# A Large Set of Secure Signatures for DS-SS Long Range Radars in Autonomous Cars

MAHDIYAR SARAYLOO, ENNIO GAMBI, SUSANNA SPINSANTE
Universita' Politecnica delle Marche
Dipartimento di Ingegneria dell'Informazione
Via Brecce Bianche 12, 60131 Ancona
ITALY
m.sarayloo, e.gambi, s.spinsante@univpm.it

*Abstract:* The current trend in the use of ICT to boost the development of the automotive sector is mainly addressed towards so called autonomous vehicles, equipped with appropriate sensors, actuators and processors, that make them able to move safely, without the intervention of a human driver. Actually, since several years, ICT permitted a widespread implementation of systems to help the driver maintaining the control of the vehicle, even when exceeding its normal limits of handling. Among them, vehicle radars may work under all weather conditions, provide a satisfactory coverage, and see several meters ahead. This paper investigates the performance, in terms of detection capability and false detection rate, of Direct Sequence Spread Spectrum Long Range Radars adopting binary De Bruijn sequences as radar signatures, compared to more classical solutions adopting Gold codes. Following the analysis of the correlation and security properties of De Bruijn sequences, the radar detection performance are discussed in two typical scenarios, and by means of specific tools, such as the ambiguity function to account for Doppler effects. Even if De Bruijn sequences do not provide disruptive improvements with respect to Gold codes, they exhibit better behavior in the presence of Doppler, and a much greater cardinality of their set, at a parity of the length, which may be useful to accommodate many potential users in a vehicular scenario.

*Key–Words:* Vehicle radar, Direct Sequence Spread Spectrum, signature, De Bruijn sequence, correlation

## 1 Introduction

Modern societies depend on mobility, which provides personal freedom and access to services for business and leisure. However, rising volumes of freight traffic contribute to deteriorate the problems related to road transport, which include congestion of urban areas and main roads, harmful effects on the environment and public health, and above all, accidents which cause fatalities, injuries, and material damage [1, 2]. Information and Communications Technologies (ICT) are widely in use in all areas of mobility, most notably in vehicles, which are becoming more and more intelligent, safe, and efficient. Already in 2002, the eSafety Working Group Final Report [3] concluded that the greatest potential of ICT in solving road transport safety problems was offered by intelligent vehicle safety systems, providing new, intelligent solutions addressing together the involvement of, and interaction between, the driver, the vehicle, and the road environment.

The development of appropriate sensors, actuators and processors, has already permitted a widespread implementation of systems to help the driver maintaining the control of the vehicle even when exceeding its normal limits of handling. Examples of systems that already made a major contribution to road safety, are Anti-lock Braking Systems (ABS), and Electronic Stability Programme (ESP). However, collisions during lane changes and involuntary lane departure still remain two of the most important causes of accidents. This problem requires suitable in-vehicle technology to help detecting and warning drivers of vehicles in adjacent lanes, or when the vehicle is about to unintentionally depart from the lane. Automotive radars [4] permit an automatic vision of the environment where the vehicle is moving, to draw the information required for performing the safest actions for the vehicle and the passengers on board. As shown in Fig. 1, several kinds of sensors may be installed on a vehicle; usually, vision based sensors, such as cameras, can usefully complement the radar. But, on the other hand, the radar alone may work under all weather conditions, provide a satisfactory coverage, and see several meters ahead.

Short Range Radars (SRRs) [6], and Long Range Radars (LRRs) [7–9] have been considered for automotive applications up to now. Restricting ourselves to LRRs, operating in the $[76, 77]$ GHz band for a

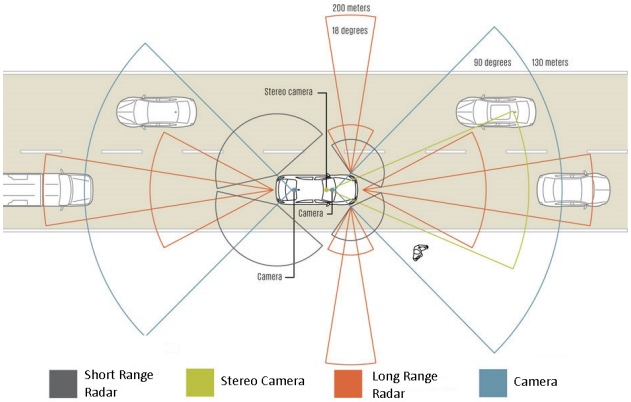


Figure 1: Different kinds of sensors aimed at implementing an autonomous car (illustration by John MacNeill from [5]), such as SRR, LRR, and cameras.

visibility range of up to 150 m, classic implementations employ signal processing techniques based on Frequency Modulation-Continuous Wave (FM-CW) transmission, for a maximum bandwidth of 1 GHz. FM-CW systems are very simple to implement but their performance can be strongly degraded by interfering signals from neighboring radars of the same type. A possible solution to this problem is presented in [10], where a Frequency-Hopping (FH) random chirp FM-CW technique changes the chirp sweep frequency and time at every cycle, to result in interference signals less likely to be correlated to the desired signal, and in noise-like frequency response for the mutual interference after the received signal is demodulated. Despite these advantages, however, the frequency stability of the Volt Controlled Oscillator (VCO), required to implement the frequency synthesizer, limits the processing gain factor, thus reducing the ability to discriminate different targets in heavy traffic conditions [11].

An alternative approach relies on the use of Spread Spectrum (SS) signals in Direct Sequence (DS) configuration [12, 13], based on the adoption of Pseudo Noise (PN) sequences, as in classical Code Division Multiple Access (CDMA) communications. The specific PN sequence acts as the radar "signature", which allows to compute the distance of a vehicle by selecting its echo among a very large number of interfering signals, including the other vehicle's echoes, and different radar emissions. The use of SS signals brings resistance to multipath fading, and intentional or unintentional jamming [14]. The knowledge of the sequence used as spreading code is required to recover the correct target echo, by maximizing the correlation between the transmitted signal and the received target echo. From the performance viewpoint, an automotive radar should exhibit a high detection capability but also a low false detection rate. These metrics are influenced by the auto- and the cross-correlation properties, respectively, exhibited by the sequences selected as radar signatures.

Following a similar analysis developed in [15], where the performance of DS-SS LRRs adopting chaotic signatures were compared to more classical PN signatures (Gold codes), in this paper we investigate the performance, in terms of detection capability and false detection rate, of DS-SS LRRs adopting binary De Bruijn sequences (DBSs) as radar signatures. Binary DBSs (BDBSs) are generated by Non Linear Feedback Shift Registers (NLFSRs) and exhibit, at a parity of the span $n$, i.e. the number of memory cells within the generating register, a much greater cardinality than any other set of binary sequences generated by LFSRs. This feature can be of interest in the automotive scenario, where the number of vehicles present at the same time in a road may be quite high, in heavy traffic conditions, and dynamically change. As a matter of fact, if linear binary sequences are used as radar signatures, it is necessary to increase a lot the length of the sequences in order to get enough signatures, i.e. to have a bigger set. In its turn, an increased sequence length implies greater complexity at the receiver, and possible delays in the echo detection step. Further, the bandwidth constraint does not allow to arbitrarily extend the sequence length, to get a set of bigger cardinality. In this paper, the same algorithm proposed in [15] is used to discern multiple echoes, and a comparison to a solution based on Gold codes is developed by considering typical, though simplified, road environments.

The paper is organized as follows: Section 2 presents the reference model for the DS-SS LRR system considered within the paper. Section 3 provides basic information on binary De Bruijn sequences, and related properties relevant to the vehicular application for which they are adopted as radar signatures. Section 4 describes the simulated road scenarios and the results on detection capability and false detection rate. Finally, Section 5 concludes the paper.

## 2 System model

As shown in the general model of Fig. 2, a DS-SS radar uses a PN sequence, composed by $L$ chips, to modulate the pilot signal. Each radar equipment uses a different sequence, chosen from the same set. The distance between the target and the radar is computed from the traveling time of the wave reflected from the target, namely $T_d$. To obtain $T_d$, the correlation between the received (and delayed) spreading code and the reference spreading code, locally generated at the

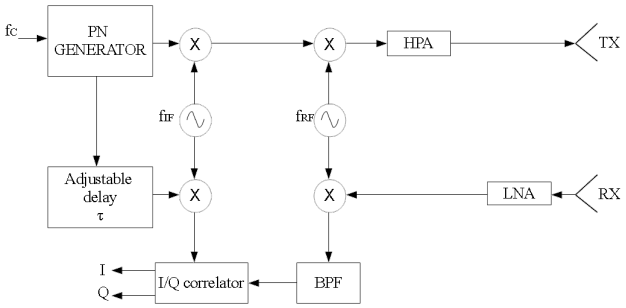


Figure 2: General model of a DS-SS radar.

host vehicle, is computed. The auto-correlation function of the spreading code will, in effect, show a peak at the time shift corresponding to $2 \cdot T_d$, from which the distance of the target can be computed as $d = c \cdot T_d$, being $c$ the speed of light. The ability of a DS-SS radar to correctly detect the distance of a target depends on the auto-correlation properties of the sequence adopted as signature. At the same time, rejection of different radars' signals depends on the cross-correlation properties of the sequences used to identify different radars, usually belonging to the same set.

## 2.1 Spreading Waveforms and Sequences

PN spreading waveforms are designed primarily for their auto-correlation properties. The design criterion for multiple DS-SS codes is the overall cross-correlation: orthogonal waveforms are used when multiple access is the primary application, and synchronization between signals can be maintained. In asynchronous systems, Quasi-Orthogonal (QO) codes are used, or spreading sequences able to minimize the overall cross-correlation.

Assuming a chip waveform $p(t)$ time-limited to the interval $[0, T_C)$, being $T_C$ the chip pulse period, the spreading signal of the $k$-th radar may be described as:

$$a_k(t) = \sum_{i=-\infty}^{+\infty} a^{(k)}_{imodL} \cdot p(t - iT_C) \qquad (1)$$

where $a^{(k)}$ is a sequence of period $L$ of bipolar elements $a^{(k)}_i = (-1)^{b_i}$, where $b_i \in \{0, 1\}$ are the binary spreading code values. The signal transmitted from the $k$-th radar equipment may be expressed as:

$$s_k(t) = A \cdot a_k(t) \cdot cos(\omega_c t + \phi_k) \qquad (2)$$

where $\omega_c$ is the carrier frequency.

The auto-correlation function over the period of the waveform $T_w = L \cdot T_c$, is defined as:

$$R_{a_k a_k}(\tau) = \frac{1}{T_w} \int_0^{T_w} a_k(t) a_k(t + \tau) dt \qquad (3)$$

The cross-correlation between two waveforms $a_k(t)$ and $a_v(t)$ is similarly written as:

$$R_{a_k a_v}(\tau) = \frac{1}{T_w} \int_0^{T_w} a_k(t) a_v(t + \tau) dt \qquad (4)$$

Both $R_{a_k a_k}(\tau)$ and $R_{a_k a_v}(\tau)$ are periodic in $T_w$. By substituting Eq. (1) and elaborating on previous expressions, it turns out that the periodic auto- and cross-correlation between waveforms depend on the discrete periodic auto- and cross-correlation between sequences (i.e. codes), respectively defined as:

$$C_{a^{(k)} a^{(k)}}[\tau] = \frac{1}{L} \sum_{i=0}^{L-1} a^{(k)}_i a^{(k)}_{i+\tau} \qquad (5)$$

and

$$C_{a^{(k)} a^{(v)}}[\tau] = \frac{1}{L} \sum_{i=0}^{L-1} a^{(k)}_i a^{(v)}_{i+\tau} \qquad (6)$$

where $a^{(k)}_i = (-1)^{b_i}$, $b_i \in \{0, 1\}$ are the binary spreading code values, $\tau$ is the shift among sequences, and $L$ is the length of the spreading codes [16].

The discrete auto- and cross-correlation functions of the sequences affect the behavior of the spreading waveforms. Sequences that are easy to generate, have good auto- and cross-correlation properties, and a large number of codes within the set, are desirable.

## 2.2 Target Echo Detection and Interference Rejection

The signal $r_k(t)$ received back by the $k$-th radar (on board the host vehicle) consists of the superposition of several (namely $K$) replicas (echoes) of the transmitted signal $a_k(t)$, due to the target, to other vehicles, and to clutter from surrounding objects. Each replica features a different amplitude $A_i$ and delay $\tau_i$, that the host system aims to estimate:

$$r_k(t) = \sum_{i=1}^{K} A_i \cdot a_k(t - \tau_i) \cdot cos(\omega_c t + \phi_i) \qquad (7)$$

and, after ideal demodulation,

$$r'_k(t) = \sum_{i=1}^{K} A'_i \cdot a_k(t - \tau_i) \qquad (8)$$

To simplify the discussion, we neglect the contribution of noise, phase, and Doppler effects on the received signals. The correlation computed between $r'_k(t)$ and $a_k(t)$ will output several peaks located at different $\tau_i$'s: once detected the greatest one, typically by comparison against a threshold, the processor can also determine the distances from the other intercepted objects. Named $Z_v$ the decision variable related to the $v$-th target, given by:

$$Z_v = \int_0^{T_w} r_k(t) a_k(t - \tau_v) dt \tag{9}$$

the probability of correct detection $P_D$ will be given by the probability that $Z_v > TH_D$, where $TH_D$ is the value of the threshold corresponding to the presence of the target. On the other hand, the probability of false alarm $P_{FA}$ will be given by the probability that $Z_v > TH_{FA}$, being $TH_{FA}$ the value of the threshold corresponding to no targets present in the scanned area.

Interfering radar signals generated by vehicles moving in the opposite lanes, with respect to the host vehicle, and coded by different signatures, should be similarly taken into account, as they may disturb target detection. When several automotive radars operate in the same vicinity, the mutual interference from the other radars may lead to false alarm or degradation of sensitivity. In the presence of $I$ interfering radars, the signal received at the $k$-th system (after ideal demodulation) may be described as:

$$r'_k(t) = \sum_{i=1}^{K} A'_i \cdot a_k(t - \tau_i) + \sum_{j=1}^{I} B'_j \cdot a_j(t - \tau_j) \tag{10}$$

where the second sum represents interfering radar contributions, and $\tau_j$ accounts for both the propagation delay of the interfering radar signals, and the lack of synchronization among the transmitters. The most dangerous condition occurs when the interfering signal comes from a vehicle moving in the opposite direction with respect to the host vehicle. Despite the very low cross-correlation between interfering and host radar signals, in this situation the amplitude of the interfering signal is proportional to the inverse of the distance, $B'_j \propto \frac{1}{d}$, whereas $A'_i \propto \frac{1}{d^2}$. Due to the different propagation conditions of the reflected and interfering radar signals, a risk exists that the higher power level of the interfering signal blinds the host radar, and the useful echoes get masked. Usually, narrow antenna beams are deemed enough to strongly decrease the probability such a condition may occur.

To optimize the detection process and reduce $P_{FA}$, the threshold value should be set as a function of the number and distance of the vehicles the system should detect at any scan. A false detection occurs when a correlation value over the threshold is not due to a useful echo generated by a target but, instead, to clutter or interfering signals from different radars. The threshold required for minimizing the probability of false detection depends either on the Signal-to-Interfering radar Ratio (SIR), and the sequence length; for a given SIR value, the threshold decreases when the sequence length increases. A good choice for the threshold value is a multiple of the correlation standard deviation.

# 3 De Bruijn binary sequences and their properties

DBSs may be categorized among the sequences generated by means of NLFSRs [17]. The length and the number of distinct sequences are the most important two parameters for each sequence family. For the case of BDBSs, the length equals to $2^n$ and $2^{2^{n-1}-n}$ where *n* is the span value. BDBSs have interesting correlation and security properties. In the following sections, these properties are investigated separately.

## 3.1 Correlation properties

Correlation is one of the most significant properties of sequences, based on which the system performance is evaluated and improved. Due to this fact, it attracts a huge attention. Generally, correlation is a measure that shows the amount of similarity between two sequences. Periodic auto- and cross-correlation (*AC, CC*) may be classified in *Even* and *Odd* (denoted as EC and OC, respectively). Periodic correlation functions consider the real data stream, in which consecutive bits may take different signs, and thus generate different correlation patterns. Therefore, at least two neighboring bits are to be taken into account when calculating the periodic correlation functions. If the two consecutive bits carry the same sign, the even periodic correlation function is computed, otherwise the odd one. The following equations are utilized to calculate the even and odd auto-correlation of a sequence $a$ of period (length) $L$:

$$EC(k) = \frac{1}{L} \sum_{i=1}^{k} a_i a_{i+k} \tag{11}$$

$$OC(k) = \frac{1}{L} \left( - \sum_{i=1}^{k} a_i a_{i+k} + \sum_{i=k+1}^{L} a_i a_{i+k} \right) \tag{12}$$

When considering the results on EC and OC, it comes out that the same number of unique CC values

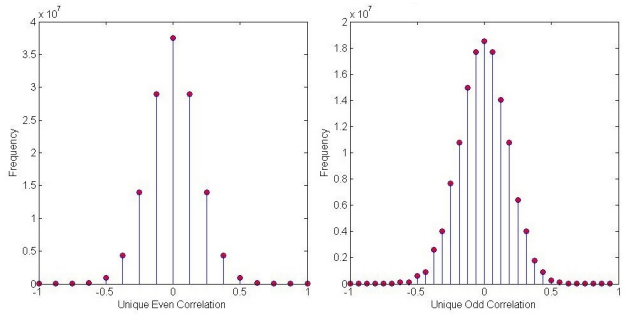


Figure 3: Number of BDBSs having the same EC (left) and OC (right) for $n = 5$

computed as OC is noticeably higher than the number of unique EC values. Eq. (13) indicates the relation between the number of unique EC and OC, which are presented as NEC and NOC. All the EC values may be found in the OC, except the value "+1". The amount of unique correlation values in the both EC and OC exponentially decreases to the right and left from the origin, as illustrated in Fig. 3 which shows the number of sequences having the same correlation for all the possible rotation indices.

This figure clearly shows that EC has a completely symmetric behavior with respect to the origin while OC follows a semi-symmetric trend. For instance, both EC and OC may have correlation value of 0.5. But then, the number of sequences having $OC = +0.5$ is not equal to the number of sequences having $OC = -0.5$.

$$NEC = \frac{NOC}{2} + 1 \tag{13}$$

Another important feature of EC and OC that should deserve attention is the maximum absolute correlation value (MAC) exhibited. According to the simulation results, quite lower MAC values may be achieved for OC than EC. Fig. 4 refers to the case in which sequences are rotated. Also the symmetric behavior in this graph is clear for both OC and EC, except for the last rotation index.

Orthogonality is an important feature of spreading sequences in order to be used for channelization purpose and to cancel or mitigate inter-user interference. It also takes effect on the reverse link to perform forward error correction [18]. Due to these facts, Walsh codes are typically chosen as spreading codes, for their striking orthogonality properties [18]. When checking the orthogonality properties of BDBSs, simulation results show a great outcome, as detailed in Table 1 for the case of span 5 sequences, i.e. 2048 sequences in the same family. To clarify the meaning of this Table, the last values state that 4 DBSs exist,

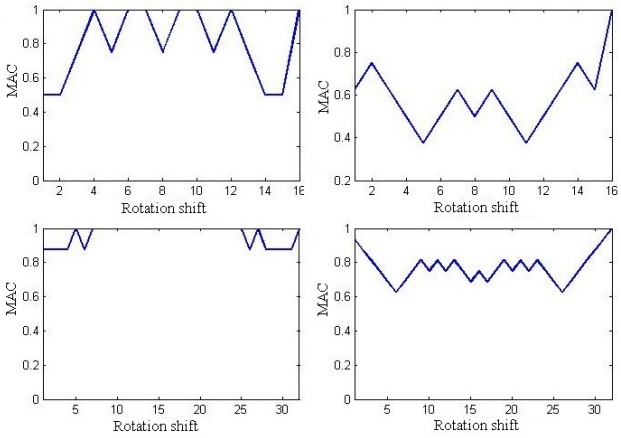


Figure 4: Maximum value of MAC at each rotation, for spans 4 (top) and 5 (bottom), for EC (left) and OC (right)

so that each of them is orthogonal to 2044 different DBSs. The important point is that all the sequences start with the 0 $n$-tuple and the orthogonality is evaluated for zero rotation, which means synchronization among the sequences must be ensured.

Table 1: Number of orthogonal sequences for BDBSs of span 5

| # Orthogonal | 2048 | 2046 | 2044 |
|---|---|---|---|
| # Sequences | 1984 | 60 | 4 |

It can be argued that the orthogonality is not enough to avoid interference. The fact is that the synchronization should be ensured to meet the orthogonality among the sequences [18, 19]. For this reason, AC is indeed the main feature to be evaluated. Both EC and OC exhibit striking features. Rotating to the right and to the left does not produce differences in EC and OC values. Finally, many references deal with the Zero Correlation Zone (ZCZ) property and its application in telecommunications [20–22]. ZCZ is also a inherent property of DBSs [23], as indicated in Eq.s (14)-(16) [24], where $n$ is the span value.

Likewise, the achieved results ensure that unnormalized OC of the first and the one before the last rotations equal 2, for any span value. Further, the OC is zero when the the rotation equals half the sequence length. These properties are clearly illustrated in the left graph of Fig. 5. Note that the figure shows the normalized OC, hereby the first sidelobe of BDBSs of span 5 (with a length of 32) should equal $2/32$.

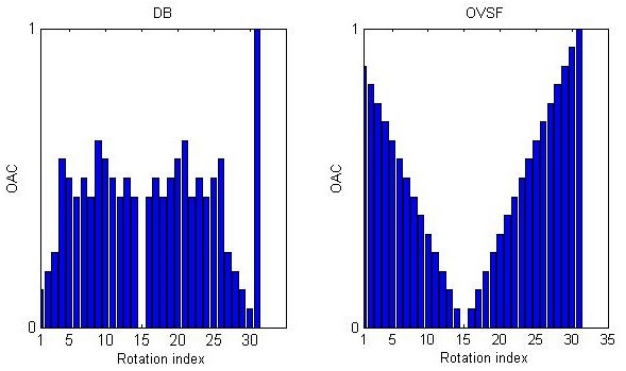


Figure 5: Normalized OC of DBSs (left), and OVSF sequences (right)

$$EC_{\mathbf{a}}(k) = 2^n, \text{ for } k = 0 \quad (14)$$
$$EC_{\mathbf{a}}(k) = 0, \text{ for } 1 \leq |k| \leq n-1 \quad (15)$$
$$EC_{\mathbf{a}}(k) \neq 0, \text{ for } |k| = n \quad (16)$$

The OC and EC have an interesting property which is indicated in Eq.s (17) and (18), $\forall i\ 0 \leq i \leq L$:

$$EC(i) = -EC(L-i) \quad (17)$$

$$OC(i) = OC(L-i) \quad (18)$$

The above equations show the difference in EC and OC properties. Different sequence families, which are DBSs, Orthogonal Variable Spreading Factor (OVSF), Maximal length (M) and Gold sequences, are studied from the OC point of view. The simulation results indicate that the best OC behavior belongs to BDBSs. In fact, the OC function of all the sequence families exhibits the same general trend, which is having the lowest value at the middle rotation index. Among the mentioned sequence families, BDBS and OVSF reach the zero OC at the middle rotation index. As it is clearly illustrated in Fig. 5, in the case of BDBSs, both the left and the right sidelobes have the lowest correlation values, whereas the OC of OVSF sequences gradually decreases from the main-lobe to the middle rotation index.

### 3.2 Security related analysis

NLFSRs may help to provide better sequences than LFSRs from the security aspect [25]. Randomness is a possible measure to evaluate the suitability of sequences with respect to security-related features. The National Institute of Standards and Technology (NIST) provides different tests in order to assess the randomness property of sequences [26]. The intention of this section is to apply these tests on the B-DBSs and conclude with a discussion on the achieved results. All the parameters of the tests are set based on the NIST recommendation. BDBSs of span 5 are only tested and it is due to the need of having access to the whole set of sequences for the given span value. An exhaustive generation of all the BDBSs is much more complex for span values greater than 5.

In order to apply the NIST suite tests on the B-DBSs, the C code provided by the NIST website [27] is utilized. In this tests all distinct DBSs of span 5 (i.e. 2048 sequences) are tested. According to the NIST suite tests, a parameter, named *P-Value*, given as output by each test, indicates whether the sequence is random or not. The achieved outcomes are illustrated in Fig. 6. In this bar chart, the blue and the red bars represent the ratio of the randomness to the whole number of sequences, and the average *P-Value*, respectively. All the sequences are random according to the tests included in the suite that have been applied. Six tests (namely the Longest Run, Rank, Overlapping Template, Universal, Random Excursion and Random Excursion Variant) could not be executed, due to the fact that they require a minimal length of sequences longer than 128, 38912, 38840, and $10^6$, respectively [26]. Considering the obtained results, we may reckon on having all the sequences as random. Sequences with a *P-Value* greater than 0.01 are random [26] and, as shown in Fig. 6, the minimum value for the achieved average *P-Value* ($\approx 0.2$) is much greater than as required.

Regarding to the Linear Complexity (LC), it is noticeable that Berlekamp-Massey Algorithm (BMA) is utilized to calculate the LC of each independent block. Simulation results show that increasing the span value of BDBSs improves LC in terms of having better and the same LC for all the sequences, approximately. Note that LC is calculated for both finite and infinite sequences [28]. From the derived formula and explanation in [28], it can be concluded that the LC of the finite and infinite sequences equal to $L/2$ and $L$, respectively, where $L$ is the length of sequence. Table 2 compares the distribution of the periodic infinite LC of 4 sequence families (OVSF, Gold, M-sequences, and DBSs of span 5). The majority of BDBSs perfectly meet the expected value of LC and they have a remarkable difference with respect to other sequence families. Not only BDBSs of span 5 have higher LC than other sequences, but also their cardinality is incredibly larger. For instance, 1024 BDBSs have an LC of 31, while 16 OVSF sequences are able to reach their highest LC which is limited to 17.

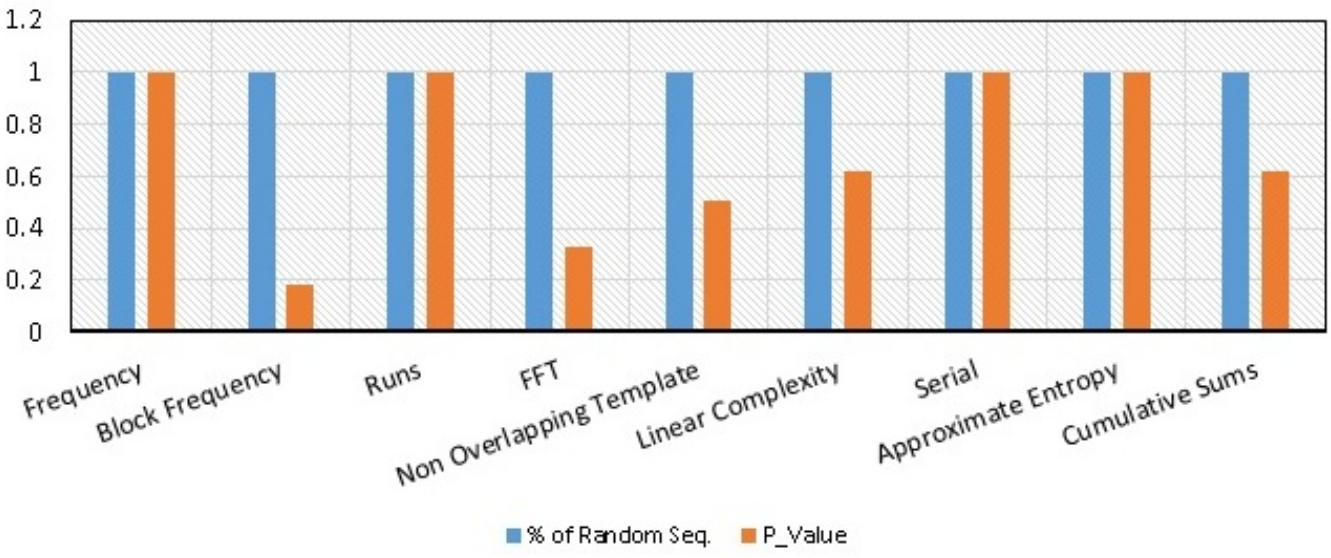


Figure 6: Results of NIST suite tests for BDBSs of span 5

Table 2: Comparison of periodic finite LC. Following pattern is used: *% of Sequences - LC value*

| DB (2048) | OVSF (32) | Gold (31) | M (31) |
|---|---|---|---|
| 0.3906 - 21 | 3.125 - 1 | 6.0606 - 5 | 100 - 5 |
| 0.5859 - 23 | 3.125 - 2 | 93.939 - 10 | - |
| 0.9766 - 24 | 6.25 - 3 | - | - |
| 1.5625 - 25 | 12.5 - 5 | - | - |
| 1.7578 - 26 | 25 - 9 | - | - |
| 3.1250 - 27 | 50 - 17 | - | - |
| 8.7891 - 28 | - | - | - |
| 10.937 - 29 | - | - | - |
| 21.875 - 30 | - | - | - |
| 50 - 31 | - | - | - |

# 4 Simulations and Results

Following the discussion on correlation-related properties of De Bruijn sequences, this Section provides simulation results concerning the adoption of such sequences as radar signatures in a vehicular scenario.

## 4.1 Preliminaries

The simulated scenarios assume a vehicular radar equipment, mounted in front position on a hosting vehicle, that transmits a signal encoded by a specific sequence, on a given direction. Assuming to consider LRR devices, the maximum distance unambiguously detectable is $R_{max} = 150$ m. From this range limit, it is possible to derive the time duration of the sequence to be used, as:

$$\Delta T_{max} = \frac{2R_{max}}{c} = \frac{2 \cdot 150[m]}{3 \cdot 10^8[m/s]} = 10^{-6}[s] \quad (19)$$

The radar-to-target distance is obtained by estimating, through a correlation process, the shift $\tau$ among the received sequence and the one locally generated. When the shift $\tau$ equals the propagation delay $\Delta T$, i.e. $\tau \cdot T_C = \Delta T$, being $T_C$ the chip time (time duration of each bit in the sequence), then it is possible to estimate the distance $R = c \cdot \tau \cdot T_C/2$. The time duration of a sequence consequently corresponds to the maximum delay of the signal, i.e. the following condition shall hold: $T = L \cdot T_C = \Delta T_{max} = 1$ $\mu$s.

Due to the inner nature of the radar system, signals generated by obstacles located at different distances will generate replicas featuring different amplitudes. Further, the received signal will include not only replicas of the transmitted one, but also possible contributions of interfering signals generated by other radar equipments located on board of different vehicles. Interfering signals may be much stronger than the received replicas of the transmitted signal, as they may be generated by radars located nearby the receiver.

The simulation results herein presented are obtained by assuming a single lane road scenario. In order to limit the computation burden, a simplified channel (no multipath) is assumed. Up to $\Gamma$ vehicles are considered, besides the vehicle hosting the reference radar equipment; among the $\Gamma$ vehicles, another one equipped by a radar system may be present, acting as an interfering device. The total received signal may be consequently represented as per Eq. (10). By

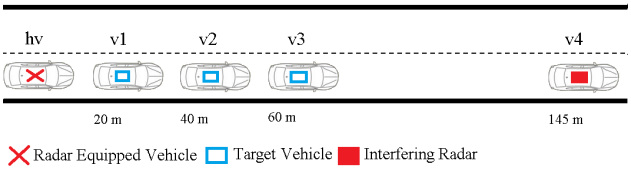


Figure 7: First single-lane simulated scenario: target vehicles (v1, v2, v3) at a distance of 20, 40, and 60 m from the hosting vehicle. The interfering radar (v4) is located on board the last vehicle, at a distance of 145 m

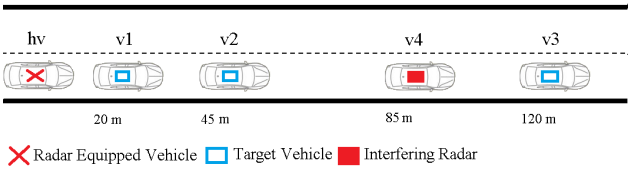


Figure 8: Second single-lane simulated scenario: target vehicles (v1, v2, v3) at a distance of 20, 45, and 120 m from the hosting vehicle. The interfering radar (v4) is located on board the second to last vehicle, at a distance of 85 m

using a correlator receiver locked on the distance of the $i$-th vehicle to detect, a decision variable $Z_i$ may be defined.

Based on the discussion provided in Section 2.2, the probability of correct detection $P_D$, and the probability of false alarm $P_{FA}$ will be evaluated, for different scenarios and signatures used. According to the value chosen for the threshold, different probabilities are obtained: the lower the threshold, the higher $P_D$ will be, but also the higher $P_{FA}$.

Radar signatures are chosen from the set of binary De Bruijn sequences of length 32, and from the set of Gold sequences of length 31. OVSF sequences are not chosen for simulation, as their orthogonality is ensured only in a strictly synchronized system; on the other hand, $m$-sequences are not considered as well, due to the very limited set (for a length equal to 31 only 6 sequences are available), and to the poor cross-correlation properties they exhibit.

## 4.2 Results and Discussion

The first simulated scenario, shown in Fig. 7 consists of 4 vehicles located in a single lane, at a distance of 20, 40, 60, and 145 m, respectively; the last vehicle is equipped by an interfering radar device. The radar onboard the hosting vehicle (i.e. vehicle hv in Fig. 7), and the interfering radar (i.e. vehicle v4 in Fig. 7), are first equipped with De Bruijn signatures, then with Gold ones. The De Bruijn sequences selected as radar signatures feature a maximum unnormalized auto-correlation sidelobe value of 8.

In the second simulated scenario, shown in Fig. 8, a different arrangement of the vehicles is considered, in which the target vehicles are located at a distance of 20, 45 and 120 m, respectively, from the hosting vehicle. The interfering radar is located on board the second to last vehicle, at a distance of 85 m from the hosting one.

By considering the two different scenarios described above, it is possible to evaluate the impact of

Table 3: $P_D$ and $P_{FA}$ obtained by simulating the first scenario

| | $P_D$ | | $P_{FA}$ | |
|---|---|---|---|---|
| vehicle | Gold | DB | Gold | DB |
| v1 | 0.34 | 0.43 | 0.65 | 0.56 |
| v2 | 0.43 | 0.50 | 0.57 | 0.49 |
| v3 | 0.49 | 0.50 | 0.50 | 0.49 |
| v4 | 0.46 | 0.50 | 0.54 | 0.50 |

the interfering radar on the target localization performance of the system. Tables 3 and 4 list the average $P_D$ and $P_{FA}$ obtained in the two scenarios, when using Gold or De Bruijn signatures ($L = 31$ and $L = 32$, respectively) for each radar equipment, randomly selected from the corresponding set of signatures. When the interfering radar is located at the greatest distance from the hosting vehicle, the choice of De Bruijn sequences as radar signatures may provide better performance than Gold codes, both in terms of higher $P_D$ and lower $P_{FA}$. Of course, values reported in Table 3 clearly show that it is not possible to rely on a LRR device only, for autonomous driving, as the detection probability should be further improved by a sensor fusion approach [29]. Problems in using De Bruijn sequences for target detection arise when the interfering radar is not located at the longest distance from the hosting vehicle. As reported in Table 4, the detection probability decreases with respect to Gold codes, and the probability of false alarm increases, with the exception of the case related to vehicle v4.

In the second simulated scenario, the interfering

Table 4: $P_D$ and $P_{FA}$ obtained by simulating the second scenario

| | $P_D$ | | $P_{FA}$ | |
|---|---|---|---|---|
| vehicle | Gold | DB | Gold | DB |
| v1 | 0.54 | 0.47 | 0.46 | 0.53 |
| v2 | 0.50 | 0.49 | 0.50 | 0.51 |
| v3 | 0.35 | 0.33 | 0.61 | 0.65 |
| v4 | 0.49 | 0.51 | 0.51 | 0.49 |

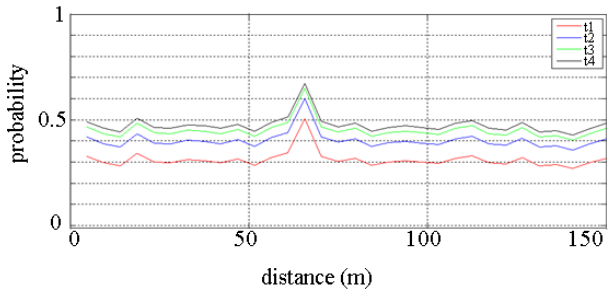


Figure 9: Probability of detection of vehicle v3 in the first scenario, for different threshold values, decreasing from $t_1$ to $t_4$

radar affects the correct detection of target vehicles, as its transmitted signal is much stronger than the received replicas. Basically, the interfering signal is able to almost totally mask the echo signal generated from the vehicle at the greatest distance from the hosting one (i.e. v3 in Fig. 8). This is further confirmed by Fig.s 9 and 10. They show how the probability of detection $P_D$ of the vehicle v3 changes, from the first to the second scenario, respectively, according to different values of the threshold $t_i$ chosen to evaluate $Z_v$, where:

$$t_i = AA_3T/i, i = 1 \dots 4 \qquad (20)$$

being $A$ the amplitude of the transmitted signal, $A_3$ the amplitude of the echo generated by the target vehicle v3, and $T$ the time duration of the sequence. In Fig. 9, following the application of a suitable algorithm designed to eliminate the signal replicas generated by targets different from the one under test [15], the probability of detecting the vehicle v3 shows an evident peak at a distance of almost 60 m, which is the distance actually simulated. Such a probability increases by decreasing the value of the detection threshold $t_i$, and, in any case, it is not affected by the interfering signal generated by the radar equipment onboard vehicle v4, that is the one located at the greatest distance from the hosting vehicle. On the contrary, Fig. 10 clearly shows that the signal replica generated by vehicle v3, when it is located at the greatest distance from the hosting vehicle, and the interfering radar is onboard the second to last vehicle, is totally masked by the interfering signal and cannot be detected by the radar onboard the hosting vehicle v1. As a consequence, the probability of detection decreases significantly.

As a final remark, the performance of De Bruijn sequences have been compared to Gold codes by means of the *ambiguity function* (AF) tool. Such a tool is typically applied for waveform analysis, and

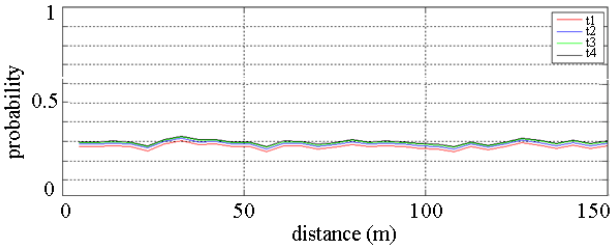


Figure 10: Probability of detection of vehicle v3 in the second scenario, for different threshold values, decreasing from $t_1$ to $t_4$

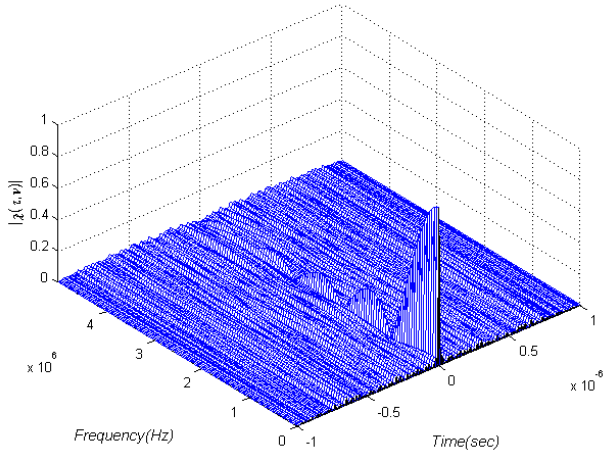


Figure 11: Sample AF plot for a De Bruijn sequence randomly selected from its set

used to estimate the radar performance provided by the selected sequence. The AF represents the time response of a filter matched to a given finite energy signal, when the signal is received with a delay and a Doppler shift $(\tau, \nu)$ relative to the nominal null values expected by the filter itself. To get an ideal range and Doppler resolution, the AF value should be maximum in $(\tau, \nu) = (0, 0)$ and zero elsewhere, but this configuration is actually unfeasible. Clearly, the Doppler effect is a quite significant phenomenon to account for in vehicular scenarios. By means of the AF, it is proved that De Bruijn sequences provide a better correlation than Gold codes, when the Doppler shift is different from zero, thus denoting better performance in target detection.

Fig. 11 shows a sample AF for a De Bruijn sequence randomly selected in the set. Looking at the graph along the frequency axis, it is evident that even for Doppler cuts different from 0, the sequence is able to provide good correlation features, with a quite evident and isolated peak, and small sidelobes, that can favor the detection process at the receiver.

# 5 Conclusion

The paper investigated the performance, in terms of detection capability and false detection rate, of Direct Sequence Spread Spectrum Long Range vehicular Radars adopting binary De Bruijn sequences as radar signatures, compared to more classical solutions adopting Gold codes. The radar detection performance have been discussed in two typical scenarios, and by means of specific tools, such as the ambiguity function, to account for Doppler effects.

Additional to security-related properties exhibited by De Bruijn sequences, that may be critical when the same set of signatures is applied not only in radar equipments but also in vehicle-to-vehicle communications, they provide a better behavior in the presence of Doppler, and a much greater cardinality of their set, at a parity of the length, which may be useful to accommodate many potential users, in a possibly dynamically changing vehicular scenario.

The results herein presented shall be further extended by taking into account the performance of radars in multipath channels, that are typical of vehicular scenarios. This activity is currently ongoing.

*References:*


[1] *Information and Communications Technologies for Safe and Intelligent Vehicles*, SEC(2003), 963, COMMISSION OF THE EUROPEAN COMMUNITIES, Brussels, BE, 2003. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52003DC0542

[2] *Global status report on road safety 2013: supporting a decade of action*, WA 275, World Health Organization, Geneva, Switzerland, 2013. [Online]. Available: http://www.who.int

[3] *Final Report of the eSafety Working Group on Road Safety*, Final Report, November, EU Commission - eSafety Working Group, Brussels, BE, 2002. [Online]. Available: http://bookshop.europa.eu/

[4] M. Murad, I. Bilik, M. Friesen, J. Nickolaou, J. Salinger, K. Geary, and J. Colburn, "Requirements for next generation automotive radars," in *Radar Conference (RADAR), 2013 IEEE*, April 2013, pp. 1–6.

[5] J. Dickmann, N. Appenrodt, and C. Brenk, "How we gave sight to the mercedes robotic car," *IEEE Spectrum*, 2014. [Online]. Available: http://spectrum.ieee.org/transportation/self-driving/how-we-gave-sight-to-the-mercedes-robotic-car

[6] I. Matsunami, N. Ryohei, and A. Kajiwara, "Target state estimation using rcs characteristics for 26ghz short-range vehicular radar," in *Radar (Radar), 2013 International Conference on*, Sept 2013, pp. 304–308.

[7] J.-C. Kedzia, B. Strand, and E. Abenius, "Simulation of automotive radar sensors extended to 77 ghz long range detection," in *Microwave Conference (GeMIC), 2014 German*, March 2014, pp. 1–2.

[8] C. Kim, P. Park, D.-Y. Kim, S.-D. Kim, and H.-K. Yu, "A 77ghz cmos array receiver, transmitter and antenna for low cost small size automotive radar," in *Wireless Symposium (IWS), 2014 IEEE International*, March 2014, pp. 1–4.

[9] J.-C. Kedzia, B. Strand, and E. Abenius, "Simulation of automotive radar sensors extended to 77 ghz long range detection," in *Microwave Conference (GeMIC), 2014 German*, March 2014, pp. 1–2.

[10] T.-N. Luo, C.-H. Wu, and Y.-J. Chen, "A 77-ghz cmos automotive radar transceiver with anti-interference function," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 60, no. 12, pp. 3247–3255, Dec 2013.

[11] J. Sanmartin-Jara, M. Burgos-Garcia, and J. Retamose-Sanchez, "Ss-fh signals used for very low interference in vehicular cruising control systems," in *Vehicular Technology Conference, 1999. VTC 1999 - Fall. IEEE VTS 50th*, vol. 2, 1999, pp. 819–823 vol.2.

[12] G. Righi, S. Spinsante, F. Chiaraluce, and E. Gambi, "Performance of automotive spread spectrum radars," in *Software in Telecommunications and Computer Networks, 2006. SoftCOM 2006. International Conference on*, Sept 2006, pp. 172–176.

[13] E. Gambi, F. Chiaraluce, G. Righi, and S. Spinsante, "A proposal of automotive anticollision radars based on spread spectrum techniques," in *Consumer Electronics, 2007. ICCE 2007. Digest of Technical Papers. International Conference on*, Jan 2007, pp. 1–2.

[14] S. Andrenacci, E. Gambi, C. Sacchi, and S. Spinsante, "Application of de bruijn sequences in automotive radar systems: Preliminary evaluations," in *Radar Conference, 2010 IEEE*, May 2010, pp. 959–964.

[15] E. Gambi, F. Chiaraluce, and S. Spinsante, "Chaos-based radars for automotive applications: Theoretical issues and numerical simulation," *Vehicular Technology, IEEE Transactions on*, vol. 57, no. 6, pp. 3858–3863, Nov 2008.

[16] S. Spinsante and E. Gambi, "De bruijn binary sequences and spread spectrum applications: A marriage possible?" *Aerospace and Electronic Systems Magazine, IEEE*, vol. 28, no. 11, pp. 28–39, Nov 2013.

[17] K. Mandal and G. Gong, "Cryptographically strong de Bruijn sequences with large periods," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7707 LNCS, pp. 104–118, 2013.

[18] L. Korowajczuk, B. de Souza Abreu Xavier, A. M. F. Filho, and Others, *Designing cdma2000 Systems*. John Wiley & Sons, 2004.

[19] H.-H. Chen, *The Next Generation CDMA Technologies*. John Wiley & Sons, 2007. [Online]. Available: http://scholar.google.com/scholar?hl=en\&btnG=Search\&q=intitle:No+Title\#0

[20] P. Fan, N. Suehiro, N. Kuroyanagi, and X. Deng, "Class of binary sequences with zero correlation zone," *Electronics Letters*, vol. 35, no. 10, pp. 777–779, May 1999.

[21] X. Jiang, "Code hopping communications for anti-interception with real-valued qzcz sequences," *Communications, IEEE Transactions on*, vol. 59, no. 3, pp. 680–685, March 2011.

[22] K. Rajawat and A. Chaturvedi, "Near optimal training sequences for low complexity symbol timing estimation in mimo systems," *Communications, IEEE Transactions on*, vol. 58, no. 1, pp. 281–288, January 2010.

[23] M. Sarayloo, E. Gambi, and S. Spinsante, "A large set of orthogonal codes for the v2v scenario," in *Connected Vehicles and Expo (ICCVE), 2014 International Conference on*, Nov 2014.

[24] Z. Z. Wende, "Correlation properties of de bruijn sequences," *Journal of Systems Science and Complexity*, vol. 2, no. 2, p. 170, 1989. [Online]. Available: http://www.sysmath.com/jweb_xtkxyfzx/EN/abstract/article_10703.shtml

[25] A. Klein, *Stream Ciphers*. London: Springer London, 2013. [Online]. Available: http://link.springer.com/10.1007/978-1-4471-5079-4

[26] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," National Institute of Standards and Technology, Tech. Rep. April, 2001. [Online]. Available: http://oai.dtic.mil/oai/oai?verb=getRecord\&metadataPrefix=html\&identifier=ADA393366

[27] "NIST.gov - Computer Security Division - Computer Security Resource Center," 2010. [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html

[28] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 2010.

[29] L. Polidori, E. Gambi, and S. Spinsante, "Proposal of a driver assistance system based on video and radar data fusion," in *Software, Telecommunications and Computer Networks, 2008. SoftCOM 2008. 16th International Conference on*, Sept 2008, pp. 300–304.