Simulation of Gold Code Sequences for Spread Spectrum Application

Anirudh Sharma, Tariq Anwar, D.K. Sharma

***Abstract*— Gold codes are a set of specific sequences found in systems employing spread spectrum or code-division multiple access (CDMA) techniques. Gold codes have cross-correlation properties necessary in a multi-user environment, where one code must be distinguished from several codes existing in the same spectrum. Secure message communication techniques, based on Spread Spectrum modulation (or message encryption scheme), use a spreading code (or an encryption key) for message security. The commonly used spreading codes or encryption keys are based on m-sequences and Gold codes. Gold sequences are preferred for many applications owing to their data hiding capabilities.**

***Index Terms*— Gold Code Sequences, M-Sequences, PN-Sequences Cross-Correlation, Auto-Correlation, Spread Spectrum**

I. INTRODUCTION

Spread Spectrum (SS) modulation is widely used in military, mobile and other modern communication systems, due to its inherent advantages, such as low probability of intercept and high anti-jamming capability. In a Spread Spectrum modulation the spectrum is deliberately spread over a wider bandwidth to realize improved process gain. There are five types of SS modulation techniques: (a) Frequency Hopping Spread Spectrum (FHSS), (b) Direct Sequence Spread Spectrum (DSSS), (c) Time Hopping Spread Spectrum (THSS), (d) FM Chirp and (e) Hybrid SS. Among all these techniques, the commonly used SS techniques are FHSS and DSSS. FHSS is usually used for implementing military communication and Bluetooth systems because of its better anti-jamming and low probability of intercept capabilities. DSSS finds application in satellite and mobile communication because of its better code division multiple access capability. In these systems the probability of intercept and capability of anti-jamming is determined by the length of code sequences used for spectrum expansion.

The desirable characteristics of CDMA codes include

(i) Availability of large number of codes.
(ii) Impulsive auto-correlation function.
(iii) Zero cross-correlation values.
(iv) Randomness
(v) Ease of generation
(vi) Low Peak to Average Power Ratio (PAPR) value
(vii) Support for variable data rates.

Hence, the choice of spreading codes in CDMA mobile systems is mainly governed by the above mentioned desirable characteristics. The commonly used PN-sequences are m-sequences, Gold sequences and Kasami sequences. In all these PN-sequences, the feedback tapings are fixed and therefore the sequences generated are limited. Gold codes are constructed using a pair of PN sequences (usually preferred pair).

In this research work we describe a methodology to generate a special class of periodic m-sequences called Gold sequences. Gold sequences yield the theoretically minimum cross-correlation values that one can possibly expect from periodic m-sequences. Implementation details and the application of Gold sequences to spread spectrum systems are also outlined. Section II of this paper provides a brief description of Gold Code, M-Sequences and its properties. In Section III the Gold Code Sequence generator is discussed. Finally in Section IV and V, Simulation Result and Conclusions are respectively provided.

II. BACKGROUND

A. Gold Code

A Gold code, also known as Gold sequence, is a type of binary sequence, use in telecommunication (CDMA) and satellite navigation (GPS). Gold codes are named after Robert Gold. Gold codes have bounded small cross-correlations within a set, which is useful when multiple devices are broadcasting in the same frequency range. A set of Gold code sequences consists of $2^n - 1$ sequences each one with a period of $2^n - 1$. A set of Gold codes can be generated with the following steps. Pick two maximum length sequences of the same length $2^n - 1$ such that their absolute cross-correlation is less than or equal to $2^{(n+2)/2}$, where n is the size of the LFSR used to generate the maximum length sequence. The set of the $2^n - 1$ exclusive-ors of the two sequences in their various phases (i.e. translated into all relative positions) is a set of Gold codes. The highest absolute cross-correlation in this set of codes is $2^{(n+2)/2} + 1$ for even n and $2^{(n+1)/2} + 1$ for odd n.

B. Gold Sequences

Gold sequences are constructed by EXOR-ing two *m*-sequences of the same length with each other. Thus, for a Gold sequence of length $m = 2^l-1$, one uses two LFSR, each of length 2^l-1. If the LSFRs are chosen appropriately, Gold sequences have better cross-correlation properties than

Manuscript received July 20, 2014.
Anirudh Sharma, M.Tech (E.C.E.) Student at A.F.S.E.T. Dhauj, Haryana (Affiliated to M.D.U.) and completed B.Tech (E.C.E.) from E.I.T.Faridabad (Affiliated to M.D.U.)
Tariq Anwar Asst. Prof. at A.F.S.E.T. (Dept. of E.C.E.), Faridabad, Haryana (Affiliated to M.D.U.)
D.K.Sharma H.O.D (E.E.) at R.I.E.T. (Affiliated to M.D.U.) Faridabad, Haryana. Retd Govt. Official Delhi Administration.

maximum length LSFR sequences. Gold (and Kasami) showed that for certain well-chosen *m*-sequences, the cross correlation only takes on three possible values, namely -1, -*t* or *t*-2. Two such sequences are called preferred sequences. Here *t* depends solely on the length of the LFSR used. In fact, for a LFSR with *l* memory elements,

if l is odd, $t = 2^{(l+1)/2} + 1$, and

if l is even, $t = 2^{(l+2)/2} + 1$.

C. M-Sequences

A maximum length sequence (MLS) is a type of pseudorandom binary sequence. They are bit sequences generated using maximal linear feedback shift registers and are so called because they are periodic and reproduce every binary sequence that can be represented by the shift registers (i.e., for length-*m* registers they produce a sequence of length $2^m - 1$). An MLS is also sometimes called an n-sequence or an m-sequence. MLSs are spectrally flat, with the exception of a near-zero DC term. These sequences may be represented as coefficients of irreducible polynomials in a polynomial ring over Z/2Z. Practical applications for MLS include measuring impulse responses (e.g., of room reverberation). They are also used as a basis for deriving pseudo-random sequences in digital communication systems that employ direct sequence spread spectrum and frequency-hopping spread spectrum transmission systems, and in the efficient design of some f-MRI experiments.

The three basic properties, which are applied to test the randomness appearance, of m-sequences are as under:

(a) *Balance Property*: In each period of the sequence, the number of 1s must differ from the number of 0s at the most by one digit, i.e., No. of 1s=2N/2 and No of 0s= (2N/2) -1.

(b) *Run property*: A run is defined as sequence of a consecutively single type of bits. Among the runs of 1s and 0s, in each period, one half of the runs are of length 1, one-fourth are of length 2, one-eight are of length 3and so on.

(c)*Correlation property*: If a period of sequence is compared term by term with any cyclic shift to itself, it is best if the number of agreements differ from the number of disagreements by not more than one count.

Mathematically, the correlation between two sequences p(k) and q(k), with the delay m, is expressed as

$$R(m)= \sum_{k=0}^{N-1} p(k)q(k+m) \qquad \text{…………(1)}$$

D. PN – Sequences

PN sequence codes are used in reverse link. These codes differentiate various mobile subscribers at base station as they are unique to all mobile subscribers. There are access and traffic channels used from mobile to Base station in CDMA. PN sequence is a sequence of binary numbers which appears to be random but it is periodic in nature.

PN sequence properties:

(i) Difference of number of 0's and 1's always be equal to 1 in any PN sequence.

(ii) Correlation value of any two PN codes is determined by following equation.
(No. of like bits- No. of unlike bits) / (Total no. of bits)
Consider PN sequence of pattern 1110010, If both the patterns are same without any delay then correlation value is 7-0/7, leads to 1 i.e. maximum value. For a bit change in this PN codes leads to bit pattern equal to 0111001 and it will give correlation value of 3-4/7 i.e. -1/7. Hence it is easy to get back the data of the Mobile/Base station if the PN code is known.

(iii) For N bit code, there will be N ones or zero runs. 1/2 of run will be of length 1, 1/4 of run will be of length 2, 1/8 of run will be of length 3 and so on.

E. Peak Auto Correlation

Auto-correlation is a measure of the similarity between a code *C(t)* and its time shifted replica. Mathematically, it is defined as:

$$\psi_a(\tau) = \int_{-\infty}^{\infty} c(t) * c(t-\tau)\, dt \qquad \text{……….(2)}$$

Ideally, this auto-correlation function (ACF) should be impulsive i.e. peak value at zero time shift and zero values at all other time-shifts (i.e. side-lobes). This is required at the receiver side for proper synchronization and to distinguish the desired user from other users producing MAI. Thus, spreading codes should be carefully chosen to ensure highest possible peak value of autocorrelation function at zero shift and lower side-lobes peaks at non-zero shifts. The larger the gap between main ACF peak (zero shift) and side-lobes peaks, the better is the performance of CDMA mobile system.

F. Peak Cross-Correlation

Like Peak Auto-Correlation, Cross-Correlation is also a crucial parameter which dictates the choice of suitable spreading codes for wireless CDMA systems. Each user in CDMA based system is being assigned a separate and unique code sequence. Cross-correlation is the measure of similarity between two different code sequences *C1(t)* and *C2(t)*. Mathematically, it is defined as:

$$\psi_c(\tau) = \int_{-\infty}^{\infty} c_1(t) * c_2(t-\tau)\, dt \qquad \text{…………..(3)}$$

Cross-correlation function (CCF) in-fact indicates the correlation between the desired code sequence and the undesired ones at the receiver. Therefore, in order to eliminate the effect of multiple access interference at the receiver, the cross-correlation value must be zero at all time shifts. The codes for which y (t) = 0 *c* i.e. zero cross-correlation value at all time shifts, are known as orthogonal codes. Therefore, it is desirable to have a code dictionary consisting of spreading codes which possess both impulsive ACF and all zero CCF characteristics. But unfortunately, no such code family exists which possess both characteristics simultaneously. Therefore, a communication engineer has to compromise with maximum possible difference between ACF peak and CCF peak of the codes selected.

III. GOLD SEQUENCE GENERATOR

If an m-sequence uses an n-bit shift register (with certain fixed feedback tapings) to generate a code of length of (2n-1) bits, it can be shown that the feedback tapings can be found if 2n bits of the code word are known. Thus jamming in such situations becomes easy. Therefore choosing a longer code sequence enables good anti-jamming capability. One way to overcome this problem is to use Gold code generators, where larger code sequences are available with better correlation properties. These sequences are generated by combining the preferred pair of m-sequences driven by the same clock as shown in figure.

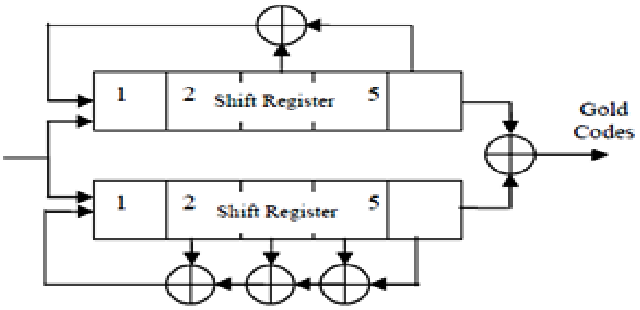

Fig.1 : Gold Code Sequence generator using shift register

Both the m-sequences use the same clock and are of equal length, the Gold code sequences generated are of the same length (N = 2n-1). By giving one of the codes a delay with respect to other code, different sequences can be generated. The number of sequences that can be obtained is S_n= 2n-1, where n is the size (length) of shift register. Thus larger number of sequences can be generated using the same shift registers. With a proper choice of m-sequence pairs, a good cross-correlation can be maintained between all created Gold Codes. In conventional Gold code sequences the feedback logic of LFSRs is fixed, and therefore the resultant sequences can be decoded by an eavesdropper or a jammer. Simplicity of the circuits makes the technique attractive for low cost CDMA applications.

A. Gold Sequence Generator using two PN Sequence Generator

Gold sequences have the property that the cross-correlation between any two, or between shifted versions of them, takes on one of three values: -t(n), -1, or t(n) - 2, where

$$t(n) = \begin{cases} 1+2^{(n+1)/2} & n \text{ even} \\ 1+2^{(n+2)/2} & n \text{ odd} \end{cases} \qquad \ldots\ldots\ldots\ldots(4)$$

The Gold Sequence Generator block uses two PN Sequence Generator blocks to generate the preferred pair of sequences, and then XORs these sequences to produce the output sequence. In this paper we simulated Gold Code using MatLab Software. With the help of two preferred M-Sequences(PN Sequences) we generated Gold Code. Gold Sequence Generator was been developed using two PN Sequence Generator on MatLab Simulink as shown in the figure

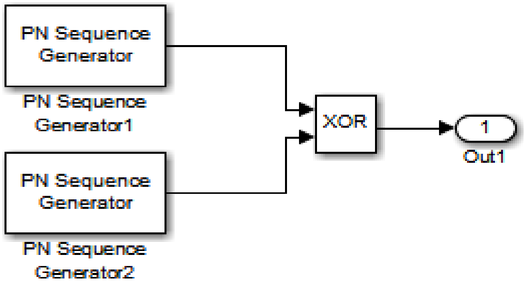

Fig.2 : MatLab Simulink Diagram for Gold Sequence Generator

After successful completion of MatLab simulink we set the parameters of Source Block Parameters of Gold Sequence Generator.
The following table provides a list of preferred pairs used for Gold sequence.

Table 1 : List of Preferred Pairs

n	N	Preferred Polynomial [1]	Preferred Polynomial [2]
5	31	[5 2 0]	[5 4 3 2 0]
6	63	[6 1 0]	[6 5 2 1 0]
7	127	[7 3 0]	[7 3 2 1 0]
9	511	[9 4 0]	[9 6 4 3 0]
10	1023	[10 3 0]	[10 8 3 2 0]
11	2047	[11 2 0]	[11 8 5 2 0]

IV. SIMULATION RESULTS

The MatLab Code for Gold Code Sequence was developed and run on MatLab Software R2007b and the following simulation results were obtained on successful debug of code. The Auto Correlation and Cross Correlation values of the code generated are plotted for the Length of Code 31.

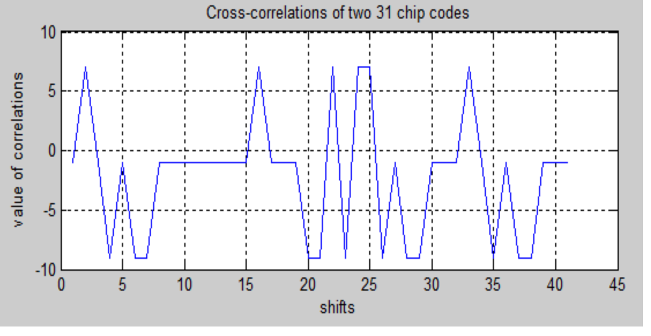

Fig.3: Cross-Correlation of two 31 Chip Codes

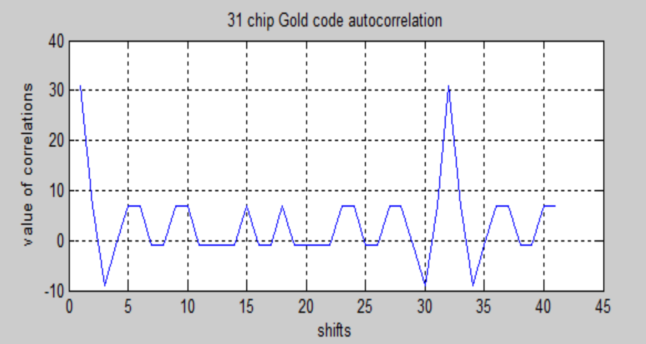

Fig.4: Auto-Correlation of two 31 Chip Gold Codes

The following table shows the standard values of ACF and CCF characteristics of Gold Codes.

Table 2 : ACF and CCF characteristics of Gold Codes

Length of Code (N)	**Code Family Size (M)**	**ACF Values**	**CCF Values**	**Peak Sidelobe ACF (dB)**	**Peak Sidelobe CCF (dB)**	**% of '-1' CCF Values**
7	9	-5, -1, 3, 7	-5, -1, 3	-7.35	-7.35	53 %
15	17	-5, -1, 3, 7,15	-5, -1, 3, 7	-6.62	-6.62	39.4 %
31	33	-9, -1, 7, 31	-9, -1, 7	-12.92	-12.92	50.8 %
63	65	-17, -1, 15, 63	-17, -1, 15	-12.47	-12.47	75.2 %
127	129	-17, -1, 15, 127	-17, -1, 15	-18.55	-18.55	50.2 %
255	257	-33, -17, -1, 15, 31, 63, 255	-33, -17, -1, 15, 31, 63, 255	-12.14	-12.14	41.2 %

After the successful debug of Matlab code for Gold Code Sequences and setting the parameters of Source Block Parameters of Gold Sequence Generator in MatLab simulink the observed values for ACF and CCF of Gold Code are :

(i) ACF value for Gold Code : 30
(ii) CCF value for Gold Code : - 7 , -1 , 9

V. CONCLUSION

While designing a CDMA system, the proper choice of spreading codes is of prime importance because the performance of a CDMA based wireless system is mainly governed by the characteristics of spreading sequences.
Ideally, a spreading code should possess both impulsive auto-correlation (zero sidelobe levels) and all zero cross-correlation characteristics. But unfortunately, no such code family exists which possess both correlation characteristics simultaneously. Therefore, in order to have tolerable MAI, one has to compromise with maximum possible difference between ACF (autocorrelation function) peak and CCF (cross-correlation function) peak of the codes selected.
In this paper an efficient and practical method was used with its corresponding Matlab implementation. By implementing this method and through the use of our Matlab-coded programs we can find and generate preferred M-Sequences and therefore construct and simulate Gold Code sequences which can eventually be used for designing a CDMA system.

ACKNOWLEDGEMENT

We express our sincere thanks to all our friends who have patiently extended all sorts of help for accomplishing this undertaking. Finally we extend our gratefulness to one and all who are directly or indirectly involved in the successful completion of this paper.

REFERENCES

[1] Comparative Analysis Of Peak Correlation Characteristics Of Non-Orthogonal Spreading Codes For Wireless Systems Dr. Deepak Kedia Department Of Electronics & Communication Engineering, G.J. University Of Science & Technology, Hisar, Haryana, India, Kedia_02in@Yahoo.Com

[2] Novel Circuit for the Generation of Gold Sequences for Increased Message Security by Faroze Ahmad and G. Mohiuddin Bhat E&C Engineering, Islamic University of Science and Technology (IUST), Awantipora, J&K, India . 2GIAN Cell (J&K), Advisor EDC and Coordinator TUC, University of Kashmir, India

[3] On Properties of PN Sequences Generated by LFSR – a Generalized Study and Simulation Modeling by Afaq Ahmad*, Sayyid Samir Al-Busaidi and Mufeed Juma Al-Musharafi, Department of Electrical and Computer Engineering, College of Engineering, Sultan Qaboos University

[4] Analysis and Simulation of Pseudo Ranging Noise codes for Geo-Stationary Satellites and its Doppler Effect by P.N.Ravichandran, Sunil Kulkarni, H.S.Vasudevamurthy, M.Vanitha Digital Systems Group ISRO Satellite Centre , Bangalore, India

[5] Generation Of Gold-Sequences With Applications To Spread Spectrum Systems by F. Rodríguez Henríquez Member, IEEE, N. Cruz Cortés , Member, Ieee, J.M. Rocha-Pérez (2) Member, Ieee. F. Amaro Sánchez

[6] Analysis of Different Pseudo Noise Sequence by Alka Sawlikar, Manisha Sharma ISSN 2249-6343 International Journal of Computer Technology and Electronics Engineering(IJCTEE) Volume 1 , Issue 2

[7] The Implementation of a Multiplexing Gold Code Generator using a Xilinx Logic Cell Array by Steven J. Merrifield and John C. Devlin School of Electronic Engineering, La Trobe University, Bundoora, Victoria, Australia,

[8] Research of Pseudo Random Noise Code and New Code Construction by Ruizhu He National Astronomical Observatories, CAS University of Chinese Academy of Sciences Beijing, China heruizhu11@mail.ucas.ac.cn Junxia Cui National Astronomical Observatories, CAS Beijing, China cuijx@nao.cas.cn

Anirudh Sharma, M.Tech (E.C.E.) Student at A.F.S.E.T. Dhauj, Haryana (Affiliated to M.D.U.) and completed B.Tech (E.C.E.) from E.I.T.Faridabad (Affiliated to M.D.U.)

Tariq Anwar Asst. Prof. at A.F.S.E.T. (Dept. of E.C.E.), Faridabad, Haryana (Affiliated to M.D.U.)

D.K.Sharma H.O.D (E.E.) at R.I.E.T. (Affiliated to M.D.U.) Faridabad, Haryana. Retd Govt. Official Delhi Administration.