Recursion polynomials of unfolded sequences*

Ana I. Gomez[1], Domingo Gomez-Perez[1], and Andrew Tirkel[2]

[1] Dep. Matemáticas, Estadística y Computación, Universidad de Cantabria, Spain
{gomezperezai,gomezd}@unican.es
http://grupos.unican.es/amac
[2] Scientific Technology, 10 Marion Street, Brighton, Vic, 3186, Australia
atirkel@bigpond.net.au

Abstract. Watermarking digital media is one of the important challenges for information hiding. Not only the watermark must be resistant to noise and against attempts of modification, legitimate users should not be aware that it is embedded in the media. One of the techniques for watermarking is using an special variant of spread-spectrum technique, called frequency hopping. It requires ensembles of periodic binary sequences with low off-peak autocorrelation and cross-correlation. Unfortunately, they are quite rare and difficult to find. The small Kasami, Kamaletdinov, and Extended Rational Cycle constructions are versatile, because they can also be converted into Costas-like arrays for frequency hopping. We study the implementation of such ensembles using linear feedback shift registers. This permits an efficient generation of sequences and arrays in real time in FPGAs. Such an implementation requires minimal memory usage and permits dynamic updating of sequences or arrays.
The aim of our work was to broaden current knowledge of sets of sequences with low correlation studying their implementation using linear feedback shift registers. A remarkable feature of these families is their similarities in terms of implementation and it may open new way to characterize sequences with low correlation, making it easier to generate them. It also validates some conjectures made by Moreno and Tirkel about arrays constructed using the method of composition.

Keywords: Periodic Sequences · Multidimensional Arrays · Watermarking.

1 Introduction

Digital media has became a widely used product in everyday life. The availability of electronic devices, like computers and smartphones, makes possible large-scale distribution of digital content without proper authorization from content producers. This situation has created a need for finding ways of hiding copyright

* Supported by Consejería de Universidades e Investigación, Medio Ambiente y Política Social, Gobierno de Cantabria (ref. VP34)

messages or serial numbers in order to trace copyright violators. Several companies decided to fund the Digital Watermarking Alliance for raising awareness and promote the adoption of digital watermarking.

There are several techniques that this consortium plan to standardize, and one proposed method to hide information in digital media is a variant of spread-spectrum techniques using ensembles of periodic sequences with low off-peak autocorrelation and low cross-correlation [12]. This makes sets of arrays with low correlations find applications in watermarking of images, audio, video, and multimedia; but they are also prized in radar and communications, because of their efficiency and noise immunity. Known ensembles of sequences, such as the small Kasami set [11], are optimal with respect to the Sidelnikov correlation bound, but their linear complexity is logarithmic in the length of the sequences, so prone to cryptanalytic attacks. Other optimal ensembles of binary sequences are Kamaletdinov ensembles of sequences [10], discovered independently by Moreno and Tirkel among other families of sequences unfolded from arrays constructed by the Extended Rational Cycle (ERC) [15]. These sequences have lengths whose factors are relatively prime, so they can be folded into two-dimensional arrays using the Chinese remainder theorem (CRT) [9]. They consist of cyclic shifts of a pseudonoise or constant column [18] and can all be generated using the *composition method* [17]. The idea behind this procedure is to build arrays using shifted versions of the same pseudonoise sequence, by means of a *shift array* or *shift sequence*. This method is very flexible and it allows also to generate higher dimensional arrays [15]. A similar family of sequences with good correlation properties are given by the interleaved sequences [8], but we remark that the definition is different and so is the theory to generated by them. While both constructions make use of the method of composition, and the concepts of shift sequence and Trace function, they are quite distinct. The constructions discussed here utilise families of novel shift sequences with low auto and cross hit correlation, together with a solitary pseudonoise column. These constructions yield sequences of length $p(p+1)$ and $p(p-1)$ [13] and multidimensional multi-periodic arrays [18, 15]. By contrast, interleaved sequences [8] use the composition of a solitary shift sequence with ingeniously chosen column sequences. This construction is limited to sequence lengths $(2^n-1)^2$. The construction is single periodic because of the choice of the shift sequence [5] and only two such shift sequences are available: exponential Welch and the folded m sequence introduced by Baumert and Games, see [6]. Moreover, the shift arrays used in the sequences can be converted into Costas-like arrays with bounded auto- and cross-hit correlations [16]. Apart from watermarking, such ensembles are useful in multiple access frequency/time hopping systems for UWB ranging, sonar, and wireless communications.

An important aspect which has been little discussed is implementation. Although all known constructions can be easily implemented in a computer, the challenge is to do it in low-resource devices. Linear Feedback Shift Registers (-LFSRs) provide the most common technique for generating sequences. However, Kamaletdinov ensembles and ERC families require quite large LFSRs. Leukhin

and Tirkel [13] proposed an implementation using cascade LFSRs and then asked for a general formula for the length of the LFSRs involved. This paper presents formulas for that parameter. For certain array sizes, this allows an efficient generation of sequences and arrays in real time in FPGAs. Such an implementation requires minimal memory usage and permits dynamic updating of sequences or arrays.

Moreover, the factorization of the minimal polynomials of these LFSRs follows a certain pattern. This provides a way to unify the above sequences and constructions and brings order to apparently haphazard discoveries. A challenging area in the field of finding families of low correlation sequences is to characterize properties of these sets like linear complexity. This is still not widely understood and this research is a step forward to close this gap. Our results also validate some conjectures made by Moreno and Tirkel about arrays constructed using the method of composition. These results build on [13], where empirical data suggested that such unification should be possible. In turn, Leukhin and Tirkel [13] drew attention upon the pioneering works [1, 4], which analysed the cycle lengths of reducible polynomials and, most importantly, those containing repeated factors. In order to understand the unified constructions, we first study the nature of the most common column sequence employed by the method of composition: the Legendre sequence which exists for every prime number. Ding et al. [3] calculated the linear complexity of the binary Legendre sequence and its minimal polynomial. We extend this result, giving the number of factors as well as their degree. Explicitly, the factors are those of cyclotomic polynomials, so similar algorithms as those by Tuxanidy and Wang [19] for odd characteristic could be applied. We leave the development of such algorithms as an open problem.

The paper is organized as follows: Section 2 introduces cascade LFSRs and shows how a recursion polynomial (or minimal polynomial) for a Legendre sequence factors into lower degree polynomials. Section 3 analyses the minimal polynomials for arrays generated by the method of composition using the Legendre sequence as column. By default, it also provides the minimal polynomials for m-sequence columns, a much simpler case. Section 4 discusses how the new theory is consistent with and validates the empirical findings in [13].

2 Cascade LFSRs and Legendre sequence

Throughout the rest of the paper, we assume that the reader is familiar with the theory of LFSRs. We recommend consulting the work by Birdsall and Ristenbatt [1].

Implementation of sequences is an important and difficult issue. Although any sequence can be generated by an LFSR, it is not always efficient because its length can be close to that of the sequence.

There is an alternative to the naive implementation using LFSRs, called *cascade LFSRs*. The idea is to speed up the generation combining the output of several LFSRs by a XOR gate, as shown in Figure 1. It is even more convenient

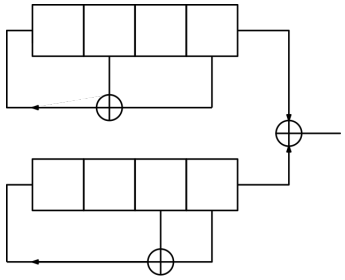

Fig. 1. A cascade with two LFSRs

when some of the LFSRs give decimated sequences of another. In this case, some memory can be saved.

Finding such a representation for a sequence is equivalent to finding factors of its minimal polynomial. In this paper, we focus on nontrivial factors, i.e. irreducible factors of degree greater than one. These are the ones which matter most, because the factor $x + 1$ represents a sequence inversion. Although there are efficient algorithms to factor polynomials with binary coefficients, our aim is deriving formulas depending directly on the parameters of the sequence.

Now, we recall that The Legendre sequence (s_i) with respect to the prime p is defined, for $0 \leq i < p$, by

$$s_i = \begin{cases} \left(1 + \left(\frac{i}{p}\right)\right)/2, & \text{if } \gcd(i,p) = 1; \\ 0, & \text{otherwise;} \end{cases} \tag{1}$$

where $\left(\frac{i}{p}\right)$ is the Legendre symbol. A binary Legendre sequence exists for all odd prime length and its correlation is perfect if $p = 3 \bmod 4$, which makes it very versatile and this is the reason it is used in the method of composition. Ding et al. proved the following result regarding its minimal polynomial.

Lemma 1 (Theorem 2 in [3]). *Let (s_i) be the Legendre sequence with respect to the prime p and $m(x)$ its minimal polynomial. We introduce the following additional elements:*

- $\mathbb{F}_2 = \{0, 1\}$*, the finite field of two elements*
- β*, a primitive root over an extension of* $\mathbb{F}_2$ *of order* p*,*
- $q(x) = \prod\{x + \beta^i \mid 0 \leq i < p, \left(\frac{i}{p}\right) = 1\}$*,*

Then,

- $m(x) = q(x)(x + 1)$*, if* $p \equiv -1 \bmod 8$
- $m(x) = q(x)$*, if* $p \equiv 1 \bmod 8$
- $m(x) = x^p + 1$*, if* $p \equiv 3 \bmod 8$
- $m(x) = (x^p + 1)/(x + 1)$*, if* $p \equiv 5 \bmod 8$

Next lemma give some properties of the factorization of $m(x)$.

Lemma 2 (Theorem 2.47 in [14]). *Let $\mathbb{F}_2[x]$ be the ring of polynomials with coefficients in $\mathbb{F}_2$. For a prime $p > 2$, the irreducible factors of $(x^p + 1)/(x + 1)$ over $\mathbb{F}_2[x]$ have all degree d, the minimal positive integer such that $2^d - 1$ is divisible by p. In particular, since $m(x)$ divides $x^p + 1$, all of its irreducible factors have degree d.*

A *decimation* of a p-periodic sequence (u_i) is a sequence (v_i) defined by $v_i = u_{\alpha i}$, where α is a positive integer. For the Legendre sequence, we can prove that a cascade representation can be given by decimations of p-periodic sequences.

Theorem 1. *Let $\mathbb{F}_p$ be the field with p elements. There exists a p-periodic sequence (u_i) such that the minimal polynomial of the Legendre sequence (s_i) can be expressed as $x+1$ times the product of the minimal polynomials of decimations of (u_i) by quadratic residues of $\mathbb{F}_p$, if $p \equiv -1, 3 \bmod 8$. All these minimal polynomials have degree d, the minimal positive integer such that $2^d - 1$ is divisible by p.*

Proof. We denote by $\mathbb{F}_{2^d}$ the finite field with 2^d elements. By Lemma 2, all factors of the polynomial $(x^p+1)/(x+1)$ have degree d and are irreducible. Indeed, any LFSR (u_i) which has as minimal polynomial one of these factors is of the form $u_i = \mathrm{Tr}(\alpha^i),$ for some $\alpha \in \mathbb{F}_{2^d},\ \alpha^p = 1$, where Tr is the trace function. If α is a generator of the multiplicative group of elements of order p, i.e. a primitive root of order p, any other LFSR must be a decimation of (u_i). Indeed, if $v_i = \mathrm{Tr}(\beta^i)$ and there exists g such that $\alpha^g = \beta$,

$$v_i = \mathrm{Tr}(\alpha^{gi}) = u_{gi \bmod p}.$$

The minimal polynomial of the Legendre sequence must be a product of these irreducible factors, each of them defining a decimation of (u_i). The fact that these decimations are obtained through quadratic residues of the finite field $\mathbb{F}_p$ is a consequence of Lemma 1. This concludes the proof. □

Example 1. We calculate the occurring LFSRs for $p = 73$. In this case, we get $2^9 = 512 \equiv 1 \bmod 73$, so $d = 9$. The factorization of the minimal polynomial of the Legendre sequence with respect to prime p is exactly

$$m(x) = (x^9 + x^4 + x^2 + x + 1)(x^9 + x^6 + x^5 + x^2 + 1) \\ (x^9 + x^7 + x^4 + x^3 + 1)(x^9 + x^8 + x^7 + x^5 + 1).$$

For general values of p, notice that we know exactly the linear complexity of the Legendre sequence $L(s_i)$, and that (s_i) can be represented in cascade LFSRs using:

- $(p-1)/(2d)$ nontrivial LFSRs, if $p \equiv -1, 1 \bmod 8$
- $(p-1)/(d)$ nontrivial LFSRs, otherwise

By Lemma 1, the output sequence has to be XORed with the constant sequence of ones if $p \equiv 3, 7 \bmod 8$.

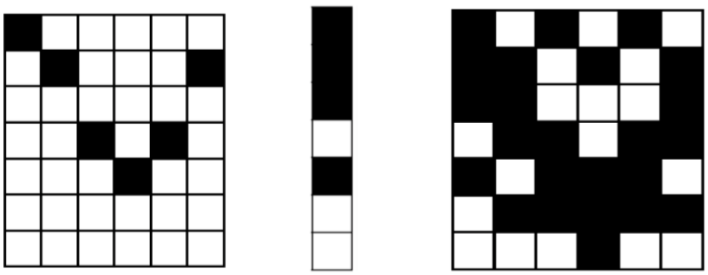

Fig. 2. Graphical example of the construction of a two-dimensional array using as column a Legendre sequence with respect to the prime 7. The doubly periodic shift sequence is $[0, 1, 3, 4, 3, 1]$ and is represented as the left two-dimensional array: the shifts for each output column are the black squares. The output is the array on the right.

3 Composition Method

The composition method builds a two-dimensional array from a shift array and a column. The output columns are cyclic shifts (as indicated by the shift array) of the input one.

This procedure admits a nice graphical representation: the shift array gets a black square in position (i, j) if the column of index i is to be shifted j positions. Figure 2 shows an example with a shift array belonging to family Kamaletdinov 1 and a Legendre sequence with respect to the prime 7 as input column. If the numbers of rows and columns are coprime, it is possible to transform the two-dimensional array into a sequence using the Chinese remainder theorem.

The shift array of $T \times N$ admits a representation as a sequence of integers between 0 and $T - 1$, which are the shifts. So, in a similar vein, consider a T-periodic binary sequence (u_i) and an N-periodic sequence of shifts (y_i) with $\gcd(N, T) = 1$. The resulting sequence using the Chinese remainder theorem is

$$S_i = u_{(i+y_{i \bmod N}) \bmod T}, \quad 0 \le i < NT. \tag{2}$$

Next result gives a lower bound for the linear complexity of (S_i), which is generated by the composition method using (u_i) and (y_i).

Theorem 2. *Let (u_i) be a binary sequence of period T and (y_i) an N-periodic sequence of shifts. We define the following NT-periodic sequence:*

$$Y_i = \begin{cases} 1, & \text{if } \exists l, \quad i \equiv (l - (l + y_l)AN) \bmod NT, \ l = 0, \ldots, N-1; \\ 0, & \text{otherwise;} \end{cases} \tag{3}$$

where A is the modular inverse of N modulo T, i.e. $AN \equiv 1 \mod T$. Then,

$$L(S_i) \ge NL(u_i) + L(Y_i) - NT.$$

Proof. We consider the generating polynomial associated with (S_i) (Eq. (2)):

$$S(x) = \sum_{i=0}^{NT-1} S_i x^i.$$

It is well known that the linear complexity of that sequence is

$$NT - \deg(\gcd(S(x), x^{TN} - 1)).$$

In order to calculate the greatest common divisor of these two polynomials, we denote by A an integer such that $AN \equiv 1 \mod T$.

$$\gcd\left(S(x), x^{TN} - 1\right) = \gcd\left(\sum_{i=0}^{NT-1} S_i x^i, x^{TN} - 1\right) =$$

$$\gcd\left(\sum_{l=0}^{N-1}\sum_{j=0}^{T-1} S_{Nj+l} x^{Nj+l}, x^{TN} - 1\right) = \gcd\left(\sum_{l=0}^{N-1}\sum_{j=0}^{T-1} u_{Nj+l+y_l} x^{Nj+l}, x^{TN} - 1\right) =$$

$$\gcd\left(u\left(x^N\right)\sum_{l=0}^{N-1} x^{(l-(l+y_l)AN) \bmod NT}, x^{TN} - 1\right),$$

whose degree is not larger than

$$\deg\left(\gcd\left(\sum_{l=0}^{N-1} x^{(l-(l+y_l)AN) \bmod NT}, x^{TN} - 1\right)\right) + \deg\left(\gcd\left(u(x^N), x^{TN} - 1\right)\right) =$$

$$\deg\left(\gcd\left(\sum_{l=0}^{N-1} x^{(l-(l+y_l)AN) \bmod NT}, x^{TN} - 1\right)\right) + N\deg\left(\gcd\left(u(x), x^{T} - 1\right)\right).$$

Using the relation between the generating function and the linear complexity, we get the result. □

This is, to our knowledge, the first result that relates the linear complexity of the column and doubly periodic shift sequences to the linear complexity generated by the composition method and the Chinese remainder theorem.

Next, we give a formula to calculate a multiple of the minimal polynomial of the unfolded sequences presented by Leukhin and Tirkel [13]. Indeed, if a plausible conjecture holds true, we can give the LFSRs in cascade representation of the unfolded sequences, up to multiplicities.

We define the following operation: given two polynomials $f, g \in \mathbb{F}_2[x]$, $f \odot g$ is the monic polynomial defined by

$$f \odot g = \prod_{f(\alpha)=0} \prod_{g(\beta)=0} (x - \alpha\beta),$$

where the products run over all roots of f and g over a closed extension of $\mathbb{F}_2$, see [19] for more about this operation.

Theorem 3. *Take a column sequence of length p whose minimal polynomial is $M(x)$ and a doubly periodic shift sequence of length T with $\gcd(T,p)=1$. The minimal polynomial of any sequence unfolded using the Chinese remainder theorem from an array output by the composition method is a divisor of $M(x)\odot(x^T+1)$, if $(x^p+1)/M(x)$ is not divisible by $x+1$. Otherwise, the minimal polynomial is a divisor of the product of $M(x)\odot((x^T+1)/(x+1))$ and $(x+1)$.*

As a consequence, sequences coming from unfolded arrays generated by the composition method can be represented as a set of cascade LFSRs. All these LFSRs are decimations of a single linear generator of degree d, the minimum integer satisfying

$$2^d \equiv 1 \bmod pT', \quad \gcd(T',2)=1, \quad T=2^fT',$$

and the multiplicity of the factors is less than 2^f.

Proof. Given $M(x)$, we define two sets:

$$\{\alpha\beta \quad | \quad M(\alpha)=0, \quad \beta^T=1\}, \tag{4}$$

$$\{\alpha\beta \quad | \quad M(\alpha)=0, \quad \beta^T=1, \quad \beta\neq 1\}\cup\{1\}. \tag{5}$$

A proof that all roots of the minimal polynomial of the unfolded array are in one of these sets can be found in [15, Lemma 5.1]. For the second statement, note that the generated sequence has period pT, which implies that the minimal polynomial is $x^{pT}+1$, whose roots are powers of a primitive root of order 2^d-1 and occur with multiplicity at most 2^f. This finishes the proof. □

As an example, let us apply the theorem above to the array generated in Figure 2. In that case, $p=7$ and the period of the doubly periodic shift sequence is $T=6$, so the length of the LFSRs in the cascade representation is at most $d=6$, which is the minimum integer such that $2^d\equiv 1 \bmod 21$.

We remark that all the appearing LFSRs are decimations of the same LFSR, but not all proper necessarily. That is why the examples in Equations 16 and 18 calculated by Leukhin and Tirkel involve factors with different degrees.

Computer experiments show that the roots of the minimal polynomial are those in either Equation (4) or (5). Indeed, it is straightforward to prove this for the shift arrays defined by ERC, Family A and Kamaletdinov 1 and 2 if the following conjecture holds [7].

Conjecture 1. The sequences generated by the composition method with shift arrays defined by Kamaletdinov families have maximal linear complexity.

Example 2. Let us go through the example in [13, Figure 7]. Take $p=7$ and a doubly periodic shift sequence of length $T=6$, so $6=2T'$ and $T'=3$. The degree d can be calculated directly:

$$2^6 = 64 \equiv 1 \bmod pT'.$$

Notice that the factor multiplicity equals 2. In this case, Conjecture 1 holds and the roots of the minimal polynomial are given exactly by Equation (4). Using [2, p. 119], it is possible to calculate a polynomial whose roots are exactly (4) or (5).

We finish this section with a corollary on the length of the LFSRs in the cascade representation when the Legendre sequence is used as column.

Corollary 1. *Under the conditions of Theorem 3 and for the cascade representation defined in the theorem, using as input column the Legendre sequence with respect to the prime p, all nontrivial LFSRs of the resulting cascade representation have degree d, if $T' = 1$. Otherwise, write ϕ for the Euler totient function and, for an integer $D > 1$, let d_D be the minimum positive integer such that $2^{d_D} \equiv 1 \bmod pD$. One of the following cases holds:*

- *if $p \equiv -1 \bmod 8$, there are $\phi(pD)/(2d_D)$ nontrivial LFRSs of length d_D for each divisor D of T'*
- *if $p \equiv 3 \bmod 8$, there are $\phi(pD)/d_D$ nontrivial LFRSs of length d_D for each divisor D of T'*
- *if $p \equiv 1 \bmod 8$, there are $\phi(pD)/(2d_D)$ nontrivial LFRSs of length d_D for each divisor D of T', except possibly for $D = 1$.*
- *if $p \equiv 5 \bmod 8$, there are $\phi(pD)/d_D$ nontrivial LFRSs of length d_D for each divisor D of T', except possibly for $D = 1$.*

Proof. If the sequences have maximal linear complexity, the minimal polynomial must have as many roots as possible, i.e. the set of roots must be the one defined in either Equation (4) or (5). Now, the result is an immediate application of Theorem 3 and the factorization of $x^{pT'} + 1$ by cyclotomic polynomials. The number of LFSRs for the case $D = 1$ is deduced in Example 1 and can be found, in general, in [14]. □

Example 3. For $p = 23$, Leukhin and Tirkel [13] give the factorization for the minimal polynomial of the sequence generated using the Extended Rational Cycle. The parameters, in that case, are $T = 24$, $T' = 3$, and $2^f = 8$. Using our notation, we have $D_1 = 11$ and $D_3 = 22$, so, applying the formula, there is only one factor of degree 11 and another of degree 22.

Interestingly enough, Theorem 3 states that the multiplicity is less than 8. In this case, the factor of degree 11 has multiplicity 7 and the other has multiplicity 8.

4 Conclusions

This paper shows that the recursion polynomial of the Legendre sequence is the product of specific irreducible polynomials. Consequently, we compute the recursion polynomials of sequences and arrays constructed by the method of composition using the Legendre sequence as input column.

This validates empirical findings and conjectures by Leukhin, Moreno, and Tirkel. It also shows that apparently unrelated constructions by Kamaletdinov, Moreno, and Tirkel can be unified under these results.

We leave two open problems: the first one is to develop similar algorithms as those in [19]. This would recover explicitly the factors of the minimal polynomial

of the sequence. Although there are tables with the factorization of $X^{pT}+1$ for some values of pT, it would still be interesting to obtain faster algorithms.

The second problem is to find an explicit formula for the multiplicity of the different factors. Computer experiments show some regularities, for example, there are always factors with maximal multiplicity, i.e. 2^f. Again, it is possible to compute the multiplicity efficiently.

As a final remark, the ideas outlayed here apply if the column is replaced by any other sequence. However, only the Legendre sequence is presented because it provides the most interesting case, due to its applications.

References

1. Birdsall, T.G., Ristenbatt, M.P.: Introduction to linear shift-register generated sequences. Tech. rep., The University of Michigan (1958)
2. Brawley, J.V., Carlitz, L.: Irreducibles and the composed product for polynomials over a finite field. Discrete Mathematics **65**(2), 115–139 (1987). https://doi.org/10.1016/0012-365X(87)90135-X
3. Ding, C., Hesseseth, T., Shan, W.: On the linear complexity of Legendre sequences. IEEE Transactions on Information Theory **44**(3), 1276–1278 (1998)
4. Elspas, B.: The theory of autonomous linear sequential networks. IRE Transactions on Circuit Theory **6**(1), 45–60 (1959)
5. Games, R.A.: Crosscorrelation of m-sequences and gmw-sequences with the same primitive polynomial. Discrete Applied Mathematics **12**(2), 139–146 (1985). https://doi.org/10.1016/0166-218x(85)90067-8, https://doi.org/10.1016/0166-218x(85)90067-8
6. Golomb, S.W., Gong, G.: Signal design for good correlation: for wireless communication, cryptography, and radar. Cambridge University Press (2005)
7. Gomez-Perez, D., Høholdt, T., Moreno, O., Rubio, I.: Linear complexity for multidimensional arrays-a numerical invariant. In: Proceedings of the IEEE International Symposium on Information Theory (ISIT 2015). IEEE (2015)
8. Gong, G.: Theory and applications of q-ary interleaved sequences. IEEE Transactions on Information Theory **41**(2), 400–411 (1995)
9. Gyorfi, L., Massey, J.L., et al.: Constructions of binary constant-weight cyclic codes and cyclically permutable codes. IEEE Transactions on Information Theory **38**(3), 940–949 (1992)
10. Kamaletdinov, B.: Optimal sets of binary sequences. Problemy peredachi informatsii **32**(2), 39–44 (1996)
11. Kasami, T.: Weight distribution formula for some class of cyclic codes. Coordinated Science Laboratory Report no. R-285 (1966)
12. Katzenbeisser, S., Petitcolas, F.: Information hiding techniques for steganography and digital watermarking. Artech house (2000)
13. Leukhin, A., Tirkel, A.: Ensembles of sequences and arrays. In: 2015 Seventh International Workshop on Signal Design and its Applications in Communications (IWSDA). pp. 5–9. IEEE (2015)
14. Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge University Press (1994). https://doi.org/10.1017/CBO9781139172769
15. Tirkel, A., Gomez-Perez, D., Gomez, A.I.: Arrays composed from the Extended Rational Cycle. Advances in Mathematics of Communications **11**(2), 313–327 (2017)

16. Tirkel, A., Gomez-Perez, D., Gomez, A.I.: Large families of sequences for CDMA, frequency hopping, and UWB. Cryptography and Communications **12**(1), 389–403 (2020)
17. Tirkel, A., Osborne, C., Hall, T.: Steganography-applications of coding theory. In: IEEE Information Theory Workshop, Svalbard, Norway. pp. 57–59 (1997)
18. Tirkel, A.Z., Hall, T.E.: Matrix construction using cyclic shifts of a column. In: Proceedings. International Symposium on Information Theory, 2005. ISIT 2005. pp. 2050–2054. IEEE (2005)
19. Tuxanidy, A., Wang, Q.: Composed products and factors of cyclotomic polynomials over finite fields. Designs, codes and cryptography pp. 1–29 (2013)