A wavelet transform approach for the design of orthogonal sequences

by

Todor Cooklev

Department of Electrical and Computer Engineering
University of Toronto

1996

Report on Contract U6800-6-2438
Scientific authority: Dr. Michael Sablatash
Manager, Communications Signal Processing Division, CRC, Ottawa: Dr. John Lodge

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. The Communications Research Centre has made every attempt to supply trademark information about manufacturers and their products mentioned in this report. A list of the trademark designations and their owners appears at the bottom of this page.

Trademark notice
MATLAB^R is a registered trademark of The MathWorks Incorporated.
PostScript^{TM} is a trademark of Adobe Systems Incorporated.
Unix^{TM} is a trademark of AT& T.

Contents

Chapter 1

Introduction

There is a wealth of literature on the design of pseudo-random (or pseudo-noise) sequences for wireless communications with different properties of their autocorrelation and cross-correlation functions (ACF and CCF).

The theory of filter banks was developed completely independently and it is widely accepted that it dates back to 1976 [6]. The first digital filter bank was designed by Croisier, Esteban and Galand in 1976 and the first perfect-reconstruction filter bank was designed by three research groups independently around 1984 (for a collection of references see [6]). The main application of filter banks is in data compression. Subband coding of audio, images and video, as the method is called, is one of the competing technologies for data compression with a number of theoretical and practical advantages (including relationship with multiresolution analysis, interoperability and fast computation) . The discovery of I. Daubechies that orthogonal filter banks provide orthogonal bases for the Hilbert space of square-summable sequences stimulated a tremendous research activity in the area. Furthermore I. Daubechies showed that provided the filters satisfy constraints additional to PR, regular (or smooth) continuous-time functions (scaling functions and wavelets) can be obtained, which are orthogonal bases for the space of square-integrable functions [5]. Note that filter banks have always been designed so that in addition to perfect reconstruction the filters have "good" frequency responses, e. g. $H_0(z)$ has always been required to be a good lowpass filter and $H_1(z)$ – to be a good highpass filter. This requirement is tantamous to requiring that the filter bank offer energy concentration and perform well in compression. In this paper we are interested in filter banks where the filters $H_0(z)$ and $H_1(z)$ are not "good" filters in this traditional sense, i. e. we would like them to have pseudo-noise frequency responses.

In this paper we shall consider one important class of sequences, namely complementary sequences. These sequences were recently found to be efficient in a new modulation for wireless communications, called spread-signature CDMA [13]. Recently it was observed by several researchers that these complementary sequences are a special case of two-channel orthogonal FIR filter banks [7, 12]. The main lesson is that the theories of complementary sequences and of orthogonal wavelet transforms can borrow results from each other for mutual benefit. In this paper we present the relationship between filter banks and *aperiodic* complementary sequences and their generalizations, including Welti codes, multilevel complementary sequences and multidimensional complementary sequences.

Then we study *periodic* complementary sequences using the cyclic wavelet transform approach. Two novel sets of orthogonal sequences are constructed, which are periodic symmetric and antisymmetric, correspondingly. Systematic algorithms for their generation are given. These two new sets of orthogonal sequences are generalizations of the GRS sequences in the sense that the GRS sequences are members of both of these sets. As a result we have a systematic algorithm for the generation of all GRS sequences of a given length. Another result, borrowed from filter bank theory, is that the GRS sequences are realizable by a lattice structure.

Chapter 2

Two-channel orthogonal FIR filter banks

Two-channel orthogonal FIR filter banks are the most fundamental and widely used class of filter banks [5, 6]. They consist of two parts (Fig. 2.1): an analysis part of two filters $H_0(z)$ and $H_1(z)$, each followed by downsampling, and a synthesis part, consisting of upsampling in each channel followed by two filters $G_0(z)$ and $G_1(z)$.

The two signals coming out of the analysis part, denoted by $Y_0(z)$ and $Y_1(z)$ and called subband signals, are equal to

$$Y_0(z) = \frac{1}{2}\left[H_0(z^{1/2})X(z^{1/2}) + H_0(-z^{1/2})X(-z^{1/2})\right] , \tag{2.1}$$

$$Y_1(z) = \frac{1}{2}\left[H_1(z^{1/2})X(z^{1/2}) + H_1(-z^{1/2})X(-z^{1/2})\right] . \tag{2.2}$$

It is easily shown that the output signal, $\hat{X}(z)$ is given by

$$\hat{X}(z) = \frac{1}{2}\left[H_0(z)G_0(z) + H_1(z)G_1(z)\right]X(z) + \tag{2.3}$$

$$\frac{1}{2}\left[H_0(-z)G_0(z) + H_1(-z)G_1(z)\right]X(-z) \tag{2.4}$$

In perfect-reconstruction (PR) filter banks we have $\hat{X}(z) = X(z)$ and therefore

$$H_0(z)G_0(z) + H_1(z)G_1(z) = 0, \tag{2.5}$$

$$H_0(-z)G_0(z) + H_1(-z)G_1(z) = 2 . \tag{2.6}$$

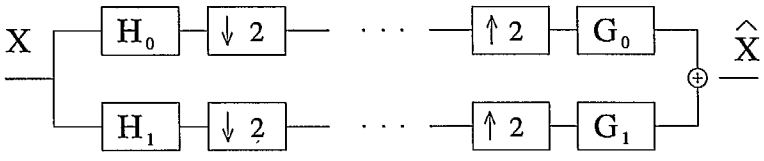

Figure 2.1: Two-channel bank

The transform which represents the computation of the two subband signals $y_0[n]$ and $y_1[n]$ from $x[n]$ is called a forward wavelet transform. The transform which computes the signal $\hat{x}[n]$ (which is equal to $x[n]$ provided the filter bank is PR) is called an inverse wavelet transform. Note that PR is very important even though the signals $y_0[n]$ and $y_1[n]$ are often perturbed in a controlled fashion prior to reconstruction. We are assured that the sole reason for the deviation from PR lies in the additional processing of the subband signals.

In orthogonal filter banks the impulse response $h_0[n]$ together with its integer translates forms an orthogonal basis for the Hilbert space of square summable sequences. The aperiodic auto-correlation function (ACF) of the impulse responses $h_0[n]$ and $h_1[n]$ are half-band functions:

$$< h_0[n],\ h_0[n+2k] > \ = \ \delta_k\ , \tag{2.7}$$

$$< h_1[n],\ h_1[n+2k] > \ = \ \delta_k, \tag{2.8}$$

while the cross-corellation is identically zero

$$< h_0[n],\ h_1[n+2k] >= 0. \tag{2.9}$$

Any two sequences $h_0[n]$ and $h_1[n]$ with the auto-correlation and cross-correlation properties in (2.7), (2.8) and (2.9) form an orthogonal two-channel FIR filter bank and the two sequences are an orthogonal basis for the Hilbert space of square-summable sequences. The synthesis filters are completely determined from the analysis filters:

$$G_0(z) \ = \ H_1(-z) = z^{-N}\tilde{H}_0(z) \tag{2.10}$$

$$G_1(z) \ = \ -H_0(-z) = z^{-N}\tilde{H}_1(z)\ , \tag{2.11}$$

where the $\tilde{\ }$ operation means transposition, conjugation of the coefficients and replacing z by z^{-1}. The highpass filter is related to the lowpass as

$$H_1(z) = -z^{-N}\tilde{H}_0(-z)\ , \tag{2.12}$$

where N is the order of the filters and is necessarily odd. In the time-domain (2.12) is equivalent to

$$h_1[n] = -h_0[N-n](-1)^{-n+1}\ . \tag{2.13}$$

The product filter $P(z)$ is very important

$$P(z) = H_0(z)G_0(z) = H_0(z)H_1(-z) = H_0(z)\tilde{H}_0(z)z^{-N} \tag{2.14}$$

A necessary and sufficient condition for perfect-reconstruction is that $P(z)$ is half-band:

$$P(z) + P(-z) = 2z^l \ . \tag{2.15}$$

Splitting the even-indexed and odd-indexed coefficients is called a polyphase decomposition:

$$H_0(z) = H_{00}(z^2) + z^{-1} H_{01}(z^2) \ , \tag{2.16}$$

$$H_1(z) = H_{10}(z^2) + z^{-1} H_{11}(z^2) \ . \tag{2.17}$$

From (2.12) the relationship between the polyphase components of the two filters can also be obtained.

$$H_{10}(z) = z^{-(N-1)/2} \tilde{H}_{01}(z), \tag{2.18}$$

$$H_{11}(z) = -z^{-(N-1)/2} \tilde{H}_{00}(z). \tag{2.19}$$

2.1 The lattice structure

The lattice structure found by Vaidyanathan (see the appropriate references in [6]) is an efficient way to implement these filter banks. It has two important properties: (i) without sacrificing computational efficiency it preserves the perfect-reconstruction property even under the constraints of finite-word-length arithmetic, and (ii) it is general, every paraunitary filter bank can be implemented using the lattice structure. The generality of the lattice structure suggests that it can also be used to design the filter bank.

In general we have

$$H_1(z) = c \, z^{-L} \, \tilde{H}_0(-z) \tag{2.20}$$

and

$$H_0(z)\tilde{H}_0(z) + |c|^2 \tilde{H}_0(-z) \, H_0(-z) = 2d \tag{2.21}$$

where $|c|^2 = 1$ and d is an arbitrary constant. The paraunitary lattice [6] is based on the elementary paraunitary building blocks

$$\boldsymbol{\Lambda} = \begin{pmatrix} 1 & 0 \\ 0 & z^{-1} \end{pmatrix} \tag{2.22}$$

and

$$\boldsymbol{R}_m = \begin{pmatrix} 1 & \alpha_m \\ -\alpha_m & 1 \end{pmatrix}. \tag{2.23}$$

The polyphase matrix of every paraunitary filter bank can be factored in the following way

$$\mathrm{H}_p(z) = \alpha \boldsymbol{R}_N \, \Lambda(z) \, \boldsymbol{R}_{N-1} \, \Lambda(z) \cdots \boldsymbol{R}_0 \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix}. \tag{2.24}$$

Given the impulse response coefficients, there are algorithms to compute the lattice coefficients and vice-versa [10].

2.2 Conclusions

It must be noted at this point, that the theory of filter banks is usually developed assuming linear (or aperiodic) convolutions. However, when filter banks are used in data compression to avoid the increase in the number of samples (which would have compromized the compression performance) linear (or cyclic) convolution is used. The corresponding wavelet transforms are called periodic (or cyclic). The theory of aperiodic and periodic wavelet transforms can be developed over finite fields, and this, for example, immediately would lead to complementary polynomials over finite fields.

In this Chapter the most fundamental results of filter bank theory were presented. The opportunities for generalization of this theory are numerous. Filter banks can be classified in many ways:

- two-channel or multi-channel
- one-dimensional or multi-dimensional
- maximally-decimated or oversampled
- orthogonal or non-orthogonal
- FIR or IIR
- scalar or vector
- perfect-reconstruction or approximate reconstruction
- many combinations of the above are possible

There is a significant body of literature on the design of sequences for communications applications. The author believes that the majority of these sequences can, in principle, be obtained from filter banks. Furthermore, using filter banks and wavelet transforms, new sequences can be obtained, that have useful properties for communications.

Chapter 3

Aperiodic complementary sequences

The theory of Golay-Rudin-Shapiro (or complementary) sequences dates back to 1949 [1]. By definition a complementary series consists of two finite sequences of 1's and -1's such that the sum of autocorrelation functions of the two sequences is constant. These complementary sequences have been rediscovered many times in the last 40 years. They have challenging and still unclear properties from a theoretical perspective, and since the coefficients are binary have obvious computational advantages in practical implementations. In 1957 Shapiro showed how to construct polynomials of order N, with coefficients equal to 1 or -1, such that $|P(z)|$ is minimal as z ranges over the unit circle. The coefficients in these pairs of polynomials turned out to be exactly the Golay complementary sequences. These polynomials later became known as Rudin-Shapiro polynomials (or equivalently Golay sequences, or even δ codes). To give credit to all of them we shall call them Golay-Rudin-Shapiro (GRS) sequences. Thus, two sequences of length l,

$$A = (a_0,\ a_1,\ \cdots a_l), \tag{3.1}$$

$$B = (b_0,\ b_1,\ \cdots b_l), \tag{3.2}$$

where each entry equals 1 or -1, form a pair of Golay complementary sequences if they satisfy the $l-1$ conditions

$$\sum_{i=0}^{l-j-1} (a_i a_{i+j} + b_i b_{i+j}) = 0, \tag{3.3}$$

for $j = 1, \cdots l-1$. The polynomial notation is sometimes more useful,

$$A(z) = \sum_{i=0}^{l-1} a_i z^i, \tag{3.4}$$

$$B(z) = \sum_{i=0}^{l-1} b_i z^i. \tag{3.5}$$

We shall use t the notations $A(z)$ or A, and $B(z)$ or B, whichever is more convenient. The two sequences A and B are complementary if and only if the corresponding polynomials satisfy the identity

$$A(z)A(z^{-1}) + B(z)B(z^{-1}) = 2l \tag{3.6}$$

If A and B are The following operations also yield complementary sequences:

1. interchanging $A(z)$ and $B(z)$.
2. reversing A and/or B. Thus $\tilde{A}(z)$ and $\tilde{B}(z)$; $\tilde{A}(z)$ and $B(z)$; $A(z)$ and $\tilde{B}(z)$ are also complementary sequences.
3. negating A and/or B
4. negating the polyphase components of $A(z)$ and $B(z)$. Thus $A(-z)$ and $B(-z)$ are also complementary sequences.

The above four operations produce complementary sequences of the same length as the original complementary pair.

There are formulae to produce longer complementary pairs starting from shorter ones. If $A(z)$ and $B(z)$ is a Golay pair of sequences of length N, then $C(z)$ and $D(z)$, defined below, is also a Golay pair of length $2N$:

$$\begin{aligned} C(z) &= A(z) + z^{-N}B(z) && (3.7)\\ D(z) &= \tilde{B}(z) - z^{-2N}\left(\tilde{A}(z)\right) && (3.8) \end{aligned}$$

$$\begin{aligned} C(z) &= B(z) + z^{-N}A(z) && (3.9)\\ D(z) &= -z^{-N}\tilde{B}(z) + z^{-2N}\left(\tilde{A}(z)\right) && (3.10) \end{aligned}$$

$$\begin{aligned} C(z) &= A(z) + z^{-N}B(z) && (3.11)\\ D(z) &= -A(z) + z^{-N}B(z) && (3.12) \end{aligned}$$

$$C(z) = A(z) + z^{-N}B(z) \tag{3.13}$$

$$D(z) = A(z) - z^{-N}B(z) \tag{3.14}$$

$$C(z) = A(z) + z^{-2N}\tilde{B}(z) \tag{3.15}$$

$$D(z) = \tilde{B}(z) - z^{-2N}\left(\tilde{A}(z)\right) \tag{3.16}$$

Another way to construct longer complementary sequences starting from shorter ones is as follows. Given a Golay pair (A_1, B_1) of length N_1 and another pair (A_2, B_2) of length N_2, a new Golay pair (T_1, T_2) can be obtained in the following fashion:

$$T_1 = A_2 \otimes \frac{A_1 + B_1}{2} + B_2 \otimes \frac{A_1 - B_1}{2} \tag{3.17}$$

$$T_2 = A_2 \otimes \frac{\tilde{A}_1 - \tilde{B}_1}{2} - B_2 \otimes \frac{\tilde{A}_1 + \tilde{B}_1}{2} \tag{3.18}$$

The $\tilde{}$ applied to a sequence means simply reversal of the order of the elements.

A Golay pair is called a kernel if it cannot be obtained by a transform method from Golay pairs of the same length, nor derived from Golay pairs of shorter lengths. Kernels of lengths 2, 10 and 26 have been found by computer search. Other kernels at the present time have not been found. Furthermore it is not known whether they exist or not. In general, in addition to the requirement that the length of a complementary pair l be even, l must be the sum of two integral squares and must satisfy some other conditions [1]. Even after almost 50 years since the notion of complementary sequences was advanced the question of the possible lengths of these complementary sequences remains an open and extremely difficult problem. The more this problem is investigated, the more difficult it looks. It appears that the question of the possible lengths of complementary sequences is similar in difficulty to the proof of the famous theorem of Pierre Fermat. This statement is not an exaggeration, since Fermat's theorem was proven recently.

With the help of a computer it can be shown that the total number of different Golay pairs of lengths $N = 1, 2, 4, 8, 10$ is equal to 4, 8, 32, 192, 128, respectively. Complementary sequences have found various applications in CDMA wireless communication systems [13] and data communications systems [21].

The aim here is to demonstrate the intimate relationship between PR filter banks and Golay-Rudin-Shapiro systems, which has not been recognized before.

Consider for example two-channel filter bank with no downsampling and upsampling. This is an *oversampled filter bank.* The input-output relationship is

$$\hat{X}(z) = (H_0(z)G_0(z) + H_1(z)G_1(z))\, X(z) \tag{3.19}$$

Since there is redundancy it is not difficult to achieve perfect-reconstruction. The design in this case corresponds to solving the Bezout identity

$$H_0(z)G_0(z) + H_1(z)G_1(z) = \text{const} \tag{3.20}$$

It is plain to see that if we choose $G_0(z) = H_0(z^{-1})$ and $G_1(z) = H_1(z^{-1})$ then the system achieves PR. In this case $H_0(z)$ and $H_1(z)$ satisfy the same relationship as Golay-Rudin-Shapiro polynomial pairs.

Theorem 1 *A Golay-Rudin-Shapiro polynomial pair forms a tight frame for $l_2(Z)$ with a redundancy factor 2.*

Proof: Consider a scalar two-channel filter bank with no downsampling and upsampling. This is an *oversampled filter bank.* The input-output relationship is

$$\hat{X}(z) = (H_0(z)G_0(z) + H_1(z)G_1(z))\, X(z) \tag{3.21}$$

Since there is redundancy it is not difficult to achieve perfect-reconstruction. The design in this case corresponds to solving the Bezout identity

$$H_0(z)G_0(z) + H_1(z)G_1(z) = \text{const} \tag{3.22}$$

It is plain to see that if we choose $G_0(z) = H_0(z^{-1})$ and $G_1(z) = H_1(z^{-1})$ then the system achieves PR. In this case $H_0(z)$ and $H_1(z)$ satisfy the same relationship as Golay-Rudin-Shapiro polynomial pairs. □

The fact that a_i and b_i form a tight frame means that they can represent any square-summable sequence. However, in general, they do not form an orthonormal basis. The simplest example of Golay complementary sequences is, of course,

$$A = (1,\ 1) \tag{3.23}$$

$$B = (1,\ -1), \tag{3.24}$$

which is the Haar case. In this case the Golay-Rudin-Shapiro polynomial pair is realizable by a maximally-decimated filter bank. In this particular case, the complementary sequences form not only a tight frame, but an orthonormal basis. It is believed that only in this case the complementary polynomials are realizable by a maximally-decimated filter bank (this requires a proof, however).

Recently it was shown that the GRS sequences are a special case of orthogonal FIR filter banks [7, 12].

Theorem 2 *(Cooklev'95) The Golay-Rudin-Shapiro (GRS) polynomial pairs are polyphase components of a lowpass filter in an orthogonal maximally-decimated two-channel FIR filter bank.*

Proof: Suppose we are given a filter $H(z)$ of length $2l-1$ with coefficients which are only $+1$ and -1 satisfying

$$H(z)H(z^{-1}) + H(-z)H(-z^{-1}) = \text{const} = 4l. \tag{3.25}$$

It can be proved that the polyphase components of $H(z)$ satisfy (3.6), i. e. they form a GRS polynomial pair:

$$\begin{aligned} 4l &= \left[H_0(z^2) + z^{-1}H_1(z^2)\right]\left[H_0(z^{-2}) + zH_1(z^{-2})\right] \\ &+ \left[H_0(z^2) - z^{-1}H_1(z^2)\right]\left[H_0(z^{-2}) - zH_1(z^{-2})\right] \\ &= 2\left[H_0(z^2)H_0(z^{-2}) + H_1(z^2)H_1(z^{-2})\right]. \end{aligned} \tag{3.26}$$

Therefore the polyphase components of every power-complementary filter $H(z)$ are a GRS pair. Now it is straightforward to establish that the filter with polyphase components equal to a GRS pair is power-complementary. □

The GRS sequences being the polyphase components of orthogonal filter banks are realizable by a lattice structure. The lattice coefficients are not integers in general and no obvious relationship among them was found.

Years before the advent of wavelet transforms it was recognized that these GRS pairs provide orthonormal bases for the Hilbert space [4].

Note that while there are PR FIR filter banks of every even length, the requirement the length of the Golay sequences to be even is not sufficient. It probably should be mentioned that the idea that these GRS sequences are very closely related to filter banks occured for the first

time to M. Sablatash [11]. Later, J. Byrnes in [12] realized that GRS sequences are related to filter banks, but he didnot state exactly that they are the polyphase components. Furthermore Byrnes did not go into other details of the relationship between GRS pairs and filter banks, such as the fact that GRS pairs are realizable by a paraunitary lattice structure. The above theorem was proven for the first time in [7]. It seems that the first lowpass filter with more than 2 coefficients for FIR perfect-reconstruction filter banks have been designed by Golay as early as 1949! Note that the restriction the coefficients to be binary (1 and -1) constraints the zeros of the filter $H(z)$ and, in particular, this filter a has a pseudo-random frequency response.

3.1 Extensions of GRS sequences

Following Golay's work, mathematical properties, computer searches and existence problems for certain lengths were further investigated by various researchers. Different applications have required different generalizations of the original concept of Golay to be made. For their research into surface acoustic wave (SAW) devices Tseng and Liu studied complementary sets of sequences [20]. Welti advanced sequences of vectors which could be successfully used in pulsed radar for range detection [17]. Complex-valued complementary sequences were considered by Frank; they have become known as Frank codes and have applications in the area of radar pulse compression. The fact that using a GRS pair we can build an orthogonal filter $H(z)$ which forms a basis for square-summable sequences was observed in [4]. Note that the Barker polynomials [3] are somewhat related to the Rudin-Shapiro polynomials, and thus to filter banks as well.

In this Section we briefly review some extensions of GRS sequences. This Section is short, as the time frame of this Contract does not allow a deeper study of the extensions of the original concept of Golay. It is, however, clear that the set of all possible extensions of GRS sequences is isomorphic to the set of all possible filter banks. Just as all filter banks have useful properties, by using the filter bank framework new sequences can be obtained that have useful properties.

3.1.1 Welti codes

A quaternary Welti sequence is defined as a sequence of length $2N$ whose elements are $\pm\alpha$ or $\pm\gamma$, where multiplication is defined by

$$\alpha\gamma = \gamma\alpha = 0 \tag{3.27}$$

$$\alpha^2 = \gamma^2 = 1 \tag{3.28}$$

and the out-of-phase aperiodic ACF is identically zero. It can be shown that the set of all Welti sequences is isomorphic to the set of all complementary sequences [19] and thus to filter banks as well. In fact, from a Welti sequence of length $2N$ the first polyphase component of which has elements $\pm\gamma$ and the second polyphase component has elements $\pm\alpha$ a pair of complementary sequences can be constructed; for a Welti sequence of length $2N$ for which the first N elements are of the form $\pm\alpha$ and the last N elements are of the form $\pm\gamma$, the first N and the last N elements form a pair of complementary sequences. On the other hand, a Welti sequence can be constructed from a pair of complementary sequences by considering them to be the first and second polyphase components of a Welti sequence (i. e. interleave them); or by concatenating them as long as the elements of the complementary sequences satisfy (3.27) and (3.28). Note that by concatenating complementary sequences orthogonal FIR filter banks can be obtained if and only if the filter coefficients obey the multiplication rules (3.27) and (3.28). It is clear that such filter banks have not been studied in the past.

3.1.2 Complex-coefficient complementary pairs

Theorem 3 *Suppose $A(z)$ and $B(z)$ are a complementary sequence. Then $A(W_M)$ and $B(W_M)$ are complementary sequences as well for $\forall M > 0$.*

Note that the set of complex-coefficient complementary pairs has more elements than the set of complementary pairs with real coefficients. For example, for $M = 4$, complex-coefficient complementary sequences have been found for lengths 3,5,6,12,13,18,24,30,36,48,50,60,72,78 and 96, while they have been found to be non-existing only for lengths $7, 9, 11, 15, 17$.

If $A(z)$ and $B(z)$ are complementary sequences with complex elements, then similar properties are also valid, i. e. by interchange, negate, reverse and conjugate, and negate alternate, we can also obtain complementary sequences of the same length.

The recursive method for constructing Golay pairs, by which sequences of length $N2^k$ can be constructed starting from a pair of length N, also applies to complex-coefficient complementary pairs.

3.1.3 Complementary sequences over finite fields

It should be noted that wavelet transforms can be defined over finite fields, and immediately, according to the above Theorem, we can obtain complementary sequences (and Welti codes) over finite fields. Complementary sequences over finite fields have not been investigated and could be an avenue for future work on the design of sequences for wireless communications.

3.1.4 Subcomplementary and supercomplementary sequences

Subcomplementary and supercomplementary sequences are two relatively new extensions of GRS sequences. Subcomplementary sequences [26] comprise two or more finite sequences of equal length, assumes to be $2^k p_0$ such that the sum of their aperiodic autocorrelation functions is zero for all shifts $p \leq p_0$, minimum for $0 < p < p_0$, and maximum for $p = 0$.

In supercomplementary sequences not only the autocorrelation functions are complementary, but the crosscorrelation between two appropriately defined sequences is also complementary. These sequences have a number of useful applications in radar, such as complementarity of the ambiguity functions. The Gold sequences are a special case of these supercomplementary sequences.

Chapter 4

Orthogonal periodic symmetric codes

Note that filter banks are designed assuming aperiodic convolutions and ACF and CCF. However, when filter banks are used to perform data compression, periodic (or cyclic) convolutions are employed. In this paper we use cyclic convolutions and therefore cyclic wavelet transforms to design cyclic extensions of complementary sequences.

Here we consider the problem of the design of orthogonal system $\{s_0, s_2, \cdots s_{m-1}\}$. To simplify the signal processing operations it is desirable to deal with binary symbols, i. e. ± 1. It is convenient and simple to assume that all orthogonal signals s_i are generated by cyclic shifts of $s_0 = (a_0\ a_1\ \cdots a_{N-1})$ and that the sequence a_i is periodic with period N: $a_{N+i} = a_i$. It is clear that the maximum size of this cyclic code, that is the maximum number of different codewords, is equal to N. If the code is of maximum size then $s_i = (a_i, \cdots a_{N-1+i})$. It is plain to see the formal similarity of this problem with filter bank theory. The codewords play the role of impulse responses of digital filters in a filter bank and the codewords (i. e. the impulse responses) are of length N. If orthogonality is imposed orthogonal cyclic codes of maximum size do not exist. Following the wavelet transform approach, however, orthogonal periodic codes can be constructed with size equal to $N/2$. The properties of sequences depend on their autocorrelation functions (AFs). Since we assumed periodic sequences it is convenient to use the periodic autocorrelation function (PAF)

$$r[n] = \sum_{i=0}^{N-1} a[i]a[< i+n >_N] \quad a[i] \in 1, -1, \tag{4.1}$$

where $a[N+i] = a[i]$ and $< . >$ is the modulo notation.

Theorem 4 *The system of codewords formed by double cyclic shifts of the sequence* $s_0 =$

$(a_0, a_1, \cdots, a_{N-1})$ *with length* N *is orthogonal iff*

$$r[2n] = 0 \quad n = 1, 2, \cdots N/4 \tag{4.2}$$

and its size is $N/2$.

Using the DFT it can be written that

$$\begin{aligned} R[k] &= \sum_{n=0}^{N-1} r[n] W_N^{nk} \\ &= \sum_{n=0}^{N-1} \sum_{i=0}^{N-1} a[i] a[< i+n >_N] W_N^{nk} \quad < i+n >_N = l \\ &= \sum_{i=0}^{N-1} a[i] \sum_{l=0}^{N-1} a[l] W_N^{(l-i)k} \\ &= A[k]\, A[-k] = |A[k]|^2 \end{aligned} \tag{4.3}$$

In our notation

$$W_N = e^{-j2\pi/N} \tag{4.4}$$

and thus the relationship between the z-transform and DFT is given by $z = W_N^{-k}$. A fundamental property of the DFT is that it assumes periodicity in both time- and frequency-domains. Note that the DFT of the PACF is non-negative, which corresponds to the condition that the frequency response of the product filter in filter banks be non-negative. A polyphase decomposition can be applied on the PCF

$$R(z) = R_0(z^2) + z^{-1} R_1(z^2)\,. \tag{4.5}$$

which in the DFT domain corresponds to

$$R[k] = R_0[2k] + W_N^k R_1[2k] \tag{4.6}$$

where

$$\begin{aligned} R_0[2k] &= \sum_{i=0}^{N/2-1} r[2i] W_N^{i2k} \\ R_1[2k] &= \sum_{i=0}^{N/2-1} r[2i+1] W_N^{i2k}\,. \end{aligned} \tag{4.7}$$

Note that $R_0[2k]$ and $R_1[2k]$, as well as the similarly defined $A_0[2k]$ and $A_1[2k]$, are not DFTs themselves. Since all even-indexed coefficients $r[2i]$ are equal to zero, with the exception of $r[0]$ we get

$$R_0[2k] = r[0] = N \,. \tag{4.8}$$

Taking (4.3) into consideration we get

$$\begin{aligned} R[k] &= (A_0[2k] + W_N^k A_1[2k])(A_0[-2k] + W_N^{-k} A_1[-2k]) \\ &= A_0[2k]A_0[-2k] + A_1[2k]A_1[-2k] + W_N^k A_1[2k]A_0[-2k] + W_N^{-k} A_0[2k]A_1[-2k] \end{aligned} \tag{4.9}$$

Note that $W_N^k A_1[2k]A_0[-2k]$ and $W_N^{-k} A_0[2k]A_1[-2k]$ are complex conjugates of each other. The conclusion is that

$$R_0[2k] = |A_0[2k]|^2 + |A_1[2k]|^2 \tag{4.10}$$

$$W_N^k R_1[2k] = 2\,\mathrm{Re}\{W_N^k A_1[2k]A_0[2k]\} \tag{4.11}$$

Formulae (4.10) and (4.11) are not known in the cyclic wavelet transform literature. The necessary and sufficient condition for orthogonality of the codewords is

$$|A_0[2k]|^2 + |A_1[2k]|^2 = N \tag{4.12}$$

The problem is how to find all orthogonal filters with binary coefficients? The conditions of orthogonality are invariant under the following operations:

- sign inversion, i. e. if $A(z)$ is a codeword, then $-A(z)$ is also a codeword.
- inversion of the order $a_i \leftarrow a_{N-1-i}$, i. e. if $A(z)$ is a codeword, then $z^{-N}\tilde{A}(z)$ is also a codeword.
- cyclic shifts

4.1 The structure of codewords

The polynomial representation of the codeword s_0 is given by $A(z)$, which can be decomposed as

$$A(z) = A_0(z^2) + z^{-1}A_1(z^2) \,. \tag{4.13}$$

In the same way, as it was done before it can be established that these polyphase components are complementary sequences, which are periodic, however. (The non-periodic complementary sequences are the GRS sequences)

An interesting question is whether these complementary sequences are themselves codewords. The PCF of $(a_i, a_{i+2}, \cdots a_{i+N-2})$, $i = 0, 1$ are

$$r_i[n] = \sum_{k=0}^{N/2-1} a[2k+i]a[2(k+n)+i] \tag{4.14}$$

where the indice must be evaluated $\pmod N$. Therefore

$$R_i[k] = \sum_{n=0}^{N/2-1} r_i[n]W_{N/2}^{nk} = A_i[k]A_i[-k] = |A_i[k]|^2 \; i = 0, 1 \tag{4.15}$$

From (4.14) it follows that

$$\begin{aligned} r_0[n] + r_1[n] &= \sum_k a[2k]a[2k+2n] + \sum_k a[2k+1]a[2k+2n+1] \\ &= r[2n] \quad n = 1, \cdots N/4 \end{aligned} \tag{4.16}$$

Since we know that $r[2n] = 0 \quad n \neq 0$, the the necessary and sufficient conditions for orthogonality are

1. Each of these complementary sequences are themselves codewords, i. e. $r^i[2n] = 0$ and $r_0[2n-1] = -r_1[2n-1] \quad k = 1, 2, \cdots N/8$

2. The complementary sequences are not codewords, i. e. the condition $r^i[2n] = 0$ fails for at least one n; then

$$r_0[n] = -r_1[n] \tag{4.17}$$

Let G_N is the set of all codewords with length N. This set is a union of two sets: the set G_N^1 of codewords the polyphase components of which are themselves codewords of length $N/2$ and the set G_N^2 of codewords the polyphase components of which are not codewords. The set G_N is isomorphic to the set of all orthogonal wavelet filters corresponding to a circular wavelet transform.

Theorem 5 *A periodic cyclic code with length $N = 2^k$ exists for all values of k greater than 2.*

Proof: First, it will be shown that a periodic cyclic code exists for $k = 2$. It is recognized that filter banks whose polyphase components are GRS polynomials with length $N/2$ belong to the set G_N. Therefore $(1, 1, 1, -1)$ is a codeword. By cyclic shifts and sign inversions we can get 7 other codewords, or the total size of the set G_4 is 8. Now, suppose that $A_0(W_{N/2}^k) \in G_{N/2}$ which has the polyphase decomposition

$$A_0(W_N^{2k}) = A_{00}(W_N^{4k}) + W_N^{2k} A_{01}(W_N^{4k}) \tag{4.18}$$

Since $A_0(W_{N/2}^k) \in G_{N/2}$ the condition of orthogonality

$$|A_{00}(W_N^{4k})|^2 + |A_{01}(W_N^{4k})|^2 = N/2 \tag{4.19}$$

holds. Let us define

$$A_1(W_N^{2k}) = \pm W_N^l \left[A_{00}(W_N^{4k}) - W_N^{2k} A_{01}(W_N^{4k}) \right] \tag{4.20}$$

The polyphase components of A_1 also satisfy (4.19) and thus A_1 is also a codeword, $A_1 \in G_{N/2}$. The sequence $\tilde{A}_1$ is also a codeword. Finaly A_0 and A_1 can be shown to be polyphase components of a codeword with length N by taking into account (4.12) and (4.19)

$$|A_0(W_N^{2k})|^2 + |A_1(W_N^{2k})|^2 = N \tag{4.21}$$

Therefore $A(z) = A_0(z^2) + z^{-1} A_1(z^2)$ is a codeword belonging to the set G_N. Q. E. D.

4.2 Construction of codewords

4.2.1 The case $N = 4$

It is convenient to introduce three DFTs:

$$B(W_4^k) = 1 - W_4^k - W_4^{2k} - W_4^{3k} \tag{4.22}$$

$$C(W_4^k) = 1 + W_4^k - W_4^{2k} - W_4^{3k} \tag{4.23}$$

$$D(W_4^k) = 1 + W_4^k + W_4^{2k} + W_4^{3k} \tag{4.24}$$

$$E(W_4^k) = 1 - W_4^k - W_4^{2k} - W_4^{3k} \tag{4.25}$$

The codewords for $N = 4$ correspond to cyclic shifts and sign inversions of B and C. The capacity of this code is $Q_4 = 8$.

4.2.2 Codewords with length $N = 8$

For $N = 8$ the codeword can be expressed as

$$A[k] = A(W_N^k) = \pm W_N^{kl} B(W_N^{2k})(1 \pm W_N^{k(2m+1)}) \qquad l, m \in \{0, 1, 2, 3\} \tag{4.26}$$

In this case the total number of such sequences is $4.4.2.2 = 2^6$. For example when $l = 0$ and $m = 0$ we get the codeword (1,1,-1,-1,-1,-1,-1,-1).

4.2.3 Codewords with length $N = 16$

. For $N = 16$ we know that all codewords from G_8 are first polyphase components of codewords from G_{16}. The second polyphase components can be found from (4.20)

$$\begin{aligned} A_{16,1}(W_{16}^k) &= \pm W_{16}^{kl} B(W_{16}^{4k}) \left[(1 \pm W_{16}^{2k(2m+1)}) + W_{16}^{2p+1}(1 - \pm W_{16}^{2k(2m+1)})\right] \\ m &\in \{0, 1, 2, 3\},\ l, p \in \{0, 1, 2, 3, 4, 5, 6, 7\}. \end{aligned} \tag{4.27}$$

By counting the number of free variables we get for the capacity of this code $G_{16}^1 = 4.16.8.2 = 2^{10}$.

But there are more orthogonal sets of sequences in G_{16}. The set G_8 does not exhaust all complementary pairs. Note that

$$2|C(W_4^k)|^2 + |D(W_4^k)|^2 + |E(W_4^k)|^2 = 16 \quad \forall k \in \{0, 1, 2, 3\}\ . \tag{4.28}$$

Therefore we can construct more codewords in the set G_{16} as follows

$$A_{16,2}(W_{16}^k) = W_{16}^{lk} \left[C(W_{16}^{4k}) \pm W_{16}^{\pm 2k} E(W_{16}^{4k}) + W_{16}^{(2p+1)k} \left(C(W_{16}^{4k}) \pm W_{16}^{2k} D(W_{16}^{4k})\right)\right] \tag{4.29}$$

This can be verified to be codeword by checking the PCF:

$$\begin{aligned} |A_{16,2}(W_{16}^k)|^2 &= |C \pm W_{16}^{\pm 2k} E|^2 + |C \pm W_{16}^{2k} D|^2 \\ &+ 2\ \mathrm{Re}\{W_{16}^{k(2p+1)}(C \pm W_{16}^{2k} D)(C \pm W_{16}^{\pm 2k} E)^*\} \\ &= 16 + 2\ \mathrm{Re}\{W_{16}^{(2m+1)k}|C|^2\} = 16 + 8\mathrm{Re}\{W_{16}^{(2p+1)k}(1 - W_{16}^{8k})\} \end{aligned} \tag{4.30}$$

where $C = C(W_4^k)$ $D = D(W_4^k)$. This means that the PCF is half-band, or

$$r[2n] = 0 \tag{4.31}$$

$$r[2n+1] \in \{0, \pm 4\}\ . \tag{4.32}$$

Taking into consideration the number of sequences in (4.26) it is figured out that there are 2^9 such sequences and the total capacity of G_{16} is $Q_{16} = 2^{10} + 2^9 = 3.2^9$. Equations (4.27) and (4.29) are a systematic way to construct codewords with $N = 16$. For example when $l = m = p0$ from (4.27) we get

$$A_{16,1}(W_{16}^k) = B\left[(1 + W_{16}^2) + W_{16}^1(1 - W_{16}^2)\right] \tag{4.33}$$

There are eight codewords generated by $A_{16,1}$:

$$111 - 1 - 1 - 1 - 11 - 1 - 1 - 11 - 1 - 1 - 11 \tag{4.34}$$

$$1 - 1 - 1 - 1 - 11 - 1 - 1 - 11 - 1 - 1 - 1111 \tag{4.35}$$

$$-1 - 1 - 11 - 1 - 1 - 11 - 1 - 1 - 11111 - 1 \tag{4.36}$$

$$-11 - 1 - 1 - 11 - 1 - 1 - 11111 - 1 - 1 - 1 \tag{4.37}$$

$$-1 - 1 - 11 - 1 - 1 - 11111 - 1 - 1 - 1 - 11 \tag{4.38}$$

$$-11 - 1 - 1 - 11111 - 1 - 1 - 1 - 11 - 1 - 1 \tag{4.39}$$

$$-1 - 1 - 11111 - 1 - 1 - 1 - 11 - 1 - 1 - 11 \tag{4.40}$$

$$-11111 - 1 - 1 - 1 - 11 - 1 - 1 - 11 - 1 - 1 \tag{4.41}$$

all of which, according to the cyclic wavelet transform principle, are generated by double cyclic shifts.

4.2.4 Codewords with length $N = 32$

Again we know that the codewords from G_{16} are the first polyphase components of codewords in G_{32}. From (4.27) we obtain

$$\begin{aligned} |A_{16,1}(W_{16}^k)|^2 &= |B(W_{16}^{4k})|^2 \left[|1 \pm W_{16}^{k(2m+1)}|^2 + |1 - \pm W_{16}^{k(2m+1)}|^2 + \right. \\ &+ \left. 2\mathrm{Re}\left(W_{16}^{k(2p+1)}(1 \pm W_{16}^{2k(2m+1)})(1 \pm W_{16}^{-2k(2m+1)})\right)\right] \\ &= 16 + 8\mathrm{Re}\left[W_{16}^{k(2p+1)}(\pm W_{16}^{-2k(2m+1)} - \pm W_{16}^{2k(2m+1)})\right] \end{aligned} \tag{4.42}$$

From (4.27) and (4.42) it follows that complementary vectors of (4.27) can be found in two ways:

$$A_{16,1,1}(W_{16}^k) = W_{32}^{kl} B(W_{16}^{4k}) \left[\left(1 + W_{16}^{2k(2m+1)}\right) - W_{16}^{k(2p+1)} \left(1 - W_{16}^{k(2m+1)}\right)\right] \tag{4.43}$$

$$A_{16,1,2}(W_{32}^k) = W_{16}^{kl} B(W_{16}^{4k}) \left[\left(1 - W_{16}^{2k(2m+1)}\right) + W16^{k(2p+1)} \left(1 + W_{16}^{k(2m+1)}\right)\right] \tag{4.44}$$

Table 4.1: Number of codewords in the symmetric orthogonal periodic code

N	2^2	2^3	2^4	2^5	2^6	2^7	2^8
number of codewords	2^3	2^6	3×2^9	7×2^{15}	$\geq 7 \times 2^{22}$	$\geq 7 \times 2^{30}$	$\geq 7 \times 2^{39}$

Thus for each first polyphase component we can find $4N = 2^7$ second polyphase components ($N/2 \times 2$ shifts, N sign inversions, and $2N$ vectors generated by the tilde operation). As a result there are $4N2^{10} = 2^{17}$ codewords with length 32, generated according to

$$A_{32} = A_{16,1} + W\ A_{16,1,i} \tag{4.45}$$

If we take (4.29) as the first polyphase component the second polyphase component can be found according to (4.20). In this way we can generate $4N2^9$ more codewords with length $N = 32$.

The third way to construct codewords with length $N = 32$ is as follows. The first polyphase component can be chosen as

$$A_{16,3} = W_{16}^{kl}\left[\pm E(W_{16}^{4k}) \pm W_{16}^{2k} D(W_{16}^{4k}) + W_{16}^{k} C(W_{16}^{4k})\left(1 + W_{16}^{2k(2m+1)}\right)\right] \tag{4.46}$$

the complementary vector of which is

$$A_{16,3,1} = [\pm E(W_{32}^{4k}) \pm W_{16}^{2k} D(W_{16}^{4k}) - W_{16}^{k} C(W_{16}^{4k})\left(1 + W_{16}^{\pm 2k(2m+1)}\right)] \tag{4.47}$$

There are 2^8 vectors of the type (4.46) and for each of them there are $4N$ complementary vectors of the type (4.47). Therefore the number of codewords of the third type is $4N2^8 = 2^{15}$. The total number of codewords with length $N = 32$ is found to be $2^{17} + 2^{16} + 2^{15} = 7.2^{15}$.

In general, when the second polyphase components are formed according to (4.20) and $N = 2^k \quad k = 6, 7, \cdots$ a lower bound on the number of codewords is $G_N > 2NG_{N/2}$.

Table 4.1 summarizes the number of codewords of this periodic symmetric code.

Chapter 5

Orthogonal antisymmetric periodic codes

In this chapter again orthogonal codes are constructed using wavelet-based approach. The orthogonal sets that are obtained offer high capacities and simple signal processing operations.

The orthogonal set of codewords is $\{s_0\ s_1\ s_{M-1}\}$ where $s_i = (a[2i], a[2i+1], \cdots, a[2i+N-1])$, and $a[N+i] = -a[i]$, $a[2N+i] = a[i]$. It also assumed that $a[i]$ can take only two values: 1, or -1. The number of codewords is $M = N/2$ each having length N. Since periodicity is assumed the properties of the periodic autocorrelation function

$$r[n] = \sum_{i=0}^{N-1} a[i]a[i+n] \tag{5.1}$$

which has a period equal to $2N$, are very important. The periodic autocorrelation function has the following propertis:

1. $r[0] = \sum_{i=0}^{N-1} a^2[i] = N$

2. $r[\pm N] = \sum_{i=0}^{N-1} a[i]a[i \pm N] = -\sum_{i=0}^{N-1} a^2[i] = -N$

3. $r[n] = -\sum_{i=0}^{N-1} a[i]a[i \pm N + n] = -r[n \pm N] = r[-n]$

4. $r[N/2] = 0$. This property can be established by

$$\begin{aligned} r[N/2] &= \sum_{i=0}^{N-1} a[i]a[N/2+n] && (5.2)\\ &= a[0]a[N/2] + a[1]a[N/2+1] + \cdots + a[N/2-1]a[N-1] && (5.3)\\ &- a[N/2]a[0] - a[N/2+1]a[1] - \cdots - a[N-1]a[N/2-1] = 0 && (5.4) \end{aligned}$$

5. $r[2n] = 0 \pmod 4$, $r[2n+1] = 2 \pmod 4$. These properties are not trivial and need a proof. It is convenient to use the transform $b[i] = (1 - a[i])/2$. Then the PAF becomes

$$r[n] = \sum_{i=0}^{N-1} (1 - 2b[i])\,(1 - 2b[i+n]) \tag{5.5}$$

$$= \sum_{i=0}^{N-1} (1 - 2b[i] - 2b[i+n] + 4b[i]b[i+n]) \tag{5.6}$$

$$= N - 2\left[\sum_{i=0}^{N-1} (b[i] + b[i+n])\right] + 4\sum_{i=0}^{N-1} b[i]b[i+n] \tag{5.7}$$

But considering the antisymmetry $a[N+i] = -a[i]$ we have

$$1 = b[N+i] + b[i]\,, \tag{5.8}$$

and therefore

$$\sum_{i=0}^{N-1} (b[i] + b[i+n]) = 2\sum_{i=0}^{N-1} b[i] + n - 2\sum_{i=0}^{n-1} b[i] \tag{5.9}$$

and therefore

$$r[n] = N - 4\sum_{i=0}^{N-1} b[i] - 2n + 4\sum_{i=0}^{n-1} b[i] + 4\sum_{i=0}^{N-1} b[i]b[i+n] \tag{5.10}$$

Since N is a power of 2, the properties are easily established.

The DFT of the periodic autocorrelation function is

$$R[k] = \sum_{n=0}^{N-1} r[n]W_N^{nk} = A[k]\,A[-k] = |A[k]|^2 \tag{5.11}$$

The DFT of the sequence $a[0], a[1], \cdots, a[N-1]$ can be represented in polyphase form:

$$A[k] = A_0[2k] + W_N^1 A_1[2k] \tag{5.12}$$

and the same decomposition can be applied with respect to the PAF:

$$R[k] = R_0[2k] + W_N^1 R_1[2k]\,. \tag{5.13}$$

In a similar way, as was done in the previous chapter it can be shown that

$$R_0[2k] = |A_0[2k]|^2 + |A_1[2k]|^2 \tag{5.14}$$

$$W_N^1 R_1[2k] = 2\mathrm{Re}\{W_N^1 A_1[2k]A_0[-2k]\} \tag{5.15}$$

The necessary and sufficient condition to have orthogonality is that the autocorrelation is half-band:

$$r[2n] = 0, \quad n = 1, 2, \cdots N/4 - 1 \tag{5.16}$$

which also means that

$$R_0[2k] = |A_0[2k]|^2 + |A_1[2k]|^2 = N \tag{5.17}$$

Now, for the polyphase components, T the PCF of $(a_i, a_{i+2}, \cdots a_{i+N-2})$, $i = 0, 1$ are

$$r_i[n] = \sum_{k=0}^{N/2-1} a[2k+i]a[2(k+n)+i]]; a[N+i] = -a[i], \tag{5.18}$$

$$R_i[k] = \sum_{n=0}^{N/2-1} r_i[n]W_{N/2}^{nk} = A_i[k]A_i[-k] = |A_i[k]|^2 \; i = 0, 1 \tag{5.19}$$

where $r[2n] = r_0[n] + r_1[n]$ and therefore, a necessary and sufficient condition for orthogonality is that

$$r_0[n] = -r_1[n] \quad n = 1, 2, \cdots N/4 - 1 \; . \tag{5.20}$$

The vectors for which the above condition is fulfilled are called complementary. The complementary property is invariant under the following transformations:

1. If $A_0(z)$ and $A_1(z)$ are complementary, then $\tilde{A}_0(z)$ and $\tilde{A}_1(z)$ will also be complementary.

2. The complementary property is invariant under cyclic shifts. $z^l A_0(z) \pmod{z^{N/2} - 1}$ and $z^l A_1(z) \pmod{z^{N/2} - 1}$ are also complementary.

The GRS sequences are contained entirely in the new class of sequences, i. e. they are a subset of it. This implies, of course, that the number of the new sequences exceeds the number of GRS sequences for the same length.

The codewords of length N are obtained as $s_{2i} = (a[2i], a[2i+1] \cdots a[2i+N-1])$. One sequence generates two codes s_{2i} and s_{2i+1} with volume $M = N/2$ each having $N/2$ words.

There are two cases:

1. The polyphase components (i. e. the complementary vectors) of a codeword are themselves codewords:

$$r_0[2n] = r_1[2n] = 0 \quad r_0[2n+1] = -r_1[2n+1] \tag{5.21}$$

2. The polyphase components of a codeword are not codewords themselves:

$$r_i[2n] \neq 0 \tag{5.22}$$

but still then $r_0[n] = -r_1[n]$ continues to hold.

It is clear that in the first case an orthogonal antisymmetric periodic code with length N and volume $N/2$ can be constructed iteratively, starting from codewords with length $N/2$. Suppose we have a codeword with length $N/2$, which is also a complementary vector, $A_0(z) \in G_{N/2}$. It must be the first polyphase component of a codeword in the set G_N, but it can be further decomposed using the polyphase decomposition

$$A_0[2k] = A_{00}[4k] + W_{N/2}^1 A_{01}[4k] \; . \tag{5.23}$$

The second polyphase component can be constructed in two ways. The first is

$$A_1[2k] = W^{2l} \left(A_{00}(4k) - W^{2k} A_{01}(4k) \right) \quad l = 0, \cdots N-1 \tag{5.24}$$

and the second

$$A_1[2k] = W_N^{-2l} (A_{00}(4k) - \tilde{W}^{2k} A_{01}(4k)) \tag{5.25}$$

It is obvious that $A_1 \in G_{N/2}$, since A_1 has polyphase components which have equal magnitudes as the polyphase components of A_0. Then, a codeword can be constructed, of which A_0 and A_1 are the first and second polyphase components, correspondingly:

$$|A_0|^2 + |A_1|^2 = 2 \left[|A_{00}|^2 + |A_{01}|^2 \right] = N \; . \tag{5.26}$$

5.1 Examples

From the properties of the autocorrelation function, discussed in the beginning of this chapter, it follows that all combinations of four bits are codewords and therefore the volume of the code is $Q_4 = 2^4$.

Two cyclic groups of sequences can be constructed as cyclic shifts of the basic elements

$$p(W_8) = 1 + W_8 + W_8^2 + W_8^3 \tag{5.27}$$

$$q(W_8) = 1 - W_8 + W_8^2 - W_8^3 \tag{5.28}$$

The elements of these groups are $W_8^i p(W_8)$ and $W_8^i q(W_8)$. Cyclic shifts of $p(W_8)$ and $q(W_8)$ exhaust all combinations of four bits, i. e. all codewords in the set G_4. Note that

$$p^*(W_8) = -W_8 p(W_8) \tag{5.29}$$

$$|p(W_8)|^2 = 4 + 2(W_8 + W_8^{-1}) = 4 + 2\sqrt{2} \tag{5.30}$$

$$q^*(W_8) = W_8 q(W_8) \tag{5.31}$$

$$|q(W_8)|^2 = 4 - 2(W_8 + W_8^{-1}) = 4 - 2\sqrt{2} \tag{5.32}$$

and

$$p(W_8)\, q^*(W_8) = 2(W_8 - W_8^{-1}) = j2\sqrt{2}\,. \tag{5.33}$$

For $N = 8$, using (5.21) and (5.24) the codeword is expressed by the formula

$$A(W_{16}) = W_{16}^l \left[p(W_{16}^2) + W_{16}^{2k+1} q(W_{16}^2)\right] \quad l = 0, 1, \cdots, 15, k = 0, 1 \cdots 7 \tag{5.34}$$

The first polyphase component comes from $p(W_8)$, and its cyclic shifts, and the second – from $q(W_8)$ and its cyclic shifts. The number of different codewords is $C_8 = 2^4.2^3 = 2^7$, since l can take 2^4 values and k can take 2^3 values.

The next value of N is 16. All polyphase components belong to G_8. We are looking for codewords of the type

$$A(W_{32}) = W_{32}^l \left[W_{32}^a \left(p(W_8) + W_{32}^b q(W_8)\right) + (p(W_8) + W_{32}^c q(W_8))\right] \tag{5.35}$$

$$l = 0, 1, \cdots, 31, \tag{5.36}$$

$$a = 1, 3, 5, \cdots, 31, \tag{5.37}$$

$$b, c \in \{2(2k+1)\},\ k = 0, 1, \cdots, 7. \tag{5.38}$$

Now the orthogonality constraint is imposed to get

$$\begin{aligned} & Re\left[r(2)W_{32}^2 + r(4)W_{32}^4 + r(6)W_{32}^6\right] \\ = \; & Re\left[(W_{32}^{-4} - W_{32}^4)(W_{32}^b + W_{32}^c)\right] = 0 \end{aligned} \tag{5.39}$$

which is true for

$$b = c \pm 16 \tag{5.40}$$

or

$$b = -c. \tag{5.41}$$

This leads to two posiible forms of the codewords from G_{16}:

$$A(W_{32}) = W^l \left[W^a(p + W^b q) + (p - W^c q)\right] \tag{5.42}$$

or

$$W(W_{32}) = W^l \left[W^a(p + W^b q) + (p + W^{-c} q)\right] \tag{5.43}$$

The total number of codewords of the type (5.42) is $2^3 2^3 2^5 = 2^{11}$ and the total number of codewords of the type (5.43) is the same. This makes the total number of codewords with length 16 equal to 2^{12}. The search of codewords for higher values of N becaomes considerably more complicated.

Chapter 6

Systematics synthesis of GRS pairs

The problem of generation of all Golay-Rudin-Shapiro sequences is of considerable importance. For example, in the context of wireless communications, every user is assigned a different sequence, and then it is necessary to generate all sequences of a given length.

The E-sequences having zero values of the autocorrelation function in even shifts have correlation properties close to optimal. It has apparently escaped evidence the fact that these E-sequences are, in fact, filter banks. Note that [4] does give a method for the generation of these E-sequences, which is not complete, however. For example for $N = 32$ it is possible to obtain only 2^9 sequences, while there are 3.2^9 E-sequences of this length. The aperiodic correlation function is

$$A[m] = \sum_{i=0}^{N-1-m} \alpha[i]\ \alpha[i+m] \tag{6.1}$$

In the previous chapters two periodic extensions of the sequence ($\alpha[0]\ \alpha[1] \quad \alpha[N-1]$) were considered: symmetric, where $\alpha[N+i] = \alpha[i]$, and antisymmetric, where $\alpha[N+i] = -\alpha[i]$. It is convenient to denote the periodic autocorrelation functions by $r^s[n]$ and $r^a[n]$ for the symmetric and antisymmetric cases, respectively.

Theorem 6 *The relationship among the aperiodic autocorrelation function $A[m]$, and the two periodic autocorrelation functions $r_s[m]$ and $r_a[m]$ is*

$$A[m] = r^s[m] + r^a[m] \tag{6.2}$$

$$r^s[m] = A[m] + A[N-m] \tag{6.3}$$

$$r^a[m] = A[m] - A[N-m] \tag{6.4}$$

Theorem 7 *The necessary and sufficient condition the aperiodic autocorrelation function to be half-band,*

$$r[2m] = 0 \quad m = 1, 2, \cdots N/2, \tag{6.5}$$

is that

$$r^s[2m] = r^a[2m] = 0, \quad m \neq 0 \tag{6.6}$$

The proof can immediately be obtained using (6.5).

Corollary 1 *The set of Golay sequences is the intersection of the sets of codewords belonging to the orthogonal symmetric and antisymmetric cyclic codes. In other words the Golay sequences are simultaneously codewords of the two codes.*

Next, the codewords for the antisymmetric code are given when $N = 4$. Only those of the type $W\ B$ belog to the symmetric orthogonal code, which total eight in number.

$$D^a = (1,1,1,1) = D^s \tag{6.7}$$
$$W_8^1\ D^a = (-1,1,1,1) = -B^s \tag{6.8}$$
$$W_8^2\ D^a = (-1,-1,1,1) = -C^s \tag{6.9}$$
$$W_8^3\ D^a = (-1,-1,-1,1) = W_8^3 B^s \tag{6.10}$$
$$W_8^4\ D^a = (-1,-1,-1,-1) = -D^s \tag{6.11}$$
$$W_8^5\ D^a = (1,-1,-1,-1) = B^s \tag{6.12}$$
$$W_8^6\ D^a = (1,1,-1,-1) = C^s \tag{6.13}$$
$$W_8^7\ D^a = (1,1,1,-1) = -W_8^3 B^s \tag{6.14}$$

$$E^a = (1,-1,1,-1) = E^s \tag{6.15}$$
$$W_8^1\ E^a = (-1,1,1,1) = -W_8^2 B^s \tag{6.16}$$
$$W_8^2\ E^a = (-1,-1,1,1) = W_8^1 C^s \tag{6.17}$$
$$W_8^3\ E^a = (-1,-1,-1,1) = -W_8^1 B^s \tag{6.18}$$
$$W_8^4\ E^a = (-1,-1,-1,-1) = -E^s \tag{6.19}$$
$$W_8^5\ E^a = (1,-1,-1,-1) = -W_8^2 B^s \tag{6.20}$$
$$W_8^6\ E^a = (1,1,-1,-1) = -W_8^1 C^s \tag{6.21}$$
$$W_8^7\ E^a = (1,1,1,-1) = W_8^1 B^s \tag{6.22}$$

When $N = 8$ the codewords in the symmetric code are described by the formulae

$$A^s(W_8) = \pm W_8^l B \left(1 \pm W_8^{2m+1}\right) \tag{6.23}$$

and for the antisymmetric code

$$A^a(W_{16}) = W_{16}^l \left(D + W_{16}^{2m+1} E\right) \tag{6.24}$$

where $A(W)$ are the DFTs of the codewords. For the antisymmetric code we can write

$$A^a(W) = W_{16}^l \left(W_8^m D + W_{16} W_8^n E\right) \tag{6.25}$$

When m and n are odd then the codewords of the antisymmetric code have the same structure with the codewords of the symmetric code of the type $\pm W_8^l B$. In this case $m, n = 1, 3, 5, 7$ and the volume of the set is $4.4.2 = 2^5$, which coincides with previously obtained estimates for the size of the GRS set.

For $N = 16$ the antisymmetric codewords can be written in the following form:

$$A^a(W) = W^{2l}\left(W_8^m D + W_{16}^2 W_8^n E\right) + W_{16}^{2l+1} W_8^p \left(W_8^m D - W_{16}^2 W_8^n E\right) \tag{6.26}$$

$$A^a(W) = W_8^m \left[W_{16}^{2l+q}\left(D + W_{16}^2 W_8^{n-m} E\right) + W_{16}^{2p-4(n-m)-q-1}\left(E + W_{16}^2 W_8^{n-m} D\right)\right] \tag{6.27}$$

where $p = 0, 1, \cdots 15$, $l, q = 0, 1$. For the same length the structure of the codewords belonging to the symmetric orthogonal code is

$$A_1^s = \pm W^l B \left[\left(1 \pm W^{2t_0}\right) + W^{t_1}\left(1 - \pm W^{2t_0}\right)\right] \tag{6.28}$$

$$A_2^s = W^l \left[C \pm W_{16}^{\pm 2} E + W^{t_1}\left(C \pm W_{16}^2 D\right)\right] \tag{6.29}$$

The codewords (6.27) have identical structure with (6.28) when m and n are odd which yields $4^3.2 = 2^7$ E-sequences. The codewords (6.27) are reduced to (6.29) in other cases, which yields an additional 2^6 E-sequences. The total volume of the set of E-sequences with length 16 is $2^6 + 2^7 = 192$. For example when $m = 0$, $l = q = 0$, $n = 2$ and $t_3 = 5$ then

$$A^a = D + W_{16}^2 W_8^2 E + W_{16}\left(E + W_{16}^2 W_8^2 D\right) = 11 - 1 - 11 - 11 - 111111 - 1 - 11 \tag{6.30}$$

This polynomial is equivalent to a E-sequence, the ACF of which is $(-10 - 10 - 101050 - 3010)$.

It would appear that the above analytic solutions are novel and provide useful insight into the theory of GRS sequences. They follow from the theory of cyclic and aperiodic wavelet transforms. This analytic approach becomes too cumbersome for higher lengths, but is obviously very convenient for short lengths.

Bibliography

[1] M. Golay, "Multislit spectrometry," *J. Opt. Soc. America,* vol. 39, pp. 437-444, 1949.

[2] M. Golay, "Complementary series," IRE Trans. Inform. Theory, vol. IT-17, pp. 82-87, 1961.

[3] R. Turyn and J. Storer, "On binary sequences," *Proc. Amer. Math. Soc.,* vol. 12, pp. 394-399, 1961.

[4] Y. Taki, H. Miyakawa, M. Hatori and S. Namba, "Even-shift orthogonal sequences," *IEEE Trans. Inform. Theory,* vol. 15, pp. 295-300, 1969.

[5] I. Daubechies, *Ten lectures on wavelets,* CBMS-NSF Regional Conf. in Appl. Math., vol. 61, SIAM, Philadelphia, PA, 1992.

[6] P. P. Vaidyanathan, *Multirate systems and filter banks,* Prentice-Hall, Englewood Cliffs, NJ, 1993.

[7] T. Cooklev, "Regular perfect-reconstruction filter banks and wavelet bases," *Ph.D. thesis,* Tokyo Institute of Technology, Japan, 1995.

[8] T. Cooklev, A. Nishihara, M. Kato and M. Sabalatsh "Two-channel multifilter banks and multiwavelets," *IEEE ICASSP'96,* Atlanta, GA, pp. 2769-2773, May 1996.

[9] T. Cooklev, M. Kato, A. Nishihara, M. Sablatash, "Multifilter banks and multiwavelet bases," *IEICE Tech. Rept. IE95-22,* Tokyo, Japan, pp. 51-58, May 1995.

[10] T. Cooklev, "On the design and implementation of filter bank trees for multiple access communications," Technical Rept. 67CRC-5-3315, CRC, Ottawa, 1996.

[11] M. Sablatash, "Theory and applications of wavelets," *Seminar at the University of British Columbia,* Vancouver, BC, 1992.

[12] J. Byrnes, "Quadrature mirror filters, low crest factor arrays, functions achieving optimal uncertainty principle bounds, and complete orthonormal sequences – a unified approach," *Applied and computational harmonic analysis*, vol. 1, pp. 261-266, 1994.

[13] G. W. Wornell, "Spread-signature CDMA: Efficient multiuser communication in the presence of fading," *IEEE Trans. Inform. Theory,* vol. 41, pp. 1418-1438, Sept. 1995.

[14] G. Benke, "Generalized Rudin-Shapiro systems," *Journal of Fourier analysis and applications,* vol. 1, No. 1, pp. 87-101, 1994.

[15] S. Eliahou, M. Kervaire, and B. Saffari, "On Golay polynomial pairs," *Advances in applied mathematics,* vol. 12, pp. 235-292, 1991.

[16] S. Eliahou, M. Kervaire, and B. Saffari, "A new restriction on the lengths of Golay complementary sequences," *Journal of combinatorial theory,* ser. A 55, pp. 49-59, 1990.

[17] G. R. Welti, "Quaternary codes for pulsed radar," *IEEE Trans. Inform. Theory,* vol. IT-6, pp. 400-408, 1960.

[18] L. Bömer and M. Antweiler, "Periodic complementary binary sequences," *IEEE Trans. Information Theory,* vol. 36, No. 6, pp. 1487-1494, 1990.

[19] R. Turin, "Ambiguity functions of complementary sequences," *IEEE Trans. Inform. Theory,* vol. 9, pp. 46-47, 1963.

[20] C. C. Tseng and C. L. Liu, "Complementary sets of sequences," *IEEE Trans. Inform. Theory,* vol. 18, pp. 644-652, 1972.

[21] I. M. I. Habbab and L. F. Turner, "New class of m-ary communication systems using complementary sequences," *IEE Proc. pt. F,* vol. 133, pp. 293-300.

[22] H. D. Luke, "Sets of one and higher dimensional Welti codes and complementary codes," *IEEE Trans. Aerospace Electr. Syst.*, vol. 21, pp. 170-179, 1985.

[23] A. Gavish and A. Lempel, "On ternary complementary sequences," *IEEE Trans. Inform. Theory,* vol. 40, pp. 522-526, 1994.

[24] E. E. Hollis, "Another type of complementary sequences," *IEEE Trans. Aerospace Electron. Syst.,* vol. AES-11, pp. 916-919, 1975.

[25] E. E. Hollis, "Quasi-complementary sequences," *IEEE Trans. Aerospace Electron. Syst.,* vol. AES-11, pp. 115-118, 1975.

[26] R. Srivaswamy, "Self-clutter cancellation and ambiguity properties of subcomplementary sequences," *IEEE Trans. Aerospace Electron. Syst.,* vol. AES-18, pp. 163-181, 1982.

[27] B. M. Popovic, and S. Z. Budisin, "Generalized subcomplementary sets of sequences," *Electronics Letters,* vol. 23, pp. 422-424, 1987.

[28] S. Z. Budisin, "Supercomplentary sets of sequences," *Electronics Letters,* vol. 23, pp. 504-506, 1987.