(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 095 551 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
11.04.2012 Bulletin 2012/15

(21) Application number: **07847596.9**

(22) Date of filing: **30.11.2007**

(51) Int Cl.:
H04J 13/00 *(2011.01)* ***G01S 1/00*** *(2006.01)*

(86) International application number:
PCT/EP2007/063080

(87) International publication number:
WO 2008/065191 (05.06.2008 Gazette 2008/23)

(54) CHAOTIC SPREADING CODES AND THEIR GENERATION

CHAOTISCHE SPREIZCODES UND IHRE ERZEUGUNG

CODES D'ÉTALEMENT CHAOTIQUE ET LEUR GÉNÉRATION

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR

(30) Priority: **01.12.2006 LU 91292**

(43) Date of publication of application:
02.09.2009 Bulletin 2009/36

(73) Proprietor: **The European Union, represented by the European Commission**
1049 Brussels (BE)

(72) Inventors:
- **HADEF, Mahmoud**
  London E1 0QE (GB)
- **REISS, Josh**
  London E1 4NS (GB)
- **CHEN, Xiaodong**
  London E1 4NS (GB)

(74) Representative: **Office Freylinger**
P.O. Box 48
8001 Strassen (LU)

(56) References cited:
US-A- 5 321 409

- **PENAUD S ET AL: "POTENTIALITES DES SEQUENCES D'ETALEMENT CHAOTIQUES POUR L'AMELIORATION DU TEEB D'UN SYSTEME DS-CDMA ASYNCHRONE BER IMPROVEMENT OF AN ASYNCHRONOUS DS-CDMA SYSTEM USING CHAOTIC SPREADING SEQUENCES" ANNALES DES TELECOMMUNICATIONS - ANNALS OF TELECOMMUNICATIONS, GET LAVOISIER, PARIS, FR, vol. 58, no. 3/4, March 2003 (2003-03), pages 656-672, XP001170104 ISSN: 0003-4347**
- **MIRZAEE A ET AL: "Design of a new class of spreading sequence using chaotic dynamical systems for asynchronous DS-CDMA applications" COMPUTERS AND COMMUNICATIONS, 2004. PROCEEDINGS. ISCC 2004. NINTH INTERNATIONAL SYMPOSIUM ON ALEXANDRIA, EGYPT JUNE 28 - JULY 1, 2004, PISCATAWAY, NJ, USA,IEEE, vol. 2, 28 June 2004 (2004-06-28), pages 720-724, XP010742125 ISBN: 0-7803-8623-X**
- **KOHDA T ET AL: "PSEUDONOISE SEQUENCES BY CHAOTIC NONLINEAR MAPS AND THEIR CORRELATION PROPERTIES" IEICE TRANSACTIONS ON COMMUNICATIONS, COMMUNICATIONS SOCIETY, TOKYO, JP, vol. E76-B, no. 8, 1 August 1993 (1993-08-01), pages 855-862, XP000396888 ISSN: 0916-8516**
- **SOUALLE F ET AL: "Spreading Code Selection Criteria for the future GNSS Galileo" GNSS 2005, 19 July 2005 (2005-07-19), - 22 July 2005 (2005-07-22) pages 1-10, XP002476956 Munich cited in the application**

EP 2 095 551 B1

Printed by Jouve, 75001 PARIS (FR)

Description

Technical Field

[0001] The present invention relates to chaotic spreading codes, in particular a method for generating a set of chaotic spreading codes having autocorrelation and cross-correlation properties suitable for satellite navigation systems and CDMA communication systems.

Background Art

[0002] Satellite radio navigation offers wide-range and precise positioning services with guaranteed reliability, thanks to the state-of-the-art technologies adopted by the existing GPS system. In a few years time, these will be further enhanced by the introduction of the European Galileo satellite navigation constellation, an initiative launched by the European Union and the European Space Agency (ESA). Galileo along with the upcoming third generation GPS III are expected to ensure wider coverage and more precise time and location positioning facilities. However, ensuring such services requires careful reconsideration of different navigation signal parameters such as modulation scheme, navigation message structure and spreading codes design.

[0003] The use of spreading codes makes signals appear wide band and noise-like. It is this very characteristic that makes these signals difficult to intercept, hard to jam and unlikely to interfere with narrowband signals. Therefore, spreading codes play an important role in ensuring a reliable and secure transmission, without producing significant interference with other signals. In spread-spectrum multiple access transmission, such as Direct Sequence Code Division Multiple Access (DS-CDMA) and satellite navigation systems, different signals are assigned different codes and the receiver recovers the desired user's signal by making use of the knowledge of the corresponding spreading code. These spreading codes are desired to have delta-peak-like autocorrelations for an accurate synchronization and low cross-correlations in order to reduce co-channel interferences. Conventional Linear Feedback Shift Register (LFSR) sequences are the most known and studied pseudo-random binary codes in literature and largely used in various applications such as DS-CDMA and satellite navigation systems.

[0004] With regard to the future Galileo satellite navigation system, there is a need to generate new codes in addition to the baseline codes already described in the SIS ICD [1] and assessed in Phase C0 document [2]. Assessment of the baseline codes will require direct comparison with other codes and code sets. Most of the codes described previously, such as the existing E5 Galileo codes, suffer from problems due to truncation from their maximal length. Thus, one should generate codes which have maximal length that is not restricted to a value 2^N-1, for some N. Many codes have been proposed which, in theory, may outperform standard linear feedback shift register-based codes. Thus these codes are worthy of investigation as potential alternatives to the baseline codes, and may be considered for deployment in a flexible Galileo architecture.

[0005] The baseline Galileo codes, are either memory or combined and truncated maximum length sequences (m-sequences). Undeniably, m-sequences are easy to be generated and possess perfect autocorrelation behaviour. However, besides the typical moderate cross-correlation performance of m-sequences, the truncation process, required to ensure the desired code length, destroys the perfect autocorrelation behaviour of such sequences and has an adverse effect on their performance. Conversely, the memory codes can be optimised to have better performance but are difficult to generate on-chip in real-time and hence have to be stored in memory. Therefore, the investigation of alternative schemes such as chaotic codes, which could offer better performance and ease of implementation, would certainly be in the interest of the spread spectrum community.

[0006] One of the problems with pseudo-random codes is their generation. The PRN codes generated by digital signal processors tend to be periodic due to the digital nature of the processors. There has been significant interest in recent years in exploiting chaotic generators to create spreading codes in Spread Spectrum systems [3-5]. The simplicity of these generators, the non-periodicity of the chaotic signals, their sensitivity to initial conditions and their flexibility in terms of length make these generators of significant interest in utilization e.g. in satellite navigation technology or communication technology. These chaotic codes have the benefits of simple implementation, broadband and noise-like appearance, improved transmission privacy, especially over standard m-sequences and Gold sequences, and robustness against channel imperfections like multipath propagation and jamming [3, 4]. Furthermore, the inclusion of chaotic code implementations which are not based on shift registers allows one to generate spreading codes of arbitrary length without the need for truncation. Recent results [5, 8-10] have demonstrated that suitable spreading code generators, based on chaotic maps, may be generated robustly and efficiently, in digital hardware. The high performance of such maps was investigated in [11], where it was also shown how these maps may be modified to yield near ideal correlation properties. Furthermore, the concept of the utilization of chaotic sequences with finite bits by means of a linear feedback shift register has been realized in [8-10] and an algorithmic approach of how to design a decimal m-sequence with prescribed autocorrelation function has been described in [11].

[0007] However, these studies are only suitable for maximal length sequences and are not suitable to arbitrary length codes such as found in Galileo. In fact, extensive simulations have been carried out, where numerous chaotic sets, based on above studies, have been generated and assessed. Despite the good autocorrelation behaviour of such chaotic codes, the random process used in selecting these codes has caused unacceptably weak cross-correlation performance. Furthermore, Gold and Kasami strategies have been to overcome this drawback, however, since these two methods were initially proposed for m-sequences and not for chaotic codes, both failed to provide satisfactory cross correlation performance. In the paper "Design of a new class of spreading sequence using chaotic dynamical systems for asynchronous DS-CDMA applications", by A. Mirzaee et al., a method of generating spreading codes is presented, wherein M randomly chosen seed values are applied as the initial points in chaotic map functions. The sequences thus obtained are then quantized according to different methods. Among the quantized sequences, the one having the best merit factor is selected and the procedure is then repeated.

Object of the Invention

[0008] It is an object of the present invention to propose a method of generating a set of spreading codes that overcomes the above-mentioned problems. This object is achieved by the method as claimed in claim 1.

General Description of the Invention

[0009] The method of generating a set of spreading codes, starts with the determination of first and second chaotic pseudo-random noise codes (seed codes) of the desired length, which have delta-peak-like autocorrelation functions and a low cross-correlation function. Although the meaning of the latter terms should be clear for those skilled in the art, a binary code exhibits a "delta-peak-like" autocorrelation function if its autocorrelation is 0, or at least close to 0 for all delays different from 0; similarly two codes are said to have low cross-correlation if their cross-correlation is 0 or close to 0 for all delays. Further pseudo-random noise codes are obtained by carrying out the steps:

(a) generating a further pseudo-random noise code by computing

$$D_k = F(C_1) + T^k C_2 + F(C_2),$$

where k represents a positive integral index, D_k represents the further pseudo-random noise code being generated, C_1 represents the first code, C_2 represents the second code, F represents a binary function based on basic binary operations and T^k represents the operator that cyclically shifts a code by k chip positions (a "chip" denotes a "bit" of a pseudo-random noise code; however, the term "bit" usually infers that information is encoded);

(b) adding the code D_k to the set of already determined pseudo-random noise codes if the code has a delta-peak-like autocorrelation and low cross-correlation functions with the pseudo-random noise codes already determined;

(c) discarding the code D_k if the conditions for being added to the set of already determined pseudo-random noise codes of step (b) are not satisfied;

(d) modifying (incrementing or decrementing) index k and repeating steps (a)-(d) until the cardinal number of the set of determined pseudo-random noise codes reaches the cardinal number of the set of spreading codes to be generated.

[0010] Those skilled will appreciate that in the present method is not restricted to the generation of codes having a particular length but may be used for codes of arbitrary length. The code length may be fixed at the beginning by the choice of the initial two codes.

[0011] According to a preferred embodiment of the method, the first chaotic pseudo-random noise code is determined by generating a preliminary set of chaotic pseudo-random noise codes based upon an iterative chaotic map (such as e.g. a tent map, a split shift map, an n-way Bernoulli map) and choosing as the first chaotic pseudo-random noise code the code of the preliminary set that exhibits the best delta-peak-like auto-correlation function of the codes of the preliminary set.

[0012] The second chaotic pseudo-random noise code may then be determined by selecting from the preliminary set a code having delta-peak-like autocorrelation and whose cross-correlation with the first chaotic pseudo-random noise code exhibits only one predominant peak for a certain delay, hereinafter denoted L, the delay preferably corresponding

to about half the code length, flipping the first L chips of the selected code and maintaining the remaining chips of the selected code.

[0013] Most preferably, the binary function F mentioned in step (a) is based on (cyclical) shifting and/or on flipping (i.e. inverting the order of a sequence of chips) and/or reversing. In case only these basic operations are used in the method, simple and low cost circuits may be used if the method is implemented in hardware.

[0014] As those skilled will appreciate, the generation of the preliminary set of chaotic pseudo-random noise codes may comprise emulating the chaotic map by an extended linear feedback shift register.

[0015] As discussed hereinafter in more detail, it has been shown that the sets of spreading codes obtained from the present method have better cross-correlation performance than the sets of spreading codes obtained from conventional methods. Given that lower correlation means lower interference and thus permits more efficient use of the available bandwidth, the present method is interesting for all areas related to the spread spectrum technology.

Brief Description of the Drawings

[0016] Further details of the present invention will now be discussed with reference to the following figures, wherein:

Fig. 1 illustrates a conventional LFSR-based code generator for Galileo E5 primary codes [1];

Fig. 2 shows the balance of the codes E5a-I, E5a-Q, E5b-I, and E5b-Q;

Fig. 3 shows Galileo E5a-I codes' even autocorrelation histograms for different Doppler offsets;

Fig. 4 shows even autocorrelation histogram of (left) Existing Galileo E5a-I codes and (right) new tent map based codes;

Fig. 5 shows (left) even cross correlation histogram of the new tent map based codes and (right) cross correlation function between two randomly selected tent map codes;

Fig. 6a shows the maximum rate of occurrence (MRO) of even autocorrelation of a set of tent map codes based on the generation strategy according to the present method in comparison with existing Galileo E5a-I codes, at zero Doppler frequency (DF=0Hz);

Fig. 6b shows the maximum rate of occurrence (MRO) of even cross-correlation of a set of tent map codes based on the generation strategy according to the present method in comparison with existing Galileo E5a-I codes, at zero Doppler frequency (DF=0Hz);

Fig. 7 shows even and odd cross correlation histograms of the tent map codes based on the generation strategy according to the present method;

Fig. 8 shows a flow diagram of a preferred embodiment of a method according to the invention.

Detailed Description

[0017] Fig. 8 illustrates the operation of a preferred embodiment of a method according to the present invention. First, the seed codes are determined by generating a number of preliminary chaotic codes of the desired length N based on an iterative chaotic map, such as the tent map or another of the maps mentioned hereinbefore. These preliminary chaotic codes are generated from randomly selected initial conditions and no specific constraints are used at this stage. From the preliminary chaotic codes obtained based on the tent map, the best code C_1 in terms of autocorrelation is chosen as the first seed code. The second seed code is then obtained by selecting from the preliminary codes another code ("intermediary code") having delta-peak-like autocorrelation and whose cross-correlation with the first seed code exhibits only one predominant peak for a certain delay L corresponding to about half the code length ($L \approx N/2$). As illustrated in Fig. 8 by the insert named "seed selection process", the second seed code C_2 is then obtained from the intermediary code by flipping the first L chips thereof and keeping the remaining N-L chips.

[0018] Once the two seed codes C_1 and C_2 have been fixed, a further pseudo-random noise code D_1 is obtained by computing for k=1:

$$D_k = F(C_1) + T^k C_2 + F(C_2),$$

where F denotes in this case the operator that flips the entire code. In a more elaborate embodiment, the flipping of the entire code could be supplemented by other basic operators based on shifting and/or reversing (inverting the value of some chips). T^k denotes the operator that cyclically shifts a code by k chip positions either to the left or the right.

[0019] The so-obtained code D_k is added to the set of pseudo-random noise codes
if the code has a delta-peak-like autocorrelation, i.e. $AC(D_k)<AC_{max}$, where AC_{max} is the predetermined maximum allowed autocorrelation value for all delays different from 0,
and if the code has low cross-correlation functions with the pseudo-random noise codes already determined, i.e. if for each code C already determined and for all delays: $CC(D_k,C)<CC_{max}$, where CC_{max} denotes the predetermined maximum allowed cross-correlation value.

[0020] If one or both of the above conditions are not satisfied, the code D_k is discarded, the index k is incremented by 1 and the above steps are carried out with the incremented value of k. After having added a code D_k to the set of codes, it is checked whether the required number of codes M has been reached. If this is not the case, k is also incremented by 1 and the above steps are carried out again.

[0021] In the following some issues related to the existing Galileo E5 spreading codes, due to truncation from their maximal length, are highlighted and some results of a set of spreading codes obtained based on the tent map are presented.

GALILEO E5 SPREADING CODES

[0022] The Galileo E5-signal consists of the signals E5a, E5b and is transmitted in the frequency band 1164 - 1215 MHz allocated to RNSS with a worldwide co-primary status [2]. Both E5a and E5b consist of a data-channel, E5a-I and E5b-I signals, transmitted in the in-phase component and a pilot-channel, E5a-Q and E5b-Q signals, transmitted in the quadrature component. The main parameters allocated to the various Galileo E5 spreading codes for each signal component are stated in Table 1. These parameters include the code periods in milliseconds and the code lengths in chips for both so-called primary and secondary sequences.

Table 1: E5 Galileo signal components parameters [2]

Signal Component	Code period (ms)	Code length (chips)	
		Primary	Secondary
E5a-I	20	10230	20
E5a-Q	100	10230	100
E5b-I	4	10230	4
E5b-Q	100	10230	100

[0023] The E5 spreading codes are generated by a tiered code construction, whereby a secondary code sequence is used to modify successive repetitions of a primary code [1]. The primary codes are truncated and combined M-sequences generated by Linear Feedback Shift Registers (LFSR).

E5 Primary Codes

[0024] The E5a-I, E5a-Q, E5b-I and E5b-Q primary codes are basically truncated and combined M-sequences and generated by a simple technique based on two LFSRs [1]. In this technique two parallel shift registers base register 1 and base register 2 are used, as shown in Fig. 1. The primary code is simply the exclusive OR of base registers 1 and 2 outputs. In this specification, each shift register j (j=1 or 2) of length R is fed back with a particular set of feedback taps $a_j = [a_{j,1}, a_{j,2},..., a_{j,R}]$ and its content is represented by a vector $c_j = [c_j^1, c_j^2,..., c_j^R]$, as illustrated in Fig. 1.

[0025] Each cycle, a new primary code-chip is generated and the new shift-register cell contents $c_j(k+1)$ for cycle k+1 are obtained from the contents $c_j(k)$ for cycle k as follows:

$$c_j^i(k+1) = \begin{cases} c_j^{i-1}(k) & \text{for } i = 2,\ldots,R \\ \mathrm{mod}\left(\left(\sum_{k=1}^{R} c_j^i(k)a_{jj}\right),2\right) & \text{for } i = 1 \end{cases} \quad (1)$$

[0026] The content of the two shift registers are reinitialised with start-values sj = $[s_j^1, s_j^2,..., s_j^R]$ after 10230 cycles. The duration of 10230 cycles is also called a primary code epoch. The start-values correspond to the content of the base-start registers 1 and 2 used to generate the 200 Galileo E5 primary codes can be found in [1].

[0027] In information theory the randomness is a vital criterion and an early indicator of the performance of the codes. In practice, no algorithm using a finite state mechanism can produce truly random sequences, since the finiteness forces the sequences to be periodic. However, sequences that closely emulate the randomness could be obtained and are known as pseudo-random sequences. There are many properties which have been derived in literature to measure the randomness of such pseudo-random sequences. The most used and recognised criterion is the Balance property. The balance property simply states that the number of zeros and ones should be as equal as possible per period.

[0028] As can be seen from Fig 2, the spreading codes for E5 band are unbalanced. For example some codes show a relatively significant difference of around 100 more zeros than ones, or vice versa. The main reason behind this drawback is the truncation process performed on the two *m*-sequences (length $16383=2^{14}-1$) at N=10230. Even though some codes have shown good balance hardly any of them has exhibited a perfect balance.

CORRELATION CALCULUS

[0029] Generally speaking, the cross-correlation between two different spreading codes (p and q), should be as small as possible in order to achieve good acquisition and tracking performances. This property should be maintained if the Doppler Effect is taken into account.

[0030] Consider the above two codes are defined by $\{a_{i,p}\}_{i=1}^{N}$ and $\{a_{i,p}\}_{i=1}^{N}$ of length N, where $a_{i,p}$ and $a_{i,q} \in \{-1,1\}$. At the receiver, the cross-correlation between the above two codes, considering the Doppler Effect, can be given by

$$CC_{p,q}(d,f) = \frac{1}{N_p}\sum_{k=1}^{N_p} a_{k,p}a_{k-d,q}e^{2\pi j\frac{f}{f_s}(k-1)} \quad (2)$$

[0031] Where *f* is the Doppler frequency offset, d is the delay and f_s is the sampling frequency.

[0032] The secondary codes used to generate the long Galileo E5 sequences render the cross correlation computation process unrealistic and time consuming. In order to overcome this problem the computation of the cross-correlation can be split up into the calculation of an even cross-correlation CC^e and an odd cross-correlation CC° [2]. Therefore, the total cross-correlation can be given as a linear combination of odd and even cross-correlations:

$$CC_{p,q} = \alpha CC_{p,q}^{e} + \beta CC_{p,q}^{o} \quad (3)$$

[0033] The coefficients α and β, which represent the contribution amounts of both even and odd correlations respectively on the total correlation, can be accurately determined by careful analysis of the secondary codes' randomness properties. Nevertheless, the secondary codes usually are assumed to be random enough to consider that $\alpha = \beta$. The latter assumption may not be compelling in all cases especially for secondary codes with small lengths. This issue is not addressed here and might be considered in future work.

[0034] Fig. 2 shows the autocorrelation histograms of the 50 E5a-I primary codes at different Doppler frequencies 0 Hz, 100 Hz and 6000 Hz. In these histograms the relative frequency or the rate of occurrence of certain correlation value represents the quotient of the number of how many times this value appears by the total number of correlation. For example if we assume a correlation value of a -35dB occurs 15 times between two specific codes with N=10230, hence the relative frequency is simply 15/10230=0.01466. The marks "V" and "Δ" represent respectively the maximal and the

minimal relative frequency. The vertical lines observed for some high correlations mean that at least one of the codes does not exhibit this correlation value. In other words, the minimum value for such correlation over the set of codes is zero and can not been represented in logarithmic scale. The Welch bound is the theoretical boundary towards we aim to shift all out of phase correlations and maximise the distance between them and the autocorrelation peak corresponds to zero delay.

[0035] By analyzing the results shown in Fig. 3, the following observations can be made:

- The number of possible autocorrelations increases significantly with the Doppler frequency offset, and the histogram becomes denser for high Doppler offsets compared to the coarse histogram for zero offset.
- The relative frequency of any given autocorrelation value decreases when the Doppler offset increases.
- The width of vertical lines at high correlation values become larger which means some of the high correlations are disappearing from some codes when the Doppler offset increases.
- The maximum correlation value is shifting toward the Welch bound for higher offsets.

[0036] Therefore, the introduction of Doppler offsets makes the codes looking more random and shifts the maximum correlation value towards the Welch bound. In another term, the Doppler offset leads to some desirable codes characteristics.

NEW CHAOTIC SPREADING CODES

[0037] Most of the codes described previously show sub-optimum correlation performance and suffer from problems due to truncation from their maximal length. In literature many codes have been proposed which, in theory, may outperform standard, linear feedback shift register-based codes such as the chaotic codes. This section is concerned with practical implementations of chaotic codes as possible future candidate as Galileo spreading codes. The chaotic codes are usually generated based on different maps such as tent maps, split shift maps, and n-way Bernoulli maps. Here we are only concerned with the implementation of the generation of chaotic spreading codes based on tent map.

Tent map codes

[0038] The tent map is a well-known chaotic map. It is given by:

$$x_{n+1} = \begin{cases} a x_n & 0 \le x_n \le 0.5 \\ a(1 - x_n) & 0.5 \le x_n \le 1 \end{cases} \quad (4)$$

where $1<a<2$. For example, if we start with initial condition $x_0=0.1$, and $a=1.5$, we get the sequence 0.1, 0.15, 0.225, 0.3375, 0.50625, 0.740625... This is an infinite, non-repeating sequence with excellent correlation properties. If a is set to 2, then many initial conditions will yield periodic output, but it is centred on 0.5. Thus, for a given initial condition $0<x_1<1$, the sequence $x_1, x_2,...$, generated from (4) can be used to generate a finite length spreading code $X_1, X_2,...$ using

$$X_j = \begin{cases} 1 & if \ x_j > 0.5 \\ 0 & otherwise \end{cases} \quad (5)$$

[0039] However, we would like to generate a chaotic sequence based on the tent map, but implemented using binary algebra (similar to standard linear feedback shift register implementations). Our approach of generating the Tent map is to devise an LFSR-based spreading code generator, then transform it into an approximation of the tent map (or extended LFSR, e-LFSR) [5], and then verify it by plotting the output of decimal representation, in similar manner to the procedure described in [5]. Based on the latter procedure a preliminary set of chaotic sequences of length 10230 have been generated and simulated by using an algorithm which takes as input the degree of shift register of an e-LFSR and a random initial state of the shift register.

[0040] Fig. 4 (right) illustrates the even autocorrelation histogram of a preliminary set of 50 tent map codes of length 10230, generated randomly based on the above procedure at zero Doppler frequency. The histogram on the left of Fig. 4 represents the even autocorrelation of the existing E5a-I codes. As we can see the tent map codes demonstrates better autocorrelation performance by a gain of around 4.5dB. This result reflect how the new codes are good as individuals but not as a set. In order to assess mutual performance between the codes the cross correlation histogram are analysed next.

[0041] Fig. 5 (left) even cross correlation histogram of the previously generated tent map based set. The right figure represents the cross correlation function between two randomly selected codes from this set. As can be seen very unacceptable high cross correlation values appeared which reflect the arbitrary codes choice performed in first place. More specifically the cross correlation between these codes shows almost similar pattern with one dominant cross correlation value.

[0042] This issue is overcome by the method described hereinbefore. In the following, an assessment of a new set of spreading codes designed for the E5 band, obtained from the method and based upon two seed codes generated using the tent map set is presented and discussed. A set of 50 chaotic codes has be generated using the method of the present invention, based on the tent map with a code length of 10230 chips. The new codes have outperformed the existing E5a-I Galileo codes in numerous tests including various cross- and auto-correlation calculations over a large range of Doppler frequencies and various selection criteria which assess tracking, acquisition and robustness performance. Fig. 6a shows the maximum rate of occurrence (MRO) of even autocorrelation, and Fig. 6b shows the even cross-correlation, of both new generated chaotic codes and existing Galileo E5a-I sequences, at zero Doppler frequency (DF=0Hz). The desired performance is to shift all out of phase correlations towards the Welch bound as much as possible and maximise the distance between them and the autocorrelation peak corresponding to zero delay. As can be seen the new codes exhibit closer even/odd curves to the Welch bound than the existing E5a-I curves and show lower correlation values.

[0043] For more comprehensive comparison the whole selection process described in Phase C0 [2] and initially used to select the spreading sets for Galileo is considered next. This process includes five different metrics and the final weighting factor of the E5 band for user group A2 described in [12].

Table 2: Metrics Values of both Existing E5a-I Codes and the New Chaotic Set

Criterion	Weighting factors	Metric value		Normalised value	
		Existing	New	Existing	New
$AMEWSD_{MP}$	9%	0.70986	0.68676	-1.65%	+1.65%
$AMEWSD_{CT}$	36%	0.71044	0.70796	-0.17%	+0.17%
AMF_{MP}	4.5%	4.102e-4	4.034e-4	-0.83%	+0.83%
AMF_{CT}	40.5%	1.00007	0.99998	-0.005%	+0.005%
AELW	10%	-2.83410	-2.77975	-0.97%	+0.97%

[0044] Table 2 depicts the existing metric values of the baseline Galileo E5a-I codes and the new chaotic code set, where the weighting factors are determined by multiplying the user group A2 weighting factors and the relevant crosstalk or multipath weighting factors. As can be seen from this table the new chaotic set has outperformed the existing one over all five metrics. The best performance of the new codes is found on the $AMEWSD_{MP}$ criteria with 3.3% enhancement over the existing ones. The smallest improvement is on the AMF with an absolute improvement of 0.01%. The weighted metric is calculated and given in Table 3. It acts as the ultimate judge to decide which code set is preferred. As can be seen overall, based on the selection process used in Phase C0, the new set outperforms the existing one by a margin of 0.7%.

Table 3: Performance Comparison between E5a-I Existing and the New Set

Codes set	Performance
Existing Galileo E5a-I set	-0.35%
New Tent map set	+0.35%

REFERENCES

[0045]

[1] D. Flachs, V. Oehler, S. Bouchired, E. E. Canalis, P. P. Muller-Remmers, M. Marinelli, H. De Gaujac, U. Gageur, and M. Falcone, "Galileo Signal In Space Interface Control Document (SIS-ICD), Ver. 10.1," Galileo Industries September 28 2005.

[2] S. Wallner, "Consolidated Code Design (TN ID31)," Galileo Phase C0 / CN001, November 10 2004.

[3] V. Varadan and H. Leung, "Design of Piecewise Maps for Chaotic Spread-Spectrum Communications Using Genetic Programming," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 49, pp. 1543-1553,2002.

[4] G. Mazzini, G. Setti, and R. Rovatti, "Chaotic complex spreading sequences for asynchronous DS-CDMA - Part I: System modeling and results," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 44, pp. 937-947, 1997.

[5] D. Yoshioka, A. Tsuneda, and T. Inoue, "On Transformation between Discretized Bernoulli and Tent Maps," IEICE TRANS, Fundamentals, vol. E88-A, 2005.

[6] R. Rovatti, G. Setti, and G. Mazzini, "Chaotic complex spreading sequences for asynchronous DS-CDMA - Part II: Some theoretical performance bounds," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 45, pp. 496-506, 1998.

[7] T. Kohda and A. Tsuneda, "Statistics of chaotic binary sequences," IEEE Trans. Inf. Theory, vol. 43, pp. 104-112, 1997.

[8] A. L. Baranovski, F. Dachselt, and W. R.. "Nonlinear dynamics of PN-sequences," Proceedings of the IST Mobile & Wireless Communications Summit 2005, 2005.

[9] A. L. Baranovski, "On Generation of Chaotic M-Sequences," Proceedings of the International Symposium on Nonlinear Theory and its Applications (NOLTA), Bruges, Belgium, 2005.

[10] D. Yoshioka, A. Tsuneda, and T. Inoue, "An algorithm for the generation of maximal-period sequences based on one-dimensional chaos maps with finite bits," IEICE Trans. Fundamentals, vol. E87-A, no.6, pp.1371-1376, June 2004.

[11] A. L. Baranovski and A. J. Lawrance, "Sensitive parameter dependence of autocorrelation function in piecewise linear maps," International Journal of Bifurcations and Chaos, 2006.

[12] F. Soualle, M. Soellner, S. Wallner, J.-A. Avila-Rodriguez, G. W. Hein, B. Barnes, T. Pratt, L. Ries, J. Winkel, C. Lemenager, and P. Erhard, "Spreading Code Selection Criteria for the future GNSS Galileo," Proceedings of the GNSS 2005, Munich, 2005.

Claims

1. A method of generating a set of spreading codes, comprising:

determining first and second chaotic pseudo-random noise codes, said first and second codes having delta-peak-like autocorrelation functions, i.e. autocorrelations functions that take a value of 0 or close to 0 for all delays different from 0, and a low cross-correlstion function, i.e a cross-correlation function that takes a value of 0 or close to 0 for all delays;
said method being **characterized in that** further pseudo-random noise codes are determined by carrying out the steps:

a) generating a further pseudo-random noise code by computing

$$D_k = F(C_1) + T^k C_2 + F(C_2),$$

where k represents a positive integral index, D_k represents the further pseudo-random noise code being generated, C_1 represents the first code, C_2 represents the second code, F represents a binary function based on basic binary operations and T^k represents the operator that cyclically shifts a code by k chip positions;
b) adding the code D_k to the set of already determined pseudo-random noise codes if said code has a delta-peak-like autocorrelation and low cross-correlation functions with the pseudo-random noise codes already determined;
c) discarding the code D_k if the conditions for being added to the set of already determined pseudo-random noise codes of step (b) are not satisfied;
d) modifying index k and repeating steps (a)-(d) until the cardinal number of the set of determined pseudo-random noise codes reaches the cardinal number of the set of spreading codes to be generated.

2. Method according to claim 1, wherein said first chaotic pseudo-random noise code is determined by generating a preliminary set of chaotic pseudo-random noise codes based upon an iterative chaotic map and choosing as said first chaotic pseudo-random noise code the code of said preliminary set that exhibits the best delta-peak-like autocorrelation function of the codes of said preliminary set.

3. The method according to claim 2, wherein said second chaotic pseudo-random noise code is determined by selecting from said preliminary set a code having delta-peak-like autocorrelation and whose cross-correlation with said first chaotic pseudo-random noise code exhibits only one predominant peak for a certain delay, hereinafter denoted L, said delay preferably corresponding to about half the code length, flipping the first L chips of the selected code and maintaining the remaining chips of the selected code.

4. The method according to claim 2, wherein said iterative chaotic map is a tent map or a split shift map or an n-way Bernoulli map.

5. The method according to any one of claims 1 to 4, wherein said binary function is based on shifting and/or on flipping and/or reversing.

6. The method according to claim 2, wherein generating said preliminary set of chaotic pseudo-random noise codes comprises emulating said chaotic map by an extended linear feedback shift register.

7. Storage medium having stored therein a set of spreading codes obtained from the method according to any one of claims 1 to 6.

8. Storage medium having stored therein computer-executable instructions for implementation of the method according to any one of claims 1 to 6.

9. Use of the set of spreading codes obtained from the method according to any one of claims 1 to 6 in a CDMA system or a satellite navigation system.

Patentansprüche

1. Verfahren zur Erzeugung eines Satzes von Spreizcodes, umfassend:

Bestimmen eines ersten und zweiten chaotischen Pseudozufallsrauschcodes, wobei der erste und der zweite Code Delta-Peak-artige Autokorrelationsfunktionen, d.h. Autokorrelationsfunktionen, die einen Wert von 0 oder nahe bei 0 für alle Verzögerungen ungleich 0 annehmen, und eine niedrige Kreuzkorrelationsfunktion, d.h. eine Kreuzkorrelationsfunktion, die einen Wert von 0 oder nahe bei 0 für alle Verzögerungen annimmt, aufweisen; wobei das Verfahren **dadurch gekennzeichnet ist, dass** weitere Pseudozufallsrauschcodes durch Durchführen der folgenden Schritte bestimmt werden:

a) Erzeugen eines weiteren Pseudozufallsrauschcodes durch Berechnen von

$$D_k = F(C_1) + T^k C_2 + F(C_2),$$

wobei k einen positiven ganzzahligen Index repräsentiert, D_k den weiteren Pseudozufallsrauschcode, der erzeugt wird, repräsentiert, C_1 den ersten Code repräsentiert, C_2 den zweiten Code repräsentiert, F eine binäre Funktion auf Basis von binären Grundoperationen repräsentiert und T^k den Operator, der zyklisch einen Code um k Chip-Positionen verschiebt, repräsentiert;
b) Hinzufügen des Codes D_k zu dem Satz von bereits bestimmten Pseudozufallsrauschcodes, wenn der Code eine Delta-Peak-artige Autokorrelationsfunktion und eine niedrige Kreuzkorrelationsfunktion mit den bereits bestimmten Pseudozufallsrauschcodes aufweist;
c) Verwerfen des Codes D_k, wenn die Bedingungen für das Hinzufügen zu dem Satz von bereits bestimmten Pseudozufallsrauschcodes des Schritts (b) nicht erfüllt sind;
d) Modifizieren des Indexes k und Wiederholen der Schritte (a)-(d), bis die Kardinalzahl des Satzes von bereits bestimmten Pseudozufallsrauschcodes die Kardinalzahl des Satzes von zu erzeugenden Spreizcodes erreicht.

2. Verfahren nach Anspruch 1, wobei der erste chaotische Pseudozufallsrauschcode durch Erzeugen eines vorläufigen Satzes von chaotischen Pseudozufallsrauschcodes auf Basis einer iterativen chaotischen Abbildung bestimmt wird und als der erste chaotische Pseudozufallsrauschcode der Code des vorläufigen Satzes ausgewählt wird, der die beste Delta-Peak-artige Autokorrelationsfunktion der Codes des vorläufigen Satzes zeigt.

3. Verfahren nach Anspruch 2, wobei der zweite chaotische Pseudozufallsrauschcode bestimmt wird durch Auswählen, aus dem vorläufigen Satz, eines Codes, der eine Delta-Peak-artige Autokorrelation aufweist und dessen Kreuzkorrelation mit dem ersten chaotischen Pseudozufallsrauschcode nur einen vorherrschenden Peak für eine nachstehend als L bezeichnete gewisse Verzögerung zeigt, wobei die Verzögerung vorzugsweise ungefähr der Hälfte der Codelänge entspricht; Umdrehen der ersten L Chips des ausgewählten Codes; und Beibehalten der übrigen Chips des ausgewählten Codes.

4. Verfahren nach Anspruch 2, wobei die iterative chaotische Abbildung eine Zeltabbildung oder eine geteilte Shift-Abbildung oder eine n-Weg-Bernoulli-Abbildung ist.

5. Verfahren nach irgendeinem der Ansprüche 1 bis 4, wobei die binäre Funktion auf dem Verschieben und/oder Umdrehen und/oder Umkehren basiert.

6. Verfahren nach Anspruch 2, wobei das Erzeugen des vorläufigen Satzes von chaotischen Pseudozufallsrauschcodes das Emulieren der chaotischen Abbildung durch ein erweitertes linear rückgekoppeltes Schieberegister umfasst.

7. Speichermedium, in welchem ein Satz von Spreizcodes gespeichert ist, der durch das Verfahren nach irgendeinem der Ansprüche 1 bis 6 erhalten wurde.

8. Speichermedium, in welchem von einem Computer ausführbare Anweisungen zur Implementierung des Verfahrens nach irgendeinem der Ansprüche 1 bis 6 gespeichert sind.

9. Verwendung des Satzes von Spreizcodes, der durch das Verfahren nach irgendeinem der Ansprüche 1 bis 6 erhalten wurde, in einem CDMA-System oder einem Satellitennavigationssystem.

Revendications

1. Procédé de génération d'un ensemble de codes d'étalement, comprenant :

la détermination d'un premier et d'un deuxième codes de bruit pseudo aléatoires chaotiques, lesdits premier et deuxième codes ayant des fonctions d'autocorrélation de type pic delta, à savoir des fonctions d'autocorrélation qui prennent une valeur de 0 ou proche de 0 pour tous les retards différents de 0, et une fonction de corrélation croisée basse, à savoir une fonction de corrélation croisée qui prend une valeur de 0 ou proche de 0 pour tous les retards ;

ledit procédé étant **caractérisé en ce que** d'autres codes de bruit pseudo aléatoires sont déterminés en exécutant les étapes :

a) de génération d'un autre code de bruit pseudo aléatoire en calculant

$$D_k = F(C_1) + T^k C_2 + F(C_2),$$

où k représente un indice entier positif, D_k représente l'autre code de bruit pseudo aléatoire étant généré, C_1 représente le premier code, C_2 représente le deuxième code, F représente une fonction binaire basée sur des opérations binaires basiques et T^k représente l'opérateur qui décale cycliquement un code de k positions de bribe ;
b) d'ajout du code D_k à l'ensemble de codes de bruit pseudo aléatoires déjà déterminés si ledit code a des fonctions d'autocorrélation de type pic delta et de corrélation croisée basse avec les codes de bruit pseudo aléatoires déjà déterminés ;
c) de rejet du code D_k si les conditions pour être ajouté à l'ensemble de codes de bruit pseudo aléatoires déjà déterminés de l'étape b) ne sont pas satisfaites ;
d) de modification de l'indice k et de répétition des étapes (a)-(d) jusqu'à ce que le nombre cardinal de l'ensemble de codes de bruit pseudo aléatoires déterminés atteigne le nombre cardinal de l'ensemble de codes d'étalement devant être généré.

2. Procédé selon la revendication 1, dans lequel ledit premier code de bruit pseudo aléatoire chaotique est déterminé en générant un ensemble préliminaire de codes de bruit pseudo aléatoires chaotiques sur la base d'une application chaotique itérative et en choisissant comme ledit premier code de bruit pseudo aléatoire chaotique le code dudit ensemble préliminaire qui affiche la meilleure fonction d'autocorrélation de type pic delta parmi les codes dudit ensemble préliminaire.

3. Procédé selon la revendication 2, dans lequel ledit deuxième code de bruit pseudo aléatoire chaotique est déterminé en sélectionnant parmi ledit ensemble préliminaire un code ayant une autocorrélation de type pic delta et dont la corrélation croisée avec ledit premier code de bruit pseudo aléatoire chaotique n'affiche qu'un pic prédominant pour un certain retard, ci-après dénoté L, ledit retard correspondant préférablement à environ la moitié de la longueur de code, en retournant les premières L bribes du code sélectionné et en maintenant les bribes restantes du code sélectionné.

4. Procédé selon la revendication 2, dans lequel ladite application chaotique itérative est une application tente ou une application à décalage fractionné ou une application de Bernoulli à n critères.

5. Procédé selon l'une quelconque des revendications 1 à 4, dans lequel ladite fonction binaire est basée sur un décalage et/ou sur un retournement et/ou une inversion,

6. Procédé selon la revendication 2, dans lequel la génération dudit ensemble préliminaire de codes de bruit pseudo aléatoires chaotiques comprend l'émulation de ladite application chaotique par un registre à décalage à boucle fermée linéaire étendu.

7. Support de stockage ayant, stocké dans celui-ci, un ensemble de codes d'étalement obtenu à partir du procédé selon l'une quelconque des revendications 1 à 6.

8. Support de stockage ayant, stockées dans celui-ci, des instructions exécutables par un ordinateur pour une mise en oeuvre du procédé selon l'une quelconque des revendications 1 à 6.

9. Utilisation de l'ensemble de codes d'étalement obtenu à partir du procédé selon l'une quelconque des revendications 1 à 6 dans un système AMRC ou un système de navigation par satellite.

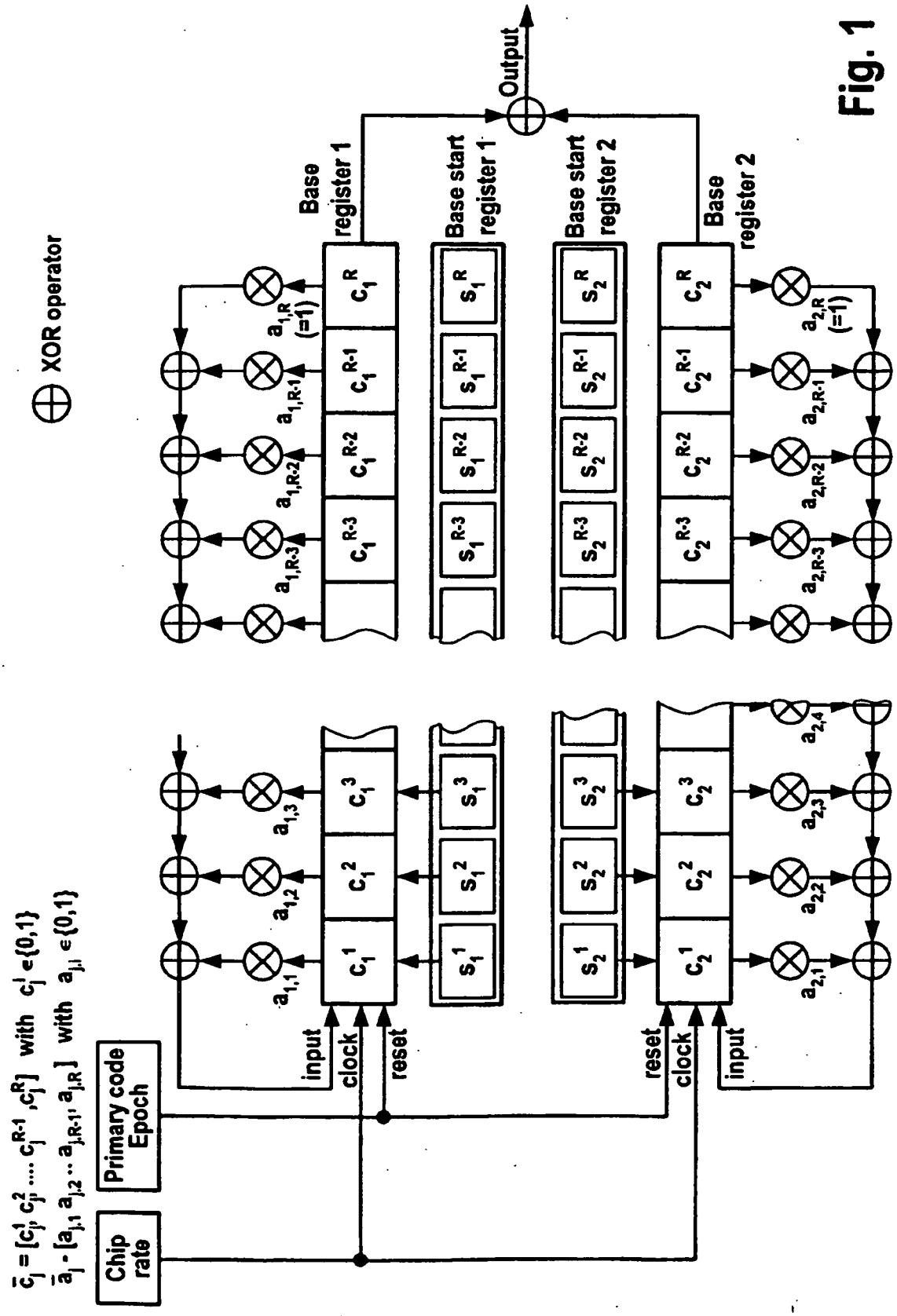

XOR operator
Output
Base register 1
Base start register 1
Base start register 2
Base register 2
Chip rate
Primary code Epoch
input
clock
reset
reset
clock
input

Fig. 1

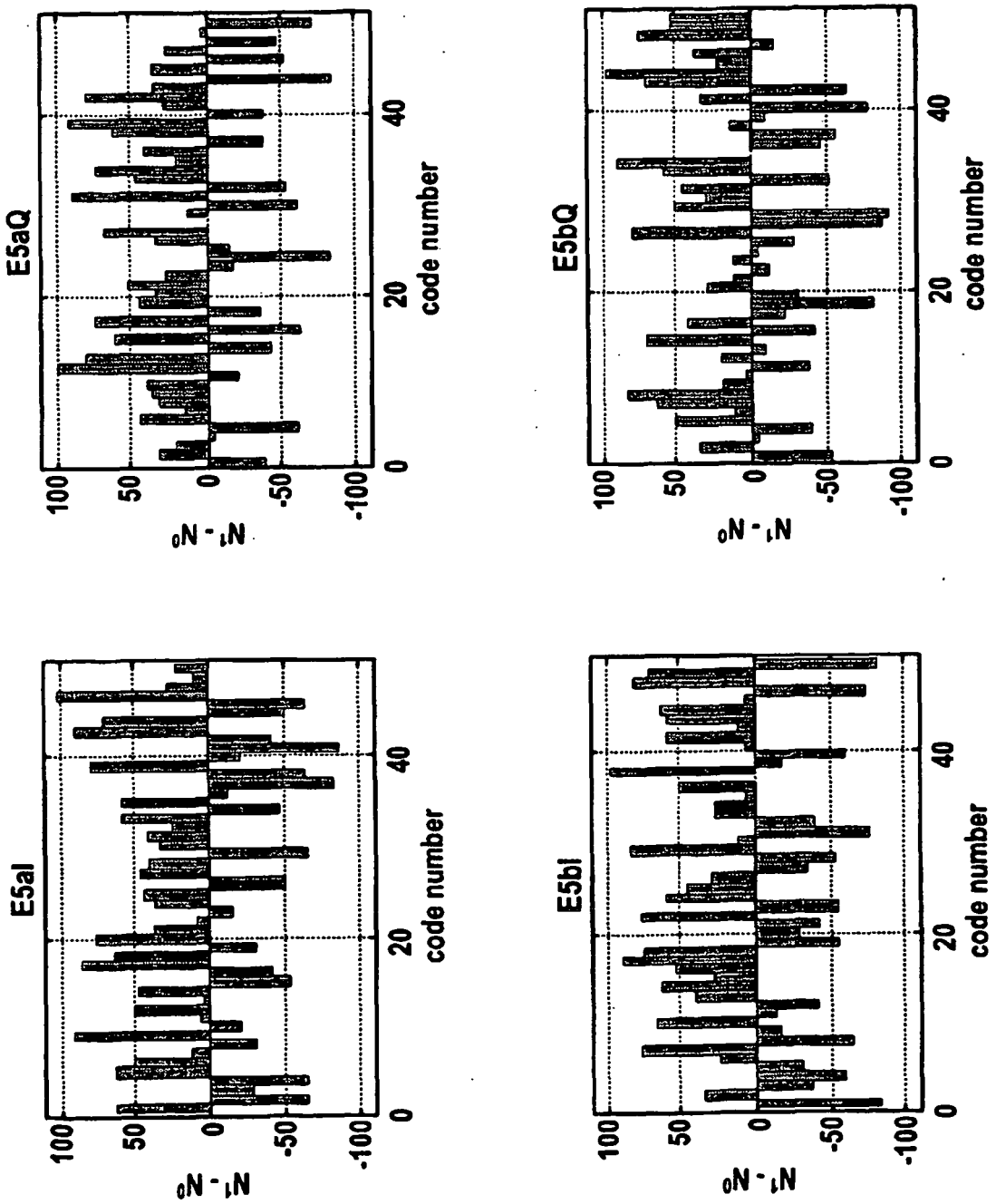
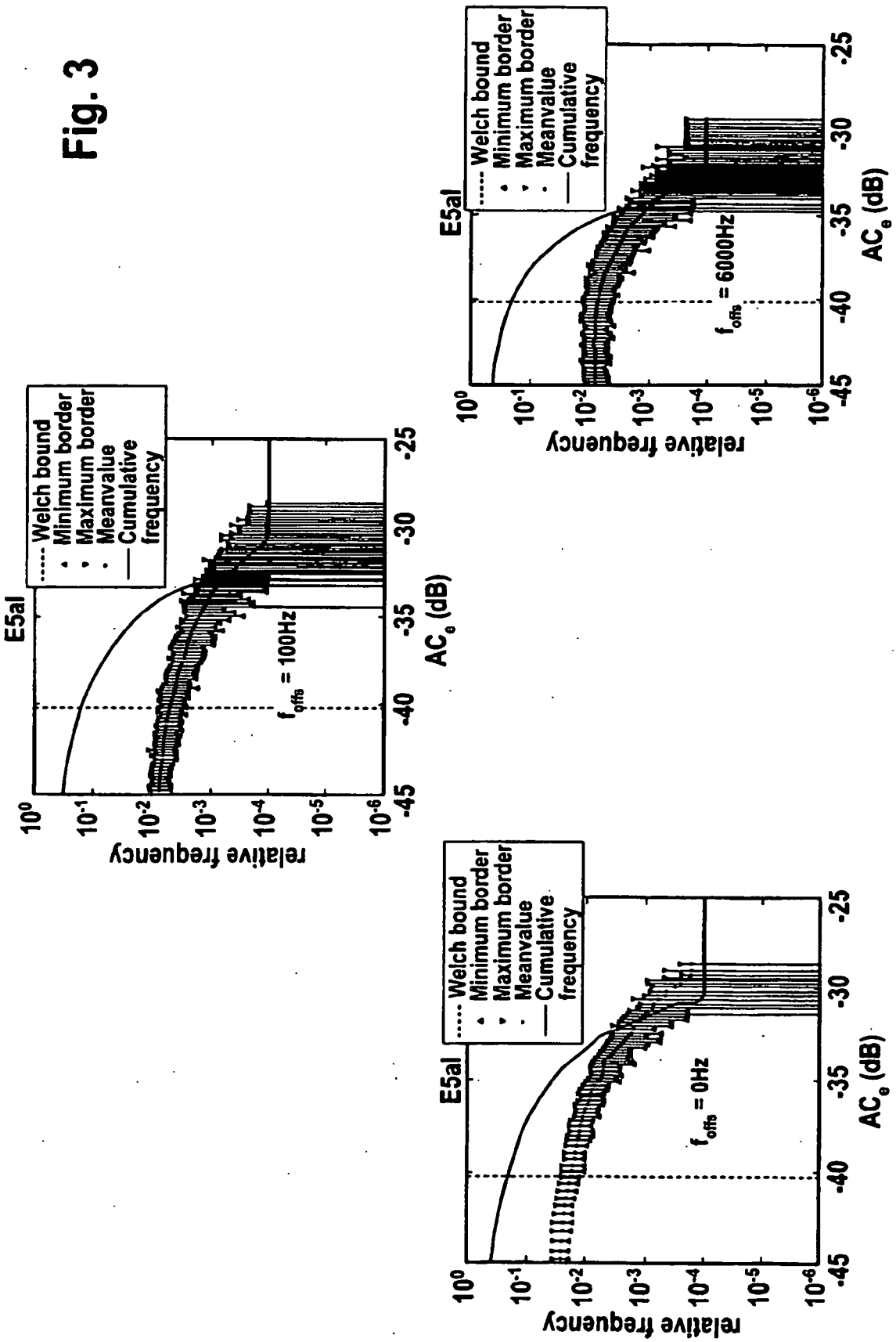


Fig. 2

Fig. 3


E5aI
Welch bound
Minimum border
Maximum border
Meanvalue
Cumulative frequency
f_{offs} = 100Hz
f_{offs} = 6000Hz
f_{offs} = 0Hz
relative frequency
AC_e (dB)

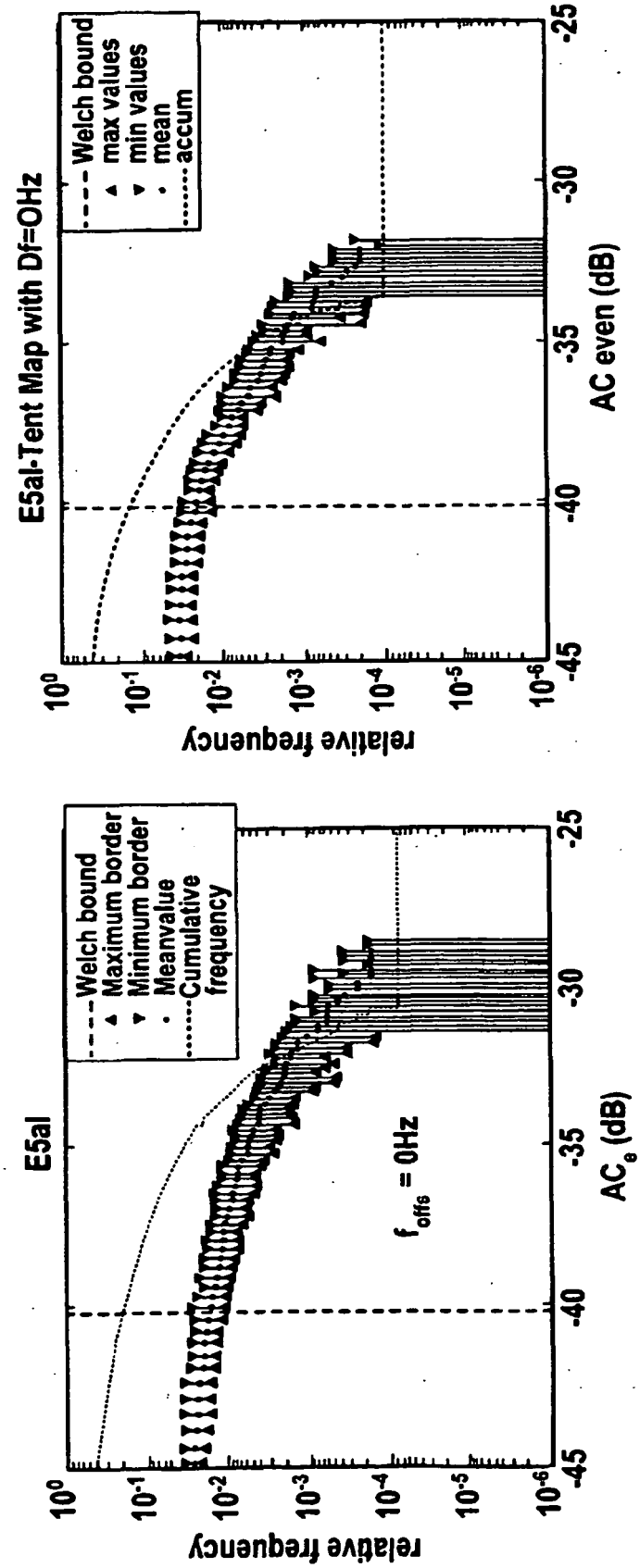

E5aI-Tent Map with Df=OHz
Welch bound
max values
min values
mean
accum
relative frequency
AC even (dB)
E5aI
Welch bound
Maximum border
Minimum border
Meanvalue
Cumulative frequency
f_{offs} = 0Hz
relative frequency
AC_e (dB)

Fig. 4

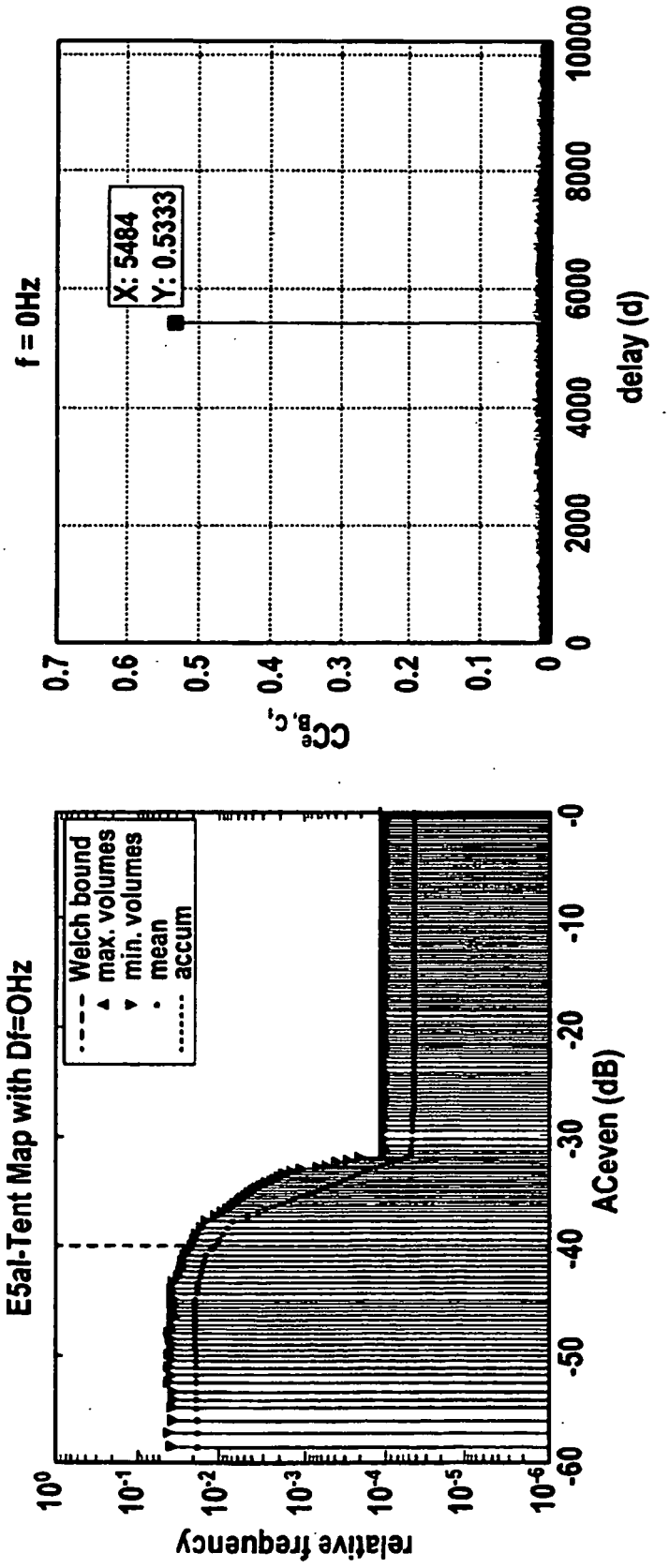

f = 0Hz
X: 5484
Y: 0.5333
delay (d)
0
2000
4000
6000
8000
10000
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
E5al-Tent Map with Df=OHz
Welch bound
max. volumes
min. volumes
mean
accum
relative frequency
ACeven (dB)
-0
-10
-20
-30
-40
-50
-60

Fig. 5

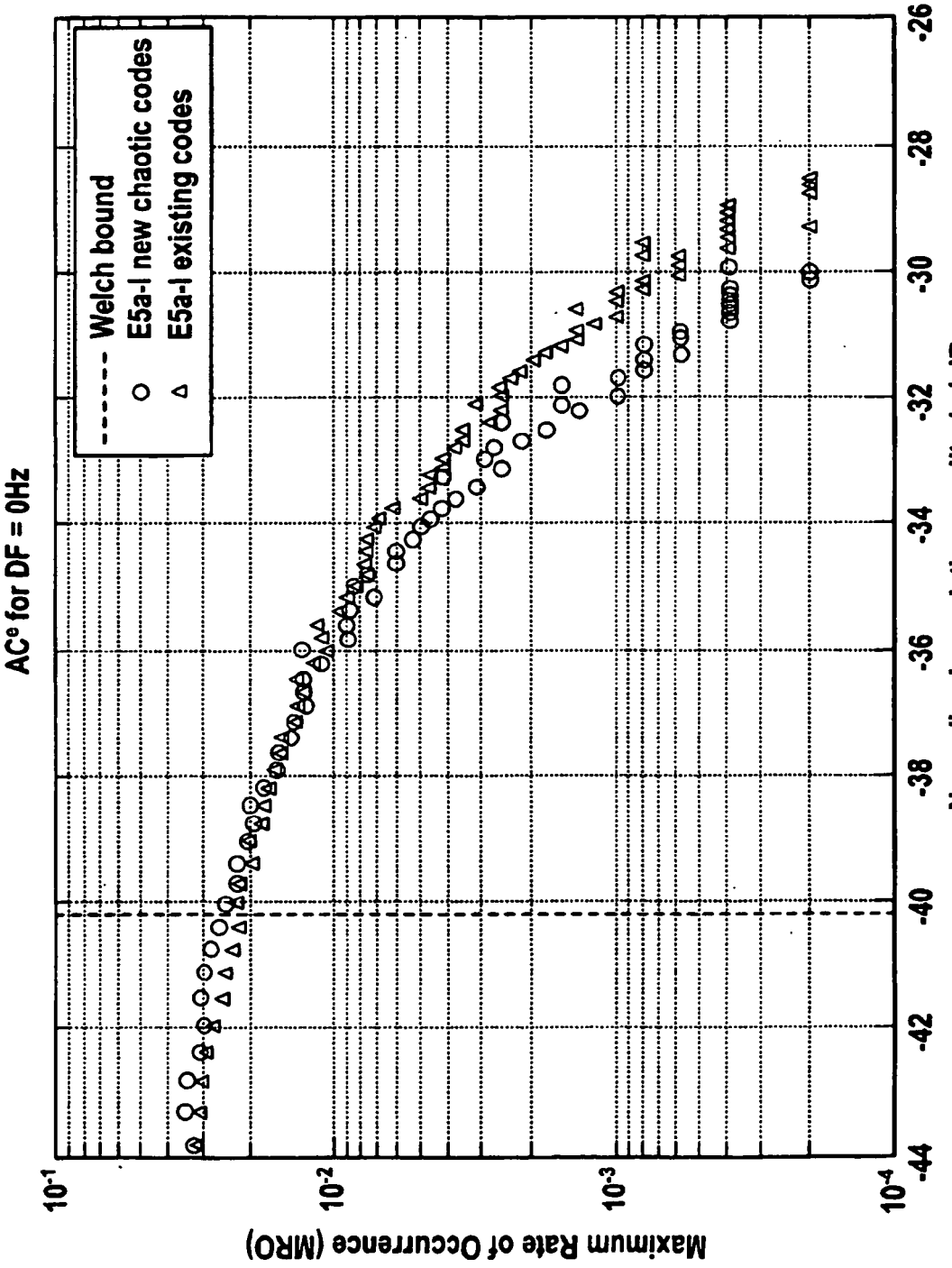

ACe for DF = 0Hz
Welch bound
E5a-I new chaotic codes
E5a-I existing codes
Maximum Rate of Occurrence (MRO)
10-1
10-2
10-3
10-4
-44
-42
-40
-38
-36
-34
-32
-30
-28
-26
Normalised correlation amplitude / dB

Fig. 6a

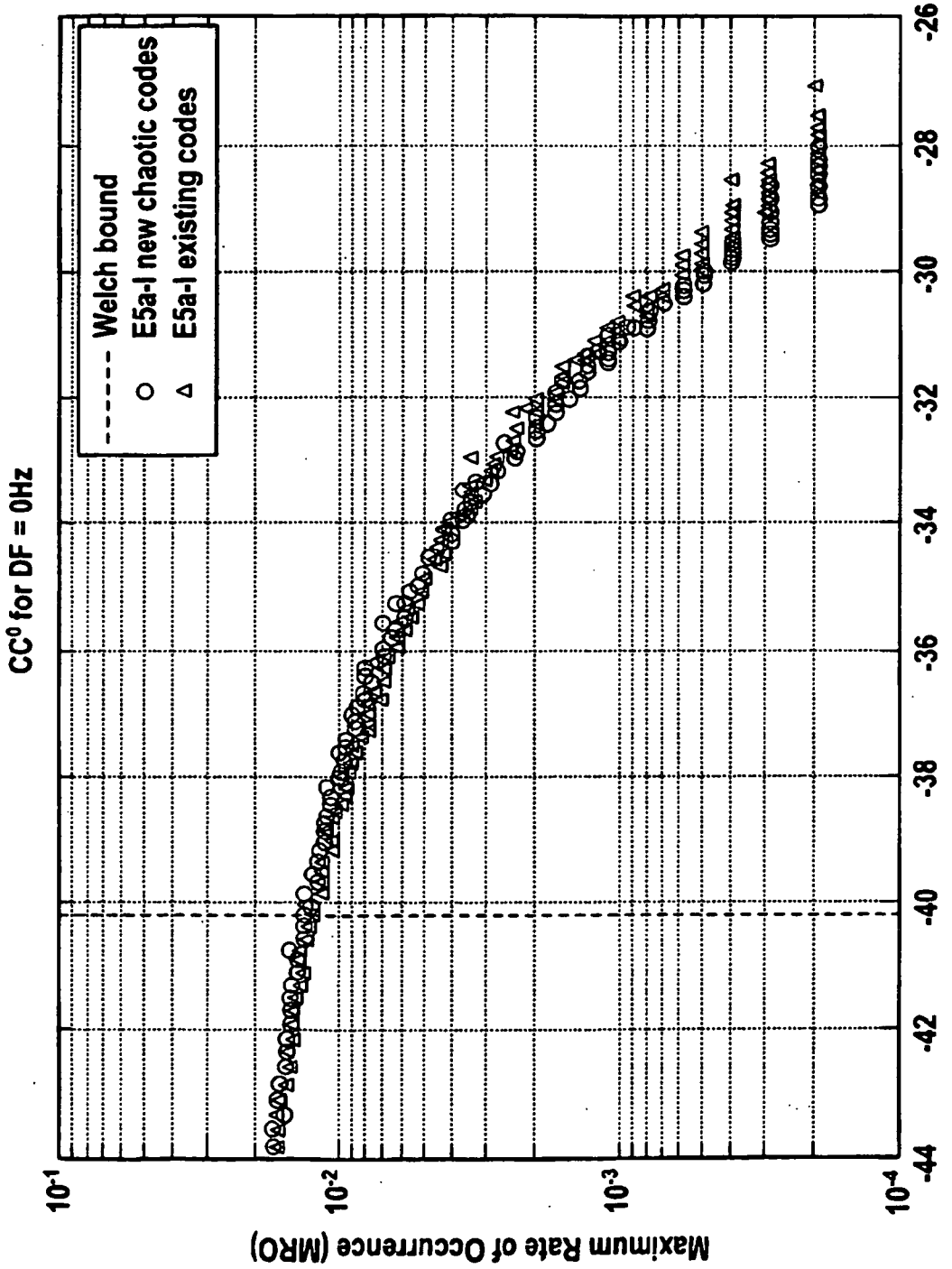
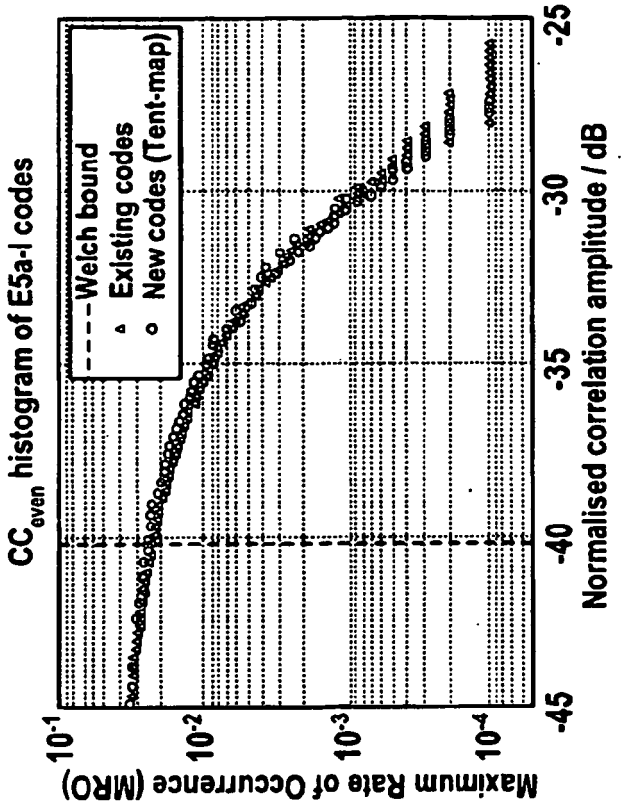

Welch bound
E5a-I new chaotic codes
E5a-I existing codes
CC⁰ for DF = 0Hz
Maximum Rate of Occurrence (MRO)
Normalised correlation amplitude / dB
10⁻¹
10⁻²
10⁻³
10⁻⁴
-26
-28
-30
-32
-34
-36
-38
-40
-42
-44

Fig. 6b


CC_even histogram of E5a-I codes
Welch bound
Existing codes
New codes (Tent-map)
Maximum Rate of Occurrence (MRO)
Normalised correlation amplitude / dB
10^-1
10^-2
10^-3
10^-4
-45
-40
-35
-30
-25

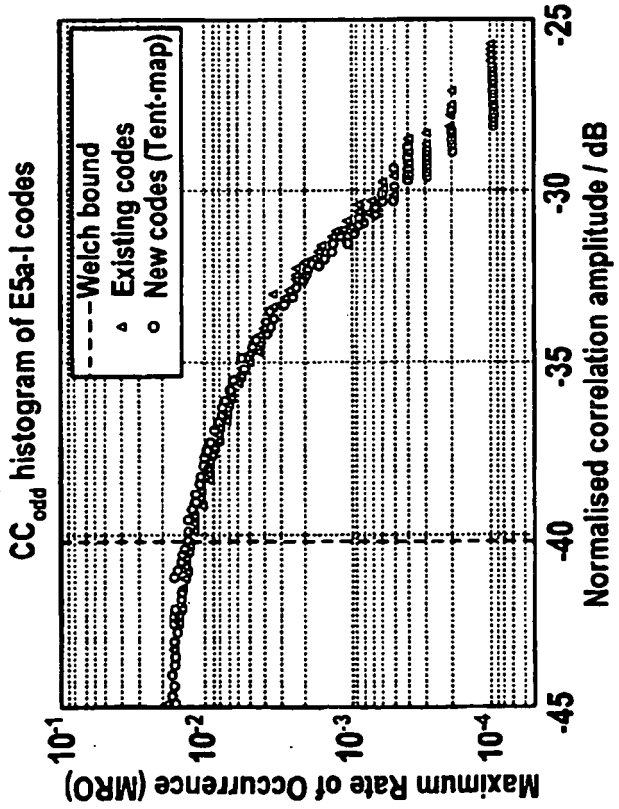

CC_odd histogram of E5a-I codes
Welch bound
Existing codes
New codes (Tent-map)
Maximum Rate of Occurrence (MRO)
Normalised correlation amplitude / dB
10^-1
10^-2
10^-3
10^-4
-45
-40
-35
-30
-25

Fig. 7

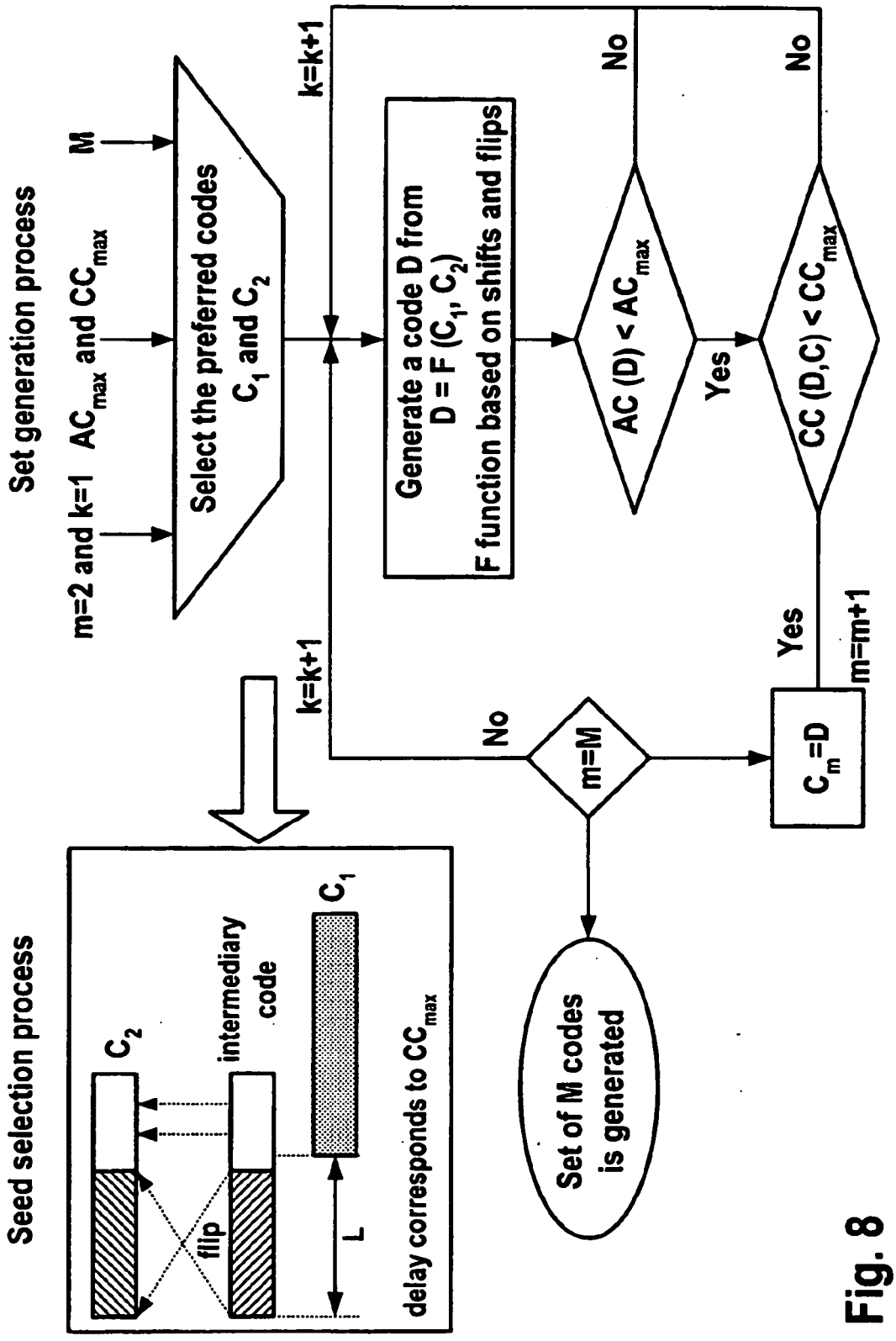

Set generation process
M
m=2 and k=1
AC_{max} and CC_{max}
Select the preferred codes
C_1 and C_2
k=k+1
Generate a code D from
D = F (C_1, C_2)
F function based on shifts and flips
No
$AC(D) < AC_{max}$
Yes
No
$CC(D,C) < CC_{max}$
Yes
C_m=D
m=m+1
No
m=M
k=k+1
Set of M codes
is generated
Seed selection process
C_2
intermediary
code
C_1
flip
L
delay corresponds to CC_{max}

Fig. 8

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- **D. FLACHS ; V. OEHLER ; S. BOUCHIRED ; E. E. CANALIS ; P. P. MULLER-REMMERS ; M. MARINELLI ; H. DE GAUJAC ; U. GAGEUR ; M. FALCONE.** Galileo Signal In Space Interface Control Document (SIS-ICD), Ver. 10.1. *Galileo Industries,* 28 September 2005 **[0045]**
- **S. WALLNER.** Consolidated Code Design (TN ID31. *Galileo Phase C0 / CN001,* 10 November 2004 **[0045]**
- **V. VARADAN ; H. LEUNG.** Design of Piecewise Maps for Chaotic Spread-Spectrum Communications Using Genetic Programming. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications,* vol. 49, 1543-15532002 **[0045]**
- **G. MAZZINI ; G. SETTI ; R. ROVATTI.** Chaotic complex spreading sequences for asynchronous DS-CDMA - Part I: System modeling and results. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications,* 1997, vol. 44, 937-947 **[0045]**
- **D. YOSHIOKA ; A. TSUNEDA ; T. INOUE.** On Transformation between Discretized Bernoulli and Tent Maps. *IEICE TRANS, Fundamentals,* 2005, vol. E88-A **[0045]**
- **R. ROVATTI ; G. SETTI ; G. MAZZINI.** Chaotic complex spreading sequences for asynchronous DS-CDMA - Part II: Some theoretical performance bounds. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications,* 1998, vol. 45, 496-506 **[0045]**
- **T. KOHDA ; A. TSUNEDA.** Statistics of chaotic binary sequences. *IEEE Trans. Inf. Theory,* 1997, vol. 43, 104-112 **[0045]**
- **A. L. BARANOVSKI ; F. DACHSELT ; W. R.** Nonlinear dynamics of PN-sequences. *Proceedings of the IST Mobile & Wireless Communications Summit,* 2005, 2005 **[0045]**
- **A. L. BARANOVSKI.** On Generation of Chaotic M-Sequences. *Proceedings of the International Symposium on Nonlinear Theory and its Applications (NOLTA),* 2005 **[0045]**
- **D. YOSHIOKA ; A. TSUNEDA ; T. INOUE.** An algorithm for the generation of maximal-period sequences based on one-dimensional chaos maps with finite bits. *IEICE Trans. Fundamentals,* June 2004, vol. E87-A (6), 1371-1376 **[0045]**
- **A. L. BARANOVSKI ; A. J. LAWRANCE.** Sensitive parameter dependence of autocorrelation function in piecewise linear maps. *International Journal of Bifurcations and Chaos,* 2006 **[0045]**
- **F. SOUALLE ; M. SOELLNER ; S. WALLNER ; J.-A. AVILA-RODRIGUEZ ; G. W. HEIN ; B. BARNES ; T. PRATT ; L. RIES ; J. WINKEL ; C. LEMENAGER.** Spreading Code Selection Criteria for the future GNSS Galileo. *Proceedings of the GNSS 2005,* 2005 **[0045]**