

Eichenauer-Herrmann, Jürgen; Niederreiter, Harald

Lower bounds for the discrepancy of inversive congruential pseudorandom numbers with power of two modulus. (English) [Zbl 0762.65001](#)
Math. Comput. 58, No. 198, 775-779 (1992).

The discrepancy $D_{m/2}^{(k)}$ of k -tuples of consecutive pseudorandom numbers generated by the inversive congruential method with modulus $m = 2^\omega$ with maximum period length $m/2$ is studied. It is shown that for a given modulus m there exist multipliers in the inversive congruential method such that $D_{m/2}^{(k)}$ is at least of the order of magnitude $m^{-1/2}$ for all dimensions $k \geq 2$ and all increments b . Therefore, the upper bound $D_{m/2}^{(2)} = O(m^{-1/2}(\log m)^2)$ is in general best possible up to the logarithmic factor.

Reviewer: V.Burjan (Praha)

MSC:

65C10 Random number generation in numerical analysis
11K45 Pseudo-random numbers; Monte Carlo methods

Cited in **13** Documents

Keywords:

lower bounds; pseudorandom number generator; power of two modulus; discrepancy; pseudorandom numbers; inversive congruential method

Full Text: [DOI](#)

References:

- [1] Jürgen Eichenauer and Jürgen Lehn, A nonlinear congruential pseudorandom number generator, Statist. Hefte 27 (1986), no. 4, 315 – 326. · [Zbl 0607.65001](#)
- [2] Jürgen Eichenauer, Jürgen Lehn, and Alev Topuzoğlu, A nonlinear congruential pseudorandom number generator with power of two modulus, Math. Comp. 51 (1988), no. 184, 757 – 759. · [Zbl 0701.65008](#)
- [3] Harald Niederreiter, The serial test for congruential pseudorandom numbers generated by inversions, Math. Comp. 52 (1989), no. 185, 135 – 144. · [Zbl 0657.65007](#)
- [4] Harald Niederreiter, Lower bounds for the discrepancy of inversive congruential pseudorandom numbers, Math. Comp. 55 (1990), no. 191, 277 – 287. · [Zbl 0708.65006](#)
- [5] Hans Salié, Über die Kloostermanschen Summen $\sum_{n=1}^m e^{2\pi i n^2 x/m}$, Math. Z. 34 (1932), no. 1, 91 – 109 (German). · [Zbl 0002.12801](#) · [doi:10.1007/BF01180579](#)

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.