EFFICIENT MULTIPLY-WITH-CARRY RANDOM NUMBER GENERATORS WITH OPTIMAL DISTRIBUTION PROPERTIES.

MARK GORESKY[1] AND ANDREW KLAPPER[2]

1. Introduction

1.1. A pseudo random number generator (RNG) for high speed simulation and Monte Carlo integration should have several properties: (1) it should have enormous period, (2) it should exhibit uniform distribution of d-tuples (for all d), (3) it should exhibit a good lattice structure in high dimensions, and (4) it should be efficiently computable (preferably with a base b which is a power of 2). Typically the RNG is a member of a family of similar generators with different parameters and one hopes that parameters and seeds may be easily chosen so as to guarantee properties (1), (2), (3) and (4). There is no known family of RNG with all four properties (see, for example, [M1]).

1.2. In [MZ], Marsaglia and Zaman showed that their add-with-carry (AWC) generators satisfy condition (1). By giving up on (4) and using an appropriate base b, they achieve good distribution properties of d-tuples for values d which are less than the "lag." It has been shown [TE] that these generators fail the spectral test [CM] for large d. A generalization, the multiply-with-carry (MWC) generator, was described in [M2], [C2] and independently, (motivated by some questions in cryptography) in [KG1], [KG2], [KG3], where it was called a feedback-with-carry shift register, or FCSR. The MWC generator was proposed in [C2] as a way of possibly generating random numbers which satisfy (1), (2), and (4) and which had a chance at (3). Using some results from number theory, estimates on the distribution properties of this generator were made, and the spectral test was used in order to search for parameters which satisfy (3) (although they also described limits on what one might hope to achieve with respect to the lattice structure). In this paper we propose a slight modification of the MWC generator, for which it is possible to retain properties (1) and (4), and to guarantee property (2): that the resulting random numbers have optimal d-dimensional distributional properties for d less than the "lag." It is expected, however, that

1. The Institute for Advanced Study, School of Mathematics, (www.math.ias.edu/~goresky/). Research partially supported by N.S.F. grant # 0002693.

2. Dept. of Computer Science, 779A Anderson Hall, University of Kentucky, Lexington, KY, 40506-0046 and the Institute for Advanced Study, School of Mathematics. E-mail: klapper@cs.uky.edu. Project sponsored by the National Science Foundation under grant # 9980429.

for large d the lattice structure will suffer from the same shortcomings as those described in [C2].

1.3. Recall that a MWC generator of order r and base b consists of a state

$$\sigma = (x_{-1}, \dots , x_{-r}; c)$$

where $0 \le x_i < b$ and $c \in \mathbf{Z}$, and a transformation rule $T : \sigma \mapsto \sigma' = \left(x'_{-1}, \dots , x'_{-r}, c'\right)$. The transformation rule is determined by a fixed choice of coefficients $a_1, \dots , a_r$ and is given as follows: x'_{-1} and c' are the unique solutions to

$$x'_{-1} + c'b = \sum_{i=1}^{r} a_i x_{-i} + c \tag{1.3.1}$$

with $0 \le x'_i < b$ while $x'_i = x_{i+1}$ for $i < -1$. The values x'_{-1} and c' are most easily computed by introducing an auxiliary variable $\tau = \sum_{i=1}^{r} a_i x_{-i} + c$. Then $x'_{-1} = \tau \pmod b$ and $c' = (\tau - x'_{-1})/b$.

The integer c is called the "carry" or the "memory" of the state. The analysis of this generator relies heavily on the number theoretic properties of the *connection integer*

$$m = -1 + \sum_{i=1}^{r} a_i b^i.$$

If the "base" b is chosen to be a power of 2, then these generators admit efficient implementations; however the connection integer m is constrained to be of the form $Nb - 1$ for some integer N, and this constraint limits the effectiveness of the generator. A similar criticism applies to the subtract-with-borrow (SWB) generator.

1.4. In this paper we show that (at the cost of introducing two more multiplications per round) a simple modification (as first described in [KX]) of the transformation rules (1.3.1) may be used in order to produce MWC generators whose connection integer is *any* positive integer m relatively prime to b. In particular, it is possible to choose m to be a prime number so that b is a primitive root $\pmod m$ (and in Section 5 we indicate how to do so). This leads to properties (1), (2) and (4) listed above: (1) the period of the generator is $m - 1$, which is maximal; (2) the d dimensional distribution properties of this generator are optimal, for each $d < r$ and (4) the modulus b may be taken to be a power of 2.

2. Multiply-with-carry generators

2.1. Fix an integer "base", $b > 0$ and fix integer coefficients $a_0, a_1, \dots , a_r$ with a_0 chosen to be relatively prime to b. (If b is a power of 2, this simply means that a_0 is odd.) The (modified) MWC generator of base b and order r corresponding to this data consists of a state $\sigma = (x_{-1}, \dots, x_{-r}; c)$ with $0 \le x_i < b$ and $c \in \mathbf{Z}$ as above. The state changes according to the following rules: x'_{-1} and c' are the unique solutions to

$$a_0 x'_{-1} + c' b = \sum_{i=1}^{r} a_i x_{-i} + c \tag{2.1.1}$$

with $0 \le x'_i < b$; while $x'_i = x_{i+1}$ for $i < -1$. The values of x'_{-1} and c' may be computed as follows. Calculate once and for all

$$A = a_0^{-1} \pmod{b}$$

and realize this as an integer between 0 and $b - 1$. Set $\tau = \sum_{i=1}^{r} a_i x_{-i} + c$. Then:

$$x'_{-1} = (A\tau) \pmod{b} \tag{2.1.2}$$

$$c' = (\tau - a_0 x'_{-1})/b. \tag{2.1.3}$$

Define the *connection integer*

$$m = -a_0 + \sum_{i=1}^{r} a_i b^i. \tag{2.1.4}$$

It follows that m is relatively prime to b. Every such $m > 0$ has a unique representation of the form (2.1.4) with $0 \le a_i < b$ and with a_0 relatively prime to b. In this paper we allow the a_i to be arbitrary integers, so for a given connection integer m the representation (2.1.4) is not necessarily unique: one could even take $a_0 = -m$. It would be interesting to study to what extent the computations (2.1.2) and (2.1.3) might be optimized by appropriate choice of coefficients a_i.

In the next few paragraphs we show that these generators have many desirable properties. The proofs for most of these facts follow from standard techniques which may be distilled from the literature ([C1],[C2],[MZ],[TE]). However, short and efficient proofs may be obtained by an algebraic technique, which is a simple but not entirely obvious modification of the method of [KG3], so we include them at the end for completeness.

2.2. Throughout the rest of this section we fix a modulus b and consider the MWC generator corresponding to a connection integer m as in (2.1.4), where b is relatively prime to m.

Let us say that a state of the generator is degenerate if the output remains constant. The "bottom" state, in which all $x_i = 0$ and $c = 0$ is degenerate with output 0. The "top" state, in which all $x_i = b - 1$ and

$$c = -a_0 + \sum_{i=1}^{r} a_i$$

is degenerate with output $b - 1$. (There may be more degenerate states.)

Suppose $\sigma = (x_{-1}, x_{-2}, \ldots, x_{-r}; c)$ is a state of the generator. Define the integer

$$h = b^r c + a_0 \sum_{j=0}^{r-1} x_{-r+j} b^j - \sum_{k=1}^{r-1} b^k \sum_{i=1}^{k} a_i x_{-r+k-i}. \tag{2.2.1}$$

The number h determines the output sequence (see Lemma 4.5 below) although it is not clear whether h also determines the state. (That is, can two distinct states determine the same output sequence?) If σ is the bottom state, then $h = 0$. If σ is the top state, then $h = m$.

2.3. Theorem. *The output sequence is strictly periodic if and only if* $0 \le h \le m$.

Define $B = b^{-1} \pmod{m}$ and represent it as a non-negative integer $0 < B < m$. Define $A = a_0^{-1} \pmod{b}$, and represent it as a non-negative integer $0 < A < b$.

2.4. Theorem. *Suppose the register is in a strictly periodic state. Then the sequence of numbers in the rightmost cell is given by*

$$x_{-r+i} = -A\left(hB^i \pmod{m}\right) \pmod{b}. \tag{2.4.1}$$

Equation (2.4.1) means that first the number $hB^i = hb^{-i}$ is computed modulo m, and is represented as a number between 0 and $m-1$. Then this number is multiplied by $-A$ and reduced modulo b to give an integer between 0 and $b-1$.

In particular, if $b = 2^\omega$ and $A = a_0 = 1$ then the sequence (2.4.1) coincides (up to a sign) with the sequence of lowest-order ω bits taken from a linear congruential generator (LCG) with modulus m and multiplier B, as observed in [C2]. In this case, however, if $\omega \ge 3$ then b is never a primitive root modulo m. In this paper we allow nontrivial values for a_0 so it is possible to take m to be prime and B to be a primitive root $\pmod{m}$, thereby achieving the optimal distribution properties which are characteristic of a LCG with prime modulus.

2.5. Corollary. *If m is prime and if b is a primitive root modulo m then the period of the MWC generator is* $m-1$.

In this case we say the resulting periodic sequence is a (generalized) ℓ-sequence (or long sequence), because of the many properties it shares with m-sequences (or maximal length sequences) from the theory of finite fields.

2.6. Theorem. *Suppose m is prime and b is a primitive root $\pmod{m}$. Fix $d \ge 1$ and let $\mathbf{z} = (z_1, z_2, \ldots, z_d)$ with $0 \le z_i < b$. Then the number $N(\mathbf{z})$ of occurrences of the d-tuple $\mathbf{z}$ which begin in any fixed period of the sequence (2.4.1) can vary at most by 1, that is $N(z)$ is either*

$$\left\lfloor \frac{m-1}{b^d} \right\rfloor \quad \text{or} \quad \left\lfloor \frac{m-1}{b^d} \right\rfloor + 1.$$

In particular, if $b^d < m-1$ then every $d-$tuple occurs at least once in any fixed period.

3. Bounds on the carry

3.1. Throughout this section we consider a MWC generator of order r with base b, coefficients $a_0, a_1, \ldots, a_r$ and state $\sigma = (x_{-1}, x_{-2}, \ldots, x_{-r}; c)$ as described in §2. Recall that c and a_i are integers and that $0 \le x_i < b-1$. We will show that the carry rapidly converges to a narrow range.

There are two classes of generators which we refer to as singular generators. The first type of singular generator has $a_0 > 0$ and all the remaining coefficients $a_i \le 0$ (for $1 \le i \le r$). The second type has $a_0 < 0$ and all the remaining coefficients $a_i \ge 0$.

3.2. If $a_0 > 0$ define

$$w^+ = \sum_{\substack{a_i>0\\1\le i\le r}} a_i \quad \text{and} \quad w^- = -a_0 + \sum_{\substack{a_i<0\\1\le i\le r}} a_i.$$

If $a_0 < 0$ define

$$w^+ = -a_0 + \sum_{\substack{a_i>0\\1\le i\le r}} a_i \quad \text{and} \quad w^- = \sum_{\substack{a_i<0\\1\le i\le r}} a_i.$$

3.3. Theorem. *Suppose the generator is not singular. If the generator is in a strictly periodic state then the carry c lies in the range*

$$w^- < c < w^+. \tag{3.3.1}$$

If $c > w^+$ then it will drop monotonically and exponentially until it lies within this range and it will remain within this range thereafter. If $c < w^-$ then it will rise monotonically and exponentially until it lies within this range, and it will remain within this range thereafter. If the generator is singular then c will move monotonically until it lies within the range

$$w^- \le c \le w^+$$

and it will remain within this range thereafter.

3.4. **Proof.** Let us assume $a_0 > 0$. (The proof for $a_0 < 0$ is completely parallel.) From (2.1.1), since $0 \le x_i \le b-1$ we have

$$c' = \frac{1}{b}\left[\sum_{i=1}^{r} a_i x_{-i} + c - a_0 x'_{-1}\right] \le \left(\frac{b-1}{b}\right) w^+ + \frac{c}{b}. \tag{3.4.1}$$

If $c < w^+$ this gives $c' < w^+$. If $c = w^+$ this gives $c' \le w^+$. If $c > w^+$ this gives

$$c' - c \le (w^+ - c)\left(\frac{b-1}{b}\right) < 0,$$

hence the carry decreases monotonically. Moreover, if $c >> bw^+$ then $c' \approx c/b$ which is to say that c decreases exponentially. It is easy to see that there are no strictly periodic states with $c = w^+$ unless the generator is singular. For if $c = c' = w^+$ then (2.1.1) gives

$$(b-1)w^+ = \sum_{i=1}^{r} a_i x_{-i} - a_0 x'_{-1}.$$

The right side of this equation achieves its maximum value, $(b-1)w^+$, when $x'_{-1} = 0$ and

$$x_{-i} = \begin{cases} 0 & \text{whenever } a_i < 0 \\ b-1 & \text{whenever } a_i > 0. \end{cases}$$

Eventually this $0 = x'_{-1}$ will get shifted into one of the positions where $a_i > 0$ and then the value of c will drop below w^+. (If $a_i \leq 0$ for all i, then the generator is singular, $w^+ = 0$, and the degenerate "bottom" (all-zero) state satisfies $c = w^+$.) In summary, if the generator is not singular and if the carry starts out at any positive value, it will drop until $c < w^+$ and will remain there forever.

To obtain the lower bound on c, equation (2.1.1) gives

$$c' = \frac{1}{b}\left[\sum_{i=1}^{r} a_i x_{-i} + c - a_0 x'_{-1}\right] \geq \frac{b-1}{b} w^- + \frac{c}{b}.$$

If $c > w^-$ then $c' > w^-$. If $c = w^-$ then $c' \geq w^-$. If $c < w^-$ then

$$c' - c \geq \left(\frac{b-1}{b}\right)(w^- - c) > 0$$

so the value of c will increase monotonically (and exponentially). Let us examine the possible periodic states with $c = c' = w^-$. For such a state, equation (2.1.3) gives

$$(b-1)w^- = \sum_{i=1}^{r} a_i x_{-i} - a_0 x'_{-1}.$$

The right side of this equation achieves its minimum value, $(b-1)w^-$ when $x'_{-1} = b-1$ and

$$x_i = \begin{cases} b-1 & \text{whenever } a_i < 0 \\ 0 & \text{whenever } a_i > 0. \end{cases}$$

If some coefficient a_i is positive (which is to say, if the generator is not singular) then this $b-1 = x'_{-1}$ will eventually be shifted into the i-th position, and the value of c will rise above w^-. However, if the generator is singular (that is, if $a_i \leq 0$ for $1 \leq i \leq r$) then this argument fails and indeed, the degenerate "top" state satisfies $c = w^-$ and $x_i = b-1$ for all i. In summary, if the generator is not singular and if the carry starts out at some negative value, then it will rise until $c > w^-$ and it will remain there forever. $\square$

4. Proofs

4.1. As in §2 we fix a base b and consider the MWC generator which corresonds to a connection integer m of equation (2.1.4). In the literature, it is customary to analyze this generator by associating to each fraction h/m its fractional digital expansion in base b. Instead, we will use the equivalent, but more abstract expansion of $-h/m$ as an element of the ring $\mathbf{Z}_b$ of b-adic numbers. (One expansion is just the reverse of the other.) The proofs become cleaner since various number-theoretic operations, such as $(\bmod b)$, may be applied to elements of $\mathbf{Z}_b$.

4.2. A b-adic number $\alpha \in \mathbf{Z}_b$ is a formal power series,

$$\alpha = x_0 + x_1 b + x_2 b^2 + \dots \tag{4.2.1}$$

with $0 \le x_i < b$. The sequence $x_0, x_1, \dots$ is referred to as the coefficient sequence of α. Addition and multplication in $\mathbf{Z}_b$ are performed "with carry", that is, $xb^r + (b-x)b^r = b^{r+1}$. It is clear that $\mathbf{Z}_b$ contains the positive integers, but it also contains the negative integers since $-1 = (b-1) + (b-1)b + (b-1)b^2 + \dots$ as may be seen by adding 1 to both sides. It also contains all fractions of the form h/m where m is relatively prime to b. In fact, if a positive integer m is expanded in base b,

$$m = m_0 + m_1 b + \dots + m_r b^r$$

then m is relatively prime to b iff m_0 is invertible in $\mathbf{Z}/(b)$, say, $m_0 a_0 \equiv 1 \pmod b$. Then the inverse is given by $1/m = a_0 + a_1 b + \dots$ and it can be computed by long division. It is easy to see that these fractions h/m (with m relatively prime to b) are precisely the elements of $\mathbf{Z}_b$ whose coefficient sequence (4.2.1) is eventually periodic, and we refer to this sequence as the b-adic expansion of h/m.

4.3. By summing the relevant geometric series, it is easy to see that the fractions h/m with $-m \le h \le 0$ are precisely the elements of $\mathbf{Z}_b$ whose coefficient sequence is *strictly* periodic (cf. [KG3] Thm. 2.1). The case $h = 0$ corresponds to the coefficient sequence $0, 0, \dots$ and the case $h = -m$ corresponds to the coefficient sequence $b-1, b-1, \dots$

4.4. Now suppose we have a MWC generator with base b and with parameters $a_0, a_1, \dots, a_r$, where a_0 is relatively prime to b. Let $m = -a_0 + \sum_{i=1}^{r} a_i b^i$ be the connection integer as in equation (2.1.4). Choose a seed state $\sigma = (x_{-1}, x_{-2}, \dots, x_{-r}; c)$ as in §2. If we observe the contents of the rightmost cell we obtain an infinite sequence of numbers x_{-r}, $x_{-r+1}, \dots, x_{-1}$, x_0, $x_1, \dots$ to which we can associate the following b-adic number

$$\alpha = x_{-r} + x_{-r+1} b + \dots + x_0 b^r + x_1 b^{r+1} + \dots \tag{4.4.1}$$

4.5. Lemma. *Let $\sigma = (x_{-1}, x_{-2}, \dots, x_{-r}; c)$ be the seed state of the generator and define the integer $h \in \mathbf{Z}$ by equation (2.2.1). Then the resulting b-adic number α is the b-adic expansion of the fraction $-h/m$.*

4.6. **Proof.** This is a special case of [KX] Theorem 3. Alternatively, one may easily adapt the proof of [KG3] Theorem 4.1, replacing 2 by b. (In both cases, the proof is parallel to the original method of [G] Sect. 2.5.) $\square$

4.7. **Proof of Theorem 2.3.** This follows immediately from Lemma 4.5 and §4.3. $\square$

4.8. **Proof of Theorem 2.4.** To a given state $\sigma = (x_{-1}, x_{-2}, \ldots, x_{-r}; c)$ we associate the b-adic number $f(\sigma) = \alpha$ of (4.4.1). By Lemma 4.5, $\alpha = -h/m$ for some integer h. (The precise value of h is given by (2.2.1) however this fact is not needed for the argument.) If $\sigma' = (x'_{-1}, \ldots, x'_{-r}; c')$ represents the next state then

$$f(\sigma') = x_{-r+1} + x_{-r+2}b + \ldots = -h'/m$$

for some integer h'. So the following equation holds in $\mathbf{Z}_b$:

$$bf(\sigma') + x_{-r} = f(\sigma)$$

or

$$h = bh' - mx_{-r}. \tag{4.8.1}$$

Although this is an equation in $\mathbf{Z}_b$, all the terms are integers, so it is an equality among integers. Reading this equation modulo b gives $x_{-r} \equiv -m^{-1}h \equiv -Ah \pmod b$ (since $m \equiv a_0 \pmod b$). In other words, the contents of the rightmost cell is given by $-Ah \pmod b$.

Reading equation (4.8.1) modulo m gives $h' \equiv Bh \pmod m$. Now suppose the state σ is a nonzero, strictly periodic state. Then the same is true for σ', hence by Theorem 2.3, $0 < h, h' < m$. So we have the following equality,

$$h' = Bh \pmod m,$$

provided we interpret the instructions $\pmod m$ to mean: reduce modulo m then represent this quantity as an integer between 0 and $m-1$.

It follows that the i-th state $\sigma^{(i)}$ will correspond to the fraction $f(\sigma^{(i)}) = h^{(i)}/m$ where $h^{(i)} = B^i h \pmod m$, and the contents of the rightmost cell will therefore be

$$-Ah^{(i)} \pmod b = -A(B^i h \pmod m) \pmod b. \quad \square$$

4.9. **Proof of Theorem 2.6.** (This proof is parallel to [KG3] Sect. 13.4.) A purely periodic nonzero sequences $\mathbf{x} = (x_0, x_1, \ldots)$ with connection integer m is the b-adic expansion of a rational number $-h/m$ with $0 < h < m$. Since b is chosen to be primitive, the different nonzero choices of h correspond to cyclic shifts of $\mathbf{x}$. Thus, a d-digit subsequence $\mathbf{z} = (z_1, z_2, \ldots, z_d)$ occurs in $\mathbf{x}$ iff it occurs as the first d digits in the b-adic expansion of some rational number $-h/m$. Moreover, two such rational numbers $-h_1/m$ and $-h_2/m$ have the same first d digits iff

$$-\frac{h_1}{m} \equiv -\frac{h_2}{m} \pmod{b^d},$$

that is, iff $h_1 \equiv h_2 \pmod{b^d}$. So we only need to count the number of h with a given first d digits and with $0 < h < m$.

Suppose that $b^r < m < b^{r+1}$. If $d > r$ then there is at most one such h and the result follows. Thus we may assume that $d \le r$. Now we will count the number of possible h with $0 < h < m$ whose first d digits are fixed. Write

$$h = (h_0 + h_1 b + \ldots + h_{d-1} b^{d-1}) + b^d (h_d + \ldots + h_r b^{r-d}) = h' + b^d h'' \tag{4.9.1}$$

with $0 \le h_i < b$. Similarly set $m = m' + b^d m''$. Then

$$m'' = \left\lfloor \frac{m}{b^d} \right\rfloor = \left\lfloor \frac{m-1}{b^d} \right\rfloor$$

and

$$0 \le h', m' < b^d. \tag{4.9.2}$$

First note that $h'' \le m''$. For if $h'' \ge m'' + 1$ then

$$h \ge b^d h'' \ge b^d m'' + b^d > b^d m'' + m' = m$$

which contradicts $h < m$. We now consider two cases.

Case 1: $h' \ge m'$ Every choice of $h'' \le m'' - 1$ will give $0 < h < m$ since, by (4.9.2),

$$h = h' + b^d h'' < b^d + b^d h'' \le b^d + b^d (m'' - 1) \le b^d m'' + m' = m.$$

There are m'' such choices.

Case 2: $h' < m'$ Any choice of $h'' \le m''$ will give $h < m$. If $h' \ne 0$ then then all such choices give $0 < h < m$ and there are $m'' + 1$ possible such choices. If $h' = 0$ then all nonzero choices of $h'' \le m''$ give $0 < h < m$ and there are m'' such choices. □

We remark that if $b = 1$ and $d = 1$ (that is, when counting the number of occurrences of a single bit in a binary ℓ-sequence), then $m' = 1$ so the two cases are: $h' = 1$ and $h' = 0$. In particular, Case 2 with $h' \ne 0$ never occurs. In other words, the sequence (2.4.1) is balanced: the number of 0's equals the number of 1's, and this number is $(m-1)/2$.

5. Examples

5.1. Let $m > 2$ be a prime number and let $b = 2^\omega$ with $\omega \ge 1$. Then b is a primitive root modulo m if and only if 2 is a primitive root modulo m and ω is relatively prime to $m - 1$. Moreover 2 is *not* primitive modulo m if and only if

$$2^{(m-1)/p} \equiv 1 \pmod{m} \tag{5.1.1}$$

for some prime factor p of $m-1$. If 2 is a primitive root modulo m then $m \equiv 3$ or $5 \pmod 8$. These facts make it fairly easy to find large primes for which 2 is a primitive root. The following examples were found in a few hours using MAPLE. They use auxiliary primes p and q. According to Theorem 2.6, in each of these cases, the resulting MWC generator will have period $m - 1$ and the resulting d-tuples will be uniformly distributed, with every

d-tuple occurring whenever $d \leq d_0$. The last column, T, gives the approximate period of the generator.

b	p	q	m	d_0	T
2^{21}	$b^{14} - b^2 + 1$	$b^{58} - b^{36} + 1$	$4pq + 1$	71	10^{455}
2^{21}	$b^{52} - b^7 - 1$		$4p^2 + 1$	103	10^{657}
2^{21}	$b^{60} - b^{13} - 1$	$b^{60} - b^{26} - 1$	$2pq + 1$	119	10^{758}
2^{23}	$b^{12} + b^7 + 1$	$b^{25} + b^{19} + 1$	$2pq + 1$	37	10^{256}
2^{23}	$b^{14} - b^7 - 1$	$b^{27} + b^{26} + 1$	$4pq + 1$	41	10^{284}
2^{24}	$b^{48} - b^{46} - b^{38} - b^{14} + 1$		$2p + 1$	47	10^{347}
2^{24}	$b^{41} - b^{38} - 2b^{14} + 1$		$2p + 1$	40	10^{296}
2^{25}	$b^6 - b^4 - 1$	$b^{16} - b^{11} - 1$	$2pq + 1$	21	10^{166}
2^{31}	$b^7 + b^4 + 1$	$b^{30} + b^{14} - 1$	$4pq + 1$	37	10^{345}
2^{32}	$b^{33} - b^{20} - b^{14} - b^{11} - b^4 + 1$		$4p + 1$	32	10^{318}
2^{33}	$b^3 + b^2 + 1$	$b^{27} + b^{14} + 1$	$4pq + 1$	30	10^{298}
2^{35}	$b^2 + b - 1$	$b^{41} - b^{28} + 1$	$4pq + 1$	43	10^{453}

References

[CM] R. Coveyou and R. MacPherson, Fourier analysis of uniform random number generators. J. ACM **14** (1967), pp. 100–119.

[C1] R. Couture and P. L'Ecuyer, On the lattice structure of certain linear congruential sequences related to AWC/SWB generators. Math. Comp. **62** (1994), pp. 799–808.

[C2] R. Couture and P. L'Ecuyer, Distribution properties of multiply-with-carry random number generators. Math. Comp. **66** (1997), pp. 591–607.

[G] S. Golomb, **Shift Register Sequences**, Aegean Park Press, Laguna Hills, CA, 1982.

[KG1] A. Klapper and M. Goresky, 2-adic shift registers, in **Fast Software Encryption**, Cambridge Security Workshop, Cambridge UK, Dec. 9-11, 1993. Lecture Notes in Computer Science **809** (1994), Springer Verlag, N.Y.

[KG2] A. Klapper and M. Goresky, Feedback shift registers, combiners with memory, and arithmetic codes. Univ. of Kentucky Dept. of Comp. Sci. Tech. Rep. No. 239-93.

[KG3] A. Klapper and M. Goresky, Feedback shift registers, 2-adic span, and combiners with memory. J. Crypt. **10** (1997), pp. 111–147.

[KX] A. Klapper and J. Xu, Algebraic feedback shift registers. Theor. Comp. Sci. **226** (1996), pp. 61–92.

[M1] G. Marsaglia, The mathematics of random number generators, in **The Unreasonable Effectiveness of Number Theory**, Proc. Symp. Pure Math. **46** (1992), Amer. Math. Soc., Providence R.I., pp. 73-90.

[M2] G. Marsaglia, yet another rng, posted to electronic bulletin board **sci.stat.math**, Aug1, 1994.

[MZ] G. Marsaglia and A. Zaman, A new class of random number generators. Ann. Appl. Probabl. **1** (1991), pp. 462–480.

[TE] S. Tezuka, P. L'Ecuyer, and R. Couture, On the lattice structure of add-with-carry and subtract-with-borrow random number generators. ACM Trans. Model. Comp. Sim. **3** (1993), pp. 315–331.