Pseudorandom Sequences II: Exponential Sums and Uniform Distribution

Arne Winterhof

Austrian Academy of Sciences
Johann Radon Institute for Computational and Applied Mathematics
Linz

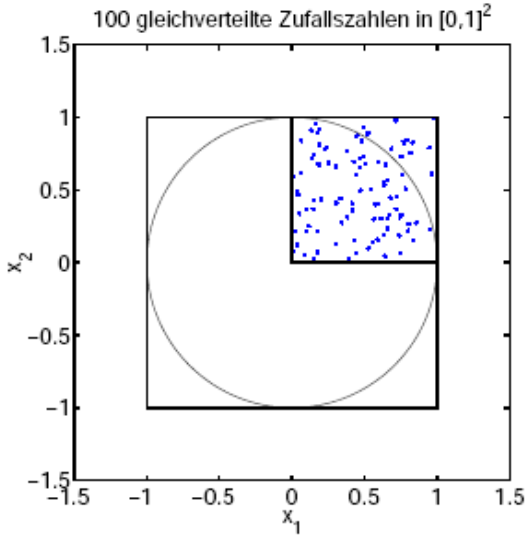
Carleton University 2010

Pseudorandom sequences are generated by a deterministic algorithm and 'look random'.

Desirable 'randomness properties' depend on the application!

cryptography: unpredictability
numerical integration (quasi-Monte Carlo): uniform distribution
radar: distinction from reflected signal
gambling: a good lawyer

Uniform distribution?



k	π
10	3.2000000
100	2.9600000
1000	3.2040000
10000	3.1196000
100000	3.1390000
1000000	3.1460440
10000000	3.1416592

Discrepancy

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

sequence of N points in the s-dimensional unit interval $[0,1)^s$

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

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

$$B = [\alpha_0, \beta_0) \times \cdots \times [\alpha_{s-1}, \beta_{s-1}) \subseteq [0,1)^s$$

and the supremum is taken over all such boxes.

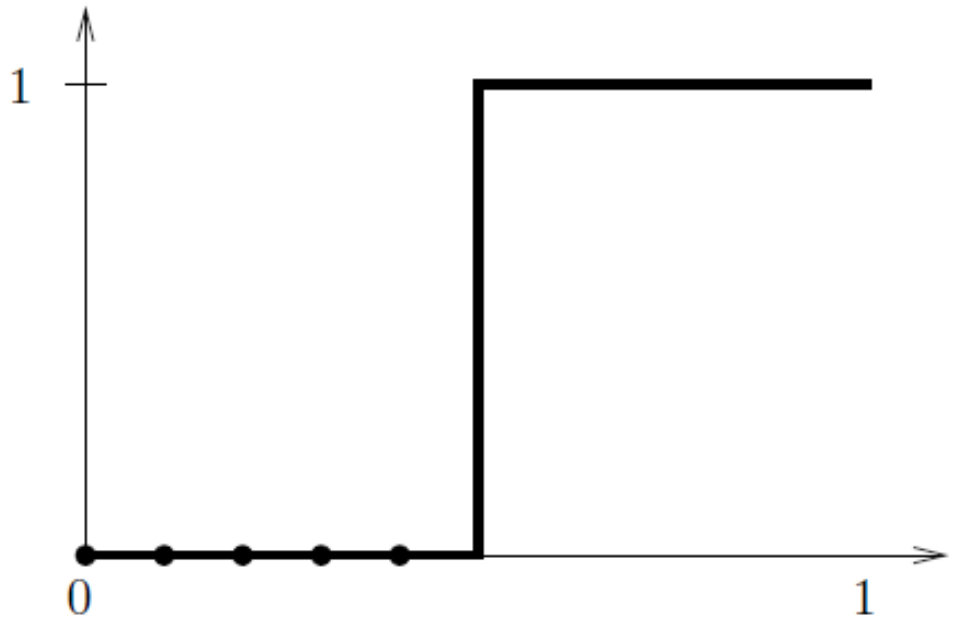
Quasi-Monte Carlo Integration

$\mathbf{x}_0, \ldots, \mathbf{x}_{N-1} \in [0,1)^s$

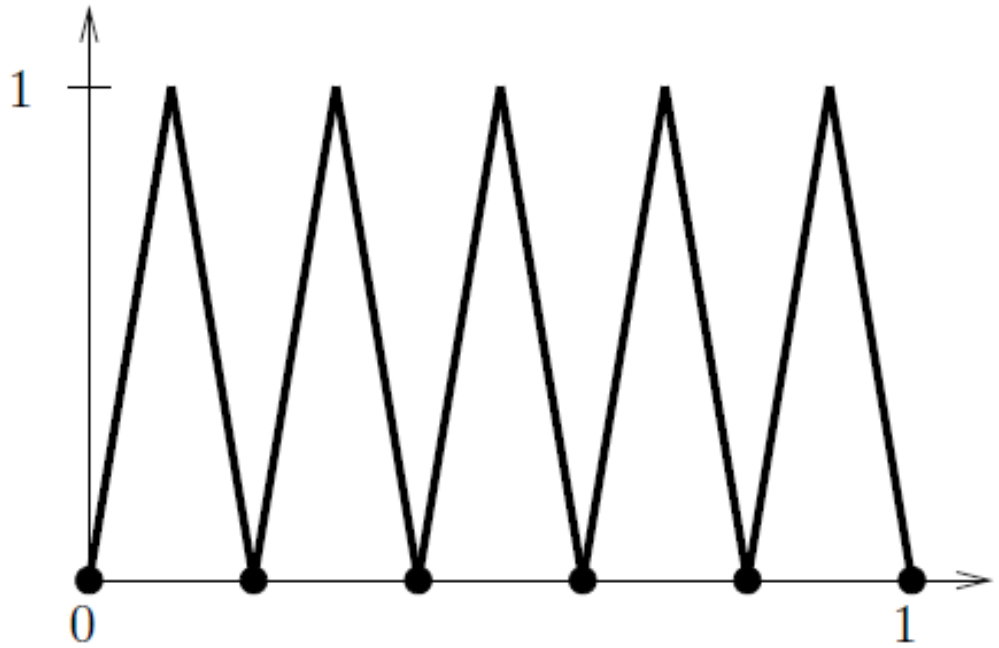
$$\int_{[0,1)^s} f(\mathbf{x}) d\mathbf{x} \sim \frac{1}{N} \sum_{n=0}^{N-1} f(\mathbf{x}_n)$$

How big is the integration error?

$$\left| \int_{[0,1)^s} f(\mathbf{x}) d\mathbf{x} - \frac{1}{N} \sum_{n=0}^{N-1} f(\mathbf{x}_n) \right| = ?$$



Uniform distribution is important!



Bounded variation is important!

Koksma-Hlawka Inequality

$\Gamma = (\mathbf{x}_0, \ldots, \mathbf{x}_{N-1})$

$$\left| \int_{[0,1)^s} f(\mathbf{x}) d\mathbf{x} - \frac{1}{N} \sum_{n=0}^{N-1} f(\mathbf{x}_n) \right| \ll V(f) \Delta(\Gamma),$$

where $V(f)$ is a measure for the variation of f.

How do we estimate the discrepancy?

We estimate the discrepancy using exponential sums (additive character sums).

Erdős-Turan-Koksma inequality

$$\Delta(\Gamma) \leq \left(\frac{3}{2}\right)^s \left(\frac{2}{H+1} + \frac{1}{N} \sum_{0<|\mathbf{a}|\leq H} \prod_{j=0}^{s-1} \frac{1}{\max\{|a_j|,1\}} \left|\Sigma_N^{(s)}(\Gamma,\mathbf{a})\right| \right),$$

where

$$\Sigma_N^{(s)}(\Gamma,\mathbf{a}) = \sum_{n=1}^{N} \exp\left(2\pi i \sum_{j=0}^{s-1} a_j \gamma_{n,j}\right)$$

and the outer sum is taken over all integer vectors $\mathbf{a} = (a_0, \ldots, a_{s-1}) \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$ with $|\mathbf{a}| = \max_{j=0,\ldots,s-1} |a_j| \leq H$.

Group characters

Let $(G, \circ)$ be a finite Abelian group. A mapping

$$\chi : G \to \mathbb{C}^* \quad (\mathbb{F}^* = \mathbb{F} \setminus \{0\})$$

is called a character of G if

$$\chi(g \circ h) = \chi(g)\chi(h) \quad \text{for all } g, h \in G.$$

Example. $\chi_0(g) = 1$ for all $g \in G$ is called the trivial character.

The character group

With the following multiplication of two character χ and ψ is the set of characters $\hat{G}$ a group isomorphic to G:

$$\chi\psi(g) = \chi(g)\psi(g), \quad g \in G.$$

Example. G cyclic of order n with generator g

$$\chi(g^j) = \chi(g)^j$$

$$\chi(g)^n = 1$$

$$\chi_k(g) = \exp(2\pi ik/n), \quad 0 \leq k \leq n-1$$

Orthogonality relation

$$\sum_{g \in G} \chi(g) = 0, \quad \chi \neq \chi_0$$

$$\sum_{\chi \in \hat{G}} \chi(g) = 0, \quad g \neq 1_G$$

$$\frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(g \circ h^{-1}) = \begin{cases} 1, & g = h, \\ 0, & g \neq h. \end{cases}$$

Equations and character sums

Let $f : G^s \to G$ be a mapping and $h \in G$. Let $N(h, f)$ be the number of solutions of

$$f(g_1, \ldots, g_s) = h, \quad (g_1, \ldots, g_s) \in G^s.$$

Then we have

$$\begin{aligned} N(h,f) &= \frac{1}{|G|} \sum_{g_1,\ldots,g_s \in G} \sum_{\chi \in \hat{G}} \chi(f(g_1,\ldots,g_s)h^{-1}) \\ &= |G|^{s-1} + \frac{1}{|G|} \sum_{\chi \neq \chi_0} \chi(h^{-1}) \sum_{g_1,\ldots,g_s \in G} \chi(f(g_1,\ldots,g_s)). \end{aligned}$$

$$|N(h,f) - |G|^{s-1}| < \max_{\chi \neq \chi_0} \left| \sum_{g_1,\ldots,g_s \in G} \chi(f(g_1,\ldots,g_s)) \right|$$

From $\mathbb{F}_q$ to the unit interval

(s_n) sequence over $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$, p prime

$$x_n = s_n/p \in [0, 1)$$

$q = p^r$, $\{\beta_1, \ldots, \beta_r\}$ basis of $\mathbb{F}_q$ over $\mathbb{F}_p$
(s_n) sequence over $\mathbb{F}_q$ with $s_n = s_{n,1}\beta_1 + \ldots + s_{n,r}\beta_r$

$$x_n = s_{n,r}p^{-1} + \ldots + s_{n,1}p^{-r} \in [0, 1)$$

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

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

$$B = [\alpha_0, \beta_0) \times \cdots \times [\alpha_{s-1}, \beta_{s-1}) \subseteq [0,1)^s.$$

$T_\Gamma(B)$ can be expressed in terms of character sums (cf. Erdős-Turan-Koksma).

Characters of finite fields

$\mathbb{F}_q$ finite field of q elements

additive characters: $(G, \circ) = (\mathbb{F}_q, +)$

$q = p$ prime: $\psi_a(x) = \exp(2\pi i a x/p)$, $a \in \mathbb{F}_p$

$q = p^r$, $Tr(x) = x + x^p + \ldots + x^{p^{r-1}}$, $\psi_a(x) = \exp(2\pi i Tr(ax)/p)$

multiplicative characters: $(G, \circ) = (\mathbb{F}_q^*, *)$

g primitive element of $\mathbb{F}_q$ $(\mathbb{F}_q^* = \{g^j : 0 \le j \le q-2\})$

$\chi_k(g^j) = \exp(2\pi i j k/(q-1))$, $0 \le k, j \le q-2$

Example: $\chi_{(q-1)/2}(g^j) = (-1)^j$ quadratic character

$q = p$: $\chi_{(p-1)/2}(x) = \left(\frac{x}{p}\right)$ Legendre symbol

convention: $\chi_k(0) = 0$, $k \neq 0$, $\chi_0(0) = 1$

Character sums

$f, g : \mathbb{F}_q \to \mathbb{F}_q$
χ multiplicative character and ψ additive character of $\mathbb{F}_q$

Complete sum:

$$S(\chi, \psi, f, g) = \sum_{x \in \mathbb{F}_q} \chi(f(x))\psi(g(x))$$

Incomplete sum: $X \subset \mathbb{F}_q$

$$S(\chi, \psi, f, g, X) = \sum_{x \in X} \chi(f(x))\psi(g(x))$$

Trivial bound: $|S(\chi, \psi, f, g, X)| \leq |X|$

Complete sums

Weil-bound: Let $f, g \in \mathbb{F}_q[X]$, χ a multiplicative character and ψ and additive character of $\mathbb{F}_q$. If χ is nontrivial of order $s > 1$ and f is not of the form $f = au^s$, $a \in \mathbb{F}_q^*$, $u \in \mathbb{F}_q[X]$, or ψ is nontrivial and g is not of the form $g = v^p - v + b$, $b \in \mathbb{F}_q$, $v \in \mathbb{F}_q[X]$, then we have

$$|S(\chi, \psi, f, g)| \leq (\deg(f) + \deg(g) - 1)q^{1/2}.$$

Gauss sums

Let χ be a multiplicative and ψ an additive Character of $\mathbb{F}_q$. Then

$$G(\chi,\psi)=\sum_{c\in\mathbb{F}_q^*}\chi(c)\psi(c)$$

are called *Gauss sums*.

If χ and ψ are both nontrivial, we have

$$|G(\chi,\psi)|=q^{1/2}.$$

$$
\begin{aligned}
|G(\chi,\psi)|^2 &= G(\chi,\psi)\overline{G(\chi,\psi)} \\
&= \sum_{c,d\in\mathbb{F}_q^*} \chi(\underbrace{cd^{-1}}_{u})\psi(c-d) \\
&= \sum_{u\in\mathbb{F}_q^*} \chi(u) \sum_{c\in\mathbb{F}_q^*} \psi(c(1-u^{-1})) \\
&= -\sum_{u\neq 0,1} \chi(u) + q - 1 = q
\end{aligned}
$$

Gauss sums Type II

$$S_n(\psi) = \sum_{c \in \mathbb{F}_q^*} \psi(c^n), \quad n|q-1$$

Let χ be a multiplicative character of order n:

$$\frac{1 + \chi(x) + \chi^2(x) + \ldots + \chi^{n-1}(x)}{n} = 1 \Longleftrightarrow \chi(x) = 1 \Longleftrightarrow x = c^n$$

and 0 otherwise.

$$|S_n(\psi)| = \left| \sum_{j=0}^{n-1} G(\chi^j, \psi) \right| \leq (n-1)q^{1/2}$$

Incomplete sums over intervals

Main Idea: Reduce to complete sums and apply, say, the Weil bound.

$q = p$ prime, χ nontrivial multiplicative character of $\mathbb{F}_p$

$$\left|\sum_{n=0}^{N-1} \chi(n)\right| = O(p^{1/2} \log p).$$

Method of Polya and Vinogradov:

$$\begin{aligned}\left|\sum_{n=0}^{N-1} \chi(n)\right| &= \left|\sum_{n=0}^{N-1} \sum_{x\in\mathbb{F}_p} \chi(x) \frac{1}{p} \sum_{\psi} \psi(x-n)\right| \\ &\leq \frac{1}{p} \sum_{\psi} \underbrace{\left|\sum_{x\in\mathbb{F}_p} \chi(x)\psi(x)\right|}_{\leq p^{1/2}} \left|\sum_{n=0}^{N-1} \psi(n)\right|\end{aligned}$$

Vinogradov's inequality:

$$\begin{aligned}
& \sum_{\psi \neq \psi_0} \left| \sum_{n=0}^{N-1} \psi(n) \right| \\
= & \sum_{a=1}^{p-1} \left| \frac{\exp(2\pi i a N/p) - 1}{\exp(2\pi i a/p) - 1} \right| \\
\ll & \sum_{a=1}^{p-1} \frac{1}{\sin(\pi i a/p)} \ll p \sum_{a=1}^{p-1} \frac{1}{\min\{a, p-a\}} \\
\ll & \; p \int_1^p \frac{dx}{x} = p \log p
\end{aligned}$$

Linear Pseudorandom Number Generators

$\mathbb{F}_q$ finite field of q elements, $a, b, x_0 \in \mathbb{F}_q$, $a \neq 0$

$$\boxed{x_{n+1} = ax_n + b, \quad n \geq 0}$$

Corresponding exponential sums are *Gauss sums*.

Nonlinear recurrence sequences

$u_0 \in \mathbb{F}_p$, $f \in \mathbb{F}_p[X]$, $d = \deg(f) \geq 2$

$$u_{n+1} = f(u_n), \quad n \geq 0$$

(purely) periodic with period $t \leq q$

$$S_N = \sum_{n=0}^{N-1} \psi(u_n) = O(N^{1/2} p^{1/2} (\log p)^{-1/2})$$

Polya-Vinogradov fails!

Extend and conquer

$X, Y \subseteq \mathbb{F}_q$

$$\left| \sum_{x \in X} \sum_{y \in Y} \psi(xy) \right| \leq (|X||Y|q)^{1/2}$$

$$\left|\sum_{x\in X}\sum_{y\in Y}\psi(xy)\right|^2 \leq \left(\sum_{x\in X}\left|\sum_{y\in Y}\psi(xy)\right|\right)^2 \quad \text{Cauchy-Schwarz}$$

$$\leq |X|\sum_{x\in X}\left|\sum_{y\in Y}\psi(xy)\right|^2 \quad \text{extend}$$

$$\leq |X|\sum_{x\in \mathbb{F}_q}\left|\sum_{y\in Y}\psi(xy)\right|^2 \quad \text{conquer}$$

$$= |X|\sum_{y_1,y_2\in Y}\sum_{x\in\mathbb{F}_q}\psi(x(y_1-y_2)) = |X||Y|q$$

Clone

$$\left|\sum_{n=0}^{N-1}\psi(u_n)-\sum_{n=0}^{N-1}\psi(u_{n+k})\right|\leq 2k$$

$$K|S_N|\leq\left|\sum_{n=0}^{N-1}\sum_{k=0}^{K-1}\psi(u_{n+k})\right|+\underbrace{2\sum_{k=0}^{K-1}k}_{<K^2}$$

Nonlinear Pseudorandom Numbers

$f \in \mathbb{F}_q[X]$, $2 \leq \deg(f) \leq q-1$, $x_0 \in \mathbb{F}_q$

$$\boxed{u_{n+1} = f(u_n), \quad n \geq 0}$$

$$S_N = \sum_{n=0}^{N-1} \psi(u_n)$$

Niederreiter/Shparlinski, 1999:

$$S_N = O\left(N^{1/2} p^{1/2} \log(d)^{1/2} \log(p)^{-1/2}\right)$$

Main idea of proof:
Reduction to Weil-bound via cloning and extend and conquer:

$$\left|\sum_{x \in \mathbb{F}_q} \psi(F(x))\right| \leq (\deg(F) - 1) q^{1/2}$$

Here:

$$F(X) = \sum a_i F_{k_i}(X)$$

Exponential degree growth when iterating $f(X)$ is the reason for the weakness of these bounds. (Cf. linear complexity bounds.)

Inversive Generators

$a, b, y_0 \in \mathbb{F}_q$, $a \neq 0$

$$y_{n+1} = a y_n^{q-2} + b = \begin{cases} a y_n^{-1} + b, & y_n \neq 0, \\ b, & y_n = 0. \end{cases}$$

Niederreiter/Shparlinski, 2001:

$$D_N = O(N^{-1/2} p^{1/4} \log^s(p))$$

Reason for better result:
$f(X) = \frac{bX+a}{X}$, $F_j(X) = \frac{a_j X + b_j}{c_j X + d}$

Dickson and Power Generator

The Dickson polynomial $D_e(X, a) \in \mathbb{F}_q[X]$ is defined by the following recurrence relation

$$D_e(X, a) = XD_{e-1}(X, a) - aD_{e-2}(X, a), \quad e = 2, 3, \ldots,$$

with initial values

$$D_0(X, a) = 2, \quad D_1(X, a) = X,$$

where $a \in \mathbb{F}_q$. Obviously, the degree of D_e is e. Moreover, if $a \in \{0, 1\}$ then we have $D_e(D_f(X, a), a) = D_{ef}(X, a)$.

$a = 0$:
$D_e(X, 0) = X^e$, $e \geq 2$

$$p_{n+1} = p_n^e, \quad n \geq 0$$

power generator

power generator: Friedlander/Shparlinski, 2001
Reason for better result: $F_k(X) = X^{e^k \mod p-1}$

$a = 1$:

$$u_{n+1} = D_e(u_n, 1), \quad n \geq 0,$$

with some initial value u_0 and $e \geq 2$.
Dickson generator

Dickson generator: Gomez/Gutierrez/Shparlinski, 2006

Redéi generator

Suppose that

$$r(X) = X^2 - \alpha X - \beta \in \mathbb{F}_p[X]$$

is an irreducible quadratic polynomial with the two different roots ξ and $\zeta = \xi^p$ in $\mathbb{F}_{p^2}$. Then any polynomial $b(X) \in \mathbb{F}_{p^2}[X]$ can uniquely be written in the form $b(X) = g(X) + h(X)\xi$ with $g(X), h(X) \in \mathbb{F}_p[X]$. We consider the elements

$$(X + \xi)^e = g_e(X) + h_e(X)\xi.$$

e is the degree of the polynomial $g_e(X)$, and $h_e(X)$ has degree at most $e - 1$. The Rédei function $f_e(X)$ of degree e is then given by

$$f_e(X) = \frac{g_e(X)}{h_e(X)}.$$

$$u_{n+1} = f_e(u_n), \quad n \geq 0,$$

with a Rédei permutation $f_e(X)$ and some initial element $u_0 \in \mathbb{F}_p$.

Redéi generator: Gutierrez/W., 2007

p-Weight Degree

n nonnegative integer
p-weight of n:

$$\sigma_p\left(\sum_{i=0}^{l} n_i p^i\right) = \sum_{i=0}^{l} n_i, \quad 0 \le n_i < p.$$

$0 \le e_1 < e_2 < \cdots < e_l$ integers, $q = p^r$, $f(X) = \sum_{i=1}^{l} \gamma_i X^{e_i} \in \mathbb{F}_q[X]$ nonzero polynomial over $\mathbb{F}_q$ with $\gamma_i \neq 0$, $i = 1, \ldots, l$
p-weight degree of f:

$$\mathrm{w}_p(f) = \max\{\sigma_p(e_i) : 1 \le i \le l\}.$$

$\mathrm{w}_p(f) \le \deg(f)$

If $g(X) \in \mathbb{F}_q[X]$ and $\{\beta_1, \ldots, \beta_r\}$ is a fixed ordered $\mathbb{F}_p$-basis of $\mathbb{F}_q$, we define

$$G(X_1, \ldots, X_r) = \mathrm{Tr}(g(X_1\beta_1 + \ldots + X_r\beta_r)),$$

where $\mathrm{Tr}(X) = X + X^p + \ldots + X^{p^{r-1}}$ is the absolute trace function of $\mathbb{F}_q$. Then the transformed polynomial $G_R(X_1, \ldots, X_r)$ of $g(X)$ is the unique polynomial with all local degrees smaller than p such that

$$G_R(X_1, \ldots, X_r) \equiv G(X_1, \ldots, X_r) \mod (X_1^p - X_1, \ldots, X_r^p - X_r).$$

The interest of this construction relies on the fact that, under certain assumptions, the total degree of $G_R(X_1, \ldots, X_r)$ coincides with the p-weight degree of $g(X)$.

Instead of univariate Weil-bound

$$\left|\sum_{x\in\mathbb{F}_q}\psi_q(g(x))\right| \leq (\deg(g)-1)q^{1/2}$$

we apply the multivariate Weil-bound

$$\left|\sum_{x_1,\ldots,x_r\in\mathbb{F}_p}\psi_p((G_R(x_1,\ldots,x_r))\right| \leq (w_p-1)p^{r-1/2}$$

(Ibeas/W., 2010)

$$f(X) = \alpha X^d + \tilde{f}(X) \in \mathbb{F}_q[X] \quad \text{with} \quad \alpha \neq 0, \quad w_p(\tilde{f}) < \sigma_p(d), \quad d \geq 2, \tag{1}$$

and

$$\gcd\left(d, \frac{q-1}{p-1}\right) \leq \sigma_p(d)^r. \tag{2}$$

If the sequence (x_n) defined by $x_{n+1} = f(x_n)$, $n \geq 0$, $x_0 \in \mathbb{F}_q$, with $f(X) \in \mathbb{F}_q[X]$ of the form (1) satisfying (2) is purely periodic with period t, then

$$S_{\mathbf{a},N}(f) \ll N^{1/2} q^{1/2} (\log w)^{1/2} / (\log p)^{1/2}, \quad 1 \leq N \leq t, \quad \mathbf{a} \neq \mathbf{0},$$

where $w = \sigma_p(d) > 1$ is the p-weight degree of $f(X)$ and the implied constant depends only on s.

Polynomial Systems

Let $\{F_1, \ldots, F_r\}$ be a system of $r \geq 2$ polynomials $F_i \in \mathbb{F}_q[X_i, \ldots, X_m]$, $i = 1, \ldots, r$, defined in the following way:

$$
\begin{aligned}
F_1(X_1, \ldots, X_r) &= X_1 G_1(X_2, \ldots, X_r) + H_1(X_2, \ldots, X_r), \\
F_2(X_1, \ldots, X_r) &= X_2 G_2(X_3, \ldots, X_r) + H_2(X_3, \ldots, X_r), \\
&\ldots \\
F_{r-1}(X_1, \ldots, X_r) &= X_{r-1} G_{r-1}(X_r) + H_{r-1}(X_r), \\
F_r(X_1, \ldots, X_r) &= g_r X_r + h_r.
\end{aligned}
$$

Using the following vector notation

$$\vec{F} = (F_1(X_1, \ldots, X_r), \ldots, F_r(X_1, \ldots, X_r)),$$

we define the following vector sequence

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

(Ostafe, Shparlinski 2009)

Open Problem

Find more good nonlinear generators.

Thank you for your attention.