Nonlinear congruential pseudorandom number generators

Diplomarbeit
zur Erlangung des Magistergrades
an der Naturwissenschaftlichen Fakultät
der Universität Salzburg

eingereicht von
Andreas Weingartner

Salzburg, im Juni 1994

Contents

Chapter 1

Introduction

This master's thesis is about pseudorandom number generation. It deals with nonlinear methods to generate uniform pseudorandom numbers of high statistical quality. In his well-known monograph, Ripley [28, p.2] writes :

> "The first thing needed for a stochastic simulation is a source of randomness."

Usually, this source of randomness is a pseudorandom number generator, that is, a deterministic algorithm to produce a sequence of numbers with certain statistical properties. Users of pseudorandom numbers (abbreviated prn) should be aware — and sometimes beware — of the generator they apply. This is not always the case:

> "Many users of simulation are content to remain ignorant of how such numbers are produced, merely calling standard functions to produce them. Such attitudes are dangerous, for random numbers are the foundations of our simulation edifice, and problems at higher levels are frequently traced back to faulty foundations." (Ripley [28, p.14].)

The task in uniform prn - generation is to generate a sequence of real numbers that simulates a sequence of independent uniformly distributed random variables in [0,1[. Nonuniform prns are obtained by transforming uniform prns to a given distribution. For this, see the comprehensive monograph of Devroye [5]. We will deal exclusively with uniform prns.

How to generate uniform pseudorandom numbers? A widespread method for generating prns is the linear congruential generator (abbreviated LCG). It is defined by the recursion

$$y_{n+1} \equiv a y_n + b \pmod{M}, \qquad n \geq 0,$$

and the normalization

$$x_n = \frac{y_n}{M},$$

where M is a large positive integer called the modulus and y_0, a and b are well-chosen nonnegative integers less than M. We will denote this generator by LCG$(a, b, M; y_0)$. The LCG was first introduced by D.H.Lehmer in 1951. The most eyecatching deficiency of a sequence $x_0, x_1, x_2, \dots$ of linear congruential prns is the coarse lattice structure of the s-tuples $(x_n, x_{n+1}, \dots, x_{n+s-1})$.

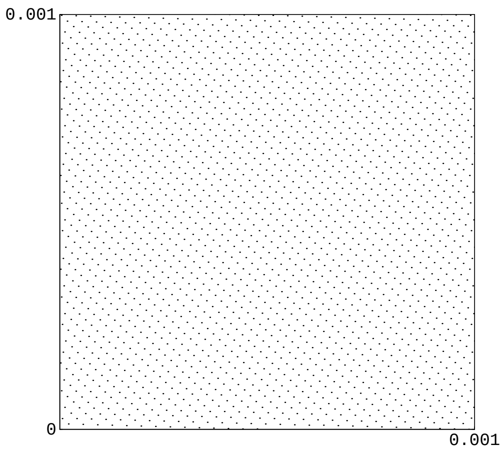

Figure 1

Figure 1 shows the distribution of the points (x_n, x_{n+1}) in the unit square from a sequence $x_0, x_1, x_2, \dots$ generated by a LCG with a=950706376, b=0, M=$2^{31}-1$ and $y_0 = 1$ (see Fishman and Moore [17]). This particular generator has a very good lattice structure in the sense of Beyer quotients.

As Marsaglia pointedly observed, "Random numbers fall mainly in the planes " (see [22]). Figure 2 illustrates this fact. It shows the fifteen planes in $[0,1[^3$, that contain all triples (x_n, x_{n+1}, x_{n+2}) from a sequence of prns generated by the "scientific subroutine RANDU". RANDU , the linear congruential generator LCG(65539, 0, 2^{31}), was proposed by a famous computer-firm.

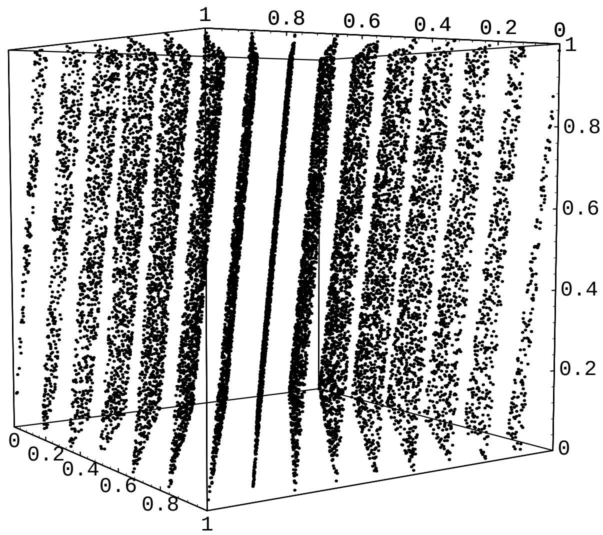

Figure 2: The hyperplane structure of RANDU

These regularities of linear congruential prns, which stem from the linearity of the underlying recursion, led to the development of nonlinear congruential methods.

We will now give an example of such a nonlinear congruential generator (abbreviated NLCG). All NLCGs are defined by congruences of a certain – nonlinear – type. The inversive congruential generator (ICG) with prime modulus was introduced by Eichenauer and Lehn [7] and is defined as follows:

Let M be a large prime and let a and b be well-chosen fixed integers. For $c \in \mathbf{Z}_M = \{0, 1, 2, ..., M-1\}$ we define $\overline{c} \in \mathbf{Z}_M$ as the unique solution modulo M of the congruence $c\overline{c} \equiv 1 \bmod M$ if $c \not\equiv 0 \pmod{M}$ and $\overline{c} := 0$ if $c = 0$. Then the sequence $y_0, y_1, y_2, ...$ is defined by the recursion

$$y_{n+1} \equiv a\overline{y}_n + b \pmod{M}.$$

The initial value y_0 may be chosen arbitrarily in $\mathbf{Z}_M$. A sequence $x_0, x_1, x_2, ...$ of prns in [0,1[is obtained by the normalization $x_n := y_n/M$.

We now look at the structure of overlapping pairs (x_n, x_{n+1}) of a sequence $x_0, x_1, x_2, ...$ of inversive congruential prns: The points in Figure 3 come from an inversive congruential generator with $M = 2^{31} - 1$, $a = 1$, $b = 1$ and $y_0 = 1$.

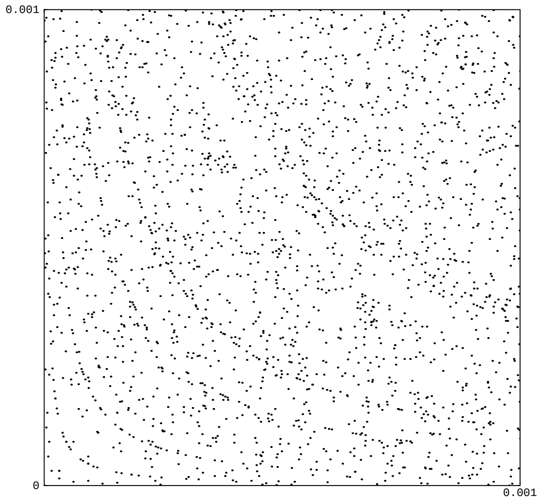

Figure 3: Pairs of inversive congruential numbers

Unlike Figure 1 there is no recognizable line structure in Figure 3. In fact, this property remains valid for higher dimensions: No hyperplane in $[0, 1[^s$ contains more than s of the overlapping s-tuples from a sequence of prns generated by the ICG (not counting points at the boundery of the s-dimensional unit cube), (see [9]). This is best possible since s points define a hyperplane in dimension s.

We see that linear congruential prns and inversive congruential prns behave quite differently under the criterion "number of points lying on a hyperplane in $[0,1[^s$ ". This should illustrate the importance of knowing the properties or defects of the prn generator one uses.

In the remaining part of the introduction we will be concerned mainly with the following questions : What does "high quality" with respect to prns mean and how can we assess the quality of prns? Ripley's definition of prns may be helpful (see [28, p.15]):

> "A sequence of pseudo-random numbers (u_i) is a deterministic sequence of numbers in [0,1[having the same relevant statistical properties as a sequence of random numbers."

Relevant statistical properties of a sequence of independent uniformly distributed random numbers are, first of all, uniformity and independence. If prns $x_0, x_1, \ldots$ should simulate realizations of these random variables, then they will have to fulfill two basic requirements:

1. *Uniformity* : The pseudorandom numbers should be approximately uniformly distributed in [0,1[.
2. *Independence* : Consecutive pseudorandom numbers should be uncorrelated.

Departures from uniformity or independence can be detected by theoretical and empirical tests. Theoretical tests use number-theoretical and algebraic methods to provide once and for all a quality certificate for a whole group of prn generators, whereas empirical tests are applied to a certain given sequence of prns.

It is the aim of this thesis to show how nonlinear congruential numbers behave under important theoretical tests. Further we will provide the mathematical background that is necessary to proof selected important results.

In the following we will give a sketch of several criteria to asses the quality of pseudorandom numbers. First of all we will consider *uniformity*: Let $x_0, x_1, \ldots, x_{N-1}$ be a sequence of prns in [0,1[. How can we measure the uniformity of these numbers? One possibility is to compare the empirical distribution function

$$F_N(x) = \frac{\#\{n, \quad 0 \le n < N : \quad x_n \le x\}}{N}$$

with the distribution function of the uniform distribution $U[0,1[$, which is

$$F(x) = \begin{cases} 0 & \text{for } x < 0 \\ x & \text{for } 0 \le x \le 1 \\ 1 & \text{for } x > 1 \end{cases} .$$

This is the idea behind the Kolmogorov-Smirnov (KS) test. The two-sided KS test works as follows: We form the test statistics

$$D_N^* := \sup_{x \in [0,1[} |F_N(x) - x|,$$

which measures the maximal distance between the empirical distribution function of $x_0, x_1, \ldots, x_{N-1}$ and the distribution function of $U[0,1[$. The distribution of the quantity D_N^* is known (see, for example, [4]). According to these tables we accept or reject the null hypothesis, which says: "$x_0, x_1, \ldots, x_{N-1}$ are independent realizations of a uniformly distributed random quantity X."

The numerical quantity D_N^* plays an important role in the theory of prns. In metric number theory, it is called the *star discrepancy* of the points $x_0, x_1, \ldots, x_{N-1}$. A closely related quantity is the *extreme discrepancy*, which is defined by

$$D_N := \sup_{[a,b[\subseteq[0,1[} \left| \frac{\#\{n, \ 0 \le n \le N-1 : \quad x_n \in [a,b[\ \}}{N} - (b-a) \right| .$$

The star discrepancy and the extreme dicrepancy satisfy the inequality $D_N^* \leq D_N \leq 2D_N^*$ for any sequence $x_0, x_1, \ldots, x_{N-1}$ in [0,1[. Niederreiter [26] writes:

> "The discrepancy can be viewed as a quantitative measure for the deviation from uniform distribution."

The evaluation of upper bounds for the discrepancy of nonlinear congruential prns will be a major concern of this thesis.

The second fundamental statistical property of pseudorandom numbers is *independence*. Before we introduce a measure for the independence of prns we will look at real random numbers. We know that s random variables $X_1, X_2, \ldots, X_s$ are independent if and only if the distribution function of the s-dimensional random variable
$(X_1, X_2, \ldots, X_s)$ is the product of the s distribution functions of the X_i. In particular, this means that, if $X_1, X_2, \ldots, X_s$ are uniformly distributed in [0,1[, $X_1, X_2, \ldots, X_s$ are independent if and only if $(X_1, X_2, \ldots, X_s)$ is uniformly distributed in $[0,1[^s$.

This fact enables us to test the independence of prns as follows: From our sequence $x_0, x_1, \ldots, x_{N-1}$ of prns in [0,1[we derive a sequence $\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \ldots$ of points (vectors) in $[0,1[^s$ by putting

- $\mathbf{x}_n := (x_n, x_{n+1}, \ldots, x_{n+s-1})$ ("overlapping s-tuples"), or
- $\mathbf{x}_n := (x_{ns}, x_{ns+1}, \ldots, x_{ns+s-1})$ ("nonoverlapping s-tuples"), or
- $\mathbf{x}_n := (x_{n+k_0}, x_{n+k_1}, \ldots, x_{n+k_{s-1}})$ with $0 = k_0 < k_1 < \ldots < k_{s-1}$ fixed integers.

There is no strict rule of how to construct those s-tuples, although some theoretical results can only be proved for overlapping s-tuples. If the prns $x_0, x_1, x_2, \ldots$ are independent from each other, then the points $\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \ldots$ should be approximately uniformly distributed in $[0,1[^s$. Again we can use the s-dimensional two-sided KS-test statistics $D_N^{*(s)}$ to decide whether the sequence $\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \ldots$ "fits" the uniform distribution in $[0,1[^s$ or not. However, in most cases, the computational complexity for the test statistics $D_N^{*(s)}$ is too large for practical calculations. Therefore theoretical analysis of the generator is necessary to provide bounds for the s-dimensional discrepancy $D_N^{*(s)}$, resp. $D_N^{(s)}$.

Beside discrepancy there exist other important criteria for the independence of prns. One of them is the *hyperplane structure* of s-tuples taken from a sequence $x_0, x_1, \ldots$ of prns. The investigation of the hyperplane structure can detect undesirable regularities, as has been illustrated in Figure 1 and Figure 2. A sequence of numbers in [0,1[, with all overlapping triples falling into only fifteen planes in $[0,1[^3$ cannot be regarded as a realization of independent, identically $U[0,1[$-distributed random variables (see Figure 2). We have observed in Figure 3 that inversive congruential prns show no hyperplane structure, in strong contrast to linear congruential prns for dimension $s = 2$. This result and the proof of it, which does not require any special knowledge of number-theory or algebra, are part of this thesis (see Theorem 2.6).

Another interesting test where linear congruential prns fail is the *lattice test*, which measures the linear independence of overlapping s-tuples. More precisely: a sequence $x_0, x_1, \ldots$ of prns passes the s-dimensional lattice test if s of the vectors $\quad (y_n, y_{n+1}, \ldots, y_{n+s-1}) - (y_0, y_1, \ldots, y_{s-1})\,, \qquad n \geq 1,$ are linearly independent over F_p. We will see that an ICG with prime modulus M passes the s-dimensional lattice test for all $s \leq (M+1)/2$, whereas a LCG with prime modulus passes this test only for dimension $s = 1$. This is another weakness of linear congruential prns with regard to lattice structure.

Nevertheless, the requirements for prns vary with the individual applications. Therefore we will not distinguish between "good" and "bad" prns, but between prns that do have a certain property and others, that do not. Whether a certain property is considered as relevant or decisive for the simulation problem is up to the user of prns.

Chapter 2

Results

In this thesis, we present results for four types of nonlinear pseudorandom number generators:

1. the general class of (first order) nonlinear congruential generators (abbreviated NLCG)
2. as an important subclass, the inversive congruential generator (ICG)
3. as a further subclass of NLCG, the quadratic congruential generator (QCG)
4. the explicit inversive congruential generator (EICG).

The proofs of most of the results for NLCGs and ICGs will be given in Chapter 4; the necessary mathematical "tools" like linear recurring sequences, permutation polynomials and bounds for exponential sums are part of Chapter 3.

2.1 General nonlinear congruential generators with prime modulus

In order to understand the results we need to know exactly what is meant by a nonlinear congruential generator, abbreviated NLCG: Let $M = p$ be a prime modulus. The sequence $y_0, y_1, y_2, \ldots$ of integers in the finite field $F_p = \mathbf{Z}_p$ is generated by the first order recursion

$$y_{n+1} \equiv f(y_n) \pmod{p} \qquad \text{for } n \geq 0 \ ,$$

where f is an integer valued nonlinear function on F_p. Since the recursion is of first order, the sequence is periodic and $per(y_n) \leq p$. Now let f be such that the sequence $y_0, y_1, \ldots$ is purely periodic with least period length p. Then the map $n \in F_p \mapsto y_n \in F_p$, like any selfmap of a finite field can be represented by a uniquely determined polynomial $g \in F_p[x]$ with $d := deg(g) < p$ (see Chapter 3, Lemma 3.11). Therefore we can write

$$y_n = g(n) \in F_p \qquad \text{for } n = 0, 1, \ldots \ ,$$

where n is also viewed as an element of F_p. We derive the corresponding prns in [0,1[by the normalization $x_n := y_n/p$ for $n = 0, 1, \ldots$. This type of prns was first proposed by Eichenauer, Grothe, and Lehn [6]. The value of $d := deg(g)$ will play a central role in the following results.

2.1.1 Lattice test

The following definition follows [26] and makes sense for any congruential generator with prime modulus.

Definition 2.1 *For a given $s \geq 1$, a congruential generator $y_0, y_1, \ldots$ with modulus $M = p$ prime passes the s-dimensional lattice test if the vectors $\mathbf{y}_n - \mathbf{y}_0$, $n = 1, 2, \ldots$, span F_p^s, where*

$$\mathbf{y}_n := (y_n, y_{n+1}, \ldots, y_{n+s-1}) \in F_p^s \qquad \textit{for } \ n = 0, 1, \ldots .$$

As we have mentioned in the introduction, a linear congruential generator with prime modulus passes the lattice test only for dimension $s = 1$ (see [26, p.178]). For nonlinear congruential generators the value of $d := deg(g)$, g being the polynomial introduced above, is decisive. The following theorem was shown by Eichenauer, Grothe and Lehn [6].

Theorem 2.1 *A nonlinear congruential generator with prime modulus passes the s-dimensional lattice test if and only if $s \le d = deg(g)$.*

The proof, which follows Niederreiter [26], can be found in Chapter 4. We will make some remarks about the value of d:

- $d = 1$ is impossible for a NLCG: The congruence $y_n \equiv an + b \pmod p$ leads to the recursion $y_{n+1} \equiv y_n + a \pmod p$, which is a linear congruential generator with multiplier 1 (a bad choice).
- we will obtain from Corollary 3.10 that the degree of a permutation polynomial over F_p does not divide $p - 1$. Since we consider only NLCGs with maximal period length p, $g(n)$ is a permutation polynomial. Therefore we have $3 \le d = deg(g) \le p - 2$.

This means that any nonlinear congruential generator with prime modulus and maximal period length p passes the s-dimensional lattice test at least for $s = 1, 2, 3$.

2.1.2 Uniformity and independence

The one-dimensional respectively the s-dimensional discrepancy allow us to measure how well a given sequence of prns fulfills the two basic requirements for prns, uniformity and independence. Beside discrepancy, there exist other measures for the uniformity of prns. We will restrict our attention to the (extreme) discrepancy, since it is the most important measure in connection with prns.

Definition 2.2 *The $s-$dimensional (extreme) discrepancy of a set $\mathcal{P} = (\mathbf{x}_n)_{n=0}^{N-1}$ in $[0,1[^s$ is defined by*

$$D_N^{(s)}(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}) := \sup_{J \in \mathcal{J}} \left| \frac{A(J, \mathcal{P})}{N} - \lambda_s(J) \right|,$$

where $\mathcal{J}$ is the class of all subintervals J of $[0,1[^s$ of the form $J = \prod_{i=1}^{s} [u_i, v_i[$, $0 \le u_i < v_i \le 1$, and $A(J, \mathcal{P})$ denotes the cardinality of $\mathcal{P} \cap J$.

For a first order congruential generator with modulus M and maximal period length M we clearly have

$$\{x_0, x_1, \ldots, x_{M-1}\} = \left\{0, \frac{1}{M}, \frac{2}{M}, \ldots, \frac{M-1}{M}\right\}.$$

A result of Niederreiter [26, p.16] yields $D_M(0, \frac{1}{M}, \frac{2}{M}, \ldots, \frac{M-1}{M}) = \frac{1}{M}$, therefore we have

Theorem 2.2 *For any first order congruential generator with modulus M and $per(x_n)$=M we have $D_M(x_0, x_1, \ldots, x_{M-1}) = 1/M$.*

Next we will provide upper bounds for the s-dimensional discrepancy ($s \ge 2$) of overlapping s-tuples $\mathbf{x}_n := (x_n, x_{n+1}, \ldots, x_{n+s-1})$ of nonlinear congruential prns with prime modulus. The following result from Eichenauer-Herrmann and Niederreiter [15] is only usefull if the number $d = deg(g)$ is known. The reader should note that it has been possible to obtain discrepancy estimates even for parts of the period. For special types of NLCGs, this result can be improved considerably, see [10], [25], [16].

Theorem 2.3 *For a sequence of nonlinear congruential prns $x_0, x_1, \ldots$ with prime modulus p we have*

(1) $D_p^{(s)}(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{p-1}) \leq 1 - \left(1 - \frac{1}{p}\right)^s + (d-1)p^{-1/2}\left(\frac{4}{\pi^2}\log p + 1.72\right)^s$

for $2 \leq s \leq d$,

(2) $D_N^{(s)}(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1}) \leq 1 - \left(1 - \frac{1}{p}\right)^s + (d-1)\frac{p^{1/2}}{N}\left(\frac{4}{\pi^2}\log p + 1.72\right)^{s+1}$

for $2 \leq s \leq d-1$, $1 \leq N < p$,

where $\mathbf{x}_n = (x_n, x_{n+1}, \ldots, x_{n+s-1})$.

The proof of Theorem 2.3 can be found in Chapter 4 of this thesis. Again, we see that the degree d of the polynomial g plays an important role. If d is of magnitude $p^{1/2}$ or larger, the bounds become useless, since we always have $0 \leq D_N^{(s)} \leq 1$. The inequality in Theorem 2.3(2), which gives a bound for the s-dimensional discrepancy for parts of the period p, is only useful if N, the number of points, is of higher order of magnitude than $p^{1/2}(d-1)$.

Due to Eichenauer-Herrmann [10], the upper bound in Theorem 2.3 (2) is, in case $s = 1$, in general best possible up to the logarithmic factor.

We will now consider two special cases of nonlinear congruential generators, namely the inversive congruential generator and the quadradic congruential generator.

2.2 Inversive congruential generators with prime modulus

The inversive congruential generator (abbreviated ICG) was first proposed by Eichenauer and Lehn [7]. An ICG is defined by the recursion

$$y_{n+1} \equiv a\overline{y}_n + b \pmod{p} \qquad \text{for } n = 0, 1, \dots ,$$

where a, b and y_0 are well chosen integers in F_p. For $c \in F_p$, $\overline{c}$ is defined as the unique solution modulo p of the congruence $c\overline{c} \equiv 1 \bmod p$ if $c \neq 0$, and $\overline{c} := 0$ if $c = 0$. Clearly $\overline{c} \equiv c^{p-2} \bmod p$ for $p \geq 3$. A sequence of prns $x_0, x_1, \dots$ in [0,1[is obtained by the normalization $x_n := y_n/p$.

2.2.1 Period length

The parameters a and b should be chosen in such a way that the least period length of the sequence $x_0, x_1, \dots$ is as large as possible. Since an ICG is defined by a first order recursion, the maximal value for the least period length is equal to the modulus p. The following theorem, which was shown J.Eichenauer and J.Lehn [7], yields a sufficient condition for maximal period length p.

Theorem 2.4 *If $a, b \in F_p$ are such that the polynomial $x^2 - bx - a$ is primitive over F_p, then the sequence $x_0, x_1, \dots$ of inversive congruential prns with modulus p satisfies $per(x_n) = p$.*

A monic irreducible polynomial over F_p of degree 2 is called a *primitive polynomial* over F_p, if it has a root in F_{p^2} that generates the cyclic group $F^*_{p^2}$. Parameters $a, b \in F_p$, such that $x^2 - bx - a$ is primitive over F_p, are tabulated in Grothe [18] for some large primes such as $p = 2^{31} - 1$.

The condition, that $x^2 - bx - a$ is a primitive polynomial over F_p, is *$sufficient$* but *not necessary* for maximal period length p. A polynomial x^2-

$bx - a$ is called an inversive maximal period polynomial ("IMP-polynomial"), if the corresponding ICG with parameters a and b yields a sequence with maximal period p. An algorithm to find all IMP-polynomials over a given field F_p was given in the paper of Wun-Seng Chou [2].

2.2.2 Lattice test

The following theorem is due to Niederreiter [24].

Theorem 2.5 *An inversive congruential generator with prime modulus p and maximal period length passes the s-dimensional lattice test for all $s \leq (p+1)/2$.*

The proof is based on the corresponding result for the general nonlinear congruential generator and can be found in Chapter 4 of this thesis. As we have pointed out before, the lattice structure of LCGs is completely different. LCGs fail this test for all dimensions $s \geq 2$.

2.2.3 Hyperplane structure

The following strong nonlinearity property of inversive prns was shown by Eichenauer-Hermann [9]. It stands in sharp contrast to the lattice structure of linear congruential prns (see the introduction).

Theorem 2.6 *Let $s \geq 2$. For every inversive congruential generator*

$$y_{n+1} \equiv a\overline{y}_n + b \bmod p$$

with prime modulus p and maximal period length p any hyperplane in F_p^s contains at most s of the points $\mathbf{y_n} = (y_n, y_{n+1}, \ldots, y_{n+s-1})$ with $0 \leq n \leq p-1$ and $y_n \cdots y_{n+s-2} \neq 0$.

Note that the condition $y_n \cdots y_{n+s-2} \neq 0$ eliminates exactly $s-1$ of the points $\mathbf{y}_n$ with $0 \leq n \leq p-1$ (these are the points on the boundary of $[0,1[^s)$. The remaining $p-s+1$ points "avoid" planes. The proof of this result is contained in Chapter 4.

It is well-known that pseudo-random points from an LCG "fall mainly in the planes", as Marsaglia [22] has pointed out. For references on the hyperplane structure of LCGs, see Ripley [27, 28] and Afflerbach and Grothe [1].

2.2.4 Independence

The discrepancy bound for the general class of nonlinear congruential generators does not provide a bound for the discrepancy of inversive congruential prns, since we have $d = deg(g) \geq (p+1)/2$ in case of the ICG (see the proof of Theorem 2.5). The following upper and lower bounds for the discrepancy of inversive congruential prns are due to Niederreiter [26, Theorem 8.7 and Theorem 8.8].

Theorem 2.7 *For inversive congruential prns $x_0, x_1, \ldots$ with prime modulus and maximal period length we have*

$$D_p^{(s)}(\mathbf{x_0}, \mathbf{x}_1, \ldots, \mathbf{x}_{p-1}) \leq 1 - \left(1 - \frac{1}{p}\right)^s + \left(\frac{2s-2}{p^{1/2}} + \frac{s-1}{p}\right)\left(\frac{4}{\pi^2}\log p + 1.72\right)^s$$

for $s \geq 2$, where $\mathbf{x}_n := (x_n, x_{n+1}, \ldots, x_{n+s-1})$, $n \geq 0$.

This inequality gives a bound of the discrepancy of the points $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{p-1}$. For the discrepancy of parts of the period, that is $D_N^{(s)}(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1})$ with $N < p$, there are no theoretical results available.

The next theorem shows that the order of magnitude of the bound in Theorem 2.7, $p^{-1/2}(\log p)^s$, is, in general, best possible up to the logarithmic factor. From Lidl and Niederreiter [21] we infer that the total number of primitive polynomials $x^2 - bx - a$ over F_p is $(\varphi(p^2-1))/2$, where φ is Euler's totient function.

Theorem 2.8 *Let $p \geq 5$ be a prime and let $0 < t < 1$. Then there are more than $A_p(t)\varphi(p^2-1)/2$ primitive polynomials $x^2 - bx - a$ over F_p such that, for the corresponding inversive congruential prns with modulus p, we have*

$$D_p^{(s)}(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{p-1}) > \frac{t}{2\pi + 4} p^{-1/2} \qquad \textit{for all } s \geq 2,$$

where the numbers $A_p(t)$ satisfy

$$\lim_{p \to \infty} A_p(t) = \frac{1-t^2}{4-t^2} > 0 \qquad \textit{for all } t.$$

2.3 Generalized inversive congruential generators

The following definition and the subsequent results for the generalized version of the inversive congruential generator are due to Eichenauer-Hermann [12]. Let $M = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ be the modulus with arbitrary distinct primes $p_1, p_2, \ldots, p_r \geq 3$. For integers $a, b \in \mathbf{Z}_M$ with $\gcd(a, M) = 1$ a *generalized inversive congruential sequence* $(y_n)_{n\geq 0}$ of elements of $\mathbf{Z}_M$ is defined by

$$y_{n+1} \equiv a y_n^{\varphi(M)-1} + b \pmod{M}, \quad n \geq 0,$$

where $\varphi(M) = (p_1 - 1) \cdot \ldots \cdot (p_r - 1)$ denotes the number of positive integers less than M which are relatively prime to M. A sequence of generalized inversive congruential prns is obtained by $x_n = y_n / M$ for $n \geq 0$.

The subsequent result shows that these sequences are closely related to (ordinary) inversive congruential sequences.
For $1 \leq i \leq r$ let $M_i = M/p_i$, and $a_i, b_i \in \mathbf{Z}_{p_i}$ be integers with

$$a \equiv M_i^2 a_i \pmod{p_i}$$

and

$$b \equiv M_i b_i \pmod{p_i}.$$

Let $(y_n^{(i)})_{n\geq 0}$ be a sequence of elements in $\mathbf{Z}_{p_i}$ given by

$$y_{n+1}^{(i)} \equiv a_i (y_n^{(i)})^{p_i - 2} + b_i \pmod{M_i}, \quad n \geq 0,$$

where $y_0 \equiv M_i y_0^{(i)} \pmod{p_i}$ is assumed. Note that $z^{p_i - 1} \equiv 1 \pmod{p_i}$ for any integer $z \in \mathbf{Z}_{p_i}^* = \mathbf{Z}_{p_i} \setminus \{0\}$ according to Fermat's Theorem. Hence $(y_n^{(i)})_{n\geq 0}$ is an (ordinary) inversive congruential sequence with prime modulus. A sequence $(x_n^{(i)})_{n\geq 0}$ in [0,1[is obtained by $x_n^{(i)} = y_n^{(i)} / p_i$ for $n \geq 0$.

Theorem 2.9 *Let* $(y_n^{(i)})_{n\geq 0}$ *and* $(x_n^{(i)})_{n\geq 0}$ *for* $1 \leq i \leq r$ *be defined as above. Then*

$$y_n \equiv M_1 y_n^{(1)} + \ldots + M_r y_n^{(r)} \pmod{M}$$

and

$$x_n \equiv x_n^{(1)} + \ldots + x_n^{(r)} \pmod{1}$$

for $n \geq 0$.

As for an implementation of generalized inversive congruential generators, integer computations have to be performed only in $\mathbf{Z}_{p_1}, \ldots, \mathbf{Z}_{p_r}$, but not in $\mathbf{Z}_M$. This is a definite advantage in comparison to the ICG with prime modulus. With $x^2 - b_i x - a_i$ being a primitive polynomial over F_{p_i} for $1 \leq i \leq r$, the sequences $(y_n^{(i)})_{n\geq 0}$ are periodic with period p_i (see Theorem 2.4); since $p_1, p_2, \ldots, p_r$ are distinct primes, we obtain $per(y_n) = M$.

2.3.1 Independence

Suppose that the generalized inversive congruential sequence $(y_n)_{n\geq 0}$ is purely periodic with maximal period length $M = p_1 \cdot \ldots \cdot p_r$. In the following two theorems upper and lower bounds for the s-dimensional discrepancy of overlapping s-tuples of generalized inversive congruential prns are established. Their proofs are given in [12].

Theorem 2.10 *Let* $s \geq 2$ *and* $\mathbf{x}_n = (x_n, x_{n+1}, \ldots, x_{n+s-1})$ *for* $n \geq 0$. *Then the discrepancy* $D_M^{(s)}$ *satisfies*

$$D_M^{(s)}(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{M-1}) < M^{-1/2}\left(\frac{2}{\pi}\log M + \frac{7}{5}\right)^s \prod_{i=1}^{r}\left(2s - 2 + s p_i^{-1/2}\right) + sM^{-1}$$

for any generalized inversive congruential generator with maximal period length M.

Theorem 2.11 *Let* $\mathbf{x}_n = (x_n, x_{n+1}, \ldots, x_{n+s-1})$ *for* $n \geq 0$. *Then there exist generalized inversive congruential generators with*

$$D_M^{(s)}(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{M-1}) \geq \frac{1}{2(\pi+2)} M^{-1/2} \prod_{i=1}^{r} \left(\frac{p_i - 3}{p_i - 1} \right)^{1/2}$$

for all dimensions $s \geq 2$.

2.4 Quadratic congruential generators

The quadratic congruential generator with modulus M was proposed by Knuth [20]. For integers $a, b, c, y_0 \in \{0, 1, \ldots, M-1\}$ with $a \neq 0$ a quadratic congruential sequence $y_0, y_1, \ldots$ is defined by the recursion

$$y_{n+1} \equiv a y_n^2 + b y_n + c \pmod{M}, \quad n \geq 0.$$

We will denote this generator by $QCG(a, b, c, M; y_0)$. A sequence of prns $x_0, x_1, \ldots$ is obtained by the normalization $x_n := y_n/M$.

2.4.1 Period length

For the following result, see Knuth [20].

Theorem 2.12 *A sequence of quadratic congruential prns has period length M if and only if the following conditions are satisfied:*

1. *c is relatively prime to M;*
2. *a and $b-1$ are both multiples of p for all odd primes p dividing M;*
3. *a is even and $a \equiv b - 1 \bmod 4$, if M is a multiple of 4,*
   $a \equiv b - 1 \bmod 2$, if M is a multiple of 2;
4. *either $a \equiv 0$ or $ca \equiv 6 \bmod 9$, if M is a multiple of 9.*

Corollary 2.13 *A quadratic congruential generator with modulus $M = 2^\alpha$, $\alpha \geq 2$, yields a sequence with maximal period length M if and only if*

1. *a is even,*
2. *$b \equiv a + 1 \pmod 4$,*
3. *c is odd.*

2.4.2 Lattice structure

Eichenauer and Lehn [8] analyzed the lattice structure of quadratic congruential prns with arbitrary modulus and maximal period length. We will only give a sketch of the result for the special case $M = 2^\alpha$, following Niederreiter [26].

Theorem 2.14 *Let $x_0, x_1, \ldots$ be a sequence of quadratic congruential prns with maximal period length M. For a given dimension $s \geq 2$, the set of all nonoverlapping s-tuples $\mathbf{x}_{ns} = (x_{ns}, x_{ns+1}, \ldots, x_{ns+s-1}) \in [0,1[^s$, $n = 0, 1, \ldots, M-1$, is the same as the intersection of $[0,1[^s$ with a union of $2^{\omega-\eta}$ grids with explicity known shift vectors and lattice bases.*
Here η and ω are determined by $gcd(s, M) = 2^\eta$, $gcd(a, M) = 2^\beta$, and $\omega = \max([(\alpha - \beta + 1)/2], \eta)$.

2.4.3 Independence

Eichenauer-Herrmann and Niederreiter [14] studied the performance of quadratic congruential prns with modulus $M = p^m$, p a prime, under the 2-dimensional serial test.
Let $x_0, x_1, \ldots$ be the full period of a sequence of quadratic congruential prns with maximal period $M = p^m$. The following two theorems yield upper and lower bounds for the two-dimensional extreme discrepancy of overlapping tuples $\mathbf{x}_n := (x_n, x_{n+1})$. Both results are due to Eichenauer-Herrmann and Niederreiter [14].

Theorem 2.15 *The discrepancy of pairs of consecutive prns obtained by a QCG with maximal period length satisfies*

$$D_{p^m}^{(2)}(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{p^m-1}) < 2p^{-m} + p^{-(m-\alpha-\tau)/2}\left(1 - p^{-3/2}\right)\left(\frac{2}{\pi}\log p^m + \frac{2}{5}\right)^2,$$

where α *and* τ *are defined by*

$$gcd(a, p^m) = p^\alpha, \quad \tau = \begin{cases} 1 & for\ p = 2 \\ 0 & for\ p > 2 \end{cases}$$

and $\mathbf{x}_n := (x_n, x_{n+1})$.

This upper bound depends only on the choice of a, not on b and c. The following theorem shows that the upper bound is, in general, best possible up to logarithmic factors.

Theorem 2.16 *Suppose that* $\alpha \leq m - 1 - \tau$ *and* $b \equiv 1 \bmod p^{\alpha+\tau}$. *Then the discrepancy of pairs of consecutive prns obtained by any corresponding quadratic congruential generator with maximal period length satisfies*

$$D_{p^m}^{(2)}(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{p^m-1}) \geq \frac{1}{2(\pi+2)}p^{-(m-\alpha-\tau)/2}.$$

2.5 Explicit inversive congruential generators with prime modulus

The explicit inversive congruential method was introduced by Eichenauer-Herrmann [13]. Here we choose $a, b \in F_p$ with $a \neq 0$ and explicitly define

$$y_n = \overline{an + b} \quad \text{for } n = 0, 1, \ldots,$$

where $\overline{z} \equiv z^{p-2} \bmod p$, $z \in F_p$, p prime. Note that $\overline{z}$ is the multiplicative inverse of z in F_p if $z \neq 0$, $p \geq 3$. Pseudorandom numbers in [0,1[are derived by putting $x_n = y_n/p$ for $n = 0, 1, \ldots$. It is obvious that the sequence $x_0, x_1, \ldots$ is purely periodic with $per(x_n) = p$, i.e., $\{y_0, y_1, \ldots, y_{p-1}\} = \mathbf{Z}_p$, which guarantees that the one-dimensional distribution of the corresponding prns is as good as possible.

2.5.1 Lattice test

From the definition of explicit inversive congruential prns we have

$$y_n = (an + b)^{p-2} \quad \text{for } n = 0, 1, \ldots.$$

Thus we can apply Theorem 2.1 to obtain the following result.

Theorem 2.17 *A sequence $y_0, y_1, \ldots$ generated by the explicit inversive congruential method passes the s-dimensional lattice test for all $s \leq p - 2$.*

2.5.2 Hyperplane structure

The following strong nonlinearity property of explicit inversive congruential prns, which was proved by Niederreiter [25], is similar to the corresponding result for inversive congruential prns (see Theorem 2.6).
For $a_1, \ldots, a_s, b_1, \ldots, b_s \in F_p$ with $a_i \neq 0$ for $i = 1, 2, \ldots, s$ we put

$$y_n^{(i)} = \overline{a_i n + b_i} \quad \text{for } i = 1, 2, \ldots, s \text{ and } n = 0, 1, \ldots, \tag{2.1}$$

and we define

$$\mathbf{z}_n = \left(y_n^{(1)}, \dots, y_n^{(s)}\right) \in F_p^s \quad \text{for } n = 0, 1, \dots.$$

Theorem 2.18 *If $b_1\overline{a}_1, \dots, b_s\overline{a}_s \in F_p$ are distinct, then every hyperplane in F_p^s contains at most s of the points $\mathbf{z}_n = \left(y_n^{(1)}, \dots, y_n^{(s)}\right)$, $n = 0, 1, \dots, p-1$, with $y_n^{(1)} \cdots y_n^{(s)} \neq 0$. If the hyperplane passes through the origin of F_p^s, then it contains at most $s-1$ of these points $\mathbf{z}_n$.*

Note that the condition $y_n^{(1)} \cdots y_n^{(s)} \neq 0$ eliminates exactly s values of n, namely $n = -b_1\overline{a}_1, \dots, -b_s\overline{a}_s \in F_p$. The result is optimal in the sense that there do exist hyperplanes in F_p^s through any s given points.

2.5.3 Independence

Let $y_n^{(i)}$ be as in (2.1) and put $x_n^{(i)} := y_n^{(i)}/p$ for $1 \leq i \leq s$ and $n \geq 0$. For $1 \leq N \leq p$ let $D_N^{(s)}$ be the discrepancy of the points

$$p^{-1}\mathbf{z}_n = \left(x_n^{(1)}, \dots, x_n^{(s)}\right) \in [0,1[^s,\ 0 \leq n \leq N-1.$$

The following two upper discrepancy bounds for the full period and for parts of the period are due to Niederreiter [25]. Theorem 2.19 generalizes a result from Eichenauer-Herrmann [13], if we put $a_i := a \neq 0$ and $b_i := an_i + b$.

Theorem 2.19 *If $b_1\overline{a}_1, \dots, b_s\overline{a}_s \in F_p$ are distinct and $2 \leq s < p$, then for $p \geq 5$ we have*

$$D_p^{(s)} \leq 1 - \left(1 - \frac{1}{p}\right)^s + \left(\frac{2s-2}{p^{1/2}} + \frac{s+1}{p}\right)\left(\frac{4}{\pi^2}\log p + 1.38 + \frac{0.64}{p}\right)^s.$$

Theorem 2.20 *If $b_1\overline{a}_1, \ldots, b_s\overline{a}_s \in F_p$ are distinct and $1 \le s < p$, then for $p \ge 5$ and $1 \le N < p$ we have*

$$\begin{aligned} D_N^{(s)} &< 1 - \left(1 - \frac{1}{p}\right)^s \\ &\quad + \left(\frac{2s-2}{p^{1/2}} + \frac{s+1}{p} + \frac{s}{N}(2p^{1/2}+1)(\frac{4}{\pi^2}\log p + 0.38 + \frac{0.64}{p})\right) \cdot \\ &\quad \cdot \left(\frac{4}{\pi^2}\log p + 1.38 + \frac{0.64}{p}\right)^s . \end{aligned}$$

Eichenauer-Herrmann and Niederreiter [16] showed that the upper bounds in Theorems 2.19 and 2.20 are, in general, best possible up to logarithmic factors.

2.6 Compound explicit inversive congruential generators

For the ordinary explicit inversive congruential generator a large prime modulus p has to be chosen, which makes it necessary to perform exact integer computations in F_p. The following compound explicit inversive congruential generator overcomes this practical disadvantage.
The following definition and the subsequent results are from Eichenauer-Herrmann [11].

Let $p_1, p_2, \dots, p_r \geq 5$ be distinct primes. For $1 \leq i \leq r$ let $a_i \in F_p^*$ and $b_i \in F_p$ be integers, and define

$$y_n^{(i)} \equiv \overline{a_i n + b_i} \pmod{p_i}, \quad n \geq 0.$$

Let $M = p_1 \cdot p_2 \cdot \dots \cdot p_r$ and $M_i = M/p_i$ for $1 \leq i \leq r$. The compound explicit inversive congruential sequence $(y_n)_{n \geq 0}$ of elements of $\mathbf{Z}_M$ is defined by

$$y_n \equiv M_1 y_n^{(1)} + \ldots + M_r y_n^{(r)} \pmod{M}, \quad n \geq 0.$$

Since the sequences $(y_n^{(i)})_{n \geq 0}$ are periodic with period p_i for $1 \leq i \leq r$, the compound explicit inversive congruential sequence $(y_n)_{n \geq 0}$ is periodic with least period M. With $x_n = y_n / M$ we have

$$x_n \equiv y_n^{(1)}/p_1 + \ldots + y_n^{(r)}/p_r \pmod{1}, \quad n \geq 0.$$

For $2 \leq s \leq \min\{p_1, \dots, p_r\}$ let $n_1, n_2, \dots, n_s$ be arbitrary integers with $0 = n_1 < n_2 < \ldots < n_s < \min\{p_1, \dots, p_r\}$ and consider the s-tuples

$$\mathbf{x}_n := (x_{n+n_1}, x_{n+n_2}, \dots, x_{n+n_s}) \in [0,1[^s, \quad n \geq 0,$$

of compound explicit inversive congruential prns.

Theorem 2.21 *Let $2 \leq s \leq \min\{p_1, \ldots, p_r\}$. Then the discrepancy $D_M^{(s)}$ satisfies*

$$D_M^{(s)}(\mathbf{x}_0, \ldots, \mathbf{x}_{M-1}) < M^{-1/2}\left(\frac{2}{\pi}\log M + \frac{7}{5}\right)^s \prod_{i=1}^{r}\left(2s - 2 + (s+2)p_i^{-1/2}\right) + sM^{-1}$$

for any compound explicit inversive congruential generator.

Theorem 2.22 *Let n_2 be fixed and $0 < t \leq 1$. Then there exist more than $A(t)\prod_{i=1}^{r}(p_i - 1)$ values of $(a_1, \ldots, a_r) \in F_{p_1}^* \times \cdots \times F_{p_r}^*$ such that the discrepancy $D_M^{(s)}$ of any corresponding compound explicit inversive congruential generator satisfies*

$$D_M^{(s)}(\mathbf{x}_0, \ldots, \mathbf{x}_{M-1}) \geq \frac{t}{2(\pi + 2)} M^{-1/2}$$

for all dimensions $s \geq 2$, where

$$A(t) = \frac{1 - t^2}{\prod_{i=1}^{r}\left(2 + 3p_i^{-1/2}\right)^2 - t^2}.$$

Chapter 3

Methods

3.1 Linear recurring sequences and the minimal polynomial

Linear recurring sequences play an important role in the theory of pseudo random number generation. A well-known example is the linear congruential generator ("LCG"), where the underlying congruence is of the form

$$s_{n+1} = as_n + b \qquad a, b \neq 0$$

in the ring $\mathbf{Z}_M$. This is an inhomogeneous linear recurrence relation of first order. Every inhomogeneous linear recurrence relation can be replaced by a homogeneous recurrence of higher order with suitable initial values. In case of the LCG we have

$$s_{n+2} = as_{n+1} + b,$$

therefore

$$s_{n+2} - s_{n+1} = as_{n+1} - as_n \ ,$$

which is equivalent to

$$s_{n+2} = (a+1)s_{n+1} - as_n.$$

This is a homogeneous second order linear recurrence relation. With given initial values s_0, s_1 both recursions, the homogeneous and the inhomogeneous one, yield the same sequence $(s_n)_{n\geq 0}$.

Now consider the first order nonlinear congruential generator (see Chapter 2)

$$s_{n+1} = f(s_n), \qquad n \geq 0 ,$$

where f is a nonlinear function from F_p into F_p , p a prime. It will turn out later that the sequence $(s_n)_{n\geq 0}$ of elements of F_p satisfies an $(d+1)$-th order homogeneous linear recurrence relation, where d is the degree of the polynomial g, which is uniquely determined by

$$g(n) := s_n \qquad \text{for all } n \in F_p \text{ and } 0 \leq deg(g) \leq p-1$$

(see Lemma 3.11).

This is the reason why we deal with linear recurring sequences although we study nonlinear congruential generators. The main purpose of this section is not to give a comprehensive introduction to the theory of linear recurring sequences, but to provide a result (Theorem 3.3), which will be needed in Chapter 4. The results of this section are from Lidl and Niederreiter [21].

In the following let F_q be the uniquely determined field with q elements, where $q = p^m$, p a prime and $m \geq 1$.

Definition 3.1

(i) Let k be a positive integer, and let $a_0, a_1, \ldots, a_{k-1}$ be given elements of F_q. A sequence $(s_n)_{n\geq 0}$ of elements of F_q satisfying the relation

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n \qquad n = 0, 1, 2, \ldots \quad (3.1)$$

is called a (k-th order homogeneous) linear recurring sequence in F_q.

(ii) The terms $s_0, s_1, \ldots, s_{k-1}$, which uniquely determine the rest of the sequence, are referred to as the initial values.

(iii) *The polynomial*

$$f(x) = x^k - a_{k-1}x^{k-1} - \ldots - a_1 x - a_0 \qquad \in F_q[x] \qquad (3.2)$$

is called the characteristic polynomial of the linear recurrence relation (3.1).

(iv) *The generating function of a given sequence* $(s_n)_{n\geq 0}$ *of elements of* F_q *is defined by*

$$G(x) = \sum_{n=0}^{\infty} s_n\, x^n.$$

Let $F_q[[x]]$ be the set of all formal power series over the field F_q with addition and multiplication as usual:

$$\sum_{n=0}^{\infty} b_n x^n + \sum_{n=0}^{\infty} c_n x^n := \sum_{n=0}^{\infty}(b_n + c_n)x^n \ ,$$

$$(\sum_{n=0}^{\infty} b_n x^n)(\sum_{n=0}^{\infty} c_n x^n) := \sum_{n=0}^{\infty}(\sum_{k=0}^{n} b_k c_{n-k})x^n \ .$$

Then $F_q[[x]]$ is a commutative ring with unity.

Lemma 3.1 *The formal power series* $B(x) = \sum_{n=0}^{\infty} b_n x^n \in F_q[[x]]$ *has a multiplicative inverse if and only if* $b_0 \neq 0$.

Proof. If $B(x)$ has a multiplicative inverse, say $C(x)$, then $B(x)C(x) = 1$, which means that $\sum_{n=0}^{\infty}(\sum_{k=0}^{n} b_k c_{n-k})x^n = 1$. Therefore $b_0 c_0 = 1$ and hence $b_0 \neq 0$.

Conversely, if $b_0 \neq 0$, we can find a c_0 such that $b_0 c_0 = 1$. Furthermore we can compute

$$\begin{array}{ll} c_1 & \text{by } b_0c_1 + b_1c_0 = 0 \ , \\ c_2 & \text{by } b_0c_2 + b_1c_1 + b_2c_0 = 0 \ , \ldots \end{array}$$

and

$$c_n \quad \text{by } b_0c_n + b_1c_{n-1} + \ldots + b_nc_0 = 0 \; .$$

Hence the coefficients $c_0, c_1, \ldots$ can be computed recursively. The resulting formal power series $C(x)$ is the multiplicative inverse of $B(x)$. □

Now, let $(s_n)_{n\geq 0}$ be a sequence in F_q, satisfying the linear recurrence relation (3.1). We define its *reciprocal characteristic polynomial* as

$$f^*(x) = 1 - a_{k-1}x - a_{k-2}x^2 - \ldots - a_0x^k \quad \in F_q[x]. \tag{3.3}$$

It is obvious that $f^*(x) = x^k \cdot f(\frac{1}{x})$, f being the characteristic polynomial in (3.2). The following Lemma yields an interesting relation between the reciprocal characteristic polynomial and the generating function of a given linear recurring sequence:

Lemma 3.2 *Let $(s_n)_{n\geq 0}$ be a kth-order homogeneous linear recurring sequence in F_q satisfying the linear recurrence relation (3.1); let $f^*(x) \in F_q[x]$ be its reciprocal characteristic polynomial, and let $G(x) \in F_q[[x]]$ be its generating function.Then*

(1) the identity

$$G(x) = \frac{g(x)}{f^*(x)} \tag{3.4}$$

holds with

$$g(x) = -\sum_{j=0}^{k-1}\sum_{i=0}^{j} a_{i+k-j}s_i\, x^j \; ,$$

where we set $a_k := -1$;

(2) Conversely, let $f^*(x) \in F_q[x]$ be the reciprocal characteristic polynomial of a given kth-order linear recurrence relation (3.1), and let $g(x)$ be an arbitrary polynomial over F_q with $deg(g) < k$, then the formal power series $G(x) \in F_q[[x]]$, defined by

$$G(x) := \frac{g(x)}{f^*(x)}$$

is the generating function of a sequence, which satisfies the given kth-order linear recurrence relation (3.1).

Proof. Part 1. With $a_k := -1$ we have

$$\begin{aligned} f^*(x)\,G(x) &= -\left(\sum_{n=0}^{k} a_{k-n}x^n\right)\left(\sum_{n=0}^{\infty} s_n x^n\right) \\ &= -\sum_{j=0}^{\infty}\left(\sum_{i=0}^{j} a_{k-(j-i)}s_i\right)x^j \qquad \text{where } a_l := 0 \text{ for } l \leq -1 \\ &= -\sum_{j=0}^{k-1}\left(\sum_{i=0}^{j} a_{i+k-j}s_i\right)x^j - \sum_{j=k}^{\infty}\left(\sum_{i=0}^{j} a_{i+k-j}s_i\right)x^j \\ &= g(x) - \sum_{j=k}^{\infty}\left(\sum_{i=j-k}^{j} a_{i+k-j}s_i\right)x^j\ . \end{aligned}$$

Hence

$$f^*(x)\,G(x) = g(x) - \sum_{j=k}^{\infty}\left(\sum_{i=0}^{k} a_i s_{j-k+i}\right)x^j\ .$$

But $\left(\sum_{i=0}^{k} a_i s_{j-k+i}\right) = 0$ because the sequence $s_0, s_1, \ldots$ satisfies the linear recurrence relation (3.1). Therefore $f^*(x)\,G(x) = g(x)$. By Lemma 3.1 $f^*(x)$ has a multiplicative inverse in $F_q[[x]]$, since the constant coefficient is 1, which concludes the proof of the first part.

Part 2. Let $f^*(x)$ be the reciprocal characteristic polynomial of a given kth-order linear recurrence relation (3.1), and let $g(x)$ be an arbitrary polynomial over F_q with $deg(g) < k$. If we put

$$G(x) := \frac{g(x)}{f^*(x)},$$

then we obtain from above that $f^*(x)\,G(x)$ is equal to a polynomial of degree less than k only if $\sum_{i=0}^{k} a_i s_{j-k+i} = 0$ for all $j \geq k$. But this implies that the sequence $s_0, s_1, \ldots$ of coefficients of $G(x)$ satisfies the linear recurrence relation (3.1). $\square$

Consider a linear recurring sequence $(s_n)_{n\geq 0}$, defined by a given linear recurrence relation. Then the sequence $(s_n)_{n\geq 0}$ satisfies numerous other linear recurrence relations beside the one by which it is defined. The following theorem discusses this fact and exhibits the relationship between the various linear recurrence relations valid for a given homogeneous linear recurring sequence.

Theorem 3.3 *Let $(s_n)_{n\geq 0}$ be a homogeneous linear recurring sequence in F_q. Then there exists a uniquely determined monic polynomial $m(x) \in F_q[x]$ having the following property: a monic polynomial $f(x) \in F_q[x]$ of positive degree is a characteristic polynomial of $(s_n)_{n\geq 0}$ if and only if $m(x)$ divides $f(x)$.*

Proof. Let $s_0, s_1, \dots$ be a homogeneous linear recurring sequence defined by a linear recurrence relation and let $f_0(x) = -\sum_{j=0}^{k} a_j x^j$ be its characteristic polynomial, where $a_k = -1$. Then we define

$$h_0(x) := \sum_{j=0}^{k-1} \sum_{i=0}^{k-1-j} a_{i+j+1} s_i\, x^j \quad \in F_q[x],$$

a polynomial determined by $f_0(x)$ and the sequence, and $d(x) := gcd(f_0(x), h_0(x))$, the monic greatest common divisor of $f_0(x)$ and $h_0(x)$. Let $f_0(x) = m(x)\, d(x)$ and $h_0(x) = b(x)\, d(x)$ with $m(x),\ b(x)\ \in F_q[x]$. We will prove that $m(x)$ is the desired polynomial. $m(x)$ is monic, because $d(x)$ and $f_0(x)$ are monic.

Now let $f(x) \in F_q[x]$ be an arbitrary characteristic polynomial of the given sequence $s_0, s_1, \dots$, say $f(x) = -\sum_{j=0}^{l} b_j x^j$ and $b_l = -1$. We have to show that $m(x)$ divides $f(x)$. To do this we need the polynomial $h(x) \in F_q[x]$, determined by $f(x)$ and the given sequence:

$$h(x) := \sum_{j=0}^{l-1} \sum_{i=0}^{l-1-j} b_{i+j+1} s_i\, x^j\ .$$

By Lemma 3.2, the generating function $G(x)$ of the sequence satisfies

$$G(x) = \frac{g_0(x)}{f_0^*(x)} = \frac{g(x)}{f^*(x)}$$

with

$$g_0(x) = -\sum_{j=0}^{k-1} \sum_{i=0}^{j} a_{i+k-j} s_i\, x^j$$

and

$$g(x) = -\sum_{j=0}^{l-1}\sum_{i=0}^{j} b_{i+l-j} s_i\, x^j,$$

and therefore

$$g(x)f_0^*(x) = g_0(x)f^*(x). \tag{3.5}$$

We have

$$x^{k-1}g_0\left(\frac{1}{x}\right) = -h_0(x) \quad \text{and} \quad x^{l-1}g\left(\frac{1}{x}\right) = -h(x), \tag{3.6}$$

because

$$\begin{aligned} x^{k-1}g_0\left(\frac{1}{x}\right) &= -\sum_{j=0}^{k-1}\sum_{i=0}^{j} a_{i+k-j} s_i\, x^{k-1-j} \\ &= -\sum_{j'=0}^{k-1}\sum_{i=0}^{k-1-j'} a_{i+j'+1} s_i\, x^{j'} \qquad (j' := k-1-j) \\ &= -h_0(x) \end{aligned}$$

and, in the same way, we see that $x^{l-1}g\left(\frac{1}{x}\right) = -h(x)$. By applying the identities (3.5) and (3.6) we arrive at

$$\begin{aligned} h(x)f_0(x) &= -x^{l-1}g\left(\frac{1}{x}\right) x^k f_0^*\left(\frac{1}{x}\right) \\ &= -x^{k-1}g_0\left(\frac{1}{x}\right) x^l f^*\left(\frac{1}{x}\right) = h_0(x)f(x). \end{aligned}$$

We divide this equation by $d(x)$ and get

$$h(x)m(x) = b(x)f(x).$$

Since $m(x)$ and $b(x)$ are relatively prime, it follows that $m(x)$ divides $f(x)$.

Conversely, let $f(x) \in F_q[x]$ be monic with $deg(f) > 0$ such that $m(x)$ divides $f(x)$; say $f(x) = -\sum_{i=0}^{l} b_i\, x^i$ with $b_l = -1$. We have to show that $f(x)$ is a characteristic polynomial of the sequence $(s_n)_{n\geq 0}$.

Since $m(x)$ divides $f(x)$, $f(x) = m(x)c(x)$ with $c(x) \in F_q[x]$. Passing to reciprocal polynomials we get

$$f^*(x) = (m(x)c(x))^* = m^*(x)c^*(x)\ , \tag{3.7}$$

because $(u := deg(m))$

$$\begin{aligned}(m(x)c(x))^* &= \left(\sum_{i=0}^{u} m_i\, x^i \cdot \sum_{j=0}^{v} c_j\, x^j\right)^* \\ &= \sum_{i=0}^{u}\sum_{j=0}^{v} m_i c_j\, x^{u+v-(i+j)} \\ &= \left(\sum_{i=0}^{u} m_i\, x^{u-i}\right) \cdot \left(\sum_{j=0}^{v} c_j\, x^{v-j}\right) = m^*(x) \cdot c^*(x)\,.\end{aligned}$$

We also have

$$h_0(x)m(x) = b(x)f_0(x)\ , \tag{3.8}$$

since $h_0(x) = b(x)d(x)$ and $f_0(x) = m(x)d(x)$. Therefore, using the relations (3.6) and (3.8), we obtain

$$\begin{aligned}g_0(x)m^*(x) &= -x^{k-1}h_0\left(\frac{1}{x}\right)x^u m\left(\frac{1}{x}\right) \\ &= -x^{u-1}b\left(\frac{1}{x}\right)x^k f_0\left(\frac{1}{x}\right)\,.\end{aligned}$$

Now $k = deg(f_0) > deg(h_0)$, hence, by looking at (3.8), $deg(b) < deg(m) = u$. Thus $-x^{u-1}b\left(\frac{1}{x}\right)$ is a polynomial $a(x) \in F_q[x]$, and we have

$$g_0(x)m^*(x) = a(x)f_0^*(x)\,. \tag{3.9}$$

From Lemma 3.2 it follows that the generating function $G(x)$ of the sequence satisfies $G(x) = \frac{g_0(x)}{f_0^*(x)}$. Using (3.9) and (3.7), we have

$$G(x) = \frac{g_0(x)}{f_0^*(x)} = \frac{a(x)}{m^*(x)} = \frac{a(x)c^*(x)}{m^*(x)c^*(x)} = \frac{a(x)c^*(x)}{f^*(x)}\ ,$$

where

$$\begin{aligned}deg(a(x)c^*(x)) &= deg(a(x)) + deg(c^*(x)) \\ &< deg(m(x)) + deg(c(x)) = deg(f(x))\ ,\end{aligned}$$

because $deg(a(x)) < deg(m(x))$ and $deg(c^*(x)) \leq deg(c(x))$. The second part of Lemma 3.2 shows that $\frac{a(x)c^*(x)}{f^*(x)}$ is the generating function of a sequence that satisfies a linear recurrence relation with characteristic polynomial $f(x)$. Since it equals the generating function $G(x)$ of the sequence $(s_n)_{n\geq 0}$, $f(x)$ is a characteristic polynomial of this sequence.

To see the uniqueness of $m(x)$, let us assume that there exists a $\tilde{m}(x)$ with the indicated properties. Then

$$\begin{aligned}
m(x)|\tilde{m}(x) &\Rightarrow m(x)p(x) = \tilde{m}(x) && \text{for a monic } p(x) \in F_q[x], \\
\tilde{m}(x)|m(x) &\Rightarrow \tilde{m}(x)q(x) = m(x) && \text{for a monic } q(x) \in F_q[x], \\
&\Rightarrow \tilde{m}(x)p(x)q(x) = \tilde{m}(x) \\
&\Rightarrow p(x)q(x) = 1 \\
&\Rightarrow p(x) = 1 \text{ and } q(x) = 1. \qquad \square
\end{aligned}$$

Definition 3.2 *The uniquely determined polynomial $m(x)$ over F_q of Theorem 3.3 is called the minimal polynomial of the sequence $(s_n)_{n\geq 0}$.*

The minimal polynomial is the characteristic polynomial of the linear recurrence relation of least possible order satisfied by the sequence.

3.2 The difference operator Δ

We define the difference operator Δ^t applied to a sequence $(u_n)_{n\geq 0}$ of elements of a field F in the usual way:

$$\begin{aligned} \Delta^0 u_n &:= u_n \\ \Delta^t u_n &:= \Delta^{t-1}u_{n+1} - \Delta^{t-1}u_n \qquad \text{for } t \geq 1. \end{aligned}$$

The set of all sequences of elements of F with component-wise addition and scalar multiplication forms a vector space, called the sequence space over F :

$$\begin{aligned} (u_n)_{n\geq 0} + (v_n)_{n\geq 0} &:= (u_n + v_n)_{n\geq 0} \\ \lambda(u_n)_{n\geq 0} &:= (\lambda u_n)_{n\geq 0}. \end{aligned}$$

Lemma 3.4 *Δ^t is a linear operator on the sequence space over F.*

Proof. By induction on t, we see that Δ^t is an additive operator:

$$\begin{aligned} \Delta^0(u_n + v_n) &= u_n + v_n = \Delta^0 u_n + \Delta^0 v_n \\ \Delta^t(u_n + v_n) &= \Delta^{t-1}(u_{n+1} + v_{n+1}) - \Delta^{t-1}(u_n + v_n) \\ &= \Delta^{t-1}u_{n+1} + \Delta^{t-1}v_{n+1} - (\Delta^{t-1}u_n + \Delta^{t-1}v_n) \\ &= \Delta^{t-1}u_{n+1} - \Delta^{t-1}u_n + \Delta^{t-1}v_{n+1} - \Delta^{t-1}v_n) \\ &= \Delta^t u_n + \Delta^t v_n \end{aligned}$$

Δ^t is a homogeneous operator:

$$\begin{aligned} \Delta^0(\lambda u_n) &= \lambda u_n = \lambda\Delta^0 u_n \\ \Delta^t(\lambda u_n) &= \Delta^{t-1}(\lambda u_{n+1}) - \Delta^{t-1}(\lambda u_n) \\ &= \lambda\Delta^{t-1}(u_{n+1}) - \lambda\Delta^{t-1}(u_n) \\ &= \lambda(\Delta^{t-1}(u_{n+1}) - \Delta^{t-1}(u_n)) \\ &= \lambda\Delta^t u_n \qquad \square \end{aligned}$$

Lemma 3.5 $\Delta^t u_n = \sum_{j=0}^{t}(-1)^{t-j}\binom{t}{j}u_{n+j}$.

Proof. Again we proceed by induction on t :

$$\begin{aligned}
\Delta^0 u_n &= u_n = \sum_{j=0}^{0}(-1)^0\binom{0}{j}u_{n+j} \\
\Delta^t u_n &= \Delta^{t-1}u_{n+1} - \Delta^{t-1}u_n \\
&= \sum_{j=0}^{t-1}(-1)^{t-1-j}\binom{t-1}{j}u_{n+1+j} - \sum_{j=0}^{t-1}(-1)^{t-1-j}\binom{t-1}{j}u_{n+j} \\
&= \sum_{j=1}^{t}(-1)^{t-j}\binom{t-1}{j-1}u_{n+j} + \sum_{j=0}^{t-1}(-1)^{t-j}\binom{t-1}{j}u_{n+j} \\
&= u_{n+t} + \sum_{j=1}^{t-1}(-1)^{t-j}\binom{t}{j}u_{n+j} + (-1)^t u_n \\
&= \sum_{j=0}^{t}(-1)^{t-j}\binom{t}{j}u_{n+j} \qquad \square
\end{aligned}$$

Lemma 3.6 *Let $g(x) \in F_p[x]$ with $deg(g) = d$ and $1 \leq d \leq p-1$, then $deg(\Delta g(n)) = d-1$.*

Proof. Let $g(x) = a_d x^d + \ldots + a_1 + a_0$ with $a_i \in F_p$ for $0 \leq i \leq d$ and $a_d \neq 0$.

$$\begin{aligned}
\Delta g(n) &= g(n+1) - g(n) \\
&= a_d(n+1)^d + a_{d-1}(n+1)^{d-1} + \ldots + a_1(n+1) + a_0 \\
&\quad -a_d n^d - a_{d-1}n^{d-1} - \ldots - a_1 n - a_0
\end{aligned}$$

Now, let us consider the coefficients of n^d and n^{d-1} : The coefficient of n^d is $a_d - a_d = 0$, whereas the coefficient of n^{d-1} is $da_d + a_{d-1} - a_{d-1} = da_d \neq 0$. Therefore $deg(\Delta g(n)) = d-1$. $\square$

Lemma 3.7 *Let $g(x) \in F_p[x]$ with $deg(g) = d$ and $d \geq 1$. Then we have*

1. $\Delta^d(g(n)) \neq 0 \qquad \forall n \in F_p,$
2. $\Delta^{d+1}(g(n)) = 0 \qquad \forall n \in F_p.$

Proof.

1. For $d = 1$ we have
$$\Delta^1(g(n)) = \Delta^1(an + b) = a(n + 1) + b - an - b = a \neq 0.$$
If $d > 1$, then, by induction on n,
$$\Delta^d(g(n)) = \Delta^{d-1}(\Delta g(n)) \neq 0, \text{ since } deg(\Delta g(n)) = d - 1.$$

2. For $d = 1$ we have
$$\Delta^2(g(n)) = \Delta(\Delta^1(an + b)) = \Delta a = a - a = 0.$$
If $d > 1$, then, again by induction on n,
$$\Delta^{d+1}(g(n)) = \Delta^d(\Delta g(n)) = 0, \text{ since } deg(\Delta g(n)) = d - 1. \qquad \square$$

Theorem 3.8 *Let $g(x) \in F_p[x]$ with $deg(g) = d$ and $1 \leq d \leq p - 2$, and $u_n := g(n)$ for all $n \in F_p$ and $u_{n+p} := u_n \quad \forall n \geq 0$. Then the sequence $(u_n)_{n \geq 0}$ is a linear recurring sequence with minimal polynomial $(x - 1)^{d+1}$.*

Proof. By applying the difference operator Δ^{d+1} on both sides of the equation $u_n = g(n)$ we get

$$\sum_{j=0}^{d+1} (-1)^{d+1-j} \binom{d+1}{j} u_{n+j} = 0 \qquad \forall n \in F_p,$$

since $\Delta^{d+1}(g(n)) = 0 \quad \forall n \in F_p$, according to Lemma 3.7. This shows, that the sequence $u_0, u_1, \ldots$ satisfies a linear recurrence relation of order $d + 1$. The corresponding characteristic polynomial is

$$\sum_{j=0}^{d+1} (-1)^{d+1-j} \binom{d+1}{j} x^j = (x-1)^{d+1}.$$

From Theorem 3.3 we know that the uniquely determined minimal polynomial divides any characteristic polynomial of a given sequence. Therefore the minimal polynomial of the sequence $(u_n)_{n \geq 0}$ is of the form $(x-1)^k$ with $k \leq d+1$.

Now suppose that $k \leq d$, then $(x-1)^d$ would be a characteristic polynomial. But if we apply the difference operator Δ^d on both sides of the equation $u_n = g(n)$ we get

$$\sum_{j=0}^{d} (-1)^{d-j} \binom{d}{j} u_{n+j} = \Delta^d(g(n)) \neq 0$$

according to Lemma 3.7. Thus $(x-1)^d = \sum_{j=0}^{d} (-1)^{d-j} \binom{d}{j} x^j$ cannot be a characteristic polynomial. So the assumption that $k \leq d$ was wrong. This yields $k = d+1$. $\square$

Let us summerize the essence of Theorem 3.8: If we have a sequence $(u_n)_{n \geq 0}$ generated by a polynomial $g \in F_p[x]$ (i.e. $u_n := g(n) \quad n \geq 0$), with $deg(g) = d$, then the sequence satisfies the linear recurrence relation

$$\sum_{j=0}^{d+1} (-1)^{d+1-j} \binom{d+1}{j} u_{n+j} = 0 \qquad n \geq 0.$$

Since we have said nothing about the polynomial g except that $deg(g) = d$, all polynomials of a given degree d generate sequences that have the same minimal polynomial, namely $(x-1)^{d+1}$, and therefore satisfy the same linear recurrence relation of order $d+1$. The different sequences with minimal polynomial $(x-1)^{d+1}$ are uniquely determined by the initial values $u_0, \ldots, u_d$. We will apply Theorem 3.8 with g being a permutation polynomial in Chapter 4.

3.3 Permutation polynomials

A central idea of some of the proofs in Chapter 4 is to replace the first order nonlinear recursion

$$u_{n+1} \equiv f(u_n) \pmod{p}, \qquad n \in F_p\,,$$

by the relation

$$u_n \equiv g(n) \pmod{p}, \qquad n \in F_p,$$

f being a nonlinear function from F_p into F_p and $g \in F_p[x]$. Since f is chosen in such a way that the least period of the sequence $u_0, u_1, \ldots$ is p, g is a permutation polynomial. In order to preserve generality, the statements in this paragraph use the finite field F_q, where $q = p^m$, p is prime and m is a positive integer. Clearly, the results are valid in the special case $q = p$ a prime.

In the previous paragraph we have made use of a polynomial $g \in F_p[x]$ and put $u_n := g(n)$ for $n \geq 0$. It has turned out that $u_0, u_1, \ldots$ is a linear recurring sequence with minimal polynomial $(x-1)^{d+1}$, where $d := deg(g)$. Now, let $u_0, u_1, \ldots$ be a given sequence in F_p with period p. Lemma 3.11 shows how to find a polynomial g with $g(n) = u_n$ for all $n \in F_p$. Furthermore the polynomial g is uniquely determined if $deg(g) < p$.

Hermite's Criterion (Theorem 3.9) yields an algorithm to check whether a given polynomial is a permutation polynomial or not. Although this criterion is not of practical use for large q because of the computational complexity, we can nevertheless deduce Corollary 3.10. The latter will be helpful in Chapter 4. Our presentation closely follows the monograph of Lidl and Niederreiter [21, Chapter 7].

Definition 3.3 *A polynomial $f \in F_q[x]$ is called a permutation polynomial if $\{f(c) : \ c \in F_q\} = F_q$.*

Theorem 3.9 *(Hermite's Criterion) Let F_q be of characteristic p (i.e. $q = p^m$, p prime). Then $f \in F_q[x]$ is a permutation polynomial of F_q if and only if the following two conditions hold:*

1. *f has exactly one root in F_q,*
2. *for each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \pmod{p}$, the reduction of $f(x)^t$ modulo $x^q - x$ has degree less or equal to $q-2$.*

An interesting consequence of Hermite's Criterion is the following

Corollary 3.10 *If $d > 1$ is a divisor of $q-1$, then there does not exist a permutation polynomial of F_q of degree d.*

Proof. Let f be a polynomial over F_q with $deg(f) = d$, where d divides $q-1$, say $d\,c = q-1$ with $1 \leq c \leq q-2$. Then $deg(f^c) = d\,c = q-1$, and therefore condition 2 of Theorem 3.9 is not satisfied for $t = c$. $\square$

In order to prove Theorem 3.9 we have to show some basic results:

Lemma 3.11 *If φ is an arbitrary function from F_q into F_q, then there exists a unique polynomial $g \in F_q[x]$ with $deg(g) < q$ representing φ (i.e. $g(c) = \varphi(c) \quad \forall c \in F_q$).*

g can be found by the formula

$$g(x) = \sum_{c \in F_q} \varphi(c) \left(1 - (x-c)^{q-1}\right). \tag{3.10}$$

Proof. Since (3.10) yields a polynomial with degree less than q, which represents φ, we only have to show the uniqueness of g.

Consider the mapping Φ from the set of all polynomials over F_q with degree $< q$ into the set of all functions from F_q into F_q, which maps each polynomial to the function it represents. Because of (3.10), Φ is surjective. Since the number of polynomials over F_q with degree $< q$ is equal to the number q^q of functions from F_q into F_q, Φ is bijective. $\square$

The polynomial g can also be found by computing the Lagrange interpolation polynomial for the function φ.

Lemma 3.12 *Let $f, g \in F_q[x]$. Then*

$$f(c) = g(c) \quad \forall c \in F_q \;\Leftrightarrow\; f(x) \equiv g(x) \pmod{x^q - x}.$$

Proof. Using the division algorithm in $F_q[x]$ we can write $f(x) - g(x) = h(x)\,(x^q - x) + r(x)$ with $h(x), r(x) \in F_q[x]$ and $deg(r(x)) < q$. In F_q we have the relation $c^q = c \quad \forall c \in F_q$, hence

$$\begin{aligned} f(c) = g(c) \quad \forall c \in F_q &\Leftrightarrow r(c) = 0 \quad \forall c \in F_q \\ &\Leftrightarrow r = 0 \quad \text{in } F_q[x] \\ &\Leftrightarrow f(x) - g(x) \equiv 0 \pmod{x^q - x} \\ &\Leftrightarrow f(x) \equiv g(x) \pmod{x^q - x}. \qquad \square \end{aligned}$$

The following two lemmata are rather technical. They will only be needed in the subsequent proof of Theorem 3.9 (Hermite's Criterion).

Lemma 3.13 *Let $a_0, a_1, \ldots, a_{q-1} \in F_q$. Then the following two conditions are equivalent:*

1. *$a_0, a_1, \ldots, a_{q-1}$ are distinct* $\quad$ (*i.e.* $\{a_0, a_1, \ldots, a_{q-1}\} = F_q$)
2. $$\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & \textit{for } t = 0, 1, \ldots, q-2 \\ -1 & \textit{for } t = q-1 \end{cases}.$$

Proof. Consider the polynomial

$$g_i(x) := 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} x^j \qquad \text{for fixed } i \text{ with } 0 \le i \le q-1.$$

We have $g_i(a_i) = 1 - \sum_{j=0}^{q-1} a_i^{q-1} = 1 - 0 = 1$ and $g_i(0) = 1 - a_i^{q-1} = 0$ for $a_i \neq 0$. For $b \in F_q^*$ with $b \neq a_i$, and hence $a_i b^{-1} \neq 1$, we have

$$\begin{aligned}
g_i(b) &= 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} b^j \\
&= 1 - b^{q-1} \sum_{j=0}^{q-1} a_i^{q-1-j} b^{-(q-1-j)} \\
&= 1 - \sum_{j=0}^{q-1} (a_i b^{-1})^{q-1-j} \\
&= 1 - \frac{1 - (a_i b^{-1})^q}{1 - a_i b^{-1}} = 1 - \frac{1 - a_i b^{-1}}{1 - a_i b^{-1}} = 0.
\end{aligned}$$

Now let

$$\begin{aligned}
g(x) := \sum_{i=0}^{q-1} g_i(x) &= \sum_{i=0}^{q-1} \left(1 - \sum_{j=0}^{q-1} a_i^{q-1-j} x^j \right) \\
&= -\sum_{j=0}^{q-1} \left(\sum_{i=0}^{q-1} a_i^{q-1-j} \right) x^j.
\end{aligned}$$

$g(x)$ is a polynomial with degree $< q$, that maps each element of F_q to 1 if and only if $\{a_0, a_1, \ldots, a_{q-1}\} = F_q$. Hence we have

$$\{a_0, a_1, \ldots, a_{q-1}\} = F_q \Leftrightarrow g(c) = 1 \quad \forall c \in F_q.$$

Due to Lemma 3.11, we see that this is equivalent to the conditions

$$-\sum_{i=0}^{q-1} a_i^{q-1-j} = \begin{cases} 0 & \text{for } j = 1, 2, \ldots, q-1 \\ 1 & \text{for } j = 0 \end{cases}$$

and, hence,

$$\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & \text{for } t = 0, 1, \ldots, q-2 \\ -1 & \text{for } t = q-1 \end{cases} . \qquad \square$$

Lemma 3.14

$$\left(\sum_{i=1}^{m} a_i\right)^{p^j} = \sum_{i=1}^{m} a_i^{p^j} \qquad \textit{with } a_i \in F_q, \quad 1 \le i \le m, \quad j \ge 1,$$

where the prime p denotes the characteristic of the finite field F_q.

Proof. First we show that $(a+b)^p = a^p + b^p$ for $a, b \in F_q$:

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \ldots + \binom{p}{p-1} a b^{p-1} + b^p$$

$$\text{where } \binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdots i}$$

For $1 < i < p$ we have $\binom{p}{i} \equiv 0 \bmod p$ since $\binom{p}{i}$ is an integer and the prime p in the numerator cannot be canceld. The characteristic of F_q is p, therefore $(a+b)^p = a^p + b^p$.

The desired result follows now by induction on m and j :

$$\begin{aligned}
\left(\sum_{i=1}^{m} a_i\right)^{p^j} &= \left(\left(\left(\sum_{i=1}^{m-1} a_i\right) + a_m\right)^{p^{j-1}}\right)^p = \left(\left(\sum_{i=1}^{m-1} a_i\right)^{p^{j-1}} + a_m^{p^{j-1}}\right)^p \\
&= \left(\sum_{i=1}^{m} a_i^{p^{j-1}}\right)^p = \sum_{i=1}^{m} a_i^{p^j}. \qquad \square
\end{aligned}$$

Proof of Theorem 3.9 :

If f is a permutation polynomial of F_q, then, trivially, f has exactly one root in F_q, thus the first part is trivial. To verify condition 2, we look at the reduction of $f(x)^t \pmod{x^q - x}$, which is some polynomial, say

$$b^{(t)}(x) = \sum_{j=0}^{q-1} b_j^{(t)} x^j.$$

According to Lemma 3.12, $b^{(t)}(c) = f(c)^t$ for all $c \in F_q$. Hence, following Lemma 3.11, we have

$$\sum_{j=0}^{q-1} b_j^{(t)} x^j = \sum_{c \in F_q} f(c)^t \left(1 - (x-c)^{q-1}\right),$$

and by comparing the coefficient of x^{q-1} on each side we see that

$$b_{q-1}^{(t)} = -\sum_{c \in F_q} f(c)^t.$$

Since f is a permutation polynomial,

$$b_{q-1}^{(t)} = -\sum_{c \in F_q} c^t$$

and, according to Lemma 3.13, $\sum_{c \in F_q} c^t = 0$ for $t = 1, 2, \ldots, q-2$; hence 2. follows.

Conversely, let conditions 1 and 2 be satisfied. Then condition 1 implies that

$$\sum_{c \in F_q} (f(c))^{q-1} = \sum_{c \in F_q^*} 1 = -1.$$

Condition 2 implies

$$-b_{q-1}^{(t)} = \sum_{c \in F_q} f(c)^t = 0 \qquad \text{for } 1 \le t \le q-2 \text{ and } t \not\equiv 0 \pmod{p}.$$

Using Lemma 3.14, we have

$$\sum_{c \in F_q} f(c)^{tp^j} = \left(\sum_{c \in F_q} f(c)^t\right)^{p^j}$$

and, therefore,

$$\sum_{c \in F_q} f(c)^t = 0 \qquad \text{for all } t \text{ with } 1 \le t \le q-2.$$

This identity holds trivially for $t = 0$. Now Lemma 3.13 implies that f is a permutation polynomial of F_q. $\square$

3.4 A trigonometric inequality

For the estimation of discrepancy bounds we will make use of the following result from Cochrane [3].

Theorem 3.15 *For any positive integers m, n with $m > 1$ we have*

$$\sum_{a=1}^{m-1} \frac{|\sin \pi an/m|}{|\sin \pi a/m|} < \frac{4}{\pi^2} m \log m + 0.38m + 0.608 + 0.116 \frac{d^2}{m},$$

where $d = gcd(m, n)$.

In our notation m denotes the modulus and n will be an integer with $1 \leq n \leq m$. If m is prime we have $d = 1$ except for $n = m$. But for the case $m|n$ the trigonometric sum equals zero. Therefore we have

$$\sum_{a=1}^{p-1} \frac{|\sin \pi an/p|}{|\sin \pi a/p|} < \frac{4}{\pi^2} p \log p + 0.38p + 0.64$$

for any prime $p > 5$ and any integer n.
If m is not a prime, then the maximum value for $d = \gcd(m, n)$ with $1 \leq n < m$ is $m/2$. Hence we arrive at

$$\sum_{a=1}^{m-1} \frac{|\sin \pi an/m|}{|\sin \pi a/m|} < \frac{4}{\pi^2} m \log m + 0.41m + 0.61$$

for any positive integer m and any n with $1 \leq n < m$.

3.5 General discrepancy bounds

For a given sequence of prns, the extreme discrepancy can be used as a measure for the deviation from uniformity (see introduction). For higher dimensions, the computational complexity of $D_N^{(s)}$ is too large to allow a determination of its value. Therefore we will provide upper and lower bounds for $D_N^{(s)}$. The following general discrepancy bound, which is based on exponential sums, is due to Niederreiter [26]. Our proof follows Hellekalek [19].

For an integer $M \geq 2$, let $C(M) =]-M/2, M/2] \cap \mathbf{Z}$ and $C^*(M) = C(M) \setminus \{0\}$. Furthermore, let $C_s(M)$ be the cartesian product of s copies of $C(M)$ and $C_s^*(M) = C_s(M) \setminus \{\mathbf{0}\}$. Put

$$r(h, M) = \begin{cases} M \sin \frac{\pi |h|}{M} & \text{for } h \in C^*(M) \\ 1 & \text{for } h = 0 \end{cases} .$$

For $\mathbf{h} = (h_1, \ldots, h_s) \in C_s(M)$, put

$$r(\mathbf{h}, M) = \prod_{i=1}^{s} r(h_i, M).$$

We will use the abbreviation $e(u) := e^{2\pi\sqrt{-1}u}$ for $u \in \mathbf{R}$ and we write $\mathbf{x} \cdot \mathbf{y}$ for the standard inner product of $\mathbf{x}, \mathbf{y} \in \mathbf{R}^s$.

The following Lemma (see [26, Lemma 3.9]) will be used to provide an upper bound for the difference of volumes of an arbitrary given subinterval of $[0,1[^s$ and a suitable approximating subinterval.

Lemma 3.16 *Let $t_i, u_i \in [0,1]$ for $1 \leq i \leq s$ and let $v \in [0,1]$ be such that $|t_i - u_i| \leq v$ for $1 \leq i \leq s$. Then*

$$\left| \prod_{i=1}^{s} t_i - \prod_{i=1}^{s} u_i \right| \leq 1 - (1-v)^s.$$

Proof. We proceed by induction on s : For $s = 1$ we have $|t_1 - u_1| \leq 1 - (1-v)^1 = v$, which is true, since we have assumed $|t_1 - u_1| \leq v$.

Now, let the inequality be shown for some $s \geq 1$. Without loss of generality we may assume that $t_{s+1} \geq u_{s+1}$. Then

$$\prod_{i=1}^{s+1} t_i - \prod_{i=1}^{s+1} u_i = (t_{s+1} - u_{s+1}) \prod_{i=1}^{s} t_i + u_{s+1} \left(\prod_{i=1}^{s} t_i - \prod_{i=1}^{s} u_i \right).$$

Hence

$$\begin{aligned} \left| \prod_{i=1}^{s+1} t_i - \prod_{i=1}^{s+1} u_i \right| &\leq (t_{s+1} - u_{s+1}) \prod_{i=1}^{s} t_i + u_{s+1} \left| \prod_{i=1}^{s} t_i - \prod_{i=1}^{s} u_i \right| \\ &\leq t_{s+1} - u_{s+1} + u_{s+1}(1 - (1-v)^s) \\ &= t_{s+1}(1 - (1-v)^s) + (t_{s+1} - u_{s+1})(1-v)^s \\ &\leq 1 - (1-v)^s + v(1-v)^s = 1 - (1-v)^{s+1}. \qquad \square \end{aligned}$$

Theorem 3.17 *For an integer $M \geq 2$ and $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{N-1} \in \mathbf{Z}_M^s$, let $\mathcal{P}$ be the point set $(\mathbf{x}_n)_{n=0}^{N-1}$, where $\mathbf{x}_n := \mathbf{y}_n / M \bmod 1$. Then*

$$D_N^{(s)}(\mathcal{P}) \leq 1 - \left(1 - \frac{1}{M}\right)^s + \sum_{\mathbf{k} \in C_s^*(M)} \frac{1}{r(\mathbf{k}, M)} \left| \frac{1}{N} \sum_{n=0}^{N-1} e\left(\frac{1}{M} \mathbf{k} \cdot \mathbf{y}_n\right) \right|.$$

Proof. From the definition of $D_N^{(s)}(\mathcal{P})$ we have

$$D_N^{(s)}(\mathcal{P}) = \sup_{J \in \mathcal{J}} \left| \frac{A(J; \mathcal{P})}{N} - \lambda_s(J) \right|,$$

where $\mathcal{J}$ is the family of all subintervals of $[0,1[^s$ of the form $\prod_{i=1}^{s} [u_i, v_i[$, and $A(J; \mathcal{P})$ denotes the cardinality of $\mathcal{P} \cap J$.

For a given subinterval J we choose a "suitable" approximating subinterval $G = G(J)$ in $[0,1[^s$, where "suitable" means

- $A(J, \mathcal{P}) = A(G, \mathcal{P})$,
- $\lambda_s(J)$ and $\lambda_s(G)$ are close,
- $A(G, \mathcal{P})$ may be expressed by exponential sums.

Then as a consequence,

$$\left|\frac{A(J,\mathcal{P})}{N} - \lambda_s(J)\right| \leq |\lambda_s(J) - \lambda_s(G)| + \left|\frac{A(G,\mathcal{P})}{N} - \lambda_s(G)\right|.$$

With $R_N(J) := \frac{1}{N}A(J,\mathcal{P}) - \lambda_s(J)$ this amounts to

$$|R_N(J)| \leq |\lambda_s(J) - \lambda_s(G)| + |R_N(G)|. \tag{3.11}$$

How to choose $G = G(J)$: We have $J = \prod_{i=1}^{s}[u_i, v_i[$ and

$$\mathcal{P} \subseteq \left\{\left(\frac{a_1}{M}, \ldots, \frac{a_s}{M}\right) :\ a_i \in \{0, 1, \ldots, M-1\},\ 1 \leq i \leq s\right\} =: \frac{1}{M}\mathbf{Z}_M^s \pmod 1.$$

For $\mathbf{p} \in \frac{1}{M}\mathbf{Z}_M^s$, $\mathbf{p} = (p_1, \ldots, p_s)$, let $I_{\mathbf{p}} := \prod_{i=1}^{s}[p_i, p_i + 1/M[$. We define the approximating interval of J to be

$$G = G(J) := \bigcup_{\mathbf{p} \in J} I_{\mathbf{p}}.$$

Then $A(G,\mathcal{P}) = A(J,\mathcal{P})$, and $G = \prod_{i=1}^{s}[a_i/M, b_i/M[$ with

$$a_i = \min\left\{a \in \{0, 1, \ldots, M-1\} : \quad u_i \leq \frac{a}{M}\right\}$$

$$b_i = \min\left\{b \in \{1, \ldots, M\} : \quad v_i \leq \frac{b}{M}\right\}.$$

- Case 1: $G = \emptyset$. This implies that there exists a coordinate i such that $v_i - u_i < 1/M$ and $A(J,\mathcal{P}) = 0$. Hence

$$|R_N(J)| = \lambda_s(J) < \frac{1}{M} \leq 1 - \left(1 - \frac{1}{M}\right)^s.$$

- Case 2: $G \neq \emptyset$. From $A(J,\mathcal{P}) = A(G,\mathcal{P})$ we obtain

$$\begin{aligned} |R_N(J)| &\leq |R_N(J) - R_N(G)| + |R_N(G)| \\ &= |\lambda_s(J) - \lambda_s(G)| + |R_N(G)|. \end{aligned}$$

We now use Lemma 3.16 to estimate $|\lambda_s(J) - \lambda_s(G)|$: with

$$\lambda_s(J) = \prod_{i=1}^{s}(v_i - u_i), \qquad \lambda_s(G) = \prod_{i=1}^{s}\left(\frac{b_i}{M} - \frac{a_i}{M}\right),$$

we have

$$\left|\left(\frac{b_i}{M} - \frac{a_i}{M}\right) - (v_i - u_i)\right| = \left|\left(\frac{b_i}{M} - v_i\right) - \left(\frac{a_i}{M} - u_i\right)\right| \leq \frac{1}{M},$$

since $0 \leq b_i/M - v_i \leq 1/M$ and $0 \leq a_i/M - u_i \leq 1/M$. Hence Lemma 3.16 yields $|\lambda_s(J) - \lambda_s(G)| \leq 1 - \left(1 - \frac{1}{M}\right)^s$. Thus

$$D_N^{(s)}(\mathcal{P}) = \sup_{J\in\mathcal{J}} |R_N(J)| \leq 1 - \left(1 - \frac{1}{M}\right)^s + \sup_{J\in\mathcal{J}} |R_N(G)|. \tag{3.12}$$

Let us study $R_N(G)$.

$$\begin{aligned}
R_N(G) &= \frac{A(G,\mathcal{P})}{N} - \lambda_s(G) \\
&= \frac{1}{N}\sum_{n=0}^{N-1}\left(1_G(\mathbf{x}_n) - \lambda_s(G)\right) \\
&= \sum_{\mathbf{p}:\mathbf{p}\in G}\frac{1}{N}\sum_{n=0}^{N-1}\left(1_{I_\mathbf{p}}(\mathbf{x}_n) - \frac{1}{M^s}\right)
\end{aligned}$$

$$= \sum_{\mathbf{p}:\mathbf{p}\in G}\frac{1}{N}\sum_{n=0}^{N-1}\left(\delta(\mathbf{p},\mathbf{x}_n) - \frac{1}{M^s}\right) \tag{3.13}$$

$$\text{with} \quad \delta(\mathbf{p},\mathbf{x}_n) := \begin{cases} 1 & \text{for } \mathbf{p} = \mathbf{x}_n \\ 0 & \text{for } \mathbf{p} \neq \mathbf{x}_n \end{cases}.$$

We will now replace the expression $\delta(\mathbf{p}, \mathbf{x}_n)$ by exponential sums. Let $a \in \{0, 1, \ldots, M-1\}$, then

$$\begin{aligned}
\frac{1}{M} \sum_{k \in C(M)} e\left(\frac{a}{M}k\right) &= \frac{1}{M} \sum_{k=0}^{M-1} e\left(\frac{a}{M}k\right) \\
&= \frac{1}{M} \sum_{k=0}^{M-1} \left(e\left(\frac{a}{M}\right)\right)^k = \begin{cases} 1 & \text{for } a \equiv 0 \pmod{M} \\ 0 & \text{for } a \not\equiv 0 \pmod{M} \end{cases}.
\end{aligned}$$

Therefore we can write

$$\delta(a \bmod M, 0) = \frac{1}{M} \sum_{k \in C(M)} e\left(\frac{a}{M}k\right) \qquad \text{for all } a \in \mathbf{Z}.$$

For any $\mathbf{a} = (a_1, \ldots, a_s) \in \mathbf{Z}^s$ we have

$$\begin{aligned}
\frac{1}{M^s} \sum_{\mathbf{k} \in C_s(M)} e\left(\frac{1}{M}\mathbf{k} \cdot \mathbf{a}\right) &= \prod_{i=1}^{s} \frac{1}{M} \sum_{k_i \in C(M)} e\left(\frac{1}{M}k_i a_i\right) \\
&= \prod_{i=1}^{s} \delta(a_i \bmod M, 0) \\
&= \begin{cases} 1 & \text{for } a_i \equiv 0 \bmod M \qquad \forall i \text{ with } 1 \leq i \leq s \\ 0 & \text{else} \end{cases} \\
&= \delta(\mathbf{a} \bmod M, \mathbf{0}).
\end{aligned}$$

We choose $\mathbf{g}(\mathbf{p}) \in \mathbf{Z}^s$ such that

$$\mathbf{p} \equiv \frac{1}{M}\mathbf{g}(\mathbf{p}) \pmod{1}.$$

Then

$$\begin{aligned}
\delta(\mathbf{x}_n, \mathbf{p}) &= \delta(\mathbf{y}_n \bmod M, \mathbf{g}(\mathbf{p}) \bmod M) \\
&= \delta(\mathbf{y}_n - \mathbf{g}(\mathbf{p}) \bmod M, \mathbf{0}).
\end{aligned}$$

Hence

$$\delta(\mathbf{x}_n, \mathbf{p}) = \frac{1}{M^s} \sum_{\mathbf{k} \in C_s(M)} e\left(\frac{1}{M}\mathbf{k} \cdot (\mathbf{y}_n - \mathbf{g}(\mathbf{p}))\right)$$

and

$$\delta(\mathbf{x}_n, \mathbf{p}) - \frac{1}{M^s} = \frac{1}{M^s} \sum_{\mathbf{k} \in C_s^*(M)} e\left(\frac{1}{M}\mathbf{k} \cdot (\mathbf{y}_n - \mathbf{g}(\mathbf{p}))\right).$$

Therefore , together with (3.13), we have

$$\begin{aligned} R_N(G) &= \sum_{\mathbf{p}:\mathbf{p}\in G} \frac{1}{N} \sum_{n=0}^{N-1} \frac{1}{M^s} \sum_{\mathbf{k} \in C_s^*(M)} e\left(\frac{1}{M}\mathbf{k} \cdot (\mathbf{y}_n - \mathbf{g}(\mathbf{p}))\right) \\ &= \sum_{\mathbf{k} \in C_s^*(M)} \left(\frac{1}{M^s} \sum_{\mathbf{p}:\mathbf{p}\in G} e\left(\frac{1}{M}\mathbf{k} \cdot (-\mathbf{g}(\mathbf{p}))\right)\right) \cdot \left(\frac{1}{N} \sum_{n=0}^{N-1} e\left(\mathbf{k} \cdot \mathbf{x}_n\right)\right). \end{aligned}$$

Thus

$$|R_N(G)| \le \sum_{\mathbf{k} \in C_s^*(M)} \left|\frac{1}{M^s} \sum_{\mathbf{p}:\mathbf{p}\in G} e\left(\frac{1}{M}\mathbf{k} \cdot (-\mathbf{g}(\mathbf{p}))\right)\right| \cdot \left|\frac{1}{N} \sum_{n=0}^{N-1} e\left(\mathbf{k} \cdot \mathbf{x}_n\right)\right|. \quad (3.14)$$

The remaining part of the proof is concerned with the evaluation of

$$\left|\frac{1}{M^s} \sum_{\mathbf{p}:\mathbf{p}\in G} e\left(\frac{1}{M}\mathbf{k} \cdot (-\mathbf{g}(\mathbf{p}))\right)\right|.$$

$\mathbf{p}$ is an element of $G = \prod_{i=1}^{s} [a_i/M, b_i/M[$ if and only if $a_i \le g(p)_i < b_i$, $\forall i, \quad 1 \le i \le s$. From this we obtain

$$\begin{aligned} \left|\frac{1}{M^s} \sum_{\mathbf{p}:\mathbf{p}\in G} e\left(\frac{1}{M}\mathbf{k} \cdot \mathbf{g}(\mathbf{p})\right)\right| &= \frac{1}{M^s} \left|\sum_{\mathbf{t}:a_i \le t_i < b_i} e\left(\frac{1}{M}\mathbf{k} \cdot \mathbf{t}\right)\right| \\ &= \prod_{i=1}^{s} \frac{1}{M} \left|\sum_{a_i \le t_i < b_i} e\left(\frac{1}{M} k_i t_i\right)\right|. \end{aligned}$$

If $k_i \neq 0$ then

$$\left|\sum_{a_i \le t_i < b_i} e\left(\frac{1}{M} k_i t_i\right)\right| = \left|\sum_{t_i=0}^{b_i - a_i - 1} \left(e\left(\frac{1}{M} k_i\right)\right)^{t_i}\right|$$

$$= \left| \frac{e\left((b_i - a_i)\frac{1}{M}k_i\right) - 1}{e\left(\frac{1}{M}k_i\right) - 1} \right|$$
$$= \left| \frac{\sin \pi \left|\frac{b_i - a_i}{M}k_i\right|}{\sin \frac{k_i}{M}} \right| \leq \frac{M}{r(k_i, M)}.$$

If $k_i = 0$ then

$$\left| \sum_{a_i \leq t_i < b_i} e\left(\frac{1}{M}k_i t_i\right) \right| = b_i - a_i \leq M = \frac{M}{r(k_i, M)}.$$

Hence

$$\left| \frac{1}{M^s} \sum_{\mathbf{p}:\mathbf{p}\in G} e\left(\frac{1}{M}\mathbf{k}\cdot\mathbf{g}(\mathbf{p})\right) \right| \leq \prod_{i=1}^{s} \frac{1}{M} \frac{M}{r(k_i, M)} = \frac{1}{r(\mathbf{k}, M)}.$$

Together with (3.14) this yields

$$|R_N(G)| \leq \sum_{\mathbf{k}\in C_s^*(M)} \frac{1}{r(\mathbf{k}, M)} \left| \frac{1}{N} \sum_{n=0}^{N-1} e\left(\mathbf{k}\cdot\mathbf{x}_n\right) \right|.$$

The result of the theorem follows from (3.12). $\square$

Corollary 3.18 *Let the point set $\mathcal{P} = (\mathbf{x}_n)_{n=0}^{N-1}$ be as in Theorem 3.17. Suppose that the real number B is such that*

$$\left| \sum_{n=0}^{N-1} e\left(\frac{1}{M}\mathbf{k}\cdot\mathbf{y}_n\right) \right| \leq B \qquad \textit{for all } \mathbf{k} \in C_s^*(M).$$

Then

$$D_N^{(s)}(\mathcal{P}) \leq 1 - \left(1 - \frac{1}{M}\right)^s + \frac{B}{N}\left(\frac{4}{\pi^2}\log M + 1.72\right)^s.$$

Proof. From (3.12) and (3.14) in the proof of Theorem 3.17 we obtain

$$|R_N(J)| < 1 - \left(1 - \frac{1}{M}\right)^s + \frac{B}{M^s N} \sum_{\mathbf{k}\in C_s^*(M)} \left| \sum_{\mathbf{t}:a_i \leq t_i < b_i} e\left(\frac{1}{M}\mathbf{k}\cdot\mathbf{t}\right) \right|.$$

Now,

$$\left|\sum_{\mathbf{t}:a_i\le t_i<b_i} e\left(\frac{1}{M}\mathbf{k}\cdot\mathbf{t}\right)\right| = \prod_{i=1}^{s}\left|\sum_{t_i=0}^{b_i-a_i-1} e\left(\frac{1}{M}h_ik_i\right)\right|,$$

therefore

$$\begin{aligned}
\sum_{\mathbf{k}\in C_s^*(M)}\left|\sum_{\mathbf{t}:a_i\le t_i<b_i} e\left(\frac{1}{M}\mathbf{k}\cdot\mathbf{t}\right)\right| &< \sum_{\mathbf{k}\in C_s(M)}\prod_{i=1}^{s}\left|\sum_{t_i=0}^{b_i-a_i-1} e\left(\frac{1}{M}h_ik_i\right)\right| \\
&= \prod_{i=1}^{s}\left(\sum_{k\in C(M)}\left|\sum_{t_i=0}^{b_i-a_i-1} e\left(\frac{1}{M}h_ik_i\right)\right|\right) \\
&\le \prod_{i=1}^{s}\left(M+\sum_{k=1}^{M-1}\left|\frac{\sin(\pi k(b_i-a_i)/M)}{\sin(\pi k/M)}\right|\right),
\end{aligned}$$

We use the following inequality from Cochrane [3] (see Theorem 3.15):

$$\sum_{k=1}^{M-1}\left|\frac{\sin(\pi kj/M)}{\sin(\pi k/M)}\right| < \frac{4}{\pi^2}M\log M + 0.41M + 0.61$$

for any integer j with $0\le j\le M$. This yields

$$\begin{aligned}
|R_N(J)| &< 1-\left(1-\frac{1}{M}\right)^s + \frac{B}{M^sN}\prod_{i=1}^{s}\left(M+M\frac{4}{\pi^2}\log M + 0.41M + 0.61\right) \\
&= 1-\left(1-\frac{1}{M}\right)^s + \frac{B}{M^sN}M^s\prod_{i=1}^{s}\left(\frac{4}{\pi^2}\log M + 1.41 + \frac{0.61}{M}\right),
\end{aligned}$$

and for $M\ge 2$ we have

$$|R_N(J)| < 1-\left(1-\frac{1}{M}\right)^s + \frac{B}{N}\left(\frac{4}{\pi^2}\log M + 1.72\right)^s. \qquad \square$$

3.6 The Bombieri-Weil bound for character sums

For the upper bound of the discrepancy of inversive congruential prns we need a result from the theory of finite fields, namely the Bombieri-Weil bound for character sums over F_q.
Let $\overline{F}_q$ be the algebraic closure of the field F_q and $\overline{F}_q(x)$ the field of rational functions over $\overline{F}_q$. We state a slight specialization of the result given by Moreno and Moreno [23].

Theorem 3.19 *Let Q/R be a rational function over F_q with $deg(Q) > deg(R)$, and suppose that Q/R is not of the form $A^p - A$ with $A \in \overline{F}_q(x)$. Then*

$$\left| \sum_{\substack{\gamma \in F_q \\ R(\gamma) \neq 0}} \chi\left(\frac{Q(\gamma)}{R(\gamma)}\right) \right| \leq (deg(Q) + r - 1)q^{1/2},$$

where $\chi(z) = e^{2\pi\sqrt{-1}z/p}$ and r is the number of distinct roots of the polynomial R in $\overline{F}_q$.

Remark 3.1 *If R is a constant polynomial, then $r = 0$. In this case the bound in Theorem 3.19 equals a well-known result from Weil [29].*

Chapter 4

Proofs

4.1 Proofs of the results for general nonlinear congruential generators

4.1.1 Proof of Theorem 2.1

Our proof of Theorem 2.1 follows Niederreiter [26].

Passing the s-dimensional lattice test means that the vectors $(\mathbf{y}_n - \mathbf{y}_0)$, $n = 1, 2, \ldots, p-1$, span F_p^s, where $\mathbf{y}_n = (y_n, \ldots, y_{n+s-1}) \in F_p^s$. This is equivalent to $\mathrm{rank}(U_s) = s$, where U_s is the matrix

$$\begin{pmatrix} y_1 - y_0 & y_2 - y_0 & \cdots & y_{p-1} - y_0 \\ y_2 - y_1 & y_3 - y_1 & \cdots & y_p - y_1 \\ \cdots & \cdots & \cdots & \cdots \\ y_s - y_{s-1} & y_{s+1} - y_{s-1} & \cdots & y_{s+p-2} - y_{s-1} \end{pmatrix}$$

since the columns of U_s are the vectors $(\mathbf{y}_n - \mathbf{y}_0)$ for $n = 1, 2, \ldots, p-1$. If $\mathrm{rank}(U_s) = s$, then $\mathrm{rank}(U_{s-1}) = s - 1$ (note that we get U_{s-1} by canceling the last row of U_s). Thus, passing the s-dimensional lattice test implies passing any lower dimensional lattice test. Therefore it suffices to show that $\text{rank}(U_d) = \text{rank}(U_{d+1}) = d$. We put

$$\mathbf{u}_j = (y_{j+1} - y_j, y_{j+2} - y_j, \ldots, y_{j+p-1} - y_j) \quad \in F_p^{p-1} \qquad \text{for } j = 0, 1, \ldots,$$

so $\mathbf{u}_j$ is the $(j+1)$-th row of U_s. Let Δ^k be the difference operator defined in Chapter 3 and let g be the uniquely determined polynomial with $deg(g) < p$ and $g(n) = y_n$ in F_p, $n \in F_p$ (see Lemma 3.11).
The property of Δ^k we use in the following equation has been shown in Section 2 of Chapter 3.
For $i = 1, 2, \ldots, p-1$, we have

$$\begin{aligned}
\sum_{j=0}^{d}(-1)^{d-j}\binom{d}{j}(y_{j+i} - y_j) &= \sum_{j=0}^{d}(-1)^{d-j}\binom{d}{j}\sum_{n=0}^{i-1}(y_{n+j+1} - y_{n+j}) \\
&= \sum_{j=0}^{d}(-1)^{d-j}\binom{d}{j}\sum_{n=0}^{i-1}\Delta y_{n+j} \\
&= \sum_{n=0}^{i-1}\sum_{j=0}^{d}(-1)^{d-j}\binom{d}{j}(\Delta y_{n+j}) \\
&= \sum_{n=0}^{i-1}\Delta^d(\Delta y_n) = \sum_{n=0}^{i-1}\Delta^{d+1}y_n \\
&= \sum_{n=0}^{i-1}\Delta^{d+1}g(n) = 0.
\end{aligned}$$

The last step follows from Lemma 3.7, since $deg(g) = d$. Now $(y_{j+i} - y_j)$ is the i-th component of $\mathbf{u}_j$, therefore

$$\sum_{j=0}^{d}(-1)^{d-j}\binom{d}{j}\mathbf{u}_j = 0,$$

which is equivalent to

$$\mathbf{u}_d = -\sum_{j=0}^{d-1}(-1)^{d-j}\binom{d}{j}\mathbf{u}_j.$$

Hence $\mathbf{u}_d$ is a linear combination of $\mathbf{u}_0, \mathbf{u}_1, \ldots, \mathbf{u}_{d-1}$; thus rank$(U_{d+1}) \leq d$ and rank(U_{d+1}) =rank(U_d). It remains to show that rank$(U_{d+1}) \geq d$.
With $\mathbf{y}_j = (y_j, \ldots, y_{j+d}) \in F_p^{d+1}$, we claim that $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_d$ are linearly independent over F_p. Suppose that there exist $b_0, b_1, \ldots, b_d \in F_p$, not all zero, such that $\sum_{j=0}^{d} b_j \mathbf{y}_j = 0$. By comparing components, we see that

$$\sum_{j=0}^{d} b_j y_{n+j} = 0 \qquad \text{for } n = 0, 1, \ldots, d$$

which is equivalent to

$$\sum_{j=0}^{d} b_j g(n+j) = 0 \qquad \text{for } n = 0, 1, \ldots, d.$$

If we put $h(x) = \sum_{j=0}^{d} b_j g(x+j)$, then $h(x)$ has at least $d+1$ distinct roots in F_p, namely $x = 0, 1, \ldots, d$. Now $h(x)$ is a polynomial over F_p with $deg(h) \leq d$, however, and so h is the zero polynomial, which means that

$$\sum_{j=0}^{d} b_j g(x+j) = 0 \qquad \text{for all } x \in F_p.$$

From this we obtain $\sum_{j=0}^{d} b_j y_{n+j} = 0$ for all $n \in F_p$. Thus the sequence $y_0, y_1, \ldots$ satisfies a linear recursion of order $\leq d$. This contradicts the fact that the minimal polynomial of the sequence $y_0, y_1, \ldots$ is $(x-1)^{d+1}$ (see Theorem 3.8).
Therefore $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_d$ are linearly independent over F_p; this implies the linear independence of $(\mathbf{y}_1 - \mathbf{y}_0), \ldots, (\mathbf{y}_d - \mathbf{y}_0)$, and since the transposes of the latter vectors are the first d columns of U_{d+1}, we obtain rank$(U_{d+1}) \geq d$. $\square$

4.1.2 Proof of Theorem 2.3

The following proof of Theorem 2.3 is due to Eichenauer-Herrmann and Niederreiter [15].

Proof of Part 1: From Corollary 3.18 we have

$$D_N^{(s)} \leq 1 - \left(1 - \frac{1}{p}\right)^s + \frac{B}{N}\left(\frac{4}{\pi^2}\log M + 1.72\right)^s,$$

if $|\sum_{n=0}^{N-1} e(\frac{1}{p}\mathbf{h}\cdot\mathbf{y}_n)| \leq B$ for all $\mathbf{h} \in C_s^*(p)$. Thus the exponential sum has to be evaluated. Now, take an arbitrary but fixed $\mathbf{h} = (h_1, \ldots, h_s) \quad \in C_s^*(p)$ and consider

$$\mathbf{h}\cdot\mathbf{y}_n = \sum_{i=1}^{s} h_i y_{n+i-1}$$

as an element of F_p. We put $y_n = g(n)$, with $g \in F_p[x]$ and $deg(g) = d < p$ (see Lemma 3.11). Then, as a consequence, $\mathbf{h}\cdot\mathbf{y}_n = G(n)$ with $G \in F_p[x]$ and $deg(G) = d < p$. In order to use a result from Weil [29] (see Theorem 3.19), we have to show that $deg(G) \geq 1$. Suppose that there would exist such $b \in F_p$, that

$$G(n) = h_1 y_n + h_2 y_{n+1}, \ldots, +h_s y_{n+s-1} = b \qquad \text{for all } n \geq 0.$$

By applying the difference operator Δ on both sides (see chapter 3) we get

$$\Delta\left(\sum_{i=1}^{s} h_i y_{n+i-1}\right) = 0 \qquad \text{for all } n \geq 0.$$

Since Δ is a linear operator on the sequence space over F_p we have

$$\Delta(G(n)) = \sum_{i=1}^{s} h_i \Delta(y_{n+i-1}) = \sum_{i=1}^{s} h_i(y_{n+i} - y_{n+i-1}) = 0$$

which is equivalent to

$$y_n(-h_1) + y_{n+1}(h_1 - h_2) + y_{n+2}(h_2 - h_3) + \ldots + y_{n+s-1}(h_{s-1} - h_s) + y_{n+s}h_s = 0.$$

This means that the sequence $y_0, y_1, \ldots$ satisfies a nontrivial linear recursion of order $\leq s$. The recursion is not trivial, since $(h_1, \ldots, h_s) \neq \mathbf{0}$ and hence

$(-h_1, h_1 - h_2, h_2 - h_3, \ldots, h_{s-1} - h_s, h_s) \neq \mathbf{0}$. Therefore the corresponding characteristic polynomial has degree $\leq s \leq d$. This is a contradiction to the fact that this sequence has minimal polynomial $(x-1)^{d+1}$ (see Theorem 3.8), since the minimal polynomial of a given linear recurring sequence divides any characteristic polynomial of the same sequence (see Theorem 3.3).
Thus $deg(G(n)) \geq 1$. From Weil's bound for character sums [29] (see Theorem 3.19) we then obtain

$$\left|\sum_{n \in F_p} e\left(\frac{1}{p}\mathbf{h} \cdot \mathbf{y}_n\right)\right| = \left|\sum_{n \in F_p} e\left(\frac{G(n)}{p}\right)\right| \leq (d-1)p^{1/2} \qquad \text{for all } \mathbf{h} \in C_s^*(p).$$

Therefore the hypothesis of Corollary 3.18 is satisfied with $B = (d-1)p^{1/2}$. The result of Part 1 of the theorem follows.

Proof of Part 2: We proceed as in the proof of Part 1. Fix $\mathbf{h} = (h_1, \ldots, h_s) \in C_s^*(p)$, with $s \leq d-1$. Let $Q(n) = \mathbf{h} \cdot \mathbf{y}_n$ with $deg(Q) \leq d$. Let us show that $deg(Q) \geq 2$.
Suppose that $deg(Q) < 2$, then there exist elements $a, b \in F_p$, such that

$$h_1 y_n + h_2 y_{n+1}, \ldots, + h_s y_{n+s-1} = an + b \qquad \text{for all } n \geq 0.$$

We now apply the difference operator Δ^2 on both sides and get

$$\Delta^2\left(\sum_{i=1}^{s} h_i y_{n+i-1}\right) = \Delta^2(an+b) = 0.$$

Δ^2 is a linear operator, thus we have

$$\sum_{i=1}^{s} h_i\left(\Delta^2 y_{n+i-1}\right) = \sum_{i=1}^{s} h_i\left(y_{n+i+1} - 2y_{n+i} + y_{n+i-1}\right) = 0$$

which is equivalent to

$$\begin{aligned} y_n h_1 \;&+\; y_{n+1}(-2h_1 + h_2) + y_{n+2}(h_1 - 2h_2 + h_3) + \ldots \\ \ldots \;&+\; y_{n+s-1}(h_{s-2} - 2h_{s-1} + h_s) + y_{n+s}(h_{s-1} - 2h_s) + y_{n+s+1} h_s = 0. \end{aligned}$$

This is a nontrivial homogeneous linear recursion of order $\leq s+1$. The nontriviality is clear, since $\mathbf{h} \in C_s^*(p)$ and hence $\mathbf{h} = (h_1, \ldots, h_s) \neq \mathbf{0}$. The

corresponding characteristic polynomial has degree $\leq s+1 \leq d$. As in part 1 of the proof, this is a contradiction to the fact that this sequence has minimal polynomial $(x-1)^{d+1}$ (see Theorem 3.8), since the minimal polynomial of a given linear recurring sequence divides any characteristic polynomial of the same sequence (see Theorem 3.3).
Therefore $2 \leq deg(Q) \leq d < p$. We consider any such Q and $1 \leq N < p$. As in the proof of Theorem 3.17 we have the identities

$$\sum_{c=0}^{p-1} \chi(ck) = \sum_{c=0}^{p-1} (\chi(k))^c = \frac{(\chi(k))^p - 1}{\chi(k) - 1} = 0 \qquad \text{for } k \in F_p \setminus \{0\}$$

and

$$\sum_{c=0}^{p-1} \chi(ck) = p \qquad \text{for } k = 0,$$

where $\chi(c)$ is an abbreviation for $e(c/p) = e^{2\pi i c/p}$. Therefore we can write

$$\sum_{n=0}^{N-1} \chi(Q(n)) = \sum_{n=0}^{p-1} \chi(Q(n)) \cdot \left(\sum_{j=0}^{N-1} \frac{1}{p} \sum_{c=0}^{p-1} \chi(c(n-j)) \right),$$

since the sum over j is 1 for $0 \leq n \leq N-1$ (for $j = n$ the inner sum has value p) and 0 for $N \leq n \leq p-1$ ($n - j \neq 0$ for $j = 0, 1, \ldots, N-1$).
By rearranging the sums on the right hand side we get

$$\sum_{n=0}^{N-1} \chi(Q(n)) = \frac{1}{p} \sum_{c=0}^{p-1} \sum_{n=0}^{p-1} \chi(Q(n) + cn) \cdot \sum_{j=0}^{N-1} \chi(-cj)$$

and, hence,

$$\left| \sum_{n=0}^{N-1} \chi(Q(n)) \right| \leq \frac{1}{p} \sum_{c=0}^{p-1} \left| \sum_{n=0}^{p-1} \chi(Q(n) + cn) \right| \cdot \left| \sum_{j=0}^{N-1} \overline{\chi(cj)} \right|,$$

where $\overline{\chi(cj)}$ is the complex conjugate of $\chi(cj)$. From above we know that $2 \leq deg(Q) \leq d$ which implies $deg(Q(n) + cn) \geq 1$. This enables us to use Weil's bound for character sums [29] (see Theorem 3.19):

$$\begin{aligned} \left| \sum_{n=0}^{N-1} \chi(Q(n)) \right| &\leq \frac{1}{p}(d-1)p^{1/2} \sum_{c=0}^{p-1} \left| \sum_{j=0}^{N-1} \chi(cj) \right| \\ &= (d-1)p^{-1/2} \left(N + \sum_{c=1}^{p-1} \left| \frac{\sin(\pi N c/p)}{\sin(\pi c/p)} \right| \right). \end{aligned}$$

For the latter equation see the proof of Theorem 3.17. By an inequality of Cochrane (see Theorem 3.15) we have

$$\sum_{c=1}^{p-1} \left| \frac{\sin(\pi N c/p)}{\sin(\pi c/p)} \right| < \frac{4}{\pi^2} p \log p + 0.38p + 0.64$$

and so we get

$$\begin{aligned} \left| \sum_{n=0}^{N-1} \chi\left(Q(n)\right) \right| &< (d-1)p^{-1/2} \left(N + \frac{4}{\pi^2} p \log p + 0.38p + 0.64 \right) \\ &= (d-1)p^{1/2} \left(\frac{4}{\pi^2} \log p + 0.38 + \frac{N+0.64}{p} \right) \\ &< (d-1)p^{1/2} \left(\frac{4}{\pi^2} \log p + 1.72 \right). \end{aligned}$$

The desired result now follows from Corollary 3.18 with
$B := (d-1)p^{1/2}\left(\frac{4}{\pi^2}\log p + 1.72\right)$. □

4.2 Proofs of selected results for inversive congruential generators

The subsequent proofs for inversive congruential generators follow Niederreiter [26].

4.2.1 Proof of Theorem 2.5

Let $y_n = g(n) \in F_p$ for $n = 0, 1, \ldots$, where g is a permutation polynomial. By Theorem 2.1 it suffices to show that $d = deg(g) \geq (p+1)/2$. From the definition of inversive congruential prns we have

$$y_{n+1} = a\overline{y}_n + b \qquad \text{for } n \geq 0,$$

thus

$$y_{n+1}y_n = a\overline{y}_n y_n + b y_n \qquad \text{for } n \geq 0$$

and

$$y_{n+1}y_n - b y_n - a\overline{y}_n y_n = 0 \qquad \text{for } n \geq 0.$$

If we put $\omega_n = y_{n+1}y_n - by_n - a \qquad \text{for } n \geq 0$, then $\omega_n = 0$ for $(p-1)$ values $n \in F_p$, namely for those with $y_n \neq 0$ (note that $\overline{y}_n y_n = 1$ if $y_n \neq 0$).
Now ω_n is represented by a polynomial $h(x)$ over F_p, with

$$h(n) = g(n)g(n+1) - bg(n) - a \qquad \text{for } n \geq 0.$$

Therefore $h(n)$ is a polynomial over F_p of degree $2d$. Since $\omega_n = 0$ for $p-1$ values $n \in F_p$, $h(x)$ has $p-1$ roots in F_p. Thus we must have $2d \geq p-1$. Now $d = (p-1)/2$ is impossible by Corollary 3.10, and so $d \geq (p+1)/2$. □

4.2.2 Proof of Theorem 2.6

Let $y_0, y_1, \ldots$ be generated by the recursion

$$y_{n+1} = a\overline{y}_n + b \qquad \text{in } F_p, \quad n \geq 0,$$

where a and b are chosen such that the least period is p. Without loss of generality we may assume that $y_0 = 0$.
Define $\psi(n) := a\overline{n} + b \quad \in F_p$ for $n \in F_p$ and let ψ^j be the j-th iterate of the function ψ, with $\psi^0(n) = n$. Whenever $n \neq -a\overline{y}_i$ for $0 \leq i \leq j-1$, we have

$$\psi^j(n) = y_j \frac{n + a\overline{y}_j}{n + a\overline{y}_{j-1}} \qquad \text{for } 1 \leq j \leq p-1. \tag{4.1}$$

This can be checked by induction on j :
Let $j = 1$ and $n \neq -a\overline{y}_0 = 0$. Note that $y_0 = 0$ and $y_1 = b$. Thus

$$\psi^1(n) = a\overline{n} + b = \frac{a + bn}{n} = b\frac{a\overline{b} + n}{n} = y_1 \frac{a\overline{y}_1 + n}{a\overline{y}_0 + n}.$$

For an arbitrary $j \geq 1$ we have

$$\psi^{j+1}(n) = \psi^j(\psi(n)) = \psi^j(a\overline{n} + b).$$

The condition $n \neq -a\overline{y}_i \quad$ for $0 \leq i \leq j$ yields

$$a\overline{n} + b \neq -y_i + b \qquad \text{for } 0 \leq i \leq j;$$

furthermore

$$-y_i + b = -a\overline{y}_{i-1} \qquad \text{for } i \geq 1,$$

thus

$$a\overline{n} + b \neq -a\overline{y}_i \qquad \text{for } 0 \leq i \leq j-1.$$

This allows us to use identity (4.1) for the evaluation of $\psi^j(a\overline{n} + b)$. Note that in particular $n \neq 0$ and $y_j \neq 0$ for $1 \leq j \leq p-1$.

$$\begin{aligned}
\psi^{j+1}(n) &= \psi^j(a\overline{n} + b) = y_j \frac{a\overline{n} + b + a\overline{y}_j}{a\overline{n} + b + a\overline{y}_{j-1}} = y_j \frac{a\overline{n} + y_{j+1}}{a\overline{n} + y_j} \\
&= y_j \frac{a + y_{j+1}n}{a + y_j n} = \frac{a + y_{j+1}n}{a\overline{y}_j + n} = y_{j+1} \frac{a\overline{y}_{j+1} + n}{a\overline{y}_j + n}.
\end{aligned}$$

Thus (4.1) is valid for all j with $1 \leq j \leq p-1$. If $s \geq p$, then the theorem is trivial, therefore we may assume $s < p$. We now write the set of points in terms of the function ψ. We have

$$\{\mathbf{y}_n : \ 0 \leq n \leq p-1\} = \{(\psi^0(n), \psi^1(n), \ldots, \psi^{s-1}(n)) : \ 0 \leq n \leq p-1\}. \tag{4.2}$$

The elements of the first set have first component y_n, whereas the elements of the second set have first component n. Since both, y_n and n, run through all elements of F_p for $0 \le n \le p-1$, the sets are equal.
How can we write the condition $y_n \cdots y_{n+s-2} \neq 0$ in terms of the second set? The condition $y_n \cdots y_{n+s-2} \neq 0$ means that the first $(s-1)$ components are all different from 0. Now, $\psi^0(n) \neq 0$ is equivalent to $n \neq -a\overline{y}_0$. If $n \neq -a\overline{y}_0$, we can use (4.1) to see that $\psi^1(n) \neq 0$ is equivalent to $n \neq -a\overline{y}_1$. Again, if $n \neq -a\overline{y}_0$ and $n \neq -a\overline{y}_1$, we can apply (4.1) to verify that $\psi^2(n) \neq 0$ is equivalent to $n \neq -a\overline{y}_2$ etc. Finally, if $n \neq -a\overline{y}_i$ for $0 \le i \le s-3$, (4.1) yields that $\psi^{s-2}(n) \neq 0$ if and only if $n \neq -a\overline{y}_{s-2}$.

Therefore the condition $y_n \cdots y_{n+s-2} \neq 0$ in the first set amounts to the condition $n \neq -a\overline{y}_i$ for $0 \le i \le s-2$ in the second set.
This enables us to use (4.1) to express the components of our set of points. Now let a hyperplane H in F_p^s be defined by

$$\sum_{j=1}^{s} b_j z_j = b_0 \qquad \text{with } b_0, b_1, \ldots, b_s \in F_p \text{ and } (b_1, \ldots, b_s) \neq \mathbf{0}.$$

Then identity (4.1) shows that, for $n \neq -a\overline{y}_i$, $0 \le i \le s-2$, we have $(\psi^0(n), \psi^1(n), \ldots, \psi^{s-1}(n)) \in H$ if and only if

$$b_1 n + \sum_{j=2}^{s} b_j y_{j-1} \frac{n + a\overline{y}_{j-1}}{n + a\overline{y}_{j-2}} = b_0.$$

Clearing denominators, we see that this is equivalent to $h(n) = 0$, where the polynomial h over F_p is given by

$$h(x) = (b_1 x - b_0) \prod_{j=2}^{s} (x + a\overline{y}_{j-2}) + \sum_{j=2}^{s} b_j y_{j-1} (x + a\overline{y}_{j-1}) \cdot \prod_{\substack{i=2 \\ i \neq j}}^{s} (x + a\overline{y}_{i-2}).$$

Since $deg(h) \le s$, the result of the theorem will follow if we can show that h is not the zero polynomial. If h were the zero polynomial, then, by looking at the coefficient of x^s, we would get $b_1 = 0$. Furthermore, for $2 \le k \le s$, we would obtain

$$0 = h(-a\overline{y}_{k-2}) = b_k y_{k-1} (-a\overline{y}_{k-2} + a\overline{y}_{k-1}) \prod_{\substack{i=2 \\ i \neq j}}^{s} (-a\overline{y}_{k-2} + a\overline{y}_{i-2}).$$

Since $y_m \neq y_n$ for $m \neq n$, we have $a\overline{y}_m \neq a\overline{y}_n$ if $m \neq n$. There are no non-trivial zero divisors in F_p, hence $b_k = 0$ for $2 \leq k \leq s$. This is a contradiction to $(b_1, \ldots, b_s) \neq \mathbf{0}$. $\square$

4.2.3 Proof of Theorem 2.7

Let $y_0, y_1, \ldots$ be generated by the recursion

$$y_{n+1} \equiv a\overline{y}_n + b \pmod{p} \qquad \text{for } n \geq 1.$$

Again, a and b are chosen in such a way, that the least period of the sequence $y_0, y_1, \ldots$ is p. For a given $s \geq 2$, put $\mathbf{y_n} = (y_n, y_{n+1}, \ldots, y_{n+s-1})$ for $n \geq 0$. The theorem is trivial for $s \geq p$, since the upper bound for the discrepancy is greater than one; therefore we can assume that $s < p$. From Corollary 3.18 we have

$$D_p^{(s)} \leq 1 - \left(1 - \frac{1}{p}\right)^s + \frac{B}{p}\left(\frac{4}{\pi^2}\log p + 1.72\right)^s,$$

$$\text{if} \quad \left|\sum_{n=0}^{p-1} e\left(\frac{1}{p}\mathbf{h} \cdot \mathbf{y}_n\right)\right| \leq B \quad \text{for all } \mathbf{h} \in C_s^*(p).$$

Hence our task amounts to find the smallest possible number B. For a fixed $\mathbf{h} = (h_1, \ldots, h_s) \in C_s^*(p)$, we define

$$S(\mathbf{h}) := \sum_{n=0}^{p-1} e\left(\frac{1}{p}\mathbf{h} \cdot \mathbf{y}_n\right) = \sum_{n=0}^{p-1} e\left(\frac{1}{p}\sum_{j=1}^{s} h_j y_{n+j-1}\right).$$

We use (4.2) to obtain

$$\begin{aligned} S(\mathbf{h}) &= \sum_{n=0}^{p-1} e\left(\frac{1}{p}\sum_{j=1}^{s} h_j \psi^{j-1}(n)\right) \\ &= \sum_{n=0}^{p-1} \chi\left(\sum_{j=1}^{s} h_j \psi^{j-1}(n)\right), \end{aligned}$$

where $\chi(c) := e(c/p) = e^{2\pi i c/p}$ for $c \in F_p$. Now, consider an arbitrary but fixed $\mathbf{h} = (h_1, \ldots, h_s)$ and let k be the least index with $h_k \neq 0$. The function

$\psi(n) = a\overline{n} + b$ is a permutation of F_p; thus $\psi^j(n)$ is also a permutation of F_p, since $\psi^j(n)$ is the j-th iterate of ψ.
If $k = s$ we use $\psi^{s-1}(n)$ as a new summation variable and get

$$\begin{aligned} S(\mathbf{h}) &= \sum_{n=0}^{p-1} \chi(h_s \psi^{s-1}(n)) = \sum_{n=0}^{p-1} \chi(h_s n) \\ &= \sum_{n=0}^{p-1} (\chi(h_s))^n = \frac{1 - (\chi(h_s))^p}{1 - \chi(h_s)} = 0. \end{aligned}$$

For $k < s$ we have

$$\begin{aligned} S(\mathbf{h}) &= \sum_{n \in F_p} \chi\left(\sum_{j=k}^{s} h_j \psi^{j-1}(n) \right) \\ &= \sum_{n \in F_p} \chi\left(\sum_{j=k}^{s} h_j \psi^{j-k}(\psi^{k-1}(n)) \right). \end{aligned}$$

Now we use $\psi^{k-1}(n)$ as a new summation variable and derive

$$S(\mathbf{h}) = \sum_{n \in F_p} \chi\left(\sum_{j=k}^{s} h_j \psi^{j-k}(n) \right) = \sum_{n \in F_p} \chi\left(\sum_{j=0}^{s-k} h_{j+k} \psi^{j}(n) \right).$$

From the proof of Theorem 2.6 we have

$$\psi^j(n) = u_j \frac{n + a\overline{u}_j}{n + a\overline{u}_{j-1}}, \quad 1 \le j \le p-1,$$

whenever $n \neq -a\overline{u}_j$, for $0 \le i \le j-1$, where $u_0, u_1, \ldots \in F_p$ is generated by

$$u_{n+1} \equiv a\overline{u}_n + b \pmod p$$

and $u_0 = 0$. Therefore

$$\begin{aligned} S(\mathbf{h}) &= \sum_{n \in F_p} \chi\left(\sum_{j=0}^{s-k} h_{j+k} \psi^j(n) \right) \\ &= \sum_{\substack{n \in F_p \\ n \neq -a\overline{u}_i,\ 0 \le i \le s-k-1}} \chi\left(h_k n + \sum_{j=1}^{s-k} h_{j+k} u_j \frac{n + a\overline{u}_j}{n + a\overline{u}_{j-1}} \right) \\ &\quad + \sum_{i=0}^{s-k-1} \chi\left(\sum_{j=0}^{s-k} h_{j+k} \psi^j(-a\overline{u}_i) \right). \end{aligned}$$

The expression

$$h_k n + \sum_{j=1}^{s-k} h_{j+k} u_j \frac{n + a\overline{u}_j}{n + a\overline{u}_{j-1}}$$

is a rational function Q/R of n with $Q \in F_p[x]$ and

$$R(x) = \prod_{j=1}^{s-k} (x + a\overline{u}_{j-1}) \in F_p[x].$$

Hence

$$\begin{aligned}
|S(\mathbf{h})| &\leq \left| \sum_{\substack{n \in F_p \\ R(n) \neq 0}} \chi\left(\frac{Q(n)}{R(n)}\right) \right| + \sum_{i=0}^{s-k-1} \left| \chi\left(\sum_{j=0}^{s-k} h_{j+k} \psi^j(-a\overline{u}_i) \right) \right| \\
&= \left| \sum_{\substack{n \in F_p \\ R(n) \neq 0}} \chi\left(\frac{Q(n)}{R(n)}\right) \right| + s - k,
\end{aligned}$$

since $|\chi(c)| = 1$ for $c \in F_p$. Before we can apply Theorem 3.19, we have to ascertain that the hypotheses of this theorem are satisfied. First of all, $h_k n \neq 0$ implies that $deg(Q) = deg(R) + 1$. Now, suppose that Q/R is of the form $A^p - A$ with $A \in \overline{F}_q(x)$. Then

$$\frac{Q}{R} = \left(\frac{K}{L}\right)^p - \frac{K}{L}$$

with relatively prime polynomials K, L over $\overline{F}_q$, hence

$$L^p Q = K^p R - L^{p-1} K R = (K^{p-1} - L^{p-1}) K R.$$

From $\gcd(K, L) = 1$ it follows that L^p divides R. But the definition of R implies that R has only simple roots; thus the divisibility relation can only hold if L is a nonzero constant polynomial. This implies

$$Q = (c_1 K^p + c_2 K) R$$

for some $c_1, c_2 \in \overline{F}_q$ with $c_1, c_2 \neq 0$. Therefore we have $deg(Q) = deg(R) + p \cdot deg(K)$, which is a contradiction to $deg(Q) = deg(R) + 1$.

Hence, all hypotheses of Theorem 3.19 are satisfied, and so we arrive at

$$\begin{aligned}\left|\sum_{\substack{n\in F_p\\ R(n)\neq 0}} \chi\left(\frac{Q(n)}{R(n)}\right)\right| &\leq (deg(Q)+s-k-1)p^{1/2}\\ &= 2(s-k)p^{1/2} \leq 2(s-2)p^{1/2}.\end{aligned}$$

Altogether, we obtain

$$|S(\mathbf{h})| \leq 2(s-2)p^{1/2}+s-k \leq 2(s-2)p^{1/2}+s-1 \qquad \text{for all } \mathbf{h} \in C_s^*(p).$$

Thus we can apply Corollary 3.18 with $B = 2(s-2)p^{1/2}+s-1$, and this yields the desired result. $\square$

Bibliography

[1] L. Afflerbach and H. Grothe. Calculation of Minkowski-reduced lattice bases. *Computing*, **35**:269–276, 1985.

[2] Wun-Seng Chou. On inversive maximal period polynomials over finite fields. *Preprint, Austrian Academy of Sciences*, 1993.

[3] T. Cochrane. On a trigonometric inequality of Vinogradov. *J. Number Th.*, **27**:9–16, 1987.

[4] W. J. Conover. *Practical Nonparametric Statistics*. Wiley, New York, 1971.

[5] L. Devroye. *Non-Uniform Random Variate Generation*. Springer-Verlag, 1986.

[6] J. Eichenauer, H. Grothe, and J. Lehn. Marsaglia's lattice test and non-linear congruential pseudo random number generators. *Metrika*, **35**:241–250, 1988.

[7] J. Eichenauer and J. Lehn. A non-linear congruential pseudo random number generator. *Statist. Papers*, **27**:315–326, 1986.

[8] J. Eichenauer and J. Lehn. On the structure of quadratic congruential sequences. *Manuscripta Math.*, **58**:129–140, 1987.

[9] J. Eichenauer-Herrmann. Inversive congruential pseudorandom numbers avoid the planes. *Math. Comp.*, **56**:297–301, 1991.

[10] J. Eichenauer-Herrmann. Equidistribution properties of nonlinear congruential pseudorandom numbers. *Metrika*, **40**:333–338, 1993.

[11] J. Eichenauer-Herrmann. Explicit inversive congruential pseudorandom numbers: the compound approach. *Preprint*, Technische Hochschule Darmstadt, Darmstadt, Germany, 1993.

[12] J. Eichenauer-Herrmann. On generalized inversive congruential pseudorandom numbers. *Preprint*, Technische Hochschule Darmstadt, Darmstadt, Germany, 1993.

[13] J. Eichenauer-Herrmann. Statistical independence of a new class of inversive congruential pseudorandom numbers. *Math. Comp.*, **60**:375–384, 1993.

[14] J. Eichenauer-Herrmann and H. Niederreiter. On the discrepancy of quadratic congruential pseudorandom numbers. *J. Comp. Appl. Mathh.*, **34**:243–249, 1991.

[15] J. Eichenauer-Herrmann and H. Niederreiter. On the statistical independence of nonlinear congruential pseudorandom numbers. *Preprint*, Technische Hochschule Darmstadt, Darmstadt, Germany, 1992.

[16] J. Eichenauer-Herrmann and H. Niederreiter. Bounds for exponential sums and their applications to pseudorandom numbers. *Preprint*, Technische Hochschule Darmstadt, Darmstadt, Germany, 1993.

[17] George S. Fishman and Louis R. Moore. An exhaustive analysis of multiplicative congruential generators with modulus $2^{31}-1$. *SIAM J. Sci. Stat. Comput.*, **7**:24–45, 1986.

[18] H. Grothe. *Matrixgeneratoren zur Erzeugung gleichverteilter Pseudozufallsvektoren.* PhD thesis, Technische Hochschule Darmstadt, Darmstadt, Germany, 1988.

[19] P. Hellekalek. General discrepancy estimates : the Walsh function system. *Acta Arith.*, to appear.

[20] Donald E. Knuth. *The Art of Computer Programming*, volume 2. Addison-Wesley series in computer science and information processing, 2 edition, 1981.

[21] R. Lidl and H. Niederreiter. *Finite fields.* Addison-Wesley, Reading, Mass., 1983.

[22] G. Marsaglia. Random numbers fall mainly in the planes. *Proc. Nat. Acad. Sci.*, **61**:25–28, 1968.

[23] C.J. Moreno and O. Moreno. Exponential sums and Goppa codes: I. *Proc. Amer. Math. Soc.*, **111**:523–531, 1991.

[24] H. Niederreiter. Statistical independence of nonlinear congruential pseudorandom numbers. *Monatsh. Math.*, **106**:149–159, 1988.

[25] H. Niederreiter. On a new class of pseudorandom numbers for simulation methods. *J. Comput. Appl. Math.*, to appear, 1992.

[26] H. Niederreiter. *Random Number Generation and Quasi-Monte Carlo Methods.* SIAM, Philadelphia, USA, 1992.

[27] Brian D. Ripley. The lattice structure of pseudo-random number generators. *Proc. Roy. Soc. London Ser.A*, **389**:197–204, 1983.

[28] Brian D. Ripley. *Stochastic Simulation.* John Wiley & Sons, Inc., 1987.

[29] A. Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U.S.A.*, **34**:204–207, 1948.

Curriculum vitae

Name: Andreas Weingartner

Date of birth: June 15, 1971

Place of birth: Salzburg, Austria

Parents: Paul and Ursula Weingartner

Education:

1977-1981: Volksschule in Hallwang, Salzburg
1981-1989: Gymnasium in Liefering, Salzburg
1989-1994: University studies (M.Sc. in Mathematics) at the University of Salzburg