Olexandr Pustovit
Department of ontological systems and applied algebraic combinatorics, Institute of Telecommunications and the Global Information Space of the National Academy of Sciences of Ukraine (ITGIP NAS of Ukraine), Kyiv, Ukraine
Email address: sanyk_set@ukr.net

Key words and phrases. Extremal graphs, Information Security, Post Quantum Cryptography, Message Authentication Codes

Exponential sums on the sequences of inversive congruential pseudorandom numbers with the variable shifts

Pavel Varbanets, Sergey Varbanets

The investigation of the sequences $\{x_n\}$ of pseudorandom numbers under the interval [0,1) can be executed by the estimates of special exponential sums over the sequences of these numbers. A nontrivial estimate of such sum was being obtained by H. Niederreiter in the work [**1**]:

Let $\{x_k\}$ is the linear congruential pseudorandom numbers with the period τ produced by the congruential recursion $x_{n+1} \equiv ax_n + b \pmod m$. Then

$$\left|\sum_{n=0}^{N-1} e^{2\pi i \frac{hx_n}{m}}\right| \le \left(\frac{m\tau}{\ell}\right)^{\frac{1}{2}} \left(\frac{2}{\pi}\log\tau + \frac{3}{4}\right),$$

where $1 \le N \le \tau$; ℓ is the exponent of $a \pmod m$.

In our talk we consider the analogous exponential sum for the sequence $\{x_n\}$ generated by the inversive congruential generators of type

(1) $x_{n+1} \equiv \frac{a}{x_n} + b(n) \pmod{p^m}$,
(2) $x_{n+1} \equiv \frac{a}{x_{n-1}x_n} + b(n) \pmod{p^m}$

with conditions $(a,p) = 1$, $b(n) \equiv 0 \pmod{p^\beta}$ for all $n \in \mathbb{N}$.

Moreover, we use the representations $\{x_n\}$ as a polynomials on n over $\mathbb{Z}_{p^m}$ and derive the nontrivial estimates for "Kloosterman sums" on the sequences of pseudorandom numbers produced by the recursion (1) or (2).

References

1. Niederreiter H., On the distribution of pseudorandom numbers generated by the linear congruential method, III, Math. Comp., 30 (1976), 571-597.

Contact information

Pavel Varbanets
Department of Computer Algebra and Discrete Mathematics, I.I. Mechnikov Odessa National University, Odessa, Ukraine
Email address: varb@sana.od.ua

Sergey Varbanets
Department of Computer Algebra and Discrete Mathematics, I.I. Mechnikov Odessa National University, Odessa, Ukraine
Email address: varb@sana.od.ua

Key words and phrases. Exponential sums, Kloosterman sums, pseudorandom numbers sequences

Inversive congruential generator of the second order with a variable shift

Sergey Varbanets

Our talk is devoted to research of statistical properties of the sequences of pseudorandom numbers produced by the inversive generator of second order

$$y_{n+1} \equiv \frac{a}{y_{n-1}y_n} + b + cF(n) \pmod{p^m}, \tag{1}$$

with $(a,p) = (y_0,p) = (y_1,p) = 1$, $b \equiv c \equiv 0 \pmod{p}$, and $F(n) \in \mathbb{Z}[n]$.

Using the recursion (1) we obtaine the representation

$$y_n = \frac{A_0^{(n)} + A_1^{(n)}y_0 + A_2^{(n)}y_1 + A_3^{(n)}y_0y_1}{B_0^{(n)} + B_1^{(n)}y_0 + B_2^{(n)}y_1 + B_3^{(n)}y_0y_1}, \tag{2}$$

where the coefficients $A_j^{(n)}$, $B_j^{(n)}$, $j = 0,1,2,3$ can be prescribe as the polynomials $f_i(k)$ for $n = 3k+i$, $i = 0,1,2$.

We determinate a period length of the sequence $\{y_n\}$, besides this period reaches a maximum $\tau = 3p^{m-\nu_0-\alpha}$ if $\nu_p(y_0y_1^2 - a) < \nu_p(b) = \alpha$.

Moreover, we prove that the sequence of pseudorandom numbers passes 3-dimensional test on the statistical independence. Obtained results are analogue of similar results for the congruential inversive pseudorandom sequences of the first order investigated in **[1]**,**[2]**.

References

1. H. Niederreiter, *I. Shparlinski Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus.* Acta Arith. 2000. V. 90 N. 1. P. 89-98.
2. S. Varbanets, *Generalizations of Inversive Congruential Generator. Analytic and Probabilistic Methods in Number Theory*, Proceedings of the Fifth International Conference in Honour of J. Kubilius, Palanga, Lithuania, 4-10 September 2011, 2012. P. 265-282.

Contact information

Sergey Varbanets
Department of Computer Algebra and Discrete Mathematics, I.I. Mechnikov Odessa National University, Odessa, Ukraine
Email address: varb@sana.od.ua

Key words and phrases. Congruential generators, pseudorandom numbers sequences, discrepancy