ISSN 0735-2727, Radioelectronics and Communications Systems, 2016, Vol. 59, No. 11, pp. 510–517. © Allerton Press, Inc., 2016.
Original Russian Text © M.I. Mazurkov, A.V. Sokolov, N.A. Barabanov, 2016, published in Izvestiya Vysshikh Uchebnykh Zavedenii, Radioelektronika, 2016, Vol. 59, No. 11, pp. 47–55.

Synthesis Method for Bent Sequences in the Vilenkin-Chrestenson Basis

M. I. Mazurkov, A. V. Sokolov*, and N. A. Barabanov

Odessa National Polytechnic University, Odessa, Ukraine
**e-mail: radiosquid@gmail.com*

Received in final form July 28, 2016

Abstract—The paper presents a method developed for building a complete class of bent sequences of length $N = 9$ in the Vilenkin–Chrestenson basis based on employing three reference constructions. The first construction allows the bent sequences of arbitrary length $N = 3^{2k}$, $k \in \mathbb{N}$ to be built. The resultant bent sequences can be used both in cryptographic applications and as constant amplitude codes in the MC-CDMA technology. A design of the gamma xoring block of graphic and video information based on bent sequences in the Vilenkin–Chrestenson basis was also proposed.

DOI: 10.3103/S0735272716110054

In recent decades, the perfect algebraic constructions have found numerous applications in different applied uses of the theory of radio communications, data transmission, and cryptography [1]. Binary bent sequences representing truth tables of bent functions are among the most commonly used perfect algebraic constructions in the field of cryptography. It should be noted that the specified functions are the most nonlinear Boolean functions possessing uniform Walsh–Hadamard spectrum.

The efficient and high-speed generators of pseudorandom key sequences (PKSG) based on dual pairs of bent functions are available in literature [2, 3]. The specified generators can be used as a basis of stream encryption algorithms and gamma xoring units of encryption block algorithms; in addition, they can be applied for the generation of key information.

The development of principles of multi-valued logic, in particular, the development of methods for construction of multi-valued perfect algebraic constructions, is necessary for enhancing the efficiency of systems designed for the encryption and scrambling of graphic and video data.

Many state-of-the-art systems for graphic data processing are based on the principle of separation of data stream into color components in accordance with the employed color model. The RGB color models based on representing colors in the form of tuples of three numbers called color components are most often applied. Hence, in performing the gamma xoring operation, the above tuples are combined into one number that is summed up with gamma.

Thus, the required length of key sequence should be three times as large as the length of key sequence required for gamma xoring of the image having the same size but specified in shades of grey scale. This circumstance is undesirable in encrypting or scrambling of a large number of images in real time, e.g., for network transmission.

The use of such perfect algebraic constructions as multi-valued bent functions [4] makes it possible to build systems allowing all three color components to be processed simultaneously.

Bent functions also find application in the technology of code separation of MC-CDMA channels for building constant amplitude codes possessing the optimal value of peak factor $\kappa = 1$ [5]. The application of such codes makes it possible to significantly enhance the efficiency of using transmitter power and reduce the level of nonlinear distortions.

One of the promising directions in development of the MC-CDMA technology is associated with introduction of principles of multi-valued logic via the transition to using the Vilenkin–Chrestenson transform [6]. This approach involves the need of conducting further investigations directed on building new multi-valued codes with constant amplitude based on bent sequences in the Vilenkin–Chrestenson basis.

Quantum cryptography is another practically important application of multi-valued perfect algebraic constructions. The quantum cryptography problems require the construction of generators of multi-valued pseudorandom sequences possessing a high level of stochastic and cryptographic quality [7].

REFERENCES

1. M. I. Mazurkov, *Broadband Radio Communication Systems* (Nauka i Tekhnika, Odessa, 2010) [in Russian], ISBN 978-966-8335-95-2.
2. M. I. Mazurkov, N. A. Barabanov, A. V. Sokolov, "The key sequences generator based on bent functions dual couples," *Odes'kyi Politechnichnyi Universystet. Pratsi*, No. 3, 150 (2013), http://pratsi.opu.ua/articles/show/1017.
3. A. V. Sokolov, "Quick key sequences generator based on cellular automata," *Odes'kyi Politechnichnyi Universystet. Pratsi* **43**, No. 1, 180 (2014), http://pratsi.opu.ua/articles/show/1087.
4. A. S. Ambrosimov, "Properties of bent functions of q-valued logic over finite fields," *Diskr. Mat.* **6**, No. 3, 50 (1994), http://mi.mathnet.ru/eng/dm639.
5. Kenneth G. Paterson, "Sequences for OFDM and multi-code CDMA: two problems in algebraic coding theory," *Proc. of 2nd Int. Conf. on Sequences and Their Applications*, Seta 2001, May 13–17, 2001, Bergen, Norway (Springer, Berlin, 2002), pp. 46–71, DOI: 10.1007/978-1-4471-0673-9_4.
6. M. I. Mazurkov, A. V. Sokolov, N. A. Barabanov, "On the effect of the type of orthogonal transform on PAPR of signal spectrum in CDMA systems," *Informatics and Mathematical Methods in Simulation* **5**, No. 1, 28 (2015).
7. S. O. Hnatiuk, T. O. Zhmurko, V. M. Kinzeriavyi, N. A. Seilova, "Method for quality evaluation of trip pseudorandom sequence to cryptographic applications," *Information Technology and Security* **3**, No. 2, 108 (2015), http://its.iszzi.kpi.ua/article/view/60891.
8. A. M. Trakhtman, V. A. Trakhtman, *Foundations of the Theory of Discrete Signals over Finite Intervals* (Sov. Radio, Moscow, 1975) [in Russian].
9. A. V. Sokolov, O. N. Zhdanov, N. A. Barabanov, "On the existence of triple bent sequences," *Proc. of 19th Int. Youth Conf. on Radioelectronics and Youth in the XXI Century*, 2015, Kharkiv, Ukraine (KhNURE, Kharkiv, 2015), Vol. 3.
10. N. N. Tokareva, "Bent functions: results and applications. A survey," *Appl. Discrete Math.*, No. 1, 15 (2009), http://journals.tsu.ru/pdm/en/&journal_page=archive&id=431&article_id=26255.
11. B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (Wiley, 2015).