# Application of Groebner bases techniques for searching new sequences with good periodic correlation properties

Vitaly V. Shorin and Pierre Loidreau
Laboratoire de mathématiques appliquées
Ecole Nationale Supérieure de Techniques avancées
32 bd Victor, 75739 Paris, France

***Abstract*— The Groebner basis calculation algorithms were successfully applied to construct new sequences analytically. New unimodular perfect sequences with $6$ phases were proposed for various sequence lengths.**

**For perfect root-of-unity sequences and for binary sequences with ideal autocorrelation this new approach was used to find sequences analytically. Although this approach was not able to find previously unknown sequences in both cases, it is still better than any other analytical method and almost on par with exhaustive search.**

## I. Introduction

Sequences with good periodic correlation properties with unit magnitude have been extensively studied since the middle of the twentieth century. They have been adopted widely in numerous applications such as a linear system parameter identification, real-time channel evaluation, fast synchronization, source coding, timing measurements, constant-wave radars and two-dimensional processing.

There are three kinds of such sequences that attract a lot of interest: unimodular perfect sequences (UPS), perfect root-of-unity sequences (PRUS, a subclass of UPS), and binary sequences with ideal autocorrelation (BSIA). Constructions for UPS of square-free length can be found in ([2], [3], [6], [12], [13], [11], [5], [1], [4], [7]). A very general construction for PRUS can be found in ([9]). Also in that paper the results of exhaustive search were presented, namely, there is no other PRUS sequence exists for $N \leq 15,\ L \leq 20,$ and $N^L \leq 11^{11}$. There is a recent survey on BSIA and related sequences ([14]). A full classification of BSIA of length $2^{10}-1$ is presented in ([29]).

In order to construct unimodular perfect sequences, in ([1], [4]) it was proposed to choose sequence components from alphabet with very small size, to rewrite autocorrelation properties (2) as a polynomial system and to solve it using resultants. However in practice this system has been solved only for $3$ (in some cases for $4$) different unknown phases. This is due to double exponential (in number of variables) complexity of multivariate resultant algorithms.

Among all available methods for solving polynomial systems, computation of Groebner bases remains one of the most powerful. Historically, the Buchberger algorithm ([15], [16]) was the first algorithm for computing Groebner bases. Recently, new very efficient algorithms $F_4$ ([20]) and $F_5$ ([21]) were proposed. These algorithms were successfully applied to many problems, including cryptanalysis of LFSR-based stream ciphers and HFE cryptosystem ([19] and [18], resp.), decoding cyclic codes beyond the correction capacity ([17]), and many others.

There was an attempt to represent autocorrelation properties as a polynomial system. This approach is referred to as "Cyclic-N" problem ([23], [24], [22]). This problem is considered to be very hard. The biggest $N$ for which Groebner basis was calculated is $10$ ([21]). On computer algebra system and hardware been used only the Cyclic-7 problem can be solved.

The purpose of this work is to apply recent results on Groebner bases computations to construct new sequences with good autocorrelation properties. Two different constructions are used for unimodular perfect sequences: for lengths $n = p = 5f+1$ and $n = p_1p_2 = (4Q+3)(4P+1)$, where $p, p_1, p_2$ are prime numbers and $f, P, Q$ are integers. For $n = p_1p_2$, a new family of sequences is constructed and a direct formulae is obtained. For perfect root-of-unity sequences and for ideal binary sequences we determined the maximum length of the sequence that can be obtained via Groebner bases approach.

All computations were performed using 32-bit version of Magma software ([25]) running on dual Opteron $2.4$ GHz server with $4$ Gb of available memory. Most of the results cannot be presented in the paper due to the space limitation. Instead, the sizes of the Groebner bases as well as time and memory required for computation are presented.

## II. Preliminaries

### A. Definitions

Let $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ be a complex valued sequence of length $n$ containing at least one non-zero component. The periodic autocorrelation function (PAF) of $\mathbf{x}$ is defined by

$$R_{\mathbf{x}}(\tau) = \sum_{s=0}^{n-1} x_s x_{s+\tau}^*,\ \tau = 0, 1, \ldots, n-1, \qquad (1)$$

where all indices are calculated $\pmod n$ and $x^*$ denotes the complex conjugation of $x$.

A sequence $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ is called a **perfect** sequence if and only if all the out-of-phase autocorrelation coefficients are equal to 0, i.e.

$$R_{\mathbf{x}}(\tau) = \sum_{s=0}^{n-1} x_s x_{s+\tau}^* = 0, \ \tau = 1, \ldots, n-1. \tag{2}$$

The sequence $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ is called a **phase shift keyed** (PSK), or a **polyphase**, or a **unimodular** sequence if all the components of the sequence are unimodular (lie on the unit circle):

$$|x_i| = 1, \quad i = 0, \ldots, n-1. \tag{3}$$

If all the components are roots of unity of some degree, then the sequence is called a **polyphase**, or a **root-of-unity** sequence. In this paper the terms **unimodular** and **root-of-unity** are used in order to avoid ambiguity.

If all components of the sequence are roots of unity of degree 2, i.e. are equal to $\pm 1$, then the sequence is called **binary**. Perfect binary sequences would receive a lot of applications, particularly in communications, but so far only one such sequence is known: $\{1, 1, 1, -1\}$. The best autocorrelation property that can be attained by binary sequences of length $n > 4$ is so-called **ideal** autocorrelation:

$$R_{\mathbf{x}}(\tau) = \sum_{s=0}^{n-1} x_s x_{s+\tau}^* \equiv \sum_{s=0}^{n-1} x_s x_{s+\tau} = -1, \ \tau = 1, \ldots, n-1, \tag{4}$$

and only for $n \equiv 3 \bmod 4$.

This paper uses Groebner Bases calculation algorithm only as a "black box". All the definitions can be found in ([26]). Only two properties will be used. First, Groebner basis of the original polynomial system has exactly the same solution as original system has. Second, if one calculate the Groebner basis with respect to lexicografic order ($x_0 > x_1 > x_2 > \ldots > x_{n-1}$) , and the system is known to have only finitely many solutions, then the last polynomial of the basis will be of only one variable ($x_{n-1}$), previous one polynomial or several polynomials — of two variables $x_{n-1}, x_{n-2}$, and so forth. This trianglular form of Groebner basis makes the computation of the solution very easy. In fact, Groebner basis can be considered as an exact solution, given in terms of algebraic numbers.

## III. Unimodular perfect sequences

### A. Construction method

Similarly to [1], [4], [7], [8], the algebraic methods for polynomial system solving will be used. Instead of using resultants, as it was in [1], [4], [7], the Groebner bases technique will be utilized. Thus it will be possible to overcome experimental limitation of 4 variables, that was found to be the most significant issue with resultant-based approach.

We interpret the autocorrelation properties (2) together with unimodularity (3) as a system of equations. All the solutions of the system are (probably new) unimodular perfect sequences. We will solve the system by converting it into system of polynomial equations, and then to apply polynomial system solving techniques, like Groebner Bases computation. The system can be converted but new roots will appear (for example, restriction $|x_i| = 1$ cannot be expressed as a polynomial equation), that may affect the performance of polynomial system solving method. In some cases, we may receive an algebraic system with infinite number of solutions from original non-algebraic system which has only finitely many solutions.

Three different options were considered:

1) $x_i^* = 1/x_i$,
2) $y_i = x_i^*$, $x_i y_i - 1 = 0$,
3) $y_i = x_i x_{i+1}^*$.

It turns out that the first option requires least amount of memory to compute Groebner bases, so it was used throughout the paper.

In order to compose a sequence out of few different phases, the following two experiment-based conjectures are used:

*Conjecture 1:* Any unimodular perfect sequence of prime length $p$ is equivalent to the sequence:

$$x_i = z_k, \quad i \in G_k, \quad k = -\infty, 0, \ldots, e-1, \tag{5}$$

where $p = ef + 1$, $(G_{-\infty}, G_0, \ldots, G_{e-1})$ — Gaussian cyclotomic classes for $p$. For convenience, one can denote $G_{-\infty} = \{0\}$. The sequence contains $e$ different values $z_k$, plus one more value $x_0 = 1$.

*Conjecture 2:* Any unimodular perfect sequence of length $p_1 p_2$, where $p_1, p_2$ are different primes, is equivalent to the sequence:

$$x_i \equiv x_{i_1, i_2} = z_{k_1, k_2}, \ \ i_1 \in G_{k_1}^{(1)}, i_2 \in G_{k_2}^{(2)}, \tag{6}$$

where $p_1 = e_1 f_1 + 1, p_2 = e_2 f_2 + 1$, $i_1 = i \bmod p_1$, $i_2 = i \bmod p_2$, $(G_0^{(1)}, \ldots, G_{e_1-1}^{(1)})$ and $(G_0^{(2)}, \ldots, G_{e_2-1}^{(2)})$ — Gaussian cyclotomic classes for $p_1$ and $p_2$, respectively. Here $G_{-\infty}^{(1)} = G_{-\infty}^{(2)} = \{0\}$ is denoted for consistency. The sequence contains $e_1 e_2 + e_1 + e_2$ different values $z_{k_1, k_2}$, plus one more value $x_0 = z_{-\infty, -\infty} = 1$.

After substitution of variables, the following steps should be undertaken.

1) Calculation of Groebner basis in lexicografic ordering.
2) Sequencial elimination process (Chapter 3 of [26]) yields union of triangular polynomial systems that have exactly the same roots as the original system.
3) Subsystems that do not have unimodular roots should be removed from the union.

Thus the set of polynomial systems can be obtained, each of them being very easy to solve. This set of systems can be considered as an analytical solution to our problem.

### B. $n = p = ef + 1$, *prime* $p$, $e = 4$, 5 *phases*

In this case, we use the template as in the Conjecture 1. The alphabet $\{1, x_0, x_1, x_2, x_3\}$ will be used to construct sequences. For example, a template for sequence of length $29 = 4 \times 7 + 1$ is as follows: $x = (1, x_0, x_1, x_1, x_2, x_2, x_2, x_0, x_3, x_2, x_3, x_1, x_3, x_2, x_1, x_3, x_0, x_1, x_3, x_1, x_0, x_1, x_2, x_0, x_0, x_0, x_3, x_3, x_2)$. Previously ([1]) the sequence of length $13 = 4 * 3 + 1$ of this type was

constructed using resultants approach. That required several days of computations on Athlon-1000. With Groebner basis approach, now it requires a few seconds and several Megabytes of memory.

The lexicografic ordering $x_0 < x_1 < x_2 < x_3$ was chosen. For every $f$ that was tried, it were found that solution consisted of two systems. Solution that is defined by the first system is already known ([10]) and the second system has a polynomial of degree $48$ in variable $x_0$. All other polynomials are in the from $x_i = F_i(x_0)$ for some polynomials $F_i(x)$. The polynomial of degree $48$ has $4$ unimodular solutions, thus there are two non-equivalent sequences. Please note that complementary roots of this polynomial yield equivalent sequences.

The experimental results for memory required, calculation time and Groebner basis size are summarized in Table I.

### C. $n = p = ef + 1$, *prime* $p$, $e = 5$, $6$ *phases*

In this case, we use the template as in the Conjecture 1. The alphabet $\{1, x_0, x_1, x_2, x_3, x_4\}$ will be used to construct sequences. There were no previously known sequences of this type.

The lexicografic ordering $x_0 < x_1 < x_2 < x_3 < x_4$ was chosen. For every $f$ that was tried, it were found that solution is a single system. The system has a polynomial of degree $150$ in variable $x_0$. All other polynomials are in the from $x_i = F_i(x_0)$ for some polynomials $F_i(x)$. The polynomial of degree $150$ has $40$ unimodular solutions, thus there are $20$ non-equivalent sequences.

The experimental results for memory required, calculation time and Groebner basis size are summarized in Table I.

### D. *Case* $n = p_1 p_2$, $p_1 = 4Q + 3$, $p_2 = 4P + 3$, $6$ *different phases*

The case of 4-phased unimodular perfect sequences of length $n = 3p$ and $n = p_1 p_2$, $p, p_1, p_2 \equiv 3 \bmod 4$, were considered in ([4], [7]). The sequences had alphabet $\{1, a, d, e\}$. We will use more general template, with alphabet $\{1, a, b, c, d, e\}$. The particular case of this constructions for $Q = 0$, $n = 3p$ was considered in ([8]).

We create template according to conjecture 2. Gaussian cyclotomic classes for $p_1$ and $p_2$ for $e_1 = e_2 = 2$ coinside with sets of quadratic residues and non-residues modulo $p_1$ and $p_2$. According to conjecture 2, the template should have $8$ different variables. We will use a template with reduced number of variables. It should be noticed that at least two different sequences satisfy this template: CRT-sequence constructed from two-phase sequences of length $p_1$ and $p_2$, and . The alphabet is as follows:

$$z_{-\infty,-\infty} = z_{0,-\infty} = 1, \quad z_{1,-\infty} = d,$$
$$z_{-\infty,0} = z_{0,0} = e, \quad z_{1,0} = a,$$
$$z_{-\infty,1} = z_{0,1} = b, \quad z_{1,1} = c.$$

For example, let us consider a sequence of length $n = 77 = 7{\times}11 = (1{\times}4{+}3)(2{\times}4{+}3)$. The quadratic residues sets $\Gamma_1 = \{1 = 1^2 = 6^2, 4 = 2^2 = 5^2, 2 = 3^2 = 4^2\} = \{1, 2, 4\}$ and $\Gamma_2 = \{1 = 1^2 = 10^2, 4 = 2^2 = 9^2, 9 = 3^2 = 8^2, 5 = 4^2 = 7^2, 3 = 5^2 = 6^2\} = \{1, 3, 4, 5, 9\}$. The matrix representation is as follows:

$$\mathbf{x} = \begin{bmatrix} 1 & e & b & e & e & e & b & b & b & e & b \\ 1 & e & b & e & e & e & b & b & b & e & b \\ 1 & e & b & e & e & e & b & b & b & e & b \\ d & a & c & a & a & a & c & c & c & a & c \\ 1 & e & b & e & e & e & b & b & b & e & b \\ d & a & c & a & a & a & c & c & c & a & c \\ d & a & c & a & a & a & c & c & c & a & c \end{bmatrix}, \quad (7)$$

and the corresponding 6-phase sequence is as follows: $x = (1, e, b, a, e, a, c, b, b, e, c, 1, a, c, e, e, e, c, b, c, a, b, 1, e, c, e, a, a, b, b, b, a, b, d, a, b, e, e, a, b, c, c, e, b, 1, a, b, a, a, e, b, b, c, e, c, d, e, b, e, a, e, c, c, b, e, b, d, e, c, a, e, e, b, c, b, a, c)$.

It turns out that for every $p_1$ and $p_2$ autocorrelation properties yield only $5$ different equations with $5$ variables. Coefficients of the equations depend on parameters $P$ and $Q$:

$$\begin{cases} 2P(4Q+3)ecbad + 2(Q+1)(Pb^2cad + (P+1)e^2cad) + \\ +(2Q+1)((P+1)a^2ebd + Pc^2ebd) + \\ +2(Q+1)(cbad + ecb^2ad) + (2Q+1)(c^2eba + d^2ecb) = 0, \\ (4P+3)(2Q+1)ecbad + (Q+1)(ecba + ecbad^2) + \\ +(Q+1)(2P+1)(b^2ead + a^2cbd + c^2ead + e^2cbd) = 0, \\ 2P(4Q+3)ecbad + 2(Q+1)((P+1)b^2cad + Pe^2cad) + \\ +(2Q+1)(Pa^2ebd + (P+1)c^2ebd) + \\ +(2Q+1)(d^2eba + a^2ecb) + 2(Q+1)(ecad + e^2cbad) = 0, \\ 2P(2Q+1)ecbad + (P+1)(Q)c^2ebd + \\ +P(Q+1)(b^2ead + a^2cbd + c^2ead + a^2ecd) + \\ +P(Q+1)(e^2cad + e^2cbd + e^2bad) + \\ +Q(d^2eba + a^2ecb) + \\ +(P+1)(Q+1)(b^2ecd + c^2bad + b^2cad) + \\ +PQa^2ebd + (Q+1)(ebad + ecad) + \\ +(Q+1)(ecba^2d + e^2cbad + e^2cba + d^2eca) = 0, \\ 2P(2Q+1)ecbad + Q((P+1)a^2ebd + c^2eba + d^2ecb) + \\ +P(Q+1)(b^2cad + b^2ead + b^2ecd) + \\ +P(Q+1)(a^2cbd + c^2ead + e^2cbd + c^2bad) + \\ +(P+1)(Q+1)(e^2bad + a^2ecd + e^2cad) + \\ +(Q+1)(cbad + ecbd) + PQc^2ebd + \\ +(Q+1)(b^2eca + d^2cba + ecb^2ad + ec^2bad) = 0. \end{cases} \quad (8)$$

The lexicografic ordering $a > b > c > e > d$ was chosen since it is easy to classify solutions according to polynomial in variable $d$. Several solutions of this system are already known (for every suitable $P$ and $Q$), namely, two CRT-constructions (the last polynomial is $d^2 + \frac{2Q+1}{Q+1}d + 1$) and two 4-phase sequence ([7]). For every parameters $P$ and $Q$ that was tried, 2 new solutions were found, namely, they contain irreducible over $\mathbb{Q}$ polynomials of degree 2 and 52 in variable $d$, respectively. Each of the two systems yields $4$ non-equivalent unimodular perfect sequences.

The experimental results for memory required, calculation time and Groebner basis size are summarized in Table I.

### E. *Infinite family of sequences $n = p_1 p_2$, $p_1 = 4Q + 3$, $p_2 = 4P + 3$, 6 different phases*

Now we are going to present an infinite family of unimodular perfect sequences of length $n = p_1 p_2$, where $p_1, p_2 \equiv 3 \bmod 4$ — any different primes. It was mentioned that one of particular solutions has a very simple polynomial of degree 2 in $d$:

$$d^2 + 2\frac{p_1 - p_2}{p_1 + p_2} d + 1. \tag{9}$$

By adding this polynomial to autocorrelation equation system (8) for every given $p_1$ and $p_2$, the Groebner bases calculation speed increases significantly, and a resulting Groebner basis is as follows:

$$\begin{cases} a - A(e,d), \\ b - B(e,d), \\ c - C(e,d), \\ e^4 + \frac{4P+2Q+5}{4(P+1)(Q+1)} e^3 d - \frac{4P+2Q+5}{4(P+1)(Q+1)} e^3 + \\ + \frac{(16(2Q^2-1)P^2 + (-56-48Q+64Q^2+32Q^3)P - (51+96Q+36Q^2))e^2 d}{8(2(P+1)^2+(P+1)(2Q+1))(Q+1)^2} - \\ - \frac{(8P^2-(20Q+2)P-(12Q^2+36Q+15))}{4(Q+1)(P+1)(2(P+1)+(2Q+1))} ed + \frac{4P+2Q+5}{4(P+1)(Q+1)} e + \\ + \frac{2(4P-4Q)}{(4P+4Q+6} d - 1, \\ d^2 + 2\frac{p_1-p_2}{p_1+p_2} d + 1, \end{cases} \tag{10}$$

where $A(e,d)$, $B(e,d)$, $C(e,d)$ are polynomials of total degree 4 in $e$ and $d$ with coefficients depending on $P, Q$. These polynomials are not placed here due to space limitation.

After finding the partial solution of the system (8) one should prove that all the values are unimodular. The following criterion is used: $|y| = 1 \Leftrightarrow \{(y + 1/y)/2 \in \mathbb{R}\ and\ |(y + 1/y)/2| \leq 1\}$. It is easy to see that it holds for variable $d$. In order to prove unimodularity for other variables, one can compute Groebner basis of (8) plus (9) with coefficients in univariate rational function field over integer ring. The following lexicografic orders should be used: $(a > b > c > d > e)$, $(a > b > d > e > c)$, $(a > c > d > e > b)$, $(b > c > d > e > a)$. In each of the Groebner basis attained, the last polynomial is of degree 8 in one variable, $e, c, b, a$, respectively with coefficients being rational functions in parameters $P$ and $Q$. The proof is quite technical and is omitted here.

So for every $P$ and $Q$ such that $4P+3$ and $4Q+3$ are different primes, there exists 4 previously unknown inequivalent sequences of length $(4P + 3)(4Q + 3)$, each is composed of roots of polynomials of degree 8.

## IV. Perfect root-of-unity sequences

For root-of-unity sequences ($x_i^n = 1 \quad \forall i$), it is possible to express perfect autocorrelation properties as an algebraic equations. Indeed, $x_i^* = x_i^{n-1}$. In addition, unimodularity properties are implicitly present via root-of-unity restriction, $x_i^n = 1$. So there will be no parasite particular solutions.

In order to slightly simplify construction of PRUS, one should use unimodularity properties together with the following equivalence transforms ([10]): $x_i' := a x_i$ (to make the first element equal to 1) and $x_i' := x_i \zeta^{si}$, $\zeta = exp\{\frac{2\pi j}{n}\}$ (to make another element equal to 1 too). In this case, it is possible to compute PRUS of length up to 9. For example, Groebner basis for PRUS of length 9 is as follows ($x_1$ and $x_2$ were fixed): $\{x_3 - x_7 x_8 x_9, x_4 + x_7 x_8 + x_8^2, x_5 - x_8^2, x_6 + x_7 x_9 + x_8 x_9, x_7^2 + x_7 x_8 + x_8^2, x_8^3 - 1, x_9^9 - 1, x_2 - 1, x_1 - 1\}$. For PRUS of length 10, computations have run out of memory.

The experimental results for memory required, calculation time and Groebner basis size are summarized in Table I.

## V. Binary sequences with ideal autocorrelation

Construction of BSIA is another example of pure algebraic task. Indeed, autocorrelation properties $R_{\mathbf{x}}(\tau) = \sum_{s=0}^{n-1} x_s x_{s+\tau} = -1$ should be accompanied by restriction of variables to be binary, i.e. $\pm 1$. These restrictions are algebraic too: $x_i^2 - 1 = 0$. Due to equivalence transforms, it is possible to fix several variables without loss of generality: $x_0 = 1, \quad x_1 = 1, \quad x_2 = 1, \quad x_3 = -1$. This trick will slightly simplify the Groebner bases calculation. Using these restrictions together with autocorrelation properties and restriction of values to binaries $x_i^2 - 1 = 0$ it is possible to construct binary sequences of length up to 19. For $n = 23$ system runs out of memory.

However this result can be improved due to the fact that Groebner basis calculations with polynomials over $GF(2)$ are much more efficient than calculations over $\mathbb{Z}$. So we use sequences with alphabet $y_i \in \{0, 1\}$ by considering mapping $x_i := 2y_i - 1$. Alphabet restrictions are $y_i^2 - y_i = 0$. Autocorrelation properties are as follows: $\sum_{i=0}^{n-1} y_i y_{i+\tau} - \sum_{i=0}^{n-1} y_i + \frac{n+1}{4} = 0$. In order to solve this system all equations can be considered $\bmod 2$. Then the solutions of this system should be checked against original system. For $n = 27$ no sequences were found, although there is a number of solutions that satisfies system taken ($\bmod 2$). For $n = 31$ system have run out of memory. Also it is possible to consider this system of equations modulo 3. In this case, the system can be solved for $n$ up to 39. The best known result for exhaustive search is the sequences of length 43 ([14]).

All the above results were obtained from the autocorrelation properties only. However in certain cases it is possible to use additional properties ([27], [28]) that simplify solution process significantly:

1) If $n$ is not prime, then for every $w$, divisor of $n$, additional integer variables
$$b_i^{(w)} = \sum_{\substack{y_j = 1 \\ i \equiv j \bmod w}} y_j,\ 0 \leq b_i^{(w)} < n/w, 0 \leq i < w \tag{11}$$
can be used. These variables satisfy equations $\sum_{i=0}^{w-1} b_i^{(w)} b_{i-k}^{(w)} = \frac{n(n-3)}{4}$, $k = 1, \ldots, w-1$. It is possible ([29]) to compute all possible $b_i^{(w)}$ and then to add linear equations (11) to original polynomial system.
2) Sometimes BSIA has so-called *multiplier* $t$, i.e. an equation $x_{ti} = x_{i+s}$ holds for every $i$ and some $s = s(t)$. In this case, BSIA is constant on cyclotomic cosets. For sequences of length $2^N - 1$, 2 is always a multiplier.

Using these properties it is possible ([29]) to find all BSIA of length $2^{10}-1$. For BSIA of length $2^{11}-1$, we computed all $b_i^{(w)}$ for $w = 23$ and 89. With restrictions (11) been added to the system, Groebner bases computation took 8 Gb of RAM and then ran out of memory.

## VI. Conclusion

The Groebner basis calculation algorithms were successfully applied to construct new sequences analytically. For $n = p_1p_2$ and for $n = p = 5f + 1$, where $p, p_1, p_2$ are primes, new unimodular perfect sequences of length $n$ with 6 phases are proposed. For $n = p_1p_2$, a new family of sequences is constructed and a direct formulae is obtained. For perfect root-of-unity sequences and for binary sequences with ideal autocorrelation this new approach was used to find sequences analytically. Although this approach was not able to find previously unknown sequences, it is still better than any other analytical method. Since a great progress was achieved in recent years in the area of Groebner Bases computations, it seems possible for Groebner bases approach to outperform exhaustive search. This also can be true due to the fact that the fastest know algorithm $F_5$ ([21]) is now being implemented into computer algebra software system been used.

The results of computation are presented below.

TABLE I

Time and memory required for GB calculation

| Construction | Memory | Time | Size of GB |
|---|---|---|---|
| $n = p_1p_2$, $Q = 4$, $P = 10$ | 150 Mb | 580 s | 14 Mb |
| $Q = 4$, $P = 1000$ | 311 Mb | 1660 s | 32 Mb |
| $n = p = fe + 1$, $e = 4$, $f = 3$ | 3.5 Mb | 1.4 s | 300 Kb |
| $e = 4$, $f = 100$ | 4.8 Mb | 5.7 s | 670 Kb |
| $e = 4$, $f = 1000009$ | 45 Mb | 65 s | 4.7 Mb |
| $e = 5$, $f = 6$ | 99 Mb | 2500 s | 41 Mb |
| $e = 5$, $f = 12$ | 143 Mb | 4500 s | 62 Mb |
| PRUS, $n = 8$ | 96 Mb | 205 s | $< 1$ Kb |
| PRUS, $n = 9$ | 2.5 Gb | 21000 s | $< 1$ Kb |
| PRUS, $n = 10$ | out of memory | | |
| binary, via GF(2), $n = 27$ | 103 Mb | 922 s | 0 |
| binary, via GF(2), $n = 31$ | out of memory | | |
| binary, via GF(3), $n = 31$ | 1583 Mb | 7200 s | 34 sequences |
| binary, via GF(3), $n = 35$ | 3348 Mb | 7500 s | 10 sequences |
| binary, via GF(2), $n = 39$ | 107 Mb | 9.9 s | 0 |

## References


[1] Ernst M. Gabidulin, Vitaly V. Shorin, "New families of unimodular perfect sequences of prime length based on Gaussian periods," *Proceedings of the 2002'IEEE International Symposium on Information Theory*, June 30 – July 05, 2002, p.68, Lausanne, Switzerland.

[2] E. M. Gabidulin, "On Classification of Sequences with the Perfect Periodic Auto-Correlation Function," *Proceedings of the third International Colloquium on Coding Theory*, Sept. 25 – Oct. 02, 1990, Dilijan, pp. 24–30, Yerevan, 1991.

[3] E. M. Gabidulin "There Are Only Finitely Many Perfect Auto-Correlation Polyphase Sequences of Prime Length," *Proceedings of the 1994'IEEE International Symposium on Information Theory*, June 27 – July 01, 1994, p.282, Trondheim, Norway.

[4] E. M. Gabidulin, V. V. Shorin, "Perfect sequences of length $3p$," *Proceedings of the 2003'IEEE International Symposium on Information Theory*, June 30 – July 04, 2003, Yokohama, Japan.

[5] E. M. Gabidulin, "New perfect sequences of length $2p$," Proceedings of the ACCT-6, pp. 119–122, 1998.

[6] E. M. Gabidulin, "Further Results on PSK-Sequences with the Perfect Periodic Autocorrelation Function," B. Honary, M. Darnell, P. Farrell (Eds), *COMMUNICATION THEORY AND APPLICATIONS I*, HW Communications Ltd. 1993, pp. 171–176.

[7] E.M.Gabidulin , V.V.Shorin , "Perfect sequences of length $p_1p_2$, *Proceedings of the Seventh International Symposium on Communication Theory and Applications,* pp. 282–287, July 13 – 18, 2003, Ambleside, Lake District, UK.

[8] Vitaly V. Shorin, "Construction of New Perfect Sequences Using Groebner Bases," *Proceedings of the Eighth International Symposium on Communication Theory and Applications,* July 17 – 22, 2005, Ambleside, Lake District, UK.

[9] W. H. Mow, "A new unified construction of perfect root-of-unity sequences," *Proc. Int. Symp. on Spread Spectrum Techniques and Its Applications ISSSTA'96,* 1996, pp. 955–959.

[10] P. Fan, M. Darnell, *"Sequences Design for Communicational Applications,"* RSP Ltd, Taunton, Somerset, England, 1996.

[11] V. P. Ipatov, "Contribution to the theory of sequences with perfect periodic autocorrelation properties," *Radio Eng. Electron. Phys.* 25, April 1980, pp. 31–34.

[12] S. W. Golomb, "Two-valued sequences with perfect periodic autocorrelation" *IEEE Trans. Aerosp. Electron. Syst.,* vol. 28 , 2 , April 1992, pp. 383 – 386.

[13] L. Bomer, M. Antweiler, "Perfect three-level and three-phase sequences and arrays" *IEEE Trans. Commun.,* vol. 42, 234 , Feb.–Apr. 1994, pp. 767 – 772.

[14] H. D. Lke, H. D. Schotten, H. Hadinejad-Mahram, "Binary and quadriphase sequences with optimal autocorrelation properties : a survey" *IEEE Trans. Inform. Theory,* vol. IT-49, Dec. 2003, pp.3271–3282.

[15] B. Buchberger, *"Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal."* PhD thesis, Innsbruck, 1965.

[16] B. Buchberger, "Gröbner Bases : an Algorithmic Method in Polynomial Ideal Theory." In *Recent trends in multidimensional system theory,* Ed. Bose, 1985.

[17] D. Augot, M. Bardet, J.C. Faugère, "Efficient decoding of (binary) cyclic codes above the correction capacity of the code using Gröbner bases," *Proceedings of the 2003'IEEE International Symposium on Information Theory*, June 30 – July 04, 2003, Yokohama, Japan, p. 362.

[18] J.C. Faugère, "Algebraic cryptanalysis of HFE using Gröbner bases," *Rapport de recherche de l'INRIA, RR-4738, Feb. 2003, available online at http://www.inria.fr/rrrt/rr-4738.html*

[19] J.C. Faugère, G. Ars, "An Algebraic Cryptanalysis of Nonlinear Filter Generators using Gröbner bases ," *Rapport de recherche de l'INRIA, RR-4739, Feb. 2003, available online at http://www.inria.fr/rrrt/rr-4739.html*

[20] J.C. Faugère, "A new efficient algorithm for computing Gröbner Bases (F4)," *Journal of Pure and Applied Algebra,* Vol. 139, 1–3 (June 1999), pp. 61–88.

[21] J.C. Faugère, "A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)," *Proc. ISSAC 2002*, ACM-Press, 75–83, 2002.

[22] J.-C. Faugère, "How my computer find all the solutions of Cyclic 9," *Rapport de recherche LIP6.2000.007, 2000, available online at ftp://ftp.lip6.fr/lip6/reports/2000/lip6.2000.007.ps.gz .*

[23] J. Backelin, R. Fröberg, "How we proved that there are exactly 924 cyclic 7roots," In *ISSAC' 91 (July 1991),* S. M. Watt, Ed., ACM, pp. 103–111.

[24] G. Björk, R. Fröberg, "Methods to "divide out" certain solutions from systems of algebraic equations, applied to find all cyclic-8 roots," preprint 1993, 1993.

[25] The Magma Computational Algebra System for Algebra, Number Theory and Geometry, *http://magma.maths.usyd.edu.au/magma/* .

[26] D. Cox, J. Little, and D. O'Shea, *"Ideals, varieties, and algorithms."* Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997.

[27] M. Hall Jr, "A survey of difference sets," *Proc. Amer. Math. Soc.,* 7 (1956), pp.975-986.

[28] L.D. Baumert, "Cyclic difference sets," *Lecture Notes in Mathematics,* vol. 182, Springer-Verlag, Berlin, 1971.

[29] P.Gaal and S.W.Golomb, "Exhaustive determination of (1023, 511, 255)-cyclic difference sets," *Mathematics of Computation,* pp.357-366, 2001.