Algorithm And A C++ Program For CCS Of Binary Sequences With Primary Lengths

Dimitar M. Kovachev[1], Ventsislav Valchev[2], Ekaterina Dimitrova[2]

Abstract - **This paper focuses on the calculation of cross-correlation functions of binary sequences with maximal length, precisely in the case when lengths are prime numbers. Algorithm has been developed and C++ program has been written and its performance has been compared with those of a convolution and a DFT. The results have been discussed. The programs developed have been used in a program generator for FPGA-based generators of MS.**

Keywords: **FPGA, PRS, DFT**

I. Introduction

The sequences with a maximum length (M-sequences, or MS) are widely used in radio-location for creating signals with a complex shape [1], in different audio and acoustic measurements [2], in systems of wireless communication [3] and so on.

Their main advantage is excellent auto-correlation properties - binary auto-correlation function (ACF) with a single maximum, surrounded by side lopes with an insignificant level [4.]:

$$\vartheta(k)=\begin{cases}N,\rightarrow k\equiv 0 \bmod N,\\ -1,\rightarrow k\not\equiv 0 \bmod N.\end{cases}, \qquad (1)$$

where N denotes the length of the sequence, $\vartheta(k)$ - the value of ACF at shift k.

If we denote two MSs as vectors $\boldsymbol{x_i}$ and $\boldsymbol{x_j}$, their periodic cross-correlation function (CCF) is received after (2):

$$\vartheta_{ij}(k)=N-2w(x_i\oplus T^k x_j) \qquad (2)$$

where $w(\bullet)$ is the weight of the vector after Hemming (the number of ones in it), T^k is an operator for k-multiple cyclic shift to the right [4].

If $A_k=A(x_i,x_j)_k$ denotes the positions in which vectors x_i and $T^k x_j$ coincide, and $D_k=D(x_i,x_j)_k$ - the number of their non-coincidences, thus:

$$\vartheta(k)=A_k-D_k, \qquad (3)$$

In most practical applications, a binary sequence is actually transmitted as a sequence of unit amplitude, positive and negative pulses, obtained by replacing each 1 by a –1 and each 0 by a +1. As the expression (2) is suitable only for cases with binary sequences of {0,1}, the most commonly used expression to determine ACF and CCF in engineering literature is (3) [4]. (3) is often calculated by convolution for short sequences, but with the increase of length the time for defining CCF significantly increases. In such cases it is usual to move to the frequency area and use fast convolution.

When processing necessitates the calculation of the periodical CCF of two different MSs, as it is during the correlation processing of the reflections from moving targets, the maximum value of CCF is more significant than its particular values.

One of the possibilities to define CCF is by fast convolution [5], using the direct and reverse discrete Fourier transform (DFT). But when the MS length is a prime number, the calculation time greatly increases (the square of the length). That is why it is necessary to design special algorithms for these cases.

The paper treats an algorithm and a program for determination of the CCF values for MSs with lengths of a prime number by using the Rader conversion.

The response time is estimated in relation to the direct application of DFT. The program has been used as part of programming system for generating FPGA-based (Field Programmable Gate Array) generators of MSs, whose CCF has values lower than the pre-set limiting value.

II. Setting the Task

The calculation of ACF or CCF of MSs differs merely because in the second case two different sequences are used. Hence, the calculation procedure is completely equivalent, the difference lays in the preparation of the input data. For that reason the procedure execution can be carried out despite its particular designation.

On the other hand, in this case not the particular values of CCF are to be considered, but the achieved maximum value. At the same time CCF receives relatively small number of different values. In order to facilitate the processing and discussion, and - on analogy with [4] - for the purposes of compact writing, we introduce the *spectrum of CCF*, and it means different values, included in CCF, and the number of their appearance. The developed algorithm and the program of its implementation are used to extract sets of MSs when the CCF determination is combined with the process of determining their spectrums, denoted as cross - correlation spectrums (CCS).

Therefore, in order to determine CCS we have to define the CCF of both sequences, and after that to count the number of its appearances for each received value.

During the CCF calculation, the operation of convolution is realized as multiplication of Fourier transforms of the involved sequences. For that purpose it is done within the frequency area by element-by-element multiplication of the two Fourier representations and then the CCF is found by a reverse Fourier transform.

III. Solving the Task

In order to work out the calculations in the frequency area 2 algorithms have been implemented, taking into

[1] Dept. of Electronics, Technical University of Varna 9010, Bulgaria, E-mail: dimiter_98@yahoo.com

[2] Dept. of Electronics, Technical University of Varna, 9010, Bulgaria

consideration the fact, that the length N of the MS cannot be a power of 2.

The first algorithm is implemented as a Fourier transform for compound lengths. A C-program version [6] has been used as a basis, then it has been revised considering the particular peculiarities - multiple cyclic usage of one and the same lengths, usage of one and the same algorithm for direct and reverse transform and so on. If N is non-factorable (i.e. it is a prime number) the program realizes DFT, whose number of operations is O(N^2).

Since the time of the algorithm operation increases significantly for big lengths, that are prime numbers, a version has been developed and implemented, in which a Rader method [7] is applied for DFT with a length of N (N is a prime number) by cyclic convolution for the length $N_1 = N - 1$.

As it is known [5, 6, 7], if the length N of DFT can be presented as $N = N_1 N_2$, where N_1 and N_2 are mutually prime numbers, DFT can be put down as (4):

$$y[k] = \sum_{n=0}^{N-1} x[n]\xi^{nk} \Rightarrow y[k_1 + N_1 k_2] =$$

$$= \sum_{n_2=0}^{N_2-1} \xi^{k_1 n_2} \left[\sum_{n_1=0}^{N_1-1} x[N_2 n_1 + n_2] \xi_1^{k_1 n_1} \right] \xi_2^{k_2 n_2} \,, \qquad (4)$$

where : $\xi_1 = \xi^{N_2}$ are primitive roots of unit from order N_1 and N_2; $n = N_2 n_1 + n_2$ and $k = N_1 k_2 + k_1$ can be obtained by using the algorithm for the remainders [5], that gives us the correspondence:

$$\begin{matrix} n & \Leftrightarrow & (n_1, n_2) \\ 0 \le n < N & 0 \le n_1 < N_1 & 0 \le n_2 < N_2 \end{matrix} .$$

Starting from this record, but for the non-factorable length, we observe $(\xi^k)^n$ as a sequence with a length of N, that can be put down as a series after the powers of ξ, i.e. as in (5), then the DFT is defined by the equation (6).

$$\varsigma = \{\xi^j\},\ j \in \{0, N-1\} \qquad (5)$$

$$y[k] = \sum_{n=0}^{N-1} x[n]\varsigma[kn \bmod N] \qquad (6)$$

If we choose r to be a primitive root of N, then the sequence (7) is a set of numbers $\{1, N-1\}$, i.e.:

$$\{r^0, r^1, ..., r^{N-2}\} \qquad (7)$$

In this case the sequence (5) can be reordered in (8):

$$\zeta = \{\xi^{r^k}\},\ r = \{0, N-2\}. \qquad (8)$$

Except the element 1, the sequences (5) and (8) are the same, but just reordered. If we put down:

$$n = r^{-m} \bmod N \,,\ k = r^s \bmod N \qquad (9)$$

and use the Fermat's theorem, according to which

$$r^{-m} \bmod N = r^{N-1-m} \bmod N \,, \qquad (10)$$

we can rewrite DFT as (11):

$$Y_c[s] = x[0] + (x_c[m] \otimes \zeta[s-m]) \bmod (N-1)\,, \qquad (11)$$

where $x_c[m] = x[r^{-m} \bmod N]$, $\otimes$ denotes cyclic convolution with a period $(N-1)$ and $Y_c[s] = Y[r^s \bmod N]$.

Therefore, the received in such a way $Y_c[s]$ consists of the elements of the searched $Y[k]$, but in a permuted order (sequence ζ is used for the re-arrangement). Only the value of $Y[0]$ is defined on its own by $Y[0] = \sum_0^{N-1} x[n]$.

The algorithm for DFT implementation at lengths of sequences - prime numbers is shown in Figure 1 and it has been developed following the above mentioned formulae.

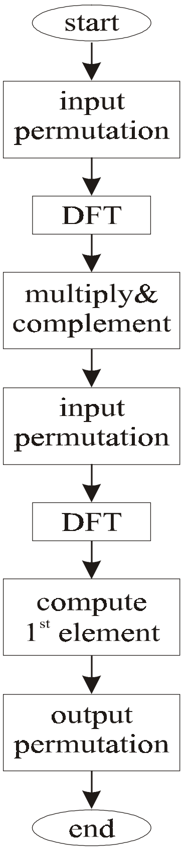

Fig.1. Prime-Factor Algorithm (PFA)

Since the purpose of our investigation is to calculate CCS of the sets of MSs, permutations of the input and output data are implemented once, not in the shown algorithms, and the received re-arrangements are used for re-addressing of the given input data, which accelerates the processing.

The particular implementation is used for finding the CCS, which allows reporting a number of specific peculiarities, such as the necessity of multiple processing of DFT of different sequences, but at the constant length. In this case the processes of factorization and re-arrangement at the input and output (that is compulsory at moving from linear to cyclic convolution and vice versa) are implemented as a common procedure to a certain extend. Figure 2 shows the designed and implemented algorithm for defining CCS.

The designed programs are included as part of a program system for defining FPGA-based generators of MS [8]. Table 1 contains the received results for the response time of a particular C++ implementation of PFA, together with those, obtained during the calculation of the same CCS but by a direct convolution, as well as by DFT.

TABLE 1
TIME FOR CALCULATING CCS

Time Length	Convolution	DFT	PFA
7	0.015873	0.015873	0.016369
15	0.015873	0.015873	
31	0.015873	0.015873	0.016369
63	0.015873	0.015873	
127	0.015873	0.016865	0.016865
255	0.016865	0.016865	
511	0.020833	0.020337	
1023	0.034226	0.022321	
2047	0.0899	0.038075	
4095	0.3	0.042512	
8191	1.18333	4.933333	0.12949
16383	4.83333	0.275	
32767	19.7333	0.616667	
65535	77.7857	1.733333	
131071	308	*	5.875

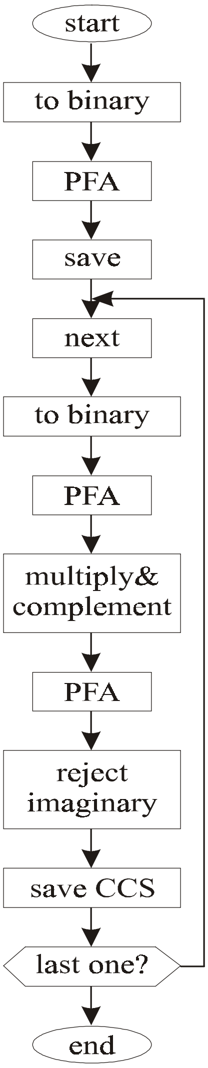

Fig.2. Cross-Correlation Spectrum Algorithm

The calculations are carried out on a computer with a Pentium IV processor, 1.8GHz, 512MB RAM. Symbol “*” denotes quite a long time (considerably increasing that in the previous column). The blank fields are for the lengths, which are not prime numbers.

IV. RESULTS

These data leads us to the conclusion that during the calculation of the mentioned MCS, the response time of the implementation (i.e. at which the calculations are carried out by the help of direct convolution) is comparable with that of the frequency one up to the lengths of $N = 2^{10} - 1 = 1023$. The times for small lengths are almost equal, which is obviously due to the implemented common auxiliary activities – data preparation, defining of the spectrum and sorting its values, file operations, etc.

The actual time for small lengths is much shorter, but it requires averaging in a great number of spectrums for its defining, and during that the number of file operations, operations of dynamic reserve and memory release increases.

V. CONCLUSION

An algorithm for DFT calculation for lengths of prime numbers has been designed and implemented. It has been applied in a designed and implemented algorithm for CCS calculation of MS sets.

The response time of the designed algorithms is compared to the results from the implementation of the same calculation operations, but with the use of convolution and DFT with an factorization of the length. The expected decrease in the time for calculation for cases in which the lengths of MS are non-factorable (prime) numbers is obtained.

The implementations are in a programming C++ language and are incorporated in the designed programming system for automated synthesizing of FPGA-based generators of MS.

REFERENCES

[1] M.I. Skolnik (editor in chief) – RADAR Handbook, 2nd edition, McGraw-Hill, Inc, 1990

[2] N. Xiang, M.R. Schroeder – Reciprocal maximum-length sequence pairs for acoustical dual source measurements, J.Acoust. Soc. Am. 109, 2001, pp.2418

[3] T. Rapparport - Wireless Communications: Principles and Practice, Prentice–Hall Inc., 1996

[4] Д.В.Сарвате, М.Б.Персли – Взаимно-корреляционные свойства псевдослучайных и родственных последовательностей, ТИИЭР, т.68, 5, 1980

[5] R. Tolimieri, M. An, Ch. Lu – Algorithms for Discrete Fourier Transform and Convolution, 2bd Ed., Springer-Verlag, New York, Inc., 1997

[6] http://hjem.get2net.dk/jjn/fft.htm

[7] H.J. Nussbaumer – Fast Fourier Transform and Convolution Algorithms, New York, Springer-Verlag, 1982

[8] Dimitar M.Kovachev - A Method for Automated Synthesis of FPGA-based Generators of Non-intersected Sets of M-sequences, IJCI Proceeding of International Conference on Signal Processing, ICSP 2003, ISSN 1304-2386, Volume 1, Number 2, Sept. 2003, pp:76-81, Canakkale, Turke