DESIGN OF QUASIORTHOGONAL CODE FOR BPSK SIGNALS AT ASYNCHRONOUS TRANSMISSION

Stanisław Tujaka

Telecommunications Research Institute, ul. Hallera 13, 80–401 Gdańsk, Poland

1. INTRODUCTION

The paper submits to use binary phase–shift keyed (BPSK) signals in the multiple–access ranging system like an underwater positioning system with many transponders. Code sequences of the signals for the purpose should have adequate autocorrelation properties to measure the range, as well as adequate crosscorrelation properties to identify transponders. In the system the time of arrival of the signal is a parameter to be established, therefore application of synchronous transmission methods is impossible. The signal can be received only as a whole by means of a matched filter. This is why the main problem for designing the asynchronous system consists in determining the optimal structure of the set of signals for the given set of messages (addresses, orders etc.).

The method of approach to the problem is based on calculation of a correlation distance for various sets of pseudorandom and related sequences according to the assumed definition. The correlation distance and the power of the required code should be as great as possible. Codes built around maximal–length (Huffman), Walsh, derivative (Digilock) and composed (Gold, Kasami) sequences were examined this way.

The best results are obtained for the code, the words of which are combined of cyclic shifts of the M–sequence. The first bit of each word in the code is a reference chip sequence of the same cyclic shift for every word, and the next bits have cyclic shifts different for each word. The presented solution provides simpler technical implementation and higher bandwidth efficiency than a frequency coding.

2. CODING AT ASYNCHRONOUS TRANSMISSION

An asynchronous transmission system can be shown in general case like in Fig.1. The system is composed of some number of transmitters and receivers connected with a common channel. The transmitters produce discrete signals $s_i(t)$ which belong to a finite set – the assembly of signals

$$S=\{\ s_i(t)\ \}; \qquad\qquad i = 1,2,...,N$$

The signals are transmitted independently one of another. We assume that in our application the condition is met

$$t_i << T_0$$

where t_i – duration of signal $s_i(t)$

T_0 – mean time interval between signal transmissions in the system

Such a condition means that the throughput capacity of the channel is much greater than the performance of particular signal sources. It enables to employ asynchronous multiplexing. All transmitted signals go to the input of any receiver, while their mutual position in time is free. Some receiver k' is designed to detect a certain signal $s_k(t)$. This signal will be the desirable one for this receiver, and all other signals will be the crosstalk interferences. Therefore, it is necessary to choose the signals so that they will be easy to distinguish each other as well as resistant against noise $\sigma(t)$. This way a problem arises to design an assembly of N adequate signals. Since a code word corresponds to each signal in the considered case, so the design is resolved to obtain the assembly of code words, i.e. the code.

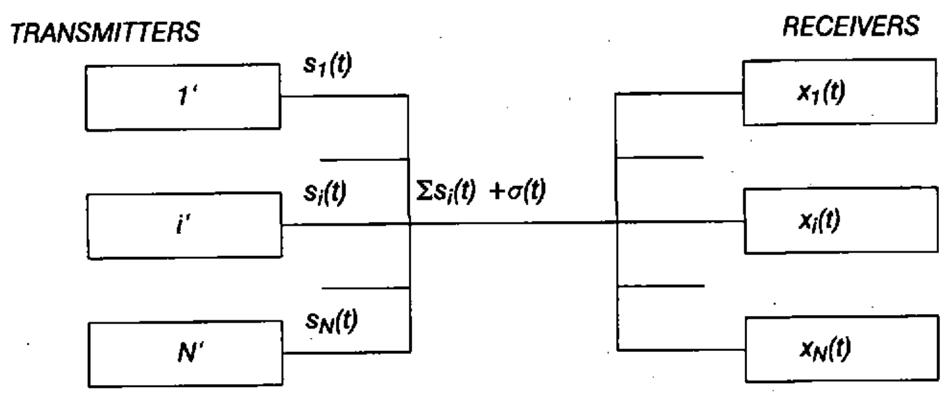

Fig.1. Asynchronous transmission system

3. METHOD OF RECEPTION

Optimal reception of a BPSK signal can be achieved by means of a matched filter in the shape of a transversal filter composed of delay lines and phase shifters. However, implementation of such a filter for hydroacoustic purposes is impossible in practice. Thus, suboptimal reception by means of a digital filter matched to the code word of the signal is accomplished in the proposed system. The digital matched filter is composed of an identification circuit for the signal chips (first decision circuit) and an identification circuit for the code word (second decision circuit). Digital signal processing comprises coherent filtration on a synchronous detector followed by noncoherent registration in shift registers. The registered signal is compared with the replica of the desired signal in a decoder.

It is necessary to take into account that at coherent detection of BPSK signals the phenomenon of inversed operation appears. This precludes to establish that the given code word or its complement is received. The non-continuous BPSK signal has three states: in-phase signal state, out-of-phase signal state and no-signal state. The digital receiver made of two-state logic devices cannot distinguish between a no-signal state and an out-of-phase signal state. Lack of the signal is associated with one of the signal states. This fact is called as a change of the symbol alphabet.

4. EXAMINATION OF CODES

Examination of correlation properties for codes was carried out according to the following definitions.

A binary code Φ of power M and length N is an assembly of M binary words of the same length N, which are called as code words c_i.

$$\Phi = \{ c_i , i=0,...,M-1 \}$$

A Hamming distance $d(c_i,c_j)$ is a number of digit positions in which the corresponding digits of two code words are different.

A minimal code distance d_H is equal to the least of all Hamming distances for different pairs of code words, i.e.

$$d_H = min\ d(c_i,c_j), \qquad i \neq j$$

A correlation is a number of agreements between digits of two sequences for the given relative displacement of the both sequences. In order to determine the correlation of two sequences we compute digit–by–digit the negation of modulo 2 sum for the sequences and add the results. It is an unnormalized correlation. A normalized correlation we obtain by dividing the number of agreements by the length of the sequence.

A correlation function is a set of correlation values for all displacements. When the correlation function concerns two different sequences, then we say on crosscorrelation function. When it concerns two the same sequences, then we say on autocorrelation function. For the given code the maximal value of the autocorrelation function is equal to the code length N.

Let us designate the maximal sidelobe value of the autocorrelation function by L_{ii} and the maximal lobe value of the crosscorrelation function by L_{ij}. Then the value

$$d_k = N - max\ (L_{ii}, L_{ij})$$

is called as a correlation code distance. It serves as a measure of the distance between the code words in the space of code words and displacements. By comparing the definitions we can see that the minimal code distance d_H describes the differences between the code words "in point", whereas the correlation code distance d_k – "on segment".

Correlation properties of codes are examined in the relevant literature [1,2] for periodic sequences or for alphabet composed of three symbols. There the correlation is calculated as the number of agreemants minus the number of disagreements. Here, we are interested in aperiodic correlation functions with regard to effects of inversed operation and changing the symbol alphabet caused by application of the digital matched filter to receive the BPSK signal. Therefore the adequate code was searched for by computer simulation of operation of the decoder. The decoder is represented by a code word to which it is matched

$$A_i = \{a_k,\ \ k=1,...,N\}$$

DESIGN OF QUASIORTHOGONAL CODE

The signal led to the decoder is represented by a code word surrounded from both sides with zero words of the same length

$$B_j = \{b_l,\ l=1,...,3N\}$$

In the initial moment all zeros are written into the decoder. For each program step corresponding to the displacement of the signal in the shift register of the decoder the number of agreements (i.e. correlation) between digits of the docoder and signal code word is calculated

$$C_{ij}(p) = \sum_{k=1}^{N} \overline{a_k \oplus b_{2N+k-p}}$$

where $p=1,..., 2N-$ displacement

For remaining displacements the correlation function has a constant value. The mechanism of calculations is illustrated in Fig.2 that shows the initial stage (a), the intermediate one (b) and the final one (c) of passing the signal through the decoder. The set of signal code words is two times greater than the set of decoder code words, because it includes also the inversed words.

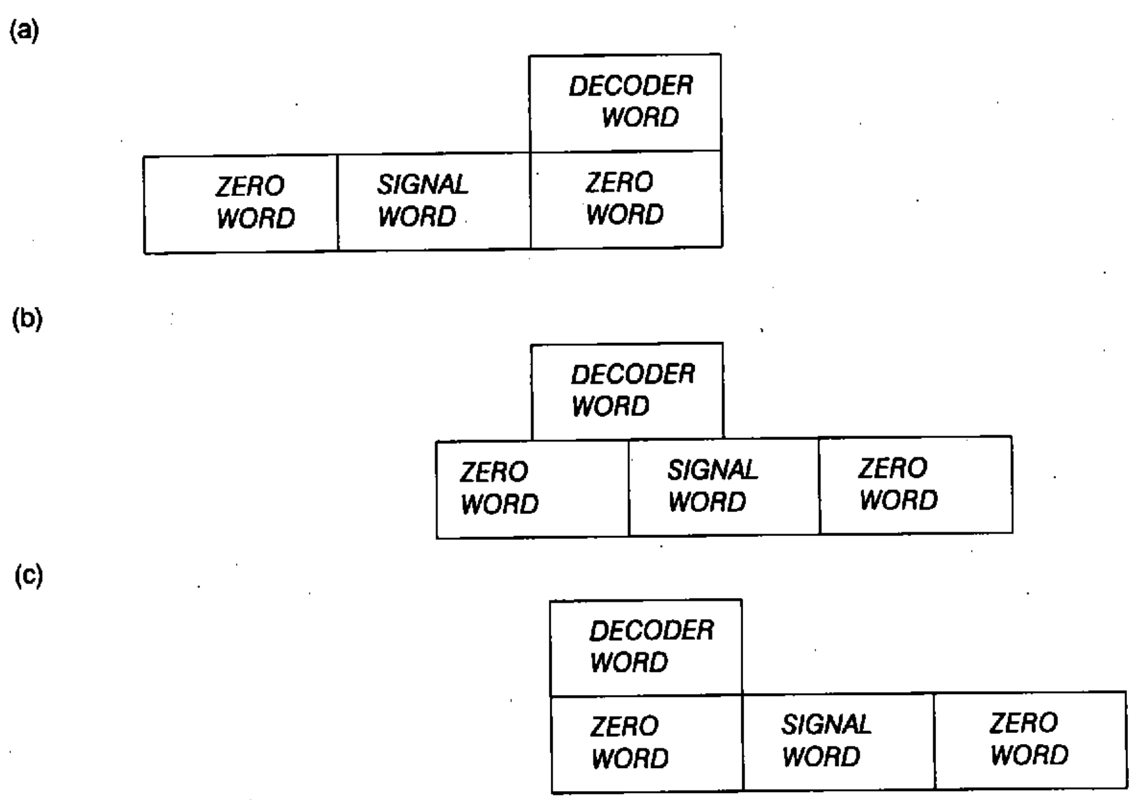

Fig.2. Passing of signal through decoder

DESIGN OF QUASIORTHOGONAL CODE

If the set of the decoder words is composed of 15 words and each word has the length of 15 digits, than a two dimensional array of 15x15 is needed to write the set. An array of 45x30 is needed to write the signal words and a three-dimensional array of 30x30x15 to write the correlation values.

5. EXAMINED CODES

Using the method of examination described in the previous chapter we were looking for a code, the normalized correlation distance and the power of which at the given length would be as great as possible. For practical reasons a criterion of compactness for the code was introduced. It is known, that in the best case it is possible to find $M=N$ orthogonal words composed of N digits.

We took the preassumption that the pseudorandom and related sequences preserve at least partially their excellent correlation properties under the imposed conditions, too.
Such a verification was carried out for the following codes.

5.1. Maximal-length sequences

Binary maximal-length sequences (M-sequences) were examined at first because of their famous correlation properties. It was examined a code, the words of which are all cyclic shifts of the M-sequence. The correlation distance for the code equals zero.

A code composed of a M-sequence family reveals quasiorthogonality. E.g. the normalized correlation distance of 8/31=26% is achieved for the family of 6 sequences being 31 digits long.

5.2. Walsh sequences

A code of Walsh sequences is a classic orthogonal code. After changing the symbol alphabet by substituting "1" for "-1" and "0" for "+1" we obtain the code that is also known as Reed-Miller code. The code reveals zero correlation distance.

5.3. Derivative sequences

To create derivative sequences the Walsh sequences are used as the originative ones. As the generative sequence it is possible to choose any sequence that meets the following requirements:
- it should have better autocorrelation properties than the generative sequence,
- a length of the originative and generative sequences should be the same.

Such requirements are met by e.g. nonlinear shift-register sequences. For the so produced Digilock codes [3] the correlation distance is 0. The Stiffler code [3] is produced similarly. Cyclic shifts of a M-sequence completed with one digit so that their length will be the same as the length of Walsh sequences are used as generative sequences. It has also zero correlation distance.

5.4. Composed sequences

A Gold sequence is constructed by adding modulo 2 two M-sequences. A code of Gold sequences includes the both originative sequences and results of adding modulo 2 one of the sequences to each of the cyclic shifts of the second sequence. The code is composed of $N+2$ words of the length N. The correlation distance for the code of Gold sequences is 0, as well as for the code of Kasami sequences, which are generated similarly, but in more complicated way.

6. OBTAINED RESULTS

The described examinations give evidence that a compact quasiorthogonal code was searched persistently. Such compact codes of about the same power and length are created by derivative and composed sequences. Unfortunately, the sequences are wrong balanced, i.e. the numbers of zeros ond ones within the sequences differ significantly. They do not provide a good correlation properties. The best correlation distance is achieved for families of M–sequences. However, in this case the length of words exceeds many times the number of words.

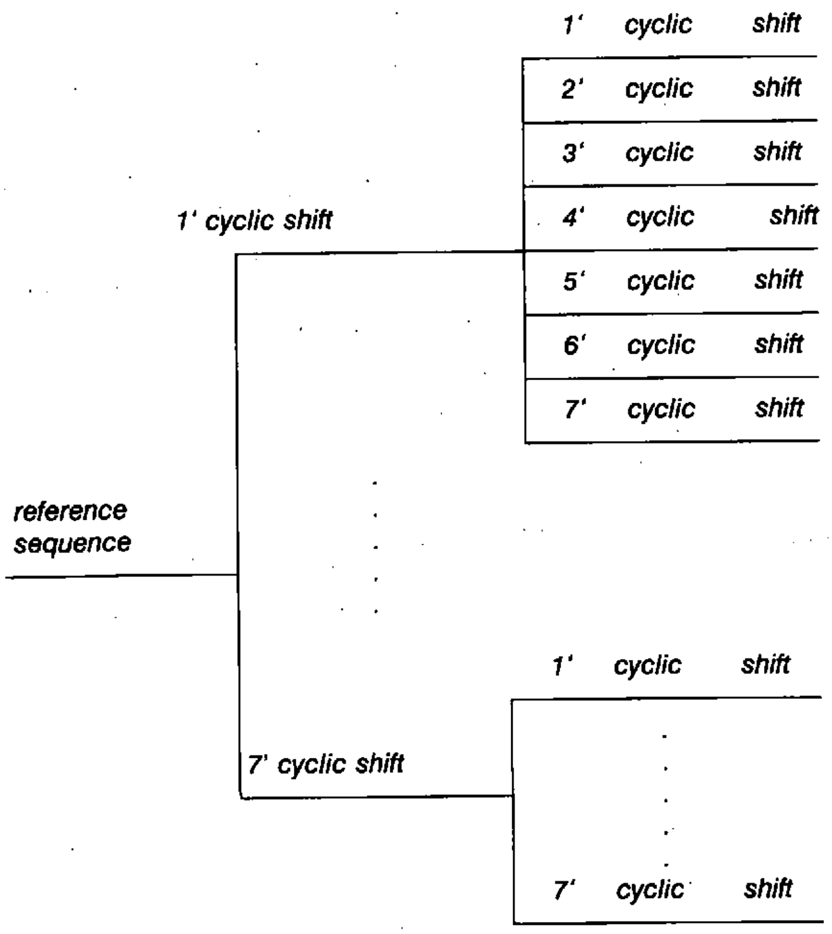

Fig.3. Design of code words by combining cyclic shifts (example for 7–chips sequence)

A new proposition for designing the quasiorthogonal code is prepared. It consists in combining the code words of two or more M–sequences, which are called in further as bits according to the terminology used in spread–spectrum communications. The first bit of each word in the code is a reference chip sequence of the same cyclic shift for every word, and the next bits have cyclic shifts different for each word.

An algorithm how to create the words is illustrated by the diagram shown in Fig.3. An example of such a code is given in Tab.1. The words are 2–bits long, each bit being a cyclic shift of 7–chips long M–sequence.

Tab.1. Quasiorthogonal code of power 7

Signal No.	Code word	
1	1110010	1110010
2	1110010	1100101
3	1110010	1001011
4	1110010	0010111
5	1110010	0101110
6	1110010	1011100
7	1110010	0111001

The two greatest lobes of correlation functions for the code given in Tab.1 are shown in Tab.2 (a), and for the complements of code words in Tab.2 (b). As we can see, the maximal lobes in Tab.2 (b) do not exceed the maximal lobes of crosscorrelation functins and maximal sidelobes of autocorrelation functins in Tab.2 (a). So, in this meaning we can say that the code is resistant to inversed operation. The correlation distance for the code amounts 3, so it is a single–error correcting code. The correlation distance is 3/14=21%.

The code of 3–bit words (see Fig.3) possesses also correlation distance equal to 3. The normalized correlation distance is 3/21=14%, but the code has power of 7x7=49 that is greater than the length of 3x7=21. The correlation distance for the compact code designed this way can be improved up to 4 by throwing away 15 words of poorer correlation properties. Obviously, the power of the code is then lowered.

We can generalize the results obtained for the combined codes so that at increasing the length of the chip sequence the correlation distance tends towards the limit of half the length and is independent on the number of bits in code words.

7. REFERENCES

[1] D.V. Sarwate, M.B. Pursley,'Crosscorrelation Properties of Pseudorandom and Related Sequences' Proceedings of the IEEE, Vol.68, No.5, May 1980, pp. 593–620

[2] F.R.K. Chung, I.A. Salehi, V.K. Wei,'Optical Orthogonal Codes: Design, Analysis and Applications' IEEE Transactions on Information Theory, Vol.35, No.8, May 1989, pp. 595–604

[3] S.W. Golomb (editor),'Digital Communications with Space Applications', Prentice – Hall, Inc. 1964

DESIGN OF QUASIORTHOGONAL CODE

Tab.2. Maximal lobes of correlation functions for code composed of two M-sequences

(a)

Signal No.

Decoder No.	1	2	3	4	5	6	7
1	14,10	10,10	11,10	11,10	11,10	10,10	11,10
2	10,10	14,10	11,10	10,9	10,9	10,9	10,10
3	10,10	10,10	14,9	10,9	10,9	10,9	10,10
4	10,10	10,9	10,9	14,9	10,10	10,9	10,10
5	10,10	10,9	10,10	11,10	14,9	10,10	10,10
6	10,10	10,10	10,9	10,10	11,10	14,9	10,10
7	10,10	10,10	10,10	10,10	10,10	10,10	14,10

Decoder No.

(b)

Inversed signals

Signal No.

Decoder No.	1	2	3	4	5	6	7
1	9,8	9,8	9,8	8,8	9,8	9,8	9,8
2	8,8	9,8	9,8	8,8	10,9	8,8	9,8
3	8,8	8,8	9,9	8,8	8,8	8,8	8,8
4	8,8	8,8	8,8	9,8	9,8	8,8	8,8
5	8,8	9,9	8,8	9,8	8,8	8,8	8,8
6	9,8	8,8	9,8	8,8	10,9	10,8	10,8
7	8,8	9,8	8,8	8,8	9,8	10,9	10,9

Decoder No.