Van der Corput Sequences and Permutation Polynomials

Florian Pausinger

IST AUSTRIA
Institute of Science and Technology

Smolenice, 25. Juni 2012

Let $X = (x_n)_{n \geq 1}$ be a one-dimensional infinite sequence. For $N \geq 1$ and for an interval $I := [\alpha, \beta[$, where α, $\beta \in [0, 1]$

$$A(I, N, X)$$

gives the number of indices $n \leq N$, for which $x_n \in I$. We call

$$E(I, N, X) = A(I, N, X) - \lambda(I)N.$$

the discrepancy function of the interval I.

Diaphony

Let $X = (x_n)_{n \geq 1}$ be a one-dimensional infinite sequence. The diaphony F of the first N points of X was defined by Zinterhof (1976) in terms of exponential sums. We use the following equivalent definition in terms of the discrepancy function:

$$F^2(N, X) = 2\pi^2 \int_0^1 \int_0^1 E^2([\alpha, \beta[\,; N; X) d\alpha d\beta.$$

Generalized van der Corput sequence

Definition

Given an integer $n \geq 1$ in b-adic representation $\sum_{j=0}^{\infty} a_j(n) b^j$ and a permutation $\sigma \in \mathfrak{S}_b$, then the generalized van der Corput sequence S_b^σ in fixed base b is defined by

$$S_b^\sigma(n) = \sum_{j=0}^{\infty} \frac{\sigma(a_j(n))}{b^{j+1}}.$$

The generalized van der Corput sequence is a low discrepancy sequence and we define

$$f(S_b^\sigma(n)) := \limsup_{N \to \infty} (F^2(N, S_b^\sigma(n)) / \log N).$$

Graph of a χ-function

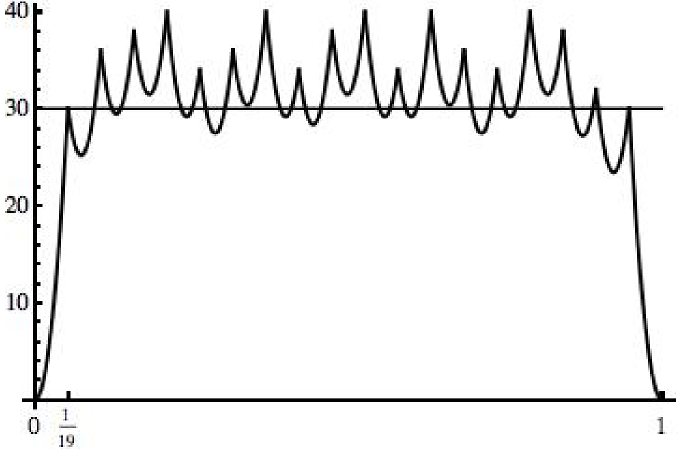

Figure: Graph of a χ-function in base 19

Analysis of the diaphony

Proposition (Chaix/Faure, 1993)

For each interval $[\frac{k}{b}, \frac{k+1}{b}]$ the parabolic arcs of χ_b^σ are translated versions of the parabola $y = b^2(b^2-1)x^2/12$.

Remark

This means that it suffices to know the values of χ_b^σ at the *b*-adic positions $\frac{k}{b}$ since for every interval $[\frac{k}{b}, \frac{k+1}{b}]$ χ_b^σ is of the form $Ax^2 + Bx + C$ with A only depending on the base b.

- Take the set of the first k elements of a permutation σ.
- Order this set and denote the ordered vector by

$$Z_k^\sigma = (z_0, \ldots, z_{k-1}).$$

- For each Z_k^σ, define the k-**th difference vector**

$$D_k^\sigma := (d_1, \ldots, d_k)$$

  such that $d_{h+1} := z_{h+1} - z_h - 1$, for $0 \leq h \leq k-1$, where $z_k := b + z_0$.
- The elements of D_k^σ represent the number of consecutive values of $\mathbb{Z}_b$ that are missing between two elements of Z_k^σ.

A new formula

Theorem (F.P., 2012)

Let $b \in \mathbb{N}$ and $\sigma \in \mathfrak{S}_b$. Then for all integers $1 \leq k \leq b$,

$$\chi_b^\sigma(k/b) = \frac{1}{2}\left(S_1(D_k^\sigma) + S_2(D_k^\sigma) - \frac{1}{6}(b-k)k(2bk - 2k^2 + 3k - 2)\right),$$

in which $S_1(D_1^\sigma) = 0$ and

$$S_1(D_k^\sigma) = \sum_{h=1}^{k} d_h \sum_{i=1}^{k-1} i^2 d_{h\oplus i} \quad \text{and} \quad S_2(D_k^\sigma) = \frac{k^2}{2}\sum_{h=1}^{k}(d_h+1)d_h.$$

Important Theorems I

Theorem (Chaix/Faure, 1993)

For all $N \geq 1$, we have

$$F^2(N, S_b^\sigma) = 4\pi^2 \sum_{j=1}^{\infty} \chi_b^\sigma(Nb^{-j}))/b^2.$$

Important Theorems II

Theorem (Chaix/Faure, 1993)

Let

$$\gamma_b^\sigma = \inf_{n \geq 1} \sup_{x \in \mathbb{R}} \left(\sum_{j=1}^{n} \chi_b^\sigma(x/b^j)/n \right),$$

then

$$f(S_b^\sigma) := \limsup_{N \to \infty} (F^2(N, X)/\log N) = 4\pi^2 \gamma_b^\sigma/(b^2 \log b).$$

Results for id perms

Theorem (Chaix/Faure, 1993)

$$f(S_b^{id}) = \begin{cases} \pi^2 \frac{b^4+2b^2-3}{48b^2 \log b} & \text{if } b \text{ is odd,} \\ \pi^2 \frac{b^3+b^2+4}{48(b+1)\log b} & \text{if } b \text{ is even.} \end{cases}$$

Theorem (Faure, 2005)

$$f(S_b^{\sigma}) \leq f(S_b^{id}).$$

A result for linear permutations

For coprime integers a, b $\pi_a(i) := ai \pmod{b}$ is called linear permutation with mulitplier a.

Theorem (F.P., 2012)

Let a be a multiplier that either divides $b+1$ or $b-1$. Then

$$f(S_{\sqrt{b}}^{id}) \leq f(S_b^{\pi_a}).$$

Motivation to study Permutation Polynomials

- New formula for χ_b^σ functions allows to study whole classes of permutations.
- In contrast to the above theorem, set of best linear permutations shows a very good distribution behavior.
- Optimal permutations are known until base 70 and are better than best linear permutations in a given base.

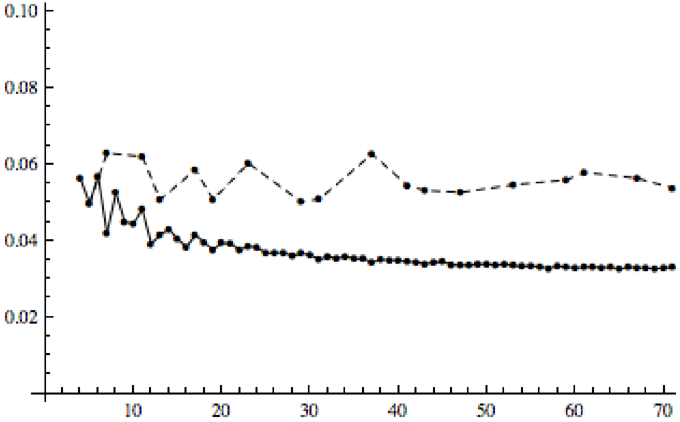

Figure: Comparison optimal with best linear permutations.

- A **permutation polynomial** is a polynomial that acts as a permutation P of the elements of a finite field.
- Carlitz (1953) proved that every permutation P in base p can be represented by a polynomial

$$P_n(x) = (\dots((a_0 x + a_1)^{p-2} + a_2)^{p-2} \dots + a_n)^{p-2} + a_{n+1},$$

  for some $n \geq 0$.
- Defining $P_0(x) := a_0 x + a_1$, the above can be written as $P_n(x) = (P_{n-1}(x))^{p-2} + a_{n+1}$, for $n \geq 1$.
- The smallest integer n such that P_n defines P is called the *Carlitz rank* of P (Topuzoglu et al., 2009).

Numerical results

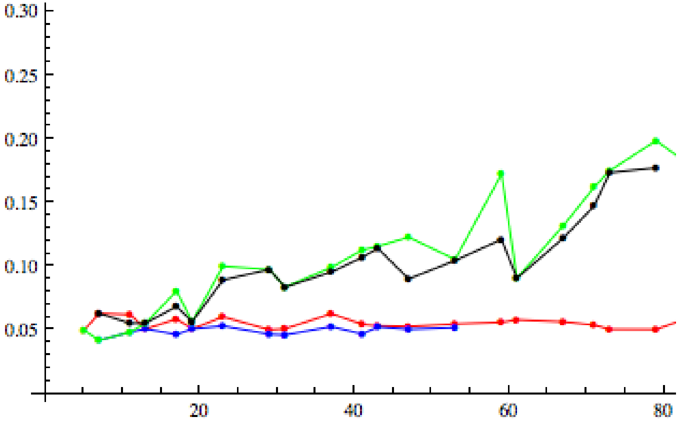

Figure: Comparison of best P_0, P_1, P_2, P_3.

Acknowledgements

- Alev Topuzoglu
- Henri Faure
- Herbert Edelsbrunner