数理解析研究所講究録 1384 巻 2004 年 190-198

Sound - Image Processing and Random Numbers

法政大学・工学部 長坂建二 (Kenji Nagasaka)
Department of System and Control Engineering
Faculty of Engineering, Hosei University

1. INTRODUCTION

Since computers become powerful tool in many fields, simulation studies and Monte-Carlo method have been widely used by many reseachers in engineering, physice, chemistry and mathematics, etc. $\cdots$. Random numbers or random sequences are indeed indispensable for simulation studies. Introduction is devoted a quick survey for random numbers generation by digital computers of von Neumann type.

The first method is proposed by von Neumann himself called Middle-Square Method. Select one natural number m_0 with k digits in its decimal expansion and calculate m_0^2; m_0^2 has approximately $2k$ digits, then we choose k digits from the central part of the decimal expansion of m_0^2 which can be considered as a nutural number of k digits, denoted by m_1. Then we repeat this procedure by replacing m_0 by m_1, and m_i by m_{i+1} after repeating i-times this procedure, so that we obtain a sequence of natural numbers $\{m_i\}$.

At the early stage of digital computers, they act with very slow speed and the storage size is quite limited. Hence, von Neumann proposes a simple algorithm without consuming the memory of computers. Unfortunately, the period of sequences $\{m_i\}$ generated by the Middle-Square Method is proved to be fairly short and keenly dependent on the initial number m_0, then this algorithm is abondoned almost immediately.

In 1948, D. H. Lehmer propose the linear congruential method such as

$$x_{n+1} \equiv ax_n \pmod{m}, \tag{1}$$

and also its simple exention called mixed congruential method defined by

$$x_{n+1} \equiv ax_n + c \pmod{m}, \tag{2}$$

where a is a non-zero integer called the multiplier, m is the mudulus of linear congruences (1) and (2), and the second constant c of natural number signifies the shift operator, [9]. The mudulus m is chosen to be a multiple of the bits of CPU (Central Processing Unit), and 2^{32} or 2^{64} are popular moduli for the main frame. This algorithm generates an integer sequence $\{x_n\}$ of 0 to $2^{32}-1$ or $2^{64}-1$, accoring to the number of bits of CPU, respectively. Then, by dividing each x_n (mod m) by 2^{32} or 2^{64}, we obtain a quantified sequence of real numbers $\{u_n\}$ satisfying $0 \leq u_n < 1$. Appropriate choice of the multiplier a and the shift operator c, gives uniformity of the qenerated sequence $\{x_n\}$. Further, we have very long penriod for $\{x_n\}$ and consequently for $\{u_n\}$.

Generally speaking, sequences generated by a simple formula in digital computers are called pseudo random numbers, since they behave as outcomes of the observed sample values from the uniform distribution on the right-open unit interval $I_0 = [0, 1)$, which is supposed to be independent identically distributed. abbrevited to i. i. d. The conditions on the identically distributed, in this case, the uniformity on $I_0 = [0, 1)$ are not so difficult to obtain theoretically. Indeed, the period of pseudo random sequence is determinde by the index of the multiplier a, so that the problem becomes how we realize independence in pseudo random numbers.

Thesretically from the results of Dieter [1], we can calculate autocorrelation functions of linear congruential random sequences by means of Dedekind sums. Some further detailed investigations on linear congruential method are reviewed in [16] by H. Niederreiter, hence this linear congruential methods has a very long life and even now this method is used, for example, in the library of C computer language as a standard random number generation method. Nevertheless, the defect of linear congruential method, i.e. a crystal structure is pointed out by Marsaglia [10], and also in [16].

Here, we give a simple example of a crystal structure : let us consider a linear congruential method ; $x_{n+1} \equiv 5x_n + 1 \pmod{16}$, with the initial value $x_1 = 1$. Then, the generated sequence by the above congruence is ; $(1, 6, 15, 12, 13, 2, 11, 8, 9, 14, 7, 4, 5, 10, 3, 0)$, which satisfies the uniformity. From this sequence, we construct a 2- dimensional sequence, defined by $(x_k, x_{k;1})$ for $k = 1, 2, \cdots, 14$, ,which fall on the line : $3y + x - 21 = 0$.

Henceforth, we need to find other methods for random number generations. One eminent candidate is so-called M-sequence. M-sequence is a sequence over the finite field GF(2) generated by a primitive polynomial, of maxmum piriod $T = 2^p - 1$, from which this sequence is called M-sequence (Maximum-length lineary recurring sequence), where the primitive polynomial $f(x)$ of degree p is represented by $f(x) = \sum_{i=0}^{p} c_i x^i$, where $c_0 = c_p = 1$, and $c_i \in GF(2)$. Further, in this sequence, every block of 0 and 1 of length p appears once and only once, except $(0, 0, \cdots, 0)$ in the whole sequence of full period. Thus, M-sequence is much betler then linear congruential pseudo random sequence, [2], [6]. Futher investigation on random number generating methods and their preperies are to be confered in [4] from the point of view of monte-Carlo Methods, in [17] of Quasi-Monte Carlo Methods, in [19] of Markov Chains, and in [3] of cryptology.

2. STATISTICAL TESTS FOR RANDOM NUMBERS

From the compeny HMI, two systems of random number generators called the Clutter Box are offerd to us with some amount of research fund [1] . This random number generator is a hardware, which produces sequences of real numbers with prescribed number of digits in decimal expansion by means of heat noises. These type of random numbers are call "phisical random numbers", since they are generated by phisical devices via a phisical phenomena.

Robert Davies gives his report on Clutter Box random number generator on 28th October, 2001 to HMI company. National Institute of Standards and Technology in USA publish a standard for Security requirements for cryptographic modules FIPS-PUB 140-1, [18]. He also tested Clutter Box by Diehard tests by Marsaglia [11] and some other investigations are also included in his report. Kenji Nagasaka and H. Yamashita [15] reported their results of χ^2- test with the specification of the Clutter Box. The values

[1] Special thanks to HMI company and the generocity to give Nagasaka Laboratory the product; 2 Clutter Boxes made by HMI company which generates random numbers via heat noises.

of χ^2- statistic of $20,000$ physical numbers for subintervals of equsl length in the unit interval are ; $11.589, 15.765, 19.002, 18.715$ and 15.050.

It is of course a standard routine to execute a certain number of statistical tests, such as FIPS 1401. On the other hands, there exist theoretical notions and theorems for finite sequences, and we made some simulation studies for these theoretical facts and compare several kinds of random numbers generated by different methods including phisical random numbers. The following Section is devoted to the explanation of theoretical notions and theorems and also physical random numbers. Then, in the successive Section, we give our simulation studies to compare various kinds of random number generation methods.

Final Section is devoted to the choice of random sequences of $+1$ and -1, called PN-Sequences, to an application problem: Digital watermark in audio signals.

3. THEORETICAN NOTION AND PROPERTIES AND PHYSICAL RANDOM NUMBERS

One of the main applications of random numbers is numerical integrations and the notion of the uniform distribution mod 1 is intoroduced by H. Weyl [21] in 1916.

A real sequence $\underline{x} = (x_n)$ is uniformly distributed mod 1 if the number of indices n less than or equal to N such that the fractional part $\{x_n\}$ falls in any intervak $[a, b)$ in the right open unit interval $I_0 = [0, 1)$, that we denote by $A_N(\underline{x}; [a, b))$, divided by N tends to $b - a$ as N tends to infinity, where a real number x_n can be written as $x_n = [x_n] + \{x_n\}$. Here $[x_n]$ means the integral part of x_n and $\{x_n\}$ is the fractional part of x_n satisfying $0 \leq a < b \leq 1$.

Let us consider a finite real sequence $\underline{x} = (x_n)_{n=1}^{N}$ and the discrepancy of $\underline{x}$ is denoted by $D_N(\underline{x})$ and defined by

$$D_N(x) = \sup_{[a,b)} \left| \frac{A_N(\underline{x}; [a, b))}{N} - (b - a) \right|, \tag{3}$$

where a, b run over $0 \leq< 1$, $0 < b \leq 1$ with $a < b$. Then; $D_N(x) \to 0$ as $N \to \infty$, is the necessary and sufficient condition for which a real sequence $(x_n)_{n=1}^{\infty}$ is uniformly distributed mod 1.

A small change of the discrepancy $D_N(\underline{x})$ is called the modified discrepancy denoted by $D_N^*(\underline{x})$, defined by

$$D_N^*(x) = \sup_{[a,b)} \left| \frac{A_N(\underline{x}; [a, b))}{N} - (b - a) \right|, \tag{4}$$

that is, the supremum is taken over restricted interval $[0, a)$ with $0 < a \leq 1$ instead of any interval $[a, b)$.

Another necessary and sufficient condition of a real sequence (x_n) is uniformly distributed mod 1 is that the following equality

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(x_n) = \int_0^1 f(x)dx, \tag{5}$$

holds for any Riemann integrable function f of period 1.

For a real finite sequence $\underline{x} = (x_n)_{n=1}^N$, Koksma's inequality:

$$\left|\frac{1}{N}\sum_{n=1}^{N} f(x_n) - \int_0^1 f(x)dx\right| \leq V(f)D_N^*(\underline{x}), \tag{6}$$

is shown as theorem 5.1 in [8], where $f(x)$ is a periodic function of bounded variation $V(f)$ of period 1. We may suppose further that f has a continuous derivative on $I_0 = [0, 1)$, then the total variation $V(f)$ can be written as $V(f) = \int_0^1 |f'(x)|dx$. The koksma's inequality (6) represents the upper estimate of evaluation of numerical integrations by the procducts $V(f)$ and $D_N^*(\underline{x})$, from which we can evaluate the degree of uniformity of $\underline{x} = (x_n)_{n=1}^N$, since $V(f)$ is determined uniquely by $f(x)$.

Discrepancy and modified discrepaney of $\underline{x}$ are related by $D_N^*(\underline{x}) \leq D_N(\underline{x}) \leq 2D_n^*(\underline{x})$, which, therefore, assures the validity of Koksma's inequality.

This Koksma's inequality can be viewed as an estimate of the difference

$$\left|\frac{1}{N}\sum_{n=1}^{N} f(x_n) - \int_0^1 f(x)dx\right|, \tag{7}$$

by L_0-norm. Thus it is quite natural to estimate (7) by L^p–norm; that is

$$D_N^{(p)}(\underline{x}) = \left(\int_0^1 \left|\frac{A_N(\underline{x}; [0, a))}{N} - a\right|^p da\right)^{1/p}, \tag{8}$$

which may be called L^p– discrepancy of $\underline{x} = (x_n)_{n=1}^N$.

Niederreiter shows in [8] as Cor. 1.2 that

$$\left(D_N^{(2)}\right)^2 = \frac{1}{12N^2} + \frac{1}{2}\sum_{n=1}^{N}(x_n - s_n)^2, \tag{9}$$

where $s_n = (2n-1)/2N$. This equality shows that the minimum value of L^2-duscrepancy is attained by the sequence $(s_n)_{n=1}^N$. For the general even p, an analogous relsults are proven by the author [13].

Physical random numbers are so-called sequence of real numbers or integers generated by a hardware by means of a certain phisical phenomena. M-sequences are able to be generated by an appropriate combination of Shift Feedback Registers, which we do not call physical random number generator. The first physical random number generator in Japan is settled at the Insititute of Statistical Mathematics in 1956 [5].

By using zener diode, we constructs physical devices which generate random digits and further investigations with a short history of physical random number generator are to be reffered in [14].

4. COMOARISON OF RANDOM NUMBERS

Inthis Section, we give our results of simulation studies based on theoretical results in the preceding Section.

We calculate the difference (6) with test functions:

(a) $f_1(x) = 2x - 1$, $V(f_1) = 2$,

(b) $f_2(x) = 3x^2 - 2$, $V(f_2) = 5/3$,
(c) $f_3(x) = 32\sin(32\pi x)$, $V(f_3) = 2048$,
(d) $f_4(x) = \sin(32\pi x)$, $V(f_4) = 64$.
we use the following different random numbers:
(A) $1/2N, 3/2N, \cdots, (2N - 1/2N)$,
(B) Systematic Farey Fractopms,
(C) Rand( ) (Library Function in C),
(D) M-Sequence of degree 15,
(E) M-Sequence of degree 18,
(F) M-Sequence of degree 20,
(G) Physical Random Numbers generated by Clutter Box.
Our simulation results are compiled in

Table 1: Simulation Result 1

Random	Test functions			
Numbers	(a)	(b)	(c)	(d)
A	0.000000	0.000000	0.000000	0.000000
B	0.000122	0.000061	0.000000	0.000000
C-1	0.001341	0.001846	0.140260	0.004383
C-2	0.013910	0.006980	0.176375	0.005512
C-3	0.003038	0.005719	0.125490	0.003922
C-4	0.004617	0.002359	0.506651	0.015833
D-1	0.015793	0.000045	0.361343	0.011292
D-2	0.015901	0.000018	0.362667	0.011333
D-3	0.015845	0.000035	0.367596	0.011487
D-4	0.015867	0.000025	0.359357	0.011230
E-1	0.007446	0.001192	0.111607	0.003488
E-2	0.010157	0.008153	0.209423	0.006544
E-3	0.010071	0.008219	0.210876	0.006590
E-4	0.013597	0.009810	0.228891	0.007153
F-1	0.017331	0.009113	0.425495	0.013297
F-2	0.021130	0.011356	0.494390	0.015450
F-3	0.014452	0.009412	0.433619	0.013551
F-4	0.007350	0.002711	0.244237	0.007632
P-1	0.003633	0.004018	0.416623	0.013019
P-2	0.002855	0.003094	0.070002	0.002188
P-3	0.008995	0.002582	0.046476	0.001452
P-4	0.008557	0.001125	0.117469	0.003671

Table 2: Simulation Result 2

Random			
Numbers	p=2	p=4	p=6
A	0.000000	0.000000	0.000000
B	0.222100	0.129281	0.088379
C-1	0.338219	0.272939	0.219355
C-2	0.335490	0.269122	0.216720
C-3	0.336856	0.268148	0.213945
C-4	0.325764	0.256735	0.204355
D-1	0.329048	0.260038	0.206604
D-2	0.329045	0.260041	0.206612
D-3	0.328966	0.259888	0.206424
D-4	0.328937	0.259853	0.206399
E-1	0.343428	0.277986	0.223157
E-2	0.330682	0.265305	0.213479
E-3	0.330672	0.265139	0.213204
E-4	0.340306	0.277258	0.225826
F-1	0.344505	0.282922	0.232293
F-2	0.341257	0.276686	0.223532
F-3	0.344391	0.278607	0.224591
F-4	0.338142	0.271182	0.216797
P-1	0.331884	0.265155	0.213005
P-2	0.336236	0.268052	0.214209
P-3	0.338956	0.273393	0.221239
P-4	0.334009	0.269950	0.219222

5. SIGNAL PROCESSING AND CONCLUDING REMARKS

In order to protect the authorship right, watermarking is a powerful tool for analogue contents and also digital contents. Takano and Nagasaka propose a digital watermarking system in [ ], for audio signals of CD-MA quality.

One digital watermark embedding method proposed is thhe direct sequence system of spectrum spreading. Let $S(t)$ be the original audio signal at time t, then by

$$x(t) = S(t) \cdot g_{ks}(t), \tag{10}$$

$x(t)$ is spectrally spread signal by $g_{ks}(t)$, where $g_{ks}(t)$ is an element of PN-sequence of $+1$

and -1. Then we embed digital watermarks δ and the invense spectrum spreading by

$$x(t) \cdot g_{ks}(t) + \delta \cdot g_{ks}(t) = S(t) + \delta \cdot g_{ks}(t), \tag{11}$$

since $(r_{ks}(t))^2 = 1$, where $\delta \cdot g_{ks}$ signifies embedded watermark signals in wide range of low level of noises.

$g_{ks}(t)$ for $t = 1, 2, \cdots, N$ is called PN-sequence of $+1$ and -1, where k_s denotes the key to distinguish PN-sequence. The autocorrelation function of $\{g_{ks}(t)\}_{t=1}^{N}$ with delay h is defined by

$$R_N(g_{ks}; h) = \frac{1}{N} \sum_{t=1}^{N} g_{ks}(t) \cdot g_{ks}(t+h), \tag{12}$$

where h is an integer running form 0 to $N-1$, and we put $g_{ks}(N+u) = g_{ks}(u)$ for $u = 1, 2, \cdots N-1$ in order to calculate $R_N(g_{ks}; h)$.

The ideal PN-sequence for spectrum spreading in known as the values of autocorrelation functions, that is $R_N(g_{ks}; h) = 0$ for au non-zero delay h, Unfortunately there exist no such PN-sequences except $N = 4$, [12]. Thus we generate PN-sequence with value of autocorrelation functions and consider their effects. There exist three kinds of PN-sequences generated by using Genetic Algorithm, called GA1, GA2 and GA3, respectively. The population size of GA1 and GA2 is 128 and 256 for GA3. For all used genetic algorithms, the roulette selection rule, selection provability 0.6, one point crossing with probability 0.055 and mutation with probability 0.05 are employed. The length of GA1 is 512 and that of GA2 and GA3 is 1024 which are used repeatedly with different start point. The order of noises with digital watermarking for piano solo is: (D) < GA3 < (C) < (F) < (G) < (E) < GA2 < GA1, where (C) $\sim$ (G) represent is the last Section.

For song with piano accompanied, the order is: (F) < GA3 < GA1 < (D) < (E) < (C) < (G) < GA2.

Instead of direct sequence system with spectrum spreading, we use MDCT and Inverse MDCT (Modified Discrete Cosine Transformation) which diminishes dramatically the noises of digital watermark for every PN-sequences.

From out simulation study, we can not conclude concrete statements, nevertheless each simulation problem and required properties for random numbers are to be considered, that is our conclusion.

REFERENCES

[1] Dieter, U. : Statistical interdependence of pseudo-random numbers generated by the linear congruential methods, *Application of Number Theory to Numerical Analysis*, Ed. by S. K. Zaremba, Academic Press, (1972), 287-312.

[2] Fushimi, M. : *Random Numbers*, in Japanese. UP Applied Mathmatics Series, 12, Tokyo Univ. Publisher, (1989).

[3] Goldreich, O. : *Modern Cryptology, Probabilistic Proofs and Pseudorandomness.* Spring-Verlag, Berlin, Heidelbeng, (1999).

[4] Hammensley, J. M. and Handscomb, D. C. : *Monte Corlo Methods.* Methuen & Co. Ltd., London, (1964).

[5] Ishida, M. and Ikeda, H. : Random number generator. *Ann. Inst. Statist. Math.*, Vol. 7-2, (1956), 119-126.

[6] Kashiwagi, J. : *M-Seguences and Their Applications*, in Japanese. Sencing and Cognitions Series, 8, Shokodo Publisher, (1996).

[7] Knuth, D. E. : *The Art of Computer Programming, Vol.* 2, *Seminumerical Algorithms*, 2nd Ed., Addison-Wesloy, Reading, Mass., Translation by Shibuya, M. : *Seminumerical Algorithms/Random Numbers*, Science Publisher, Tokyo, (1981).

[8] Kuipers, L. and Niederreiter, H. : *Uniform Distribution of Sequences.* Pure and Applied Mathematics, A Wiley- Interscience Publication, John Wiley & Sons, New York · London · Sydney · Toronto, (1974).

[9] Lehmen, D. H. : Mathematical methods in large-scale computing units, *Ann. Comp. Lab. Harvard Univ.*, 26, (1951), 141-146.

[10] Marsaglia, G. : Random numbers fall mainly in the plane. *Proc. National Academy* of *Scineces*, Vol. 60, (1968), 25-28.

[11] Marsaglia, G. : *Monkey tests for random number generations.* ⟨http://stat.fsu.edu/pub/diehard/cdrom/pscript/monkey.ps⟩.

[12] Nagasaka, K. Okuda, T. and Takahashi, T. : On finite sequences with low autocorrelations, in Japanese. *Proc. 24th SITA*, Vol. 2, Kobe, Japan, (2001), 319-322.

[13] Nagasaka, K. and Shiue, J.-S.-P. : On a theorem of Koksma on discrepancy. *Proc. First International Symp. Algebraic Structure and Number Theory*, Ed. by S. P. Lam and K. P. Shum, World Scentific Publisher, Singapore · New Jersy · London · Hong Kong, (1988), 209-22[44] Nagasaka, K. and Takahashi, T. : Phisical random numbers and pseudo random numbers, in Japanese. *Bull. of the College of Engineering, Hosei Univ.*, Vol. 39, (2003), 27-34.

[15] Nagasaka, K. and Yamashita, H. : Phiaical random numbers and pseudo-random numbers, in Japanese. *Proc. Congres of* 2002 *Japan Statistical Society*, Meisei-Univ., Tokyo, (2002), 216-217.

[16] Niederreiter, H. : Quasi-Monte Carlo methods and pseuo-random numbers. *Bull. Amer. Math. Soc.* Vol. 84, (1978), 957-1041.

[17] Niederreiter, H. : *Random Number Generation and Quasi-Monte Carlo Methods.* CBMS-NSF Regional Conference in Applied Mathematics, SIAM, Philadelphia, Penn. , (1992).

[18] NIST : ⟨ http://esrc.nist.gov/publications/fips/fips1401.pdf/ ⟩.

[19] Sinclair, A. : *Algorithms for Random Generation & Counting, A Marker Chain Approach.* Progress in Theoretical Computer Science, Birkhäuser, Boston · Basel · Berlin, (1993).

[20] Takano, H. and Nagasaka, K. : Advanced digital watermarking system for high quality audio data. *Proc. 4-th ARS Conf. of the IASC*, Pusan, Korea, (2002), 257-260.

[21] Weyl, H. : Über die Gleichverteilung von Zahlen mod. Eins. *Math. Ann.*, Vol. 77, (1916), 313-352.

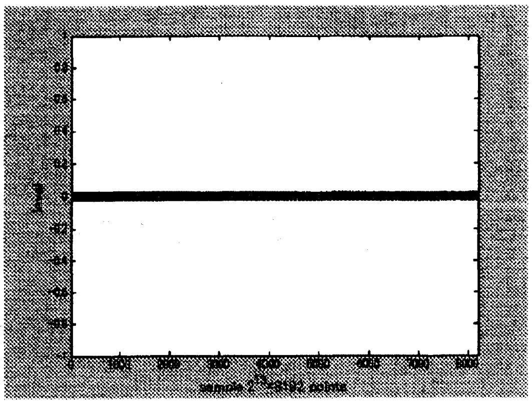

Figure 1: M-sequence (15-1-0-0-0) [piano]

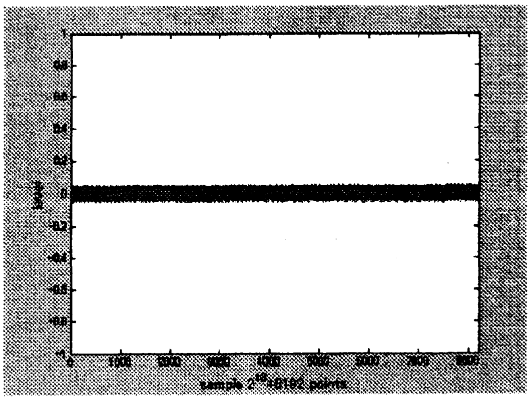

Figure 2: M-sequence (17-16-15-12-0) [piano]

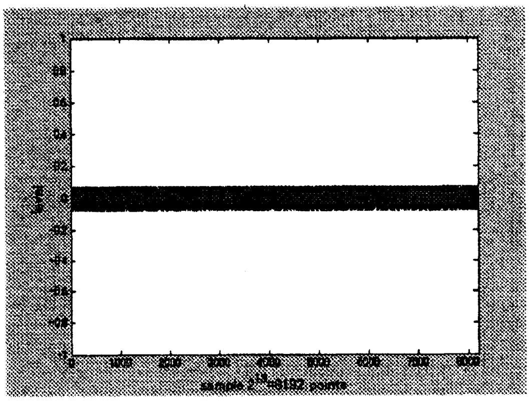

Figure 3: GA2 [piano]

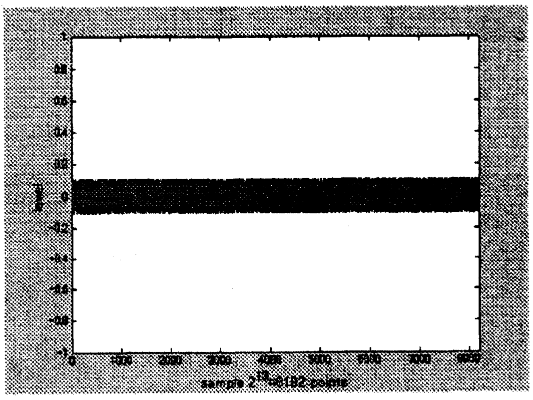

Figure 4: GA1 [piano]

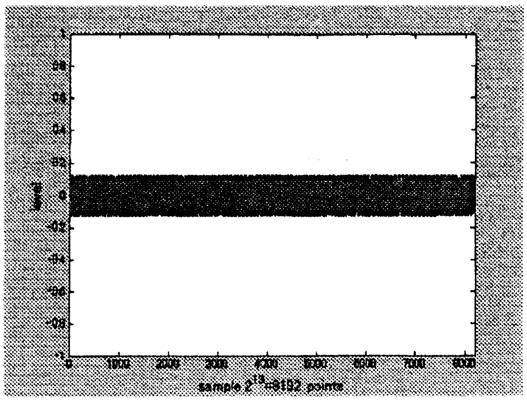

Figure 5: M-sequence (20-3-0-0-0) [song]

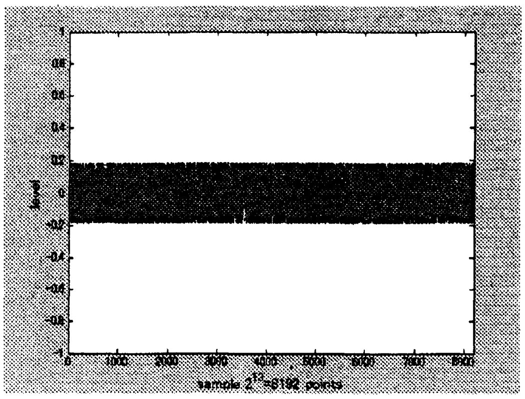

Figure 6: GA3 [song]

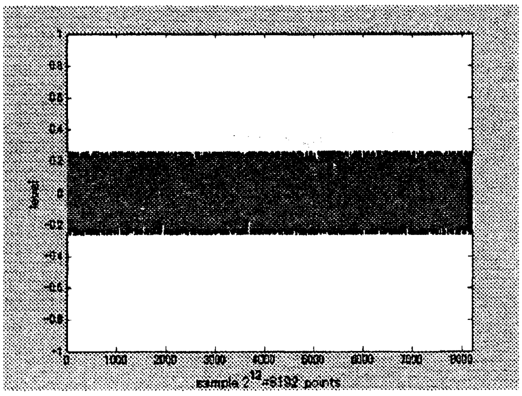

Figure 7: GA1 [song]

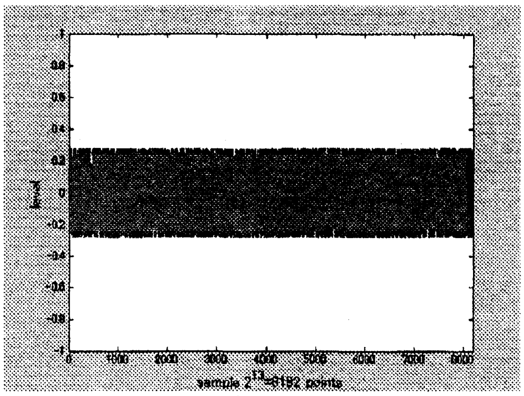

Figure 8: M-sequence (15-1-0-0-0) [song]

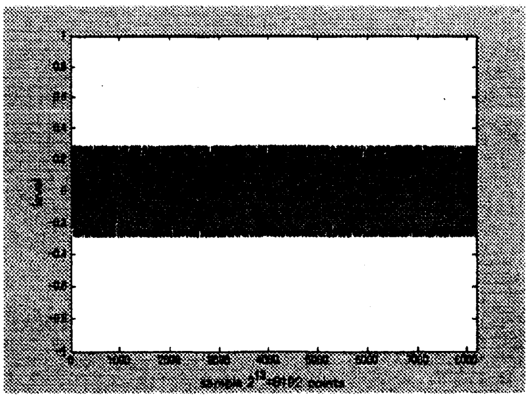

Figure 9: M-sequence (17-16-15-12-0) [song]