Е.В. Вернигора (Одесский национальный университет им.И.И. Мечникова, Украина)

Составной инверсный конгруэнтный генератор по степени простого модуля

Пусть $p_1,...,p_r$ – различные простые числа, $p_i \geq 5, i = 1,...,r$, и пусть $m_1,...,m_r$ – натуральные числа. Рассмотрим пары чисел (a_i, b_i), такие, что $(a_i, p_i) = 1$, $b_i \equiv 0 (\mathrm{mod}\, p_i)$, $i = 1,...,r$.
Зафиксируем $y_0^{(i)} \in Z_{\mathrm{p}_i^{m_i}}$, $(y_0^{(i)}, p_i) = 1$ и рассмотрим для каждого $i = 1,...,r$ инверсный конгруэнтный генератор

$$G_i: \quad y_{n+1}^{(i)} \equiv \frac{a_i}{y_n^{(i)}} + b_i (\mathrm{mod}\, p_i), \qquad n = 0,1,2,...$$

Генераторы G_i порождают периодические последовательности с периодом $\tau_i \leq 2p_i^{m_i - \nu_i}$, где ν_i - показатель, с которым p_i входит в каноническое разложение b_i. Известно, что если $a_i^2 \not\equiv (y_0^i)^4 (\mathrm{mod}\, p_i)$, то $\tau_i = 2p^{m_i - \nu_i}$.

Зафиксируем $c_i \in Z_{p_i^{m_i}}, (c_i, p_i) = 1$, и рассмотрим рекурсию

$$G_0: \quad z_{n+1}^{(i)} \equiv a_i c_i^2 (z_n^{(i)})^{-1} + c_i b_i (\mathrm{mod}\, p_i^{m_i}), \quad z_0^{(i)} \equiv c_i y_0^{(i)} (\mathrm{mod}\, p_i^{m_i})$$

Тогда последовательность $\{x_n\}$, где

$$x_n \equiv x_n^{(1)} + ... + x_n^{(r)} (\mathrm{mod} 1), \quad n \geq 0,$$

и где $$x_n^{(i)} = \frac{z_n^{(i)}}{p_i^{m_i}},$$

будем называть составной инверсной последовательностью псевдослучайных чисел (PRN), а генератор G_0 - составным инверсным генератором.
Генератор G_0 является обобщением составного инверсного генератора, впервые полученного в работах J.Eichenauer [1-3].
Целью нашего исследования, было построение верхней и нижней оценок discrepancy function на части периода для двух последовательностей s-мерных точек.

$x_n = (x_{sn}, x_{sn+1}, ..., x_{sn+s-1}) \in [0,1)^s$ (“non-overlapping” points)

$\widetilde{x}_n = (x_n, x_{n+1}, ..., x_{n+s-1}) \in [0,1)^s$ (“overlapping” points).

Доказано, что для «почти всех» наборов $c_1,...,c_r$ справедливы неравенства

$$(2\sqrt{s})^r N^{-\frac{1}{2}} << D_N^{(s)}(x_0,...,x_{N-1}) << (2\sqrt{s})^r N^{-\frac{1}{2}} (\log \tau)^r,$$

где $$\tau = 2p_1^{m_1 - \nu_1} ... p_r^{m_r - \nu_r}, \qquad N >> \tau^{\frac{1}{2}},$$

$$D_N^{(s)}(x_0,...,x_{N-1}) := \sup_{\Delta\subset[0,1)^s}\left|\frac{A_N(\Delta)}{N}-|\Delta|\right|$$

$A_N(\Delta)$ - число точек последовательности $x_0,x_1,...,x_{N-1}$, попавших в параллелепипед Δ;
$|\Delta|$ - объем Δ, и sup берется по всем Δ из $[0,1)^s$.
Аналогичные оценки справедливы и для точек $\widetilde{x}_n$, если $s < \min(p_1,...,p_r)$.

[1] J.Eichenauer-Herrmann, Compound nonlinear congruential pseudorandom numbers, Monats. Math., 117(1994), 213-222.
[2] J.Eichenauer-Herrmann and F.E. Emmerich, Compound inversive congruential pseudorandom numbers: An average case analysis, Math. Comput., 65(1996), 215-225.
[3] J.Eichenauer-Herrmann, F.E. Emmerich and G.Larcher, Average discrepancy, hyperplanes and compound pseudorandom numbers, Finite Fields Appl., 3(1997), 203-218.