

С. П. Варбанець (Одеський національний університет ім. І.І. Мечникова, Одеса, Україна)

Інверсні конгруентні генератори псевдовипадкових чисел

У 1989 році Eichenauer та Lehn побудували інверсний конгруентний генератор псевдовипадкових чисел

$$y_{n+1} \equiv a\bar{y}_n + b \pmod{p} \quad (1)$$

де a, b, y_0 - фіксовані числа за модулем p , p - просте число, а $\bar{y}_n$ є мультиплікативне обернене для y_n , якщо $(y_n, p) = 1$, і $\bar{y}_n = 0$, якщо $y_n = 0$.

В подальшому генератор (1) узагальнювали різні автори (Eichenauer, Niederreiter, Shparlinski, Emerich Kato, Grothe, Topuzoğlu та інші).

В роботах [1](для $p = 2$), [2, 3](для $p > 2$) досліджувались узагальнення інверсного конгруентного генератору псевдовипадкових чисел (1):

$$\begin{aligned} y_{n+1} &\equiv ay_n^{-1} + b + cy_n \pmod{p^m}, \quad (m \geq 2) \\ (a, p) &= (y_0, p) = 1, \quad b \equiv c \equiv 0 \pmod{p}, \end{aligned} \quad (2)$$

Метою нашої доповіді є дослідження генератору

$$\begin{aligned} y_{n+1} &\equiv ay_n^{-1} + b + c(n+1)y_n \pmod{p^m}, \quad (m \geq 2) \\ (a, p) &= (y_0, p) = 1, \quad b \equiv c \equiv 0 \pmod{p}, \end{aligned} \quad (3)$$

Ми будемо зображення y_{2k} і y_{2k+1} , $k = 0, 1, \dots$, у вигляді многочленів від k .

За допомогою цих зображень ми отримуємо оцінки тригонометричних сум на згенерованій послідовності псевдовипадкових чисел

$$S_N(h_1, \dots, h_s) = \sum_{n=0}^{N-1} e^{2\pi i \frac{h_1 y_n + h_2 y_{n-1} + \dots + h_s y_{n+s-1}}{p^m}}, \quad (4)$$

які дозволяють знайти нетривіальні оцінки функції розкиду

$$D_N(X_0, \dots, X_{N-1}) \leq \frac{s}{p^m} + \frac{1}{p^{\frac{m}{2}-\nu}} \left(1 - \frac{1}{p^\nu} \left(\frac{2}{\pi} \log p^m + \frac{7}{5} \right)^s \right), \quad (5)$$

де $X_n^{(s)} = (x_n, x_{n-1}, \dots, x_{n+s-1})$, $x_n = \frac{y_n}{p^m}$, $s = 1, 2, 3, 4$.

А це означає, що побудована послідовність псевдовипадкових чисел $\{x_n\}$ проходить тести на рівномірність і непередбачуваність.

-
- [1] Kato T., Wu L.-M. and Yanagihara N., On a nonlinear congruential pseudorandom number generator, Math. Comput. 65(213)(1996), 227-233.
 - [2] Varbanets S., Exponential sums on the sequences of inversive congruential pseudorandom numbers, Šiauliai Math. Semin., 3(11)(2008), 247-261.
 - [3] Varbanets S., On inversive congruential generator for pseudorandom numbers with prime power modulus, Annales Univ. Sci. Budapest, Sect. Comp., 29(2008), 277-296.
-