Math Meth Oper Res (2003) 57:41–48

Mathematical Methods
of Operations Research

Using an adaptive genetic algorithm with reversals to find good second-order multiple recursive random number generators

Hui-Chin Tang

Department of Industrial Engineering and Management, National Kaohsiung University of Applied Sciences, Kaohsiung 807, Taiwan (E-mail: tang@cc.csit.edu.tw)

Manuscript received: March 2002/Final version received: August 2002

Abstract. This paper considers the problem of searching for good second-order multiple recursive generators (MRGs) with long period and good lattice structure. An adaptive genetic algorithm with reversals is proposed. The proposed algorithm is compared with forward/backward and random methods, and its effectiveness and efficiency is numerically confirmed by the experiments. The extensively tested second-order MRG (1259791845, 1433587751) found from the proposed algorithm possesses the properties of long period and good lattice structure and is therefore recommended.

Key words: Genetic algorithm, Multiple recursive generator, Random number, Statistics

1. Introduction

For the requirements of long sequence, reproduction, and verification in applications, it is preferable to use deterministic functions that random numbers (RNs) can be generated directly in the computer. The method of deterministic RN generator seems to have been proposed first by Lehmer [17]. Since then, a large variety of methods have been developed in an attempt to devise ideal RN generators. Important methods may be categorized into five classes (i) multiple recursive generator (MRG), (ii) generalized feedback shift register generator, (iii) add-with carry and subtract-with-borrow generator, (iv) combined generator, and (v) inverse generator. For more details, see Fishman [6], Knuth [11], and Niederreiter [19]. This paper deals with the MRG proposed initially by Knuth. L'Ecuyer and Blouin [14] performed the first practical implementation. Later, the MRG literature has grown explosively. A kth-order MRG is based on the following formula:

$$X_n \equiv a_1 X_{n-1} + a_2 X_{n-2} + \cdots + a_k X_{n-k} \pmod{m}, \tag{1}$$

where modulus m is usually chosen to be the largest prime number less than the computer's word size, a_k and at least one multiplier $a_{j\neq k}$ are not zero, and starting values $X_0, X_1, \ldots, X_{k-1}$ are not all zero.

In designing an ideal MRG, the sets of multipliers $(a_1, a_2, \ldots, a_k)$ with long period and high spectral value are sought. Several articles have addressed this issue and three approaches have been devised: exhaustive search (ES) proposed by Fishman and Moore [7], random search (RS) proposed by L'Ecuyer, Blouin, and Couture [15], and forward/backward search (FBS) proposed by Kao and Tang [10]. In fact, searching for full period MRGs with maximum spectral value criterion is a rather difficult task. We have two reasons to believe that this task is a combinatorial optimization problem (COP). One is that the number of possible sets of multipliers is usually large enough so that an ideal kth-order MRG with modulus $2^{31} - 1$, when $k \geq 2$, has not been reported to date. The other reason is that the corresponding nonconvex multimodal objective function (spectral value) is very bump. As a result, heuristic methods are often used. Recent developments in heuristic methodology include simulated annealing, genetic algorithm (GA) (see, e.g., Reeves [20]), and taboo search (TS). GA is widely recognized as a powerful tool for dealing with COPs. The scheme of GAs is to update the population of solutions iteratively to maximize globally some objective functions. But since it uses the fixed crossover and mutation rates, several variants of GAs have been proposed in an attempt to accelerate the convergence rate. On the other hand, according to the analysis of Schrack and Choit [21], the search with reveals, originally proposed by Lawrence and Steiglitz [12], is theoretically superior to the search without reversals in terms of both the probability of success and the expected relative improvement per function evaluation. Therefore, this paper proposes a modification to GA whose incorporates crossover-rate and mutation-rate adaptive method and applies the Lawrence-Steiglitz reversal method.

The remainder of this article is organized as follows. We first provide a concise review of ideal MRGs. In section 3, we describe a GA, and propose an adaptive GA with reversals. Section 4 introduces a number of evaluation measures to evaluate and compare the lattice structure of MRGs derived from the proposed algorithm, RS, and FBS methods. The computational experimentation is conducted and one extensively tested second-order MRG is presented in section 5. Finally, section 6 gives some concluding remarks.

2. Ideal MRGs

This section contains a survey of some basic concepts of ideal MRGs that will be employed in the following. Long period, good lattice structure, and efficient implementation are three prerequisites for an ideal MRG. To achieve the maximum period $m^k - 1$, Knuth described the following conditions of obtaining a full period kth-order MRG:

$$\begin{aligned} &(-1)^{k-1} a_k \text{ is a primitive root modulo } m; \\ &x^r \bmod f(x) \equiv (-1)^{k-1} a_k \pmod{m}; \\ &\deg\{[x^{r/q} \bmod f(x)] \bmod m\} > 0 \text{ for each prime factor } q \text{ of } r, \end{aligned} \tag{2}$$

where $r = (m^k - 1)/(m - 1)$, $f(x) = x^k - a_1 x^{k-1} - \cdots - a_{k-1}x - a_k$, and $\deg(f(x))$ is the degree of polynomial $f(x)$. From finite field theory, $\varphi(m^k - 1)/k$ sets of multipliers satisfy these conditions, where $\varphi(m^k - 1)$ is the Euler's function, defined as the number of integers smaller than and relatively prime to $m^k - 1$. For the second-order MRGs with modulus $2^{31} - 1$, 5.740E17 sets of multipliers are able to produce RNs of full period. Thus, the number of full period MRGs is usually large enough so that such MRGs are easy to find.

For any positive integer t, the set L_t of all possible overlapping t-tuples of successive values of X_n/m with zero vector included is the intersection of a lattice with $(0, 1)^t$. The points of L_t lie in a family of parallel $(t - 1)$-dimensional hyperplanes. The maximal distance d_t between adjacent parallel hyperplanes is adopted as a judging criterion for ranking MRGs. This is the so-called spectral test. From the geometry of number, a theoretical lower bound on d_t is known exactly for $t \leq 8$:

$$d_t^* = \begin{cases} m^{-k/t}/\gamma_t & \text{if } t > k \\ 1/m & \text{if } t \leq k \end{cases} \tag{3}$$

where γ_t is defined in Knuth. The worst-case performance measure

$$S_8 = \min_{k<t\leq 8} d_t^*/d_t \tag{4}$$

is widely adopted for rating various MRGs. The value of S_8 is always between zero and one. The larger the value of S_8 is, the smaller empty slice in L_t is and vice versa. Consequently, we seek generators with S_8 close to one.

Regarding the computationally implementing a MRG, the most fundamental requirements are to compute one term of (1) generally and efficiently. The general and efficient implementing

$$Y = a_i X_{n-i} \pmod m \tag{5}$$

has been extensively studied and developed by many scholars [16, 22]. Since the largest prime modulus is the Mersenne prime $2^{31} - 1$ on a 32-bit computer, Tang [22] indicated that the simulated division method (SDM) is a general and efficient implementation. For the sake of the completeness, we recall the SDM as follows. In computing equation (5), it is easier to compute $Z = a_i X_{n-i} \pmod E$, where $E = 2^{31}$. Let $l = \lfloor a_i X_{n-i}/E \rfloor$. The steps of SDM are as follows. First, compute $Z \leftarrow -m + Z + l$. Secondly, if $Z < 0$ then $Z \leftarrow Z + m$. Therefore, a kth-order MRG can be implemented generally and efficiently by repeated applications of the SDM.

3. Genetic algorithm

The objective of this paper is using an adaptive GA with reversals to search for good full period MRGs with maximum spectral value criterion. Several strategies can have an important influence on the effectiveness and efficiency of a GA. Although we test a wide variety of variants of GAs, we come to rely almost exclusively on the version described below, which seem to exhibit the best spectral value.

The decision variables of searching for good full period MRGs in terms of spectral value are discrete. For such problem, the search space is $\Omega = \{A = (a_1, a_2, \ldots, a_k) \mid 0 \leq a_i < m, 1 \leq i \leq k, a_k \neq 0\}$ and a simple measure of its fitness is using the spectral value S_8. The encoding of a set of multipliers as a binary string seems obvious. More precisely, the coding of the set of multipliers can be represented by a binary string of length $31k$, each 31 bits corresponding to one multiplier.

To cover the solution space adequately and achieve the computational efficiency, the population size of 100 is more common by many reported implementations. An initial population of good randomized approach is used to yield better final solutions, to reduce the running time, and to increase the diversification [2]. This effective approach is adopted by using the best two MRGs proposed by L'Ecuyer, Blouin, and Couture, and using randomly generated 98 MRGs.

At each generation, we preserve the best two sets of multipliers so far and replace the remaining 98 members of the population with new ones by selection, crossover, and mutation operations. De Jong [4] calls this the population overlaps. There are three selection schemes: roulette-wheel, Baker's stochastic universal selection (SUS) [3], and rank selection methods. In this paper, we adopt the SUS method, which is the most effective one in terms of accurate, consistent, and efficient sampling [3].

Two recombination operations are distinguished: crossover and mutation operations. The uniform crossover and standard mutation operations are used in this paper. An associated problem is that of determining the crossover and mutation rates. To allow wider and deeper exploration, we apply the adaptive crossover and mutation rates proposed by Tang and Kao [23]. Specifically, the crossover rate P_c and mutation rate P_m are increased or decreased in a heuristic fashion according to the improvement or deterioration of the population of solutions. The performance of a population of solutions is defined as its maximum (Max) of S_8. When the population of solutions is improving, the value of P_c is increased by step 0.05 to explore a new area of the search space, while the corresponding P_m is reduced by step 0.01 to accelerate the convergence [8]. More precisely, we have $P_c = P_c + 0.05$ and $P_m = P_m - 0.01$. Note that $0 \leq P_c, P_m \leq 1$ is a trivial bound on the crossover and mutation rates. When the population of solutions is deteriorating, the values of P_c and P_m are adjusted as $P_c = P_c - 0.05$ and $P_m = P_m + 0.01$. The value of initial crossover rate is 0.95 suggested by Grefenstette [9], while the initial mutation rate is a small mutation probability 0.01. However, the crossover and mutation operations may generate offspring that do not represent full period MRGs, even though both parents represent full period MRGs. This difficulty can be overcome by allowing non-full period MRGs, but to penalize them in dividing 2 into its fitness. Based on the concept of aspiration derived from TS, a non-full period MRG that its value of S_8 is larger than the second largest fitness is to ignore them and insert it into the population.

Via the operations of selection, crossover, and mutation, temporary population of solutions TP_i are generated from the current population of solutions CP_i for $1 \leq i \leq 100$. An application of the search with reversals, new population of solutions NP_i, $1 \leq i \leq 100$, are given by the following form:

$$NP_i = \begin{cases} 2CP_i - TP_i & \text{if } S_8(TP_i) < S_8(CP_i) < S_8(2CP_i - TP_i) \\ TP_i & \text{otherwise} \end{cases}$$

where $S_8(G)$ is the spectral value of a MRG G. After the reversals, the operations of selection, crossover, and mutation are applied again to produce the next generation. This process is continued until the specified number of generations, say 100, is reached.

4. Evaluation measures

We adopt a number of evaluation measures to assess and compare the proposed algorithm with RS and FBS in terms of efficiency and effectiveness. In concern with the efficiency, since the computer systems adopted in the literature are not always same, the computational times can not be used to measure the efficiency. In this paper, the ratio of the smallest number of MRGs required among the various types of search and that of the method is used. It is known as relative proportion (RP) and, clearly, takes values in $(0, 1)$.

On the other hand, the term 'effectiveness' can be defined as the possession of global and local randomness. The number of MRGs that pass all the tests can serve as a judging criterion. Several tests have been proposed to make this assessment in the literature (see, e.g., Knuth). The theoretical and empirical tests are two ways of evaluating the global and local randomness, respectively. First, in the case of the theoretical tests, spectral and lattice tests are the two most powerful test known. The algorithms developed by Fincke and Pohst [5], and by Afflerbach and Grothe [1] are the most efficient to compute spectral and lattice values, respectively. Secondly, the empirical tests can be classified as either classical statistical tests or sparse occupancy (SO) tests [11, 18]. In concern with the classical statistical tests, runs and auto-correlation of lags one to three statistics are chosen for testing independence, while the chi-square and serial of dimensions two and three statistics for testing uniformity. Four SO tests, namely, overlapping-pairs-sparse-occupancy (OPSO), overlapping-triples-sparse-occupancy (OTSO), overlapping-quadruples-sparse-occupancy (OQSO), and DNA tests, are used to examine both uniformity and independence. To increase the power of empirical tests, a two-level test proposed by L'Ecuyer [13] is used. The steps of the two-level empirical tests are as follows. Firstly, each empirical test is duplicated 1000 times on consecutive subsequences of 2^{21} RNs. Then, the empirical distribution of those 1000 statistics is compared to the theoretical distribution by using the Kolmogorov-Smirnov test.

To summarize, we compare the effectiveness of the proposed algorithm with that of RS and FBS in terms of spectral value, lattice value, two-level classical statistical tests, and two-level SO tests. We also compare their efficiency with respect to RP.

5. Results

This paper proposes the adaptive GA with reversals to search for good full period MRGs with respect to spectral value. As an illustration, the proposed algorithm is applied to find good second-order MRGs. The whole computation is conducted on a 733 MHz Pentinum III PC using Microsoft Visual C++ compiler under Microsoft Windows 98 operating system. The best second-order MRG is the set $(a_1, a_2) = (1259791845, 1433587751)$ with a spectral value of 0.78741.

Table 1. Results of the evaluation measures for the second-order MRGs found by three methods

Method	Proposed algorithm	Forward/Backward search	Random search	Random search
a_1	1259791845	210826083	1498809829	46325
a_2	1433587751	−885300443	1160990996	1084587
Spectral	0.78741	0.78559	0.64358	0.58103
Lattice	0.71792	0.66877	0.66843	0.35748
Runs	0.70119	0.51479	0.32158	0.04918
AR1	0.07813	0.44276	0.29976	0.31992
AR2	0.25646	0.22547	0.19011	0.00870
AR3	0.24325	0.04375	0.41696	0.53739
Chi-square	0.08677	0.38877	0.35965	0.04507
Serial2	0.34831	0.52973	0.09794	0.58315
Serial3	0.16478	0.10361	0.18279	0.01075
OPSO	0.29980	0.17840	0.30984	0.37209
OTSO	0.18415	0.00369	0.07409	0.04746
OQSO	0.08409	0.09905	0.14243	0.24288
DNA	0.13683	0.00914	0.00159	0.00021
Number of MRGs	10000	6442450941	N.A.	N.A.
RP	1	644245.09	N.A.	N.A.

We give comparative results of the theoretical and empirical tests for the second-order MRGs found by the proposed algorithm, RS, and FBS methods. The RS found two sets of multipliers $(1498809829, 1160990996)$ and $(46325, 1084587)$ with the good lattice structure in terms of lattice value. The FBS sought the good set of multipliers $(210826083, -88530043)$ with a spectral value of 0.78559. The values of the spectral test, lattice test, and the p-values of different two-level empirical tests of these four MRGs are shown in Table 1, where ARi denotes the auto-correlation test of lag i, and Serial$i$ the serial test of dimension i. The set $(1259791845, 1433587751)$ found from the proposed algorithm has the largest spectral and lattice values. Moreover, at the 0.05 significant level, this set $(1259791845, 1433587751)$ passes all the two-level empirical tests. Notably, all the rest of the sets of multipliers fail the DNA test.

We now return to the computational efficiency of these methods for good second-order MRGs. On basis of the RP, the most efficient method is the proposed algorithm, next FBS. Since in the literature, L'Ecuyer, Blouin, and Couture made no mention of the number of MRGs for the RS. We cannot compare it with other methods, and use term 'NA' to refer to not available.

Therefore, the adaptive GA with reversals is a good way of obtaining an ideal second-order MRG.

6. Conclusion

By dynamically adapting the crossover and mutation rates during searching, and applying the Lawrence-Steiglitz reversal method, a heuristic algorithm is proposed to find the ideal second-order MRGs with long period and good lattice structure. Simulations are conducted to compare and evaluate its lattice structure and computational efficiency with RS and FBS methods. Three

conclusions can be drawn from this paper. Firstly, the proposed algorithm improves the lattice structure in terms of spectral test, lattice test, two-level classical statistical tests, and two-level SO tests. Thus, it is the most effective one. Secondly, the proposed algorithm is preferred in terms of the RP and thus, is the most computational efficiency. Thirdly, the DNA test is the most stringent one among the two-level empirical tests. Therefore, the adaptive GA with reversals provides good lattice structure and computational efficiency, and can be applied to find ideal MRGs of higher orders.

Acknowledgment. This work was supported by the National Science Council of the Republic of China under Contract NSC89-2213-E-230-003.

References

[1] Afflerbach L, Grothe H (1985) Calculation of Minkowski-reduced lattice bases. Computing 35:269–276
[2] Aggarwal CC, Orlin JB, Tai RP (1997) Optimized crossover for the independent set problem. Oper. Res. 45:226–234
[3] Baker EB (1987) Reducing bias and inefficiency in the selection algorithm. In: Grefenstette JJ (ed.) Proceedings of 2nd International Conference on Genetic Algorithms, Lawrence Erlbaum Associate, Hillsdale, NJ, pp. 14–21
[4] De Jong KA (1975) An analysis of the behavior of a class of genetic adaptive systems. Doctoral dissertation, University of Michigan, Ann Arbor, MI
[5] Fincke U, Pohst M (1985) Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. Math. Comp. 44:463–471
[6] Fishman GS (1996) Monte Carlo: Concepts, algorithms, and applications. Springer Series in Operations Research, Springer-Verlag, New York
[7] Fishman GS, Moore III LR (1986) An exhaustive analysis of multiplicative congruential random number generators with modulus $2^{31} - 1$. SIAM J. Sci. Stat. Computing 7:24–45
[8] Fogarty TC (1989) Varying the probability of mutation in the Genetic Algorithm. In: Schaffer JD (ed.) Proceedings of 3rd International Conference on Genetic Algorithms, Morgan Kaufmann, Los Altos, CA, pp. 104–109
[9] Grefenstette JJ (1986) Optimization of control parameters for genetic algorithms. IEEE Trans. on Systems, Man and Cybernetics SMC-16:122–128
[10] Kao C, Tang HC (1997) Systematic searches for good multiple recursive random number generators. Computers Ops Res. 24:899–905
[11] Knuth DE (1997) The art of computer programming, vol 2: Semi-numerical algorithms. Third edition, Addison-Wesley, Reading MA
[12] Lawrence JP III, Steiglitz K (1972) Randomized pattern search. IEEE Trans. on Computers C-21:382–385
[13] L'Ecuyer P (1992) Testing random number generators. Proceeding of the 1992 Winter Simulation Conference 305–313
[14] L'Ecuyer P, Blouin F (1988) Linear congruential generators of order $k > 1$. Proceeding of the 1988 Winter Simulation Conference 432–439
[15] L'Ecuyer P, Blouin F, Couture R (1993) A search for good multiple recursive random number generators. ACM Trans. on Modeling and Computer Simu. 3:87–98
[16] L'Ecuyer P, Côté S (1991) Implementing a random number package with splitting facilities. ACM Trans. on Math. Software 17:98–111
[17] Lehmer DH (1951) Proceedings 2nd symposium on large-scale digital calculating machinery. Cambridge, Harvard University Press, pp. 141–146
[18] Marsaglia G, Zaman A (1993) Monkey tests for random number generators. Computers Math. Applic. 26:1–10
[19] Niederreiter H (1992) Random number generation and quasi-Monte Carlo methods. SIAM CBMS-NSF Regional Conference Series in Applied Mathematics 63: SIAM, Philadelphia

[20] Reeves CR (1997) Genetic algorithms for the operations researcher. INFORMS J. Computing 9:231–250
[21] Schrack G, Choit M (1976) Optimized relative step size random searches. Math. Prog. 10:230–244
[22] Tang HC (2000) Implementing a multiple recursive generator with Mersenne prime modulus. Inter. J. Computer Math. 76:35–43
[23] Tang HC, Kao C (2002) Searching for good multiple recursive random number generators via the Genetic Algorithm. working paper