13 Multiply-With-Carry (MWC) Generators

To fix ideas, start with an example. Consider the multiply-with-carry generator

$$x_n = 6x_{n-1} + \text{carry mod } 10.$$

The 'multiplier' is $a = 6$ and the 'base' is $b = 10$. To implement this recursion, we need an initial carry c and an initial x. If the initial carry is less than a, so will be all subsequent carries and the sequence will be strictly periodic.

The rule for forming a new pair (c, x) is:

The new x is $ax + c \bmod b$.
The new c is $\lfloor (ax + c)/b \rfloor$, (the number of b's dropped when forming x).

Starting with, say, $c = 4$, $x_0 = 4$, the sequence $x_0, x_1, x_2, x_3, \ldots$ becomes

$$4, 8, 0, 5, 0, 3, 8, 9, 8, 3, 3, 0, 2, 2, 3, \ldots$$

with period 58, the order of b in the group of residues prime to $ab - 1 = 59$.

If the pair (c, x) is written with c a left-superscript of the output element x, full details of the sequence take the form

$${}^44, {}^28, {}^50, {}^05, {}^30, {}^03, {}^18, {}^49, {}^58, {}^53, {}^23, {}^20, {}^02, {}^12, {}^13, \ldots,$$

from which the formation rule is easily deduced: the new ${}^cx$ is just the two-digit number formed by $ax + c$ of the previous pair. That, in turn, suggests why this is such a promising method for computer implementation—we need only let the superscript c be the top half of a word w and the element x the bottom half. Then, for example, in C with $b = 2^{16}$, the new word w comes from the statement

$$w = a * (w\&65535) + (w >> 16);\ \text{followed by return}(w\&65535);$$

For practical use, the output of a MWC generator is a sequence of x's. But in order to define and establish the period, it is necessary to provide a specific structure of elements z in a set S, and a function f whose iterates,
$z, f(z), f(f(z))(= f^2(z)), f^3(z), \ldots$ form either a periodic sequence or a *rho* sequence: a tail leading to a loop (cycle).

For the MWC sequence, the finite set S is the set of ordered pairs (c, x), the current 'carry' and the current x (output) value. As above, it is convenient to designate that ordered pair in the form ${}^cx$. Then the finite set S and the function f operating on it are

$$S = \{{}^cx :\ 0 \le c < a, 0 \le x < b\}, \qquad f({}^cx) = {}^{\lfloor (ax+c)/b \rfloor}(ax + c \bmod b).$$

For practical applications of the MWC generators, $x_n = ax_{n-1} +$ carry $\bmod b$, we will always choose a and b so that $m = ab - 1$ is a prime. That is because the period of the MWC sequence depends on the initial seed pair ${}^cx$, and is always the order of b in the group of residues relatively prime to some j, with j one of the divisors of m. If m is prime, there are only two divisors, m and 1, the latter leading to (two) trivial sequences of period 1 that are easily avoided. For any non-trivial seeds ${}^cx$ the sequence is strictly periodic with period the smallest positive i for which $b^i = 1 \bmod m$.

To illustrate the complexities of the general case for composite m, consider the MWC generator $x_n = 5x_{n-1} +$ carry $\bmod 13$.

Here $m = ab - 1 = 64$, with divisors 1,2,4,8,16,32,64. The orders of 13 for moduli 1,2,4,8,16,64 are 1,1,2,4,8,16. There will be seeds ${}^cx$ which produce sequences for each of the periods 1,2,4,8,16.

This can be seen by examining the directed graph of the function f over $S = \{{}^cx :\ 0 \le c < 5, 0 \le x < 13\}$. That graph has 13 components, each a cycle. Depending on the initial seed ${}^cx$, sequences of period 1,2,4,8, or 16 are attained.

$$\begin{array}{ccccccccccccccc} {}^{0}1 & \to & {}^{0}5 & \to & {}^{0}12 & \to & {}^{4}9 & \to & {}^{3}10 & \to & {}^{4}1 & \to & {}^{0}9 & \to & {}^{3}6 \\ \uparrow & & & & & & & & & & & & & & \downarrow \\ {}^{1}0 & \leftarrow & {}^{3}2 & \leftarrow & {}^{1}8 & \leftarrow & {}^{1}4 & \leftarrow & {}^{2}3 & \leftarrow & {}^{4}5 & \leftarrow & {}^{2}11 & \leftarrow & {}^{2}7 \end{array} \qquad \begin{array}{ccccccccccccccc} {}^{0}3 & \to & {}^{1}2 & \to & {}^{0}11 & \to & {}^{4}3 & \to & {}^{1}6 & \to & {}^{2}5 & \to & {}^{2}1 & \to & {}^{0}7 \\ \uparrow & & & & & & & & & & & & & & \downarrow \\ {}^{3}0 & \leftarrow & {}^{4}7 & \leftarrow & {}^{4}11 & \leftarrow & {}^{3}12 & \leftarrow & {}^{1}10 & \leftarrow & {}^{3}4 & \leftarrow & {}^{3}8 & \leftarrow & {}^{2}9 \end{array}$$

$$\begin{array}{ccccccc} {}^{0}2 & \to & {}^{0}10 & \to & {}^{3}11 & \to & {}^{4}6 \\ \uparrow & & & & & & \downarrow \\ {}^{2}0 & \leftarrow & {}^{1}5 & \leftarrow & {}^{3}3 & \leftarrow & {}^{2}8 \end{array} \quad \begin{array}{ccccccc} {}^{0}6 & \to & {}^{2}4 & \to & {}^{1}9 & \to & {}^{3}7 \\ \uparrow & & & & & & \downarrow \\ {}^{1}1 & \leftarrow & {}^{4}2 & \leftarrow & {}^{4}1 & \leftarrow & {}^{2}12 \end{array} \quad \begin{array}{ccc} {}^{0}4 & \to & {}^{1}7 \\ \uparrow & & \downarrow \\ {}^{4}0 & \leftarrow & {}^{2}10 \end{array} \quad \begin{array}{ccc} {}^{0}12 & \to & {}^{4}8 \\ \uparrow & & \downarrow \\ {}^{2}2 & \leftarrow & {}^{3}5 \end{array} \quad \begin{array}{c} {}^{0}8 \\ \uparrow\downarrow \\ {}^{3}1 \end{array} \quad \begin{array}{c} {}^{1}11 \\ \uparrow\downarrow \\ {}^{4}4 \end{array} \quad \begin{array}{ccc} {}^{1}3\hookleftarrow & & {}^{2}6\hookleftarrow \\ & {}^{0}0\hookleftarrow & \\ {}^{3}9\hookleftarrow & & {}^{4}12\hookleftarrow \end{array}$$

Directed graph of the MWC generator $x_n = 5x_{n-1} +$ carry mod 13.

To illustrate the theory behind the MWC generator when $m = ab - 1$ is prime, consider the first example above, $x_n = 6x_{n-1} + c \bmod 10$, with $m = ab - 1 = 59$. Look at the first few of the base-10 expansions of $k/59$, with k the successive powers of 10 mod 59 : $10, 41, 56, 29, \ldots$

$$10/59 = .1694915254237288135593220338983050847457627118644067796610169$$

$$41/59 = .6949152542372881355932203389830508474576271186440677966101694$$

$$56/59 = .9491525423728813559322033898305084745762711864406779661016949$$

These expansions all have cycles of length 58, the order of 10 for modulus 59. Successive expansions have the cycle of digits left-shifted-1, since each of them is just the fractional part of 10 times the previous one. But even more:
Our multiply-with-carry sequence $4, 8, 0, 5, 0, 3, 8, 9, 8, 3, 3, 0, 2, 2, 3, \ldots$ appears as a sequence of digits in each of those expansions, *written backwards!*. The digits in these numbers of the form $k/59$ satisfy the same recursion as that of the multiply-with-carry sequence, but backwards.

On the other hand, since $a = 6$ is the inverse of $b = 10$ modulo $ab - 1 = 59$, if we expand $k/59$ to the base 10 for $k = 6, 6^2, 6^3 \bmod 59$ then each cycle is rotated left-1:

$$6/59 = .1016949152542372881355932203389830508474576271186440677966101 6$$

$$36/59 = .6101694915254237288135593220338983050847457627118644067796610 1$$

$$39/59 = .6610169491525423728813559322033898305084745762711864406779661 0$$

and once again the MWC digits appear in reverse order, and the digits, listed backwards, satisfy the multiply-with-carry recursion.

This gives an idea of the general multiply-with-carry sequence:

$$x_n = ax_{n-1} + \text{carry} \bmod b, \qquad m = ab - 1 \text{ prime} .$$

The x's may be considered 'digits' for the base b. For any initial 'seed' ${}^{c}x$ except ${}^{0}0$ or ${}^{(a-1)}(b-1)$, the sequence $x_0, x_1, x_2, \ldots$ is strictly periodic with period the order of b in the group $\{1, 2, \ldots, m-1 \bmod m\}$. Furthermore, the x's, written backwards, are the cycle of digits in the base-b expansion of k/m for some k in $\{b, b^2, b^3, \ldots \bmod m\}$. The two sequences of period 1 arise from 0^0 and ${}^{(a-1)}(b-1)$, which are fixed points for the function f.

To prove this: With $m = ab - 1$, if the base-b expansion of k/m is

$$\frac{k}{m} = .d_1d_2d_3d_4d_5d_6d_7d_8d_9\ldots,$$

then multiplying both sides by $m = ab - 1$ and collecting terms yields

$$k.d_1d_2d_3d_4d_5d_6d_7d_8d_9\ldots = a \times d_1.d_2d_3d_4d_5d_6d_7d_8d_9\ldots.$$

If we write this as in grammar school multiplication,

$$\begin{array}{r} d_1\,.\,d_2\,d_3\,d_4\,d_5\,d_6\,d_7\,d_8\,d_9\ldots \\ \times\, a \\ \hline k\,.\,d_1\,d_2\,d_3\,d_4\,d_5\,d_6\,d_7\,d_8\ldots \end{array}$$

each d_n is seen to be the product ad_{n+1} plus the carry: the number of excess b's from the previous multiplication, all reduced modulo b—exactly the multiply-with-carry rule, but in reverse order.

The directed graph of the function $z \to f(z)$ has $n = ab$ nodes. It has two trivial components, $z = f(z)$ for $z = {}^0 0$ and $z = {}^{(a-1)}(b-1)$. If the order of b for modulus m is k, then the directed graph of f on S has $(ab-2)/k$ components, each consisting of a loop of k elements, together with the two trivial loops of single elements ${}^0 0$ and ${}^{(a-1)}(b-1)$.

Note also a certain structure in the directed graph of f: If $f(z) = w$ then $f(z') = w'$, where the prime means ${}^c x \to {}^{(a-1-c)}(b-1-x)$.

In practical applications, we choose b from $2^8, 2^{16}, 2^{32}$ (or even 2^{64} in some advanced CPU's). We then choose a so that $m = ab - 1$ is a safeprime—both m and $(m-1)/2$ are prime. Then the order of b mod m will be $(m-1)/2$. It cannot be (m-1), that is, a primitive root, because b is a square.

Cemal Koç has shown that the multiply-with-carry method can be extended to linear combinations

$$x_n = a_1 x_{n-1} + a_2 x_{n-2} + \cdots + a_r x_{n-r} + \text{carry mod } b.$$

14 Recursion With Carry (RCW) Generators

We now describe an extension of add-with-carry and multiply-with-carry generators to recursion-with-carry, in which each new x is a linear combination of r previous x's, plus carry, modulo the base b. The extension is due to Cemal Koç.

The generator is

$$x(n) = a_1 x_{n-1} + a_2 x_{n-2} + \cdots + a_r x_{n-r} + \text{ carry } \bmod b,$$

where, as before, the carry is the number of b's dropped in reducing the previous linear combination modulo the base b. The latter is called the base because, as before, proof and structure depend on viewing the x's as digits in base-b expansions of a rational k/m.

Here $m = a_r b^r + a_{r-1} b^{r-1} + \cdots + a_1 b - 1$, and we assume the a's are chosen so that m is prime. Then b has an inverse in the group of residues of m: it is $b^{-1} = a_r b^{r-1} + a_{r-2} b^{r-2} + \cdots + a_1$, since $bb^{-1} = m + 1$.

The period of the generator is the order of b for modulus m, except for the two trivial seed sets $0, 0, \ldots, 0$ and $a_1 + \cdots + a_r - 1, b-1, b-1, \ldots, b-1$.

The set of possible 'carries' for RWC sequences is $0 \le c < a_1 + \cdots + a_r$ and a seed set is one such c with $x_1, \ldots, x_r$, the x's in $0 \le x < b$.

Note however, that unlike MWC sequences, which are strictly periodic for all seeds ${}^c x$ with $0 \le c < a, 0 \le x < b$, the recursion-with-carry sequences may not be strictly periodic. They will be ultimately periodic, of course. Nonetheless, they can easily be made strictly periodic by iterating the recursion r times on a proposed set of seeds to get one that ensures strict, rather than just ultimate, periodicity.

To avoid notational difficulties and yet give the essential ideas of a proof, consider, say,

$$x(n) = 3x_{n-1} + 2x_{n-2} + 4x_{n-3} + \text{ carry } \bmod b \ (= 10).$$

Here, $m = 4b^3 + 2b^2 + 3b - 1 = 4229$ and $b^{-1} \bmod m$ is $4b^2 + 2b + 3 = 423$. (It happens that 10 is a primitive root of 4229, but that is of no import. As long as m is a prime, periodic sections of the RCW sequence will have length the order of b for modulus m.)

As before, if k is one of $b, b^2, b^3, \ldots$ mod m we may express k/m to the base b:

$$k/m = .d_1d_2d_3d_4d_5d_6d_7d_8d_9\ldots$$

And that expansion is periodic with cycles of length the period of b mod m. Let F be that base-b expansion. Multiply both sides by m and arrange to get

$$k + F = 4b^4F + 2b^2F + 3bF.$$

Now, instead of doing multiplication, use successive addition of four 3-shifted F's, two 2-shifted F's and three 1-shifted F's:

$$\begin{array}{rr}
 & d_1d_2d_3.d_4d_5d_6d_7d_8d_9\ldots \\
+ & d_1d_2d_3.d_4d_5d_6d_7d_8d_9\ldots \\
+ & d_1d_2d_3.d_4d_5d_6d_7d_8d_9\ldots \\
+ & d_1d_2d_3.d_4d_5d_6d_7d_8d_9\ldots \\
+ & d_1d_2.d_3d_4d_5d_6d_7d_8\ldots \\
+ & d_1d_2.d_3d_4d_5d_6d_7d_8\ldots \\
+ & d_1.d_2d_3d_4d_5d_6d_7\ldots \\
+ & d_1.d_2d_3d_4d_5d_6d_7\ldots \\
+ & d_1.d_2d_3d_4d_5d_6d_7\ldots \\
\hline
= & k.d_1d_2d_3d_4d_5d_6\ldots
\end{array}$$

As in grammar school addition, summing columns from right to left, each d_n comes from

$$d_n = 3d_{n+3} + 2d_{n+2} + 4d_{n+3} + \text{carry mod } b,$$

with 'carry' the number of excess b's in forming the previous d—exactly the rule of the recursion-with-carry generator, but with indices reversed.

14.1 Summary

In general, when $m = ab - 1$ is prime, the period of the RWC generator

$$x(n) = a_1x_{n-1} + a_2x_{n-2} + \cdots + a_rx_{n-r} + \text{ carry } \bmod b,$$

is the order of b for modulus $m = a_rb^r + a_{r-1}b^{r-1} + \cdots + a_1b - 1$. It requires an initial carry and seeds $x_1, x_2, \ldots, x_r$.

Formally, the period is that of the sequence $z, f(z), f^2(z), \ldots$, where z is a vector with elements bracketed by $<>$:

$$z =< c, z_r, z_{r-1}, \ldots, z_2, z_1 >$$

and

$$f(< c, z_r, z_{r-1}, \ldots, z_2, z_1 >) =< \lfloor v/b \rfloor, v \bmod b, z_r, z_{r-1}, \ldots, z_3, z_2 >,$$

with $v = a_1z_1 + a_2z_2 + \cdots + a_rz_r$.

This sequence may be a *rho* sequence—that is, like the letter ρ, with a tail leading to a loop. For the recursion-with-carry sequence, that tail is never longer than r, so for a given seed set, iterating r times with f will produce a new seed that ensures a strictly periodic sequence.

There is a certain structure in the directed graph of the function $z \rightarrow f(z)$ with nodes

$$z =< c, x_r, x_{r-1}, \ldots, x_2, x_1 >, \qquad 0 \le c < s, 0 \le x_i \le b$$

and $s = a_1 + \cdots + a_r$. There are $n = sb^r$ nodes. There are two trivial components of the graph: $z = f(z)$ for $z =< 0, 0, \ldots, 0 >$ and $< s-1, b-1, b-1, \ldots, b-1 >$.

If g is the order of b for modulus m, then the directed graph has $(n-2)/g$ non-trivial components (connected subgraphs). Furthermore if $f(z) = w$ then $f(z') = w'$, where z' is a sort of 'complement' of z: the c component of z is replaced by $s-1-c$ and each x_i is replaced by $b - 1 - x_i$.

Each of the non-trivial components of the graph can be pictured as a sort of ciliated cell, the nucleus a loop of size g and various cilia of lengths 1 to r dangling from the cell body.