Eichenauer-Herrmann, Jürgen

Equidistribution properties of nonlinear congruential pseudorandom numbers. (English)

Zbl 0787.65003

Metrika 40, No. 6, 333-338 (1993).

Let $p \geq 5$ be a prime and identify $\mathbb{Z}_p := \{0, 1, \dots, p-1\}$ with the finite field of order p. Let $\gamma \in \mathbb{Z}_p \backslash \{0\}$, $g : \mathbb{Z} \to \mathbb{Z}_p$ be a monic permutation polynomial of $\mathbb{Z}_p$ with degree s as a polynomial over $\mathbb{Z}_p$, where $3 \leq s \leq p-2$. Define a sequence of elements of $\mathbb{Z}_p$: $(y_n)_{n \geq 0}$ by $y_n \equiv \gamma g(n) (\bmod p)$, $n \geq 0$, and let $x_n = y_n/p$ $(n \geq 0)$. The author proves that the discrepancy D_N of the sequence of nonlinear congruential pseudorandom numbers $\{x_0, x_1, \dots, x_{N-1}\}$ $(1 \leq N < p)$ satisfies

$$D_N < (s-1)\frac{p^{1/2}}{N}\left(\frac{4}{\pi^2}\log p + 0.38 + \frac{0.608}{p} + \frac{0.116}{p^2}\right)^2 + \frac{1}{p},$$

and also shows that this upper bound for D_N is best possible up to the logarithmic factor. This estimate slightly improves the result of *H. Niederreiter* [Monatsh. Math. 106, No. 2, 149-159 (1988; Zbl 0652.65007)].

Reviewer: Zhu Yaochen (Beijing)

MSC:

65C10 Random number generation in numerical analysis
11K45 Pseudo-random numbers; Monte Carlo methods
11K38 Irregularities of distribution, discrepancy

Cited in **3** Documents

Keywords:

finite field; discrepancy; sequence of nonlinear congruential pseudorandom numbers

Full Text: DOI EuDML

References:

[1] Chung KL (1949) An estimate concerning the Kolmogoroff limit distribution, Trans. Amer. Math. Soc. 67:36–50 · Zbl 0034.22602

[2] Cochrane T (1987) On a trigonometric inequality of Vinogradov, J. Number Th. 27:9–16 · Zbl 0629.10030 · doi:10.1016/0022-314X(87)90045-X

[3] Eichenauer J, Grothe H, Lehn J (1988) Marsaglia's lattice test and non-linear congruential pseudo random number generators, Metrika 35:241–250 · Zbl 0653.65006 · doi:10.1007/BF02613312

[4] Eichenauer-Herrmann J (1992) Inversive congruential pseudorandom numbers: a tutorial, Int. Statist. Rev. 60:167–176 · Zbl 0766.65002 · doi:10.2307/1403647

[5] Eichenauer-Herrmann J, Niederreiter H (1992) On the statistical independence of nonlinear congruential pseudorandom numbers (submitted for publication) · Zbl 0762.65001

[6] Lidl R, Niederreiter H (1983) Finite fields, Addison-Wesley, Reading, Mass. · Zbl 0554.12010

[7] Niederreiter H (1988a) Remarks on nonlinear congruential pseudorandom numbers, Metrika 35: 321–328 · Zbl 0663.65005 · doi:10.1007/BF02613320

[8] Niederreiter H (1988b) Statistical independence of nonlinear congruential pseudorandom numbers, Monatsh. Math. 106:149–159 · Zbl 0652.65007 · doi:10.1007/BF01298835

[9] Niederreiter H (1990) Lower bounds for the discrepancy of inversive congruential pseudorandom numbers, Math. Comp. 55:277–287 · Zbl 0708.65006 · doi:10.1090/S0025-5718-1990-1023766-0

[10] Niederreiter H (1991) Recent trends in random number and random vector generation, Ann. Operations Res. 31:323–345 · Zbl 0737.65001 · doi:10.1007/BF02204856

[11] Niederreiter H (1992a) Nonlinear methods for pseudorandom number and vector generation. In: Pflug, G. and Dieter, U. (eds.) Simulation and Optimization, Lecture Notes in Economics and Math. Systems 374:145–153, Springer, Berlin · Zbl 0849.11055

[12] Niederreiter H (1992b) Random number generation and quasi-Monte Carlo methods, SIAM, Philadelphia · Zbl 0761.65002

[13] Niederreiter H (1992c) Pseudorandom numbers and quasirandom points, Z. Angew. Math. Mech. (to appear) · Zbl 0796.11028

[14] Weil A (1948) On some exponential sums, Proc. Nat. Acad. Sci. U.S.A. 34:204–207 · Zbl 0032.26102 · doi:10.1073/pnas.34.5.204