Pseudorandom Binary Sequences Over Fields of Characteristic 2

János Folláth

follathj@inf.unideb.hu

University of Debrecen

Pseudorandom generators

- Practical
  - Classical
  - Derived from a block cipher
- Theoretical
  - Reductionist
  - Pseudorandomness measures

Well-distribution

Definition 1 *The well-distribution measure of E_N is defined as*

$$W(E_N) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right|,$$

where the maximum is taken over all a, b, t with $a, b, t \in \mathbb{N}, 1 \leq a + b \leq a + tb \leq N$.

Correlation

Definition 2 *The correlation measure of order k of E_N is:*

$$C_k(E_N) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_k} \right|,$$

where the maximum is taken over all $D = (d_1, \ldots, d_k)$ ($d_1 < \ldots < d_k$ are non-negative integers) and $M \in \mathbb{N}$ with $M + d_k \leq N$.

Combined measure

Definition 3 *Combined (well-distribution-correlation) PR-measure of order k of E_N is defined as:*

$$Q_k(E_N) = \max_{a,b,t,D} |Z(a,b,t,D)|$$

where

$$Z(a,b,t,D) = \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \cdots e_{a+jb+d_k} \right| .$$

Legendre symbol

Theorem 1 *Let p be an odd prime, $\lambda \in \mathbb{F}_p^*$ be of multiplicative order T and $f(x) \in \mathbb{F}_p[x]$ be of degree k and not of the form $cx^\alpha (g(x))^2$ with $c \in \mathbb{F}_p, \alpha \in \mathbb{N}, g(x) \in \mathbb{F}_p[x]$. Define the sequence $E_T = \{e_1, \ldots, e_T\}$ by*

$$e_n = \begin{cases} \left(\frac{f(\lambda^n)}{p}\right) & if \;\; p \nmid f(\lambda^n), \\ 1 & if \;\; p \mid f(\lambda^n). \end{cases}$$

Then we have

$$W(E_T) < 5kp^{1/2} \log p$$

Moreover, assume that also $l \in \mathbb{N}$, T is a prime, and either $\min\{(4k)^l, (4l)^k\} \leq T$ or 2 is a primitive root modulo T. Then we also have

$$C_l(E_T) \leq 5klp^{1/2} \log p.$$

Additive based

Theorem 2 *Let p an odd prime, $f(x) \in \mathbb{F}_p[x]$ of degree d, and define $E_p = \{e_1, \ldots, e_p\}$ by*

$$e_n = \begin{cases} +1 & if \ \ 0 \leq r_p(f(n)) < p/2, \\ -1 & if \ \ p/2 \leq r_p(f(n)) < p \end{cases}$$

where $r_p(n)$ denotes the unique $r \in \{0, \ldots, p-1\}$ such that $n \equiv r \pmod{p}$. Then we have

$$W(E_p) \ll dp^{1/2}(\log p)^2.$$

For $2 \leq l \leq d-1$ we also have

$$C_l(E_p) \ll dp^{1/2}(\log p)^{l+1}.$$

Double twist

- Enumeration of the elements:
  - Natural enumeration
  - Permutation polynomials
  - “Good” polynomials
- Destruction of the arithmetical structure:
  - Legendre symbol
  - Additive characters

Characters of $\mathbb{F}_q$

Theorem 3 *For $b \in \mathbb{F}_q$, the function $\chi_b(c) = e^{2\pi i Tr(bc)/p}$ for all $c \in \mathbb{F}_q$ is an additive character of $\mathbb{F}_q$ and every additive character of $\mathbb{F}_q$ is obtained this way.*

Theorem 4 *Let g be a fixed primitive element of $\mathbb{F}_q$. For each $j = 0, 1, \ldots, q-2$, the function ψ_j with*

$$\psi_j(g^k) = e^{2\pi i jk/(q-1)} \text{ for } k = 0, 1, \ldots, q-2$$

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

Pseudorandomness measure

Theorem 5 *Let $\mathbb{F}_q$ be a finite field of characteristic two and its multiplicative group of prime order. Let χ be a non principal additive character, and α a primitive element of $\mathbb{F}_q$ and let $f(x) \in \mathbb{F}_q[x]$ of odd degree d and let I be the set of exponents with nonzero coefficient in $f(x)$. For the minimal polynomial of α^i over $\mathbb{F}_2$ write $m_i(x)$. Let*

$$E_{q-1} = \{\chi(f(\alpha^1)), \chi(f(\alpha^2)), \ldots, \chi(f(\alpha^{q-1}))\} \in \{-1, +1\}^{q-1},$$

Let $D' \subseteq \{1, \ldots, q-1\}$ such that $\prod_{i \in I} m_i(x)$ doesn't divide the polynomial $d(x) = \sum_{d_i \in D'} x^{d_i}$,then

$$Q'_k(E_N) = \max_{a,b,t,D'} |Z(a,b,t,D')| \leq 9dq^{1/2} \log q.$$

Let $D \subseteq \{1, \ldots, q-1\}$ such that $\prod_{i \in I} m_i(x)$ divides the polynomial $d(x) = \sum_{d_i \in D} x^{d_i}$,then

$$Q_k(E_N) = \max_{a,b,t,D} |Z(a,b,t,D)| = \max_{D}(q - 1 - \max_{d_i \in D} d_i).$$

The generator

Theorem 6 *Let $\mathbb{F}_q$ be a finite field of characteristic two and its multiplicative group of prime order. Let χ be a non principal additive character, and α a primitive element of $\mathbb{F}_q$ and let $f(x) \in \mathbb{F}_q[x]$ of odd degree $d \geq \log q$ and let the coefficients of its terms be zero if and only if the term has an even exponent. If*

$$E_{q-1} = \{\chi(f(\alpha^1)), \chi(f(\alpha^2)), \ldots, \chi(f(\alpha^{q-1}))\},$$

then :

$$\max_{k \leq \log(q-1)} Q_k(E_N) \leq 9dq^{1/2} \log q.$$

Parameters

1. Variable χ with fixed α and $f(x)$
2. Variable α with fixed χ and $f(x)$
3. Variable $f(x)$ with fixed α and χ

Thank you for your attention!

References

[1] R. Lidl and H. Niederreiter “Finite Fields”, Encyclopedia of Mathematics and its Applications, vol. 20, 1997

[2] Mauduit, C. and Sárközy, A. 1997. “ On finite pseudorandom sequences I: Measure of pseudorandomness, the legendre symbol. ” Acta Arithmetica 82, 4, 365-377.

[3] Schmidt, W. 1976. “Equations over finite fields. An elementary approach.” Lecture notes in Mathematics vol. 536. Springer-Verlag.

[4] Mauduit, C. and Sárközy, A. 2005. “Construction of pseudorandom binary sequences by using the multiplicative inverse.” Acta Math. Hungar. 108 no. 3, 239-252.

[5] Mauduit, C.; Rivat, J. and Sárközy, A. 2004. “Construction of pseudorandom binary sequences using additive characters.” Monatsh. Math. 141 no. 3, 197-208.

[6] Weil, A. 1948. “Sur les courbes algébriques et les variétés qui s’en déduisent” Acta Sci Ind. Vol. 1041, Hermann, Paris,

[7] Goubin, L.; Mauduit, C. and Sárközy, A. 2004. “Construction of large families of pseudorandom binary sequences.” J. Number Theory 106, no. 1, 56-69.

[8] Gyarmati, K.; Pethő, A. and Sárközy, A. 2005. “On linear recursion and pseudorandomness.” Acta Arith. 118 no. 4, 359-374.