1984-01-01

Proposal for a Digital Pseudorandom Number Generator

C. Downey
Dublin Institute of Technology

Recommended Citation

Downey, C.: Proposal for a digital pseudorandom number generator. Electronics Letters, May 24 1984, Vol. 20,pp435 - 436. doi:10.1049/el:19840302

indicates that the increase of the harmonic distortion in the laser output itself has little influence on the distortion of the fibre output.

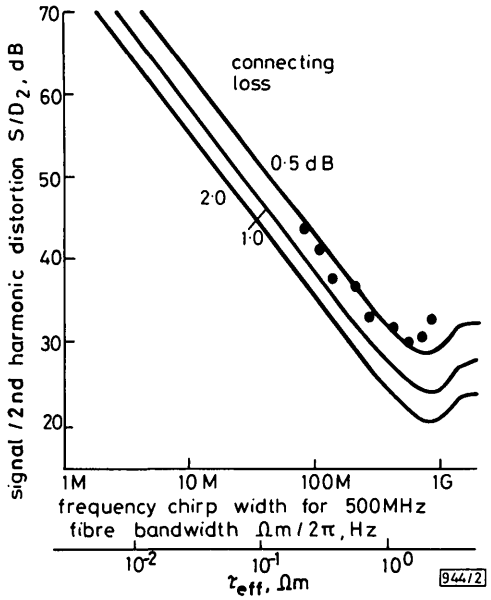

Fig. 2 *Second-harmonic distortion of fibre output against frequency chirp width*

V = 39
——— calculated
● experimental

These experimental results confirm the theoretical prediction that a slight emission frequency chirping associated with a laser intensity modulation causes serious harmonic distortions. In this experiment, $\Omega_m/2\pi$ of 200 MHz, which corresponds to a modulation degree of 0·1, results in S/D_2 of about 36 dB, in spite of low distortion in the laser output itself. It also indicates that the reduction of frequency chirping is effective in reducing harmonic distortions. If the $\Omega_m/2\pi$ is reduced by one decade, for example, the S/D_2 will improve by about 20 dB. Therefore, this parameter is the most effective in reducing the harmonic distortion compared with the other parameters such as connecting loss, fibre bandwidth, fibre V parameter and linewidth of the laser spectrum. The reduction of the frequency chirp width can be attained by using, for example, an external cavity laser structure.[12]

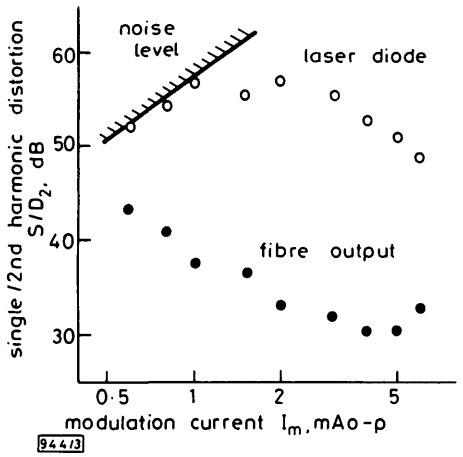

Fig. 3 *Second-harmonic distortion of laser diode output and fibre output*

Conclusion: It has been clarified experimentally that emission frequency chirping associated with laser intensity modulation causes serious harmonic distortion in multimode fibre optic analogue transmission. However, theoretical estimation indicates that the harmonic distortions can be greatly reduced by the reduction of the frequency chirping.

Acknowledgment: The authors are grateful to T. Uchida and F. Saito for their encouragement.

K. KAEDE
R. ISHIKAWA
K. MINEMURA
R. LANG
T. FURUSE
A. UEKI

Opto-electronics Research Laboratories
NEC Corporation
4-1-1 Miyazaki, Miyamae-ku, Kawasaki-City 213, Japan

11th April 1984

References

1 EPWORTH, R. E.: 'The phenomenon of modal noise in analogue and digital optical fiber systems'. Proc. 4th ECOC, 1978, pp. 492–501
2 PETERMANN, K., and ARNOLD, G.: 'Noise and distortion characteristics of semiconductor lasers in optical fiber communication systems', *IEEE J. Quantum Electron.*, 1982, **18**, pp. 543–555
3 OLESEN, H.: 'Dependence of modal noise on source coherence and fibre length', *Electron. Lett.*, 1980, **16**, pp. 217–218
4 GOODWIN, A. R., DAVIS, A. R., KIRKBY, P. A., EPWORTH, R. E., and PLUMB, R. G.: 'Narrow stripe semiconductor laser for improved performance of optical communication systems'. Proc. Opt. Commun. Conf., 1979, 4.3
5 ITO, K., FUJITA, S., and MIYAKE, Y.: 'Optical fiber transmission of ITV video signal by analog baseband modulation of laser diodes', *ibid.*, 16.9
6 SATO, K., and ASATANI, K.: 'Superimposed pulse modulation for fibre optic analogue video transmission using semiconductor laser diodes', *Electron. Lett.*, 1980, **16**, pp. 538–540
7 SATO, K., and ASATANI, K.: 'Linearity in fiber-optic analog transmission using laser diodes', *Trans. Inst. Electron. & Commun. Eng. Jpn. Sect. E*, 1980, **E64**, pp. 1086–1093
8 KOBAYASHI, S., YAMAMOTO, Y., ITO, M., and KIMURA, T.: 'Direct frequency modulation in AlGaAs semiconductor lasers', *IEEE J. Quantum Electron.*, 1982, **18**, pp. 582–595
9 UENO, M., KAWANO, H., FURUSE, T., SAKUMA, I.: '0·81 μm band AlGaAs/GaAs double-channel planar buried-heterostructure laser with large optical cavity', *Electron. Lett.*, 1983, **19**, pp. 370–371
10 TSUCHIDA, H., TAKO, T., and OHTSU, M.: 'Measurement of direct frequency modulation characteristics of semiconductor lasers by using a Michelson interferometer (in Japanese)'. Paper of technical group IECE Japan, TGOQE82-52, 1982, pp. 5–10
11 FURUSE, T.: 'Effect of transverse carrier diffusion on distortions in analog intensity modulation of semiconductor lasers'. National Conv. IECE Japan, 1980, p. 797 (in Japanese)
12 SAITO, S., NILSSON, O., and YAMAMOTO, Y.: 'Oscillation center frequency tuning, quantum FM noise, and direct frequency modulation characteristics in external grating loaded semiconductor lasers', *IEEE J. Quantum Electron.*, 1982, **18**, pp. 961–970

PROPOSAL FOR A DIGITAL PSEUDORANDOM NUMBER GENERATOR

Indexing term: Digital circuits

A digital hardware implementation of a linear congruential sequence generator using shift and add techniques of multiplication is described. The sequence is of long period, low serial correlation and is rectangularly distributed. The method has certain advantages over conventional feedback shift register techniques.

A linear congruential sequence generator which may be used as a source of pseudorandom noise has been economically implemented in digital hardware. A sequence of long period is generated in which the binary numbers have a rectangular distribution and low serial correlation. The sequence is readily converted to an anlogue pseudonoise source by means of an analogue-to-digital convertor. A serial binary output is also available. As pseudorandom number generators of this type have been widely used in software, especially in simulation techniques, their properties are well known.[1]

Although pseudorandom binary sequences generated in serial form by means of feedback shift registers have been used extensively in digital hardware,[2] unless special arrangements are made,[3,4] their outputs in parallel are a poor source of random numbers.[5] Further, when using FFT techniques, sequence lengths of $2^p - 1$ rather than 2^p lead to some problems. The method described here overcomes these difficulties.

Lehmer[6] proposed that sequences of pseudorandom integers could be generated recursively by

$$R_{n+1} = \lambda R_n + \mu \text{ (modulo } m) \quad (1)$$

where R_n and R_{n+1} are the present and next integers in the sequence, and the multiplier λ and the offset μ are integer constants. In a digital machine of word length p, it is convenient to choose m to be of the form

$$m = 2^p \quad (2)$$

The sequence is then of maximal length 2 provided that (i) λ (modulo 8) = 5 and (ii) m and μ are relatively prime.[7]

The correct choice of the multiplier λ is of crucial importance in achieving overall random number quality. Also, for simplicity in realising the algorithm in digital hardware, λ is chosen so that the multiplication may be implemented by shift and add techniques. The 'spectral test' of Coveyou and MacPherson[8] is a most demanding test for general goodness of random-number quality, and in particular for low serial correlation.

Multipliers of the form

$$\lambda = 2^{j+k} + 2^j + 2^k + 1$$
$$= (2^j + 1)(2^k + 1) \quad (3)$$

where $p > j > p/2$ and $k = 2$, achieve a sequence of maximal length 2^p for $\mu = 1$, and the 'spectral test' shows that for certain j the sequence of integers generated by the $p/2$ most significant bits can be regarded as being serially uncorrelated in pairs.

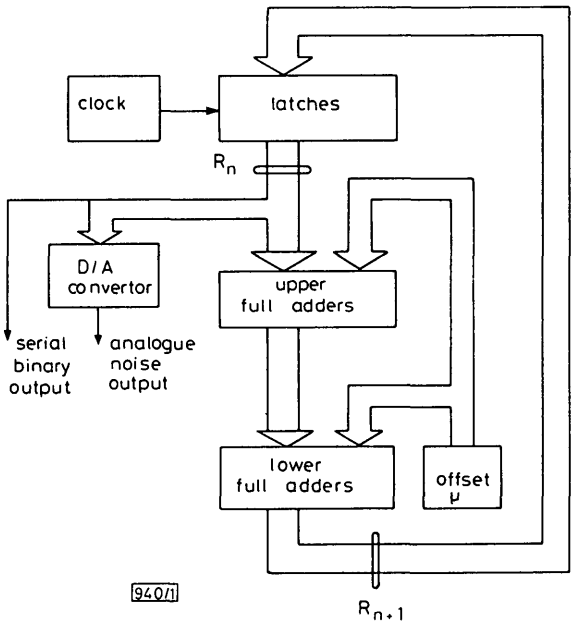

Fig. 1 *Linear congruential sequence generator with digital-to-analogue convertor*

A block diagram showing the implementation of the algorithm in digital hardware is shown in Fig. 1. The upper row of full adder scales by $(2^j + 1)$ and the lower row by a further $(2^k + 1)$, both modulo 2^p. Fig. 2 shows a typical 4 bit slice. A left shift of j bits is introduced in the upper full adder, and a further left shift of k bits (shown for $k = 2$) is introduced in the lower full adder. The $p/2$ most significant bits are applied to the digital-to-analogue convertor.

The first j bits of the upper full adders and the first k bits of the lower full adders are unused, so that the offset μ may be introduced at these inputs, as shown in Fig. 1. A range of

$$0 \leq \mu \leq (2^k + 1)(2^j - 1) + (2^k - 1) \quad (4)$$

is possible.

During one complete period the sequence generated contains all R_n, including zero, such that

$$0 \leq R_n \leq 2^p - 1$$

and as each number in this interval has one appearance in each cycle, the generator is self starting, and additional start-up logic is not required.

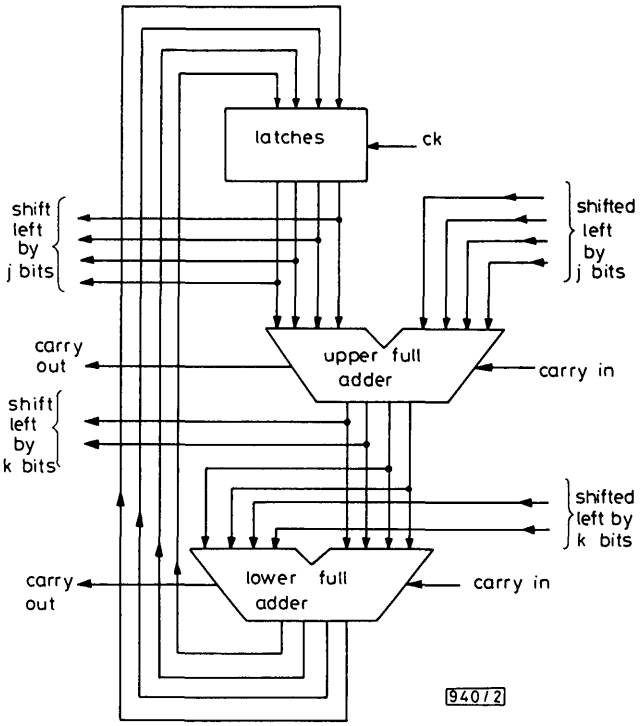

Fig. 2 *Typical 4 bit slice*

Since in a linear congruential sequence both the period of the sequence and the quality of randomness increases from the least significant to the most significant bit, the serial binary output is taken from the most significant bit.

A 16 bit prototype generator was constructed in low-power Schottky TTL. Choosing $j = 9$, $k = 2$ and $\mu = 1$ with $p = 16$ achieves a maximal-length sequence and a potency of 5. Application of the 'spectral test' has shown that the first 8 bits may be regarded as being serially uncorrelated in pairs. A sequence of period 2^{16}, rectangularly distributed on the interval [0, 225], is generated. The serial correlation[9] with a lag of 1 has been calculated to be $-8{\cdot}95 \times 10^{-6}$. Speed of operation of the circuit was limited by the digital-to-analogue convertor, the digital part of the circuit operating at up to 9·4 MHz.

C. P. DOWNING

Department of Telecommunications Engineering
Dublin Institute of Technology
Kevin Street, Dublin 8, Ireland

10th April 1984

References

1 TOCHER, K. D.: 'The art of simulation' (English Universities Press, London, 1963), Chap. 6
2 MACWILLIAMS, F. J., and SLOANE, N. J. A.: 'Pseudo-random sequences and arrays', *Proc. IEEE*, 1976, **64**, pp. 1715–1729
3 PANGRATZ, H., and WEINRICHTER, H.: 'Pseudo-random number generator based on binary and quinary maximal length sequences', *IEEE Trans.*, 1979, **C-28**, pp. 637–642
4 HARTLEY, M. G. (Ed.): 'Digital simulation methods' (Peter Peregrinus, Stevenage, 1975), Chap. 3
5 KNUTH, D. E.: 'The art of computer programming—Vol. 2' (Addison-Wesley, Reading, MA, 1971), p. 29
6 LEHMER, D. H.: 'Mathematical methods in large-scale computing units'. Proc. 2nd annual symposium on large-scale digital computing machinery (Harvard University Press, Cambridge, MA, 1951), pp. 141–145
7 KNUTH, D. E.: 'The art of computer programming—Vol. 2' (Addison-Wesley, Reading, MA, 1971), p. 15
8 COVEYOU, R. R., and MACPHERSON, R. D.: 'Fourier analysis of uniform random number generators', *J. Assoc. Comput. Mach.*, 1967, **14**, No. 1, pp. 100–119
9 KENDALL, M. G., and STUART, A.: 'The advanced theory of statistics—Vol. 3' (Charles Griffin, London, 1968), p. 361