ISSN 0735-2727, Radioelectronics and Communications Systems, 2013, Vol. 56, No. 1, pp. 36–41. © Allerton Press, Inc., 2013.
Original Russian Text © M.I. Mazurkov, A.V. Sokolov, 2013, published in Izv. Vyssh. Uchebn. Zaved., Radioelektron., 2013, Vol. 56, No. 1, pp. 42–48.

# Constructive Method for Synthesis of Complete Classes of Multilevel de Bruijn Sequences

**M. I. Mazurkov and A. V. Sokolov**
*Odessa National Polytechnic University, Odessa, Ukraine*
Received in final form February 14, 2012

**Abstract**—Two new presentation forms of multilevel de Bruijn sequences (BS) have been introduced as geometric and algebraic structures. The attractive and practical properties of these structures have been found. This formed the basis for proposing a constructive method for the synthesis of generating and complete classes of BS. It has been shown that the application of the found classes of quaternary BS in encryption ensures a two-fold reduction of the memory space required for storing the cryptographic substitution boxes (S-boxes).

**DOI:** 10.3103/S0735272713010044

## INTRODUCTION

De Bruijn sequences (BS) [1–3] have found application in problems of radiolocation and communications, and also in problems of cryptography, in particular, as bit streams or key streams in sequence (stream) ciphers. The characteristic feature of BS is their maximum closeness to random sequences. In addition, BS have the normal distribution of series, they are balanced and possess a high degree of unpredictability.

The known estimate of the capacity $W_{\text{gen}}$ of generating classes of BS with arbitrary length $N = m^n$ using the alphabet of $m$ elements (numbers) for arbitrary natural $n$ [4] has the form:

$$W_{\text{gen}} = [(m-1)!]^{m^n-1} m^{m^{n-1}-n}. \quad (1)$$

However estimate (1) indicates only the existence of a generating class of BS, and it does not give a constructive method for their construction similar to the well-known Shannon theorems related to the existence of good correcting codes. Thus, the issues of constructive building of generating and complete classes of multilevel BS have not been properly solved and require further investigation.

The present paper proposes a new approach to solving the synthesis problem of complete classes of multilevel BS. The essence of this approach implies that each BS is described by using two forms: geometric structure and algebraic structure. With due regard for the properties of these structures a constructive method for synthesis of the complete classes of multilevel BS has been created that is the main purpose of this study. The issues of application of the BS classes built for construction of economic schemes of S-boxes and cryptographic substitution tables of sequence ciphers have been considered.

## MAIN BODY

By definition each $m$th BS of length $N = m^n$, where $m$ is the alphabet size of BS, $n$ is the capacity of state (number of memory cells of conventional generator) should map on a closed loop exactly $N$ different states. For example, if the alphabet size $m = 4$ (elements $\{0, 1, 2, 3\}$, while $n = 2$, all $N = 4^2 = 16$ states of BS shall be placed in $m = 4$ storages and can be presented in the form of the following algebraic construction: