

Simple Cellular Automata as Pseudorandom m -Sequence Generators for Built-In Self-Test

MAKOTO MATSUMOTO

Keio University/Max-Planck-Institut für Mathematik

We propose an extremely simple and explicit construction of cellular automata (CA) generating pseudorandom m -sequences, which consist of only one type of cells. This construction has advantages over the previous researches in the following points. (1) There is no need to search for primitive polynomials; a simple sufficient number-theoretic condition realizes maximal periodic CA with periods $2^m - 1$, $m = 2, 3, 5, 89, 9689, 21701, 859433$. (2) The configuration does not require hybrid constructions. This makes the implementation much easier. This is a modification of the Rule-90 by Wolfram. We list our CAs with maximal period, up to the size 300. We also discuss the controllability of the CA, randomness of the generated sequence, and a two-dimensional version.

Categories and Subject Descriptors: B.7.1 [Integrated Circuits]: Types and Design Styles—*standard cells; VLSI*; G.3 [Probability and Statistics]—*random number generation*

General Terms: Algorithms, Theory

Additional Key Words and Phrases: Cellular automata, finite fields, m -sequence, pseudorandom number generation, VLSI

1. INTRODUCTION

The built-in self-test includes a pseudorandom bit-pattern generator in a VLSI to test the chip with randomized inputs. A common way is to use a feedback shift register (FSR), but recently cellular automata (CA) have attracted considerable interest, since CA have the advantage that they need only short wiring between adjacent cells and no long wiring as for FSR. Note that a long wire-line in a VLSI consumes an even larger area than a circuit, and in addition it may cause trouble because of the impedance.

Hortensius et al. [1989a,b] introduced a hybrid CA in which two different types of cells are arranged (thus the name *hybrid*), and showed that some

Author's Address: Department of Mathematics, Keio University, 3-14-1 Hiyoshi, Yokohama, 223 Japan; email: matumoto@math.keio.ac.jp.

Permission to make digital/hard copy of part or all of this work for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage, the copyright notice, the title of the publication, and its date appear, and notice is given that copying is by permission of the ACM, Inc. To copy otherwise, to republish, to post on servers, or to redistribute to lists, requires prior specific permission and/or a fee.

© 1998 ACM 1049-3301/98/0100-0031 \$05.00

such CA produce m -sequences. Bardell [1990] got some examples by random search. Tezuka and Fushimi [1994] showed that any irreducible polynomial can be realized as a characteristic polynomial of such a hybrid CA, so they gave a way to design such CA with a maximal period, for any given primitive polynomial.

The approach here is different. We consider only *pure* CA, that is, consisting of only one type of cell. Then we investigate the condition on the number of cells (or size) of CA that assures the maximality of the period.

We give a simple tight necessary condition, and a simple sufficient condition, which are purely number-theoretic.

As a consequence, we have maximal-periodic CA whose sizes are 2, 3, 5, 89, 9689, 21701, and 859433. These numbers are from the table of 35 known Mersenne primes [Caldwell 1997]. These are all p in the list with the additional condition that $2p + 1$ is also a prime.

Our methods differ from the previous works in the following points.

- (1) We do not need to search for primitive polynomials. Even by Tezuka–Fushimi’s result, a primitive polynomial must be randomly searched by computers. This is a difficult task, since even in the easiest case of trinomials, only a list up to the degree of 132049 is now available.
- (2) Our CA has a far simpler configuration, involving only one type of cell. This facilitates the implementation dramatically, and it seems possible to also use it in an experimental stage of newly developing technology in integrated circuit design.

The drawback of our method is a strong limitation on the size. We give a list of the sizes ≤ 300 that attain the maximality.

The concept of cellular automata (CA) was introduced by von Neumann [1966] in the 1940s. Wolfram [1983] classified the CA of simplest type. Among them, CA with Rule90 and Rule150 can be analyzed using linear algebra, since the transition function is a linear transformation over \mathbb{F}_2 (see Martin et al. [1984]).

In this article we show that some modification of CA90 generates m -sequences of huge length. Similar observations are also done in Hortensius et al. [1989] and Yarmolik and Murashko [1993], but our method is more number-theoretic. We also consider a two-dimensional version.

2. CELLULAR AUTOMATA AS M -SEQUENCE GENERATOR

One-dimensional cellular automata CA90(m). One-dimensional cellular automata considered in this article consist of m cells concatenated as in Figure 1.

The state set of each cell is $\{0, 1\}$, identified with the two-element field \mathbb{F}_2 . The concatenating lines denote the exchange of information. Each cell looks at the two neighbor cells (except for the ends, where there is only one neighbor cell), and decides the next state. Let t denote the time in integers:

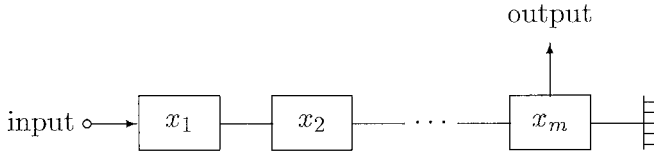


Fig. 1. A one-dimensional CA with input and output.

namely, $t = 0$ is the initial state and $t = k$ denotes k transitions of the state. We assume the transition function is \mathbb{F}_2 -linear; that is,

$$x_k(t + 1) = x_{k-1}(t) + c_k x_k(t) + x_{k+1}(t) \tag{1}$$

for some constants $c_k \in \mathbb{F}_2$, for $k = 1, 2, \dots, m$. We consider the ends later. For $c_k = 0, 1$, the k th cell is called Rule90, Rule150, respectively (see Wolfram [1983]). This transition function is \mathbb{F}_2 -linear, and the maximality of the period (i.e., the period coincides with $2^m - 1$) is equivalent to the primitivity of the characteristic polynomial of this transformation.

Hortensius et al. and Bardell considered a hybrid of these two kinds of cells, and Tezuka–Fushimi proved that any irreducible polynomial can be realized as the characteristic polynomial of such generators.

Here we return to the pure situation considered by Wolfram [1983], and consider only the case of $c_k = 0$ for all k . With a null-boundary condition, namely, the assumption that $x_0(t) \equiv x_{m+1}(t) \equiv 0$ in the recurrence (1), this coincides with CA with Rule90 in Wolfram [1983]. However, this never attains the maximal period $2^m - 1$. If the CA is maximal, then all nonzero states constitute one cyclic orbit, but if we start from a horizontally symmetric state, it can never reach a nonsymmetric state.

So, in this article, we destroy this symmetry by putting a mirror at the right end as shown in Figure 1, namely,

$$x_{m+1}(t) = x_m(t), \tag{2}$$

instead of the null boundary condition. (In other words, we put one Rule150 cell at the right end. But in the practical implementation, a cell of Rule90 with a loop wire at the right end suffices.) We call this CA $CA90(m)'$.

In Section 3 we prove some number-theoretic conditions on m to attain the maximal period.

To set an initial state, we consider an input $\iota(t) \in \mathbb{F}_2$ to the left end, namely,

$$x_0(t) = \iota(t). \tag{3}$$

We prove the controllability of this automaton in Section 6, and treat a two-dimensional version in Section 4.

Table I. List of $1 \leq m \leq 300$ satisfying the necessary condition in Theorem 3.1 (those m not marked with * give maximal periodic $CA90(m)'$)

*1	2	3	5	6	9	11	14	*18	23
26	29	30	33	35	39	41	*50	51	53
65	69	74	81	83	86	89	90	95	*98
*99	105	113	119	131	*134	135	146	155	158
173	*174	179	183	*186	189	191	*194	209	210
221	230	231	233	239	243	245	251	254	261
*270	273	*278	281	293	299				

3. CONDITIONS ON THE SIZE FOR MAXIMALITY

3.1 A Condition Equivalent to Irreducibility

For an odd integer k , let $\text{subord}(2; k)$ denote the minimum positive integer s such that $2^s \equiv \pm 1 \pmod{k}$. This is nothing but the order of 2 in the multiplicative group $(\mathbb{Z}/k)^\times / \{\pm 1\}$.

The following theorem gives a necessary and sufficient condition for the characteristic polynomial of $CA90(m)'$ to be irreducible. Thus, it gives a strong necessary condition for the CA to have the maximal period.

THEOREM 3.1 *The characteristic polynomial of the transition map of $CA90(m)'$ is irreducible¹ if and only if*

$$m = \text{subord}(2; 2m + 1).$$

This is a necessary condition for $CA90(m)'$ to have the maximal period $2^m - 1$.

A proof is given in Section 3.2. It is very difficult to obtain a simple necessary and sufficient condition on m to attain the maximal period.

Table I lists all the m , $1 \leq m \leq 300$, that satisfy the necessary condition in Theorem 3.1. For those m without *, $CA90(m)'$ has the maximal period. Thus there are 55 maximal periodic CA90's for $1 \leq m \leq 300$, and there are 11 m s that satisfy the necessary condition in Theorem 3.1 for which $CA90(m)'$ is not maximal.

If $2^m - 1$ is a prime (a prime of this form is called a Mersenne prime), then the irreducibility and the primitivity of a polynomial of degree m are equivalent.

In this case we can prove the following.

THEOREM 3.2 *Suppose that $2^m - 1$ is a prime. Then $CA90(m)'$ has the maximal period if and only if $2m + 1$ is prime.*

¹P. Moree at the Max-Planck-Institut pointed out the following. By using Hooley's method [Hooley 1967], one can prove that under the Generalized Riemann Hypothesis the asymptotic estimate $M(x) \sim 2Ax/(\log x)$ holds, where $M(x) := \#\{m \leq x : m = \text{subord}(2; 2m + 1)\}$ and $A = \prod_{p:\text{prime}}(1 - (1/p(p - 1))) = 0.39 \dots$ is Artin's constant.

This theorem shows that exactly 7 Mersenne exponents among the known 35 (see Caldwell [1997]; the largest one presently known seems to be 1398369) yield maximal periodic CA90(m)'. These are $m = 2, 3, 5, 89, 9689, 21701, 859433$.

3.2 Proof of Theorems 3.1 and 3.2

It is easy to see that the representation matrix of the linear transition given by (1) with $c_k = 0$, (2) and (3) with null input $\iota(t) \equiv 0$ is

$$\begin{pmatrix} x_1(t+1) \\ \vdots \\ x_m(t+1) \end{pmatrix} = B_m \begin{pmatrix} x_1(t) \\ \vdots \\ x_m(t) \end{pmatrix}, \quad B_m = \begin{pmatrix} & 1 & & & \\ 1 & & 1 & & \\ & 1 & & \ddots & \\ & & \ddots & & 1 \\ & & & & 1 & 1 \end{pmatrix}. \quad (4)$$

Let $\beta_m(t)$ be the characteristic polynomial of B_m . CA90(m)' has the maximal period if and only if $\beta_m(t)$ is primitive; that is, t is a generator of the multiplicative group $(\mathbb{F}_2[t]/\beta_m(t))^\times$. In this case, each cell generates a so-called m -sequence of characteristic polynomial $\beta_m(t)$.

PROOF OF THEOREM 3.1 Let us obtain all eigenvalues of B_m in $\overline{\mathbb{F}_2}$. The following easy lemma is useful.

LEMMA 3.3 *Let p, q be nonzero elements of a field. Then, $p + p^{-1} = q + q^{-1}$ holds if and only if $p = q$ or $p = q^{-1}$.*

This is because a polynomial $t^2 + (p + p^{-1})t + 1$ has at most two roots.

PROPOSITION 3.4 *Let $\xi = \xi_m$ be a primitive $(2m + 1)$ st root of 1 in the algebraic closure $\overline{\mathbb{F}_2}$. Set $\eta_i := \xi^i + \xi^{-i}$ for $i = 1, 2, \dots, m$. Then the set of the eigenvalues of B_m in $\overline{\mathbb{F}_2}$ is $\{\eta_i | i = 1, 2, \dots, m\}$, and they are all distinct.*

PROOF. Let x be a variable, and put $\mathbf{x} := {}^t(x + x^{-1}, x^2 + x^{-2}, \dots, x^m + x^{-m})$, where t denotes the transpose. By a straightforward calculation, we have

$$B_m \mathbf{x} = (x + x^{-1})\mathbf{x} + {}^t(0, 0, \dots, 0, x^{m+1} + x^{-(m+1)} + x^m + x^{-m}).$$

Thus if $x \neq 1$ and $x^{2m+1} = 1$, then $x + x^{-1}$ is an eigenvalue, and consequently the elements $\eta_i = \xi^i + \xi^{-i}$ for $i = 1, 2, \dots, m$ are eigenvalues of B_m , and all distinct by Lemma 3.3. Since B_m has at most m eigenvalues, these are all the eigenvalues of B_m . \square

LEMMA 3.5 *The Galois group of the extension $\mathbb{F}_2[\eta]/\mathbb{F}_2$ is isomorphic to the cyclic group generated by 2 in the multiplicative group $(\mathbb{Z}/(2m + 1))^\times / \{\pm 1\}$.*

PROOF. Let $F : \overline{\mathbb{F}_2} \rightarrow \overline{\mathbb{F}_2}$ be the Frobenius map defined by $F(\alpha) = \alpha^2$. It is well known that F is bijective and that the set of the conjugates of $\eta = \eta_1$

is $\{F^l(\eta) | l \in \mathbb{N}\}$. Thus, the number of conjugates of η over \mathbb{F}_2 is equal to $\min\{l | F^l(\eta) = \eta, l = 1, 2, \dots\}$, that is, the order of the Frobenius acting on η . On the other hand, $F^l(\eta) = (\xi + \xi^{-1})^{2^l} = \xi^{2^l} + \xi^{-2^l}$, and the condition $F^l(\eta) = \eta$ is equivalent to $\xi^{2^l} + \xi^{-2^l} = \xi + \xi^{-1}$. By Lemma 3.3, this is equivalent to $\xi^{2^l} = \xi^{\pm 1}$. Since the multiplicative order of ξ is $2m + 1$, the preceding identity is equivalent to $2^l \equiv \pm 1 \pmod{2m + 1}$. Thus the order of the Frobenius map is nothing but the order of 2 in the multiplicative group in the lemma. \square

COROLLARY 3.6 *Let $\eta = \xi + \xi^{-1}$, with ξ as in Proposition 3.4. Then the degree of the minimal polynomial $\varphi_\eta(t)$ of η equals $\text{subord}(2; 2m + 1)$.*

PROOF. The degree of $\varphi_\eta(t)$ equals the number of the conjugates of η over \mathbb{F}_2 , that is, the order of 2 in the multiplicative group in Lemma 3.5, which is by definition $\text{subord}(2; 2m + 1)$. \square

PROPOSITION 3.7 *The condition in Theorem 3.1 is equivalent to the irreducibility of $\beta_m(t)$.*

PROOF. This is immediate, since η is one of the roots of β_m by Proposition 3.4, and β_m is irreducible if and only if φ_η , which is irreducible and dividing β_m , has the degree m . \square

Since irreducibility is a necessary condition for primitivity, this proves Theorem 3.1.

We can state a purely numerical necessary condition on m .

THEOREM 3.8 *If β_m is irreducible, then $2m + 1$ is prime, m is not a multiple of 4, and m is not $2^s - 1$ for $s \geq 3$.*

See also Martin et al. [1984], where $2m + 1$ is proved to be prime in a very similar situation.

PROOF. By the note before Theorem 3.1, the condition $2^l \equiv \pm 1 \pmod N$ is equivalent to $\text{subord}(2; N) | l$.

Suppose that β_m is irreducible, or equivalently, that $m = \text{subord}(2; 2m + 1)$.

Then 2 is a generator of the cyclic group $(\mathbb{Z}/2m + 1)^\times / \{\pm 1\}$ of order m , and thus $(\mathbb{Z}/2m + 1)^\times$ is of order $2m$; that is, $2m + 1$ is a prime.

Retaining the condition $m = \text{subord}(2; 2m + 1)$, suppose that m is $4s$ for some s . Then $2m + 1 = 8s + 1$ is prime. Since 2 is a quadratic residue modulo $8s + 1$ (see, e.g., Serre [1973]), $2^{4s} \equiv 1 \pmod{8s + 1}$. Since $8s + 1$ is a prime number, this implies that $2^{2s} \equiv \pm 1 \pmod{8s + 1}$; that is, $4s = \text{subord}(2; 8s + 1) | 2s$, a contradiction. Thus $4 | m$ implies that β_m is not irreducible.

Also, if $m = 2^s - 1$ for some s , it is clear that $\text{subord}(2; 2m + 1) = s + 1$, and if $s \geq 3$, $\text{subord}(2; 2m + 1) = s + 1 < m$. This completes the proof. \square

The test of primitivity of β_m for large m requires computers. (But if $2^m - 1$ is known to be prime, it is equivalent to the primality of $2m + 1$.) The

author does not know a good algorithm for a primitivity test of β_m other than direct computation.

Table I was obtained by a computer program. For $m \leq 300$, check whether $m = \text{subord}(2; 2m + 1)$ and then calculate $t^{(2^m - 1)/p} \bmod \beta_m$ for every prime factor p of $2^m - 1$. If it is not 1 for any p , then β_m is primitive. The factorization of $2^m - 1$ is listed in Brillhart et al. [1988].

PROOF OF THEOREM 3.2 Suppose that m is a Mersenne exponent. Then every irreducible polynomial of degree m is primitive. Thus the condition in Theorem 3.1 is necessary and sufficient to have the maximal period. We saw in Theorem 3.8 that the primality of $2m + 1$ is necessary. We show the sufficiency. If $2m + 1$ is a prime, $2^{2m} \equiv 1 \pmod{2m + 1}$ and $2^m \equiv \pm 1 \pmod{2m + 1}$. Thus $\text{subord}(2; 2m + 1)$ divides m , and since m is a prime, $m = \text{subord}(2; 2m + 1)$. Thus irreducibility is automatic. Therefore, in this case, the primality of $2m + 1$ is equivalent to the maximality of $\text{CA90}(m)'$. This completes the proof of Theorem 3.2. There are only 7 such m among the known 35 Mersenne exponents. These are $m = 2, 3, 5, 89, 9689, 21701, 859433$.

It is interesting to note the following. The irreducibility of β_m is equivalent to a simple numerical condition on m . On the contrary, the irreducibility of a given trinomial of large degree is a difficult problem (see Kurita and Matsumoto [1991] and Heringa et al. [1992]). Thus, by number-theoretic investigation, we can find explicit irreducible polynomials without using computers.²

4. TWO-DIMENSIONAL ANALOGUE

As a two-dimensional analogue, we consider the automaton in Figure 2, called $\text{CA90}(n, m)'$. Each cell determines the next state by

$$x_{kl}(t + 1) = x_{k(l-1)}(t) + x_{k(l+1)}(t) + x_{(k-1)l}(t) + x_{(k+1)l}(t), \quad (5)$$

$1 \leq k \leq n$, $1 \leq l \leq m$, where mirrors are put at the right ends and the bottom ends. Thus we assume $x_{k(m+1)} \equiv x_{km}$ and $x_{(n+1)l} \equiv x_{nl}$. The inputs are usually zero. They are used only for the initialization. These CA generate a pseudorandom vector of size m at each step.

We have an analogue to Theorem 3.1.

THEOREM 4.1 *If $\text{CA90}(n, m)'$ has the maximal period $2^{nm} - 1$, then*

$m = \text{subord}(2; 2m + 1)$, $n = \text{subord}(2; 2n + 1)$, and $\text{gcd}(n, m) = 1$.

PROOF. Actually, this condition is again equivalent to the irreducibility of the characteristic polynomial.

Let $\xi, \zeta \in \mathbb{F}_2$ be elements with $\xi^{2n+1} = 1$, $\xi \neq 1$, $\zeta^{2m+1} = 1$, and $\zeta \neq 1$.

²During the author's stay at the Max-Planck-Institute, D. Zagier kindly informed the author of H. W. Lenstra, Jr.'s trick to prove that $t^{2^{127}-1} + t + 1$ is irreducible. It is highly likely that this is primitive, but it seems we cannot check.

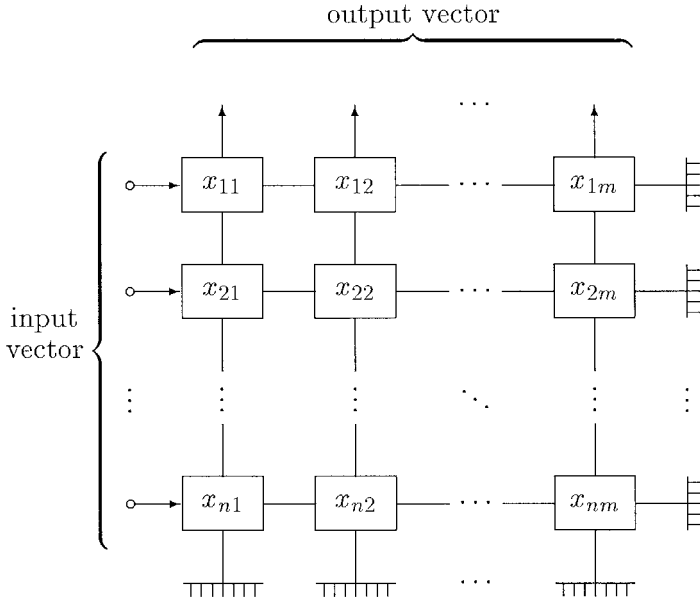


Fig. 2. CA90(n, m)' with inputs and outputs.

The transition function for CA90(n, m)' is $X \mapsto B_n X + X B_m$, when the state X is identified with an $n \times m$ matrix. From this and Proposition 3.4, it is easy to see that the $(n \times m)$ -matrix

$$((\xi^i + \xi^{-i})(\zeta^j + \zeta^{-j}))_{ij} \tag{6}$$

is an eigenvector of (5) with eigenvalue

$$\xi + \xi^{-1} + \zeta + \zeta^{-1}. \tag{7}$$

By considering the Frobenius map F , all the conjugates of (7) are again of the form (7), where ξ, ζ may be replaced by other roots of unity of the same order. The number of different such elements is at most nm .

Assume that the characteristic polynomial is irreducible. Then, since the dimension of the state space must coincide with the number of conjugates of (7), the order of the Frobenius map acting on the element (7) must be nm . It is clear that this order divides $\text{lcm}(\text{subord}(2; 2n + 1), \text{subord}(2; 2m + 1))$. Because $\text{subord}(2; 2n + 1)$ is the order of 2 in $(\mathbb{Z}/(2n + 1))^{\times}/\{\pm 1\}$, it is at most n . Now the inequality $nm \mid \text{lcm}(\text{subord}(2; 2n + 1), \text{subord}(2; 2m + 1)) \leq nm$ implies $n = \text{subord}(2; 2n + 1)$, $m = \text{subord}(2; 2m + 1)$, and that they are coprime. This is nothing but the condition in Theorem 4.1.

For the converse, it is enough to show that the order of the Frobenius mapping on the element (7) is nm , where ξ, ζ is a primitive $(2n + 1)$ st, $(2m + 1)$ st root of unity, respectively.

By the condition $\gcd(\text{subord}(2; 2n + 1), \text{subord}(2; 2m + 1)) = 1$, the orbit is the direct product of the orbits on $\xi + \xi^{-1}$ and $\zeta + \zeta^{-1}$. By the condition $n = \text{subord}(2; 2n + 1)$, $m = \text{subord}(2; 2m + 1)$, every nontrivial $(2n + 1)$ st, $(2m + 1)$ st root occurs in the orbit, respectively. Thus all we have to do is to show that (7) is distinct from each other for any distinct pairs $(\xi + \xi^{-1}, \zeta + \zeta^{-1})$, where ξ and ζ run over the nontrivial roots of unity. Suppose that some of them coincide. The extension degree of $\mathbb{F}_2[\xi + \xi^{-1}]$, $\mathbb{F}_2[\zeta + \zeta^{-1}]$ over \mathbb{F}_2 is $n = \text{subord}(2; 2n + 1)$, $m = \text{subord}(2; 2m + 1)$, respectively, and they are coprime. Thus the intersection of these two fields is trivial, that is, \mathbb{F}_2 . If (7) assumes the same value for two distinct pairs, then

$$\xi_1 + \xi_1^{-1} + \zeta_1 + \zeta_1^{-1} = \xi_2 + \xi_2^{-1} + \zeta_2 + \zeta_2^{-1}$$

holds. This implies

$$\xi_1 + \xi_1^{-1} + \xi_2 + \xi_2^{-1} = \zeta_1 + \zeta_1^{-1} + \zeta_2 + \zeta_2^{-1} \in \mathbb{F}_2.$$

If this value is zero, then by Lemma 3.3 we have $\xi_1 = \xi_2^{\pm 1}$ and $\zeta_1 = \zeta_2^{\pm 1}$, contradicting the assumption. Assume that this value is 1. By the condition that $n = \text{subord}(2; 2n + 1)$, $\xi_2 + \xi_2^{-1}$ is a nontrivial conjugate of $\xi_1 + \xi_1^{-1}$. Let σ be an element of the Galois group of $[\mathbb{F}_2[\xi + \xi^{-1}] : \mathbb{F}_2]$ which realizes this conjugate. Then

$$\begin{aligned} & \sigma^2(\xi_1 + \xi_1^{-1}) - (\xi_1 + \xi_1^{-1}) \\ &= \sigma(\sigma(\xi_1 + \xi_1^{-1}) - (\xi_1 + \xi_1^{-1})) + \sigma(\xi_1 + \xi_1^{-1}) - (\xi_1 + \xi_1^{-1}) \\ &= 1 + 1 = 0. \end{aligned}$$

Thus σ acts on $\xi_1 + \xi_1^{-1}$ with order two, and the Galois group has an even order. Therefore $2|n$. Similarly, $2|m$. This contradicts the assumption $\gcd(n, m) = 1$. \square

Unfortunately, we do not have a good sufficient condition in this two-dimensional case, since $2^{nm} - 1$ can never be a prime unless n or m is one. We used a computer program to make a list of all the parameters n, m satisfying the necessary condition in Theorem 4.1 for $1 \leq m \leq n \leq 64$ and $nm \leq 300$, as shown in Table II.

In addition to this list, we applied the same computer program to some larger values, and found that CA90(29, 35)' has the maximal period $2^{29 \times 35} - 1$. This particular value is of interest, since n and m are near 32, and many computers use 32-bit words. Another reason to select this particular value is that $2^{29 \times 35} - 1$ is completely factorized [Brillhart et al. 1988]. We need the factorization to check the maximality of the period.

Table II. List of (n, m) , $1 \leq m \leq n \leq 1$, $nm < 300$ satisfying the necessary condition in Theorem 4.1 (those (n, m) not marked with * give maximal period CA)

(2,1)	(3,1)	(3,2)	(5,1)	*(5,2)
(5,3)	*(6,1)	(6,5)	(9,1)	*(9,2)
*(9,5)	(11,1)	(11,2)	(11,3)	*(11,5)
*(11,6)	(11,9)	(14,1)	*(14,3)	(14,5)
(14,9)	*(14,11)	*(18,1)	*(18,5)	*(18,11)
(23,1)	(23,2)	(23,3)	(23,5)	*(23,6)
(23,9)	*(23,11)	(26,1)	*(26,3)	*(26,5)
(26,9)	(29,1)	*(29,2)	(29,3)	(29,5)
(29,6)	(29,9)	*(30,1)	*(33,1)	*(33,2)
*(33,5)	(35,1)	*(35,2)	*(35,3)	(35,6)
(39,1)	*(39,2)	(39,5)	(41,1)	(41,2)
*(41,3)	(41,5)	*(41,6)	*(50,1)	*(50,3)
*(51,1)	(51,2)	(51,5)		

5. RANDOMNESS

Now we discuss the randomness of the output sequence. We keep the inputs zero in this section. $CA90(n, m)$ ' generates a pseudorandom m -bit vector at each step.

THEOREM 5.1 *Let $(\mathbf{y}_1, \mathbf{y}_2, \dots)$ be the output sequence of a $CA90(n, m)$ ' with maximal period. Then, for any vectors $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n \in \mathbb{F}_2^m$ that are not all $\mathbf{0}$, there exists exactly one l in a period such that*

$$(\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n) = (\mathbf{y}_l, \mathbf{y}_{l+1}, \dots, \mathbf{y}_{l+n-1}).$$

This is called the n -distribution property, and is one of the good criteria of randomness. Thus this theorem shows that if n is large, then the generated vectors show good randomness from the point of view of n -distribution.

PROOF. Since this CA assumes all the nonzero states, the preceding property is equivalent to the fact that the mapping from the state to its n consecutive outputs is bijective. By counting the dimension, it is enough to prove the injectivity, and by linearity, it is enough to show the triviality of the kernel. Thus assume that a state X produces n consecutive zero vectors. Then the first row must be zero, since it is the output at the present state and the second row will be the output at the second step, because of the recurrence (5). Thus the second row must be zero. By induction, up to the n th row must be zero; that is, $X = 0$ as desired. \square

Note that the preceding proof is valid also for hybrid types of CA. In particular, $CA90(n)$ ' generates an n -distributed 1-bit stream.

As a criterion of randomness, the n -distribution property of the output sequence of $CA90(n, m)'$ is proved. Controllability of these automata, which provides the initialization scheme, is proved.

ACKNOWLEDGMENTS

The author is thankful to R. Couture for a dramatic simplification of the proofs of Theorems 4.1 and 5.1, and grateful to H. W. Lenstra, Jr. for the valuable comments given at Oberwolfach.

REFERENCES

- BARDELL, P. 1990. Analysis of cellular automata used as pseudorandom pattern generators. In *Proceedings of the IEEE 21st International Test Conference* (Washington D.C., Sept. 1990), 762–768.
- BRILLHART, J., LEHMER, D. H., SELFRIDGE, J. L., TUCKERMAN, B., AND WAGSTAFF, S. S., JR. 1988. Factorizations of $b^n \pm 1$ (2nd ed.), *Contemporary Mathematics*, Vol. 22, AMS, Providence, RI.
- CALDWELL, C. 1997. The prime page. <http://www.utm.edu:80/research/primes/mersenne.shtml>.
- HERINGA, J., BLÖTE, H., AND COMPAGNER, A. 1992. New primitive trinomials of Mersenne-exponent degrees for random-number generation. *Int. J. Modern Physics C* 3, 561–564.
- HOOLEY, C. 1967. Artin's conjecture for primitive roots. *J. Reine. Angew. Math.* 225, 209–220.
- HORTENSIUS, P., MCLEOD, R. D., AND CARD, H. C. 1989. Parallel random number generation for VLSI systems using cellular automata. *IEEE Trans. Comput.* 38, 1467–1472.
- HORTENSIUS, P., MCLEOD, R. D., PRIES, W., MILLER, D. M., AND CARD, H. C. 1989. Cellular automata-based pseudorandom number generators for built-in self-test. *IEEE Trans. Comput.-Aided Des. Integ. Circuits Syst.* 8, 842–859.
- KURITA, Y. AND MATSUMOTO, M. 1991. Primitive t -nomials ($t = 3, 5$) over $GF(2)$ whose degree is a Mersenne exponent ≤ 44497 . *Math. Comput.* 56, 817–821.
- MARTIN, O., ODLYZKO, A., AND WOLFRAM, S. 1984. Algebraic properties of cellular automata. *Commun. Math. Phys.* 93, 219–258.
- SERRE, J. 1973. *A Course in Arithmetic*. GTM, Vol. 7, Springer-Verlag, New York.
- TEZUKA, S. AND FUSHIMI, M. 1994. A method of designing cellular automata as pseudorandom number generators for built-in self-test for VLSI. Finite fields: theory, applications, and algorithms, *Contemp. Math.* 168, 363–367.
- VON NEUMANN, J. 1966. *Theory of Self-Reproducing Automata*. A. W. Burks, Ed., Univ. of Illinois Press, Champaign, IL.
- WOLFRAM, S. 1983. Statistical mechanics of cellular automata. *Rev. Mod. Phys.* 55, 601–644.
- YARMOLIK, V. AND MURASHKO, I. 1993. Pseudo random sequence generator construction using cellular automata. *Autom. Control Comput. Sci.* 27, 9–13.

Received January 1997; revised October 1997; accepted October 1997