_0,\ldots,v_m),\ldots,F_m^{(L)}(v_0,\ldots,v_m)\right)\right)\mathbf{e}_M(cn)\right|^2$$
$$= \sum_{v_0,\ldots,v_m\in\mathbb{F}_p}\left|\sum_{n=0}^{N-1} \mathbf{e}_p\left(\sum_{j=0}^{m-1} a_j F_j^{(n)}(v_0,\ldots,v_m)\right)\mathbf{e}_M(cn)\right|^2 = V_{\mathbf{a},c}(M,N).$$

Therefore, for any positive integer $K \le N$, separating the inner sum into at most $N/K+1$ subsums of length at most K, and using (2.17), we derive

$$V_{\mathbf{a},c}(M,N) \ll (Kp^{m+1} + K^{m+2}p^m)N^2K^{-2} = N^2(K^{-1}p^{m+1} + K^m p^m).$$

Thus, selecting $K = \min\{N, \lfloor p^{1/(m+1)}\rfloor\}$ and taking into account that $N^{-1}\ p^{m+1} \ge N^m p^m$ for $N \le p^{1/(m+1)}$, we obtain the desired result. □

Note that the estimates for $V_{\mathbf{a},c}(M,N)$ work not only over prime fields, but also over any finite field.

We also need a variant of Theorem 7, which we give in the following form

$$\sum_{-(m-1)/2\le a\le m/2} \mathbf{e}_m(ab) = \begin{cases} 0 & \text{if } b \not\equiv 0 \pmod m, \\ m & \text{if } b \equiv 0 \pmod m. \end{cases} \tag{2.18}$$

Then we have the following inequality

$$\sum_{r=L+1}^{L+Q} \mathbf{e}_m(cr) \ll \min\left\{Q, \frac{m}{|c|}\right\} \ll \min\left\{m, \frac{m}{|c|}\right\} \ll \frac{m}{|c|+1} \tag{2.19}$$

which holds for any integers c, Q and L with $|c| \le m/2$, and $m \ge Q \ge 1$, see [70, Bound (8.6)].

Now, as in [101], combining Lemma 14 with the bound obtained in Theorem 26 we obtain stronger estimates for the discrepancy "on average" over all initial values.

Corollary 27. *Let $0 < \varepsilon < 1$ and let the sequence $\{\mathbf{u}_n\}$ be given by (2.7), where the permutation system of $m+1$ polynomials $\mathcal{F} = \{F_0,\ldots,F_m\} \in \mathbb{F}_p[X_0,\ldots,X_m]$ of total degree $d \ge 2$ is of the form (2.1), satisfying the conditions (2.2) and (2.3), and such that $s_{0,1}\ldots s_{m-1,m} \ne 0$. Then for all initial values $\mathbf{v} \in \mathbb{F}_p^{m+1}$ except at most $O(\varepsilon p^{m+1})$ of them, and any positive integer $N \le p^{m+1}$, the discrepancy $\Delta_N(\Gamma(\mathbf{v}))$ of the sequence*

$$\Gamma(\mathbf{v}) = \left\{\left(\frac{u_{n,0}(\mathbf{v})}{p},\ldots,\frac{u_{n,m-1}(\mathbf{v})}{p}\right), \qquad n = 0,\ldots,N-1\right\},$$

satisfies the bound

$$\Delta_N(\Gamma(\mathbf{v})) \ll \varepsilon^{-1}B(N,p),$$

where

$$B(N,p) = \begin{cases} N^{-1/2}(\log N)^{m+1}\log p & \text{if } N \le p^{1/(m+1)}, \\ p^{-1/2(m+1)}(\log N)^{m+1}\log p & \text{if } N > p^{1/(m+1)}. \end{cases}$$

Proof. Without loss of generality we can assume that $N \ge 2$. Thus from Lemma 14 with $L = \lfloor N/2 \rfloor$ we derive

$$\Delta_N(\Gamma(\mathbf{v})) \ll \frac{1}{N} + \frac{1}{N} \sum_{0<|\mathbf{a}|\le N/2} \frac{1}{r(\mathbf{a})} \left| \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j u_{n,j}(\mathbf{v}) \right) \right|.$$

Let $m_\nu = 2^\nu$, $\nu = 0, 1, \ldots$, and define $k \ge 1$ by the condition $m_{k-1} < N \le m_k$. From (2.18) we derive

$$\begin{aligned} &\sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j u_{n,j}(\mathbf{v}) \right) \\ &\quad = \frac{1}{m_k} \sum_{n=0}^{m_k-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j u_{n,j}(\mathbf{v}) \right) \sum_{-(m_k-1)/2 \le c \le m_k/2} \sum_{r=0}^{N-1} \mathbf{e}_{m_k}(c(n-r)). \end{aligned}$$

Since $m_k/2 = m_{k-1}$, from (2.19) we obtain

$$\begin{aligned} &\left| \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j u_{n,j}(\mathbf{v}) \right) \right| \\ &\qquad \ll \sum_{|c| \le m_{k-1}} \frac{1}{|c|+1} \left| \sum_{n=0}^{m_k-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j u_{n,j}(\mathbf{v}) \right) \mathbf{e}_{m_k}(cn) \right|. \end{aligned}$$

It follows that

$$\Delta_N(\Gamma(\mathbf{v})) \ll \Delta_k(\mathbf{v}), \tag{2.20}$$

where

$$\begin{aligned} \Delta_k(\mathbf{v}) \;=\; & \frac{1}{N} + \frac{1}{m_k} \sum_{0<|\mathbf{a}|\le m_{k-1}} \frac{1}{r(\mathbf{a})} \sum_{|c|\le m_{k-1}} \frac{1}{|c|+1} \\ & \cdot \left| \sum_{n=0}^{m_k-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j u_{n,j}(\mathbf{v}) \right) \mathbf{e}_{m_k}(cn) \right|. \end{aligned}$$

Now

$$\begin{aligned} \sum_{\mathbf{v}=(v_0,\ldots,v_m)\in\mathbb{F}_p^{m+1}} \Delta_k(\mathbf{v}) = \frac{p^{m+1}}{N} + \frac{1}{m_k} & \sum_{0<|\mathbf{a}|\le m_{k-1}} \frac{1}{r(\mathbf{a})} \sum_{|c|\le m_{k-1}} \frac{1}{|c|+1} \\ & \cdot \sum_{v_0,\ldots,v_m\in\mathbb{F}_p} \left| \sum_{n=0}^{m_k-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j F_j^{(n)}(v_0,\ldots,v_m) \right) \mathbf{e}_{m_k}(cn) \right|. \end{aligned}$$

Applying the Cauchy inequality, from Theorem 26 we derive

$$\sum_{v_0,\ldots,v_m\in\mathbb{F}_p} \left| \sum_{n=0}^{m_k-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j F_j^{(n)}(v_0,\ldots,v_m) \right) \mathbf{e}_{m_k}(cn) \right| \ll p^{(m+1)/2} A(m_k,p)^{1/2}.$$

Therefore

$$\begin{aligned}\sum_{v_0,\ldots,v_m\in\mathbb{F}_p} &\Delta_k(\mathbf{v})\\ &\ll \frac{p^{m+1}}{N} + \frac{p^{(m+1)/2}A(m_k,p)^{1/2}}{m_k}\sum_{0<|\mathbf{a}|\le m_{k-1}}\frac{1}{r(\mathbf{a})}\sum_{|c|<m_{k-1}}\frac{1}{|c|+1}\\ &\ll \frac{p^{(m+1)/2}A(m_k,p)^{1/2}(\log m_k)^{m+1}}{m_k},\end{aligned}$$

where we used the standard bound for partial sums of the harmonic series in the last step. Thus, for each $k = 1, \ldots, \lceil \log(p^{m+1})\rceil$, the inequality

$$\Delta_k(\mathbf{v}) \ge \frac{A(m_k,p)^{1/2}(\log m_k)^{m+1}\log p}{\varepsilon m_k p^{(m+1)/2}} = \varepsilon^{-1}B(m_k,p) \tag{2.21}$$

can hold for at most $O(\varepsilon p^{m+1}/\log p)$ values of $v_0, \ldots, v_m \in \mathbb{F}_p$. Therefore the number of $v_0, \ldots, v_m \in \mathbb{F}_p$ for which (2.21) holds for at least one $k = 1, \ldots, \lceil \log(p^{m+1})\rceil$ is $O(\varepsilon p^{m+1})$. For all other $v_0, \ldots, v_m$, we get from (2.20),

$$\Delta_N(\Gamma(\mathbf{v})) \ll \Delta_k(\mathbf{v}) < \varepsilon^{-1}B(m_k,p) \ll \varepsilon^{-1}B(N,p)$$

for $1 \le N \le p^{m+1}$, where we used $m_k = 2m_{k-1} < 2N$ in the last step. □

We note that both Theorem 26 and Corollary 27 are nontrivial if $N \ge (\log p)^{2+\varepsilon}$ for some $\varepsilon > 0$.

We now show that the distribution of the full vectors $\{\mathbf{w}_n(\mathbf{v})\}$ can be studied as well.

For an integer vector $\mathbf{b} = (b_0, \ldots, b_m) \in \mathbb{F}_p^{m+1}$ and integers c, M, N with $M \ge 1$ and $N \ge 1$, we consider the average values of exponential sums

$$U_{\mathbf{b},c}(M,N) = \sum_{w_0,\ldots,w_m\in\mathbb{F}_p}\left|\sum_{n=0}^{N-1}\mathbf{e}_p\left(\sum_{j=0}^{m}b_jF_j^{(n)}(w_0,\ldots,w_m)\right)\mathbf{e}_M(cn)\right|^2, \tag{2.22}$$

where, as before, the polynomials $F_i^{(k)}$, $i = 0, \ldots, m$, $k = 1, 2, \ldots$ are given by (2.4).

Theorem 28. *Let $\mathcal{F}$ be a permutation polynomial system (2.1) of total degree $d \ge 2$ satisfying the conditions (2.2) and (2.3), and such that $s_{0,1}\ldots s_{m-1,m} \ne 0$. We consider the last polynomial in the system $\mathcal{F}$ to be given by*

$$F_m(X_0, \ldots, X_m) = g_mX_m + h_m$$

and denote by t the period of g_m if $g_m \ne 1$ and put $t = p$ if $g_m = 1$. Then for any positive integers c, M, N and any nonzero vector $\mathbf{b} \in \mathbb{F}_p^{m+1}$ we have

$$U_{\mathbf{b},c}(M,N) \ll C(N,t,p),$$

where

$$C(N,t,p) = A(N,p) + N^2t^{-1}p^{m+1}$$

and $A(N,p)$ is defined as in Theorem 26.

Proof. Note, as before, that if $\gcd(b_0,\dots,b_{m-1},p)=1$ then the proof of [107, Lemma 4] applies to the sums $V_{\mathbf{b},c}(M,N)$ without any changes. So it remains to consider the case

$$b_0 \equiv \ldots \equiv b_{m-1} \equiv 0 \pmod{p} \qquad \text{and} \qquad \gcd(b_m,p)=1,$$

in which case we simply obtain

$$\begin{aligned} U_{\mathbf{b},c}(M,N) &= \sum_{v_0,\dots,v_m\in\mathbb{F}_p} \left| \sum_{n=0}^{N-1} \mathbf{e}_p\left(b_m F_m^{(n)}(v_0,\dots,v_m)\right) \mathbf{e}_M(cn)\right|^2 \\ &= \sum_{k,n=0}^{N-1} \mathbf{e}_M(c(k-n)) \\ &\qquad \sum_{v_0,\dots,v_m\in\mathbb{F}_p} \mathbf{e}_p\left(b_m\left(F_m^{(k)}(v_0,\dots,v_m)-F_m^{(n)}(v_0,\dots,v_m)\right)\right) \\ &\le \sum_{k,n=0}^{N-1} \left| \sum_{v_0,\dots,v_m\in\mathbb{F}_p} \mathbf{e}_p\left(b_m\left(F_m^{(k)}(v_0,\dots,v_m)-F_m^{(n)}(v_0,\dots,v_m)\right)\right)\right|. \end{aligned}$$

We have the following explicit formulas (as in (2.12) and (2.13)):

$$F_m^{(k)} = g_m^k X_m + d_m \qquad k=0,1,\dots,$$

if $g_m \neq 1$ and

$$F_m^{(k)} = X_m + kh_m, \qquad k=0,1,\dots, \tag{2.23}$$

if $g_m = 1$, where

$$d_m = \frac{g_m^k-1}{g_m-1}h_m.$$

We treat first the case $g_m \neq 1$. In this case we get:

$$\begin{aligned} U_{\mathbf{b},c}(M,N) &\le \sum_{k,n=0}^{N-1} \left| \sum_{v_0,\dots,v_m\in\mathbb{F}_p} \mathbf{e}_p\left(b_m\left((g_m^k-g_m^n)v_m+d_k-d_n\right)\right)\right| \\ &= \sum_{\substack{k,n=0\\ k\equiv n \pmod t}}^{N-1} \left| \sum_{v_0,\dots,v_m\in\mathbb{F}_p} \mathbf{e}_p\left(b_m\left((g_m^k-g_m^n)v_m+d_k-d_n\right)\right)\right| \\ &\quad + \sum_{\substack{k,n=0\\ k\not\equiv n \pmod t}}^{N-1} \left| \sum_{v_0,\dots,v_m\in\mathbb{F}_p} \mathbf{e}_p\left(b_m\left((g_m^k-g_m^n)v_m+d_k-d_n\right)\right)\right|. \end{aligned}$$

Because $g_m^k - g_m^n \equiv 0 \pmod{p}$ if and only if $k \equiv n \pmod{t}$, we estimate the first sum trivially as $N(Nt^{-1}+1)p^{m+1}$. Furthermore, for $k \not\equiv n \pmod{t}$, using Theorem 7 we see that the second sum simply vanishes.

Thus, for $g_m \neq 1$, we obtain

$$U_{\mathbf{b},c}(M,N) \ll A(N,p) + N(Nt^{-1}+1)p^{m+1} = A(N,p) + N^2t^{-1}p^{m+1}.$$

For the case $g_m = 1$ we recall (2.23) and using similar arguments easily derive the desired result. □

As above, we now get:

Corollary 29. *Let $0 < \varepsilon < 1$ and let the sequence $\{\mathbf{w}_n\}$ be given by (2.7), where $\mathcal{F}$ is a permutation polynomial system (2.1) satisfying the conditions (2.2) and (2.3), and such that $s_{0,1} \dots s_{m-1,m} \neq 0$. We consider the last polynomial in the system $\mathcal{F}$ to be given by*

$$F_m(X_0, \dots, X_m) = g_m X_m + h_m$$

and denote by t the period of g_m if $g_m \neq 1$ and put $t = p$ if $g_m = 1$. Then for all vectors of initial values $\mathbf{v} \in \mathbb{F}_p^{m+1}$ except at most $O(\varepsilon p^{m+1})$, and any positive integer $N \leq p^{m+1}$, the discrepancy $\Delta_N(\Gamma(\mathbf{v}))$ of the sequence

$$\Gamma(\mathbf{v}) = \left\{ \left(\frac{u_{n,0}(\mathbf{v})}{p}, \dots, \frac{u_{n,m}(\mathbf{v})}{p} \right), \qquad n = 0, \dots, N-1 \right\},$$

satisfies the bound

$$\Delta_N(\Gamma(\mathbf{v})) \ll \varepsilon^{-1} D(N,t,p),$$

where

$$D(N,t,p) = B(N,p) \log N + t^{-1/2} (\log N)^{m+2} \log p$$

and $B(N,p)$ is defined as in Corollary 27.

It is easy to see that under the condition (2.15) the quantities $C(N,t,p)$ and $D(N,t,p)$ are dominated by the terms with $A(N,p)$ and $B(N,p)$, respectively:

$$C(N,t,p) \ll A(N,p) \qquad \text{and} \qquad D(N,t,p) \ll B(N,p) \log N.$$

2.6 Linear complexity

2.6.1 Outline

In this section we study the (generalized) joint linear complexity for multisequences generated by dynamical systems of multivariate polynomials with slow degree growth introduced in Section 2.2. We prove lower bounds on the linear complexity of the coordinate sequences as well as on the generalized joint linear complexity (and thus on the joint linear complexity) of these multisequences in the case of an arbitrary period. In Section 2.6.3 we improve the bound on the joint linear complexity in the case of the largest possible period and when the sequence is defined over a finite prime field.

2.6.2 General polynomial systems

Let the sequences $(\mathbf{w}_n)$ be given by (2.7), where the polynomial system of $m+1$ polynomials

$$\mathcal{F} = \{F_0, \ldots, F_m\} \in \mathbb{F}_q[X_0, \ldots, X_m]$$

is of the form (2.1), satisfying the conditions (2.2) and (2.3). First we prove a lower bound on the Nth linear complexity, see Section 1.5, of the ith coordinate sequence $(w_{n,i})$ for $i = 0, \ldots, m-1$ which implies also a lower bound on the Nth joint linear complexities of $(\mathbf{u}_n)$ and $(\mathbf{w}_n)$. Note that since $w_{n+1,m} = g_m w_{n,m} + h_m$, $n = 0, 1, \ldots$, the linear complexity of the last coordinate sequence $(w_{n,m})$ is at most 2.

Using now Lemma 1 we obtain:

Theorem 30. *Let $(\mathbf{w}_n)$ be a purely periodic sequence with period τ, given by (2.7), where the polynomial system of $m+1$ polynomials*

$$\mathcal{F} = \{F_0, \ldots, F_m\} \in \mathbb{F}_q[X_0, \ldots, X_m]$$

is of the form (2.1), satisfying the conditions (2.2) and (2.3), and such that $s_{k,k+1}s_{k+1,k+2} \cdots s_{m-1,m} \neq 0$ for some $0 \leq k \leq m-1$. Then for the linear complexity profiles of the sequences $(\mathbf{w}_n)$, $(\mathbf{u}_n)$ and $(w_{n,i})$ given by (2.6), (2.7) and (2.9) we have for $1 \leq N \leq \tau$ and $i = k, k+1, \ldots, m-1$,

$$\mathcal{L}\left((\mathbf{w}_n), N\right) \geq \mathcal{L}\left((\mathbf{u}_n), N\right) \geq \mathcal{L}\left((w_{n,i}), N\right) \gg \left(\frac{N}{q^m}\right)^{1/(m-i)},$$

where the implied constant depends on the degree of $\mathcal{F}$.

Proof. We assume that the sequence $(w_{n,i})$ satisfies the recurrence relation

$$w_{n+L,i} = c_{L-1}w_{n+L-1,i} + \ldots + c_0 w_{n,i}, \quad 0 \leq n \leq N-L-1,$$

with $c_0, \ldots, c_{L-1} \in \mathbb{F}_q$.

We know from Lemma 18 that there exists some integer $n_0 = O(1)$ such that for $n \geq n_0$ and every $i = 0, \ldots, m-1$ the degree $\deg G_{i,n}$ is a strictly increasing function of n if $s_{i,i+1} \cdots s_{m-1,m} \neq 0$. Now, by (2.8) this recurrence relation gives us

$$\begin{aligned} F_i^{(L+n_0)}(\mathbf{w}_{n-n_0}) = c_{L-1}F_i^{(L-1+n_0)}(\mathbf{w}_{n-n_0}) + \ldots \\ + c_1 F_i^{(n_0+1)}(\mathbf{w}_{n-n_0}) + c_0 F_i^{(n_0)}(\mathbf{w}_{n-n_0}), \end{aligned}$$

for $n = n_0, \ldots, N-L-1$.

In turn, this is equivalent to

$$w_{n-n_0,i}T_i(w_{n-n_0,i+1}, \ldots, w_{n-n_0,m}) + V_i(w_{n-n_0,i+1}, \ldots, w_{n-n_0,m}) = 0,$$

for $n = n_0, \ldots, N-L-1$, where the nonconstant polynomial

$$T_i \in \mathbb{F}_q[X_{i+1}, \ldots, X_m]$$

is defined by

$$T_i = G_{i,L+n_0} - c_{L-1}G_{i,L-1+n_0} - \ldots - c_1 G_{i,n_0+1} - c_0 G_{i,n_0}$$

and $V_i \in \mathbb{F}_q[X_{i+1}, \ldots, X_m]$ is defined by

$$V_i = H_{i,L+n_0} - c_{L-1}H_{i,L-1+n_0} - \ldots - c_1 H_{i,n_0+1} - c_0 H_{i,n_0}.$$

By Lemmas 1 and 18, we have $O(L^{m-i}q^{m-i-1})$ distinct zeros $(x_{i+1}, \ldots, x_m)$ of T_i. For a fixed $(x_{i+1}, \ldots, x_m)$ there are at most q^{i+1} different $n \le N \le \tau$ with $(w_{n,i+1}, \ldots, w_{n,m}) = (x_{i+1}, \ldots, x_m)$.

If

$$N < L^{m-i}q^m$$

then there is nothing to prove. Otherwise we have $\Omega\left(N - L^{m-i}q^m\right)$ remaining integers n with $n_0 \le n \le N - L - 1$ corresponding to a linear recurrence relation

$$w_{n,i}T_i(x_{i+1}, \ldots, x_m) + V_i(x_{i+1}, \ldots, x_m) = 0$$

with $T_i(x_{i+1}, \ldots, x_m) \neq 0$.

In the case $i = m - 1$ at least one of these at most q equations (since x_m takes at most q values) is satisfied by $\Omega\left(N/q - Lq^{m-1}\right)$ different n. If $i < m - 1$ we note that we have at most q^2 equations (since the polynomials T_i, V_i take each at most q values) and at least one of them is satisfied by $\Omega\left(N/q^2 - L^{m-i}q^{m-2}\right)$ different $n \ge n_0$. On the other hand each of the polynomials

$$X_i T_i(x_{i+1}, \ldots, x_m) + V_i(x_{i+1}, \ldots, x_m)$$

with $T_i(x_{i+1}, \ldots, x_m) \neq 0$ of degree one (considered as polynomial in $i + 1$ variables) can have at most q^i zeros. Now the result follows immediately. □

Now we analyse the generalized linear complexities of $(\mathbf{u}_n)$ and $(\mathbf{w}_n)$, that is, we use a natural mapping of the vectors $\mathbf{u}_n$ and $\mathbf{w}_n$ into elements of $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^{m+1}}$, respectively, and investigate the linear complexities of the corresponding sequences in $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^{m+1}}$. Namely, let us fix bases $\{\rho_0, \ldots, \rho_{m-1}\}$ and $\{\vartheta_0, \ldots, \vartheta_m\}$ of $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^{m+1}}$ over $\mathbb{F}_q$, respectively, and consider the sequences

$$U_n = \sum_{j=0}^{m-1} \rho_j w_{n,j} \qquad \text{and} \qquad W_n = \sum_{j=0}^{m} \vartheta_j w_{n,j}. \tag{2.24}$$

We now obtain a lower bound on the linear complexities of (U_n) and (W_n).

Theorem 31. *Let $(\mathbf{w}_n)$ be a purely periodic sequence with period τ, given by (2.7), where the polynomial system of $m + 1$ polynomials*

$$\mathcal{F} = \{F_0, \ldots, F_m\} \in \mathbb{F}_q[X_0, \ldots, X_m]$$

is of the form (2.1)*, satisfying the conditions* (2.2) *and* (2.3)*, and such that* $s_{0,1} \dots s_{m-1,m} \neq 0$*. Then for the linear complexity profiles of the sequences* (U_n) *and* (W_n) *given by* (2.24) *we have*

$$\mathcal{L}\left((U_n), N\right), \mathcal{L}\left((W_n), N\right) \gg \frac{N^{1/m}}{q}, \qquad 1 \leq N \leq \tau,$$

where the implied constant depends on the degree of $\mathcal{F}$*.*

Proof. We observe that the sequence (W_n) is also purely periodic with period τ. We consider only the sequence (U_n) since the sequence (W_n) can be studied fully analogously.

Let

$$U_{n+L} = c_{L-1}U_{n+L-1} + \ldots + c_0 U_n, \quad 0 \leq n \leq N - L - 1,$$

with $c_0, \ldots, c_{L-1} \in \mathbb{F}_{q^m}$.

Writing

$$\rho_i \rho_j = \sum_{h=0}^{m-1} a_{i,j,h} \rho_h, \qquad 0 \leq i, j \leq m-1,$$

and

$$c_r = \sum_{i=0}^{m-1} c_{r,i} \rho_i, \qquad 0 \leq r \leq L-1,$$

with $a_{i,j,h}, c_{r,h} \in \mathbb{F}_q$, we obtain

$$U_{n+L} = \sum_{i,j,h=0}^{m-1} a_{i,j,h} \sum_{r=0}^{L-1} c_{r,i} w_{n+r,j} \rho_h,$$

which gives the coordinate recurrence relations

$$w_{n+L,h} = \sum_{i,j=0}^{m-1} a_{i,j,h} \sum_{r=0}^{L-1} c_{r,i} w_{n+r,j}$$

for $h = 0, \ldots, m-1$.

We see from Lemma 18 that there exists some integer $n_0 = O(1)$ such that for $n \geq n_0$ and every $i = 0, \ldots, m-1$ the degree $\deg G_{i,n}$ is a strictly increasing function of n if $s_{i,i+1} \cdots s_{m-1,m} \neq 0$.

Using (2.8), we derive

$$F_h^{(n_0+L)}(\mathbf{w}_{n-n_0}) = \sum_{i,j=0}^{m-1} a_{i,j,h} \sum_{r=0}^{L-1} c_{r,i} F_j^{(n_0+r)}(\mathbf{w}_{n-n_0})$$

for $h = 0, \ldots, m-1$ and $n_0 \leq n \leq N - L - 1$.

Choosing $h = 0$, we see that

$$F_0^{(n_0+L)} - \sum_{i,j=0}^{m-1} a_{i,j,0} \sum_{r=0}^{L-1} c_{r,i} F_j^{(n_0+r)} \in \mathbb{F}_q[X_0, \ldots, X_m] \tag{2.25}$$

is a nonconstant polynomial of degree $O(L^m)$, since we assumed $s_{0,1} \cdots s_{m-1,m} \neq 0$, which has at least $N - L - n_0$ zeros. Applying now Lemma 1 we get the desired result. □

2.6.3 Permutation polynomial systems of maximal period over prime fields

In this section we assume that $q = p$ is a prime and study the coordinate sequences $(w_{n,m-1})$ of $(\mathbf{w}_n)$ and thus its joint linear complexity profile if $(\mathbf{w}_n)$ is generated by a permutation polynomial system of the form (2.1) of least period p^{m+1}. We use a similar technique as in [135]. The lower bound in this section improves Theorem 30 in this special situation if $m \geq 2$ or $m = 1$ and $N \geq p^2 + p$.

We introduce first some notations and auxiliary results, see [11, 135].

Let $\Phi(X_0, \ldots, X_m) \in \mathbb{F}_p[X_0, \ldots, X_m]$ be a polynomial of degree strictly less than p in each indeterminate. We write each integer n with $0 \leq n \leq p^{m+1} - 1$ in base p as

$$n = \sum_{k=0}^{m} n_k p^k, \qquad 0 \leq n_0, \ldots, n_m \leq p - 1.$$

Then the polynomial Φ can be expressed as

$$\Phi(X_0, \ldots, X_m) = \sum_{n=0}^{p^{m+1}-1} a_n X_0^{n_0} \cdots X_m^{n_m}$$

for uniquely determined coefficients $a_0, \ldots, a_{p^{m+1}-1} \in \mathbb{F}_p$.

As in [11, 135], we define

$$\mathcal{D}(\Phi) = \begin{cases} \max\{n \ : \ a_n \neq 0\} & \text{if } \Phi \neq 0 \\ -1 & \text{if } \Phi = 0. \end{cases}$$

We recall now the following result which is a combination of a result of Blackburn, Etzion and Paterson, see [11], on the linear complexity of p^{m+1} periodic sequences over $\mathbb{F}_p$ and a standard argument, see, for example, [91, Lemma 3] to extend linear complexity bounds to the linear complexity profile.

Lemma 32. *With the above notation, let (s_n) be the sequence of period p^{m+1} defined by*

$$s_n = g(n_0, \ldots, n_m), \quad 0 \leq n \leq p^{m+1} - 1,$$

where

$$n = \sum_{k=0}^{m} n_k p^k, \qquad 0 \leq n_k \leq p - 1.$$

Then the linear complexity profile of the sequence (s_n) satisfies

$$\mathcal{L}((s_n), N) \geq \min\{\mathcal{D}(\Phi) + 1, N + 1 - p^{m+1}\}.$$

Next we need to see what is the period of a coordinate sequence $(w_{n,i})$, $0 \leq i \leq m$, of $(\mathbf{w}_n)$.

Lemma 33. *Let the sequence* $(\mathbf{w}_n)$ *be given by* (2.7) *of least period* p^{m+1}*, where the permutation system of* $m+1$ *polynomials* $\mathcal{F} = \{F_0, \ldots, F_m\} \in \mathbb{F}_p[X_0, \ldots, X_m]$ *is of the form* (2.1)*, satisfying the conditions* (2.2) *and* (2.3)*. Then the coordinate sequence* $(w_{n,j})$ *of* $(\mathbf{w}_n)$ *is of least period* p^{m-j+1} *for* $j = 0, 1, \ldots, m$*.*

Proof. Fix $0 \le j \le m$ and let τ_j be the period of $((w_{n,j}, \ldots, w_{n,m}))$. Clearly this sequence can be defined analogously to the the sequence $(\mathbf{w}_n)$ by a polynomial system in $m - j + 1$ variables. In particular, we get $\tau_j \le p^{m-j+1}$.

On the other hand, as the vector $(w_{n,0}, \ldots, w_{n,j-1})$ of the first j components of $\mathbf{w}_n$ takes at most p^j values, we obtain $p^{m+1} \le p^j \tau_j$, thus $\tau_j \ge p^{m-j+1}$.

So $(w_{n,m})$ has least period p and τ_j, $j = m-1, \ldots, 0$, is the least common multiple of τ_{j+1} and the least period of $(w_{n,j})$, which implies the result. □

In particular we see from Lemma 33 that the sequence $(\mathbf{w}_n)$ is of least period p^{m+1} only if the coefficient of X_m in the last polynomial F_m of the system $\mathcal{F}$ has the value 1. Indeed, we note that the last polynomial $F_m = g_m X_m + h_m$ leads to the period t_m in the last component of the vectors $\mathbf{w}_n$ which is the order of g_m modulo p. This means that $t_m | (p-1)$, but in the same time is also a divisor of p^{m+1}. We obtain thus that $g_m = 1$ and $h_m \neq 0$. So in this case $(w_{n,m})$ has linear complexity 2 since we obtain the shortest linear recurrence relation by subtracting $w_{n+1,m} = w_{n,m} + h_m$ from $w_{n+2,m} = w_{n+1,m} + h_m$ to ged rid of the nonzero h_m.

We have now the following result:

Theorem 34. *Let the sequence* $(\mathbf{w}_n)$ *be given by* (2.7) *of least period* p^{m+1}*, where the permutation system of* $m+1$ *polynomials*

$$\mathcal{F} = \{F_0, \ldots, F_m\} \in \mathbb{F}_p[X_0, \ldots, X_m]$$

is of the form (2.1)*, satisfying the conditions* (2.2) *and* (2.3)*. Then the joint linear complexity profile of the sequence* $(\mathbf{w}_n)$ *and the linear complexity profile of the sequence* $(w_{n,m-1})$ *satisfy*

$$\begin{aligned} \mathcal{L}((\mathbf{w}_n), N) &\ge \mathcal{L}\left((w_{n,m-1}), N\right) \\ &\ge \min\left\{(p + 1 - \deg F_{m-1})p + 1, N + 1 - p^2\right\}. \end{aligned}$$

Proof. Let $\Phi_{m-1} \in \mathbb{F}_p[X_{m-1}, X_m]$ and $\Phi_m \in \mathbb{F}_p[X_m]$ be the unique polynomials with $\deg_{X_{m-1}} \Phi_{m-1}, \deg_{X_m} \Phi_{m-1}, \deg \Phi_m < p$, satisfying

$$w_{n,m-1} = \Phi_{m-1}(n_{m-1}, n_m) \tag{2.26}$$

for all $0 \le n < p^2$, where $n = n_{m-1} + n_m p$, $0 \le n_{m-1}, n_m \le p-1$ and $w_{n,m} = \Phi_m(n)$ for $0 \le n \le p-1$.

Put $k = \deg_{X_m} \Phi_{m-1}$. Then

$$\Phi_{m-1}(X_{m-1}, X_m) = \sum_{i=0}^{k} \varphi_i(X_{m-1}) X_m^i$$

with some polynomials $\varphi_0, \ldots, \varphi_k \in \mathbb{F}_p[X_{m-1}]$. Note that $k \geq 1$, as $(w_{n,m-1})$ has least period p^2 by Lemma 33. Hence there exists $\nu \in \mathbb{F}_p$ with

$$\varphi_k(\nu) \neq 0.$$

Consider $n = \nu + n_m p$ with $0 \leq n_m \leq p-1$. Now we define

$$P_{m-1}(\nu, X) = \Phi_{m-1}(\nu, X), \quad P_m(X) = \Phi_m(X), \tag{2.27}$$

and $Q(X)$ with

$$Q(X) = \begin{cases} P_{m-1}(\nu+1, X), & 0 \leq \nu \leq p^2-1, \\ P_{m-1}(0, X+1), & \nu = p^2. \end{cases}$$

Note that

$$Q(n) = w_{\nu+np+1,m-1}, \quad n = 0, 1, \ldots, p-1. \tag{2.28}$$

Moreover, we define

$$\begin{aligned} R(X) &= F_{m-1}(0, \ldots, 0, P_{m-1}(\nu, X), P_m(X)) - Q(X) \\ &= P_{m-1}(\nu, X) G_{m-1}(P_m(X)) + H_{m-1}(P_m(X)) - Q(X). \end{aligned} \tag{2.29}$$

We see from (2.26), (2.27) and (2.29) that for $n = 0, 1, \ldots, p-1$,

$$\begin{aligned} &F_{m-1}(0, \ldots, 0, P_{m-1}(\nu, n), P_m(n)) \\ &\qquad = w_{\nu+np,m-1} G_{m-1}(w_{n,m}) + H_{m-1}(w_{n,m}) = F_{m-1}(\mathbf{w}_{\nu+np}). \end{aligned}$$

Therefore, by (2.7) and (2.28)

$$R(n) = F_{m-1}(\mathbf{w}_{\nu+np}) - Q(n) = 0.$$

On the other hand, note that $\deg P_m = \deg \Phi_m = 1$ since $(w_{n,m})$ has linear complexity 2 and thus $R(X) \in \mathbb{F}_p[X]$ is not identical zero and has degree $\deg R = k + \deg G_{m-1}$. Using Lemma 32 we get that

$$\mathcal{L}((w_{n,m-1}), N) \geq \min\left\{(p + 1 - \deg F_{m-1})p + 1, N + 1 - p^2\right\}$$

and thus the desired result. □

We can easily obtain a bound which doesn't depend on $\deg F_{m-1}$. Precisely, put $d = \deg F_{m-1}$. Then for any integer N in the interval $2p^{m+1} \geq N > (2p+1-d)p$ we derive from Theorem 34

$$\begin{aligned} \mathcal{L}\left((\mathbf{w}_n), N\right) &\geq \min\left\{(p+1-d)p+1, N+1-p^2\right\} \\ &= (p+1-d)p + 1 \geq \frac{N}{p^{m-1}} + 1. \end{aligned}$$

2.7 Using several polynomial systems

2.7.1 Outline

In this section we consider slightly more general polynomial dynamical systems, where at each iteration a different polynomial map can be used, thus extending those of (2.1).

As in Section 2.5, the arguments used here to study the discrepancy of the sequences generated by these more general dynamical systems are also based on an elementary identity for exponential sums with linear polynomials and also on counting zeros of multivariate polynomials in finite fields, and thus we get the same estimates as for the initial construction proposed in Section 2.4.

2.7.2 Polynomial generators

We generalise now the construction (2.1). Given an integral upper triangular matrix

$$S = \begin{pmatrix} 1 & s_{0,1} & s_{0,2} & \dots & s_{0,m} \\ 0 & 1 & s_{1,2} & \dots & s_{1,m} \\ & & \dots & & \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \tag{2.30}$$

define $\mathfrak{F}(S, m)$ the set of all such polynomial systems of the form (2.1) satisfying the conditions (2.2) and (2.3).

For an integer $m \geq 1$ and an integral matrix S of the form (2.30), we consider a sequence of, not necessarily distinct, polynomial systems

$$\mathcal{F}_k = \{F_{k,0}, \dots, F_{k,m}\} \in \mathfrak{F}(S, m), \qquad k = 1, 2, \dots . \tag{2.31}$$

We consider the sequence of polynomials $F_i^{(j)}$ defined by the recurrence relation

$$F_i^{(0)} = X_i, \qquad F_i^{(k)} = F_{k,i}(F_0^{(k-1)}, \dots, F_m^{(k-1)}), \qquad k = 1, 2, \dots . \tag{2.32}$$

In particular, $\mathcal{F}_0$ denotes the identity map.

As in Lemma 18, we have the following characterisation of the polynomials $F_i^{(k)}$, which in turn generalises and refines Lemma 18.

Lemma 35. *Let $\mathcal{F}_k \in \mathfrak{F}(S, m)$ be a sequence of polynomial systems* (2.31)*. Then for the polynomials $F_i^{(k)}$ given by* (2.32) *we have*

$$F_i^{(k)} = X_i \widetilde{G}_{k,i}(X_{i+1}, \dots, X_m) + \widetilde{H}_{k,i}(X_{i+1}, \dots, X_m),$$

where $\widetilde{G}_{k,i}, \widetilde{H}_{k,i} \in \mathbb{F}[X_{i+1}, \dots, X_m]$ and

$$\begin{aligned} \deg \widetilde{G}_{k,i} &= \frac{1}{(m-i)!} k^{m-i} s_{i,i+1} \dots s_{m-1,m} + \psi_i(k), \quad 0 \leq i \leq m-1, \\ \deg \widetilde{G}_{k,m} &= 0, \end{aligned}$$

with some polynomials $\psi_i(T) \in \mathbb{Q}[T]$ of degree $\deg \psi_i < m - i$.

Proof. Writing $F_{k,i} = X_i G_{k,i} + H_{k,i}$ we get

$$F_i^{(k)} = F_i^{(k-1)} G_{k,i}\left(F_{i+1}^{(k-1)}, \ldots, F_m^{(k-1)}\right) + H_{k,i}\left(F_{i+1}^{(k-1)}, \ldots, F_m^{(k-1)}\right).$$

Thus an easy inductive argument implies that

$$F_i^{(k)} = X_i \widetilde{G}_{k,i}(X_{i+1}, \ldots, X_m) + \widetilde{H}_{k,i}(X_{i+1}, \ldots, X_m)$$

for some polynomials $\widetilde{G}_{k,i}, \widetilde{H}_{k,i} \in \mathbb{F}[X_{i+1}, \ldots, X_m]$, where $i = 0, \ldots, m$, $k = 1, 2, \ldots$.

For the asymptotic formulas for the degrees of the polynomials $\widetilde{G}_{k,i}$ see Lemma 18 where it is given for $\deg F_i^{(k)}$. We note that in Lemma 18 only the case when at each step the same polynomial system $\mathcal{F}_k = \mathcal{F}$ is applied but the proof holds for distinct systems $\mathcal{F}_k \in \mathfrak{F}(S, m)$ without any changes. Indeed, let

$$d_{k,i} = \deg(X_i \widetilde{G}_{k,i}) = 1 + \deg \widetilde{G}_{k,i}, \qquad i = 0, \ldots, m, \ k = 1, 2 \ldots.$$

Then the result follows immediately from the recursive formula

$$(d_{k,0}, \ldots, d_{k,m})^t = S^k(1, \ldots, 1)$$

implied by (2.2) and (2.3), where

$$S = \begin{pmatrix} 1 & s_{0,1} & s_{0,2} & \ldots & s_{0,m} \\ 0 & 1 & s_{1,2} & \ldots & s_{1,m} \\ & & \ldots & & \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix},$$

and $\mathbf{d}^T$ means the transposition of the vector $\mathbf{d}$, see the proof of Lemma 18 for more details. □

We generate now the sequence of vectors exactly as in the Section 2.4. Given a sequence of polynomial systems (2.31), we fix a vector $\mathbf{v} \in \mathbb{F}_p^{m+1}$ and consider the sequence defined by a recurrence congruence modulo a prime p of the form

$$u_{n+1,i} \equiv F_{n+1,i}(u_{n,0}, \ldots, u_{n,m}) \pmod{p}, \qquad n = 0, 1, \ldots, \tag{2.33}$$

with some *initial values*

$$(u_{0,0}, \ldots, u_{0,m}) = \mathbf{v}.$$

We also assume that $0 \le u_{n,i} < p$, $i = 0, \ldots, m$, $n = 0, 1, \ldots$.

Using the following vector notation

$$\mathbf{w}_n = (u_{n,0}, \ldots, u_{n,m})$$

we have the recurrence relation

$$\mathbf{w}_n = \mathcal{F}_n(\mathbf{w}_{n-1}), \qquad n = 1, 2, \ldots .$$

In particular, for any $n, k \ge 0$ and $i = 0, \dots, m$ we have

$$u_{n+k,i} = F_i^{(k)}(u_{n,0}, \dots, u_{n,m}),$$

where the polynomials $F_i^{(k)}$, $i = 0, \dots, m$, $k = 1, 2, \dots$, are given by (2.32). Clearly the sequence of vectors $\mathbf{w}_n$ is eventually periodic with some period $\tau \le p^{m+1}$. We always assume that the sequence is purely periodic, that is,

$$\mathbf{w}_{n+\tau} = \mathbf{w}_n, \qquad n = 0, 1, \dots .$$

As in (2.9), we sometimes discard the last component and define the truncated vectors

$$\mathbf{u}_n = (u_{n,0}, \dots, u_{n,m-1}).$$

2.7.3 Discrepancy estimates

In this section we generalise the results obtained in Section 2.5 regarding the distribution of vectors generated by (2.7), obtaining the same estimates for the distribution of vectors generated by (2.33) using more polynomial systems. The proofs of the next results follow exactly as in Section 2.5, so we omit them here.

For integer vectors $\mathbf{a} = (a_0, \dots, a_{m-1}) \in \mathbb{Z}^m$ and $\mathbf{b} = (b_0, \dots, b_m) \in \mathbb{Z}^{m+1}$ we consider the exponential sums $S_{\mathbf{a}}(N)$ and $T_{\mathbf{b}}(N)$ defined in (2.10).

Theorem 36. *Let the sequence $\{\mathbf{u}_n\}$ be given by (2.33), with polynomial systems $\mathcal{F}_k \in \mathfrak{F}(S, m)$, $k = 1, 2, \dots$, of the form (2.1) of total degree $d \ge 2$ and such that $s_{0,1} \dots s_{m-1,m} \ne 0$. Assume that $\{\mathbf{w}_n\}$ is purely periodic with period τ. Then for any fixed integer $\nu \ge 1$, positive integer $N \le \tau$ and nonzero vector $\mathbf{a} \in \mathbb{F}_p^m$ the bound*

$$S_{\mathbf{a}}(N) \ll N^{1-\beta_{m,\nu}} p^{\alpha_{m,\nu}}$$

holds, where

$$\alpha_{m,\nu} = \frac{m^2 + m\nu + m}{2\nu(m+\nu)} \qquad \text{and} \qquad \beta_{m,\nu} = \frac{1}{2\nu}$$

and the implied constant depends only on d, m and ν.

Corollary 37. *Let the sequence $\{\mathbf{u}_n\}$ be given by (2.33), with polynomial systems $\mathcal{F}_k \in \mathfrak{F}(S, m)$, $k = 1, 2, \dots$, of the form (2.1) of total degree $d \ge 2$ and such that $s_{0,1} \dots s_{m-1,m} \ne 0$. Assume that $\{\mathbf{w}_n\}$ is purely periodic with period τ. Then for any fixed integer $\nu \ge 1$, and any positive integer $N \le \tau$, the discrepancy of the sequence*

$$\left(\frac{u_{n,0}}{p}, \dots, \frac{u_{n,m-1}}{p}\right), \qquad n = 0, \dots, N-1,$$

satisfies the bound $O\left(p^{\alpha_{m,\nu}} N^{-\beta_{m,\nu}} (\log p)^m\right)$, where

$$\alpha_{m,\nu} = \frac{m^2 + m\nu + m}{2\nu(m+\nu)} \qquad \text{and} \qquad \beta_{m,\nu} = \frac{1}{2\nu}$$

and the implied constant depends only on d, m and ν.

We now consider polynomial systems of the form (2.31) which permute the elements of $\mathbb{F}_p^{m+1}$ and we estimate the exponential sums $U_{\mathbf{a},c}(M,N)$ and $V_{\mathbf{b},c}(M,N)$ defined by (2.16) and (2.22), respectively. As a consequence, the the discrepancy of the corresponding vectors follows.

Theorem 38. *Assume that $\mathcal{F}_k \in \mathfrak{F}(S,m)$, $k = 1,2,\ldots$, are permutation polynomial systems (2.31), and such that $s_{0,1}\ldots s_{m-1,m} \neq 0$. Then for any positive integers c, M, N and any nonzero vector $\mathbf{b} \in \mathbb{F}_p^m$ we have*

$$U_{\mathbf{a},c}(M,N) \ll A(N,p),$$

where $A(N,p)$ is given by Theorem 26.

Exactly as in Section 2.5.3, this immediately implies a discrepancy bound which holds for almost all initial values $\mathbf{v} \in \mathbb{F}_p^{m+1}$. We note that in [107] only the case of when at each step the same polynomial system $\mathcal{F}_k = \mathcal{F}$ is applied but the proof, based only on the bound of the sums $U_{\mathbf{a},c}(M,N)$, holds for distinct polynomial systems $\mathcal{F}_k \in \mathfrak{F}(S,m)$ without any changes.

Corollary 39. *Let $0 < \varepsilon < 1$ and let the sequence $\{\mathbf{u}_n(\mathbf{v})\}$ be given by (2.7) with the initial vector of initial values $\mathbf{v} \in \mathbb{F}_p^{m+1}$, where $\mathcal{F}_k \in \mathfrak{F}(S,m)$, $k = 1,2,\ldots$, are permutation polynomial systems (2.31), and such that $s_{0,1}\ldots s_{m-1,m} \neq 0$. Then for all initial values $\mathbf{v} \in \mathbb{F}_p^{m+1}$ except at most $O(\varepsilon p^{m+1})$, and any positive integer $N \le p^{m+1}$, the discrepancy $\Delta_N(\Gamma(\mathbf{v}))$ of the sequence*

$$\Gamma(\mathbf{v}) = \left\{ \left(\frac{u_{n,0}(\mathbf{v})}{p}, \ldots, \frac{u_{n,m-1}(\mathbf{v})}{p} \right), \qquad n = 0, \ldots, N-1 \right\},$$

satisfies the bound

$$\Delta_N(\Gamma(\mathbf{v})) \ll \varepsilon^{-1} B(N,p),$$

where $B(N,p)$ is given by Theorem 27.

Theorem 40. *Let $\mathcal{F}_k \in \mathfrak{F}(S,m)$ be a sequence of permutation polynomial systems (2.31) and such that $s_{0,1}\ldots s_{m-1,m} \neq 0$, satisfying also the additional condition that the last polynomial in all these systems has the same coefficient $g_m \in \mathbb{F}_p$ of X_m, that is,*

$$F_{k,m}(X_0,\ldots,X_m) = g_m X_m + h_{k,m}, \qquad k = 1,2,\ldots.$$

Denote by t the period of g_m if $g_m \neq 1$ and put $t = p$ if $g_m = 1$. Then for any positive integers c, M, N and any nonzero vector $\mathbf{b} \in \mathbb{F}_p^{m+1}$ we have

$$V_{\mathbf{b},c}(M,N) \ll C(N,t,p),$$

where

$$C(N,t,p) = A(N,p) + N^2 t^{-1} p^{m+1}$$

and $A(N,p)$ is defined as in Theorem 26.

As above, we now get:

Corollary 41. *Let $0 < \varepsilon < 1$ and let the sequence $\{\mathbf{u}_n\}$ be given by (2.7), where $\mathcal{F}_k \in \mathfrak{F}(S, m)$ is a sequence of permutation polynomial systems (2.31) and such that $s_{0,1} \dots s_{m-1,m} \neq 0$, satisfying also the additional condition that the last polynomial in all these systems has the same coefficient $g_m \in \mathbb{F}_p$ of X_m, that is,*

$$F_{k,m}(X_0, \dots, X_m) = g_m X_m + h_{k,m}, \qquad k = 1, 2, \dots.$$

Denote by t the period of g_m if $g_m \neq 1$ and put $t = p$ if $g_m = 1$. Then for all vectors of initial values $\mathbf{v} \in \mathbb{F}_p^{m+1}$ except at most $O(\varepsilon p^{m+1})$, and any positive integer $N \leq p^{m+1}$, the discrepancy $\Delta_N(\Gamma(\mathbf{v}))$ of the sequence

$$\Gamma(\mathbf{v}) = \left\{ \left(\frac{u_{n,0}(\mathbf{v})}{p}, \dots, \frac{u_{n,m}(\mathbf{v})}{p} \right), \qquad n = 0, \dots, N-1 \right\},$$

satisfies the bound

$$\Delta_N(\Gamma(\mathbf{v})) \ll \varepsilon^{-1} D(N, t, p),$$

where

$$D(N, t, p) = B(N, p) \log N + t^{-1/2} (\log N)^{m+2} \log p$$

and $C(N, p)$ is defined as in Corollary 27.

Finally, we remark that analogues of Theorem 40 and Corollary 41 can be proven also for more general permutation polynomial systems, namely for systems in which the coefficients $g_{j,m}$ of X_m in the last polynomial of each system vary in such a way that

$$\prod_{j=1}^{k} g_{j,m} \not\equiv \prod_{j=1}^{n} g_{j,m} \pmod{p} \tag{2.34}$$

if k and n are close to each other. In fact, if this is guaranteed for k and n with $0 < |k - n| < t$ then the corresponding results for such polynomial systems look identical to those of Theorem 40 and Corollary 41. Examples include such sequences of coefficients as $g_{j,m} = g_m^j$ for some element $g_m \in \mathbb{F}_p^*$. In this case, the condition (2.34) is equivalent to the quadratic congruence

$$k(k+1) \equiv n(n+1) \pmod{2t},$$

where t is the order of g_m which can be easily shown not to have too many solutions with $0 \leq k, n \leq N-1$ (in particular, if t is prime the results are again exactly the same as those of Theorem 40 and Corollary 41).

2.8 Hash functions

2.8.1 Outline

Here we propose a construction of a hash function from polynomial maps. Although we make no claims of security or efficiency, we note that our results show that this hash function has "random-like" behaviour.

Definition 7. *A hash function h maps bit strings of some finite length to bit strings of some fixed finite length, and must be easy to compute.*

Hash functions from walks on the set of isogenous elliptic curves generated by low degree isogenies, and their cryptographic applications, are considered in [28, 71]. Alternatively these walks can be described as sequences of rational function transformations on the coefficients of Weierstrass equations on elliptic curves, see [127] for a background. We hope that our results maybe useful for studying further properties of such walks, for example, in showing that the hash function of [28, 71] has sufficiently uniformly distributed outputs and maybe used as a secure pseudorandom number generator.

2.8.2 General Construction

In this section we propose a new construction of hash functions based on iterations of polynomial systems studied in the previous sections. This construction is motivated by that of D. X. Charles, E. Z. Goren and K. E. Lauter [28] and in some sense it may be considered as its extension.

Let n and r be two nonzero integers. Choose a random n-bit prime p and 2^r permutation polynomial systems $\mathcal{F}_\ell$, $\ell = 0, \ldots, 2^r - 1$, not necessary distinct, defined by (2.31) and (2.32).

We also consider a random initial vector $\mathbf{w}_0 \in \mathbb{F}_p^{m+1}$.

As in [28], the input of the hash function is used to decide what polynomial system $\mathcal{F}_\ell$ is used to iterate. More precisely, it works as follows given an input bit string Σ, we execute the following steps:

- pad Σ with at most $r-1$ zeros on the left to make sure that its length L is a multiple of r;
- split Σ into blocks σ_j, $j = 1, \ldots, J$, where $J = L/r$, of length r and interpret each block as an integer $\ell \in [0, 2^r - 1]$.
- Starting at the vector $\mathbf{w}_0$, apply the polynomial systems $\mathcal{F}_\ell$ iteratively obtaining the sequence of vectors $\mathbf{w}_j \in \mathbb{F}_p^{m+1}$.
- Output $\mathbf{w}_J$ as the value of the hash function (which can also be now interpreted as a binary $(m+1)n$-bit string).

The above construction is quite similar to that of [28] where $m = 1$, the vectors $\mathbf{w}_j$ represent the coefficients of an equation describing an elliptic curve for example, of the Weierstrass equation

$$Y^2 = X^3 + sX + r$$

and polynomial maps are associated with isogenies of a fixed degree.

2.8.3 Collision Resistance

Our belief in collision resistance is essentially based on the same arguments as in [28].

We remark that the initial vector $\mathbf{w}_0$ is fixed and in particular, does not depend on the input of the hash function. Furthermore, the collision resistance does not rely on the difficulty of inverting the maps generated by the polynomial systems $\mathcal{F}_\ell$, which are triangular and actually quite easy to invert. Rather, it is based on the difficulty of making the decision which system to apply at each step when one attempts to back trace from a given output to the initial vector $\mathbf{w}_0$ and thus produce two distinct strings Σ_1 and Σ_2 of the same length L, with the same output.

Note that for strings of different lengths, say of L and $L+1$, a collision can easily be created. It is enough to take $\Sigma_2 = (0, \Sigma_1)$ (that is, Σ_2 is obtained from Σ_1 by augmenting it by 0). If $L \not\equiv 0 \pmod r$ then they lead to the same output. Certainly any practical implementation has to take care of things like this.

We also note that the results of Section 2.7.3 suggest that the above hash functions exhibit rather chaotic behaviour, which is close to the behaviour of a random function.

We certainly make no claims about the cryptographic strength of our construction but believe that there are enough reasons to investigate it (theoretically and experimentally) more closely.

2.9 Multiplicative character sums for multivariate polynomial recurrence sequences

2.9.1 Outline

In [115] we consider multiplicative character sums with certain sequences of vectors $\mathbf{w}_n = (w_{n,1}, \ldots, w_{n,m}) \in \mathbb{F}_q^m$, $m \geq 2$, $n = 0, 1, \ldots$, which satisfy a recurrence relation

$$\mathbf{w}_{n+1} = \mathbf{F}\left(\mathbf{w}_n\right), \quad n \geq 0,$$

for some multivariate polynomial transformation

$$\mathbf{F}(X_1, \ldots, X_m) \in (\mathbb{F}_q[X_1, \ldots, X_m])^m$$

and some initial vector $\mathbf{w}_0 \in \mathbb{F}_q^m$. More precisely, we consider the polynomial transformations introduced and further analysed in [107, 110, 111, 114], such that their iterates have a very mild degree growth (instead of the "typical" exponential growth). Note that this phenomenon does not occur in the case $m = 1$ and thus there are no analogues of our results in the 1-dimensional case where the results are much weaker due to the inevitable exponential degree growth of the iterates, see [25, 105].

Our results and methods are similar to those obtained in Section 2.5 for exponential sums. However the case of multiplicative characters has turned out to be more difficult and our results are not of the same form as those known for exponential sums. Furthermore,

estimating sums of multiplicative characters requires some additional arguments, see for example, Lemma 42 below that could be of independent interest.

We note that bounds of multiplicative character sums, in a standard fashion lead to various asymptotic formulas about the distribution of power residues and primitive roots in the corresponding sequences. Such results can be derived in a very straightforward way and we do not give them here, see for example [25, 100, 105].

The results of this section are presented in the paper [115].

Let the polynomial system of m polynomials $F_1, \ldots, F_m \in \mathbb{F}_q[X_1, \ldots, X_m]$ be of the form (2.1). In this section we use a special class of multivariate polynomial systems (2.1) by imposing also the following condition on the polynomials H_i: for each $i = 1, \ldots, m$, there exists $s \in \{i+1, \ldots, m\}$, such that the polynomial H_i is of the form

$$\begin{aligned} H_i = X_{i+1}^{j_{i+1}} \ldots X_s^{j_s} \ldots X_m^{j_m} \\ + \overline{H}_i(X_{i+1}, \ldots, X_{s-1}, X_{s+1}, \ldots, X_m), \end{aligned} \tag{2.35}$$

where $j_s \geq 1$ and $\overline{H}_i \in \mathbb{F}_q[X_{i+1}, \ldots, X_{s-1}, X_{s+1}, \ldots, X_m]$.

2.9.2 Zeros of some polynomials

We need the following result.

Lemma 42. *Assume that the polynomial system of m polynomials $\mathcal{F}$ of the form (2.1) satisfies the conditions (2.2), (2.3) and (2.35), and such that $s_{1,2} \ldots s_{m-1,m} \neq 0$. We consider the polynomials $G_{j,k}, H_{j,k}$ defined as in Lemma 18. Then there exists a constant k_0, depending only on the degree of $\mathcal{F}$ such that for $k > l \geq k_0$ the polynomials*

$$R_{j,k,l} = G_{j,k}H_{j,l} - G_{j,l}H_{j,k}, \qquad j = 1, \ldots, m-1,$$

are nontrivial of degree $O(k^{m-1})$.

Proof. Easy computations show that the polynomials $G_{j,k}, H_{j,k}$ defined in Lemma 18 have the following concrete form

$$G_{j,k} = G_j G_j^{(2)} \ldots G_j^{(k)},$$

where $G_j^{(k)}(X_{j+1}, \ldots, X_m) = G_j(F_{j+1}^{(k-1)}, \ldots, F_m^{(k-1)})$, and

$$H_{j,k} = \sum_{i=1}^{k} H_j^{(i)} G_j^{(i+1)} \ldots G_j^{(k)},$$

where $H_j^{(k)}(X_{j+1}, \ldots, X_m) = H_j(F_{j+1}^{(k-1)}, \ldots, F_m^{(k-1)})$. Using this representation we get

$$R_{j,k,l} = -G_j G_j^{(2)} \ldots G_j^{(l)} \left(\sum_{i=1}^{k-l} H_j^{(l+i)} G_j^{(l+i+1)} \ldots G_j^{(k)} \right).$$

By (2.3) we see that if $k > l \ge k_0$ for sufficiently large k_0 then

$$\deg G_i^{(l+h)} \ge \deg H_i^{(l+h)} \ge \deg H_i^{(l+1)}$$

for $h = 1, \ldots, k-l$. In order to show that the polynomial $R_{j,k,l}$ is not identical zero it is sufficient to see that the $(l+1)$-th iteration of the polynomial H_i is a not identical zero. Let now X_s be the variable which gives the condition (2.35) for H_i in the construction of the polynomial system $\mathcal{F}$. We get

$$H_i^{(l+1)} = (F_{i+1}^{(l)})^{j_{i+1}} \ldots (F_s^{(l)})^{j_s} \ldots (F_m^{(l)})^{j_m} + \overline{H}_i(F_{i+1}^{(l)}, \ldots, F_{s-1}^{(l)}, F_{s+1}^{(l)}, \ldots, F_m^{(l)}),$$

and thus we note that $\deg_{X_s} H_j^{(l+1)} \ge j_s \deg_{X_s} F_s^{(l)} = j_s \ge 1$, which shows that the polynomial $R_{j,k,l}$ is not identical zero. For the degree statement we apply Lemma 18 and get the desired result if $k > l \ge k_0$ for sufficiently large k_0. □

2.9.3 General polynomial systems

Let $\chi_1, \ldots, \chi_m$ be m multiplicative characters of $\mathbb{F}_q$. We recall that a character χ is called *trivial* if $\chi(u) = 1$ for all $u \in \mathbb{F}_q^*$ and it is denoted by χ_0. We use the convention that $\chi(0) = 0$ for any multiplicative character χ of $\mathbb{F}_q$. Let $(\mathbf{w}_n)$ be a purely periodic sequence with period τ, given by (2.7), where the polynomial system of m polynomials

$$\mathcal{F} = \{F_1, \ldots, F_m\} \in \mathbb{F}_q[X_1, \ldots, X_m]$$

is of the form (2.1), satisfying the conditions (2.2), (2.3) and (2.35), and such that $s_{1,2} \ldots s_{m-1,m} \ne 0$.

We now estimate the character sums

$$S_N(\chi_1, \ldots, \chi_m) = \sum_{n=0}^{N-1} \prod_{i=1}^{m} \chi_i(w_{n,i}), \quad 1 \le N \le \tau.$$

Theorem 43. *Let $m \ge 2$, $\chi_1, \ldots, \chi_m$ be m multiplicative characters of $\mathbb{F}_q$, not all trivial, and let $(\mathbf{w}_n)$ be a purely periodic sequence with period τ, given by* (2.7)*, where the polynomial system of m polynomials*

$$\mathcal{F} = \{F_1, \ldots, F_m\} \subset \mathbb{F}_q[X_1, \ldots, X_m]$$

is of the form (2.1)*, satisfying the conditions* (2.2)*,* (2.3) *and* (2.35)*, and such that $s_{1,2} \ldots s_{m-1,m} \ne 0$. Then for any positive integer $N \le \tau$ we have*

$$S_N(\chi_1, \ldots, \chi_m) \ll N^{1/2} q^{(m^2-1)/(2m)} + N t^{-1} q^{1/2},$$

where t is the order of g_m and the implied constant depends only on the degree of $\mathcal{F}$ and m.

Proof. For any integer $k \geq 0$ we have

$$\left| S_N(\chi_1, \dots, \chi_m) - \sum_{n=0}^{N-1} \prod_{i=1}^{m} \chi_i(w_{n+k,i}) \right| \leq 2k,$$

and summing over $k = 0, \dots, K-1$ for any integer $K \geq 1$ we get

$$K \left| S_N(\chi_1, \dots, \chi_m) \right| \leq W + K^2, \tag{2.36}$$

where

$$W = \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \prod_{i=1}^{m} \chi_i(w_{n+k,i}) \right|.$$

Applying now the Cauchy-Schwarz inequality we obtain

$$W^2 \leq N \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \prod_{i=1}^{m} \chi_i(w_{n+k,i}) \right|^2 = N \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \prod_{i=1}^{m} \chi_i(F_i^{(k)}(\mathbf{w}_n)) \right|^2.$$

Completing the range of summation in the outer sum, we obtain

$$\begin{aligned} W^2 &\leq N \sum_{\mathbf{v} \in \mathbb{F}_q^m} \left| \sum_{k=0}^{K-1} \prod_{i=1}^{m} \chi_i(F_i^{(k)}(\mathbf{v})) \right|^2 \\ &\leq N \sum_{k,l=0}^{K-1} \left| \sum_{\mathbf{v} \in \mathbb{F}_q^m} \prod_{i=1}^{m} \chi_i(F_i^{(k)}(\mathbf{v})) \overline{\chi_i(F_i^{(l)}(\mathbf{v}))} \right| \\ &\leq KNq^m + 2N \sum_{0 \leq l < k < K} |T_{k,l}|, \end{aligned}$$

where

$$T_{k,l} = \sum_{\mathbf{v} \in \mathbb{F}_q^m} \prod_{i=1}^{m} \chi_i(F_i^{(k)}(\mathbf{v})) \overline{\chi_i(F_i^{(l)}(\mathbf{v}))}.$$

Let j be the least positive integer such that χ_j is a nontrivial character.

We consider first the case when $j < m$.

We now write Σ^* to denote that the values that lead to the poles of the involved rational functions are excluded from the range of summation. Then the sum $T_{k,l}$ becomes

$$T_{k,l} = q^{j-1} \sum_{v_j, \dots, v_m \in \mathbb{F}_q}^{*} \prod_{i=j}^{m} \chi_i \left(\frac{v_i G_{i,k}(v_{i+1}, \dots, v_m) + H_{i,k}(v_{i+1}, \dots, v_m)}{v_i G_{i,l}(v_{i+1}, \dots, v_m) + H_{i,l}(v_{i+1}, \dots, v_m)} \right).$$

Therefore

$$|T_{k,l}| \leq q^{j-1} \sideset{}{^*}\sum_{v_{j+1},\dots,v_m \in \mathbb{F}_q} \left| \sideset{}{^*}\sum_{v_j \in \mathbb{F}_q} \chi_j \left(\frac{v_j G_{j,k}(v_{j+1},\dots,v_m) + H_{j,k}(v_{j+1},\dots,v_m)}{v_j G_{j,l}(v_{j+1},\dots,v_m) + H_{j,l}(v_{j+1},\dots,v_m)} \right) \right|.$$

We apply now Lemma 6 and we see that the sum over the variable v_j is $O(q)$ if

$$G_{j,k}(v_{j+1},\dots,v_m)H_{j,l}(v_{j+1},\dots,v_m) = G_{j,l}(v_{j+1},\dots,v_m)H_{j,k}(v_{j+1},\dots,v_m),$$

and is $O(1)$ otherwise.

Let $R_{j,k,l} = G_{j,k}H_{j,l} - G_{j,l}H_{j,k}$. We see from Lemma 42 that if $k > l \geq k_0$ for a sufficiently large k_0 then $R_{j,k,l}$ is a nontrivial polynomial of degree $O(k^{m-j}) = O(k^{m-1})$. Thus estimating the sum $T_{k,l}$ reduces to counting the number of zeros of the polynomial $R_{j,k,l}$ over $\mathbb{F}_q$. Using now Lemma 1 we can estimate the sum $T_{k,l}$ as

$$|T_{k,l}| \ll k^{m-1}q^{m-1}.$$

Therefore, if $j < m$ then

$$W^2 \ll KNq^m + K^{m+1}Nq^{m-1}. \tag{2.37}$$

Inserting (2.37) in (2.36) we derive

$$S_N(\chi_1,\dots,\chi_m) \ll K^{-1/2}N^{1/2}q^{m/2} + K^{(m-1)/2}N^{1/2}q^{(m-1)/2} + K.$$

Choosing now

$$K = \lceil q^{1/m} \rceil$$

(and assuming that q is large enough, so $K \geq k_0$), after simple calculations we obtain that for $j < m$

$$S_N(\chi_1,\dots,\chi_{m+1}) \ll N^{1/2}q^{(m^2-1)/(2m)}. \tag{2.38}$$

We now study the case when $j = m$, that is,

$$S_N(\chi_1,\dots,\chi_m) = \sum_{n=0}^{N-1} \chi_m(w_{n,m}). \tag{2.39}$$

Clearly the bound is trivial if $t = 1$ (that is, for $g_m = 1$). So we now assume that $g_m \neq 1$. In this case we have

$$w_{n,m} = g_m^n \left(w_{0,m} - \frac{h_m}{1-g_m} \right) + \frac{h_m}{1-g_m}.$$

If

$$w_{0,m} = \frac{h_m}{1-g_m},$$

we have $\tau = 1$ and the bound is trivial. In the remaining case, we see that Corollary 13 applies to the sum in (2.39) and yields

$$S_N(\chi_1, \ldots, \chi_{m+1}) \ll Nt^{-1}q^{1/2} + q^{1/2}\log t. \tag{2.40}$$

for $j = m$.

Thus we see from (2.38) and (2.40) that for any j,

$$S_N(\chi_1, \ldots, \chi_{m+1}) \ll N^{1/2}q^{(m^2-1)/2m} + Nt^{-1}q^{1/2} + q^{1/2}\log t.$$

It remains to note that the last term never dominates and thus can be omitted. □

It is easy to see that Theorem 43 is nontrivial if for some fixed $\varepsilon > 0$ we have $N \ge q^{m-1/m+\varepsilon}$ and $t \ge q^{1/2+\varepsilon}$.

As in [107, 110, 111], we can discard the last "linear" component of the vector $\mathbf{w}_n$ and consider the sums

$$\widetilde{S}_N(\chi_1, \ldots, \chi_{m-1}) = \sum_{n=0}^{N-1}\prod_{i=1}^{m-1}\chi_i(w_{n,i}).$$

Clearly the proof of Theorem 43 implies that if at least one multiplicative character $\chi_1, \ldots, \chi_{m-1}$ is nontrivial then for any positive integer $N \le \tau$ we have

$$\widetilde{S}_N(\chi_1, \ldots, \chi_m) \ll N^{1/2}q^{(m^2-1)/(2m)}$$

(in fact in this case the estimate also holds for $h_m = 0$).

We observe that in the case $m = 1$ we have $t = \tau$ and the estimate

$$S_N(\chi_1) \ll q^{1/2}\log q$$

by Corollary 13.

We now obtain another bound, which is weaker than that of Theorem 43 for N close to q^m, but improves it for smaller values of N and in particular is nontrivial in wider range of $N \ge q^{m-1/2+\varepsilon}$ and $t \ge q^{m-1/m+\varepsilon}$. For this we consider higher powers and use the Hölder inequality in the proof of Theorem 43, but in this case instead of Lemma 6 we now have to use the Weil bound.

Theorem 44. *Let $m \ge 2$, $\chi_1, \ldots, \chi_m$ be m multiplicative characters of $\mathbb{F}_q$, not all trivial, and let $(\mathbf{w}_n)$ be a purely periodic sequence with period τ, given by (2.7), where the polynomial system of m polynomials*

$$\mathcal{F} = \{F_1, \ldots, F_m\} \subset \mathbb{F}_q[X_1, \ldots, X_m]$$

is of the form (2.1), satisfying the conditions (2.2), (2.3) and (2.35), and such that $s_{1,2}\ldots s_{m-1,m} \ne 0$. Then for any positive integer $N \le \tau$ we have

$$\begin{aligned} S_N(\chi_1, \ldots, \chi_m) \ll{}& N^{1-1/(2\nu)}q^{(m-1)(m+\nu)/(2\nu(m-1+\nu))} \\ &+ N^{1-1/(2\nu)}q^{(2m-1)/(4\nu)} + Nt^{-1}q^{1/2}, \end{aligned}$$

where t is the order of g_m and the implied constant depends only on the degree of $\mathcal{F}$, m and ν.

Proof. We recall (2.36) and the definition of W from the proof of Theorem 43. Applying now the Hölder inequality we obtain

$$\begin{aligned} W^{2\nu} &\leq N^{2\nu-1} \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \prod_{i=1}^{m} \chi_i(w_{n+k,i}) \right|^{2\nu} \\ &= N^{2\nu-1} \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \prod_{i=1}^{m} \chi_i(F_i^{(k)}(\mathbf{w}_n)) \right|^{2\nu}. \end{aligned}$$

Completing the range of summation in the outer sum, we obtain

$$\begin{aligned} W^{2\nu} &\leq N^{2\nu-1} \sum_{\mathbf{v}\in\mathbb{F}_q^m} \left| \sum_{k=0}^{K-1} \prod_{i=1}^{m} \chi_i(F_i^{(k)}(\mathbf{v})) \right|^{2\nu} \\ &\leq N^{2\nu-1} \sum_{k_1,\ell_1,\dots,k_\nu,\ell_\nu=k_0}^{K-1} \left| \sum_{\mathbf{v}\in\mathbb{F}_q^m} \prod_{i=1}^{m} \chi_i(\prod_{h=1}^{\nu} F_i^{(k_h)}(\mathbf{v}))\overline{\chi_i(\prod_{h=1}^{\nu} F_i^{(l_h)}(\mathbf{v}))} \right|. \end{aligned}$$

Let j be the least integer such that χ_j is a nontrivial character. Then

$$\begin{aligned} W^{2\nu} \leq N^{2\nu-1} q^{j-1} &\sum_{0\leq k_1,\ell_1,\dots,k_\nu,\ell_\nu<K} \sum_{v_{j+1},\dots,v_m\in\mathbb{F}_q}{}^{*} \\ &\left| \sum_{v_j\in\mathbb{F}_q}{}^{*} \chi_j \left(\prod_{h=1}^{\nu} \frac{v_j G_{j,k_h}(v_{j+1},\dots,v_m) + H_{j,k_h}(v_{j+1},\dots,v_m)}{v_j G_{j,l_h}(v_{j+1},\dots,v_m) + H_{j,l_h}(v_{j+1},\dots,v_m)} \right) \right|, \end{aligned}$$

where we write Σ^* to denote that the values that lead to the poles of the involved rational functions are excluded from the range of summation.

If in the sequence $k_1,\dots,k_\nu,l_1,\dots,l_\nu$ each element appears at least twice, we estimate the absolute value of the sum over v_j trivially by q. The number of such choices amongst $1\leq k_1,\dots,k_\nu,l_1,\dots,l_\nu\leq K$ is $O(K^\nu)$, where the implied constant depends on ν.

In the remaining $O(K^{2\nu})$ choices of $1\leq k_1,\dots,k_\nu,l_1,\dots,l_\nu\leq K$ we also estimate the sum over v_j trivially by q if

$$G_{j,h_1}H_{j,h_2} = G_{j,h_2}H_{j,h_1}$$

for some $h_1,h_2\in\{k_1,\dots,k_\nu,l_1,\dots,l_\nu\}$. By Lemmas 1 and 42 this number is

$$O(K^{m-j}q^{m-j-1}).$$

Otherwise we recall that by the Weil bound, see Theorem 10, the sum over v_j is $O(q^{1/2})$.

Collecting everything we get for $j<m$,

$$W^{2\nu} \ll N^{2\nu-1}(K^\nu q^m + K^{m-1+2\nu}q^{m-1} + K^{2\nu}q^{m-1/2})$$

and returning into (2.36) we obtain

$$S_N(\chi_1, \dots, \chi_m) \ll N^{1-1/(2\nu)} \left(K^{-1/2} q^{m/(2\nu)} + K^{(m-1)/(2\nu)} q^{(m-1)/(2\nu)} + q^{(2m-1)/(4\nu)}\right) + K.$$

Choosing now

$$K = \left\lceil q^{1/(m-1+\nu)} \right\rceil,$$

after simple calculations we obtain that for $j < m$

$$S_N(\chi_1, \dots, \chi_m) \ll N^{1-1/(2\nu)} q^{(m(m-1+\nu)-\nu)/(2\nu(m-1+\nu))} + N^{1-1/(2\nu)} q^{(2m-1)/(4\nu)}. \tag{2.41}$$

For $j = m$, exactly as in the proof of Theorem 43, we get

$$S_N(\chi_1, \dots, \chi_{m+1}) \ll N t^{-1} q^{1/2} + q^{1/2} \log t. \tag{2.42}$$

Thus, putting together the estimates (2.41) and (2.42), for any j we get the desired result. □

Note that the choice $\nu = m - 1$ in Theorem 44 gives the simpler bound

$$\max_{\gcd(a_1,\dots,a_m,p)=1} |S_{\mathbf{a}}(N)| \ll N^{1-1/(2(m-1))} q^{(2m-1)/(4(m-1))} + N t^{-1} q^{1/2},$$

where the implied constant depends only on $\deg \mathcal{F}$ and m. This bound is better than the bound of Theorem 43 if $N \le q^{m-1/(2m)-\varepsilon}$ and is nontrivial if $N \ge q^{m-1/2+\varepsilon}$.

2.9.4 Permutation polynomial systems

We now consider polynomial systems of the form (2.1) which permute the elements of $\mathbb{F}_q^m$.

In this section we estimate the following sum

$$V_N(\chi_1, \dots, \chi_m) = \sum_{\mathbf{v} \in \mathbb{F}_q^m} \left| \sum_{n=0}^{N-1} \prod_{i=1}^{m} \chi_i(F_i^{(n)}(\mathbf{v})) \right|^2.$$

Theorem 45. *Let $\chi_1, \dots, \chi_m$ be m multiplicative characters of $\mathbb{F}_q$, not all trivial and let the permutation polynomial system $\mathcal{F}$ of m polynomials of the form (2.1) satisfy the conditions (2.2), (2.3) and (2.35), and be such that $s_{1,2} \dots s_{m-1,m} \ne 0$. Then for any positive integer $N \le \tau$ we have*

$$V_N(\chi_1, \dots, \chi_m) \ll A(N, q) + N t^{-1} q^{1/2},$$

where t is the order of g_m,

$$A(N, q) = \begin{cases} N q^m & \text{if } N \le q^{1/m}, \\ N^2 q^{(m-1)(m+1)/m} & \text{if } N > q^{1/m}, \end{cases}$$

and the implied constant depends only on the degree of $\mathcal{F}$ and m.

Proof. Let j be the least positive integer such that χ_j is a nontrivial character. We consider first the case when $j < m$. Using the same arguments as in Theorem 43 we get

$$V_N(\chi_1, \dots, \chi_m) \ll Nq^m + N^{m+1}q^{m-1}. \tag{2.43}$$

Because $\mathcal{F}$ is a permutation system, for any integer L we obtain

$$\begin{aligned}
&\sum_{\mathbf{v}\in\mathbb{F}_q^m} \left| \sum_{n=L}^{L+N-1} \prod_{i=1}^{m} \chi_i(F_i^{(n)}(\mathbf{v})) \right|^2 \\
&\quad = \sum_{\mathbf{v}\in\mathbb{F}_q^m} \left| \sum_{n=0}^{N-1} \prod_{i=1}^{m} \chi_i(F_i^{(n)}(F_1^{(L)}(\mathbf{v}), \dots, F_m^{(L)}(\mathbf{v}))) \right|^2 \\
&\quad = \sum_{\mathbf{v}\in\mathbb{F}_q^m} \left| \sum_{n=0}^{N-1} \prod_{i=1}^{m} \chi_i(F_i^{(n)}(\mathbf{v})) \right|^2 = V_N(\chi_1, \dots, \chi_m).
\end{aligned}$$

Therefore, for any positive integer $K \le N$, separating the inner sum into at most $N/K+1$ subsums of length at most K and using (2.43) we obtain

$$\begin{aligned}
V_N(\chi_1, \dots, \chi_m) &\ll (Kq^m + K^{m+1}q^{m-1})N^2K^{-2} \\
&= N^2(K^{-1}q^m + K^{m-1}q^{m-1}).
\end{aligned}$$

Thus, selecting

$$K = \min\{N, \lfloor q^{1/m} \rfloor\}$$

and taking into account that $N^{-1}q^m \ge N^{m-1}q^{m-1}$ for $N \le q^{1/m}$, for $j < m$ we obtain that

$$V_N(\chi_1, \dots, \chi_m) \ll A(N, q).$$

The second summand in the bound is obtained in the case $j = m$ exactly as in the proof of Theorem 43. □

As before we note that for

$$\widetilde{V}_N(\chi_1, \dots, \chi_{m-1}) = \sum_{\mathbf{v}\in\mathbb{F}_q^m} \left| \sum_{n=0}^{N-1} \prod_{i=1}^{m-1} \chi_i(F_i^{(n)}(\mathbf{v})) \right|^2$$

we have

$$\widetilde{V}_N(\chi_1, \dots, \chi_{m-1}) \ll A(N, q),$$

provided that at least one multiplicative character $\chi_1, \dots, \chi_m$ is nontrivial and $N \le \tau$ (and again this also holds for $h_m = 0$).

We note that the bounds of Theorems 44 and 45 (but not of Theorem 43) can easily be extended to mixed sums of additive and multiplicative characters.

Furthermore, fixing a basis $\{\beta_1, \ldots, \beta_m\}$ of the finite field $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ we can identify the vector sequence $(\mathbf{w}_n) = (w_{n,1}, \ldots, w_{n,m})$ over $\mathbb{F}_q$ with the sequence (W_n) over $\mathbb{F}_{q^m}$ defined by

$$W_n = w_{n,1}\beta_1 + \ldots + w_{n,m}\beta_m, \qquad n \geq 0.$$

It would be interesting to study character sums

$$\Sigma_N(\chi) = \sum_{n=0}^{N-1} \chi(W_n), \qquad 1 \leq N \leq \tau,$$

with a nontrivial character χ of $\mathbb{F}_{q^m}$. In principle, our approach works for the sums $\Sigma_N(\chi)$ as well, however an appropriate analogue of Lemma 42 is needed, which may require some new ideas.

2.10 Triangular polynomial systems with constant multipliers

2.10.1 Outline

In the previous sections we considered multivariate polynomial systems $\mathcal{F} = \{F_1, \ldots, F_m\}$ of m polynomials in m variables over a finite field $\mathbb{F}_q$ having the "triangular" form

$$\begin{aligned}
&F_1(X_1, \ldots, X_m) = X_1 G_1(X_2, \ldots, X_m) + H_1(X_2, \ldots, X_m),\\
&\ldots\\
&F_{m-1}(X_1, \ldots, X_m) = X_{m-1} G_{m-1}(X_m) + H_{m-1}(X_m),\\
&F_m(X_1, \ldots, X_m) = g_m X_m + h_m,
\end{aligned} \tag{2.44}$$

with $G_i, H_i \in \mathbb{F}_q[X_{i+1}, \ldots, X_m]$, $i = 1, \ldots, m-1$, and $g_m, h_m \in \mathbb{F}_q$, $g_m \neq 0$, which satisfies the conditions (2.2) and (2.3). For this class of polynomials, it has been shown in Section 2.2 that the degrees of the iterations of the polynomials F_i, $i = 1, \ldots, m$, grow significantly slower, a result that leads to much better estimates of exponential sums, and thus of discrepancy, for vectors generated by these iterations.

Furthermore, it has been shown in Section 2.5.3 that in the case when such a polynomial map generates a permutation of the corresponding vector space, one can get better results "on average" over all initial values.

Let p be a prime and $\mathbb{F}_p$ be a finite field with p elements. In the paper [108] we study a special case of the systems (2.1), namely we consider the polynomials G_i to be constant polynomials. More precisely, we consider systems of $m \geq 2$ polynomials $F_i \in \mathbb{F}_p[X_1, \ldots, X_m]$, $i = 1, \ldots, m$, over $\mathbb{F}_p$ defined in the following way:

$$\begin{aligned}
&F_1(X_1, \ldots, X_m) = g_1 X_1 + H_1(X_2, \ldots, X_m),\\
&\ldots\\
&F_{m-1}(X_1, \ldots, X_m) = g_{m-1} X_{m-1} + H_{m-1}(X_m),\\
&F_m(X_1, \ldots, X_m) = g_m X_m + h_m,
\end{aligned} \tag{2.45}$$

where

$$g_i, h_m \in \mathbb{F}_p, \quad g_i \notin \{0, 1\}, \quad H_i \in \mathbb{F}_p[X_{i+1}, \ldots, X_m], \quad i = 1, \ldots, m.$$

We note that in the case when the polynomials H_i, $i = 1, \ldots, m-1$, are constant polynomials, we simply have a system of m independent polynomials. Clearly iterations of such systems generate vectors of the form $(A_1 g_1^n + B_1, \ldots, A_m g_m^n + B_m)$. Such systems have actually been suggested as pseudorandom number generators, however with very limited progress. In fact, prior the very recent work of Bourgain [15], no interesting results have been known for such systems and corresponding vectors over finite fields. However, for similar systems with constant polynomials H_i, $i = 1, \ldots, m-1$, but defined over a residue ring modulo a prime power p^α for a fixed prime p, one can also use the estimates of [124], which apply to an arbitrary linear recurrence sequence modulo p^α. However, if the polynomials H_i, $i = 1, \ldots, m-1$, are not constant polynomials over a finite field $\mathbb{F}_p$ of p elements (for prime p), this "mixing" increases the length of the orbits and also allows us to use very different methods and thus derive a series of new results. Naturally, the strength of our bounds depends on the multiplicative orders t_i of g_i in $\mathbb{F}_p$, $i = 1, \ldots, m$.

We remark that for the polynomial systems (2.45) the conditions (2.2) and (2.3) are not satisfied anymore, and thus the previous results obtained for the systems given by (2.1) are not applicable for this case.

We follow the same technique as in [107, 111] and we exploit the special structure of iterations of the polynomial systems introduced below that allows us to replace the use of the Weil bound (see [84, Chapter 5]) by a more elementary and stronger estimate on the corresponding exponential sums which in turn leads to a better final result on the distribution of the vectors generated by such dynamical systems. In fact, since our construction can easily be extended to polynomials over commutative rings, the new estimate can also be used to study polynomial maps over residue rings (while the Weil bound does not apply there).

Our results expand the class of polynomial dynamical systems which admit good estimates on exponential sums and thus have strong uniform distribution properties of elements in their orbits.

2.10.2 Iterations of triangular polynomial systems

We can describe explicitly the iterations of the polynomials F_i as follows:

Lemma 46. *Let $F_1, \ldots, F_m \in \mathbb{F}_p[X_1, \ldots, X_m]$ be as in (2.45). Then for $i = 1, \ldots, m$ and $k = 0, 1, \ldots$, for the polynomials $F_i^{(k)}$ given by (2.4) we have*

$$F_i^{(k)} = g_i^k X_i + H_{i,k}(X_{i+1}, \ldots, X_m),$$

where $H_{i,k} \in \mathbb{F}_p[X_{i+1}, \ldots, X_m]$ for $i = 1, \ldots, m$.

We note that the system defined above is a permutation system, that is a system of multivariate polynomials in $\mathbb{F}_p[X_1, \ldots, X_m]$ which induces a map that permutes the elements

of $\mathbb{F}_p^m$, given by absolutely irreducible polynomials. Moreover, the iterated polynomials $F_i^{(k)}$ have exactly the same form as the polynomials F_i and are also absolutely irreducible polynomials.

We generate the m-dimensional multisequence

$$(\mathbf{u}_n) = ((u_{n,1}, \ldots, u_{n,m}))$$

exactly as in (2.7) and we keep all the notations and conventions from Section 2.4.

2.10.3 Exponential sums and discrepancy

Assume that the sequence $\{\mathbf{u}_n\}$ generated by (2.6) and (2.7) is purely periodic with an arbitrary period τ. For an integer vector $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{Z}^m$ we introduce the exponential sum

$$S_{\mathbf{a}}(N) = \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{i=1}^{m} a_i u_{n,i} \right),$$

where

$$\mathbf{e}_p(z) = \exp(2\pi i z/p).$$

Also, as before t_i denotes the multiplicative orders of g_i in $\mathbb{F}_p$, $i = 1, \ldots, m$.

As in Lemma 21 we have the following description of the linear combinations of the iterations of the polynomials F_i:

Lemma 47. *Let $\mathcal{F}$ be the polynomial system (2.45). For any two integers $k > l$ and any nonzero integer vector $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_p^m$, we define the polynomial*

$$F_{\mathbf{a},k,l} = \sum_{i=1}^{m} a_i \left(F_i^{(k)} - F_i^{(l)} \right),$$

where the polynomials $F_i^{(k)}$ are given by (2.4). If $g_s^k \not\equiv g_s^l \pmod{t_s}$ where $1 \le s \le m$ is the smallest integer such that $a_s \ne 0$, then we have

$$\sum_{x_1, \ldots, x_m = 1}^{p} \mathbf{e}_p \left(F_{\mathbf{a},k,l}(x_1, \ldots, x_m) \right) = 0.$$

Proof. By Lemma 46 we have

$$\begin{aligned} &F_{\mathbf{a},k,l}(x_1, \ldots, x_m) \\ &\quad = \sum_{i=s}^{m} a_i \left((g_i^k - g_i^l) x_i + (H_{i,k}(x_{i+1}, \ldots, x_m) - H_{i,l}(x_{i+1}, \ldots, x_m)) \right) \\ &\quad = a_s (g_s^k - g_s^l) x_s + \Psi_{\mathbf{a},k,l}(x_{s+1}, \ldots, x_m), \end{aligned}$$

where

$$\Psi_{\mathbf{a},k,l}(x_{s+1},\dots,x_m) = \sum_{i=s+1}^{m} \left(a_i(g_i^k - g_i^l)x_i\right) + \sum_{i=s}^{m} a_i \left(H_{i,k}(x_{s+1},\dots,x_m) - H_{i,l}(x_{s+1},\dots,x_m)\right).$$

Therefore,

$$\sum_{x_1,\dots,x_m=1}^{p} \mathbf{e}_p\left(F_{\mathbf{a},k,l}(x_1,\dots,x_m)\right) = p^s \sum_{x_{s+1},\dots,x_m=1}^{p} \mathbf{e}_p\left(\Psi_{\mathbf{a},k,l}(x_{s+1},\dots,x_m)\right) \cdot \sum_{x_s=1}^{p} \mathbf{e}_p\left(a_s(g_s^k - g_s^l)x_s\right).$$

Recalling the identity

$$\sum_{u=1}^{p} \mathbf{e}_p(cu) = \begin{cases} p, & \text{if } c \equiv 0 \pmod p, \\ 0, & \text{if } c \not\equiv 0 \pmod p, \end{cases}$$

see Theorem 7, we get the desired result. □

Following the same technique as in Section 2.5 we obtain the following estimate for the exponential sum $S_{\mathbf{a}}(N)$:

Theorem 48. *Let the sequence $\{\mathbf{u}_n\}$ be generated by (2.6) and (2.7), where the system of $m \geq 2$ polynomials $\mathcal{F} = \{F_1,\dots,F_m\} \in \mathbb{F}_p[X_1,\dots,X_m]$ is of the form (2.45). Assume that $\{\mathbf{u}_n\}$ is purely periodic with period τ. Then for any positive integer $N \leq \tau$ and any nonzero vector $\mathbf{a} \in \mathbb{F}_p^m$ we have the bound*

$$S_{\mathbf{a}}(N) \ll N^{1/2} t_s^{-1/2} p^{m/2},$$

where $1 \leq s \leq m$ is the smallest integer such that $a_s \neq 0$ and t_s is the order of g_s in $\mathbb{F}_p$.

Proof. We follow the same argument as in the proof of Theorem 22.

In particular, we obtain that for any integer $K \geq 1$,

$$K|S_{\mathbf{a}}(N)| \leq W + K^2, \tag{2.46}$$

where

$$W = \left|\sum_{n=0}^{N-1} \sum_{k=1}^{K} \mathbf{e}_p\left(\sum_{i=1}^{m} a_i u_{n+k,i}\right)\right|.$$

Using the Cauchy-Schwarz inequality we derive (again exactly the same way as in Theorem 22)

$$W^2 \leq N \sum_{k,l=1}^{K} \sum_{x_1,\dots,x_m \in \mathbb{F}_p^m} \mathbf{e}_p(F_{\mathbf{a},k,l}(x_1,\dots,x_m)).$$

Because $g_s^k - g_s^l \equiv 0 \pmod{p}$ if and only if we have $k \equiv l \pmod{t_s}$, for $O(K(Kt_s^{-1}+1))$ elements k, l such that $k \equiv l \pmod{t_s}$ we estimate the sum trivially by p^m. Furthermore, for $k \not\equiv l \pmod{t_s}$, using Lemma 47 we see that the sum simply vanishes. We obtain the estimate

$$W^2 \ll NK(Kt_s^{-1}+1)p^m.$$

Choosing now $K = t_s$ and inserting the above bound in (2.46) we obtain the desired result. □

Using now Lemma 14 and Theorem 48 we obtain the following estimate on the discrepancy of the sequence of vectors generated by the polynomial systems of the form (2.45).

Theorem 49. *Let the sequence $\{\mathbf{u}_n\}$ be generated by (2.6) and (2.7), where the system of $m \geq 2$ polynomials $\mathcal{F} = \{F_1, \ldots, F_m\} \in \mathbb{F}_p[X_1, \ldots, X_m]$ is of the form (2.45). Assume that $\{\mathbf{u}_n\}$ is purely periodic with period τ. Then for any positive integer $N \leq \tau$, the discrepancy $\Delta_N(\Gamma)$ of the sequence*

$$\Gamma = \left\{ \left(\frac{u_{n,1}}{p}, \ldots, \frac{u_{n,m}}{p} \right), \qquad n = 0, \ldots, N-1 \right\},$$

satisfies the bound

$$\Delta_N(\Gamma) = O(N^{-1/2} t^{-1/2} p^{m/2} (\log p)^m),$$

where $t = \min\{t_s | s = 1, \ldots, m\}$.

We note that both Theorems 48 and 49 are nontrivial if $\tau \geq N \geq t^{-1}(\log p)^{2m} p^m$.

2.10.4 Average case over all initial values

We follow the scheme previously introduced in Section 2.5.3 for estimating the discrepancy on average of the sequence generated by (2.6) and (2.7).

For a vector $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_p^m$ and integers c, M, N with $M \geq 1$ and $N \geq 1$, we introduce

$$V_{\mathbf{a},c}(M,N) = \sum_{v_1,\ldots,v_m \in \mathbb{F}_p} \left| \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=1}^{m} a_j F_j^{(n)}(v_1, \ldots, v_m) \right) \mathbf{e}_M(cn) \right|^2.$$

Theorem 50. *Let the polynomial system of m polynomials*

$$\mathcal{F} = \{F_1, \ldots, F_m\} \in \mathbb{F}_p[X_1, \ldots, X_m], \quad m \geq 2,$$

of the form (2.45). Then for any positive integers c, M, N and any nonzero vector $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_p^m$ we have

$$V_{\mathbf{a},c}(M,N) \ll A(N,p),$$

where

$$A(N,p) = \begin{cases} Np^m & \text{if } N \leq t_s, \\ N^2 t_s^{-1} p^m & \text{if } N > t_s, \end{cases}$$

and $s \leq m$ is the smallest integer such that $a_s \neq 0$.

Proof. We have

$$V_{\mathbf{a},c}(M,N) = \sum_{k,l=0}^{N-1} \mathbf{e}_M(c(k-l)) \sum_{\mathbf{v}\in\mathbb{F}_p^m} \mathbf{e}_p\left(\sum_{j=1}^{m} a_j\left(F_j^{(k)}(\mathbf{v}) - F_j^{(l)}(\mathbf{v})\right)\right)$$
$$\le \sum_{k,l=0}^{N-1}\left|\sum_{\mathbf{v}\in\mathbb{F}_p^m} \mathbf{e}_p\left(\sum_{j=1}^{m} a_j\left(F_j^{(k)}(\mathbf{v}) - F_j^{(l)}(\mathbf{v})\right)\right)\right|.$$

As in Theorem 48, for $O(N(Nt_s^{-1}+1))$ elements k,l such that $k \equiv l \pmod{t_s}$, we estimate the inner sum trivially by p^m. Furthermore, for $k \not\equiv l \pmod{t_s}$, using Lemma 47 we see that the sum simply vanishes.

Hence,

$$V_{\mathbf{a},c}(M,N) \ll N(Nt_s^{-1}+1)p^m. \tag{2.47}$$

Because $\mathcal{F}$ is a permutation polynomial system and using (2.8), for any integer L we obtain

$$\sum_{\mathbf{v}\in\mathbb{F}_p^m}\left|\sum_{n=L}^{L+N-1} \mathbf{e}_p\left(\sum_{j=1}^{m} a_j F_j^{(n)}(\mathbf{v})\right)\mathbf{e}_M(cn)\right|^2$$
$$= \sum_{\mathbf{v}\in\mathbb{F}_p^m}\left|\sum_{n=0}^{N-1} \mathbf{e}_p\left(\sum_{j=1}^{m} a_j F_j^{(n)}\left(F_1^{(L)}(\mathbf{v}),\dots,F_m^{(L)}(\mathbf{v})\right)\right)\mathbf{e}_M(cn)\right|^2$$
$$= \sum_{\mathbf{v}\in\mathbb{F}_p^m}\left|\sum_{n=0}^{N-1} \mathbf{e}_p\left(\sum_{j=1}^{m} a_j F_j^{(n)}(\mathbf{v})\right)\mathbf{e}_M(cn)\right|^2 = V_{\mathbf{a},c}(M,N).$$

Therefore, for any positive integer $K \le N$, separating the inner sum into at most $N/K+1$ subsums of length at most K, and using (2.47), we derive

$$V_{\mathbf{a},c}(M,N) \ll K(Kt_s^{-1}+1)p^m N^2 K^{-2} = N^2 t_s^{-1} p^m + K^{-1}N^2 p^m.$$

Thus, selecting $K = \min\{N, t_s\}$ we obtain the desired result. □

Now, exactly as in Theorem 26, combining Lemma 14 with the bound obtained in Theorem 50 we obtain stronger estimates for the discrepancy "on average" over all initial values.

Theorem 51. *Let $0 < \varepsilon < 1$ and let the sequence $\{\mathbf{u}_n\}$ be generated by (2.6) and (2.7), where the system of $m \ge 2$ polynomials $\mathcal{F} = \{F_1,\dots,F_m\} \in \mathbb{F}_p[X_1,\dots,X_m]$ is of the form (2.45). Then for all initial values $\mathbf{v} \in \mathbb{F}_p^m$ except at most $O(\varepsilon p^m)$ of them, and any positive integer $N \le p^m$, the discrepancy $\Delta_N(\Gamma(\mathbf{v}))$ of the sequence*

$$\Gamma(\mathbf{v}) = \left\{\left(\frac{u_{n,1}}{p},\dots,\frac{u_{n,m}}{p}\right), \qquad n = 0,\dots,N-1\right\},$$

satisfies the bound

$$\Delta_N(\Gamma(\mathbf{v})) \le \varepsilon^{-1} B(N,p),$$

where

$$B(N,p) = \begin{cases} N^{-1/2}(\log N)^{m+1}\log p & \text{if } N \le t, \\ t^{-1/2}(\log N)^{m+1}\log p & \text{if } N > t, \end{cases}$$

and $t = \min\{t_s | s = 1, \ldots, m\}$.

We note that Theorem 51 is nontrivial if $N \ge (\log p)^{2+\varepsilon}$ for some $\varepsilon > 0$.

We remark that our bounds of exponential sums can be immediately extended to arbitrary finite fields. Furthermore, our approach also applies to the same polynomial systems over residue rings and also leads to similar results.

2.11 Combinatorial approach

2.11.1 Outline

In [109] we study the sequences generated by the iterations of m polynomials $F_j \in \mathbb{F}_p[X_1, \ldots, X_m]$, $j = 1, \ldots, m$, in m variables over a finite field $\mathbb{F}_p$ of p elements, where p is a prime. For these sequences we obtain bounds of exponential sums and also of discrepancy, provided that their period is large enough.

The approaches presented in the previous sections have been based on the precise knowledge of the growth rate of the degrees of the iterations of the polynomial system $\mathcal{F} = (F_1, \ldots, F_m)$.

In [61, 62] in the case of very special polynomial systems (with $F_i = X_{i-1}$, $i = 2, \ldots, m$) three groups of conditions have been suggested which guarantee the monotonic growth of the first component of the iterations.

In this section we suggest a new approach, based on some combinatorial arguments, which avoids the need to verify this property. It applies to arbitrary polynomial systems, such that their iterations on $\mathbb{F}_p^m$ vectors generate sufficiently long trajectories. We remark that this condition is anyway needed for the bound of exponential sums to be nontrivial so it is not an additional restriction. In particular, as two very special cases of our results we recover those of [61] and [62].

2.11.2 Construction

For a system

$$\mathcal{F} = \{F_1(X_1, \ldots, X_m), \ldots, F_m(X_1, \ldots, X_m)\}$$

of m polynomials in m variables over $\mathbb{F}_p$, we consider sequences of vectors $\mathbf{u}_n = (u_{n,1}, \ldots, u_{n,m})$ in $\mathbb{F}_p^m$ defined by the recurrence congruence modulo a prime p of the form

$$u_{n+1,i} = F_i(u_{n,1}, \ldots, u_{n,m}), \qquad n = 0, 1, \ldots,$$

given by (2.7) with some *initial values* $\mathbf{u}_0 = (u_{0,1}, \ldots, u_{0,m})$.

We consider the same conventions and notation as in Section 2.4.

Clearly the sequence of vectors $\{\mathbf{u}_n\}$ is eventually periodic with some period $t \le p^m$, that is, for some integer $s \ge 0$

$$\mathbf{u}_{n+t} = \mathbf{u}_n, \qquad n = s, s+1, \ldots .$$

We always assume that s and t are chosen to minimise the sum

$$T = s + t \le p^m.$$

Thus, in particular, T is the *trajectory length* of the iterations of the initial vector $\mathbf{u}_0$ and hence the vectors $\mathbf{u}_1, \ldots, \mathbf{u}_T$ are pairwise distinct.

Lemma 52. *Let $\mathcal{F} = \{F_1, \ldots, F_m\} \subset \mathbb{F}_p[X_1, \ldots, X_m]$ be a system of m polynomials in m variables over $\mathbb{F}_p$ of degree at most D. Assume that for some initial vector $\mathbf{u}_0 \in \mathbb{F}_p^m$ the sequence of vectors $\{\mathbf{u}_n\}$ given by (2.7) has the trajectory length T. Then for any nonnegative integers $k < \ell \le \lceil T/p^{m-1} \rceil - 1$ and any nonzero $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_p^m$,*

$$F_{\mathbf{a},k,\ell} = \sum_{i=1}^{m} a_i \left(F_i^{(\ell)} - F_i^{(k)} \right),$$

is a nonconstant polynomial of degree

$$\deg F_{\mathbf{a},k,\ell} = O(D^\ell).$$

Proof. The degree bound is immediate.

We now assume that for some $k < \ell < T/p^{m-1}$ and nonzero $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_p^m$ the polynomial $F_{\mathbf{a},k,\ell}$ vanishes, that is, we have the identity

$$\sum_{i=1}^{m} a_i F_i^{(\ell)}(X_1, \ldots, X_m) = \sum_{i=1}^{m} a_i F_i^{(k)}(X_1, \ldots, X_m).$$

Substituting $F_i^{(h)}$ instead of X_i, $i = 1, \ldots, m$, we obtain the identity

$$\sum_{i=1}^{m} a_i F_i^{(\ell)}(F_1^{(h)}, \ldots, F_m^{(h)}) = \sum_{i=1}^{m} a_i F_i^{(k)}(F_1^{(h)}, \ldots, F_m^{(h)})$$

or

$$\sum_{i=1}^{m} a_i F_i^{(h+\ell)}(X_1, \ldots, X_m) = \sum_{i=1}^{m} a_i F_i^{(h+k)}(X_1, \ldots, X_m).$$

Furthermore, if we put $\tau = \ell - k$ we see that for any $n \ge \ell$

$$\sum_{i=1}^{m} a_i F_i^{(n)}(X_1, \ldots, X_m) = \sum_{i=1}^{m} a_i F_i^{(n-\tau)}(X_1, \ldots, X_m).$$

Thus, for any $n \ge 0$ there exists an integer r with $0 \le r \le \lceil T/p^{m-1} \rceil - 1$ and such that

$$\sum_{i=1}^{m} a_i F_i^{(n)}(X_1, \ldots, X_m) = \sum_{i=1}^{m} a_i F_i^{(r)}(X_1, \ldots, X_m)$$

and thus

$$\sum_{i=1}^{m} a_i u_{n,i} = \sum_{i=1}^{m} a_i u_{r,i}. \tag{2.48}$$

Since the right hand side of (2.48) takes at most $\lceil T/p^{m-1} \rceil - 1$ possible values, if such a value is fixed, there are p^{m-1} possibilities for $\mathbf{u}_n$ to satisfy the corresponding linear equation over $\mathbb{F}_p$. We see that $\mathbf{u}_n$ takes at most $(\lceil T/p^{m-1} \rceil - 1)\, p^{m-1} < T$ possible values, which contradicts the definition of T. □

2.11.3 Exponential sums and discrepancy

In [109] we follow the scheme previously introduced in [99, 100], and obtain a broad extension of the results of [61, 62]. In particular, we use Lemma 52 instead of the degree argument as in [61, 62] to treat much more general polynomial systems.

As in the previous sections, for an integer vector $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{Z}^m$ we introduce the exponential sum

$$S_{\mathbf{a}}(N) = \sum_{n=0}^{N-1} \mathbf{e}\left(\sum_{i=1}^{m} a_i u_{n,i} \right).$$

Theorem 53. *Let the sequence $\{\mathbf{u}_n\}$ be given by (2.7), where the family of m polynomials $\mathcal{F} = \{f_1, \ldots, f_m\} \in \mathbb{F}_p[X_1, \ldots, X_m]$ is of degree at most D. Assume that the sequence $\{\mathbf{u}_n\}$ given by (2.7) has the trajectory length T. Then for any positive integer $N \le T$, the bound*

$$\max_{\gcd(a_1, \ldots, a_m, p) = 1} |S_{\mathbf{a}}(N)| = O\left(N^{1/2} p^{m/2} (\log p)^{-1/2}\right)$$

holds, where the implied constant depends only on D and m.

Proof. Select any $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{Z}^m$ with $\gcd(a_1, \ldots, a_m, p) = 1$. It is obvious that for any integer $k \ge 0$ we have

$$\left| S_{\mathbf{a}}(N) - \sum_{n=0}^{N-1} \mathbf{e}\left(\sum_{i=1}^{m} a_i u_{n+k,i} \right) \right| \le 2k.$$

Therefore, for any integer $K \ge 1$,

$$K |S_{\mathbf{a}}(N)| \le W + K^2, \tag{2.49}$$

where

$$W = \left| \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \mathbf{e}\left(\sum_{i=1}^{m} a_i u_{n+k,i} \right) \right| \le \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \mathbf{e}\left(\sum_{i=1}^{m} a_i u_{n+k,i} \right) \right|.$$

As before, we define the sequence of polynomials

$$F_i^{(k)}(X_1,\dots,X_m) \in \mathbb{F}_p[X_1,\dots,X_m]$$

by (2.4). Then using the Cauchy-Schwarz inequality and recalling that the vectors $\mathbf{u}_n$, $0 \le n < N \le T$ are pairwise distinct, we derive

$$\begin{aligned} W^2 &\le N \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \mathbf{e}\left(\sum_{i=1}^{m} a_i F_i^{(k)}(\mathbf{u}_n) \right) \right|^2 \\ &\le N \sum_{w_1,\dots,w_m \in \mathbb{F}_p} \left| \sum_{k=0}^{K-1} \mathbf{e}\left(\sum_{i=1}^{m} a_i F_i^{(k)}(w_1,\dots,w_m) \right) \right|^2 \\ &= N \sum_{k,\ell=0}^{K-1} \sum_{\mathbf{w}\in\mathbb{F}_p^m} \mathbf{e}(F_{\mathbf{a},k,\ell}(\mathbf{w})), \end{aligned}$$

where the polynomial $F_{\mathbf{a},k,\ell}$ is defined as in Lemma 52.

We now assume that

$$K \le \lceil T/p^{m-1} \rceil . \tag{2.50}$$

Then for K pairs k and ℓ with $k = \ell$, we estimate the inner sum trivially by p^m.

For the other $O(K^2)$ pairs k and ℓ we see from (2.50) that the conditions of Lemma 52 are satisfied so we can apply Lemma 9 getting the upper bound $D^{K-1}p^{m-1/2}$ for the inner sum.

Hence,

$$W^2 \ll KNp^m + D^K K^2 N p^{m-1/2}.$$

Inserting this bound in (2.49), we derive

$$S_{\mathbf{a}}(N) \ll K^{-1/2}N^{1/2}p^{m/2} + D^{K/2}N^{1/2}p^{(2m-1)/4} + K.$$

We now choose

$$K = \left\lceil 0.4 \frac{\log p}{\log(D+1)} \right\rceil,$$

and notice that if, say, $T \le p^{m-1/2}$ then the bound of the theorem is trivial, and that for $T > p^{m-1/2}$ the condition (2.50) is obviously satisfied. Now, after simple calculations, we obtain the desired result. □

Clearly, the bound of Theorem 53 is nontrivial starting with the values

$$T \ge N \ge p^m / \log m.$$

Now, combining Lemma 14 with the bound obtained in Theorem 53 and taking $L = \lceil \log p \rceil$ we obtain:

Theorem 54. *Let the sequence* $\{\mathbf{u}_n\}$ *be given by* (2.7)*, where the family of* m *polynomials* $\mathcal{F} = \{F_1, \ldots, F_m\} \in \mathbb{F}_p[X_1, \ldots, X_m]$ *of degree at most* D*. Assume that the sequence* $\{\mathbf{u}_n\}$ *given by* (2.7) *has the trajectory length* T*. Then for any positive integer* $N \le T$*, the discrepancy* $\Delta_N(\Gamma)$ *of the sequence*

$$\Gamma = \left\{ \left(\frac{u_{n,1}}{p}, \ldots, \frac{u_{n,m}}{p} \right), \qquad n = 0, \ldots, N-1 \right\},$$

satisfies the bound

$$\Delta_N(\Gamma) \ll p^{m/2} N^{-1/2} (\log p)^{-1/2} (\log \log p)^m,$$

where the implied constant depends only on D *and* m*.*

2.12 Remarks and open questions

One of the attractive choices of polynomials (2.1), which leads to a very fast pseudorandom number generator is

$$G_i(X_{i+1}, \ldots, X_m) = X_{i+1} \qquad \text{and} \qquad H_i(X_{i+1}, \ldots, X_m) = a_i$$

for some constants $a_i \in \mathbb{F}_p$, $i = 0, \ldots, m-1$. The corresponding sequence of vectors is generated at the cost of one multiplication per component. This naturally leads to a question of studying the periods of such sequences generated by such polynomial dynamical systems.

We also note that it is natural to consider joint distribution of several consecutive vectors

$$(\mathbf{u}_n, \ldots, \mathbf{u}_{n+s-1}), \quad n = 0, 1, \ldots$$

in the sm-dimensional space. It seems that our method (with some minor adjustments) can be applied to derive an appropriate variant of Corollary 20 which is needed for such a result.

One of the possible ways to improve our results, is to construct special polynomials $\mathcal{F} = \{F_0, \ldots, F_m\}$ such that linear combinations of their iterations, of the type which appear in the proof of Theorem 22, satisfy the condition of the Deligne bound [35], that is, have a nonsingular highest form. In fact even some partial control over the dimension of the singularity locus of this highest form may already lead to better estimates via results of Katz [76].

In the proof of Lemma 21 we use the estimate $O\left(\deg \Phi_{s,\mathbf{k},\mathbf{l}} p^{m-s-1}\right)$ on the number of zeros of the polynomial $\Phi_{s,\mathbf{k},\mathbf{l}}$. Perhaps this bound is hard to improve in general, but maybe this can be done for some specially selected polynomial systems. For example, if one can show that $\Phi_{s,\mathbf{k},\mathbf{l}}$ is absolutely irreducible then the Lang-Weil bound on the number of zeros of a polynomial in $m \ge 2$ variables, see [82, 119], can be used to derive a better result. Even the case of $\nu = 1$ is already of interest.

Furthermore, although low discrepancy is a very important requirement on any pseudorandom number generator, this is not the only one. For example, the notion of linear

complexity also plays an important role in this area, see [136]. In the case of vector sequences it is natural to consider linear relations with vector coefficients. Namely, we denote by $L(N)$ the smallest L such that for some m-dimensional vectors $\mathbf{c}_0, \ldots, \mathbf{c}_L$ over $\mathbb{F}_q$ where $\mathbf{c}_L$ is a non-zero vector, we have

$$\sum_{h=0}^{L} \mathbf{c}_h \cdot \mathbf{u}_{n+h} = 0 \tag{2.51}$$

for all $h = 0, \ldots, N-L-1$, where $\mathbf{c} \cdot \mathbf{u}$ denotes the scalar product. Using the same degree argument which is used in the proof of Lemma 21, we see that (2.51) leads to a nontrivial polynomial equation in $m+1$ variables over $\mathbb{F}_p$ of degree $O(L^m)$. Since for $N \le \tau$, where as τ is the period of the purely periodic sequence $\{\mathbf{w}_n\}$, the vectors $\mathbf{w}_{n+h}$, $h = 0, \ldots, N-L-1$, are pairwise distinct, this yields the estimate

$$\mathcal{L}(N) \gg N^{1/m} p^{-1}, \qquad 0 \le N \le \tau.$$

This can be extended to sequences over arbitrary finite fields. Several more estimates of this type have recently been given in [114]. It would be very interesting to get better bounds which rely on a more refined analysis of (2.51).

It would be interesting to extend Theorem 34 to arbitrary finite fields $\mathbb{F}_q$. However, Lemma 32 is not valid in general. In the case $m = 0$ we have the tight inequality

$$(\deg \Phi + 1 + p - q)\frac{q}{p} \le \mathcal{L}((s_n), N) \le (\deg \Phi + 1)\frac{p}{q} + q - p$$

for

$$N \ge (\deg \Phi + 1 + p - q)\frac{q}{p} + q - 1,$$

see [89], which is too weak to derive a nontrivial bound if q is not a prime. It would also be interesting to extend the result to other coordinate sequences.

We recall also that the *nonlinear complexity profile* of a sequence (s_n) (for some fixed positive integer d) is the sequence $\mathcal{NL}_d((s_n), N)$, $N \ge 1$, where its Nth term is defined to be the least order L of a polynomial recurrence relation

$$s_{n+L} = \psi(s_{n+L-1}, \ldots, s_n), \qquad 0 \le n \le N-L-1,$$

where $\psi \in \mathbb{F}_q[Y_1, \ldots, Y_L]$ is a polynomial of total degree at most d for which this recurrence relation holds. It would be interesting to extend the proof of Theorem 31 to the nonlinear complexity profile with $d \ge 2$. The crucial step is to show that the analogue of the polynomial in (2.25) is not identically zero.

The following *lattice test* has been introduced in [106]. Let (s_n), $n = 0, 1, \ldots$, be a T-periodic sequence over $\mathbb{F}_q$. For given integers $s \ge 1$, $0 < d_1 < d_2 < \ldots < d_{s-1} < T$, and $N \ge 2$, we say that (s_n) passes the *s-dimensional N-lattice test with lags $d_1, \ldots, d_{s-1}$* if the vectors $\{\mathbf{s}_n - \mathbf{s}_0 : 1 \le n < N\}$ span $\mathbb{F}_q^s$, where

$$\mathbf{s}_n = (s_n, s_{n+d_1}, \ldots, s_{n+d_{s-1}}), \quad 0 \le n < N.$$

In the case $d_i = i$ for $1 \le i < s$, this test is closely related to the concept of the linear complexity profile, see [41, 42, 104], and can be analysbehavioured along the same lines as here. However, it would be interesting to study the behaviour of these sequences under the above lattice test with arbitrary lags.

In Section 2.11.3, we note that the bounds of Theorems 53 and 54 coincide with those of [61, 62] but apply to essentially arbitrary polynomial systems. It is also obvious that Theorem 53 can be extended to additive character sums with similar sequences over arbitrary finite fields.

Our approach also works for iterations of multivariate rational functions (one has to take care of the poles, though).

One of the approaches to derive stronger bounds is to use the idea of [105], see also [136], where this idea has been first introduced, albeit in a slightly less efficient form. This idea leads to studying the polynomials

$$F_{\mathbf{a},k_1,\ell_1,\ldots,k_\nu,\ell_\nu} = \sum_{i=1}^{m} a_i \sum_{j=1}^{\nu} \left(F_i^{(k_j)} - F_i^{(\ell_j)} \right),$$

(and proving that they do not vanish unless $(k_1, \ldots, k_\nu)$ is a permutation of $(\ell_1, \ldots, k\ell_\nu)$). Unfortunately the argument of Lemma 52 does not apply to these polynomials. Thus, finding an alternative way to study the polynomials $F_{\mathbf{a},k_1,\ell_1,\ldots,k_\nu,\ell_\nu}$, even only for some special families of polynomial systems, is a challenging open question. One of the possible approaches is establishing the exact rate of growth of the degrees of the iterations $F_i^{(k)}$, $k = 1, 2, \ldots$, $i = 1, \ldots, m$, which is a question of independent interest.

Finally, obtaining a version of Lemma 52 without any conditions on k, ℓ and T is important for the application of the method of [124] for estimating the exponential sums $S_{\mathbf{a}}(N)$ and discrepancy D_N on average over the initial vectors $\mathbf{u}_0 \in \mathbb{F}_p^m$.

Chapter 3

Stable polynomials

3.1 Motivation

During our work on [107, 110, 111] it has become clear that further progress here can only be achieved if more detailed information about the *algebraic structure* of polynomial iterates is available. Unfortunately questions of this type are notoriously hard, and the only known results apply only to univariate even degree polynomials, see [5, 9, 72, 73, 74]. Our main contribution to this area is a series of two papers [4, 112], which introduce to the area such tools as the Weil bound of exponential sums, and explicit bounds on the solutions of Diophantine equations. Furthermore, the paper [112] further motivated the authors of [57] to attack on one of the conjectures in [112] (along the lines outlined in [112]) and make a substantial step in its direction. As we have noticed, studying the algebraic structure of iterated maps appears to be a very hard question. So the results we obtain here are still a long way from what is required for the purposes of improving the results of [107, 110, 111]. There are merely just first steps in that direction, which we hope may eventually lead to the desired goal.

3.2 Definition and characterisation

Let $\mathbb{K}$ be a field. For a polynomial $f \in \mathbb{K}[X]$ we define the sequence of iterations:

$$f^{(0)}(X) = X, \qquad f^{(n)}(X) = f\left(f^{(n-1)}(X)\right), \quad n = 1, 2, \ldots .$$

Following [5, 9, 73, 74], we say that f is *stable* if all polynomials $f^{(n)}$ are irreducible over $\mathbb{K}$.

As in [74], for a quadratic polynomial $f(X) = aX^2 + bX + c \in \mathbb{K}[X]$, $a \neq 0$, we define $\gamma = -b/2a$ as the unique critical point of f (that is, the zero of the derivative f') and consider the set

$$\mathrm{Orb}(f) = \{f^{(n)}(\gamma) \ : \ n = 2, 3, \ldots\} \tag{3.1}$$

which is called the *critical orbit* of f.

It is shown in [72, 73, 74] that critical orbits play a very important role in the dynamics of polynomial iterations.

The basis for our results on stability in the next section is a simple criterion for stability in odd characteristic, see [74, Lemma 5], which becomes a characterisation of stability in the case of finite fields.

Lemma 55. *Let $\mathbb{K}$ be a field of odd characteristic, $f(X) = aX^2 + bX + c \in \mathbb{K}[X]$, and $\gamma = -b/2a$ be the critical point of f. Suppose that $g \in \mathbb{K}[X]$ is such that $g(f^{(n-1)})$ has degree d and is irreducible over $\mathbb{K}$ for some $n \geq 1$. Then $g(f^{(n)})$ is irreducible over $\mathbb{K}$ if $(-a)^d g(f^{(n)}(\gamma))$ is not a square in $\mathbb{K}$. If $\mathbb{K}$ is finite then we may replace the "if" statement with an "if and only if" statement.*

3.3 Stable polynomials over finite fields

In [4] we estimate the length of the critical orbit, and therefore the complexity of testing even degree polynomials $f(X)$ in $\mathbb{F}_q[X]$, with q odd, for stability. We note that the results obtained in this section are a direct generalisation of the ones obtained for quadratic polynomials in [112].

Given two polynomials f and $g \in \mathbb{F}_q[X]$, we write $g \circ f$ for the composition $F(X) = g(f(X))$.

Let now f be an irreducible quadratic polynomial and $g \in \mathbb{F}_q[X]$ be an irreducible polynomial of degree d. Define $F = g \circ f \in \mathbb{F}_q[X]$ which is a polynomial of degree $2d$.

By Lemma 55, taken with $n = 1$, we have the following easy result:

Lemma 56. *Let $F = g \circ f \in \mathbb{F}_q[X]$, where $f, g \in \mathbb{F}_q[X]$ and $\deg f = 2$. Assume that $F^{(n-1)} \circ g$ is irreducible over $\mathbb{F}_q$ for some $n \geq 1$. Then $F^{(n)}$ is irreducible over $\mathbb{F}_q$ if and only if $F^{(n)}(\gamma)$, where $\gamma = -b/2a$ is not a square in $\mathbb{F}_q$.*

We consider the set

$$\mathrm{Orb}(F) = \{F^{(n)}(\gamma) \ : \ n = 2, 3, \ldots\},$$

which for $g(X) = X$ coincides with $\mathrm{Orb}(f)$. We call it the *critical orbit* of F. As before, we notice that there is some t such that $F^{(t)}(\gamma) = F^{(s)}(\gamma)$ for some positive integer $s < t$. Then $F^{(n+t)}(\gamma) = F^{(n+s)}(\gamma)$ for any $n \geq 0$. Accordingly, we denote by t_F the smallest value of t with the above condition. We then have

$$\mathrm{Orb}(F) = \{F^{(n)}(\gamma) \ : \ n = 2, \ldots, t_f\}$$

and $\#\mathrm{Orb}(F) = t_F - 1$, or $\#\mathrm{Orb}(F) = t_F - 2$ (depending whether $s = 1$ or $s \geq 2$ in the above).

A direct consequence of Lemma 56 is the following result which generalises [74, Proposition 3]:

Corollary 57. *For any odd q and any polynomial $F = g \circ f \in \mathbb{F}_q[X]$, where $f = aX^2 + bX + c \in \mathbb{F}_q[X]$ and $g \in \mathbb{F}_q[X]$ of degree d, F is stable over $\mathbb{F}_q$ if and only if the set $\overline{\mathrm{Orb}}(F) = \{-F(\gamma)\} \cup \mathrm{Orb}(F)$, does not contain squares in $\mathbb{F}_q$.*

Trivially, we have $t_F \le q + 1$. Here, we obtain a nontrivial upper bound on the orbit length of stable compositions $F = g \circ f$ where $f, g \in \mathbb{F}_q[X]$, $\deg f = 2$, $\deg g = d$ which for $d = 1$ coincides with [112, Theorem 1].

Theorem 58. *For any odd q and any stable polynomial $F = g \circ f \in \mathbb{F}_q[X]$, where $f = aX^2 + bX + c \in \mathbb{F}_q[X]$ and $g \in \mathbb{F}_q[X]$ of degree d, we have*

$$t_F = O\left(q^{1-\alpha_d}\right),$$

where

$$\alpha_d = \frac{\log 2}{2\log(4d)}.$$

Proof. The proof follows using exactly the same technique as the proof of [112, Theorem 1]. Let χ be the quadratic character of $\mathbb{F}_q$.

We know that $F^{(n)}$ is an irreducible polynomial for any $n \ge 1$. This implies that $G_{n-1} = F^{(n-1)} \circ g$ is an irreducible polynomial. Indeed, if G_{n-1} is not irreducible, then we can write it as $G_{n-1} = G_1 G_2$, where $G_1, G_2 \in \mathbb{F}_q[X]$ are nonconstant polynomials. Then $F^{(n)} = G_{n-1}(f) = G_1(f)G_2(f)$ which is in contradiction with the irreducibility of $F^{(n)}$. We now apply Lemma 56, and conclude that if $F \in \mathbb{F}_q[X]$ is stable then the set $\mathrm{Orb}(F)$ contains no squares. That is, $\chi\left(F^{(n)}(\gamma)\right) = -1$, $n = 2, 3, \ldots$.

We fix an integer parameter K and note that for any $n \ge 1$, we have simultaneously

$$\chi\left(F^{(k+n)}(\gamma)\right) = -1, \qquad k = 1, \ldots, K,$$

which we rewrite as

$$\chi\left(F^{(k)}\left(F^{(n)}(\gamma)\right)\right) = -1, \qquad k = 1, \ldots, K. \tag{3.2}$$

Since by the definition of t_F, the values $F^{(n)}(\gamma)$, $n = 1, \ldots, t_F - 1$, are pairwise distinct elements of $\mathbb{F}_q$, we derive from (3.2) that

$$t_F - 1 \le \#\mathcal{T}_q(K), \tag{3.3}$$

where

$$\mathcal{T}_q(K) = \left\{x \in \mathbb{F}_q \ : \ \chi\left(F^{(k)}(x)\right) = -1, \ k = 1, \ldots, K\right\}.$$

We have

$$\#\mathcal{T}_q(K) = \frac{1}{2^K} \sum_{x \in \mathbb{F}_q} \prod_{k=1}^{K} \left(1 - \chi\left(F^{(k)}(x)\right)\right), \tag{3.4}$$

since for every $x \in \mathcal{T}_q(K)$ the product on the right hand side of (3.4) is 2^K and is 0 when $\chi(F^{(k)}(x)) = 1$ for at least one $k = 1, \ldots, K$ (note that since by our assumption $F^{(k)}(X)$ is irreducible over $\mathbb{F}_q$, we have that $F^{(k)}(x) \ne 0$ for all $x \in \mathbb{F}_q$).

Expanding the product in (3.4), we obtain $2^K - 1$ character sums of the shape

$$(-1)^\nu \sum_{x \in \mathbb{F}_q} \chi \left(\prod_{j=1}^{\nu} F^{(k_j)}(x) \right), \qquad 1 \le k_1 < \ldots < k_\nu \le K, \tag{3.5}$$

with $\nu \ge 1$ and one trivial sum that equals q (corresponding to the terms equal to 1 in the product in (3.4)).

Clearly, $F^{(k)}(X)$ is a polynomial of degree $2^k d^k$. Furthermore, by our assumption, each one of the polynomials $F^{(k)}(X)$ is irreducible, therefore none of the polynomials

$$\prod_{j=1}^{\nu} F^{(k_j)}(X) \in \mathbb{F}_q[X], \qquad 1 \le k_1 < \ldots < k_\nu \le K,$$

is a perfect square in the algebraic closure of $\mathbb{F}_q$. Thus, the Weil bound (see [70, Theorem 11.23]), applies to every sum (3.5) and implies that each one of them is $O(2^K d^K q^{1/2})$. Hence,

$$\#\mathcal{T}_q(K) = \frac{1}{2^K} q + O(2^K d^K q^{1/2}). \tag{3.6}$$

Choosing K to satisfy

$$(4d)^K \le q^{1/2} < (4d)^{K+1}$$

and combining (3.3) and (3.6), we get the desired result. □

We also recall that $\alpha \in \mathbb{F}_q$ is a square if either $\alpha = 0$ or $\alpha^{(q-1)/2} = 1$ that can be tested (via repeated squaring) in $O(\log q)$ field operations. Combining these with the bound of Theorem 58, we immediately obtain:

Corollary 59. *For any odd q, an even degree polynomial $f \in \mathbb{F}_q[X]$ can be tested for stability in time $O\left(q^{1-\alpha_d}\right)$, where*

$$\alpha_d = \frac{\log 2}{2 \log(4d)}.$$

Finally, we remark that estimating the size of the set of even degree polynomials $f \in \mathbb{F}_q[X]$ is a very interesting question to which we hope our technique can apply as well.

We end this section by proving that over $\mathbb{F}_{2^m}$ there are no quadratic stable polynomials. We recall that a polynomial $\ell(X) \in \mathbb{F}_q[X]$ is called *linearised* if it is of the form

$$\ell(X) = \sum_{j=0}^{\nu} a_i X^{p^j},$$

where p is the characteristic of $\mathbb{F}_q$.

We now show that there are no stable shifted linearised polynomials. In particular, there are no stable quadratic polynomials over finite fields of characteristic 2. Our proof is based on one well-known statement which describes the irreducibility of polynomials of the form $\ell(X) - b \in \mathbb{F}_q[X]$, where $\ell(X)$ is a linearised polynomial over $\mathbb{F}_q$ (see [14, Lemma 3.17]).

Lemma 60. *Let $q = p^m$, where p is a prime and $m \geq 1$ is an integer. Suppose that $\ell(X)$ is a linearised polynomial over $\mathbb{F}_q$ of degree p^ν with $\nu \geq 2$. Then for any $b \in \mathbb{F}_q$, the polynomial $\ell(X) - b$ is irreducible if and only if*

$$p = \nu = 2,$$

and ℓ has the form

$$\ell(X) = X(X + A)(X^2 + AX + B),$$

with $A, B \in \mathbb{F}_q$ such that $X^2 + AX + B$ and $X^2 + BX + b$ are both irreducible.

We now show that there are no stable shifted linearised polynomial over a finite field.

Theorem 61. *Let $q = p^m$, where p is a prime as $m \geq 1$ is an integer, and let $f(X) = \ell(X) + \alpha \in \mathbb{F}_q[X]$, where $\ell(X)$ is a linearised polynomial over $\mathbb{F}_q$ of degree p^ν with $\nu \geq 1$. Then one of $f(X)$, $f^{(2)}(X)$ or $f^{(3)}(X)$ is reducible over $\mathbb{F}_q$.*

Proof. We note that for any $k \geq 1$,

$$f^{(k)}(X) = \widetilde{\ell}(X) + \widetilde{\alpha},$$

where $\widetilde{\ell}(X) \in \mathbb{F}_q[X]$ is a linearised polynomial of degree $p^{\nu k}$ and $\widetilde{\alpha} \in \mathbb{F}_q$. When $p \neq 2$, then, by Lemma 60, we get that the polynomial f is not irreducible, and thus not stable. We assume thus that $p = 2$. In this case, applying again Lemma 60 we obtain that for $k \geq 3$, $f^{(k)}$ is a reducible polynomial over $\mathbb{F}_q$, which concludes the proof. □

As a simple consequence, we obtain that there are no stable quadratic polynomials over finite fields of characteristic 2.

Corollary 62. *Let q be even, and let $f(X) = aX^2 + bX + c \in \mathbb{F}_q[x]$. Then one of $f(X)$, $f^{(2)}(X)$ or $f^{(3)}(X)$ is reducible over $\mathbb{F}_q$.*

The following example shows that Corollary 62 cannot be extended to infinite fields. Let $\mathbb{K} = \mathbb{F}_2(T)$ be the rational function field in T over $\mathbb{F}_2$, where T is transcendental over $\mathbb{F}_2$. Take $f(X) = X^2 + T \in \mathbb{K}[X]$. Then it is easy to see that

$$f^{(n)}(X) = X^{2^n} + T^{2^{n-1}} + T^{2^{n-2}} + \cdots + T^2 + T.$$

Now from Eisenstein's criterion for function fields (see [133, Proposition III.1.14]), it follows that for every $n \geq 1$, the polynomial $f^{(n)}(X)$ is irreducible over $\mathbb{K}$. Hence, $f(X)$ is stable.

3.4 Quadratic stable polynomials over $\mathbb{Q}$

We saw that for finite fields of odd characteristic we have a complete characterisation of stable quadratic polynomials which is given by Corollary 57. However, for the case of infinite fields, stability for quadratic polynomials does not occur if and only if the critical orbit has no squares. Moreover, over $\mathbb{Q}$, Jones gave the following explicit condition for a monic quadratic polynomial $f \in \mathbb{Z}[X]$ to be stable and this condition implies that $f^{(2)}(\gamma)$ is a square, see [73, Theorem 4.4]:

Theorem 63. *Let $f \in \mathbb{Z}[X]$ be monic, quadratic and irreducible, and write $f(X) = (X-\gamma)^2+\gamma+m$, where γ is the critical point. Suppose that $|m| > 6+3\sqrt{|\gamma|+1}$ (if $\gamma \in \mathbb{Z}$ then $|m| > 1+\sqrt{|\gamma|+1}$ suffices), and that*

$$\frac{-m^{+}_{-}\sqrt{f^{(2)}(\gamma)}}{2} \notin \mathbb{Q}^{*2}.$$

Then f is stable.

In [4] we use Theorem 63 to show that almost all monic quadratic polynomials $f(X) \in \mathbb{Z}[X]$ are stable over $\mathbb{Q}$.

We note that for finite fields the situation is quite different. For example, Gomez and Nicolás [57], developing some ideas from [112], have proved that there are $O(q^{14/5})$ stable quadratic polynomials over $\mathbb{F}_q$ for an odd prime power q.

In this section we also show that the presence of squares in so-called critical orbits of a quadratic polynomial $f(X) \in \mathbb{Z}[X]$ can be detected by a finite algorithm; this property is is closely related to the stability of f.

Using Theorem 63, we first show that almost all monic quadratic polynomials $f(X) \in \mathbb{Z}[X]$ are stable over $\mathbb{Q}$.

Theorem 64. *Let $E(A,B)$ be the number of pairs $(a,b) \in \mathbb{Z}^2$ with $|a| \le A$ and $|b| \le B$ for which $f(X) = X^2+aX+b$ is irreducible but not stable over $\mathbb{Q}$. Then we have*

$$E(A,B) = O\left(\min\{A^{3/2}, B^{3/4}\}\right).$$

Proof. Given an irreducible polynomial $f(X) = X^2+aX+b \in \mathbb{Z}[X]$, we denote by $\gamma = -a/2$ its critical point and write it as

$$f(X) = (X-\gamma)^2+\delta,$$

where

$$\delta = b - a^2/4.$$

By Theorem 63, we see that if $f(X)$ is not stable over $\mathbb{Q}$, then either

$$|\delta-\gamma| \le 6+3\sqrt{|\gamma|+1}, \tag{3.7}$$

or

$$\sqrt{f^{(2)}(\gamma)} \in \mathbb{Q}. \tag{3.8}$$

Clearly, the condition (3.7) implies that $b = a^2/4 + O(|a|^{1/2})$. Thus, if $|b| \le B$ then the above condition can be satisfied only if $|a| \le C_1 B^{1/2}$ where $C_1 > 0$ is some absolute constant. Furthermore, for every fixed a, there are at most $O(|a|^{1/2})$ possible values of b. Thus, (3.7) holds for at most

$$O\left(\sum_{|a| \le \min\{A, C_1 B^{1/2}\}} |a|^{1/2}\right) = O\left(\min\{A^{3/2}, B^{3/4}\}\right)$$

pairs $(a,b) \in \mathbb{Z}^2$ with $|a| \le A$ and $|b| \le B$.

For the condition (3.8), we note that

$$\begin{aligned} f^{(2)}(\gamma) &= \frac{a^4 - 4a^3 - 8a^2b + 16ab + 16b^2 + 16b}{16} \\ &= \frac{(2b + a^2 - 2a - 2)^2 - (8a + 4)}{16}. \end{aligned}$$

Hence, if (3.8) is satisfied, then

$$(2b + a^2 - 2a - 2)^2 - (8a + 4) = r^2$$

for some integer r, which implies that

$$(s - r)(s + r) = 8a + 4, \tag{3.9}$$

where $s = 2b + a^2 - 2a - 2$.

We now see that for a fixed value for a, the number of solutions $(r, s) \in \mathbb{Z}^2$ of the equation (3.9) is at most $2\tau(|8a+4|)$, where $\tau(k)$ is the number of positive integer divisors of the integer $k \ge 1$. We also notice that when a and s are fixed, the number b is uniquely defined.

Furthermore, since $r - s$ and $r + s$ are divisors of $8a + 4$, we have $s = O(|a|) = O(A)$. Thus, $b = a^2 + O(A)$. This implies that (3.8) is possible only for $|a| \le C_2 B^{1/2}$, where $C_2 > 0$ is some absolute constant.

Thus, using the well-known bound on the mean value of the divisor function (see [65, Theorem 320]), we conclude that (3.8) holds for at most

$$\begin{aligned} \sum_{|a| \le \min\{A, C_2 B^{1/2}\}} \tau(|8a + 4|) &\le 2 \sum_{k \le 8 \min\{A, C_2 B^{1/2}\} + 4} \tau(k) \\ &= O\left(\min\{A \log A, B^{1/2} \log B\}\right) \end{aligned}$$

pairs $(a,b) \in \mathbb{Z}^2$ with $|a| \le A$ and $|b| \le B$, and this last expression is dominated by the number of such pairs for which (3.7) holds. □

Taking $A = B = H$ we obtain:

Corollary 65. *Let $E(H)$ be the number of pairs $(a,b) \in \mathbb{Z}^2$ with*

$$\max\{|a|, |b|\} \le H$$

for which $f(X) = X^2 + aX + b$ is irreducible but not stable over $\mathbb{Q}$. We then have

$$E(H) = O(H^{3/4}).$$

We also derive from Theorem 64 and [57, Lemma 2] that almost all quadratic polynomials $f(X) \in \mathbb{Z}[X]$ are stable over $\mathbb{Q}$. To prove this, we need the following result which is given in [57, Lemma 2] for the case of finite fields. However, its proof applies to any field.

Lemma 66. *Let $\mathbb{F}$ be a field. Let $f(X) \in \mathbb{F}[X]$ and $\alpha \in \mathbb{F}^*$. Then $f(X)$ and $g(X) = \alpha^{-1} f(\alpha X)$ are simultaneously stable.*

Theorem 67. *Let $F(H)$ be the number of triples $(a, b, c) \in \mathbb{Z}^3$ with*

$$\max\{|a|, |b|, |c|\} \le H$$

for which $f(X) = aX^2 + bX + c$ is irreducible but not stable over $\mathbb{Q}$. We then have

$$F(H) \le H^{3/2+o(1)} \qquad \text{as} \quad H \to \infty.$$

Proof. Discarding the $O(H^2)$ triples (a, b, c) with $a = 0$ and $\max\{|b|, |c|\} \le H$, we note that Lemma 66 taken with $\alpha = a^{-1}$, implies that $f(X) = aX^2 + bX + c \in Z[X]$ is stable if only $g(X) = X^2 + bX + ac$ is stable. We also see that each such polynomial $g(X)$ corresponds to at most $\tau(|g(0)|)$ $(= ac)$ polynomials $f(X)$. Recalling the estimate $\tau(k) = k^{o(1)}$ as $k \to \infty$ on the divisor function (see [65, Theorem 317]), we derive that

$$F(H) \le E(H, H^2) H^{o(1)} \qquad \text{as} \quad H \to \infty.$$

Applying Theorem 64, we conclude the proof. □

Although over $\mathbb{K} = \mathbb{Q}$ the presence of squares in the critical orbit is known not to be necessary, it is still interesting to understand whether it can be efficiently tested.

Theorem 68. *For an irreducible polynomial $f(X) = aX^2 + bX + c \in \mathbb{Z}[X]$ the existence of squares in* $\mathrm{Orb}(f)$ *can be tested in finitely many steps.*

Proof. We show how to check in finitely many steps whether the critical orbit $\mathrm{Orb}(f)$ contains squares. If $f^{(2)}(\gamma)$ is a square, then we are done. Assume that $f^{(2)}(\gamma)$ is not a square and consider the Diophantine equation

$$y^2 = F(x), \tag{3.10}$$

where $F(X) = f(f(X))$.

As usual, given a finite set of primes $\mathcal{S}$, we say that $\alpha \in \mathbb{Q}$ is $\mathcal{S}$-integral if it can be represented as $\alpha = r/s$, where both r and s are integers divisible only by primes from $\mathcal{S}$.

If the critical orbit of f has a square, say $f^{(n)}(\gamma) = \eta^2$ for some $n \ge 2$, where $\eta \in \mathbb{Q}$, then the Diophantine equation (3.10) has an $\mathcal{S}$-integral solution $\big(f^{(n-2)}(\gamma), \eta\big)$, where $\mathcal{S}$ is the set of prime divisors of a.

We now recall the classical result of Trelina [137] in the form given in [131, Chapter 6, Theorem 7.1], which yields an explicit upper bound for the height of all $\mathcal{S}$-integral solutions to the equation (3.10), in terms of the coefficients of F and the set $\mathcal{S}$; that is, in terms of a, b, c and $\mathcal{S}$ which is valid provided that $F(X) = f(f(X))$ has at least 3 simple roots. Thus, it remains to deal with the case when $F(X)$ has multiple roots. This means that F and F' have a common root, where

$$F'(X) = 2af'(X)f(X) + bf'(X) = f'(X)(2af(X) + b).$$

Therefore,

- either $\gcd(F, f') \neq 1$;
- or $\gcd(F, 2af + b) \neq 1$.

In the first case, we observe that the only zero of f' is γ. Now, γ is a root of F if and only if $f(f(\gamma)) = 0$. As γ is a rational number, we get that f has a rational zero $f(\gamma)$, which is a contradiction with the irreducibility of f over $\mathbb{Q}$.

In the second case, we assume that F and $2af + b$ have a common root α. This means that

$$f(\alpha) = -\frac{b}{2a} = \gamma,$$

and $F(\alpha) = f(f(\alpha)) = f(\gamma) = 0$. This proves again that the polynomial $f(X)$ is reducible over $\mathbb{Q}$, and thus we get a contradiction. □

3.5 Remarks and open problems

In 3.4, we note that in the condition (3.8) we have not used the full strength of [73, Theorem 4.4]. However, surprisingly enough, the bound of Theorem 64 is dominated by the polynomials for which (3.7) is satisfied. Maybe a more careful examination of this case may help to improve Theorem 64.

We remark that the result of Trelina [137] has been improved in a number of papers. These improvements can be used to obtain an explicit estimate for the complexity of testing the existence of squares in orbits of quadratic polynomials (see, for example, [23, 24] and the references therein, for such better explicit estimates).

It is also interesting to investigate whether the stability of a quadratic polynomial $f(X) \in \mathbb{Z}[X]$ can be tested in finitely many steps.

Standard heuristics, based on the density of irreducible polynomials suggests that one should expect that there are very few stable nonlinear polynomials over finite fields while almost all polynomials over $\mathbb{Z}$ should be stable. The result of [57] and Theorem 64 provide some theoretic evidences to these expectations, respectively. Overall, the situation is not well-understood both theoretically and heuristically. There is place for much more research in this area. One direction is to study if the stability of an arbitrary polynomial over $\mathbb{F}_q$ can be tested in finitely many steps. Moreover, can the stability of a quadratic polynomial over $\mathbb{Z}$ be tested in finitely many steps?

Chapter 4

Dynamical systems with Fermat quotients

4.1 Background and motivation

For a prime p and an integer u with $\gcd(u, p) = 1$ the *Fermat quotient* $q_p(u)$ is defined as the unique integer with

$$q_p(u) \equiv \frac{u^{p-1} - 1}{p} \pmod{p}, \qquad 0 \le q_p(u) \le p - 1,$$

and we also define

$$q_p(kp) = 0, \qquad k \in \mathbb{Z}.$$

It is well-known that the p-divisibility of Fermat quotients $q_p(a)$ by p has numerous applications, which include the Fermat Last Theorem and squarefreeness testing, see [47, 51, 58, 83]. In particular, the smallest value ℓ_p of $u \ge 1$ for which $q_p(u) \not\equiv 0 \pmod{p}$ plays a prominent role in these applications, for which the following estimates are given [19]

$$\ell_p \le \begin{cases} (\log p)^{463/252+o(1)} & \text{for all } p, \\ (\log p)^{5/3+o(1)} & \text{for almost all } p, \end{cases}$$

(where almost all p means for all p but a set of relative density zero), which improve the previous estimates of the form $\ell_p = O\left((\log p)^2\right)$ of [51, 59, 68, 83]. It is widely believed that $\ell_p = 2$ for all primes p, except for a very thin set of so called *Wieferich primes*, which one expects $\ell_p = 3$ (in particular, it is expected that $\ell_p \le 3$ for all primes). The behaviour (and even the infinitude) of Wieferich primes is still very poorly understood, although several interesting results, relating Wieferich primes to other number theoretic problems are known, see [60, 93, 126].

There are also several results about the distribution of Fermat quotients. For instance, Heath-Brown [66] has proved that the Fermat quotients $q_p(u)$ are asymptotically uniformly distributed (after scaling by $1/p$ and mapping them into $q_p(u)/p \in [0, 1]$) for $u = M +$

$1, \dots, M+N$, for any integers M and $N \ge p^{1/2+\varepsilon}$, for some fixed ε and $p \to \infty$. Note that [66, Theorem 2] gives this only for $N \ge p^{3/4+\varepsilon}$ but using the full strength of the Burgess bound one can lower this threshold down to $h \ge p^{1/2+\varepsilon}$, see Lemma 69 below and also [47, Section 4].

It is also shown in [51, Proposition 2.1] that for any integer a the number of solutions to the equation $q_p(u) = a$, $0 \le u < p$, is at most

$$\#\{u \in \{0, \dots, p-1\} \ : \ q_p(u) = a\} \le p^{1/2+o(1)}. \tag{4.1}$$

Finally, we also recall several results on congruences involving Fermat quotients, see [3, 36, 134] and references therein.

In [113] we consider the dynamical system generated by Fermat quotients. That is, we fix a sufficiently large prime p and, for an initial value $u_0 \in \{0, \dots, p-1\}$ we consider the sequence

$$u_n = q_p(u_{n-1}), \qquad n = 1, 2, \dots . \tag{4.2}$$

Clearly, there is some t such that $u_t = u_k$ for some $k < t$. Then $u_{n+t} = u_{n+k}$ for any $n \ge 0$. Accordingly, for the smallest value of t with the above condition, we call $u_0, \dots, u_{t-1}$ the orbit of the initial value u_0.

Here we address various questions concerning the sequences generated by (4.2) such as the number of fixed points, image size and the "typical" orbit length. In particular, we compare their characteristics with those expected from random maps, see [49]. All our numerical results support the natural expectation that the map $u \mapsto q_p(u)$ behaves very similar to a random map on the set $\{0, \dots, p-1\}$.

We also investigate their distribution and other characteristics which are relevant to their use as pseudorandom number generators. As we have mentioned, a result of Heath-Brown [66] implies that the fractions $q_p(u)/p$ are uniformly distributed for $u = M+1, \dots, M+N$, provided that $N \ge p^{1/2+\varepsilon}$ for some fixed $\varepsilon > 0$. However, the method of [66], based on bounds of multiplicative character sums, such as the Polya-Vinogradov and Burgess bounds, see [70, Theorems 12.5 and 12.6], cannot be applied to studying the distribution of several consecutive elements. Here we use a different approach, based on the Weil bound of exponential sums with rational functions, to study the distribution of points

$$\left(\frac{q_p(u)}{p}, \dots, \frac{q_p(u+s-1)}{p}\right), \qquad u = M+1, \dots, M+N, \tag{4.3}$$

in the s-dimensional cube, which is nontrivial provided that $N \ge p^{1+\varepsilon}$ for any fixed real $\varepsilon > 0$ and integer $s \ge 1$.

We also obtain a nontrivial lower bound on the linear complexity of the sequence $q_p(u)$ which is also a very important characteristic of any sequence relevant to its applications to both cryptography and quasi-Monte Carlo methods, see [33, 92, 136].

Besides theoretic estimates, we also present results of several numerical tests. Some of these tests are based on a modification of an algorithm described in [46, 47], which seems to be more computationally efficient. We also address some other algorithmic aspects of

computation with Fermat quotients. In particular, we give asymptotic estimates of several new algorithms which we design for this purpose.

We note that all standard heuristic predictions concerning various conjectures about Fermat quotients (for example, the expected number of Wieferich primes up to x as $x \to \infty$) are based on the assumption of the pseudorandomness of the map $u \mapsto q_p(u)$. Our results provide some theoretic and experimental support to this assumption which seems to be never systematically verified prior to our work.

Finally, motivated by the pseudorandom nature of the map $u \mapsto q_p(u)$, we also discuss some possibilities of using Fermat quotients for designing cryptographically useful hash functions.

We remark that Smart and Woodcock [138] have considered iterations of a related function

$$L_p(u) = \frac{u^p - u}{p} \tag{4.4}$$

in the ring of p-adic integers. However, the settings of [138] (where p is fixed, for example $p = 2$) and our settings where p is the main growing parameter are very different. Here, we show that the fractional parts

$$\left\{\frac{L_p(x)}{p}\right\}, \qquad x = 1, \ldots, N, \tag{4.5}$$

are asymptotically uniformly distributed, provided that $N \ge p^{15/8+\varepsilon}$ for some $\varepsilon > 0$ and p is sufficiently large. We note that despite the simple relation $L_p(u) = uq_p(u)$, it seems that $L_p(u)$ is harder to study and most of the methods used for $q_p(u)$ do not apply to $L_p(u)$.

All the results of the next sections are presented in the papers [29, 113].

4.2 Preparations

4.2.1 Notation

Throughout this work, p always denotes prime numbers, while k, m and n (in both the upper and lower cases) denote positive integer numbers.

For integers a, b and $m \ge 1$ with $\gcd(b, m) = 1$, we write

$$c = a/b \text{ rem } m$$

for the unique integer c with $bc \equiv a \pmod{m}$ and $0 \le c < m$.

4.2.2 Exponential sums

First, we recall the bound of Heath-Brown [66] on exponential sums with $q_p(u)$. Although here we use it only with $\nu = 2$ (exactly as it is given in [66]) we formulate it in full generality.

As we have mentioned, the method of Heath-Brown [66] combined with the Polya-Vinogradov bound (when $\nu = 1$) and the Burgess bound (when $\nu \geq 2$), see [70, Theorems 12.5 and 12.6], implies the following generalisation of [66, Theorem 2]:

Lemma 69. *For any fixed integer $\nu \geq 1$, we have*

$$\max_{\gcd(a,p)=1} \left| \sum_{u=M+1}^{M+N} \mathbf{e}_p\left(aq_p(u)\right) \right| \ll N^{1-1/\nu} p^{(\nu+1)/2\nu^2+o(1)},$$

as $p \to \infty$, uniformly over M and $N \geq 1$.

To estimate exponential sums with $L_p(x)$ we use the bound of Heath-Brown and Konyagin [67] on the Heilbronn exponential sum defined by

$$H_p(a) = \sum_{z=0}^{p-1} \mathbf{e}_{p^2}(az^p).$$

Lemma 70. *If p is a prime and $p \nmid a$ then*

$$H_p(a) \ll p^{7/8},$$

uniformly in a.

We now recall the following well-known bound, see [70, Bound (8.6)].

Lemma 71. *For any integers K and r, we have*

$$\sum_{k=0}^{K-1} \mathbf{e}_p(kr) \ll \min\left\{K, \frac{p}{\|r\|}\right\},$$

where

$$\|r\| = \min_{s \in \mathbb{Z}} |r - sp|$$

is the distance between r and the closest multiple of p.

4.2.3 Small height ratios in multiplicative subgroups

Let $\mathcal{G}$ be a multiplicative subgroup of the group of units in the residue ring modulo an integer $m \geq 1$. Also, for a real Z, let $N(m, \mathcal{G}, Z)$ be the number of solutions to the congruence

$$wx \equiv y \pmod{m}, \qquad \text{where } 0 < |x|, |y| \leq Z,\ w \in \mathcal{G}.$$

We now recall [21, Theorem 1] which gives an upper bound on $N(m, \mathcal{G}, Z)$. We note that the proof given in [21] works only for $Z \geq m^{1/2}$ (which is always satisfied in the case we apply it); however it is shown in [22] that the result holds without this condition too, exactly as it is formulated in [21].

Lemma 72. *Let $\nu \geq 1$ be a fixed integer and let $m \to \infty$. Assume $\#\mathcal{G} = t \gg \sqrt{m}$. Then for any positive number Z we have*

$$N(m, \mathcal{G}, Z) \leq Zt^{(2\nu+1)/2\nu(\nu+1)} m^{-1/2(\nu+1)+o(1)} + Z^2 t^{1/\nu} m^{-1/\nu+o(1)}.$$

4.2.4 Basic properties of Fermat quotients

Most of our results are based on the following two well-known properties of Fermat quotients.

For any integers k, u and v with $\gcd(uv, p) = 1$ we have

$$q_p(uv) \equiv q_p(u) + q_p(v) \pmod{p} \tag{4.6}$$

and

$$q_p(u + kp) \equiv q_p(u) - ku^{-1} \pmod{p}, \tag{4.7}$$

see, for example, [47, Equations (2) and (3)].

4.3 Algorithms

As we have mentioned, computing each individual value of $q_p(u)$ can be done in $O(\log p)$ arithmetic operations on $O(\log p)$-bit integers via repeated squaring computation of u^{p-1} modulo p^2, we refer to [54] for a background on modular arithmetic and complexity of various algorithms. In particular, one can easily reformulate our complexity estimates in terms of bit operations.

Thus computing all values of $q_p(u)$, $0 \le u < p$, requires $O(p \log p)$ arithmetic operations on $O(\log p)$-bit integers. Such computation is necessary, for example, to find all fixed points of the map $u \mapsto q_p(u)$ or for finding the image size.

Here we show that there is a slightly more efficient algorithm which is based on (4.6) and (4.7).

We assume that we are given a primitive root g modulo p. This can be done at the pre-computation stage and we keep it outside of the algorithm (in any case, it can be found in $p^{1/4+o(1)}$ arithmetic operations on $O(\log p)$-bit integers, see [120], which is lower than the remaining parts of the algorithm).

Algorithm 73 (Generating $q_p(u)$, $0 \le u \le p - 1$)**.**

Input: *A prime p and a primitive root g modulo p with $1 < g < p$.*

Output: *A permuted sequence of the values $q_p(u)$, $0 \le u \le p - 1$.*

1. *Set $q_p(0) = 0$ and $q_p(1) = 0$.*
2. *Compute $q_p(g)$ using the repeated squaring modulo p^2.*
3. *Set $b_1 = g$ and $c_1 = g^{-1} \text{ rem } p$.*
4. *For $i = 2, \ldots, p - 2$ compute*
   (a) *$b_i = gb_{i-1} \text{ rem } p$ and $c_i = c_{i-1}g^{-1} \text{ rem } p$;*

(b) $k_i = (gb_{i-1} - b_i)/p$;

(c) $q_p(b_i) = q_p(g) + q_p(b_{i-1}) + k_i c_i \text{ rem } p$.

Theorem 74. *Algorithm 73 computes every value* $q_p(u)$, $0 \le u < p-1$, *in* $O(p)$ *arithmetic operations on* $O(\log p)$*-bit integers.*

Proof. The complexity estimate is immediate. The correctness of the algorithm follows from the congruences

$$\begin{aligned} q_p(b_i) \equiv q_p(gb_{i-1} - k_i p) &\equiv q_p(gb_{i-1}) + k_i (gb_{i-1})^{-1} \\ &\equiv q_p(g) + q_p(b_{i-1}) + k_i c_i \pmod p, \end{aligned}$$

which in turn follow from (4.6) and (4.7). □

Note that the algorithm of [46, 47] is very similar, except that it uses $g = 2$ instead of a primitive root. This makes each step faster, but if 2 is not a primitive root modulo p requires going trough all conjugacy classes of the group generated by 2 modulo p and thus requires more "administration" of data and also more memory.

Unfortunately Algorithm 73 does not help to compute $q_p(u)$ for a given value of u unless all values $q_p(v)$, $0 \le v \le p-1$, are precomputed and stored in a table, after which $q_p(u)$ can simple be read from there. We now describe a trade-off algorithm which requires less memory but the computation of $q_p(u)$ is more expensive than the simple table look-up. It depends on a parameter $z \ge 2$, which can be adjusted to particular algorithmic needs.

For a real $V < p$ we use $\mathcal{Q}_p(V)$ to denote the table of the values of $q_p(v)$ with $v \in [0, V]$. We see from Theorem 74 that $\mathcal{Q}_p(V)$ can be computed in $O(\min\{p, V \log p\})$ arithmetic operations on $O(\log p)$-bit integers.

Furthermore, for an integer m, we use $\mathcal{I}_m(V)$ to denote the table of the values $v^{-1} \text{ rem } m$ with $v \in [1, V]$ and $\gcd(v, m) = 1$. Since by the Euler theorem $v^{-1} \equiv v^{\varphi(m)-1} \pmod m$, where $\varphi(m)$ is the Euler function, we see that $\mathcal{I}_m(V)$ can be computed in $O(V \log m)$ arithmetic operations on $O(\log m)$-bit integers (there are even more efficient modular inversion algorithms with a better bound on the number of bit operations, see [54]; however using them does not change the overall complexity of our algorithm).

Algorithm 75 (Computing $q_p(u)$ for a given $u \in [0, p-1]$)**.**

Input: *A prime* p*, a real* $z \ge 2$*, the tables* $\mathcal{Q}_p(p/z)$*,* $\mathcal{I}_p(p/z)$*,* $\mathcal{I}_{p^2}(z)$ *and an integer* $u \in \{0, \ldots, p-1\}$.

Output: *The value of* $q_p(u)$.

1. *If* $u = 0$ *set* $q_p(u) = 0$.
2. *Find integers* v *and* w *with* $u \equiv v/w \pmod p$ *and such that* $1 \le v \le 2p/z$ *and* $|w| \le z$.

3. *Recall* $r = w^{-1} \operatorname{rem} p^2$ *if* $w > 0$ *or* $r = -((-w)^{-1} \operatorname{rem} p^2)$ *if* $w < 0$ *from the table* $\mathcal{I}_{p^2}(z)$.

4. *Compute* s *with* $s \equiv v/w \pmod{p^2}$ *and such that* $0 \le s < p^2$.

5. *Compute* $k = (s - u)/p$.

6. *Recall* $r = v^{-1} \operatorname{rem} p$ *from the table* $\mathcal{I}_p(p/z)$.

7. *Recall* $q_p(v)$ *and* $q_p(w)$ *from the table* $\mathcal{Q}_p(p/z)$.

8. *Compute* $q_p(u) = (q_p(v) - q_p(w) + krw) \operatorname{rem} p$.

Theorem 76. *For any integer* u *with* $0 \le u < p - 1$, *Algorithm 75 computes* $q_p(u)$ *in* $O(\log z)$ *arithmetic operations on* $O(\log p)$*-bit integers.*

Proof. The correctness of the algorithm follows from the congruences

$$\begin{aligned} q_p(u) &\equiv q_p(s - kp) \equiv q_p(s) + ks^{-1} \\ &\equiv q_p(v) - q_p(w) + kv^{-1}w \equiv q_p(v) - q_p(w) + krw \pmod{p} \end{aligned}$$

which in turn follow from (4.6) and (4.7).

It remains to estimate the complexity of finding the v and w with $u \equiv v/w \pmod{p}$. We can also assume that $z < p$ since otherwise the result is trivial. We start computing continued fraction convergents a_i/b_i, $\gcd(a_i, b_i) = 1$, $i = 1, 2, \ldots$, to u/p, see, for example, [132] for basic properties of continued fractions. We define j by the condition

$$b_j \le z < b_{j+1}.$$

By the well-known property of continued fractions, we have

$$\left| \frac{a_j}{b_j} - \frac{u}{p} \right| \le \frac{1}{b_j b_{j+1}} \le \frac{1}{b_j z}.$$

We now define

$$w = |a_j p - b_j u|$$

and note that (since $z < 0$)

$$0 < w = b_j p \left| \frac{a_j}{b_j} - \frac{u}{p} \right| \le \frac{p}{z}.$$

Furthermore $uv \equiv w \pmod{p}$ for either $v = a_j$ or $v = -a_j$. Finally, since the denominators of the convergents grow at least exponentially, we see that $j = O(\log b_j) = O(\log z)$ and thus find a_j and b_j in $O(\log z)$ steps, each of them requires to compute with $O(\log p)$-bit integers. □

We see from Theorem 76 taken with $z = \exp\left(\sqrt{\log p}\right)$, that evaluating (in time $p \exp\left(-(1 + o(1))\sqrt{\log p}\right)$) and storing $p \exp\left(-(1 + o(1))\sqrt{\log p}\right)$ values of Fermat quotients, we can compute any other value in time $(\log p)^{1/2+o(1)}$.

4.4 Fixed points

Let $F(p)$ denote the number of fixed points of the map $q_p(u)$ that is,

$$F(p) = \#\{u \in \{0, \dots, p-1\} \ : \ q_p(u) = u\}.$$

We derive a nontrivial estimate on $F(p)$ from Lemmas 14 and 69.

Theorem 77. *We have*

$$F(p) \ll p^{11/12+o(1)}$$

as $p \to \infty$.

Proof. Let us choose some positive integer parameter $N \in [1, p-1]$ and for an integer M we denote by $T(p; M, N)$ the number of integers $u \in [M+1, M+N]$ with $q_p(u) \in [M+1, M+N]$. Considering the discrepancy of the fractions $q_p(u)/p$, $u = M+1, \dots, M+N$, and combining Lemma 14 (taken with $s = 1$) with Lemma 69 (taken with $\nu = 2$) , we immediately conclude

$$T(p; M, N) = \frac{N^2}{p} + O\left(N^{1/2} p^{3/8+o(1)}\right).$$

Clearly every $u = M+1, \dots, M+N$ which is a fixed point contributes to $T(p; M, N)$. Covering the interval $[0, p-1]$ with at most $(p/N+1)$ intervals of length h we obtain

$$F(p) \le \left(\frac{p}{N} + 1\right)\left(\frac{N^2}{p} + O\left(N^{1/2} p^{3/8+o(1)}\right)\right).$$

Choosing $N = \left\lceil p^{11/12} \right\rceil$, we conclude the proof. □

There is little doubt that the bound of Theorem 77 is very imprecise. It is easy to see that in the full range $0 \le u \le p^2 - 1$ the relation (4.7) implies

$$\#\{u \in \{0, \dots, p^2-1\} \ : \ q_p(u) \equiv u \pmod p\} = 2p - 1.$$

Indeed, it is enough to write $u = v + kp$ with $v, k \in \{0, \dots, p-1\}$ and notice that

- either $v = 0$ and then k can take any values
- or $v > 0$ and then the relation (4.7) identify k uniquely.

Thus one can expect that $F(p) = O(1)$.

In fact it seems reasonable to expect that the map $u \mapsto q_p(u)$ behaves similar to a random map. We recall that for a random map on m elements, the probability of having k fixed points is

$$\frac{1}{m^m}\binom{m}{k} \times (m-k-1)^{m-k} \to \frac{1}{ek!}$$

as $m \to \infty$.

Below we present numerical results giving the numbers $N(k)$ of primes $p \in [50000, 200000]$ for which the map $u \mapsto q_p(u)$ has exactly $F(p) = k$ fixed points (note that we discard the "artificial" fixed point $u = 0$). We also give the proportions of such primes $\rho(k) = N(k)/N$ where $N = 12851$ is the total number of primes $p \in [50000, 200000]$ and compare them with $\rho_0(k) = (ek!)^{-1}$ for $k = 0, \dots, 6$. We note that in the above range $N(k) = 0$ for $k \geq 7$.

k	0	1	2	3	4	5	6
$\rho_0(k)$	0.368	0.368	0.184	0.0613	0.0153	0.00306	0.000511
$N(k)$	4770	4697	2327	844	174	36	3
$\rho(k)$	0.371	0.365	0.181	0.0656	0.0135	0.00280	0.000233

Statistics of fixed points

These numerical results appear to indicate a reasonable agreement between the prediction and actual results.

4.5 Concentration of values

For integers k and $h \geq 1$ we denote by $U(p; k, h)$ the number of $u \in \{0, \dots, p-1\}$ for which $q_p(u) \equiv z \pmod p$ for some $z \in [k+1, k+h]$.

As in the proof of Theorem 77, a combination of Lemma 69 (which we take with $N = p$ and $\nu = 2$) with Lemma 14 gives the following asymptotic formula

$$U(p; k, h) = h + O(p^{7/8+o(1)}) \tag{4.8}$$

as $p \to \infty$. On the other hand, using (4.1), we trivially obtain

$$U(p; k, h) \leq hp^{1/2+o(1)}$$

that improves (4.8) for $h \leq p^{3/8}$.

We now obtain a better upper bound, which improves (4.8) for $h \leq p^{3/4}$.

Theorem 78. *For any integers k and $h \geq 1$, we have*

$$U(p; k, h) \leq h^{1/2}p^{1/2+o(1)}$$

as $p \to \infty$.

Proof. Let $\mathcal{U}$ be the set of $u \in \{0, \dots, p-1\}$, which are counted by $U(p; k, h)$. Using (4.6) we see that any w of the form $w = uv$ with $uv \in \mathcal{U}$ satisfies $0 \leq w \leq p^2 - 1$ and

$$q_p(w) \equiv z \pmod p \tag{4.9}$$

for some $z \in [2k+2, 2k+2h]$. For a fixed integer z, there are $O(p)$ values of $w \in \{0, \dots, p^2-1\}$ satisfying (4.9), which follows immediately from (4.7) (see also the proof

of [51, Proposition 2.1]). So there are at most $O(hp)$ values of w satisfying (4.9) with some $z \in [2k+2, 2k+2h]$. Using the classical estimate

$$\tau(w) = w^{o(1)}, \qquad w \to \infty,$$

on the divisor function $\tau(w)$ (see [70, Bound (1.81)] with $k = 2$), we deduce that each $w = uv$ can be obtained from no more than $p^{o(1)}$ distinct pairs $(u, v) \in \mathcal{U}^2$. Therefore $(\#\mathcal{U})^2 \le hp^{1+o(1)}$, which concludes the proof. □

4.6 Image size

Let $M(p)$ be the image size of the $q_p(u)$ for $0 \le u \le p-1$, that is

$$M(p) = \#\{q_p(u) \ : \ 0 \le u \le p-1\}.$$

The bound (4.1) immediately implies $M(p) \ge p^{1/2+o(1)}$. In fact more precise bounds

$$\sqrt{p} - 1 \le M(p) \le p - \sqrt{(p-1)/2}$$

can be obtained from (4.6) and (4.7), see [47, Section 3].

We now obtain a stronger lower bound on $M(p)$.

Theorem 79. *We have*

$$M(p) \ge (1 + o(1)) \frac{p}{(\log p)^2},$$

as $p \to \infty$.

Proof. Let $Q(p, a)$ be the number of primes $\ell \in \{1, \ldots, p-1\}$ with $q_p(\ell) = a$ (note that we have discarded $u = 0$). Clearly

$$\sum_{a=0}^{p-1} Q(p, a) = \pi(p-1) \tag{4.10}$$

where, as usual, $\pi(x)$ denotes the number of primes $\ell \le x$, and also

$$\sum_{a=0}^{p-1} Q(p, a)^2 = \#\mathcal{R}(p), \tag{4.11}$$

where

$$\mathcal{R}(p) = \{(\ell, r) \ : \ 1 \le \ell, r \le p-1, \ \ell, r \text{ primes } q_p(\ell) = q_p(r)\}.$$

We see from (4.6) that if $(\ell, r) \in \mathcal{R}(p)$ and

$$w \equiv \ell/r \pmod{p^2} \tag{4.12}$$

then

$$q_p(w) \equiv q_p(\ell) - q_p(r) \equiv 0 \pmod{p}.$$

Since all w with $q_p(w) \equiv 0 \pmod{p}$ and $\gcd(w, p) = 1$ have

$$w^{p-1} \equiv 1 \pmod{p^2},$$

they are elements of the group $\mathcal{G}_p$ of the pth power residues modulo p. Thus we see from (4.12) that

$$\#\mathcal{R}(p) \le N(p),$$

where $N(p)$ is the number of solutions (ℓ, r, w) to

$$w\ell \equiv r \pmod{p^2}, \qquad \text{where } \ell, r \le p-1,\ \ell, r \text{ primes},\ w \in \mathcal{G}_p. \tag{4.13}$$

We note that for $w \equiv 1 \pmod{p^2}$ there are exactly $\pi(p-1)$ pairs (ℓ, r) with $\ell = r$ that satisfy (4.13). For any other $w \in \mathcal{G}_p$ if (4.13) is satisfied for (ℓ_1, r_1) and (ℓ_2, r_2) then

$$\ell_1 r_2 \equiv \ell_2 r_1 \pmod{p^2}$$

which in turn implies the equation

$$\ell_1 r_2 = \ell_2 r_1 \tag{4.14}$$

(since $1 \le \ell_1, \ell_2 r_1, r_2 \le p-1$). Because $\ell_1, \ell_2 r_1, r_2$ are primes, we see from (4.14) that either $(\ell_1, \ell_2) = (r_1, r_2)$, which is impossible for $w \not\equiv 1 \pmod{p^2}$, $(\ell_1, r_1) = (\ell_2, r_2)$, which means that when $w \in \mathcal{G}_p \setminus \{1\}$ is fixed, then (4.13) is satisfied for at most one pair of primes (ℓ, r). Therefore

$$\#\mathcal{R}(p) \le N(p) \le \pi(p-1) + \#\mathcal{G}_p - 1 = p + O(p/\log p). \tag{4.15}$$

Now, since by the Cauchy inequality we have

$$\left(\sum_{a=0}^{p-1} Q(p,a)\right)^2 \le M(p) \sum_{a=0}^{p-1} Q(p,a)^2,$$

recalling (4.10) and (4.11) and using (4.15), we obtain

$$M(p) \ge (1 + o(1))\pi(p-1)^2 p^{-1}.$$

which concludes the proof. □

Clearly the bound of Theorem 79 is not tight. The image size M_m of a random map on an m element set is expected to be

$$M_m = \left(1 - \frac{1}{e}\right) m = 0.63212\ldots m$$

see [49, Theorem 2], and thus it is reasonable to expect that $M(p)/p \approx 1 - 1/e$.

We now give the average value of $M(p)/p$ taken over primes p in the intervals

$$\mathcal{J}_i = [50000i, 50000(i+1)], \qquad i = 1, 2, 3. \tag{4.16}$$

and the whole interval

$$\mathcal{J} = [50000, 200000]. \tag{4.17}$$

Range	$\mathcal{J}_1$	$\mathcal{J}_2$	$\mathcal{J}_3$	$\mathcal{J}$
# of primes	4459	4256	4136	12851
$M(p)/p$	0.63212	0.63208	0.63212	0.63211

Statistics of image sizes

4.7 Statistics of orbit lengths

For any map f defined on an m element set, and any initial value u_0 from this set, we consider the iterations $u_i = f(u_{i-1})$, $i = 1, 2, \ldots$. Then for some $\rho > \mu \geq 0$ we have $u_\rho = u_\mu$. The smallest value of ρ is called the *orbit length* and the corresponding (and thus uniquely defined) value of μ is called the *tail length*.

By [49, Theorem 3] the expected values ρ_m and μ_m of the orbit and tail length, taken over all random maps and initial values u_0, satisfy

$$\frac{\rho_m}{\sqrt{m}} = \sqrt{\pi/2} + o(1) \qquad \text{and} \qquad \frac{\mu_m}{\sqrt{m}} = \sqrt{\pi/8} + o(1),$$

as $m \to \infty$.

Here we present the results of computation of the average values of the orbit and the tail lengths, scaled by $\sqrt{p}$, for the sequence (4.2) taken over primes p in the intervals $\mathcal{J}_1, \mathcal{J}_2, \mathcal{J}_3$ and $\mathcal{J}$, given by (4.16) and (4.17), respectively, and a randomly chosen initial value $u_0 \in [1, p-1]$.

Range	$\mathcal{J}_1$	$\mathcal{J}_2$	$\mathcal{J}_3$	$\mathcal{J}$
# of primes	4459	4256	4136	12851
$\rho/\sqrt{p}$	1.2423	1.2445	1.2444	1.2437
$\mu/\sqrt{p}$	0.62179	0.62200	0.61806	0.62066

Statistics of orbit and the tail lengths

The results show quite satisfactory matching with the expected values of

$$\sqrt{\pi/2} = 1.2533\ldots \qquad \text{and} \qquad \sqrt{\pi/8} = 0.62665\ldots.$$

Since the values $q_p(2)$ are of special interest, we also present similar data where the initial value is always chosen as $u_0 = 2$.

Range	$\mathcal{J}_1$	$\mathcal{J}_2$	$\mathcal{J}_3$	$\mathcal{J}$
# of primes	4459	4256	4136	12851
$\rho/\sqrt{p}$	1.2381	1.2507	1.2401	1.2429
$\mu/\sqrt{p}$	0.61778	0.63004	.62060	0.62275

Statistics of orbit and the tail lengths, $u_0 = 2$

The results show quite satisfactory matching with the expected values of

$$\sqrt{\pi/2} = 1.2533\ldots \qquad \text{and} \qquad \sqrt{\pi/8} = 0.62665\ldots.$$

Furthermore, we also give similar average values for $C(p)/p$, where $C(p)$ is the total number of cyclic points in all possible trajectories of the map $u \mapsto q_p(u)$ on the set $\{0, \ldots, p-1\}$, taken over primes from the same intervals $\mathcal{J}_1, \mathcal{J}_2, \mathcal{J}_3$ and $\mathcal{J}$.

By [49, Theorem 2] the number C_m of cyclic nodes of a random map on an m element set is expected to be

$$C_m = \sqrt{\pi/2}m = 1.2533\ldots.$$

Range	$\mathcal{J}_1$	$\mathcal{J}_2$	$\mathcal{J}_3$	$\mathcal{J}$
# of primes	4459	4256	4136	12851
$C(p)/\sqrt{p}$	1.2413	1.2527	1.23706	1.2437

Statistics of cyclic points

4.8 Distribution of consecutive elements

For integers M, $N \geq 1$, $s \geq 1$ and an integer vector $\mathbf{a} = (a_0, \ldots, a_{s-1})$ we consider the exponential sums

$$S_{s,p}(M, N; \mathbf{a}) = \sum_{u=M+1}^{M+N} \mathbf{e}_p\left(\sum_{j=0}^{s-1} a_j q_p(u+j)\right).$$

Thus the above sums are generalisations of those of Lemma 69 that correspond to the case $s = 1$. However the method of Heath-Brown [66] does not seem to apply to the sums $S_{s,p}(M, N; \mathbf{a})$ as it requires good estimates of multiplicative character sums with polynomials, which are not currently known (see however [27] for some potential approaches in the case $s = 2$).

We are now ready to prove an estimate on $S_{s,p}(M, N; \mathbf{a})$ which together with Lemma 14 implies an upper bound on the discrepancy of points (4.3).

Theorem 80. *For any integer $s \geq 1$, we have*

$$\max_{\gcd(a_0,\ldots,a_{s-1},p)=1} |S_{s,p}(M, N; \mathbf{a})| \ll N^{1/2}p^{1/2} + s^{1/2}Np^{-1/4} + sN/p$$

uniformly over M and $p^2 > N \geq 1$.

Proof. Select any $\mathbf{a} = (a_0, \ldots, a_{s-1}) \in \mathbb{Z}^m$ with $\gcd(a_0, \ldots, a_{s-1}, p) = 1$ and take $K = \lfloor N/p \rfloor$. We get

$$\begin{aligned} S_{s,p}(M, N; \mathbf{a}) &= \sum_{u=M+1}^{M+Kp} \mathbf{e}_p\left(\sum_{j=0}^{s-1} a_j q_p(u+j)\right) + O(p) \\ &= \sum_{u=1}^{Kp} \mathbf{e}_p\left(\sum_{j=0}^{s-1} a_j q_p(u+M+j)\right) + O(p) \\ &= \sum_{v=1}^{p} \sum_{k=0}^{K-1} \mathbf{e}_p\left(\sum_{j=0}^{s-1} a_j q_p(v+M+j+kp)\right) + O(p). \end{aligned}$$

Let $\mathcal{V}$ be the set of $v = 1, \ldots, p$ with $v \not\equiv -M - j \pmod p$ for any $j = 0, \ldots, s-1$. Therefore, using (4.7), we obtain:

$$S_{s,p}(M, N; \mathbf{a}) = W + O(p + sK), \tag{4.18}$$

where

$$\begin{aligned} W &= \sum_{v \in \mathcal{V}} \sum_{k=0}^{K-1} \mathbf{e}_p\left(\sum_{j=0}^{s-1} (a_j q_p(v+M+j) - a_j k (v+M+j)^{-1})\right) \\ &= \sum_{v \in \mathcal{V}} \mathbf{e}_p\left(\sum_{j=0}^{s-1} a_j q_p(v+M+j)\right) \sum_{k=0}^{K-1} \mathbf{e}_p\left(-k \sum_{j=0}^{s-1} a_j (v+M+j)^{-1}\right). \end{aligned}$$

Taking now the absolute value, we obtain

$$|W| \le \sum_{v \in \mathcal{V}} \left| \sum_{k=0}^{K-1} \mathbf{e}_p\left(k \sum_{j=0}^{s-1} a_j (v+M+j)^{-1}\right)\right|,$$

and using the Cauchy inequality we derive

$$\begin{aligned} |W|^2 &\le p \sum_{v \in \mathcal{V}} \left| \sum_{k=0}^{K-1} \mathbf{e}_p\left(k \sum_{j=0}^{s-1} a_j (v+M+j)^{-1}\right)\right|^2 \\ &= p \sum_{k_1, k_2=0}^{K-1} \sum_{v \in \mathcal{V}} \mathbf{e}_p\left((k_1 - k_2) \sum_{j=0}^{s-1} a_j (v+M+j)^{-1}\right) \\ &= p \sum_{k_1, k_2=0}^{K-1} \sum_{v \in \mathcal{V}} \mathbf{e}_p\left((k_1 - k_2) F_{\mathbf{a},s}(v)\right), \end{aligned}$$

where

$$F_{\mathbf{a},s}(V) = \sum_{j=0}^{s-1} \frac{a_j}{V+M+j}.$$

Examining the poles of $F_{\mathbf{a},s}(v)$, we see that if $\gcd(a_0,\dots,a_{s-1},p)=1$ then it is not constant modulo p.

For $O(K)$ pairs (k_1,k_2) with $k_1 \equiv k_2 \pmod p$ (which is equivalent to $k_1=k_2$ as $K \le p$) we estimate the inner sum trivially as p. For the other $O(K^2)$ pairs (k_1,k_2) we use the remark above and thus apply Lemma 9 to estimate the inner sum. Hence,

$$W^2 \ll p^2K + sp^{3/2}K^2 \ll p^2K + sp^{3/2}K^2.$$

Thus, recalling (4.18), we derive

$$|S_{s,p}(M,N;\mathbf{a})| \ll pK^{1/2} + s^{1/2}p^{3/4}K + p + sK \ll pK^{1/2} + s^{1/2}p^{3/4}K + sK.$$

Substituting $K=\lfloor N/p \rfloor$, we derive the desired result. □

Note that for a fixed s the bound of Theorem 80 simplifies as

$$\max_{\gcd(a_0,\dots,a_{s-1},p)=1} |S_{s,p}(M,N;\mathbf{a})| \ll N^{1/2}p^{1/2} + Np^{-1/4}$$

and using Lemma (14) we immediately obtain:

Corollary 81. *For any fixed s, the discrepancy $\Delta_{p,s}(M,N)$ of points (4.3) satisfies*

$$\Delta_{p,s}(M,N) \ll (p^{1/2}N^{-1/2} + p^{-1/4})(\log p)^s,$$

uniformly over M and $p^2 > N \ge 1$.

4.9 Distribution with arbitrary lags

In [29] we first study the distribution of the points

$$\Gamma(D,N,s) = \left\{ \left(\frac{q_p(u+d_0)}{p}, \dots, \frac{q_p(u+d_{s-1})}{p} \right) : u = 1,\dots,N \right\} \tag{4.19}$$

in the s-dimensional unit interval for any lags $D=(d_0,\dots,d_{s-1})$ with $0 \le d_0 < \cdots < d_{s-1} < p^2$. More precisely, we prove an exponential sum bound (which implies a discrepancy bound using the Erdős-Turán-Koksma inequality) which is nontrivial for $s=2$ and arbitrary lags $0 \le d_0 < d_1 < p^2$ and for $s>2$ if no three lags are equivalent modulo p. We note that in the case when $d_i \not\equiv d_j \pmod p$ for all $0 \le i < j < s$, the proof is exactly the same as in Theorem 80. However, the other case brings interesting twists and are discussed in Theorem 82 below. We also indicate that the exponential sums can be trivial for $s>2$ if there exist three equivalent lags modulo p.

For integers $N \ge 1$, $s \ge 1$ and $\mathbf{a}=(a_0,\dots,a_{s-1}) \in \mathbb{Z}^s$ we consider the exponential sums

$$S_{s,p}(N,D,\mathbf{a}) = \sum_{u=1}^{N} \psi\left(\sum_{j=0}^{s-1} a_j q_p(u+d_j) \right),$$

for any integer vector $D=(d_0,d_1,\dots,d_{s-1})$ with $0 \le d_0 < d_1 < \cdots < d_{s-1} < p^2$.

Theorem 82. *For $s \geq 1$ and $D = (d_0, d_1, \ldots, d_{s-1})$ with $0 \leq d_0 < d_1 < \cdots < d_{s-1} < p^2$ such that no triple (d_l, d_h, d_t) satisfies $d_l \equiv d_h \equiv d_t \pmod{p}$ for $0 \leq l < h < t < s$, we have*

$$\max_{\gcd(a_0,\ldots,a_{s-1},p)=1} |S_{s,p}(N, D, \mathbf{a})| \ll s \max\{p \log p, Np^{-1/2}\} \quad \text{for } 1 \leq N \leq p^2.$$

If $s = 2$ or $d_{s-1} < p$, the stronger bound $sp \log p$ holds.

Proof. For $s = 1$ the result follows from [66] and we assume $s \geq 2$. Select any $\mathbf{a} = (a_0, \ldots, a_{s-1}) \in \mathbb{Z}^s$ with $\gcd(a_0, \ldots, a_{s-1}, p) = 1$. Let denote by l the smallest index such that $\gcd(a_l, p) = 1$. For $d_l \not\equiv d_j \pmod{p}$ for all $l < j < s$, we can obtain the desired result by following the proof path of Theorem 80.

Now we suppose that there exists h with $l < h < s$ such that $d_l \equiv d_h \pmod{p}$ but $d_l \not\equiv d_j \pmod{p}$ for all $j \neq h$ with $l < j < s$ by our assumption. Let $d_h = d_l + k_0 p$ for some integer $1 \leq k_0 < p$. Take $K = \lceil N/p \rceil$ and note that $K \leq p$. Using (4.7) we get

$$\begin{aligned}
&S_{s,p}(N, D, \mathbf{a}) \\
&\quad = \sum_{u=1}^{Kp} \psi\left(\sum_{j=0}^{s-1} a_j q_p(u + d_j)\right) + O(p) \\
&\quad = \sum_{u=1}^{Kp} \psi\left(a_l q_p(u + d_l) + a_h q_p(u + d_l + k_0 p) + \sum_{\substack{j=l+1 \\ j \neq h}}^{s-1} a_j q_p(u + d_j)\right) + O(p) \\
&\quad = \sum_{\substack{u=1 \\ u \not\equiv -d_l \pmod{p}}}^{Kp} \psi\Big(-k_0 a_h (u + d_l)^{-1} + (a_l + a_h) q_p(u + d_l) \\
&\qquad\qquad + \sum_{\substack{j=l+1 \\ j \neq h}}^{s-1} a_j q_p(u + d_j)\Big) + O(p) \\
&\quad = \sum_{\substack{v=1 \\ v \not\equiv -d_l \pmod{p}}}^{p} \psi\left(-k_0 a_h (v + d_l)^{-1}\right) \\
&\qquad \cdot \sum_{k=0}^{K-1} \psi\left((a_l + a_h) q_p(v + d_l + kp) + \sum_{\substack{j=l+1 \\ j \neq h}}^{s-1} a_j q_p(v + d_j + kp)\right) + O(p),
\end{aligned}$$

where we substituted $u = v + kp$ in the last step.

If $a_l + a_h \not\equiv 0 \pmod{p}$ we get the result following the proof of Theorem 80. Let $\mathcal{V}$ be the set of $1 \le v \le p$ with $v \not\equiv -d_j \pmod{p}$ for $l \le j < s$. Then we have

$$\begin{aligned}
&|S_{s,p}(N, D, \mathbf{a})| \\
&\quad \le \sum_{v \in \mathcal{V}} \left| \sum_{k=0}^{K-1} \psi \left((a_l + a_h) q_p(v + d_l + kp) + \sum_{\substack{j=l+1 \\ j \ne h}}^{s-1} a_j q_p(v + d_j + kp) \right) \right| \\
&\qquad\qquad + O(sp) \\
&\quad = \sum_{v \in \mathcal{V}} \left| \sum_{k=0}^{K-1} \psi \left(k \left((a_l + a_h)(v + d_l)^{-1} + \sum_{\substack{j=l+1 \\ j \ne h}}^{s-1} a_j (v + d_j)^{-1} \right) \right) \right| + O(sp) \\
&\quad \ll sp \log p,
\end{aligned}$$

where we used [113, Lemma 3] in the last step and the fact that

$$F(X) = \frac{a_l + a_h}{X + d_l} + \sum_{\substack{j=l+1 \\ j \ne h}}^{s-1} \frac{a_j}{X + d_j}$$

is a nonconstant rational function of degree $O(s)$. (Note that $-d_l$ is a single pole of $F(X)$.)

If $a_l \equiv -a_h \pmod{p}$ and there is a $j \ne h$ with $l < j < s$ such that $\gcd(a_j, p) = 1$ and d_j is either not equivalent to any other lag d_k or $a_j \not\equiv -a_k$ we see that $F(X)$ is not constant again and derive the bound $sp \log p$ in the same way.

In the last case all lags d_j with $\gcd(a_j, p) = 1$ appear in pairs $d_j, d_{h(j)}$ with $d_{h(j)} \equiv d_j + k_j p \pmod{p}$ for some $1 \le k_j < p$ such that $a_j \equiv -a_{h(j)} \pmod{p}$. In this case we get

$$S_{s,p}(N, D, \mathbf{a}) = \sum_{u=1}^{N} \psi \left(\sum_j a_j k_j (u + d_j)^{-1} \right)$$

and get the bound

$$sp^{1/2} \left(\frac{N}{p} + \log p \right)$$

using the standard method for reducing incomplete exponential sums to complete ones, see [70, Chapter 12], and the bound of Moreno and Moreno [94]. (Note that we have $\lfloor N/p \rfloor$ complete sums and one incomplete sum.) For $s = 2$ the sum over j contains only one summand and we can obtain the better bound

$$\frac{N}{p} + p^{1/2} \log p \ll p$$

and the result follows. □

Together with Lemma 14, Theorem 82 implies an upper bound on the discrepancy of points (4.19).

Corollary 83. *For $s \geq 1$ and $D = (d_0, d_1, \ldots, d_{s-1})$ with $0 \leq d_0 < d_1 < \cdots < d_{s-1} < p^2$ such that no triple (d_l, d_h, d_t) satisfies $d_l \equiv d_h \equiv d_t \pmod{p}$, $0 \leq l < h < t < s$, the discrepancy of points $\Gamma(D, N, s)$ defined by (4.19) satisfies*

$$\Delta(\Gamma(D, N, s)) \ll \left(\frac{3}{2}\right)^s s \max\{N^{-1} p \log p, p^{-1/2}\} (\log p)^s$$

for $1 \leq N \leq p^2$. Furthermore, if $s = 2$ or $d_{s-1} < p$, we have

$$\Delta(\Gamma(D, N, s)) \ll (3/2)^s s N^{-1} p (\log p)^{s+1}.$$

However, Theorem 80, hence Corollary 81, are not extendable if there exist at least three lags congruent modulo p, as the following example shows.

Example 84. *For $D = (d_0, d_1, d_2)$ with $0 \leq d_0 < d_1 < d_2 < p^2$ and $d_0 \equiv d_1 \equiv d_2 \pmod{p}$, let $d_1 = d_0 + k_1 p$ and $d_1 = d_0 + k_2 p$ for some integers $1 \leq k_1 < k_2 < p$, then we have*

$$\begin{aligned}
&S_{3,p}(N, D, \mathbf{a}) \\
&\quad = \sum_{u=1}^{N} \psi \left(\sum_{j=0}^{2} a_j q_p(u + d_j) \right) \\
&\quad = \sum_{u=1}^{N} \psi \left(\sum_{j=0}^{2} a_j q_p(u + d_0) - a_1 k_1 (u + d_0)^{-1} - a_2 k_2 (u + d_0)^{-1} \right) \\
&\quad = \sum_{u=1}^{N} \psi \left(\sum_{j=0}^{2} a_j q_p(u + d_0) - (a_1 k_1 + a_2 k_2)(u + d_0)^{-1} \right).
\end{aligned}$$

We get a trivial bound on $S_{3,p}(N, D, \mathbf{a})$ if $a_0 + a_1 + a_2 \equiv 0 \pmod{p}$ and $a_1 k_1 + a_2 k_2 \equiv 0 \pmod{p}$. In fact, for example, one can select $a_0 = 1, a_1 = -2, a_2 = 1$ if we take $k_1 = 1$ and $k_2 = 2$.

4.10 Linear complexity

Here we estimate the linear complexity for a sufficiently long sequence of consecutive values of $q_p(u)$.

Theorem 85. *For $p^2 > N \geq 1$ the linear complexity $L_p(N)$ of the sequence $q_p(u)$, $u = 0, \ldots, N-1$, satisfies*

$$L_p(N) \geq \frac{1}{2} \min\{p - 1, N - p - 1\}.$$

Proof. Assume that

$$\sum_{j=0}^{L} c_j q_p(u+j) \equiv 0 \pmod{p}, \qquad 0 \le u \le N-L-1, \tag{4.20}$$

for some integers $c_0, \dots, c_{L-1}$ and $c_L = -1$. Let $R = \min\{p-L, N-L-p\}$. Then we see from (4.20) that for $1 \le u \le R-1$ we have

$$\sum_{j=0}^{L} c_j q_p(u+p+j) \equiv 0 \pmod{p}. \tag{4.21}$$

Recalling (4.7) and using (4.20) again, we now see that

$$\begin{aligned} \sum_{j=0}^{L} c_j q_p(u+p+j) &\equiv \sum_{j=0}^{L} c_j \left(q_p(u+j) - (u+j)^{-1}\right) \\ &\equiv -\sum_{j=0}^{L} c_j (u+j)^{-1} \pmod{p}. \end{aligned} \tag{4.22}$$

Comparing (4.21) and (4.22) we see that

$$\sum_{j=0}^{L} c_j (u+j)^{-1} \equiv 0 \pmod{p}, \qquad 1 \le u \le R-1.$$

We can assume that $L < p$ since otherwise there is nothing to prove. Clearing the denominators, we obtain a nontrivial polynomial congruence

$$\sum_{j=0}^{L} c_j \prod_{\substack{h=0 \\ h \ne j}}^{L} (u+h) \equiv 0 \pmod{p},$$

of degree L, which has $R-1$ solutions (to see that it is nontrivial it is enough to substitute $u = 0$ in the polynomial on the left hand side). Therefore $L \ge R-1$ and the result follows. □

The argument used in the proof of Theorem 85 can also be used to estimate the linear complexity of arbitrary segments of the sequence $q_p(u)$, although the resulting bound is slightly weaker.

Theorem 86. *For M and $p^2 > N \ge 1$ the linear complexity $L_p(M;N)$ of the sequence $q_p(u)$, $u = M+1, \dots, M+N$, satisfies*

$$L_p(M;N) \ge \min\left\{\frac{p-1}{2}, \frac{N-p-1}{3}\right\}.$$

Proof. Assume that

$$\sum_{j=0}^{L} c_j q_p(u+M+j) \equiv 0 \pmod{p}, \qquad 1 \le u \le N-L, \tag{4.23}$$

for some integers $c_0, \dots, c_{L-1}$ and $c_L = -1$. Let $R = \min\{p, N-L-p\}$. Then we see from (4.23) that for $1 \le u \le R$ we have

$$\sum_{j=0}^{L} c_j q_p(u+M+p+j) \equiv 0 \pmod{p}. \tag{4.24}$$

Recalling (4.7) and using (4.23) again, we now see that for any integer u with $u \not\equiv -M-j \pmod{p}$, $j = 0, \dots, L$, we have

$$\begin{aligned} \sum_{j=0}^{L} c_j q_p(u+M+p+j) &\equiv \sum_{j=0}^{L} c_j \left(q_p(u+M+j) - (u+M+j)^{-1}\right) \\ &\equiv -\sum_{j=0}^{L} c_j (u+M+j)^{-1} \pmod{p}. \end{aligned} \tag{4.25}$$

Comparing (4.24) and (4.25) we see that

$$\sum_{j=0}^{L} c_j (u+M+j)^{-1} \equiv 0 \pmod{p},$$

for at east $R-L-1$ values of u with

$$1 \le u \le R \qquad \text{and} \qquad u \not\equiv -M-j \pmod{p},\ j = 0, \dots, L.$$

As before we can assume that $L < p$ since otherwise there is nothing to prove. Clearing the denominators, we obtain a nontrivial polynomial congruence

$$\sum_{j=0}^{L} c_j \prod_{\substack{h=0 \\ h \ne j}}^{L} (u+M+h) \equiv 0 \pmod{p}$$

of degree L, which has at least $R-L-1$ solutions (to see that it is nontrivial it is enough to substitute $u = -M$ in the polynomial on the left hand side). Therefore $L \ge R-L-1$ and the result follows. □

4.11 Lattice tests

We study the lattice structure of the sequence $(q_p(u))$. The following lattice test was introduced in [106]. Let (w_u), $u = 1, 2, \ldots$, be a T-periodic sequence over the finite field $\mathbb{F}_p$ of p elements. For given integers $s \geq 1$, $0 \leq d_0 < d_1 < \ldots < d_{s-1} < T$, and $N \geq 2$, we say that (w_u) passes the *s-dimensional N-lattice test with lags $d_0, \ldots, d_{s-1}$* if the vectors $\{\mathbf{w}_u - \mathbf{w}_1 : 1 \leq u \leq N\}$ span $\mathbb{F}_p^s$, where

$$\mathbf{w}_u = (w_{u+d_0}, w_{u+d_1}, \ldots, w_{u+d_{s-1}}), \quad 1 \leq u \leq N.$$

In the case $d_i = i$ for $0 \leq i < s$, this test coincides essentially with the lattice test introduced in [41] and further analysed in [39, 40, 41, 42, 139]. The latter lattice test is closely related to the concept of the linear complexity profile, see [41, 42, 104]. If additionally $N \geq T$, this special lattice test was proposed by Marsaglia [87].

We note that in the case $d_i \not\equiv d_j \pmod p$ for all $0 \leq i < j < s$, the lattice test can be analysed essentially along the same lines as in the proof of the linear complexity bounds in Theorems 85 and 86.

We denote by

$$S((w_u), N, D) = \max\{s : \langle (w_{u+d_0} - w_{1+d_0}, \ldots, w_{u+d_{s-1}} - w_{1+d_{s-1}}), \\ 1 \leq u \leq N \rangle = \mathbb{F}_p^s\}$$

the greatest dimension s such that (w_u) satisfies the s-dimensional N-lattice test for the lags $D = (d_0, \ldots, d_{s-1})$ with $0 \leq d_0 < \cdots < d_{s-1} < p^2$.

As we mentioned before, in the case $d_i \not\equiv d_j$ for all $0 \leq i < j < s$, we can essentially proceed as in the proof of Theorem 85.

Theorem 87. *For $N \geq 2$ and $D = (d_0, d_1, \ldots, d_{s-1})$ with $0 \leq d_0 < d_1 < \cdots < d_{s-1} < p^2$ such that no triple (d_l, d_h, d_t) satisfies $d_l \equiv d_h \equiv d_t \pmod p$, $0 \leq l < h < t < s$, we have*

$$S((q_p(u)), N, D) \geq \min\left\{\frac{p-1}{2}, \frac{N-p-1}{2}\right\}.$$

Proof. We assume that the sequence $(q_p(u))$ does not pass the s-dimensional N-lattice test for some lags $0 \leq d_0 < d_1 < \ldots < d_{s-1} < p^2$. Put

$$\mathbf{w}_u = (q_p(u + d_0), q_p(u + d_1), \ldots, q_p(u + d_{s-1})), \quad \text{for } u = 1, \ldots, N,$$

and let V be the subspace of $\mathbb{F}_p^s$ spanned by all $\mathbf{w}_u - \mathbf{w}_1$ for $1 \leq u \leq N$. Let denote by $V^\perp = \{\mathbf{u} \in \mathbb{F}_p^s : \mathbf{u} \cdot \mathbf{v} = 0 \text{ for all } \mathbf{v} \in V\}$ the *orthogonal space* of V, where $\cdot$ denotes the usual inner product. Then $\dim(V) < s$ and $\dim(V^\perp) \geq 1$. Take $\mathbf{0} \neq \alpha \in V^\perp$, then

$$\alpha \cdot (\mathbf{w}_u - \mathbf{w}_1) = 0 \quad \text{for } 1 \leq u \leq N.$$

We denote

$$\delta = \alpha \cdot \mathbf{w}_u = \alpha \cdot \mathbf{w}_1 \quad \text{for } 1 \leq u \leq N.$$

If $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{s-1})$, then let j be the smallest index with $\alpha_j \neq 0$ (so $0 \leq j < s$). Then we get

$$\sum_{i=j}^{s-1} \alpha_i q_p(u + d_i) \equiv \delta \pmod{p} \quad \text{for } 1 \leq u \leq N. \tag{4.26}$$

Let $R = \min(p, N - p)$. We see from (4.26) that for $1 \leq u \leq R$ we have

$$\sum_{i=j}^{s-1} \alpha_i q_p(u + p + d_i) \equiv \delta \pmod{p}. \tag{4.27}$$

Recalling (4.7) and using (4.26) again, we now see that for any integer u with $u + d_i \not\equiv 0 \pmod{p}$, $i = j, \ldots, s-1$, we have

$$\begin{aligned} \sum_{i=j}^{s-1} \alpha_i q_p(u + p + d_i) &\equiv \sum_{i=j}^{s-1} \alpha_i \left(q_p(u + d_i) - (u + d_i)^{-1} \right) \\ &\equiv \delta - \sum_{i=j}^{s-1} \alpha_i (u + d_i)^{-1} \pmod{p}. \end{aligned} \tag{4.28}$$

Comparing (4.27) and (4.28) we see that

$$\sum_{i=j}^{s-1} \alpha_i (u + d_i)^{-1} \equiv 0 \pmod{p} \tag{4.29}$$

for at least $R - s + j$ values of u with

$$1 \leq u \leq R, \quad u + d_i \not\equiv 0 \pmod{p}, \ \ i = j, \ldots, s-1.$$

We consider first the that case $d_j \not\equiv d_h \pmod{p}$, for all $j < h < s$. Clearing the denominators of (4.29), we obtain a nontrivial polynomial congruence

$$\sum_{i=j}^{s-1} \alpha_i \prod_{\substack{e=j \\ e \neq i}}^{s-1} (u + d_e) \equiv 0 \pmod{p}$$

of degree $s - j - 1 \leq s$, which has at least $R - s + j$ solutions (to see that it is nontrivial it is enough to substitute $u \equiv -d_j \pmod{p}$ in the polynomial on the left hand side). Therefore $s - j - 1 \geq R - s + j$ and the result follows.

In the case $d_j \equiv d_h \pmod{p}$, for some $j < h < s$, taking $d_h = k_0 p + d_j$ for some $k_0 \geq 1$ and proceeding in the same way as above (but recalling that $u + d_j \equiv u + d_h \pmod{p}$), we get

$$(\alpha_j + \alpha_h) \prod_{\substack{e=j+1 \\ e \neq h}}^{s-1} (u + d_e) + (u + d_j) \sum_{\substack{i=j+1 \\ i \neq h}}^{s-1} \alpha_i \prod_{\substack{e=j \\ e \neq i}}^{s-1} (u + d_e) \equiv 0 \pmod{p}. \tag{4.30}$$

If $\alpha_j + \alpha_h \not\equiv 0 \pmod{p}$ then the nontriviality of this polynomial equation is obvious again.

In the case of $\alpha_j + \alpha_h \equiv 0 \pmod{p}$, we have reduced the s-dimensional lattice test to the $(s-2)$-dimensional one. If we are in a case where no two lags are equivalent or there are some equivalent lags $d_{j'}, d_{h'}$ with corresponding $\alpha_{j'} + \alpha_{h'} \not\equiv 0 \pmod{p}$ we easily see that (4.30) is nontrivial.

Hence, we are left with the case that there are only pairs d_i, $d_{h(i)} = d_i + k_i p$ of equivalent lags such that the sum of the corresponding coefficients $\alpha_i + \alpha_{h(i)}$ vanishes modulo p. However, in this case we get

$$\delta \equiv \sum_i (\alpha_i + \alpha_h(i)) q_p(u + d_i) + \sum_i \alpha_i k_i (u + d_i)^{-1} \equiv \sum_i \alpha_i k_i (u + d_i)^{-1}.$$

Since we can assume $\alpha_i \not\equiv 0 \pmod{p}$ for some i and the remaining d_i are pairwise distinct modulo p now, we have a nontrivial polynomial equation from which we obtain our result. □

However, in the case when there exist three lags d_l, d_h, d_t, $0 \le l < h < t < s$, such that $d_l \equiv d_h \equiv d_t \pmod{p}$, the lattice test fails as the next result shows.

Theorem 88. *For $N \ge 2$ and $D = (d_0, d_1, \ldots, d_{s-1})$ with $0 \le d_0 < d_1 < \cdots < d_{s-1} < p^2$ such that there exist a triple (d_l, d_h, d_t) satisfies $d_l \equiv d_h \equiv d_t \pmod{p}$, $0 \le l < h < t < s$, we have*

$$S((q_p(u)), N, D) = 2.$$

Proof. To prove this result it is sufficient to consider the case $s = 3$ and to see that for $d_0 \equiv d_1 \equiv d_2 \pmod{p}$ the 3-dimensional test fails. For this let $\alpha = (\alpha_0, \alpha_1, \alpha_2)$ be an orthogonal vector on each $\mathbf{w}_u$, $u = 1, 2, \ldots$, which gives the system of equations

$$\alpha_0 + \alpha_1 + \alpha_2 \equiv \alpha_1(d_1/p) + \alpha_2(d_2/p) \equiv 0 \pmod{p}.$$

It is clear that this system has a nontrivial solution α and then we easily verify that for all $u = 1, 2, \ldots$ we have

$$(\alpha_0, \alpha_1, \alpha_2) \cdot (\mathbf{w}_u - \mathbf{w}_1) = 0.$$

Hence, the orthogonal space is nontrivial and the lattice test is failed for $s = 3$, and thus for every $s > 3$. □

As in [106], the greatest dimension s such that (w_u) satisfies the s-dimensional N-lattice test for all lags $D = (d_0, \ldots, d_{s-1})$ is denoted by $S((w_u), N)$, that is,

$$S((w_u), N) = \max_D S((w_u), N, D) \max \{s \ : \ \forall\ 0 \le d_0 < \cdots < d_{s-1} < T : \\ \langle \left(w_{u+d_0} - w_{1+d_0}, \ldots, w_{u+d_{s-1}} - w_{1+d_{s-1}}\right),\ 1 \le u \le N \rangle = \mathbb{F}_p^s \}.$$

Corollary 89. *For $N \ge 2$, we have*

$$S((q_p(u)), N) = 2.$$

4.12 Distribution of $L_p(u)$

4.12.1 Exponential sums

Here we estimate the following complete exponential sums

$$S_p(a,b) = \sum_{x=0}^{p^2-1} \mathbf{e}_p(aL_p(x))\mathbf{e}_{p^2}(bx)$$

where $a, b \in \mathbb{Z}$.

Theorem 90. *For any $a, b \in \mathbb{Z}$ with*

$$|a|, |b| < p/2, \qquad a \neq 0$$

we have the following estimate

$$S_p(a,b) \ll p^{15/8}.$$

Proof. We need the following easy property of the function L_p

$$L_p(z+py) = L_p(z) - y \pmod p, \tag{4.31}$$

where $y, z \in \mathbb{F}_p$.

For $x \in \mathbb{F}_{p^2}$, we write

$$x = z + py, \quad z, y \in \mathbb{F}_p.$$

Using this notation and (4.31), the sum $S_p(a,b)$ becomes

$$\begin{aligned} S_p(a,b) &= \sum_{z=0}^{p-1}\sum_{y=0}^{p-1} \mathbf{e}_{p^2}\left(a(z^p - z) + bz - apy + bpy\right) \\ &= \sum_{z=0}^{p-1} \mathbf{e}_{p^2}\left(a(z^p - z) + bz\right) \sum_{y=0}^{p-1} \mathbf{e}_p\left((b-a)y\right). \end{aligned}$$

Recalling Theorem 7, we conclude that in the case $a \not\equiv b \pmod p$ the sum over y is identical zero.

So it now remains to consider the case $a \equiv b \pmod p$. Since $|a|, |b| < p/2$ this congruence implies that $a = b$ and we obtain

$$S_p(a,b) = p\sum_{z=0}^{p-1} \mathbf{e}_{p^2}\left(az^p\right) = pH_p(a).$$

Using Lemma 70, we conclude the proof. □

We also remark that one can use the congruence (4.31) together with the Polya-Vinogradov and Burgess bounds, see [70, Theorems 12.5 and 12.6], to show that uniformly over all nontrivial multiplicative characters χ modulo p and integers a, for any fixed integer $\nu \ge 1$, we have

$$\left|\sum_{x=0}^{N-1} \chi(L_p(x)+a)\right| \le p(N/p)^{1-1/\nu} p^{(\nu+1)/4\nu^2+o(1)} = N^{1-1/\nu} p^{(5\nu+1)/4\nu^2+o(1)}.$$

In particular, we see that for any fixed $\varepsilon > 0$, taking a sufficiently large ν, we obtain a nontrivial estimate for $N \ge p^{5/4+\varepsilon}$.

4.12.2 Discrepancy bound

We now use Theorem 90 to study the distribution of the points (4.5).

Theorem 91. *For any fixed integer $s \ge 1$, the discrepancy $\Delta_p(N)$ of the points (4.5) satisfies*

$$\Delta_p(N) \ll N p^{-15/8} (\log p)^2,$$

uniformly over $p^2 > N \ge 1$.

Proof. We note that counting how often

$$\left\{\frac{L_p(x)}{p}\right\} \in [0,\alpha], \qquad x = 1,\ldots,N,$$

is the same as counting how often

$$\left(\left\{\frac{L_p(x)}{p}\right\}, \left\{\frac{x}{p^2}\right\}\right) \in [0,\alpha]\times[0,\beta], \qquad x = 1,\ldots,p^2, \tag{4.32}$$

where $\beta = N/p^2$.

Now, applying Lemma 14 with $s = 2$ and $H = (p-1)/2$, we see, that (4.32) is satisfied for

$$\alpha\beta p^2 + O(p^2 D_p) = \alpha N + O(p^2 D_p) \tag{4.33}$$

values of $x = 1,\ldots,p^2$ (uniformly over α and β), where

$$D_p \ll p^{-1} + p^{-2} \sum_{|a|,|b|<p/2} \frac{1}{|a|+1}\frac{1}{|b|+1}|S_p(a,b)|.$$

Using now Theorem 90 we obtain $D_p = O(p^{-1/8}(\log p)^2)$. Now recalling (4.33) we obtain $\Delta_p(N) \ll p^2 D_p/N$ and the desired result follows. □

4.13 Hash functions from Fermat quotients

In this section, as in Section 2.8, we propose a new construction of hash functions based on iterations of Fermat quotients. A similar idea, however based on a very different family of functions, has been previously introduced by D. X. Charles, E. Z. Goren and K. E. Lauter [28].

Let n and r be two positive integers. Choose 2^r random $(n+1)$-bit primes $p_0, \ldots, p_{2^r-1}$. We also consider a random initial n bit integer u_0.

The has function is built from a sequence of iterations of Fermat quotients modulo $p_0, \ldots, p_{2^r-1}$. As in [28], the input of the hash function is used to decide what modulo what prime the next Fermat quotient is computed. More precisely, given an input bit string Σ, we perform the following steps:

- Pad Σ with at most $r-1$ zeros on the left to make sure that its length L is a multiple of r.
- Split Σ into blocks σ_j, $j = 1, \ldots, J$, where $J = L/r$, of length r and interpret each block as an integer $\ell \in [0, 2^r - 1]$.
- Starting at the point u_0, apply the Fermat quotient maps q_{p_ℓ} iteratively by using n least significant bits of u_{j-1} to form an n-bit integer w_{j-1} and then computing

$$u_j = q_{p_\ell}(w_{j-1}).$$

- Output the last element in the above sequence, that is, $u_J = q_{p_J}(w_{J-1})$ and outputting its n least significant bits as the value of the hash function.

We note that the results of Section 4.8 suggest that the above hash functions exhibit rather chaotic behaviour, which close to the behaviour of a random function. It is probably too early to make any suggestions about the applicability of Fermat quotients for hashing but this direction definitely deserves further studying, experimentally and theoretically.

4.14 Remarks and open problems

Unfortunately we are not able to give any estimates on the discrepancy or linear complexity of the orbits (4.2), which is a very interesting but possibly hard, question.

Obtaining analogues of Theorems 80, 85 and 86, which are nontrivial for $N < p$ is another interesting question.

The method of proof of Theorems 85 and 86 does not apply to the *non-linear complexity*. We recall the non-linear complexity of degree d of an N-element sequence $s_0, \ldots, s_{N-1}$ of elements in a ring $\mathcal{R}$ is the smallest L such that

$$s_{u+L} = \psi(s_{u+L-1}, \ldots, s_u), \qquad 0 \le u \le N - L - 1,$$

where $\psi \in \mathcal{R}[Y_1, \ldots, Y_L]$ is a polynomial of total degree at most d. Estimating the nonlinear complexity of Fermat quotients is of ultimate interest.

Finally, we remark that one can also study the sums

$$T_p(M, N; \chi) = \sum_{u=M+1}^{M+N} \chi\left(q_p(u)\right)$$

with a nonprincipal multiplicative character χ modulo p. Arguing as in the proof of Theorem 80 we get

$$|T_p(M, N; \chi)| \ll \sum_{v=M+1}^{M+p-1} \left| \sum_{k=0}^{K-1} \chi\left(q_p(v+M) - k(v+M)^{-1})\right)\right| + p,$$

where $K = \lfloor N/p \rfloor$. One can now apply the Burgess bound, see [70, Theorems 12.6], and get a nontrivial estimate on $T_p(M, N; \chi)$, starting with $N \geq p^{5/4+\varepsilon}$ for any fixed $\varepsilon > 0$, see [125]. However it is natural to expect that one can take advantage of additional averaging over v and get a nontrivial bound for smaller values of N. Furthermore, using (4.6) it is possible to estimate bilinear character sums

$$W_p(\mathcal{A}, \mathcal{B}, U, V; \chi) = \sum_{0 \leq u \leq U} \sum_{0 \leq v \leq V} \alpha_u \beta_v \chi\left(q_p(uv)\right)$$

with arbitrary complex weights $\mathcal{A} = (\alpha_u)$ and $\mathcal{B} = (\beta_v)$, and then using the Vaughan identity, see [70, Section 13.4], estimate the character sums with Fermat quotients at primes arguments, see [125] for details.

Furthermore, we remark that studying the map $x \mapsto (x^{p-1} - 1)/p$ in the field of p-adic numbers, is also of great interest, see [138] where a similar question is considered for the maps given by (4.4). The other way around, it is also quite natural to study the map (4.4) modulo p in more detail.

For example, although for the purpose of proving Theorem 91 it has been enough to estimate the sum $S_p(a, b)$ only for b with $|b| < p/2$, it is interesting to have such estimates in the full range of b, that is, for any b with $|b| < p^2/2$.

Furthermore, it is also interesting to estimate the exponential sums

$$S_p(a_0, \ldots, a_{s-1}, b) = \sum_{x=0}^{p^2-1} \mathbf{e}_p\left(\sum_{j=0}^{s-1} a_j L_p(x+j)\right) \mathbf{e}_{p^2}(bx)$$

where $a_0, \ldots, a_{s-1}, b \in \mathbb{Z}$. Even the case of $b = 0$ is already of interest.

Finally we ask for nontrivial estimates of the image size

$$J_p(N) = \#\{L_p(x) \ : \ x = 1, \ldots, N\}.$$

The congruence (4.31) immediately yields $J_p(N) \geq N/p$, however most certainly much better bounds are possible.

Finally, analogues of Fermat quotients modulo a composite number is certainly an exciting object of study with its own twists, see [1, 2, 10, 37, 130]. In particular, one can find a version of (4.6) and (4.7) in [2], and a variant of the result of [66, Theorem 2] in [130]. It is interesting that in case of composite moduli a new effect appears, namely, $\gcd(\varphi(m), m)$ enters the considerations, see [44] where this function is studied.

Bibliography

[1] T. Agoh, 'Congruences involving Bernoulli numbers and Fermat-Euler quotients', *J. Number Theory*, **94** (2002), 1–9.

[2] T. Agoh, K. Dilcher and L. Skula, 'Fermat quotients for composite moduli', *J. Number Theory*, **66** (1997), 29–50.

[3] T. Agoh and L. Skula, 'The fourth power of the Fermat quotient', *J. Number Theory*, **128** (2008), 2865–2873.

[4] O. Ahmadi, F. Luca, A. Ostafe and I. E. Shparlinski, 'On stable quadratic polynomials', *Submitted*, 2010.

[5] N. Ali, 'Stabilité des polynômes', *Acta Arith.*, **119** (2005), 53–63.

[6] V. I. Arnold, 'Fermat-Euler dynamical systems and the statistics of arithmetics of geometric progressions', *Func. Analysis Appl.*, **37** (2003), 1–15.

[7] V. I. Arnold, 'Number-theoretic turbulence in Fermat-Euler arithmetics and large Young diagrams geometry statistics', *J. Math. Fluid Mech.*, **7** (2005), S4–S50.

[8] V. I. Arnold, 'Ergodic and arithmetical properties of geometrical progression's dynamics and of its orbits', *Moscow Math. J.*, **5** (2005), 5–22.

[9] M. Ayad and D. L. McQuillan, 'Irreducibility of the iterates of a quadratic polynomial over a field', *Acta Arith.*, **93** (2000), 87–97.

[10] W. D. Banks, F. Luca and I. Shparlinski, 'Estimates for Wieferich numbers', *The Ramanujan J.*, **14** (2007), 361–378.

[11] S.R. Blackburn, T. Etzion and K.G. Paterson, 'Permutation polynomials, de Bruijn sequences, and linear complexity', *J. Comb. Theory, Ser. A*, **76** (1996), 55–82.

[12] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, 'Predicting the inversive generator', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2898** (2003), 264–275.

[13] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, 'Predicting nonlinear pseudorandom number generators', *Math. Comp.*, **74** (2005), 1471–1494.

[14] I. F. Blake, X. H. Gao, A. J. Menezes, R. C. Mullin, S. A. Vanstone and T. Yaghoobian, *Application of finite fields*, Kluwer, 1993.

[15] J. Bourgain, 'Mordell's exponential sum estimate revisited', *J. Amer. Math. Soc.*, **18** (2005), 477–499.

[16] J. Bourgain, 'Exponential sum estimates on subgroups of $\mathbb{Z}_q$, q arbitrary', *J. Anal. Math.*, **97** (2005), 317–355.

[17] J. Bourgain, 'Exponential sum estimates in finite commutative rings and applications', *J. Anal. Math.*, **101** (2007), 325–355.

[18] J. Bourgain and M. Z. Garaev, 'On a variant of sum-product estimates and explicit exponential sum bounds in prime fields', *Math. Proc. Cambridge Phil. Soc.*, **146** (2009), 1–21.

[19] J. Bourgain, K. Ford, S. V. Konyagin and I. E. Shparlinski, 'On the divisibility of Fermat quotients', *Michigan J. Math.*, (to appear).

[20] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, 'Estimates for the number of sums and products and for exponential sums in fields of prime order', *J. Lond. Math. Soc.*, **73** (2006), 380–398.

[21] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm', *Intern. Math. Research Notices*, **2008** (2008), Article ID rnn090, 1–29.

[22] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Corrigenda to: Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm', *Intern. Math. Research Notices*, **2009** (2009), 3146-3147.

[23] B. Brindza, 'On S-integral solutions of the equation $y^m = f(x)$', *Acta Math. Hungar.*, **44** (1984), 133–139.

[24] Y. Bugeaud, 'Bounds for the solutions of superelliptic equations', *Compositio Math.*, **107** (1997), 187–219.

[25] A. Çeşmelioğlu and A. Winterhof, 'On the average distribution of power residues and primitive elements in inversive and nonlinear recurring sequences ', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **5203** (2008), 60–70.

[26] M.-C. Chang, 'On a problem of Arnold on uniform distribution', *J. Funcional Analysis*, **242** (2007), 272–280.

[27] M.-C. Chang, 'Character sums in finite fields', *Proc. 9th Conf. on Finite Fields and Appl., Dublin, 2009*, Amer. Math. Soc., (to appear).

[28] D. X. Charles, E. Z. Goren and K. E. Lauter, 'Cryptographic hash functions from expander graphs', *J. Cryptology*, (to appear).

[29] Z. Chen, A. Ostafe and A. Winterhof, 'Structure of pseudorandom numbers derived from Fermat quotients', WAIFI 2010, *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, (to appear).

[30] S. D. Cohen, 'On irreducible polynomials of certain types in finite fields', *Proc. Cambridge Philos. Soc.*, **66** (1969), 335–344.

[31] S. D. Cohen and D. Hachenberger, 'The dynamics of linearized polynomials', *Proc. Edinburgh Math. Soc.*, **43** (2000), 113–128.

[32] O. Colón-Reyes, A. S. Jarrah, R. Laubenbacher and B. Sturmfels, 'Monomial dynamical systems over finite fields', *Complex Systems*, **16** (2006), 333–342.

[33] T. W. Cusick, C. Ding and A. Renvall, *Stream ciphers and number theory*, Elsevier, Amsterdam, 2003.

[34] S. Contini and I. E. Shparlinski, 'On Stern's attack against secret truncated linear congruential generators', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **3574** (2005), 52–60.

[35] P. Deligne, 'Applications de la formule des traces aux sommes trigonométriques', *Lect. Notes in Mathematics*, Springer-Verlag, Berlin, **569** (1977), 168–232.

[36] A. Di Bartolo and G. Falcone, 'Witt vectors and Fermat quotients', *J. Number Theory*, **128** (2008), 1376–1387.

[37] K. Dilcher, 'Fermat numbers, Wieferich and Wilson primes: Computations and generalizations', *Proc. the Conf. on Public Key Cryptography and Computational Number Theory, Warsaw, 2000*, Walter de Gruyter, 2001, 29–48.

[38] E. Dobrowolski and K. S. Williams, 'An upper bound for the sum $\sum_{n=a+1}^{a+H} f(n)$ for a certain class of functions f', *Proc. Amer. Math. Soc.*, **114** (1992), 29–35.

[39] G. Dorfer, 'Lattice profile and linear complexity profile of pseudorandom number sequences', *Lect. Notes in Mathematics*, Springer-Verlag, Berlin, **2948** (2004), 69–78.

[40] G. Dorfer, W. Meidl and A. Winterhof, 'Counting functions and expected values for the lattice profile at n', *Finite Fields Appl.*, **10** (2004), 636–652.

[41] G. Dorfer and A. Winterhof, 'Lattice structure and linear complexity profile of nonlinear pseudorandom number generators', *Appl. Algebra Engrg. Comm. Comput.*, **13** (2003), 499–508

[42] G. Dorfer and A. Winterhof, 'Lattice structure of nonlinear pseudorandom number generators in parts of the period', *Monte Carlo and Quasi-Monte Carlo Methods*, Springer-Verlag, Berlin, 2004, 199–211.

[43] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.

[44] P. Erdős, F. Luca and C. Pomerance, 'On the proportion of numbers coprime to a given integer', *Anatomy of Integers*, CRM Proc. and Lect. Notes, vol. 46, Amer. Math. Soc., Providence, RI, 2008, 47–64.

[45] P. Erdős and R. Murty, 'On the order of $a \pmod p$', *Proc. 5th Canadian Number Theory Association Conf.*, Amer. Math. Soc., Providence, RI, 1999, 87–97.

[46] R. Ernvall and T. Metsänkylä, 'Cyclotomic invariants for primes between 125000 and 150000', *Math. Comp.*, **56** (1991), 851–858.

[47] R. Ernvall and T. Metsänkylä, 'On the p-divisibility of Fermat quotients', *Math. Comp.*, **66** (1997), 1353–1365.

[48] G. R. Everest and T. Ward, *Heights of polynomials and entropy in algebraic dynamics*, Springer-Verlag, London, 1999.

[49] P. Flajolet and A.M. Odlyzko, 'Random mapping statistics', *Lect. Notes in Comp. Sci.*, Springer, Berlin, **434** 1990, 329–354.

[50] S. Fomin and A. Zelevinsky, 'The Laurent phenomenon', *Adv. in Appl. Math.*, **28** (2002), 119–144.

[51] W. L. Fouché, 'On the Kummer-Mirimanoff congruences', *Quart. J. Math. Oxford*, **37** (1986), 257–261.

[52] J. B. Friedlander and I. E. Shparlinski, 'On the distribution of the power generator', *Math. Comp.*, **70** (2001), 1575–1589.

[53] A. M. Frieze, J. Håstad, R. Kannan, J. C. Lagarias and A. Shamir, 'Reconstructing truncated integer variables satisfying linear congruences', *SIAM J. Comp.*, **17** (1988), 262–280.

[54] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge Univ.Press, New York, 2003.

[55] D. Gomez-Perez, J. Gutierrez and Á. Ibeas, 'Attacking the Pollard generator', *IEEE Trans. Inform. Theory*, **52** (2006), 5518–5523.

[56] D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, 'Exponential sums with Dickson polynomials', *Finite Fields Appl.*, **12** (2006), 16–25.

[57] D. Gomez and A. P. Nicolás, 'An estimate on the number of stable quadratic polynomials', *Preprint*, 2010.

[58] A. Granville, 'Some conjectures related to Fermat's Last Theorem', *Number Theory*, W. de Gruyter, NY, 1990, 177–192.

[59] A. Granville, 'On pairs of coprime integers with no large prime factors', *Expos. Math.*, **9** (1991), 335–350.

[60] A. Granville and K. Soundararajan, 'A binary additive problem of Erdős and the order of 2 mod p^2', *The Ramanujan J.*, **2** (1998), 283–298.

[61] F. Griffin, H. Niederreiter and I. E. Shparlinski, 'On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1719** (1999), 87–93.

[62] J. Gutierrez and D. Gomez-Perez, 'Iterations of multivariate polynomials and discrepancy of pseudorandom numbers', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2227** (2001), 192–199.

[63] J. Gutierrez and Á. Ibeas, 'Inferring sequences produced by a linear congruential generator on elliptic curves missing high-order bits', *Designs, Codes and Cryptography*, **41** (2007), 199–212.

[64] J. Gutierrez and A. Winterhof, 'Exponential sums of nonlinear congruential pseudorandom number generators with Redei functions', *Finite Fields Appl.*, **14** (2008), 410–416.

[65] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.

[66] R. Heath-Brown, 'An estimate for Heilbronn's exponential sum', *Analytic Number Theory: Proc. Conf. in honor of Heini Halberstam*, Birkhäuser, Boston, 1996, 451–463.

[67] D. R. Heath-Brown and S. V. Konyagin, 'New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum', *Ouart. J. Math.*, **51** (2000), 221–235.

[68] Y. Ihara, 'On the Euler-Kronecker constants of global fields and primes with small norms', *Algebraic Geometry and Number Theory*, Progress in Math., Vol. 850, Birkhäuser, Boston, Cambridge, MA, 2006, 407–451.

[69] K.-H. Indlekofer and N. M. Timofeev, 'Divisors of shifted primes', *Publ. Math. Debrecen*, **60** (2002), 307–345.

[70] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[71] D. Jao, S. D. Miller and R. Venkatesan, 'Expander graphs based on GRH with an application to elliptic curve cryptography', *J. Number Theory.*, **129** (2009), 1491–1504.

[72] R. Jones, 'Iterated Galois towers, associated martingales, and the p-adic Mandelbrot set', *Compositio Math.*, **43** (2007), 1108–1126.

[73] R. Jones, 'The density of prime divisors in the arithmetic dynamics of quadratic polynomials', *J. Lond. Math. Soc.*, **78** (2008), 523–544.

[74] R. Jones and N. Boston, 'Settled polynomials over finite fields,' *Preprint*, 2009.

[75] A. Joux and J. Stern, 'Lattice reduction: A toolbox for the cryptanalyst', *J. Cryptology*, **11** (1998), 161–185.

[76] N. Katz, 'Estimates for "singular" exponential sums', *International Mathematics Research Notices*, **16** (1999), 875–899.

[77] S. V. Konyagin, 'On estimates of Gaussian sums and the Waring problem modulo a prime', *Trudy Matem. Inst. Acad. Nauk USSR*, Moscow, **198** (1992), 111–124 (in Russian).

[78] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.

[79] H. Krawczyk, 'How to predict congruential generators', *J. Algorithms*, **13** (1992), 527–545.

[80] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Intersci., New York-London-Sydney, 1974.

[81] J. C. Lagarias, 'Pseudorandom number generators in cryptography and number theory', *Proc. Symp. in Appl. Math.*, Amer. Math. Soc., Providence, RI, **42** (1990), 115–143.

[82] S. Lang and A. Weil, 'Number of points of varieties in finite fields', *Amer. J. Math.*, **76** (1954), 819–827.

[83] H. W. Lenstra, 'Miller's primality test', *Inform. Process. Lett.*, **8** (1979), 86–88.

[84] R. Lidl and H. Niederreiter, 'On orthogonal systems and permutation polynomials in several variables', *Acta Arith.*, **22** (1973), 257–265.

[85] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[86] S. Marcello, 'Sur la dynamique arithmétique des automorphismes de l'espace affine', *Bull. Soc. Math. France*, **131** (2003), 229–257.

[87] G. Marsaglia, 'The structure of linear congruential sequences', *Applications of Number Theory to Numerical Analysis*, Academic Press, New York, 1972, 249–285.

[88] W. Meidl, 'Discrete Fourier transform, joint linear complexity and generalized joint linear complexity of multisequences', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **3486** (2005), 101–112.

[89] W. Meidl and A. Winterhof, 'Linear complexity and polynomial degree of a function over a finite field', *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*, Springer-Verlag, Berlin, 2002, 229–238.

[90] W. Meidl and A. Winterhof 'On the joint linear complexity profile of explicit inversive multisequences', *J. Complexity*, **21** (2005), 324–336

[91] W. Meidl and A. Winterhof, 'On the linear complexity profile of some new explicit inversive pseudorandom number generators', *J. Complexity*, **20** (2004), 350–355.

[92] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, Boca Raton, FL, CRC Press, 1997.

[93] S. Mohit and M. R. Murty, 'Wieferich primes and Hall's conjecture', *C. R. Math. Acad. Sci., Soc. R. Can.*, **20** (1998), 29–32.

[94] C. J. Moreno and O. Moreno, 'Exponential sums and Goppa codes I', *Proc. Amer. Math. Soc.*, **111** (1991), 523–531.

[95] H. Niederreiter, 'Quasi-Monte Carlo methods and pseudo-random numbers', *Bull. Amer. Math. Soc.*, **84** (1978), 957–1041.

[96] H. Niederreiter, *Random number generation and Quasi–Monte Carlo methods*, SIAM Press, 1992.

[97] H. Niederreiter, 'Some computable complexity measures for binary sequences', *Sequences and their applications (Singapore, 1998)*, Springer Ser. Discrete Math. Theor. Comput. Sci., Springer, London, 1999, 67–78.

[98] H. Niederreiter, 'Linear complexity and related complexity measures for sequences', *Lect. Notes in Comp. Sci.*, Springer, Berlin, **2904** (2003), 1–17.

[99] H. Niederreiter and I. E. Shparlinski, 'On the distribution and lattice structure of nonlinear congruential pseudorandom numbers', *Finite Fields and Their Appl.*, **5** (1999), 246–253.

[100] H. Niederreiter and I. E. Shparlinski, 'On the distribution of inversive congruential pseudorandom numbers in parts of the period', *Math. Comp.*, **70** (2001), 1569–1574.

[101] H. Niederreiter and I. E. Shparlinski, 'On the average distribution of inversive pseudorandom numbers', *Finite Fields and Their Appl.*, **8** (2002), 491–503.

[102] H. Niederreiter and I. E. Shparlinski, 'Recent advances in the theory of nonlinear pseudorandom number generators' *Monte Carlo and Quasi-Monte Carlo Methods*, Springer-Verlag, Berlin, 2002, 86–102.

[103] H. Niederreiter and I. E. Shparlinski, 'Dynamical systems generated by rational functions', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2643** (2003), 6–17.

[104] H. Niederreiter and A. Winterhof, 'Lattice structure and linear complexity of nonlinear pseudorandom numbers', *Appl. Algebra Engrg. Comm. Comput.*, **13** (2002), 319–326.

[105] H. Niederreiter and A. Winterhof, 'Exponential sums for nonlinear recurring sequences', *Finite Fields Appl.*, **14** (2008), 59–64.

[106] H. Niederreiter and A. Winterhof, 'On the structure of inversive pseudorandom number generators', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **4851** (2007), 208–216.

[107] A. Ostafe, 'Multivariate permutation polynomial systems and pseudorandom number generators', *Finite Fields and Their Appl.* (2010), 144–154.

[108] A. Ostafe, 'Pseudorandom vector sequences derived from triangular polynomial systems with constant multipliers', WAIFI 2010, *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, (2010), 62–72.

[109] A. Ostafe, E. Pelican and I. E. Shparlinski, 'On pseudorandom numbers from multivariate polynomial systems', *Finite Fields and Their Appl.* (2010), v.16, 320–328.

[110] A. Ostafe and I. E. Shparlinski, 'On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators', *Math. Comp.*, **79** (2010), 501–511.

[111] A. Ostafe and I. E. Shparlinski, 'Pseudorandom numbers and hash functions from iterations of multivariate polynomials', *Cryptography and Communications*, **2** (2010), 49–67.

[112] A. Ostafe and I. E. Shparlinski, 'On the length of critical orbits of stable quadratic polynomials', *Proc. Amer. Math. Soc.*, **138** (2010), 2653–2656.

[113] A. Ostafe and I. E. Shparlinski, 'Pseudorandomness and dynamics of Fermat quotients', *SIAM J. Discr. Math.* (2011), v. 25, 50–71.

[114] A. Ostafe, I. E. Shparlinski and A. Winterhof, 'On the generalized joint linear complexity profile of a class of nonlinear pseudorandom multisequences', *Adv. Math. Comm.* (2010), v.4, 369–379.

[115] A. Ostafe, I. E. Shparlinski and A. Winterhof, 'Multiplicative character sums of a class of nonlinear recurrence vector sequences', *Intern. J. Number Theory*, (in press).

[116] F. Pappalardi, 'On the order of finitely generated subgroups of $\mathbb{Q}^*$ (mod p) and divisors of $p-1$', *J. Number Theory*, **57** (1996), 207–222.

[117] R. A. Rueppel, 'Stream ciphers', *Contemporary Cryptology*, IEEE, New York, 1992, 65–134.

[118] J. Sauerberg and L. Shu, 'Fermat quotients over function fields', *Finite Fields and Their Appl.*, **3** (1997), 275–286.

[119] W. M. Schmidt, 'A lower bound for the number of solutions of equations over finite fields', *J. Number Theory*, **6** (1974), 448–480.

[120] I. E. Shparlinski, 'On finding primitive roots in finite fields', *Theor. Comp. Sci.*, **157** (1996), 273–275.

[121] I. E. Shparlinski, *Finite fields: Theory and computation*, Kluwer Acad. Publ., Dordrecht, 1999.

[122] I. E. Shparlinski, *Number theoretic methods in cryptography: Complexity lower bounds*, Birkhäuser, Basel, 1999.

[123] I. E. Shparlinski, 'Exponential sums in coding theory, cryptology and algorithms', *Coding Theory and Cryptology*, World Scientific, 2002, 323–383.

[124] I. E. Shparlinski, 'On some dynamical systems in finite fields and residue rings', *Discr. and Cont. Dynam. Syst., Ser.A*, **17** (2007), 901–917.

[125] I. E. Shparlinski, 'Character sums with Fermat quotients', *Preprint*, 2009.

[126] J. H. Silverman, 'Wieferich's criterion and the abc-conjecture', *J. Number Theory*, **30** (1988), 226–237.

[127] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995.

[128] J. H. Silverman, *The arithmetic of dynamical systems*, Springer, New York, 2007.

[129] J. H. Silverman, 'Variation of periods modulo p in arithmetic dynamics', *New York J. Math.*, **14** (2008), 601–616.

[130] I. Solan, 'Some properties of the Euler quotient matrix'. *Integers*, **6** (2006), #A36.

[131] V. G. Sprindžuk, 'Classical Diophantine equations', Springer-Verlag, 1993.

[132] J. Steuding, *Diophantine analysis*, Chapman & Hall/CRC, 2005.

[133] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin, 1993.

[134] Z.-H. Sun, 'Congruences involving Bernoulli and Euler numbers', *J. Number Theory*, **128** (2008), 280–312.

[135] A. Topuzoğlu and A. Winterhof, 'On the linear complexity profile of nonlinear congruential pseudorandom number generators of higher orders', *Appl. Algebra Engrg. Comm. Comput.*, **16** (2005), 219–228.

[136] A. Topuzoğlu and A. Winterhof, 'Pseudorandom sequences', *Topics in Geometry, Coding Theory and Cryptography*, Springer-Verlag, 2006, 135–166.

[137] L. A. Trelina, 'S-integral solutions of Diophantine equations of hyperbolic type', *Dokl. Akad. Nauk BSSR*, **22** (1978), 881–884, (in Russian).

[138] C. F. Woodcock and N. P. Smart, 'p-adic chaos and random number generation', *Experiment. Math.*, **7** (1998), 333–342.

[139] L.-P. Wang and H. Niederreiter, 'Successive minima profile, lattice profile, and joint linear complexity profile of pseudorandom multisequencess', *J. Complexity*, **24** (2008), 144–153.

[140] A. Winterhof, 'Linear complexity and related complexity measures', *Selected Topics in Information and Coding Theory*, World Scientific, Singapore, (2010), 3–40.