Full-length non-linear binary sequences with Zero Correlation Zone for multiuser communications

Mahdiyar Sarayloo[1], Ennio Gambi[1] and Susanna Spinsante[1]

[1]Dipartimento di Ingegneria dell'Informazione, Universita' Politecnica delle Marche, Italy
S1060514@pm.univpm.it, e.gambi@univpm.it, s.spinsante@univpm.it

***Abstract*:** The research on new sets of sequences that can be applied as spreading codes in multiple user communications is still an active area, even if this topic has been extensively investigated since long time. In fact, new communication paradigms like dense and decentralized wireless networks, where there is no central controller to assign the resources to the nodes, are revamping the interest on finding large sets of sequences providing adequate correlation properties to support a big number of nodes, in potentially hostile channels. This paper focuses on the Zero Correlation Zone (ZCZ) property exhibited by a family of non-linear binary sequences featuring a great cardinality of their set, and good security-related features, and provides evidence of their suitability to multiuser communications, in channels affected by multipath.

***Keywords*:** Zero Correlation Zone, non-linear binary sequences, CDMA, Gold codes, bound**.**

1. Introduction

Despite the idea of Spread Spectrum (SS) communications dates back more than one century, this technology is still applied in a wide set of different fields, ranging from satellite positioning, to multiuser mobile communications, to wireless local and personal area networks. SS communications have been recently revisited, in the framework of decentralized wireless networks [1] comprising several separate transmitter-receiver pairs, where users treat each other as noise, and there is no central controller, as it happens in traditional uplink/downlink multiuser systems, to assign the resources to them. New Medium Access Control (MAC) protocols are also being investigated [2], to support emerging communication technologies and paradigms, such as the Internet of Things (IoT).

The different SS techniques available, such as Direct Sequence (DS), Frequency Hopping (FH), Time Hopping (TH), and Hybrid (H) [3]–[5] feature different properties, limitations, and advantages, that are strongly related to the inherent nature of the sequences selected and used as spreading codes [6]. Modern communication systems also require the capability to support increasing number of users, which relies on the selection of sets of spreading codes featuring large cardinality, i.e. a large amount of sequences belonging to the same family [7].

To reduce the Multiple Access Interference (MAI) and co-channel interference in SS systems and multiuser applications, such as radars, position detection, and ultrasonic imaging, Zero Correlation Zone (ZCZ) sequences may be applied, i.e. sequences whereby the out-of-phase auto-correlation function is equal to zero, in a specified zone of phase shift [8]. In SS communications, the ZCZ property can make spreading codes more robust to the effects of multipath propagation. In fact, a delay spread τ_{max} within the ZCZ interval may be tolerated, assuming that each i^{th} user's signal, affected by a relative path delay τ_i, satisfies the condition:

$$|\tau_i| \le \tau_{\max} = Z_0 \cdot T_C \tag{1}$$

where T_C is the chip period, and Z_0 is the ZCZ width. When the ZCZ property holds, generalized orthogonal (GO) sequences may be defined, alternative to normal orthogonal (NO) ones. In fact, a set of M sequences of length N is said to be normal orthogonal if the periodic correlation function among two sequences a_i and a_j, $C_{a_i a_j}{}^P[k]$, for $0 \le k \le N-1$, $i, j \in \{1,\ldots,M\}$ satisfies the conditions:

$$C_{a_i a_j}{}^P[k] = \begin{cases} N, & for \quad k = 0, i = j \\ 0, & for \quad k = 0, i \ne j \end{cases} \tag{2}$$

The sequence set is said to be generalized orthogonal, if the periodic correlation function $C_{a_i a_j}{}^P[k]$, for $0 \le k \le N-1$, $i, j \in \{1,\ldots,M\}$ satisfies the condition:

$$C_{a_i a_j}{}^P[k] = \begin{cases} N, & for \quad k = 0, i = j \\ 0, & for \quad k = 0, i \ne j \\ 0, & for \quad 0 < |k| \le Z_0 \end{cases} \tag{3}$$

being Z_0 the width of the ZCZ. The definition of GO sequences implies that the greater the ZCZ width Z_0, the better the sequence set, i.e. the system will be robust against a greater delay spread. For a shift k value outside the range $(-Z_0, Z_0)$, $C_{a_i a_j}{}^P[k]$ can take any value: the periodic cross-correlation cannot be controlled outside the ZCZ.

It would be desirable to get both a wide ZCZ and non-linearity, within the same set of sequences used as spreading codes assigned to multiple users, in order to get more robust and secure communications.

Based on the above premises, this paper analyses the performance obtainable in a Direct Sequence Code Division Multiple Access (DS-CDMA) system, on a multipath channel, where non-linear binary sequences exhibiting the ZCZ property are chosen as spreading codes. The family of non-linear binary sequences selected for evaluation is the set of De Bruijn (DB) sequences [9]. With respect to the work presented in [10], the sequences assigned to users are selected according to their ZCZ properties. As a matter of fact, the great cardinality of the set, given by $M = 2^{2^{(n-1)}-n}$, where n is the span of the sequences, allows to apply suitable

strategies to select the spreading codes providing the best performance in terms of minimal error probability at the receiver. The results herein presented also integrate the preliminary analysis developed in [11], where an Additive White Gaussian Noise (AWGN) channel was assumed. The paper is organized as follows: Section 2 discusses related work, whereas Section 3 presents the main properties of the binary DB sequences investigated by the paper. The sequence selection strategy is detailed in Section 4. The results obtained from simulations are presented in Section 5, whereas Section 6 draws the main conclusion of the paper and highlights future research directions.

2. Related Work

All SS systems make use of code generators, usually designed as pseudorandom, or pseudonoise (PN) generators. Each code in a given family is used to set the frequency spectrum that the output signal will occupy. It also determines and controls the spreading pattern of the system: by using a carefully designed and selected set of spreading sequences, which benefits from good correlation properties, it is possible to implement multiple access technologies, and multi user transmission at the same time, in the same frequency band.

Several families of spreading codes have been proposed in the literature, either binary (two-valued), and polyphase ones (i.e. multi-valued). Codes may be even specifically designed to satisfy one or more requirements related to SS communications. Unfortunately, some requirements may be conflicting. As an example, sets of spreading codes that are optimal to reduce the MAI term, often result in a few spreading codes that may not suffice to support as many users as requested. Comparing different sets of spreading codes may be not a straightforward process, due to the amount of different codes-related parameters that shall be taken into account, and to the inherent differences in the code generation process.

Asynchronous systems, or frequency selective propagation channels, may destroy or severely impact the orthogonality of the NO spreading codes used, thus causing an increasing interference, being both Inter Symbol Interference (ISI) and MAI generated by random time offsets among the signals, that make unfeasible the code waveforms to be completely orthogonal. Well-known families of linear spreading sequences, such as *m*-sequences, Kasami, Gold, and Walsh codes, traditionally employed as channelization codes, exhibit non-zero and sometime non negligible auto- and cross-correlation out-of-phase values, which limit the achievable performance, in asynchronous or in quasi-synchronous scenarios [11].

On the other hand, full length sequences obtained through non-linear generation, such as binary De Bruijn (DB) sequences [12], [13], provide attractive features as well, such as long periods and large complexities, great cardinality of the set [14], and good randomness properties, that can be fruitfully exploited in communication systems, coding theory, and cryptography [15].

3. Non-linear Binary De Bruijn Sequences

Non-linear feedback shift registers (NLFSRs) are a generalization of linear feedback shift registers, in which a current state is a non-linear function of the previous state. While the structure of an *n*-bit LFSR can be easily deduced from *2n* consecutive bit of its sequences, by applying the Berlekamp-Massey algorithm, up to *O(2n)* bits would be needed to determine the structure of a *n*-bit NLFSR generating a given sequence [12], thus denoting a stronger resistance to attacks aimed at breaking the sequence generation algorithm. Non-linearity brings better security to spreading codes, as they become more difficult to guess by unauthorized users.

It is known that an *n*-stage LFSR has a maximum period of 2^n-1, if and only if its characteristic polynomial is primitive. Sequences generated by full-period NLFSRs have a length equal to 2^n, and they are also known as De Bruijn sequences. In a DB sequence of order (or span) *n*, all the possible 2^n different binary *n*-tuples appear exactly once.

The periodic auto-correlation function ${C_{aa}}^P[k]$ of any DB sequence *a* of span *n*, for a given shift *k*, exhibits the following properties:

$$ {C_{aa}}^P[k] = \begin{cases} 2^n, & for \quad k = 0 \\ 0, & for \quad 1 \le |k| \le n-1 \\ \neq 0, & for \quad |k| = n \end{cases} \tag{4} $$

which means that *any* binary De Bruijn sequence of span *n* exhibits a ZCZ of length *(n-1)* chips in its periodic auto-correlation function. For an arbitrary pair of De Bruijn sequences a_i and a_j, $i \neq j$, of span *n* and period *N*, the following bound on the periodic cross-correlation function ${C_{a_i a_j}}^P[k]$ holds:

$$ -2^n \le {C_{a_i a_j}}^P[k] \le 2^n - 4 \ for \ 0 \le k \le N-1 \tag{5} $$

By adopting suitable strategies, and exploiting the great cardinality of the set, it is possible to select specific subsets of DB sequences featuring the desired periodic auto- and cross-correlation properties. About the aperiodic auto-correlation (AAC) of the sequences, Table 1 compares the maximum and average AAC values of different families, namely DB sequences of length 32 bits, Gold, and *m*-sequences of length 31 bits, computed over the whole sets.

Table 1. Comparison of maximum and average AAC values of different spreading codes families

	DB (32)	**Gold (31)**	**M (31)**
Maximum	0.625	0.4194	0.1935
Average	0.0193	0.1109	0.0774

Despite the apparently worse behavior of DB sequences in terms of maximum AAC value, their greater cardinality allows for the minimum average AAC value, with respect to the other sets considered. The mentioned maximum value of AAC is not frequently occurred for the DB sequences; further, DB sequences having the maximum AAC may be removed from the selected subset, to improve the performance attainable.

Another interesting parameter is the number of zero AAC values at each shift index, that can impact the performance of the codes in synchronous systems, and control the selection of the proper codes to use. Figure 1 illustrates the percent number of sequences with null AAC values at each rotation for DB, Gold and *m*-sequences. Considering the number of distinct sequences of each sequence family, it appears that DB sequences may be chosen as the best set.

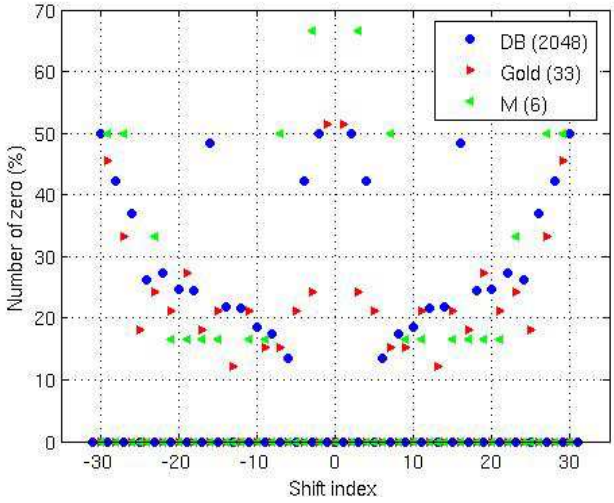

Figure 1. Percent amount of null AAC values for each shift index, for the different sets of spreading codes considered (DB, Gold and *m*-sequences)

Considering the number of sequences featuring the same amount of null AAC values, Figure 2 shows how DB sequences incredibly outperform the other sets.

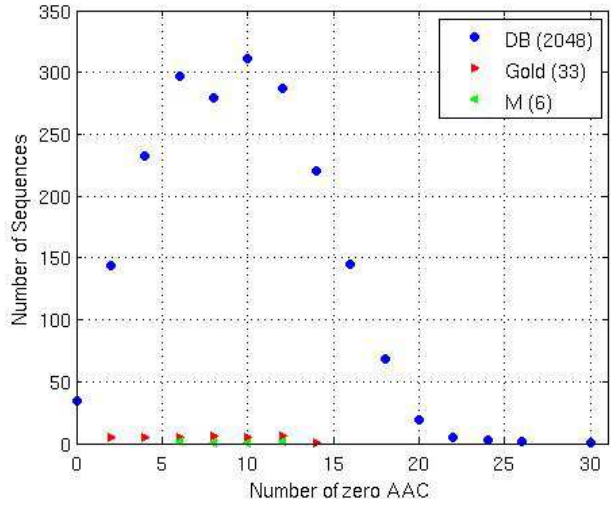

Figure 2. Amount of sequences with the same number of zero AAC values (DB, Gold and *m*-sequences)

4. Sequences Selection Strategy

The evaluation of full-length non-linear binary sequences with ZCZ property, to be used as spreading codes in a DS-CDMA system, requires to design a proper sequence selection strategy, in order to optimize the expected performance. Due to the great cardinality featured by families of DB sequences, the analysis herein presented considers only the full set of span 5 sequences, i.e. a total amount of 2048 sequences of length 32. This way, it is possible to apply an optimal selection strategy to select so called *clusters* of sequences to be used as spreading codes. On the contrary, for bigger values of the span, the exhaustive generation of the sequences becomes extremely resource-consuming, and only partial subsets could be considered, thus getting a sub-optimal selection only.

The algorithm designed to extract the span 5 sequences from their full set looks for clusters of at least 5 sequences, which have to show a ZCZ in their cross-correlation, or a maximum out-of-phase value of the cross-correlation equal to 4 or 8. The full set of 2048 De Bruijn sequences provides up to 227103 periodic cross-correlation functions that exhibit a ZCZ of variable length. According to the constraints set above, up to 30515 clusters of at least 5 sequences may be found from the original family of 2048 binary DB sequences; among them, 708 clusters include up to 6 different sequences.

5. Simulation Results

In order to gather significant results that can be assumed as representative of a general behavior, due to the big amount of different clusters possible, the simulations have been performed by randomly selecting the clusters of DB sequences to test, and comparing them against the best clusters of *m*-sequences and Gold codes possible. In fact, for a span $n = 5$, only 6 *m*-sequences exist, and only 33 Gold codes, so it is easy to find the clusters of 5 sequences that provide the best performance for these families, according to the selection rules stated above.

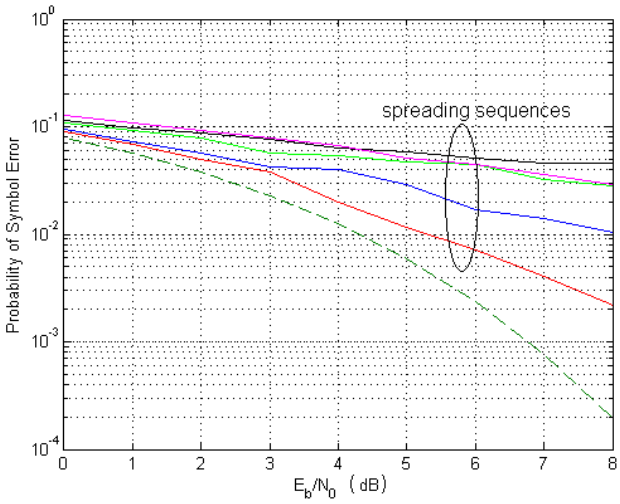

Figure 3. Probability of Symbol Error provided by a randomly selected cluster of 5 De Bruijn sequences of length 32, compared to ideal curve (dashed line)

Figure shows the performance of a DS-CDMA system employing a randomly chosen cluster of 5 DBs sequences as spreading codes (i.e. 5 users), assuming a propagation channel affected by multipath, with a multipath delay profile given by $[0,3,4]\cdot T_C$, and a Ricean factor $K = 0.2$. The Ricean factor may take different values: $K = 100$ for a channel with no multipath; $K \geq 1$ for a channel affected by Rice fading; and $K < 1$ for a channel affected by Rayleigh fading. Each curve corresponds to a different user; the dashed line gives the ideal behavior. Comparison among different sets of sequences is given in Table 2, that provides the minimum and maximum difference of the Probability of Symbol Error denoted as Δ_{PSE}, between the spreading codes in the cluster

and the ideal curve, at $E_b/N_0 = 4$ dB, for DB, *m*-sequences and Gold codes, in the same channel conditions stated above. DB sequences provide the less scattered behavior with respect to the ideal one, better than the optimal clusters of Gold and *m*-sequences.

Table 2. Spreading codes performance, with respect to the ideal behavior, in terms of minimum and maximum difference of the Probability of Symbol Error (Δ_{PSE}) for $E_b/N_0 = 4$ dB

Cluster	Code Length	min Δ_{PSE}	max Δ_{PSE}
De Bruijn	32	$2 \cdot 10^{-2}$	$6.9 \cdot 10^{-2}$
M-sequence	31	$4.5 \cdot 10^{-2}$	$1.4 \cdot 10^{-1}$
Gold	31	$3.5 \cdot 10^{-2}$	$1.1 \cdot 10^{-1}$

Randomly chosen clusters of DB sequences remain better than *m*-sequences and Gold codes, compared to the ideal curve, even when 6 users are considered. Table 3 refers to a multipath delay profile of $[0,3,6] \cdot T_C$, and a Ricean factor $K = 0.7$. Again, DB sequences outperform other clusters, even in a propagation channel affected by a stronger multipath.

Table 3. Spreading codes performance, with respect to the ideal behavior, in terms of minimum and maximum difference of the Probability of Symbol Error (Δ_{PSE}) for $E_b/N_0 = 4$ dB

Cluster	Code Length	min Δ_{PSE}	max Δ_{PSE}
De Bruijn	32	$2.5 \cdot 10^{-2}$	$1.1 \cdot 10^{-1}$
M-sequence	31	$8 \cdot 10^{-2}$	$1.7 \cdot 10^{-1}$
Gold	31	$4 \cdot 10^{-2}$	$1.2 \cdot 10^{-1}$

As a final remark, the performance improvements of raw bit error probability (BEP) attainable with DB sequences can be converted into dramatic performance improvements after de-interleaving and decoding [16]. Reed-Solomon (RS) coding has been selected for simulation, and the evaluation of RS-coded BEP (i.e.: BEP after RS decoding) has been obtained by using the well-known analytic approximation that maps the raw BEP into the RS-coded BEP. Figure 4 compares the lower and upper bounds on RS-coded BEP for DB sequences and Gold codes, assuming 4 users in the DS-CDMA system, and RS(31,23) coding. The better performance of DB sequences are clearly visible.

6. Conclusions and Future Work

The great cardinality of the De Bruijn sequences, exhibited even for small values of the span, allows to find a big amount of subsets providing the ZCZ property among the sequences, joint security-related features. This paper presented simulation results related to randomly chosen subsets of span 5 De Bruijn sequences, composed by 5 and 6 sequences, to be used as spreading codes in multiuser communications over multipath channels. The De Bruijn sequences belonging to these subsets provide better performance than *m*-sequences or Gold codes, typically adopted for their good auto-correlation properties. In channels affected by multipath, the ZCZ property ensures to keep the probability of symbol error limited to values not far from the ideally expected ones. The adoption of channel coding further emphasizes the improvements attainable. Future research on this topic will be focused on investigating the behavior of longer De Bruijn sequences, i.e. sequences featuring a span $n > 5$, on channels affected by possibly severe multipath, as in vehicular communications.

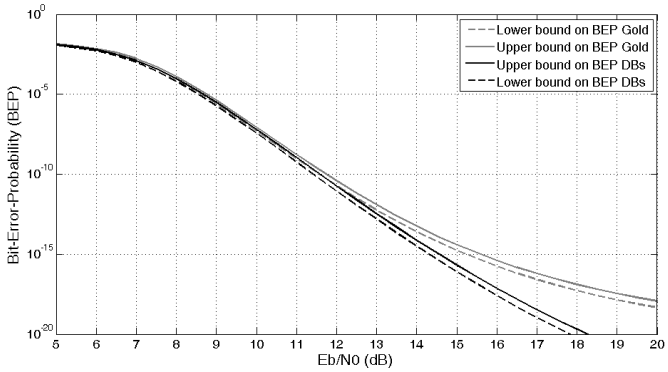

Figure 4. Improved RS-coded BEP provided by DB sequences with respect to Gold codes, in a 4 users DS-CDMA system with RS(31,23) coding

7. Acknowledgement

The authors acknowledge the support provided by Luca Di Cesare in designing part of the simulations needed to find the sequence subsets.

References

[1] K. Moshksar, A. K. Khandani, "Decentralized Wireless Networks: Spread Spectrum Communications Revisited," IEEE Transactions on Information Theory, Vol. 60, No. 5, pp. 2576-2593, 2014.

[2] M. Guerroumi, A.-S. Khan Pathan, N. Badache, S. Moussaoui, "On the Medium Access Control Protocols Suitable for Wireless Sensor Networks - A Survey," International Journal of Communication Networks and Information Security, Vol. 6, No. 2, pp. 89-103, 2014.

[3] M. B. Pursley, "Direct-sequence spread-spectrum communications for multipath channels," IEEE Transactions on Microwave Theory and Technology, Vol. 50, No. 3, pp. 653–661, 2002.

[4] R. Muammar, "Frequency-hopped multilevel frequency shift keying spread spectrum for mobile radio communication systems," IEEE Transactions on Information Theory, Vol. 28, No. 6, p. 979, 1982.

[5] A. R. Forouzan, M. Nasiri-kenari, and J. A. Salehi, "Performance analysis of time-hopping spread-spectrum multiple-access systems: uncoded and coded schemes," IEEE Transactions on Wireless Communications, Vol. 1, No. 4, pp. 671–681, 2002.

[6] F. D. Garber and M. B. Pursley, "Optimal phases of maximal length sequences for asynchronous spread-spectrum multiplexing," Electronics Letters, Vol. 16, No. 19, pp. 756–757, 1980.

[7] W. A. Imtiaz, N. Ahmad, "Cardinality Enhancement of SAC-OCDMA Systems Using new Diagonal Double Weight Code," International Journal of Communication Networks and Information Security, Vol. 6, No. 3, pp. 226-232, 2014.

[8] T. Hayashi, "A Class of Zero-Correlation Zone Sequence Set Using a Perfect Sequence," IEEE Signal Processing Letters IEEE, Vol. 16, No. 4, pp. 331–334, 2009.

[9] N. De Bruijn, "A combinatorial problem," Proceedings Koninklijke Nederlands Akademie van Wetenschappen, 1946.

[10] S. Spinsante, S. Andrenacci, and E. Gambi, "Binary De Bruijn sequences for DS-CDMA systems: analysis and results," EURASIP Journal of Wireless Communications and Networking, Vol. 4, 2011.

[11] M. Sarayloo, E. Gambi, S. Spinsante, "De Bruijn Sequences as Zero Correlation Zone Codes for Satellite Navigation

Systems," 21st International Conference on Telecommunications, Lisbon (PT), 2014.
[12] P. Fan, "Spreading Sequence Design and Theoretical Limits for Quasisynchronous CDMA Systems," EURASIP Journal of Wireless Communications and Networking, Vol. 2004, No. 1, p. 724989, 2004.
[13] T. Etzion and A. Lempel, "Algorithms for the generation of full-length shift- register sequences," IEEE Transactions on Information Theory, Vol. 30, No. 3, pp. 480–484, 1984.
[14] M. Sarayloo, E. Gambi, and S. Spinsante, "A Large Set of Orthogonal Codes for the V2V Scenario," International Conference on Connected Vehicles and Expo, Vienna (AT), pp. 653-653, 2014.
[15] S. Spinsante, C. Warty, E. Gambi, "DS-SS with de Bruijn sequences for secure Inter Satellite Links," IEEE Aerospace Conference, Big Sky (MT, USA) , pp.1-8, 2013
[16] S. Spinsante, M. Sarayloo, E. Gambi, C. Warty, C. Sacchi, "De Bruijn Sequences for DS/CDMA Transmission: Efficient Generation, Statistical Analysis and Performance Evaluation," IEEE Aerospace Conference, Big Sky (MT, USA), 2015.