Perfect Periodic Autocorrelation Codes Derived From M-Sequences

João S. Pereira [(1)] and Henrique J. A. da Silva [(2)]

(1) Instituto de Telecomunicações, Universidade de Coimbra, Polo II, P-3030-290 Coimbra, Portugal and DEI/ESTG/Campus2 do Instituto Politécnico de Leiria, Alto do Vieiro, Morro do Lena, P-2401-951 Leiria, Portugal, Phone +351-244820300, Fax. +351-244820310, e-mail: jpereira@estg.ipleiria.pt.

(2) Instituto de Telecomunicações and Departamento de Engenharia Electrotécnica e de Computadores, Faculdade de Ciências e Tecnologia, Universidade de Coimbra, Polo II, P-3030-290 Coimbra, Portugal, e-mail: hjas@ci.uc.pt.

Abstract — **A method to generate a large number of M-ary Perfect Periodic Autocorrelation (PPAC) codes of length *N*, with good correlation properties, is presented. *N*+1 perfect sequences are obtained if an inverse discrete Fourier transform (IDFT) is applied to a specific subset of *N*+1 bipolar sequences derived from maximal-length sequences. This set of perfect sequences has a maximum absolute value of periodic cross-correlation equal to the square root of *N*+1. Moreover, this absolute value is equal to 1 when all perfect sequences are in-phase.**

I. Introduction

Ideally, Code Division Multiple Access (CDMA) sequences should have a perfect periodic autocorrelation function (PACF) [1]–[3] when strong multi-path interference exists. In other words, the perfect PACF should be equal to the $\delta(n)$ unit impulse function. However, since such bipolar sequences with perfect PACF are not known (except for x = (1; 1; 1;-1), which is a periodic sequence (discrete-time) of length four [3], [4]), it is desirable to find new sequences. Alternative solutions may be found with complex periodic sequences defined by some authors as Small or Large Alphabet Polyphase sequences [1], [5]–[7], Unimodular Perfect sequences [8], Phase Shift Pulse Codes [9], Perfect Root-of-Unity sequences [10], Bent function sequences [11], or simply as Perfect sequences [12], [13]. Perfect tetra-phase sequences (small alphabet) with perfect PACF exist for lengths $N=2$, 4, 8, and 16 (Milewski and Frank sequences). Many other sequences with good PACF may be found if a mathematical transformation is used [2], [3].

Any codes with a nearly perfect PACF and low maximum absolute value of periodic cross-correlation (MaxCC) can be applied in asynchronous CDMA communication systems, for fast start-up equalization, channel estimation, synchronization, or other applications impaired by strong multi-path interference.

A variety of perfect sequences has been proposed in the literature [1]–[14]. The lower bound of MaxCC seems to be a constant and equals $\sqrt{N}$ [7], [15], [16]. It is worth noting that, to the best our knowledge, there are no perfect sequences with zero cross-correlation for any time-shift.

We present in section II a mathematical property that provides a way to find large sets of perfect sequences with low MaxCC. Despite their non constant envelope, these new complex perfect sequences may be transformed into two real M-ary Perfect Periodic Autocorrelation codes (M-ary PPAC codes with a nearly perfect periodic autocorrelation function) which may be used in CDMA systems with an adequate modulation technique. Simulation results are presented in section III for synchronous and asynchronous CDMA systems. The main conclusions are gathered in section IV.

II. Perfect Sequences

Let $x(n)$, with $n=0,1,2...,N-1$, be one of the N points of a periodic sequence x. We define its discrete Fourier transform (DFT) [17] as:

$$DFT\left[x(n)\right]=X(k)=\sum_{n=0}^{N-1}x(n)W_N^{kn}\ . \qquad (1)$$

The inverse discrete Fourier transform (IDFT) [17] is given by:

$$IDFT\left[X(k)\right]=x(n)=\frac{1}{N}\sum_{k=0}^{N-1}X(k)W_N^{-kn}\ . \qquad (2)$$

For convenience of notation, W_N is defined as $W_N=\exp(-j2\pi/N)$, where $j=\sqrt{-1}$. We should also remember that the DFT and the IDFT are linear and invertible transforms.

Using the DFT and IDFT transforms, the periodic cross-correlation may be defined as [15], [17]:

$$R_{xy}(n)=\sum_{k=0}^{N-1}x(k)\,y^*\left[\mathrm{mod}(k+n,N)\right]=IDFT\left(XY^*\right), \qquad (3)$$

where n is an integer, the superscript * stands for the complex conjugate, and mod(*a*,*b*) is the remainder of *a* divided by *b*. A complex value $x(n)$ is equal to $x\left[\mathrm{mod}(n,N)\right]$ when *x* is a periodic sequence with period *N*.

When *x* = *y*, (3) is defined as the periodic autocorrelation function. A sequence *x* is called a perfect sequence if it has an ideal periodic autocorrelation function:

$$R_{xx}(n)=N\delta(n)=\begin{cases}N, & \mathrm{mod}(n,N)=0\\ 0, & \mathrm{mod}(n,N)\neq 0\end{cases}\ . \qquad (4)$$

As it is well known, any constant amplitude sequence in the frequency domain corresponds to a perfect sequence in the time domain. In other words, we can say that the sequence:

$$x_p(n)=\sqrt{N}\times IDFT\left[x(n)\right], \qquad (5)$$

for $0\le n\le N-1$, where n is an integer, is a perfect sequence if $\left|x(n)\right|^2=1$. Using (5) we can generate perfect sequences (with non constant envelope) of any length *N*, when $\left|x(n)\right|$ is constant for all *N* values. However, what we want is to find perfect sequences with good correlation properties. The following property, defined by (12), will be useful for finding *N+1* perfect sequences with a low MaxCC.

Let T^k denote the operator which shifts complex sequences cyclically to the left by *k* places, i.e.:

$$T^k x = \left[x(k), x(k+1), \ldots x(N-1), x(0), x(1), \ldots, x(k-1)\right]. \quad (6)$$

We will consider $T^0 x = x$ and use $\oplus$ to denote modulo 2 addition (i.e. the EXCLUSIVE-OR operation). The sequences u and v are maximal-length sequences (m-sequences) with length N. It is important to remember that, for an m-sequence *v*, there is an unique integer *k,* distinct from both integers *r* and *s,* with $0 \le r, s, k \le N-1$, that verifies:

$$T^r v \oplus T^s v = T^k v. \quad (7)$$

Since it is sometimes necessary to distinguish between a $\{0,1\}$-valued binary sequence and the corresponding $\{+1,-1\}$-valued binary sequence, we introduce the function $\chi(.)$ defined by $\chi(0) = +1$ and $\chi(1) = -1$. If x denotes an arbitrary $\{0,1\}$-valued sequence, then $\chi(x)$ denotes the corresponding $\{+1,-1\}$-valued sequence (called bipolar sequence), where the *i*th element of $\chi(x)$ is just $\chi\left[x(i)\right]$. It should be noticed that:

$$\chi\left(u \oplus T^k v\right) = \chi(u)\chi\left(T^k v\right). \quad (8)$$

Other useful properties of $\{+1,-1\}$-valued m-sequences are [15]:

$$R_{\chi(v)\chi(v)}(n) = (N+1)\delta(n) - 1 = \begin{cases} N, & \operatorname{mod}(n,N)=0 \\ -1, & \operatorname{mod}(n,N)\neq 0 \end{cases} \quad (9)$$

and

$$\left|DFT\left[\chi(v)\right]\right|^2 = DFT\left[R_{\chi(v)\chi(v)}\right] = (N+1) - N\delta(n). \quad (10)$$

We should also remember that m-sequences are real sequences, and that it is possible to find the IDFT of any sequence *X* through a DFT transformation:

$$IDFT\left[X(n)\right] = \frac{1}{N}\left\{DFT\left[X^*(n)\right]\right\}^*,\ 0 \le n \le N-1. \quad (11)$$

Property: If *u* and *v* are m-sequences of length *N*, the IDFT of the $\{+1,-1\}$-valued binary sequences of the set $\varphi(u,v) \triangleq \left\{u, u \oplus v, u \oplus Tv, u \oplus T^2 v, \ldots, u \oplus T^{N-1} v\right\}$ is:

$$\Gamma(u,v) \triangleq \left\{\sqrt{N} \times IDFT\left[\chi(u)\right], \sqrt{N} \times IDFT\left[\chi\left(u \oplus T^0 v\right)\right],\right.$$
$$\left.\sqrt{N} \times IDFT\left[\chi\left(u \oplus T^1 v\right)\right], \ldots, \sqrt{N} \times IDFT\left[\chi\left(u \oplus T^{N-1} v\right)\right]\right\} \quad (12)$$

This set $\Gamma(u,v)$ has $N+1$ perfect sequences (of length N) and the maximum absolute value of its periodic cross-correlation is $\sqrt{N+1}$.

Using (5), we easily confirm that all sequences of the set $\Gamma(u,v)$ verify the condition $\left|\chi(.)\right|^2 = 1$ for all *N* elements, and generate *N+1* perfect sequences with the same length *N* when they are transformed by an IDFT.

The absolute value of periodic cross-correlation of any two distinct perfect sequences $y = \sqrt{N} \times IDFT\left[\chi\left(u \oplus T^r v\right)\right]$ and $z = \sqrt{N} \times IDFT\left[\chi\left(u \oplus T^s v\right)\right]$, when $r \neq s$, where *r* and *s* are integers, is given by:

$$\left|R_{yz}(n)\right| = \left|N \times IDFT\left\{\chi(u)\chi\left(T^r v\right)\left[\chi(u)\chi\left(T^s v\right)\right]^*\right\}\right|$$
$$= \left|N \times IDFT\left[\chi\left(T^k v\right)\right]\right|. \quad (13)$$

We have used some useful properties, namely $Y = DFT[y] = \sqrt{N} \times \chi(u)\chi\left(T^r v\right)$, $Z = \sqrt{N} \times \chi(u)\chi\left(T^s v\right)$, (7), (8), and $\chi(u)\left[\chi(u)\right]^* = 1$ (for all elements). Now, if we only want to find the MaxCC= $\max\left\{\left|R_{yz}\right|\right\}$, then the operator T^k can be dropped and:

$$\max\left\{\left|R_{yz}\right|\right\} = \max\left\{\left|N \times IDFT\left[\chi(v)\right]\right|\right\}$$
$$= \max\left[\sqrt{N+1-N\delta(n)}\right]$$
$$= \sqrt{N+1} \quad (14)$$

For a complete verification, we need to calculate the MaxCC of $\sqrt{N} \times IDFT\left[\chi(u)\right]$ with all other sequences of $\Gamma(u,v)$, which is also:

$$\max\left\{\left|N \times IDFT\left\{\chi(u)\left[\chi(u)\chi\left(T^s v\right)\right]^*\right\}\right|\right\} = \sqrt{N+1}.$$

Therefore, we can say that the MaxCC for the *N+1* perfect sequences is equal to $\sqrt{N+1}$. Besides, we can also say that this value occurs $N-1$ times and the value $\sqrt{N+1-N\delta(0)} = 1$ occurs one time (in-phase value). Result (14) is valid for any EXCLUSIVE-OR combinations of two m-sequences *u* and *v* of the same length *N.* In the next section we present simulation results obtained with some Gold sequences, which use preferred pairs of m-sequences.

III. M-ARY PPAC CODES

After some simulation tests with subsets of bipolar sequences derived from preferred pairs of m-sequences, we have concluded that the best set of perfect sequences (with length *N*) is found when the IDFT is applied to a subset of sequences of the bipolar Gold set, or alternatively to a subset of bipolar Time Inverted Gold (TIG) sequences [18], [19]. These conclusions have confirmed our property. The m-sequence v of the Gold Set:

$$G(u,v) = \left\{u, v, u \oplus v, u \oplus Tv, u \oplus T^2 v, \ldots, u \oplus T^{N-1} v\right\}$$

must be discarded before the IDFT application, because it is not possible to verify property (7) with two different m-sequences u and v. That is:

$$\max\left\{\left|N \times IDFT\left\{\chi(u)\left[\chi(v)\right]^*\right\}\right|\right\} \neq \sqrt{N+1}.$$

We should remember that, in (12), the m-sequence *v* belongs to the Gold set $G(u,v)$, but not to the $\varphi(u,v)$ set. Notice that our property is also valid for non preferred pairs of m-sequences. Our simulations confirmed that the MaxCC is equal to $\sqrt{N+1}$ (see Normalized MaxCC for "PPAC [Gold seq. without the m-seq. *v*]" in Table I). For increased confidence on the simulation results, our tests have been performed with different lengths *N* (31, 63, 127 and 511).

Table I

Normalized absolute maximum periodic cross-correlation evaluated for Gold sets and PPAC sets. The PPAC sequences were generated with subsets of Gold sequences and subsets of TIG sequences [18], for a length *N* equal to 63. *Q* is the number of sequences in each set.

Sequences	Q	Normalized MaxCC	$\sqrt{N}\,/\,N$
Gold seq.	65	0.2698	0.1260
PPAC [Gold seq.]	65	0.3436	0.1260
PPAC [Gold seq. without the m-seq. *v*]	64	0.1270	0.1260
PPAC [seq. of a TIG subset]	126	0.2540	0.1260
PPAC [seq. of a TIG subset]	256	0.4921	0.1260

Important conclusions can be drawn from Table I. For example, it is possible to find $N+1$ PPAC sequences with a MaxCC value 53% smaller than for Gold sequences. When $N=63$, it is possible to find $Q=126$ different PPAC sequences with a value of MaxCC 6% smaller than for Gold sequences with the same length. For this reason, the TIG set has been considered as an alternative solution to achieve bigger sets of PPAC sequences with a low MaxCC value. The last column of Table I, $\sqrt{N}/N$, represents the known lower bound (normalized) for the perfect sequences of Chu [7] (large alphabet polyphase sequences). Notice that the known small alphabet polyphase sequences [2] have a higher MaxCC value.

In order to enable a simple digital implementation, these PPAC complex sequences (such as the well known perfect sequences of Chu [7] or Zadoff–Chu sequences [13]) may be linearly quantized in a small number M of different phases, or alternatively in a small number M of amplitude values, in order to obtain small alphabet sequences. We chose to quantize the amplitude of our perfect sequences, thereby creating dual real M-ary PPAC codes (real and imaginary parts of the complex M-ary PPAC code) that should be almost perfect. Therefore, the real and imaginary parts of the M-ary PPAC complex codes should have M discrete amplitude values (such as the output of an analog-to-digital converter with a resolution of $n=\log_2 M$ bits). This linear amplitude quantization of the PPAC complex codes should keep all good mathematical properties if *M* is high enough. The influence of the number M of discrete amplitude values, when $N=127$ and $Q=100$, is shown in Fig. 1.

CDMA simulations with Gold codes [20] and M-ary PPAC codes have been made assuming multiple users. The performance results obtained are presented in Fig. 2 and 3. All simultaneously transmitted codes are received synchronously or asynchronously with a uniformly distributed amplitude variation around the amplitude of the selected code. Therefore, all codes have the same average power as the code selected randomly and used to find the average Bit Error Rate (BER). The *M*-ary quadrature amplitude modulation (*M*-ary QAM) has been selected. This modulation has been used to carry the real and imaginary parts of complex codes. A binary phase-shift keying (BPSK) modulation has been used to carry the bipolar Gold and orthogonal Gold codes.

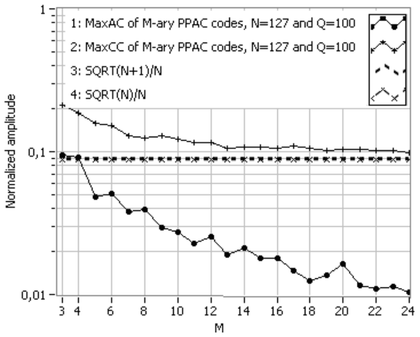

Fig. 1. Normalized maximum out-of-phase periodic autocorrelation, MaxAC, and maximum periodic cross-correlation, MaxCC, for M-ary PPAC codes.

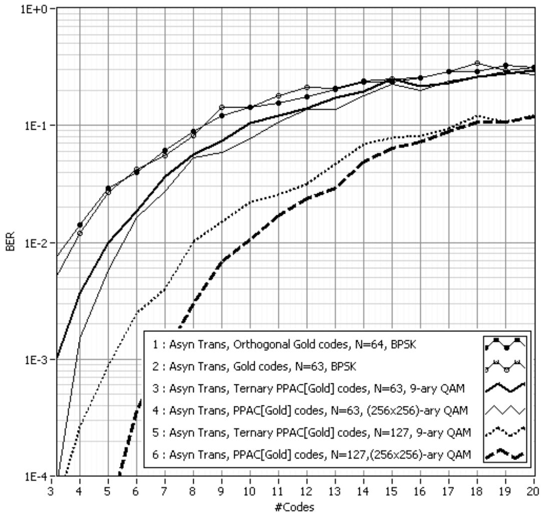

Fig. 2. Bit Error Rate *versus* number of simultaneous users (#Codes), for different sets of codes, used in asynchronous CDMA transmission scenarios.

Figs. 2 and 3 show the Bit Error Rate *versus* number of simultaneous users (#Codes) in synchronous and asynchronous CDMA transmission scenarios, respectively. The correct code detection has been made asynchronously for all different codes. More precisely, the maximum correlation value obtained corresponds to the correct selected code.

It should be noted that our set $\Gamma(u,v)$ has two additional perfect sequences, compared to the sets of Chu or Zadoff-Chu, and it seems to be more adequate for both synchronous and asynchronous CDMA transmission systems. Other simulation results have been obtained which are not included in Figs. 2 and 3. Specifically, good results were also obtained with the PPAC codes (derived from some Gold codes) impaired by strong multi-path interference.

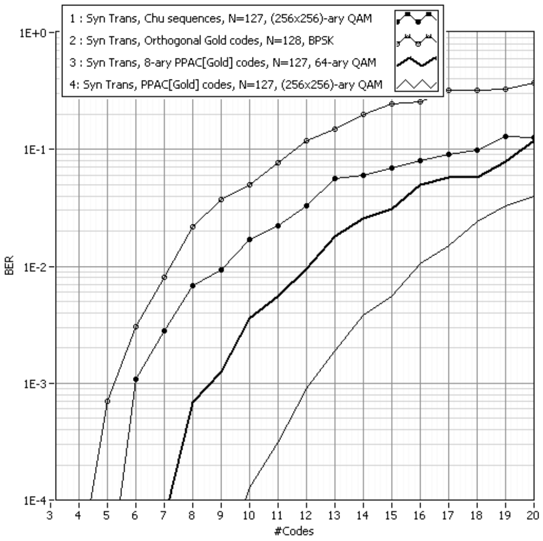

Fig. 3. Bit Error Rate *versus* number of simultaneous users (#Codes), for different sets of codes used in synchronous CDMA transmission scenarios.

IV. CONCLUSIONS

A method to obtain large sets of sequences with perfect periodic autocorrelation functions and good cross-correlation properties was presented. These perfect sequences can be obtained simply by applying an inverse discrete Fourier transform to large sets of complex sequences x with $|x|$ constant for all values of N. It was shown that, when the sequences x belong to a subset of bipolar sequences derived from m-sequences, it is possible to generate $N+1$ perfect sequences with the same length N that have a maximum absolute periodic cross-correlation value given by $\sqrt{N+1}$.

By simulation, we have confirmed all properties and found that the perfect sequences derived from bipolar m-sequences have a low maximum absolute value of periodic cross-correlation. Therefore, the PPAC sequences may be used in a synchronous or asynchronous CDMA transmission system.

In order to enable their digital implementation, the new perfect sequences have been converted into M-ary PPAC codes and tested in synchronous and asynchronous transmission scenarios. It was found that the PPAC codes can be more versatile than the well known Gold codes, orthogonal Gold codes, and perfect sequences of Chu.

REFERENCES

[1] H. Dieter Lüke, Hans D. Schotten, and Hafez Hadinejad-Mahram, “Binary and Quadriphase Sequences With Optimal Autocorrelation Properties: A Survey,” *IEEE Trans. Inf. Theory*, vol. 49, no. 12, December 2003.

[2] P. Fan and M. Darnell, *Sequence Design for Communications Applications*, New York: Wiley, 1996.

[3] H. D. Lüke, *Korrelationssignale* (in German), Springer-Verlag, Berlin, Germany, 1992.

[4] B. Schmidt, *Cyclotomic Integers and Finite Geometry*, J. Amer. Math. Soc., 1999, vol. 12, pp. 929–952.

[5] S. Park, I. Song, S. Yoon and J. Lee, “A New Polyphase Sequence With Perfect Even and Good Odd Cross-Correlation Functions for DS/CDMA Systems,” *IEEE Trans. Veh. Technol.*, vol. 51, no. 5, September 2002.

[6] Branislav M. Popovic, “Generalized Chirp-Like Polyphase Sequences with Optimum Correlation Properties,” *IEEE Trans. Inf. Theory*, vol. 38, no. 4, July 1992.

[7] P.Z. Fan, M. Darnell and B. Honary, “Crosscorrelations of Frank sequences and Chu sequences,” *Electronics Letters*, vol. 30, no. 6, March 1994.

[8] E. M. Gabidulin, V. V. Shorin, “New Families of Unimodular Perfect Sequences of Prime Length Based on Gaussian Periods,” *IEEE International Symposium Information Theory*, Lausanne, Switzerland, July 2002.

[9] R. C. Heimiller, “Phase Shift Pulse Codes with Good Periodic Correlation Properties,” *IRE Trans. Inf. Theory*, October 1961.

[10] W. H. Mow, “A New Unified Construction of Perfect Root-of-Unity Sequences,” *Proc. Int. Symp. Spread Spectrum Techniques and Its Applications (ISSSTA’96)*, Mainz, Germany, September 1996, pp. 955–959.

[11] H. Chung and P. V. Kumar, “A New General Construction for Generalized Bent Functions,” *IEEE Trans. Inf. Theory*, vol. 35, no. 1, January 1989.

[12] C. P. Li and W. C. Huang, “An Array for Constructing Perfect Sequences and Its Applications in OFDM-CDMA Systems,” *IEEE GLOBECOM 2006 proceedings*.

[13] C. P. Li and W. C. Huang, “A Constructive Representation for the Fourier Dual of the Zadoff–Chu Sequences,” *IEEE Trans. Inf. Theory*, vol. 53, no. 11, November 2007.

[14] N. Suehiro, “Pseudo-polyphase orthogonal sequence sets with good cross-correlation property,” in *Lecture Notes in Computer Science, Springer Berlin / Heidelberg, Book: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, 1991.

[15] D. Sarwate, M. Pursley, “Crosscorrelation Properties of Pseudorandom and Related Sequences,” in *Proceedings of the IEEE*, May 1980, vol. 68, no. 5.

[16] L. R. Welch, “Lower Bounds on the Maximum Cross Correlation of Signals,” *IEEE Trans. Inf. Theory*, vol. IT-20, pp. 397-399, 1974.

[17] Alan V. Oppenheim, Ronald W. Schafer, *Digital Signal Processing*, Prentice-Hall, 1975.

[18] J. Pereira and H. da Silva. (2001, December). A Larger Subset of Pseudo-Orthogonal Spreading Codes for WCDMA. *Techonline.* [online]. Available: http://www.techonline.com/community/home/14978, or http://www.techonline.com/article/192200622;jsessionid=MBXRFWYTQ42JYQSNDLPSKHSCJUNN2JVN.

[19] Gold, “Optimal binary sequences for spread spectrum multiplexing,” *IEEE Transactions on Information Theory,* p. 619–621, October 1967.

[20] A. N. Akansu, R. Poluri, “Walsh-Like Nonlinear Phase Orthogonal Codes for Direct Sequence CDMA Communications,” *IEEE Trans. Signal Process.* vol. 55, no. 7, pp. 3800-3806, July 2007.