Strong Deviations from Randomness in m-sequences based on Trinomials

Makoto Matsumoto
Keio University
and
Yoshiharu Kurita
National Research Laboratory of Metrology,

The fixed vector of any m-sequence based on a trinomial is explicitly obtained. Local nonrandomness around the fixed vector is analyzed through model-construction and experiments. We conclude that the initial vector near the fixed vector should be avoided.

Categories and Subject Descriptors: G.2.1 [**Discrete Mathematics**]: Combinatorics—*recurrences and difference equations*; G.3 [**Probability and Statistics**]: random number generation

General Terms: Algorithms, Theory, Experimentation

Additional Key Words and Phrases: finite fields, m-sequences, primitive trinomials, random number generation

1. CHARACTERISTIC M-SEQUENCE

The shift-register method is widely used for generating pseudo-random numbers for Monte-Carlo simulations. The generated sequence of 0 and 1 is called an m-sequence. The most common way is to use three-term linear recursion, in other words, to use primitive trinomials as characteristic polynomial. These primitive trinomials are intensively searched in [4][5]. In this paper, however, we shall show up a serious flaw of trinomial generators. That is, for some bad initial vectors, terrible non-randomness continues for extraordinarily long time. We will see an example in Section 2 for which during approximately two billions generations (521×2^{22} successive values), the deviation of the number of ones from its theoretical mean will always be more than thirty times the standard deviation.

This is a serious defect of trinomial-based m-sequences. We should comment that another defect, the deviation of the third moment, was already discovered by Lindholm[6] in 1968. He dealt with the whole period (for relatively short-period sequences, from nowadays point of view), while here we concentrate on a local bad behaviour near the initial vector (for arbitrarily long period sequences). We should also comment that a global bad behaviour of trinomials is also warned in [2] and, for k-nomials with small k, in [1] (see also its references), from the viewpoint of

---

Name: Makoto Matsumoto
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
Name: Yoshiharu Kurita
Address: Tsukuba, Ibaraki 305 Japan, email: kuri@nrlm.go.jp
Affiliation: National Research Laboratory of Metrology

correlation coefficients.

For a given primitive polynomial $\varphi(t) = t^n + \sum_{i=0}^{n-1} a_i t^i$ over GF(2), *an m-sequence based on* φ is a nonzero sequence $(x_k)_{k\in\mathbf{N}}$ of GF(2) satisfying the linear recurrence

$$x_{k+n} = \sum_{i=0}^{n-1} a_i x_{k+i}.$$

The n-tuple $(x_0, x_1, \ldots, x_{n-1})$ is called the *initial vector* of the m-sequence. There exists a unique initial vector for which the corresponding m-sequence satisfies $x_l = x_{2l}$ for every integer l [3]. This sequence is said to be *characteristic*, and the initial vector is called *the fixed vector*. A list of fixed vectors for primitive tri- or pentanomials of degree from 2 to 168 is obtained in [11] with the aid of a computer. It has an application to coding theory (see [10]). We shall give the explicit form of the fixed vector for trinomials. The notation 0^s indicates the sequence of 0's of length s.

THEOREM 1. *If an m-sequence* $(x_k)_{k\in\mathbf{N}}$ *is based on a trinomial* $t^n + t^m + 1$ *with* $n \geq 2m$, *then its fixed vector is determined as follows.*

(1) If n *and* m *are odd, then the fixed vector is* (10^{n-1}).

(2) If n *is odd and* m *is even, then the fixed vector is* $(10^{n-m-1}10^{m-1})$.

(3) If n *is even,* m *must be odd and the fixed vector is* $(0^{n-m}10^{m-1})$.

Thus, the fixed vector contains at most two 1*'s.*

PROOF. The necessary and sufficient condition for $(x_{k_0}, x_{k_0+1}, \ldots, x_{k_0+n-1})$ to be the fixed vector is that $x_{k_0+l} = x_{k_0+2l}$ holds for n consecutive integers l. In fact, if the above equality holds for $l = l_0, l_0+1, \cdots, l_0+n-1$, then $(x_{k_0+l_0+j})_{j\in\mathbf{N}} = (x_{k_0+2l_0+2j})_{j\in\mathbf{N}}$ holds because these two sequences have the same initial vector and the same characteristic polynomial (note that $\varphi(t)^2 = \varphi(t^2)$). Since an m-sequence can be extended in reverse order, the above equality implies that $(x_{k_0+j})_{j\in\mathbf{N}} = (x_{k_0+2j})_{j\in\mathbf{N}}$. Let us fix the initial vector to be $(1, 0, \cdots, 0)$, which is not necessarily the fixed vector. Generate the next n bits. Since $n \geq 2m$ we obtain

$$\begin{array}{cccccccccccc} x_0 & x_1 & \cdots & x_{n-1} & x_n & x_{n+1} & \cdots & x_{2n-m-1} & x_{2n-m} & x_{2n-m+1} & \cdots & x_{2n-1} \\ 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0. \end{array}$$

Generate the previous m bits backward and we obtain

$$\begin{array}{ccccccccc} x_{-m} & x_{-m+1} & \cdots & x_{-1} & x_0 & x_1 & \cdots & x_{n-1} \\ 1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0. \end{array}$$

Case 1. n and m are odd.

Since both x_n and x_{2n-m} have odd indices, we have

$$(x_0, x_2, \ldots, x_{2(n-1)}) = (1, 0, \ldots, 0) = (x_0, x_1, \ldots, x_{n-1}),$$

hence k_0 is 0 and the fixed vector is (10^{n-1}).

Case 2. n is odd and m is even.

In this case k_0 is proved to be n as follows. Set $k_0 := n$, $h := (n-1)/2$, and we have

$$\begin{aligned}&(x_{k_0-2h}, x_{k_0-2h+2}, \ldots, x_{k_0-2}, x_{k_0}, x_{k_0+2}, \ldots, x_{k_0+2h})\\&= (x_1, x_3, \ldots, x_{n-2}, x_n, x_{n+2}, \ldots, x_{2n-1})\\&= (0, 0, \ldots, 0, 1, 0, \ldots, 0)\\&= (x_{k_0-h}, x_{k_0-h+1}, \ldots, x_{k_0-1}, x_{k_0}, x_{k_0+1}, \ldots, x_{k_0+h}).\end{aligned}$$

This implies that $k_0 = n$ and that the fixed vector is $(10^{n-m-1}10^{m-1})$.

Case 3. Otherwise.

By the irreducibility of the characteristic polynomial, n even implies m odd. Since

$$\begin{aligned}&(x_{-m}, x_{-m+2}, \ldots, x_{m-2}, x_m, x_{m+2}, \ldots, x_{2n-m-2})\\&= (1, 0, \ldots, 0, 0, 0, \ldots, 0)\\&= (x_0, x_1, \ldots, x_{m-1}, x_m, x_{m+1}, \ldots, x_{n-1}),\end{aligned}$$

k_0 is equal to m and the fixed vector is $(0^{n-m}10^{m-1})$.

☐

Note that if $n < 2m$, the reversed sequence $(x_{-k})_{k \in \mathbf{N}}$[1] has the characteristic polynomial $t^n + t^{n-m} + 1$. Thus, we can obtain the fixed vector with a little calculation, and there is no problem in assuming $n \geq 2m$ as far as randomness is concerned.

2. NONRANDOMNESS

In this section, we show terrible nonrandomness around the fixed vector, for an m-sequence based on a trinomial. Let $(x_k)_{k \in \mathbf{N}}$ be a characteristic m-sequence. The *weight* $w_{k,M}$ of the kth M-tuple $(x_k, x_{k+1}, \ldots, x_{k+M-1})$ of an m-sequence is defined as the number of 1's appearing in this tuple. The *density* $d_{k,M}$ of the same M-tuple is defined by $d_{k,M} := w_{k,M}/M$. The *normalized deviation* $v_{k,M}$ is defined by $v_{k,M} := (w_{k,M} - \mu)/\sigma$ with the mean value $\mu = M/2$ and the standard deviation $\sigma = \sqrt{M}/2$.

Suppose that the m-sequence is characteristic and based on a trinomial $t^n + t^m + 1$. We assume that n is odd since most of implementation satisfies this. We may assume that m is even by considering the reciprocal trinomial if needed. Let p_0 be the density of 1's in the tuple $(x_0, x_1, \ldots, x_{n-1})$; in other words, p_0 is the number of 1's in this tuple divided by n. We shall predict the density of the next n bits $\mathbf{x} := (x_n, x_{n+1}, \ldots, x_{2n-1})$. Since n is odd, $x_{n+1} = x_{(n+1)/2}$, $x_{n+3} = x_{(n+3)/2}$, …, and $x_{2n-2} = x_{n-1}$ hold, and hence these halves of $\mathbf{x}$ would have almost the same density p_0. The remaining half n bits $(x_n, x_{n+2}, \ldots, x_{2n-1})$ of odd index are determined by the relation $x_{k+n} = x_{k+m} + x_k$. By the assumption that n is odd and m is even, each of these bits is the sum of previous two x_i's of even index. Since an x_i of even index will be 1 with "probability" p_0, it would be predicted that each x_i of odd index contained in $\mathbf{x}$ would be 1 with "probability" $2p_0(1-p_0)$. Then the density p_1 of the vector $(x_n, x_{n+1}, \ldots, x_{2n-1})$ would be

---

[1] The suffix $-k$ is considered to be modulo $2^n - 1$.

$p_0/2 + 2p_0(1-p_0)/2 = (3p_0 - 2p_0^2)/2$. This argument holds without the assumption that the starting index of the vector is the degree of the characteristic polynomial. Let p_l be the predicted density of the vector $(x_{2^{l-1}n}, x_{2^{l-1}n+1}, \ldots, x_{2^l n-1})$ for $l \geq 1$. Then for every integer $l \geq 1$

$$p_l = (3p_{l-1} - 2p_{l-1}^2)/2$$

would hold. This is a well-known *logistic recursion* in Mathematical Biology. In Section 1 we showed that p_0 is very close to 0. Thus, it takes much time for recovering p_l near 1/2.

Figure 1. Recovery of The Ratio of 1s

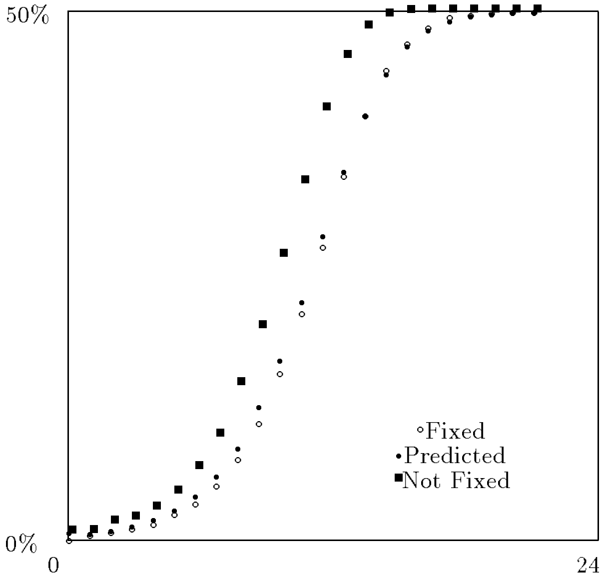

Figure 1 compares the density of an m-sequence with the one predicted by the model. The abscissa is the *logarithm* of the number of generated bits, and the ordinate is the density. Let $(x_k)_{k\in\mathbf{N}}$ be the considered m-sequence. A point (a, b) on the curve indicates that $b = d_{k,M}$ with $k = M = 2^{a-1} \cdot 521$ for $a = 1, 2, \ldots, 22$. For $a = 0$, b is the weight of the fixed vector. Thus, this figure illustrates 23 of disjoint M-tuples with M increasing exponentially.

The curve labeled "Fixed" represents the m-sequence based on a trinomial $t^{521} + t^{158} + 1$ with initial vector $(10^{362}10^{157})$, which is the fixed vector. The curve labeled "Not fixed" represents the m-sequence based on the same trinomial with initial vector (110^{519}), which is not the fixed vector. The curve labeled "Predicted" is one predicted by the model. Thus, these curves indicate the behavior of $521 \cdot 2^{22}$ bits of the m-sequences. ¿From this graph, we see that the non-fixed vector recovers far more quickly than the fixed vector.

Figure 2. Normalized Deviation

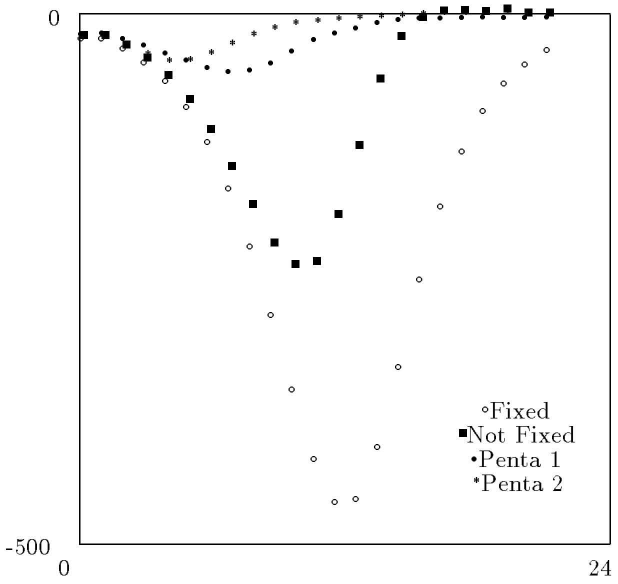

Table 1.
Normalized Deviation of Subsequences of m-sequences

a	Fixed	Not fixed	Penta 1	Penta 2
0	−2.27e+01	−2.27e+01	−1.86e+01	−2.26e+01
1	−2.27e+01	−2.25e+01	−1.73e+01	−2.23e+01
2	−3.18e+01	−3.14e+01	−2.24e+01	−3.04e+01
3	−4.47e+01	−4.38e+01	−2.86e+01	−3.97e+01
4	−6.26e+01	−6.07e+01	−3.57e+01	−4.61e+01
5	−8.71e+01	−8.30e+01	−4.26e+01	−4.50e+01
6	−1.20e+02	−1.12e+02	−4.97e+01	−3.82e+01
7	−1.64e+02	−1.47e+02	−5.35e+01	−2.94e+01
8	−2.19e+02	−1.82e+02	−5.22e+01	−2.08e+01
9	−2.84e+02	−2.18e+02	−4.55e+01	−1.47e+01
10	−3.54e+02	−2.39e+02	−3.41e+01	−1.01e+01
11	−4.20e+02	−2.36e+02	−2.31e+01	−7.95e+00
12	−4.60e+02	−1.92e+02	−1.71e+01	−6.07e+00
13	−4.57e+02	−1.26e+02	−1.23e+01	−4.88e+00
14	−4.08e+02	−6.40e+01	−7.32e+00	−3.71e+00
15	−3.33e+02	−2.36e+01	−4.61e+00	−3.13e+00
16	−2.50e+02	−5.45e+00	−3.15e+00	−1.22e+00
17	−1.81e+02	+5.22e−01	−3.18e+00	−1.05e+00
18	−1.29e+02	+7.05e−01	−2.37e+00	−9.10e−01
19	−9.11e+01	−4.87e−01	−2.30e+00	−6.74e−01
20	−6.47e+01	+2.35e+00	−2.77e+00	+5.46e−02
21	−4.65e+01	−1.43e+00	−2.47e+00	−3.87e−01
22	−3.38e+01	−1.42e+00	−2.20e+00	−4.27e−01

Figure 2 illustrates the normalized deviation of the weight from the expectation. The abscissa is the same one as in Figure 1. The ordinate is the normalized deviation. Let a be a positive integer. After calculating the normalized deviation $s_a := v_{k,M}$ with $k = M = 2^{a-1} \cdot 521$, we plot the point (a, s_a) to obtain Figure 2. For $a = 0$, s_a is the normalized deviation of the initial vector. The range of the ordinate is from -500 to 0. The same data are listed in Table 1. Since s_a should approximately conform to the standard Gaussian distribution, if $s_a < -2$, then the subsequence will be rejected with a 2.5% significance level. The curves labeled "Fixed" and "Not fixed" represent the same sequences as in Figure 1. The m-sequence "Fixed" is rejected throughout $521 \cdot 2^{22}$ bits, though "Not Fixed" recovers after $521 \cdot 2^{17}$ bits. The curve labeled "Penta-1" represents the m-sequence based on a primitive pentanomial $t^{521} + t^{510} + t^{169} + t^{158} + 1$, starting with its fixed vector $((10^{10})^{47}10^3)$. Though "Penta-1" is better than "Not fixed" for the first $521 \cdot 2^{16}$ bits, it cannot enter the 95% area throughout $521 \cdot 2^{22}$ bits (see Table 1). This implies that pentanomials do not necessarily solve the problem completely. The curve labeled "Penta-2" represents the m-sequence based on a primitive pentanomial $t^{521} + t^{170} + t^{11} + t^2 + 1$ starting with its fixed vector $(10^{350}10^{167}10)$. It can be seen from Table 1 that, in the long run, "Penta-2" is far better than "Penta-1".

Figure 3. Normalized Deviation (Nonlogarithmic abscissa)

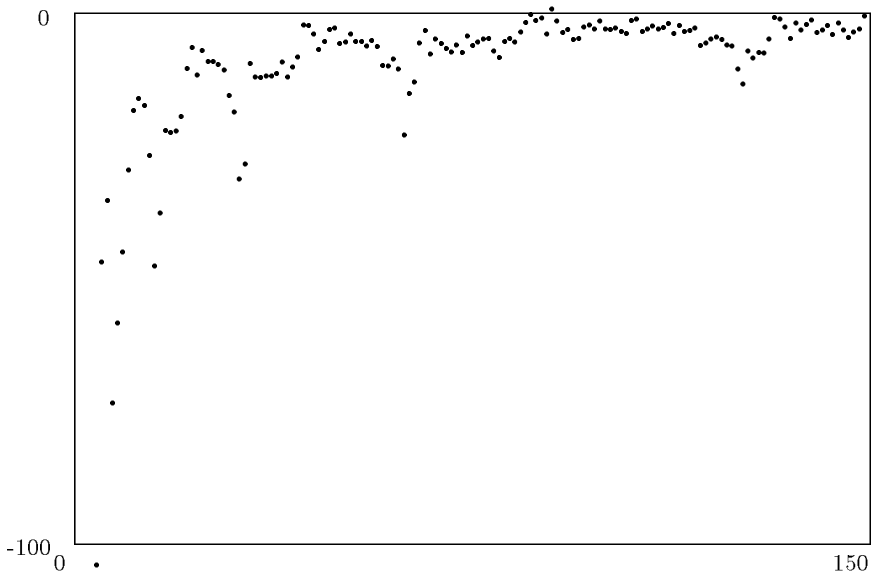

Figure 3 illustrates the normalized deviation of *disjoint* M-tuples of the m-sequence "Fixed" for fixed $M = 521 \cdot 2^{15}$. We plot $(a, v_{aM,M})$ for $a = 0, 1, \ldots, 149$. The obtained curve is not so smooth as Figure 1 or 2, and has rather "fractal" structure. This can be explained as follows. Since $x_l = x_{2l}$ for every l, the weight $w_{aM,M}$ would be much influenced by $w_{aM/2,M/2}$ rather than $w_{(a-1)M,M}$ if M is sufficiently large. Thus, the curve obtained by plotting $(a, w_{aM,M})$ is possibly not continuous and would have self-similarity. In fact, Figure 3 shows steep valleys at $a = 7, 15, 31, 63, 127$. This justifies the method used in Figures 1 and 2, where the size of the tested M-tuples is increased exponentially to make the curve smooth.

3. CONCLUDING DISCUSSIONS

How strong is the deviation observed in Table 1? A rough estimate of the probability that the normalized deviation exceeds a large positive constant C is:

$$\frac{1}{\sqrt{2\pi}} \int_C^\infty \exp(-\frac{t^2}{2})dt \le \frac{1}{\sqrt{2\pi}} \int_C^\infty \frac{t}{C} \exp(-\frac{t^2}{2})dt$$

$$= \frac{1}{C\sqrt{2\pi}}[-\exp(-\frac{t^2}{2})]_C^\infty$$
$$= \frac{1}{C\sqrt{2\pi}}\exp(-\frac{C^2}{2}).$$

We consider the probability that a tuple of length M with normalized deviation less than $-C$ occurs at least once in a random 0-1 sequence of length p ($p \gg M$). There are nearly p tuples in this sequence. If 0 and 1 are randomly chosen, the probability that at least one such tuple occurs is bounded from above by

$$p \times \frac{1}{C\sqrt{2\pi}}\exp(-\frac{C^2}{2}).$$

¿From Table 1, we observe in "Fixed" 13 consecutive tuples (6th to 18th) with normalized deviation smaller than -100. Since $p \sim 2^{521} \sim 10^{157}$ and $\exp(-5000) \sim 10^{2171}$, such a tuple appears once (or more) with probability less than 10^{-2000}. Even for $C = -30$, this probability is less than 10^{-2}. This shows that these deviations are terribly improbable in a truly random sequence.

Thus, if trinomials are used, then one should pay special attention in choosing an initial vector which is far from the fixed vector. For this, one can take an index far away from the fixed vector, and then calculate the corresponding vector by a jumping-ahead technique.

However, we note that there are other dangerous zones than the one around the fixed vector. Let $p = 2^n - 1$ be the period. Then, since $x_{(p+1)/2} = x_{p+1} = x_1, x_{(p+3)/2} = x_{p+3} = x_3, \ldots$, those x_i with index i near $(p+1)/2$ inherit the same deviation as around the fixed vector. Similarly, it holds that $x_{(p+1)/4} = x_{p+1} = x_1, x_{(p+5)/4} = x_{p+5} = x_5, \ldots$, and $x_{(3p+3)/4} = x_{3p+3} = x_3, x_{(3p+7)/4} = x_{3p+7} = x_7, \ldots$. Thus, the vectors with indices 0 modulo 2^{n-j} for small integer j (say, $j \leq 20$) would have the same tendency. There are 2^{n-j} such indices.

We conclude that trinomials should be avoided for serious simulations, since the generated sequence will show terrible nonrandom deviation many times in a period. If trinomials are used, then one should make sure that the initial vector is far from the fixed vector and from those vectors with index divisible by 2^{n-j} for small j.

There are several alternatives to trinomials. Some of them are: to use pentanomials [5], to combine trinomials [8][9], and to twist [7]. It seems that, also for these generators, the behaviour around the fixed vector would be worth testing.

ACKNOWLEDGMENTS

The authors are grateful to Prof. Nobuo Yoneda for helpful discussion, and to the anonymous referees for valuable comments.

REFERENCES

[1] Compagner, A. The hierarchy of correlations in random binary sequences. Journal of Statistical Physics **63** (1991), 883–896.

[2] Fredricsson, S. A., Pseudo-randomness properties of binary shift register sequences. IEEE Transactions on Information Theory **21** (1975), 115–120.

[3] Golomb, S. W., Shift Register Sequences Holden-Day, San Francisco, 1967.

[4] Heringa, J.R., Blöte, W.J., and Compagner, A. New primitive trinomials of Mersenne-exponent degrees for random-number generation. International Journal of Modern Physics C **3** (1992), 561–564 .

[5] Kurita, Y. and Matsumoto, M. Primitive t-nomial ($t = 3, 5$) over GF(2) whose degree is a Mersenne exponent ≤ 44497. Mathematics of Computation **56** (1991), 817–821.

[6] Lindholm, J. H. An analysis of the pseudo-randomness properties of subsequences of long m-sequences. IEEE Transactions on Information Theory **14** (1968), 569–576.

[7] Matsumoto, M. and Kurita, Y. Twisted GFSR generators II. ACM Transactions on Modeling and Computer Simulation **4** (1994), 254–266.

[8] Tezuka, S. and L'Ecuyer, P. Efficient and Portable Combined Tausworthe Random Number Generators. ACM Transactions on Modeling and Computer Simulation **1** (1991), 99–112.

[9] Wang, D. K., Compagner, A. On the use of reducible polynomials as random number generators. Mathematics of Computation **60** (1993), 363–374.

[10] Willett, M. Cycle representatives for minimal cyclic codes. IEEE Transactions on Information Theory **21** (1975), 716–718.

[11] Willett, M. Characteristic m-Sequences. Mathematics of Computation. **30** (1976), 306–311.