Simple cellular automata as pseudorandom m-sequence generators for built-in self-test

Makoto Matsumoto
Keio University/Max-Planck-Institut für Mathematik

Mathematical abstract: Let m be a positive integer, ζ be a $(2m+1)$-st primitive root of unity in the algebraic closure of the two element field $\mathbb{F}_2$. We construct a simple cellular automaton consisting of m cells, whose period is equal to the multiplicative order of $\zeta+\zeta^{-1}$. A trivial upper bound on the order is 2^m-1. We search for such m which attains this bound. Using elementary finite-field theory, for example, we show that $m = 859433$ attains the bound. This is useful as a pseudorandom-bit generator with period $2^{859433}-1$ in integrated circuits.

I would like to stress on this kind of unexpected effectiveness of classical pure algebra. Although the content is rather application-oriented, I would like to make this manuscript a MPI preprint to give an example that presently non-applicable pure mathematical researches may turn out to be unreasonably useful for the practical science in near future.

Engineering abstract: 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 two points. (1) No need to search for primitive polynomials. A simple sufficient number theoretic condition realizes maximal periodic CA's 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 also discuss the controllability of the CA, randomness of the generated sequence, and a two-dimensional version.

Categories and Subject Descriptors: B.7.1 [**Hardware**]: Types and Design Styles—*Standard cells, VLSI*; G.3 [**Mathematics of Computing**]: 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* is to include a pseudorandom bit-pattern generator in a VLSI to test the chip with randomized inputs. A common way is to use a feedbacked shift register (FSR), but recently cellular automata (CA) have gathered considerable interest, since CA has the advantage that they need only short wiring between adjacent cells and no long wiring which is necessary 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. [Hortensius et al. 1989][Hortensius et al. 1989] introduced a hybrid CA in which two different types of cells are arranged (thus called *hybrid*), and showed that some such CA produce m-sequences. Bardell[Bardell 1990] got some examples by random search. Tezuka and Fushimi[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,

Name: Makoto Matsumoto
Address: Gottfried-Claren-Strasse 26 D-53225 BONN, GERMANY. Tel. 49-228-402-0, Fax. 49-228-402-277, email:matsumoto@mpim-bonn.mpg.de
Affiliation: Max Planck Institut Für Mathematik
Address: 3-14-1 Hiyoshi, Yokohama 223 Japan, Tel. +81-45-563-1141, Fax. +81-45-563-5948, email: matumoto@math.keio.ac.jp
Affiliation: Department of Mathematics, Keio University

for any given primitive polynomial.

The approach here is different. We consider only *pure* CA's, i.e., 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's whose sizes are 2, 3, 5, 89, 9689, 21701, and 859433. These numbers are from the table of 35 known Mersenne primes[Caldwell]. These are all p in the list with the additional condition that $2p + 1$ is also a prime.

Our methods are superior to the previous works in the following two 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 available now.
It seems that $2^{859433} - 1$ is the largest period among the generators designed explicitly so far.

(2) Our CA has far a simpler configuration, involving only one type of cell. This facilitates the implementation dramatically, and it seems possible to use in an experimental stage of newly developing technology in integrated circuit design, too.

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

We also consider a two-dimensional version.

2. CA WITH RULE 90 AND OUR CA90'

The concept of cellular automata (CA) was introduced by von Neumann[von Neumann 1966] in 1940s. Wolfram[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 paper, we show that some modification of CA90 generate m-sequences of huge size. Similar observations are also done in [Hortensius et al. 1989][Yarmolik and Murashko 1993]. A new method in this paper is to use a number theoretic method to analyze the CA.

3. 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.

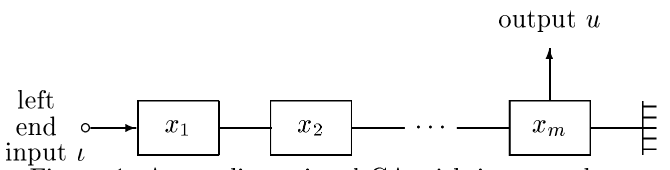

Figure 1. A one-dimensional CA with input and output.

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 the information. Each cell looks at the two directly concatenated cells (except for the ends, where there is only one concatenated cell), and decides the next state. Let t denote the time in integers, 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 $k = 1, 2, \ldots, m$. We shall consider the ends later. Accordingly to $c_k = 0, 1$, 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 and Bardell considered hybriding 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 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. However, if we start from a horizontally symmetric state, it can never reach a nonsymmetric state.

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

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

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)′*.

We shall prove some number theoretic conditions on m to attain the maximal period in §4.

To set an initial state, we consider an input to this CA. This changes the transition of the first cell as follows:

$$x_1(t+1) = \iota(t) + x_2(t), \tag{3}$$

where $\iota(t) \in \mathbb{F}_2$ is the input at the time t. We shall prove the controllability of this automaton in §7.

We shall treat a two-dimensional version in §5.

4. CONDITIONS ON THE SIZE FOR MAXIMALITY

4.1 A condition equivalent to the irreducibility

Let $\mathrm{subord}(2; k)$ denote the minimum positive integer s such that $2^s \equiv \pm 1 \bmod k$. 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 4.1. *The characteristic polynomial of the transition map of CA90$(m)'$ is irreducible* if and only if*

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

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

A proof will be given in §4.2. I think it is very difficult to obtain a simple necessary and sufficient condition for m to attain the maximal period.

Table 1 lists all the m, $1 \leq m \leq 300$, which satisfy the necessary condition in Theorem 4.1. 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 eleven m's which satisfy the necessary condition in Theorem 4.1 for which CA90$(m)'$ is not maximal.

*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				

Table 1. List of $1 \leq m \leq 300$ satisfying
the necessary condition in Theorem 4.1.
Those m not marked with $*$ give maximal-periodic CA90$(m)'$.

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

In this case we can prove

THEOREM 4.2. *Suppose that $2^m - 1$ is a prime. Then CA90$(m)'$ has the maximal period if and only if $2m+1$ is prime.*

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

---

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

4.2 Proof of Theorems 4.1 and 4.2

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

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

CA90$(m)'$ has the maximal period if and only if $\beta_m(t)$ is primitive, i.e., 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 4.1. Let us obtain all eigenvalues of B_m in $\overline{\mathbb{F}_2}$. The following easy lemma is useful.

LEMMA 4.3. *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 4.4. *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 $i = 1, 2, \ldots, m$. Then, the set of the eigenvalues of B_m in $\overline{\mathbb{F}_2}$ is $\{\eta_i \mid i = 1, 2, \ldots, m\}$, and they are all distinct.*

PROOF. Let x be a variable, and put $\mathbf{x} :=^t (x + x^{-1}, x^2 + x^{-2}, \ldots, x^m + x^{-m})$. By a straight forward calculation, we have

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

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 $i = 1, 2, \ldots, m$ are eigenvalues of B_m, and all distinct by Lemma 1. Since B_m has at most m eigenvalues, these are all the eigenvalues of B_m. □

LEMMA 4.5. *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 $F : \overline{\mathbb{F}_2} \to \overline{\mathbb{F}_2}$ 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 $\min\{l \mid F^l(\eta) = \eta, \quad l = 1, 2, \ldots\}$, i.e., 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 1, this is equivalent to $\xi^{2^l} = \xi^{\pm 1}$. Since the multiplicative order of ξ is $2m + 1$, the above identity is equivalent to $2^l \equiv \pm 1 \bmod (2m + 1)$. Thus, the order of the Frobenius map is nothing but the order of 2 in the multiplicative group in the lemma. □

COROLLARY 4.6. *Let $\eta = \xi + \xi^{-1}$, with ξ as in Proposition 4.4. Then, the degree of the minimal polynomial $\varphi_\eta(t)$ of η equals* $\mathrm{subord}(2; 2m + 1)$.

PROOF. The degree of $\varphi_\eta(t)$ equals the number of the conjugates of η over $\mathbb{F}_2$, i.e., the order of 2 in the multiplicative group in Lemma 4.5, which is by definition $\mathrm{subord}(2; 2m+1)$. $\square$

PROPOSITION 4.7. *The condition in Theorem 4.1 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 4.4, 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 4.1.

We can state a purely numerical necessary condition on m.

THEOREM 4.8. *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 4.1, the condition $2^l \equiv \pm 1 \bmod N$ is equivalent to $\mathrm{subord}(2; N) | l$.

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

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 $2m$, i.e., $2m+1$ is a prime.

Retaining the condition $m = \mathrm{subord}(2; 2m+1)$, 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, for example, [Serre 1973]), $2^{4s} \equiv 1 \bmod 8s+1$. Since $8s+1$ is a prime number, this implies that $2^{2s} \equiv \pm 1 \bmod 8s+1$, i.e., $4s = \mathrm{subord}(2; 8s+1) | 2s$, 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 $\mathrm{subord}(2; 2m+1) = s+1$, and if $s \geq 3$, $\mathrm{subord}(2; 2m+1) = s+1 < m$. 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 equvalent to the primality of $2m+1$.) The author does not know a good algorithm for primitivity test of β_m other than direct computation.

Table 1 is obtained by a computer program. For $m \leq 300$, check whether $m = \mathrm{subord}(2; 2m+1)$ 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 4.2. Suppose that m is a Mersenne exponent. Then every irreducible polynomial of degree m is primitive. Thus, the condition in Theorem 4.1 is necessary and sufficient to have the maximal period. We saw in Theorem 4.8 that the primality of $2m+1$ is necessary. We show the sufficiency. If $2m+1$ is a prime, $2^{2m} \equiv 1 \bmod 2m+1$ and $2^m \equiv \pm 1 \bmod 2m+1$. Thus $\mathrm{subord}(2; 2m+1)$ divides m, and since m is a prime, $m = \mathrm{subord}(2; 2m+1)$. Thus irreducibility is automatic. Thus, in this case, the primality of $2m+1$ is equivalent to the maximality of $\mathrm{CA90}(m)'$. This completes the proof of Theorem 4.2. There are only seven 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][Heringa et al. 1992]). Thus, by number theoretic investigation, we can find explicit irreducible polynomials without using computers†.

5. TWO DIMENSIONAL ANALOGUE CA90$(N, M)'$

As a two dimensional analogue, we consider the following automata called CA90$(n, m)'$.

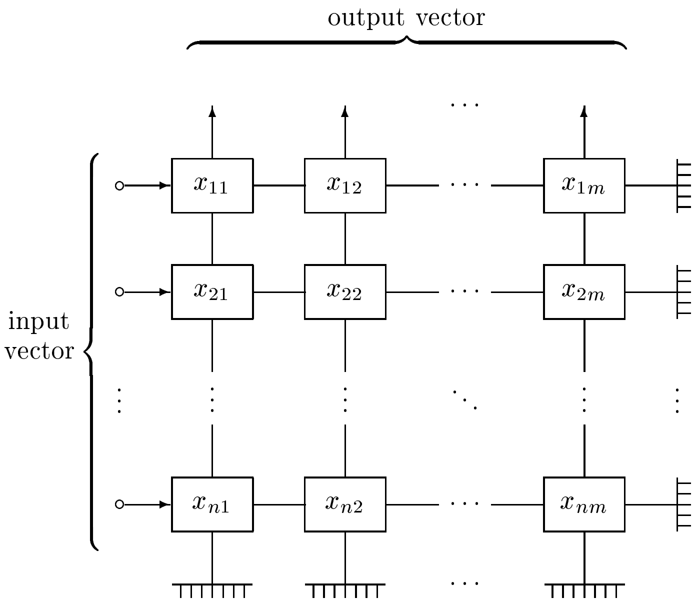

Figure 2. CA90$(n, m)'$ with inputs and outputs.

Each cell determines the next state by

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

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's generate a pseudorandom vector of size m at one time.

We have an analogue to Theorem 4.1.

THEOREM 5.1. *If CA90$(n, m)'$ has the maximal period $2^{nm} - 1$, then*

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

†During the authors' stay in Max Planck Institute, D. Zagier kindly informed the author of H.W.Jr. Lenstra'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 can not check.

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

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

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 4.4, 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), with 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 $\gcd(\mathrm{subord}(2; 2n+1), \mathrm{subord}(2; 2m+1))$. Now we claim that $\mathrm{subord}(2; 2n+1) \leq n$ for any n. This is because the extension degree of $[\mathbb{F}_2[\xi] : \mathbb{F}_2]$ is at most $2n$, that of $[\mathbb{F}_2[\xi] : \mathbb{F}_2[\xi + \xi^{-1}]]$ is two since its Galois group has an exchange of ξ and ξ^{-1}, and that of $[\mathbb{F}_2[\xi + \xi^{-1}] : \mathbb{F}_2]$ is $\mathrm{subord}(2; 2n+1)$ by the proof of Lemma 4.5. Thus we have $2 \cdot \mathrm{subord}(2; 2n+1) \leq 2n$. Now the inequality $nm | \gcd(\mathrm{subord}(2; 2n+1), \mathrm{subord}(2; 2m+1)) \leq nm$ implies $n = \mathrm{subord}(2; 2n+1)$, $m = \mathrm{subord}(2; 2m+1)$, and that they are coprime. This is nothing but the condition in Theorem 5.1.

For the converse, it is enough to show that the order of the Frobenius mapping on the element (7) is nm. By the condition $\gcd(\mathrm{subord}(2; 2n+1), \mathrm{subord}(2; 2m+1)) = 1$, the orbit is the direct product of the orbits on $\xi + \xi^{-1}$ and $\zeta + \zeta^{-1}$. By the condition $n = \mathrm{subord}(2; 2n+1)$, $m = \mathrm{subord}(2; 2m+1)$, 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 to each other for any distinct pairs $(\xi + \xi^{-1}, \zeta + \zeta^{-1})$, where ξ and ζ run over the nontrivial roots of unities. 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 $n = \mathrm{subord}(2; 2n+1)$, $m = \mathrm{subord}(2; 2m+1)$, respectively, and they are coprime. Thus, the intersection of these two fields is trivial, i.e., $\mathbb{F}_2$. If (7) assumes a 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 4.3, 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 $n = \mathrm{subord}(2; 2n+1)$, $\xi_2 + \xi_2^{-1}$ is a nontrivial conjugate of $\xi_1 + \xi_1^{-1}$. Let σ be an element of the Galois group of $[\mathbb{F}_2[\xi + \xi] : \mathbb{F}_2]$ which realizes this conjugate. Then,

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

$$= 1 + 1 = 0.$$

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

Unfortunately, we don't 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 5.1 for $1 \leq m \leq n \leq 64$ and $nm \leq 300$. We marked $*$ to those m which do not yield a 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)		

Table 2. List of (n, m), $1 \leq m \leq n \leq 1$, $nm < 300$,
satisfying the necessary condition in Theorem 5.1.
Those (n, m) without the mark $*$ give maximal period CA.

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 $2^{29\times35} - 1$. This particular value is of interest, since the input is near to and less than 32 and the output is near to and more than 32, and many computers use 32-bit words. Another reason to select this particular value is that $2^{29\times35} - 1$ is completely factorized [Brillhart et al. 1988]. We need the factorization to check the maximality of the period.

6. RANDOMNESS

Now we discuss the randomness of the output sequence. We neglect the inputs in this section. Then CA90$(m)'$ is CA90$(m, 1)'$, and it is enough to deal with only the two dimensional case. We keep the inputs zero. Then, CA90$(n, m)'$ generates a pseudorandom m-bit vector at each step.

THEOREM 6.1. *Let $(\mathbf{y}_1, \mathbf{y}_2, \ldots)$ be the output sequence of a CA90$(n, m)'$ with the maximal period. Then, for any vectors $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n \in \mathbb{F}_2^m$ which are not all $\mathbf{0}$, there exists exactly one l in a period such that*

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

This is called n-distribution property, and 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 above 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. Then, 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, i.e., $X = 0$ as desired. □

Note that the above proof is valid also for hybrid type of CA.

7. CONTROLLABILITY

In this section we neglect the outputs and deal with only the input. Thus, CA90$(m)'$ is CA90$(1, m)'$, and it is again sufficient to treat only the two-dimensional case.

An automaton with inputs is said to be *controllable with k inputs* if for any state X and Y, there exists an input sequence of length k which transforms the state X to Y.

THEOREM 7.1. *The cellular automata CA90$(n, m)'$ are controllable with m inputs.*

The proof below is again valid for hybrid type CA's. Also, it gives a method to realize a desired state from the zero state.

PROOF. By linearity, it is enough to construct a sequence of m input vectors which moves the zero state to $Y - X$.

Assume that the state is zero. (Or reset it.) Input the sequence of column vectors $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_m \in \mathbb{F}_2^n$ in this order. After this, using linearity, we see that the state matrix becomes

$$\begin{array}{l}
(\ \mathbf{y}_m,\quad \mathbf{0},\quad \mathbf{0},\quad \ldots,\quad \mathbf{0},\quad \mathbf{0})\ +\\
(B_n\mathbf{y}_{m-1},\ \mathbf{y}_{m-1},\quad \mathbf{0},\quad \ldots,\quad \mathbf{0},\quad \mathbf{0})\ +\\
(B_n^2\mathbf{y}_{m-2},\ B_n\mathbf{y}_{m-2},\ \mathbf{y}_{m-2},\quad \mathbf{0},\quad \ldots,\quad \mathbf{0})\ +\\
\qquad\qquad + \cdots +\\
(B_n^{n-1}\mathbf{y}_1,\ B_n^{n-2}\mathbf{y}_1,\ \ldots,\ B_n^2\mathbf{y}_1,\ B_n\mathbf{y}_1,\ \mathbf{y}_1).
\end{array}$$

It is clear that any matrix X can be loaded by selecting $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_m$, in this order. More precisely, $\mathbf{y}_1$ is determined as the right most row of $Y - X$. Then $\mathbf{y}_2, \mathbf{y}_3, \ldots$ is determined by

$$\mathbf{y}_2 = B_n\mathbf{y}_1 + (\text{the second right most row of } Y - X),$$

$$\mathbf{y}_3 = B_n^2\mathbf{y}_1 + B_n\mathbf{y}_2 + (\text{the third right most row of } Y - X), \ldots,$$

in this order. □

8. SUMMARY

In this paper, one-dimensional and two-dimensional linear cellular automata CA90$(m)'$ and CA90$(n,m)'$ are introduced and analyzed using finite field theory. An easy necessary condition for these CA to generate an m-sequence is provided. For the one dimensional case, a sufficient condition is also given, which realizes a very huge period. An algorithm determining the maximality of the period is given. Some such CA are listed. These CA fit to VLSI implementation better than previously studied m-sequence generators.

As a criterion of randomness, 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 5.1,6.1, and grateful to H.W.Jr. Lenstra for the valuable comment given at Oberwolfach.

REFERENCES

Bardell, P. 1990. Analysis of cellular automata used as pseudorandom pattern generators. *Proc. 1990 International Test Conference*, 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.), Volume 22 of *Contemporary Mathematics*. AMS.

Caldwell, C. 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. *International Journal of 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. on 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. Integr. 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$\leq$44497. *Mathematics of Computation 56*, 817–821.

Martin, O., Odlyzko, A., and Wolfram, S. 1984. Algebraic properties of cellular automata. *Comm. Math. Phys. 93*, 219–258.

Serre, J. 1973. *A course in arithmetic*, Volume 7 of *GTM*. Springer-Verlag.

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; Contemporary Mathematics 168*, 363–367.

von Neumann, J. 1966. *Theory of Self-Reproducing Automata* (A. W. Burks ed.). Univ. of Illinois Press.

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. *Automatic Control and Computer Sciences 27*, 9–13.