Construction of Pseudorandom Binary Sequences using Additive Characters over GF(2^k)

János Folláth, University of Debrecen

Mauduit and Sárközy studied pseudorandom binary sequences of

$$E_N = \{e_1, \ldots, e_N\} \in \{-1, +1\}^N$$

and introduced the following measures of pseudorandomness of binary sequences [7]:

- 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 $a, b, t \in \mathbb{N}, 1 \le a + b \le a + tb \le N$.
- The correlation measure of order k of E_N is:

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

  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 $M + d_k \le N$.
- Combined (well-distribution-correlation) PR-measure of order k E_N is defined as:

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

  where

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

Later several large families of pseudorandom sequences were presented with good combined pseudorandom measure. The Legendre symbol based construction designed by Goubin, Mauduit and Sárközy [3] is of particular interest: although its security cannot be proven by reduction, many mathematical argument substantiate it. It possesses the strict avalanche property [9], has a high family complexity [1], the computational complexity of the best known attacks are high and it has an extremly fast implementation [4] and the bound on its correlation measure enables one to estimate its linear complexity profile [2]. Accordingly this generator has mathematically substantiated security and still is faster than most provable secure pseudorandom sequence generator.

The above mentioned construction uses multiplicative characters over large prime fields. In this paper a new construction is intruduced wich utilizes fast arithmetic in finite fields with even characteristic in combination with additive characters. The main purpose is to find a pseudorandom binary sequence family with similar good properties as the above mentioned Legendre symbol based construction. In this paper, as a first step, a new construction will be described and its pseudorandom measures will be studied. The following result is a consequence of Weil's theorem ([8],[5]), the Vinogradov inequality ([10]) and the BCH bound ([6]).

Theorem. *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 $d \ge \log q$ and let the coefficients of its terms be zero if and only if the term has an even exponent. If*

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

then :

$$Q(E_N) \le 9dq^{1/2} \log q.$$

References

[1] Rudolf Ahlswede, Levon Khachatrian, Christian Mauduit, and András Sárközy, *A complexity measure for families of binary sequences*, Period. Math. Hungar. **46** (2003), no. 2, 107–118.

[2] Nina Brandstätter and Arne Winterhof, *Linear complexity profile of binary sequences with small correlation measure*, Period. Math. Hungar. **52** (2006), no. 2, 1–8.

[3] Louis Goubin, Christian Mauduit, and András Sárközy, *Construction of large families of pseudorandom binary sequences*, Journal of Number Theory **106** (2004), no. 1, 56–69.

[4] Jeffrey Hoffstein and Daniel Lieman, *Cryptography and computational number theory*, Progress in Computer Science and Applied Logic, vol. 20, ch. The Distribution of the Quadratic Symbol in Function Fields and a Faster Mathematical Stream Cipher, pp. 59–68, Birkhäuser Verlag, 2001.

[5] Rudolf Lidl and Harald Niederreiter, *Finite fields*, Encyclopedia of Mathematics, vol. 20, Cambridge University Press, 1997.

[6] Florence Jessie Collinson MacWilliams and Neil James Alexander Sloane, *The theory of error-correcting codes*, North-Holland Mathematical Library, vol. 16, North-Holland Publishing Company, 1977.

[7] Christian Mauduit and András Sárközy, *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arith. **82** (1997), no. 4, 365–377.

[8] Wolfgang Schmidt, *Equations over finite fields. an elementary approach*, Lecture Notes in Mathematics, vol. 536, Springer-Verlag, 1976.

[9] Viktória Tóth, *Collision and avalanche effect in families of pseudorandom binary sequences*, Period. Math. Hungar. **55** (2007), no. 2, 185–196.

[10] Ivan Matveyevich Vinogradov, *Elements of number theory*, Dover Publications, 2003.