Study on Pseudorandom Sequences with Applications in Cryptography and Telecommunications

Rizomiliotis Panagiotis*

National and Kapodistrian University of Athens,
Department of Informatics and Telecommunications,
University Campus, 15784 Athens, Greece
rizop@di.uoa.gr

Abstract. Pseudorandom sequences have many applications in cryptography and spread spectrum communications. In this dissertation, on one hand we develop tools for assessing the randomness of a sequence, and on the other hand we propose new constructions of pseudorandom sequences. More precisely, we develop tools for computing the first order approximation of a binary sequence with the minimum linear complexity, we propose two efficient algorithms for computing the second order complexity (quadratic span) of a binary sequence, and we consider and solve the problem of computing the maximum nonlinear complexity (span) of a sequence. Finally, we investigate the properties of a family of sequences constructed as the direct sum of two sequences with ideal autocorrelation, like the GMW sequences.

1 Introduction

Traditionally, *pseudorandom* sequences have been employed in numerous applications, for instance in spread spectrum, code division multiple access, optical and ultrawideband communication systems, in ranging systems, global positioning systems, circuit testing and cryptography. In this dissertation we concentrate on spread spectrum communications ([11]) and cryptography ([2], [4], [9]).

Depending on the context sequences are required to possess certain properties such as long period, balance of symbols, good correlation properties and large linear and nonlinear complexity. When families of pseudorandom sequences are applied in a *code division multiple access* (CDMA) system, low crosscorrelation combats interference from other users, whereas low out–of–phase autocorrelation facilitates synchronization. Furthermore, large linear complexity protects from jamming. On the other hand, sequences with low correlation values employed in cryptosystems, like stream ciphers, are resistant to correlation attacks, while sequences with large linear span resist register synthesis attacks, like the Berlekamp-Massey Algorithm (BMA) ([8]). An informed overview in designing such sequences is given in [5].

* Prof. Nicholas Kaloupsidis was the supervisor of this thesis.

In this dissertation, on one hand we develop tools for assessing the randomness of a sequence, and on the other hand we propose new constructions of pseudorandom sequences. More precisely, we develop tools for computing the first order approximation of a binary sequence with the minimum linear complexity. Moreover, we propose for the first time two efficient algorithms for computing the second order complexity (*quadratic span*) of a binary sequence. In addition, we consider and solve the problem of computing the maximum nonlinear complexity (*span*) of a sequence (the proposed algorithm is linear with respect of the length of the sequence). Finally, we investigate the properties of a family constructed as the direct sum of two sequences with ideal autocorrelation, like the *GMW* sequences.

The dissertation is organized as follows. Chapter 1 presents an introduction on sequences and their applications. Chapter 2 establishes the necessary mathematical background needed in the sequential chapters. In Chapter 3, the linear complexity stability of a binary sequence is investigated. In Chapter 4, we propose two efficient algorithms for computing the quadratic span of a sequence. The first algorithm exploits the properties of the equivalent system of linear equations, while the second is a modification of the well known *fundamental iterative algorithm* (FIA) ([3]). In Chapter 5, an algorithm for the calculation of the span of a binary sequence is introduced, and closed form expressions connecting the cardinality of the set of binary finite sequences of the same length with their span value are presented. In Chapter 6, a family is constructed as the direct sum of two GMW sequences. This method is applicable to any pair of sequences with ideal autocorrelation. We conclude by proposing some problems that need further investigation.

2 Background

In this section we present the notation we are going to use in this abstract paper, as well as some elementary mathematical background. For more details please refer to the full version of the dissertation.

Let $\mathbb{F}_2$ be the prime field $\{0, 1\}$, and let $\mathbb{F}_2^m$ be the mth dimensional vector space over $\mathbb{F}_2$ ([7]). Consider the finite–length binary sequence $s^n = s_1, \ldots, s_n$. An m–stage *feedback shift register* (FSR) (*see* Fig. 1) with feedback function $f : \mathbb{F}_2^m \to \mathbb{F}_2$ generates s^N if and only if

$$s_{i+m} = f(s_{i+m-1}, s_{i+m-2}, \ldots, s_i) \tag{1}$$

for all $0 < i \leq N - m$. The boolean function f can be written in the so–called *algebraic normal form* (ANF) as follows

$$f(x_1, \ldots, x_m) = a_0 + a_1 x_1 + \cdots + a_m x_m + a_{1,2} x_1 x_2 + \cdots + a_{1,\ldots,m} x_1 \cdots x_m.$$

A product of k terms is said to be a kth order product. The first and the second order products are also called *linear terms* and *quadratic terms* respectively. The

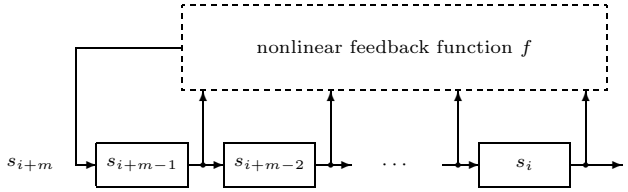

Fig. 1. The block diagram of a feedback shift register.

order of f is defined to be the maximum of the orders of the product terms appearing in the algebraic normal form with nonzero coefficients.

Definition 1. *The length of the shortest FSR having a feedback function of order k that generates s^n defines the* kth order complexity *of sequence s^n, and is denoted by $\mathcal{C}_k(s^n)$.*

Definition 2. *The length of the shortest FSR that generates s^n is called* minimum nonlinear complexity *or* span *of sequence s^n, and is given by*

$$\mathcal{SPAN}(s^n) \triangleq \min_k \{\mathcal{C}_k(s^n)\}.$$

The second order complexity of a sequence s^n is referred to as the *quadratic span* of the sequence and it is denoted by $\mathcal{QS}(s^n) \triangleq \mathcal{C}_2(s^n)$. In case the feedback function is linear and $f(0,\ldots,0) = 0$, we define the linear complexity L_s. It is clear that

$$L_s \geq \mathcal{QS}(s^n) \geq \cdots \geq \mathcal{S}_k(s^n) \geq \cdots \geq \mathcal{SPAN}(s^n).$$

Let x and y be two periodic binary sequences of period N. Their periodic crosscorrelation function is defined as

$$R_{x,y}(\tau) = \frac{1}{N}\sum_{i=0}^{N-1}(-1)^{x_i \oplus y_{i+\tau}},\ 0 \leq \tau < N.$$

When, $x = y$ the autocorrelation function is defined.

Definition 3. *Two sequences of the same period are said to be cyclically equivalent, if they are related by a left (or right) cyclic shift. Otherwise, they are cyclically distinct.*

3 First Order Approximation of Binary Sequences

Let $\boldsymbol{s}$ be a binary sequence of period $N = 2^n - 1$ and L_s its linear span. The Berlekamp–Massey algorithm needs $2L_s$ sequence digits in order to determine L_s and the linear feedback shift register (LFSR) associated to the least order homogeneous linear recursion ([8]). Therefore, the linear span is a critical index

for assessing the strength of a sequence against linear cryptanalytic attacks (such as the Berlekamp–Massey algorithm). However, even a large linear span does not ensure that a sequence is cryptographically secure. Consider the periodic extension of the length N vector $(0 \dots 01)$. This sequence has linear span N but can be approximated by the all–zero sequence with linear span 0.

In many practical applications small deviations from a given sequence can be tolerated if substantial gains in the linear span are achieved. In this context the approximate realization problem becomes relevant. Let $s = (s_0, \dots, s_{N-1})$ contain the first N elements of sequence $\boldsymbol{s}$ and e_m be a binary vector of weight 1, the single one being the mth digit, where $m \in \mathbb{Z}_N$ and $\mathbb{Z}_N = \{0, \dots, N-1\}$. Define $y_m = s + e_m$, where $+$ denotes modulo 2 addition. The approximate realization problem is equivalent to the following minimization problem

$$\mathrm{WC}_1(s) \triangleq \min_{m \in \mathbb{Z}_N} L_{y_m}. \tag{2}$$

$\mathrm{WC}_1(s)$ is known in the literature as the weight complexity of sequence $\boldsymbol{s}$ [2]. It is conceivable that the approximation problem is of interest when $\mathrm{WC}_1(s)$ is less than the linear span L_s of the original sequence. For this reason necessary conditions are provided. The optimal position $m = m^{\mathrm{opt}}$ is referred to as the *optimal shift*.

The solution of the approximate realization problem is the main subject of Chapter 3 ([12], [13]). Three methods are developed in order to determine the optimal shift, namely the sequential divisions method, the congruential equations method and the phase synchronization method. The sequential divisions method relies on the repetitive application of the Euclidean algorithm by factors of the minimal polynomial of $\boldsymbol{s}$. The congruential equations method works in the frequency domain and determines the optimal lag through a set of linear congruential equations. The solvability of these equations is analyzed and closed form expressions are derived. The phase synchronization method is based on the trace representation and builds upon cyclic equivalence in order to identify m^{opt}.

The three issues of characterization, algorithm implementation and sequence design are tightly related with the approximate realization problem. Characterization is concerned with the description of sequences $\boldsymbol{s}$ whose first–order approximations possess a given linear span. Of particular importance are those sequences for which $\mathrm{WC}_1(s) \geq L_s$. Such sequences are called *robust* because their first–order approximations do not modify their complexity performance. Directives for the design of robust sequences are proposed.

Algorithm implementation is primarily concerned with the design of efficient algorithms in order to determine $\mathrm{WC}_1(x)$, m^{opt}, $\boldsymbol{x}^{(1)}$ and $f^{(1)}(z)$. An algorithm following a decoding approach is given in [2] for determining the optimal shift but its complexity is high. Furthermore, it does not provide any insight to the design of binary sequences which are robust to such approximation attacks. High level algorithm organizations for the proposed schemes are presented.

4 On the Quadratic Span of Binary Sequences

In Chapter 4, we investigate the quadratic span of finite binary sequences ([14], [15]). In [1], the quadratic span of the de Bruijn sequences was studied, and a partial generalization of the Berlekamp–Massey algorithm, based on Gaussian elimination, was proposed. Two more efficient algorithm for calculating the quadratic span of a sequence are described in this chapter.

The first one takes advantage of the special structure of the corresponding linear systems of equations. Let $E(n,m) = (s_{m+1} \ \cdots \ s_n)^T$, and let $q(n)$ be the quadratic span of the s^n. In connection with the algebraic normal form we introduce the vector

$$F(m) = \left(a_1 \ a_2 \ a_1a_2 \ \cdots \ a_m \ a_{m-1,m} \ \cdots \ a_{1,m}\right)^T \tag{3}$$

which contains the coefficients of the unknown quadratic feedback function f. From (1), the calculation of a quadratic feedback function that generates a given sequence s^n is equivalent to solving the system of linear equations

$$M(n,m) \cdot F(m) = E(n,m) \tag{4}$$

where $M(n,m)$ is the $(n-m) \times m(m+1)/2$ matrix

$$M(n,m) = \begin{pmatrix} s_1 & \cdots & s_m & \cdots & s_1s_m \\ s_2 & \cdots & s_{m+1} & \cdots & s_2s_{m+1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ s_{n-m} & \cdots & s_{n-1} & \cdots & s_{n-m}s_{n-1} \end{pmatrix}.$$

Based on the following Theorems, we developed an iterative algorithm that computes the quadratic span of a finite binary sequence.

Theorem 1. *Let $d \geq q(n)$ be the greatest integer such that*

$$rank\,(M(n+1,d)) = rank\,(M(n,d)).$$

Then

$$q(n+1) = \begin{cases} q(n) & \text{if } rank\,(M(n+1,d)) = \\ & rank\,(M(n+1,d) \ E(n+1,d)), \\ d+1 & \text{otherwise.} \end{cases}$$

Theorem 2. *Let $q(n+1) = q(n) + \delta$, where $\delta > 0$. Then it holds $q(n+2+i) = q(n+1)$, for all $i \in [0, \delta - 1]$.*

After the computation of the quadratic span, we solve the system of linear equations (4), in order to find the feedback function of the corresponding FSR.

The second algorithm is a modified version of the *fundamental iterative algorithm* (FIA). FIA was introduced in [3] for solving the multi-sequence shift–register synthesis problem. The goal of the algorithm is to find the smallest initial set of columns, in a given matrix, which are linearly independent.

5 Results on the Nonlinear Span of Binary Sequences

The span was studied by Jansen and Boekee ([6]). We proved similar results using a different viewpoint, based on the special properties of the corresponding system of linear equations. An efficient algorithm was also introduced for computing the span and a feedback function that generates the given finite binary sequence. Finally, the properties of the cardinality of the set of finite sequences with the same span were studied. The results of Chapter 5 appear in [14], and [15].

Let $sp(n)$ denote the span of s^n and $E(n,m) = \left(s_{m+1} \cdots s_n\right)^T$. From (1), the calculation of a feedback function that generates a given sequence s^n is equivalent to solving the system of linear equations

$$M(n,m) \cdot F(m) = E(n,m) \tag{5}$$

where $M(n,m)$ is the $(n-m) \times 2^m$ matrix

$$M(N,m) = \left(\mathbf{1}_{n-m}^T \mid LP(n,m) \mid NLP(n,m)\right).$$

$\mathbf{1}_{n-m}$ denotes the all-one vector of length $n-m$ and the matrix $LP(n,m)$ consists of subsequences of s^n

$$LP(n,m) = \begin{pmatrix} s_1 & s_2 & \cdots & s_m \\ s_2 & s_3 & \cdots & s_{m+1} \\ \vdots & & \vdots & \\ s_{n-m} & s_{n-m+1} & \cdots & s_{n-1} \end{pmatrix}$$

while $NLP(n,m)$ consists of all termwise product combinations of the columns of $LP(n,m)$. $F(m)$ contains the coefficients of the unknown feedback function f written in the ANF.

Our analysis is based on the block structure of $M(n,m)$. The algorithm is divided in two steps. First we compute the span $sp(n)$ of the sequence, and then a feedback function of $sp(n)$ variables that produces the given finite binary sequence.

The computation of the span is performed by processing the sequence element by element. The following two Theorems describe the way the value of the span changes.

Theorem 3. *$sp(n) > sp(n-1)$ if and only if there is an integer $1 \leq j \leq n-1-sp(n-1)$, such that*

$$R_{n-sp(n-1)}(n, sp(n-1)) = R_j(n, sp(n-1)) \text{ and}$$
$$s_n \neq s_{j+sp(n-1)}.$$

where $R_j(n,m)$ denotes the jth row of $M(n,m)$.

Theorem 4. *If $sp(n) > sp(n-1)$, then $sp(n) = sp(n-1) + \delta$, where $\delta = n+1-sp(n-1)-r$ and $r+1$ is the index of the first linear dependent row of $M(n, sp(n-1))$.*

In order to compute a boolean feedback function of $sp(n)$ variables that generates the sequence, we have to solve the system (1). Due to the special structure of $M(n,m)$, the 2^m possible different rows of the matrix form a base $B(m)$ of $GF(2)^{2^m}$ over $GF(2)$, which can always be written as a lower triangular matrix. Thus, using appropriate outputs of the span algorithm, we show that the system (5) can be easily reduced to a low triangular system of $r = rank(M(n, sp(n)))$ equations and variables that can be easily solved by back substitution. The other $2^{sp(n)} - r$ variables of $F(sp(n))$ that do not appear in the reduced system are set equal to zero.

The system of linear equations (5) has $2^{sp(n)} - r$ degrees of freedom. Thus, there are $2^{2^{sp(n)}-r}$ functions with $sp(n)$ variables that can produce the same sequence s^n. In the case of periodic sequences of period L, it holds $r = L$.

Finally, we study the cardinality of $Z(n, SP)$, the set of binary sequences of length n with span SP, as n varies. The main results on the span distribution follow. Let $\delta > 0$.

1. $|Z(2^{SP} + SP + \delta, SP)| = |Z(2^{SP} + SP, SP)|$.
2. $|Z(n + \delta, \frac{n}{2} + \delta)| = |Z(n, \frac{n}{2})|$, for n even.

6 Construction of Sequences with four-valued Autocorrelation from GMW Sequences

One of the most important families of pseudorandom sequences are Gordon, Mills, Welch (GMW) sequences ([10]). The GMW sequences and their generalization called *cascaded GMW sequences* have been extensively studied in the literature.

In Chapter 6, we describe the construction of a large class of balanced binary sequences with four–valued autocorrelation function. Binary sequences with good autocorrelation properties play an important role in communication systems employing phase–reversal modulation techniques. The construction is based on the modulo 2 addition of two GMW sequences with relatively prime periods. The resulting sequences have period equal to the product of the periods. Additionally, other characteristics of the class members, such as the linear span and the periodic crosscorrelation, are investigated ([18]).

Definition 4 ([10]). *Let n, k be two integers such that $n = lk$, and r be an integer in the range $0 < r < 2^k - 1$ relatively prime to $2^k - 1$. Consider the binary sequence $x = \{x_i\}_{i \geq 0}$ given by*

$$x_i = \mathrm{tr}_1^k \left(\left[\mathrm{tr}_k^n(\alpha^{ti}) \right]^r \right) \tag{6}$$

where α is a primitive element of $\mathbb{F}_{2^n}$, and t is an integer in the range $0 < t < 2^n - 1$ relatively prime to $2^n - 1$. Then, x is a GMW sequence.

The above definition implies that GMW sequences are periodic with least period $N = 2^n - 1$. Some of the properties of a GMW sequence x are the following [10]:

i. The sequence x has the *ideal autocorrelation* property

$$R_x(\tau) = \begin{cases} 1 & \text{if } \tau \equiv 0 \pmod{N}, \\ -1/N & \text{otherwise.} \end{cases} \tag{7}$$

ii. Sequence x is balanced.

iii. The total number of cyclically distinct GMW sequences of period $N = 2^n - 1$ is

$$N_{\text{GMW}}^n = \frac{\varphi(2^n - 1)}{n} \sum_{k|n} \frac{\varphi(2^k - 1)}{k} \tag{8}$$

where the summation is over all divisors k of n and $\varphi(\cdot)$ denotes the Euler's totient function.

We present a new approach for the calculation of the periodic crosscorrelation function of two GMW sequences whose least periods are different. In accordance with the above analysis we assume that these sequences, say $x = \{x_i\}_{i\geq 0}$ and $y = \{y_i\}_{i\geq 0}$, are given by

$$x_i = \text{tr}_1^{k_1}\left(\left[\text{tr}_{k_1}^{n_1}(\alpha^{m_1}\alpha^{t_1 i})\right]^{r_1}\right) \tag{9}$$

and

$$y_i = \text{tr}_1^{k_2}\left(\left[\text{tr}_{k_2}^{n_2}(\beta^{m_2}\beta^{t_2 i})\right]^{r_2}\right) \tag{10}$$

where the field elements α and β are primitive elements of $\mathbb{F}_{2^{n_1}}$ and $\mathbb{F}_{2^{n_2}}$ respectively. Let us assume that the integer t_1 (resp. t_2) is relatively prime to $N_1 = 2^{n_1} - 1$ (resp. $N_2 = 2^{n_2} - 1$). Then, sequence x (resp. y) has least period N_1 (resp. N_2). Let us denote by d the greatest common divisor of N_1 and N_2, and let $N = \text{lcm}(N_1, N_2) = N_1 N_2/d$.

We prove that their crosscorrelation function becomes

$$R_{x,y}(\tau) = \frac{1}{d}\sum_{c_3=0}^{d-1} \widehat{\mathfrak{X}}_{c_3}\widehat{\mathfrak{y}}_{c_3+\tau} = R_{\widehat{\mathfrak{X}},\widehat{\mathfrak{y}}}(\tau \bmod d) \tag{11}$$

where the sequence $\widehat{\mathfrak{X}}$ and $\widehat{\mathfrak{y}}$ correspond to the autocorrelation of a special decimation of x and y respectively. Of special interest is the case $d = 1$, where we get $R_{x,y}(\tau) = 1/N$ for all integers $\tau \in \mathbb{Z}_N$.

Next, we examine the properties of binary sequences constructed by the modulo 2 addition of two GMW sequences whose least periods are different.

Define the sequence $w = \{w_i\}_{i\geq 0}$ which is given by $w_i = x_i \oplus y_i$, where the sequences $x = \{x_i\}_{i\geq 0}$ and $y = \{y_i\}_{i\geq 0}$ are defined in (9) and (10) respectively. We proved the following theorem

Theorem 5. *The spectrum of the autocorrelation function R_w of sequence w, defined as described above, is given by*

$$R_w(\tau) = \begin{cases} 1 & \text{if } \tau \equiv 0 \pmod{N}, \\ -1/N_1 & \text{if } \tau \equiv 0 \pmod{N_2}, \\ -1/N_2 & \text{if } \tau \equiv 0 \pmod{N_1}, \\ R_{\widehat{\mathfrak{X}}(\tau),\widehat{\mathfrak{y}}(\tau)}(0) & \text{otherwise.} \end{cases}$$

Of special interest is the case where the component GMW sequences have relative prime periods, i.e. $d = 1$. We introduce the sets G_1 and G_2 which contain all cyclically distinct GMW sequences with periods $N_1 = 2^{n_1}-1$ and $N_2 = 2^{n_2}-1$ respectively, and the set

$$G = \{x \oplus T^i y |\ x \in G_1 \text{ and } y \in G_2, \text{ for all } i \text{ with } 0 \le i < \min\{N_1, N_2\}\}$$

where $\gcd(N_1, N_2) = 1$. Recall that $|G_i| = N_{\mathrm{GMW}}^{n_i}$ for $i = 1, 2$. Clearly,

$$|G| = |G_1| \cdot |G_2| \cdot \min\{N_1, N_2\}.$$

Corollary 1. *The spectrum of the autocorrelation function R_w of sequence $w \in G$ is four–valued and is given by*

$$R_w(\tau) = \begin{cases} 1 & \text{if } \tau \equiv 0 \pmod{N}, \\ -1/N_1 & \text{if } \tau \equiv 0 \pmod{N_2}, \\ -1/N_2 & \text{if } \tau \equiv 0 \pmod{N_1}, \\ 1/N & \text{otherwise,} \end{cases}$$

where $N = N_1 N_2$. Moreover, the value 1 occurs one time, $-1/N_1$ occurs $N_1 - 1$ times, $-1/N_2$ occurs $N_2 - 1$ times and $1/N$ occurs $N - N_1 - N_2 + 1$ times.

The linear span of a sequence $w \in G$ depends on its component sequences $x \in G_1$ and $y \in G_2$ as the following Lemma indicates.

Lemma 1. *Let $w = x \in G$. Then,*

$$L_w = L_x + L_y. \tag{12}$$

Finally we compute the crosscorrelation function of two members of the family G. The above results can be easily extended in the case of any family of sequences with ideal autocorrelation.

References

1. A. H. Chan and R. A. Games, "On the quadratic spans of de Bruijn sequences," *IEEE Trans. Inform. Theory*, vol. IT–36, pp. 822–829, Jul. 1990.
2. T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory.* North–Holland Mathematical Library. Elsevier Science, 1998.

3. G.-L. Feng and K. K. Tzeng, "A generalization of the Berlekamp–Massey algorithm for multisequence shift–register synthesis with applications to decoding cyclic codes," *IEEE Trans. Inform. Theory*, vol. IT–37, pp. 1274–1287, Sep. 1991.
4. S. W. Golomb, *Shift Register Sequences*. Holden–Day, San Francisco, 1967.
5. T. Helleseth and V. J. Kumar, "Sequences with low correlation, correlation functions of geometric sequences," *in Handbook of Coding Theory*, V. Pless and C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998.
6. C. J. Jansen and D. E. Boekee, "The shortest feedback shift register that can generate a given sequence," in *Proc. Advances in Cryptology–CRYPTO '89*, pp. 90–99, 1990.
7. R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1996, 2nd ed.
8. J. L. Massey, "Shift register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT–15, pp. 122–127, Jan. 1969.
9. A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.
10. R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Transactions on Information Theory*, vol. IT–30, pp. 548–553, May 1984.
11. M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. McGraw–Hill, 1994, Revised ed.
12. N. Kolokotronis, P. Rizomiliotis, and N. Kalouptsidis, "First–order optimal approximation of binary sequences," in *Proc. Conference on Sequences and Their Applications*, T. Helleseth, P. V. Kumar, and K. Yang (Eds). Springer-Verlag. Series in Discrete Mathematics and Theoretical Computer Science, pp. 242-256, May 2001.
13. N. Kolokotronis, P. Rizomiliotis, and N. Kalouptsidis, "Minimum linear span approximation of binary sequences," *IEEE Transactions on Information Theory*, vol. IT–48, pp. 2758–2764, Oct. 2002.
14. P. Rizomiliotis, N. Kolokotronis, and N. Kalouptsidis, "On the Quadratic Span of Binary Sequences," in *Proc. IEEE Inter. Symp. on Inform. Theory*, pp. 377, 2003.
15. P. Rizomiliotis, N. Kolokotronis, and N. Kalouptsidis, "On the Quadratic Span of Binary Sequences," *IEEE Transactions on Information Theory*, vol. IT–51, pp. 1840–1848, May 2005.
16. P. Rizomiliotis, and N. Kalouptsidis, "Result on the nonlinear span of binary sequences," in *Proc. IEEE Inter. Symp. on Inform. Theory*, pp. 124, 2004.
17. P. Rizomiliotis, and N. Kalouptsidis, "Results on the nonlinear span of binary sequences," *IEEE Transactions on Information Theory*, vol. IT–51, pp. 1555–1563, April 2005.
18. P. Rizomiliotis, N. Kolokotronis, and N. Kalouptsidis, "Construction of sequences with four–valued autocorrelation from GMW sequences," in *Proc. IEEE Inter. Symp. on Inform. Theory*, pp. 183, 2002.