On Prime Root-of-Unity Sequences with Perfect Periodic Correlation

Mojtaba Soltanalian* and Petre Stoica, *Fellow, IEEE*

***Abstract*—In this paper, Perfect Root-of-Unity Sequences (PRUS) with entries in $\alpha_p = \{x \in \mathbb{C} \mid x^p = 1\}$ (where p is a prime) are studied. A lower bound on the number of distinct phases that are used in PRUS over α_p is derived. We show that PRUS of length $L \geq p(p-1)$ must use all phases in α_p. Certain conditions on the lengths of PRUS are derived. Showing that the phase values of PRUS must follow a given difference multiset property, we derive a set of equations (which we call the principal equations) that give possible lengths of a PRUS over α_p together with their phase distributions. The usefulness of the principal equations is discussed, and guidelines for efficient construction of PRUS are provided. Through numerical results, also contributions are made to the current state-of-knowledge regarding the existence of PRUS. In particular, a combination of the developed ideas allowed us to numerically settle the problem of existence of PRUS with $(L, p) = (28, 7)$ within about two weeks— a problem whose solution (without using the ideas in this paper) would likely take more than three million years on a standard PC.**

***Index Terms*—Perfect sequences, Root-of-unity sequences, Periodic autocorrelation, Phase distribution, Sequence construction**

I. Introduction

Perfect Root-of-Unity Sequences (PRUS), also known as perfect N-phase [1], N-ary [2], or polyphase [3] sequences, are unimodular sequences with entries in $\alpha_N = \{x \in \mathbb{C} \mid x^N = 1\}$ and the property that all their out-of-phase periodic autocorrelations are equal to zero [4]-[7]. These sequences are of interest in several applications including fast startup equalization and channel estimation [1], as well as communication schemes such as Direct-Sequence Spread-Spectrum Multiple-Access (DS/SSMA) and Frequency-Hopping Spread-Spectrum Multiple-Access (FH/SSMA) [8]. They can also be used as key sequences in pulse compression for continuous-wave radars [4]-[8].

Due to implementation issues it is usually desirable that the entries of the sequence are from a small alphabet. With this fact in mind, it is interesting to note that 4, 6 and 11 out of the first 8, 16 and 32 natural numbers, respectively, are prime. The study of PRUS with prime-size alphabets is important not only because of this relatively high density of prime numbers in small alphabet sizes, but also because of the role of prime numbers as building blocks of natural numbers. A similar building block property can be seen in the PRUS case: let $n = mk$ where m and k are co-prime and assume that there exist PRUS $\boldsymbol{u} = (u_0, \cdots, u_{m-1})$ and $\boldsymbol{v} = (v_0, \cdots, v_{k-1})$ with alphabet sizes $m^\dagger$ and $k^\dagger$ respectively; then $\boldsymbol{w} = (w_0, \cdots, w_{n-1})$ where $w_l = u_{(l \bmod m)} v_{(l \bmod k)}$ is a PRUS with alphabet size $n^\dagger = m^\dagger k^\dagger$. This construction is known as Chinese Remainder Theorem (CRT) construction or simply as the direct product [11].

A general computational framework for designing sequences with optimal correlation was proposed in [13]. It is known that for lengths L that are *square-free* there exist an infinite number of *independent* unimodular sequences with perfect periodic correlation, see [6]. A fast computational method to find perfect unimodular sequences is proposed in [14]. Algebraic constructions for perfect unimodular sequences of lengths p, $2p$, $3p$, pp' and p^s (where p and p' are prime) were introduced and studied in [16]-[20]. When it comes to root-of-unity sequences (which correspond to the finite alphabet case of the unimodular sequences), the problem appears to be more complicated. For example, it is not known whether there exists none, a few or plenty of PRUS for some lengths or alphabet sizes. Besides construction methods, some publications (e.g. [1], [21]) have introduced and used the following necessary condition on PRUS: if $\boldsymbol{x} = \{x_l\}_{l=0}^{L-1}$ is a PRUS of length L then

$$\left| \sum_{l=0}^{L-1} x_l \right| = \sqrt{L} \tag{1}$$

This necessary condition follows directly from the fact that the DFT of a PRUS has a constant magnitude (note that the DFT value at zero frequency is the sum of the sequence). In [2], several useful results are obtained which can be combined with the results in this paper. Namely, it was shown in [2] that the existence of PRUS of length $L = mp$ (for a prime p) with entries in α_p is connected to the existence of (L, p, L, m)-relative difference sets. Using some existence results of relative difference sets, the authors in [2] prove for example that there is no PRUS of length $L = p^s$ (for $s \geq 3$), $L = 2p^s$ (for $s \geq 1$), and $L = pp'$ (for prime $p' > p$) with entries in α_p. However, the strongest claim in the literature regarding the existence (and construction) of PRUS is known as the Mow's conjecture [8]:

Mow's conjecture (for prime p): Let M(L,p) be the total number of PRUS with length L over α_p. Let $L = sq^2$, where s and q are both natural numbers and s is square-free. Then

$$M(L,p) = \begin{cases} q! s^q \Phi^q(s) p^m, & p_{\min} = p, \\ 0, & otherwise, \end{cases} \tag{2}$$

This work was supported in part by the European Research Council (ERC) under Grant #228044 and the Swedish Research Council. The authors are with the Dept. of Information Technology, Uppsala University, Uppsala, SE 75105, Sweden.

* Please address all the correspondence to Mojtaba Soltanalian, Phone: (+46) 18-471-3168; Fax: (+46) 18-511925; Email: mojtaba.soltanalian@it.uu.se

where

$$p_{\min} = \begin{cases} 2sq, & \textit{for } s \textit{ even and } m \textit{ odd}, \\ sq, & \textit{otherwise}, \end{cases} \quad (3)$$

and the Euler totient function $\Phi(n)$ shows the number of $k \in \mathbb{Z}_n$ for which k and n are co-prime, and $\Phi(1) = 1$ by definition. Moreover, all such PRUS can be constructed using a unified approach, see [8].

Note that a proof of Mow's conjecture would imply that no PRUS of lengths other than $L = p$ and $L = p^2$ exists over α_p. In this work[1], PRUS with a prime-size alphabet are studied. In particular, we study the phase distribution of such sequences, and introduce a set of *principal equations* that can yield the possible phase distributions of PRUS for any given p and L. In general, the provided phase distributions can significantly reduce the size of search space for finding PRUS. Based on the obtained phase distributions, we also provide practical guidelines for construction of PRUS. A combination of the ideas in this paper provides us, for example, with the possibility to numerically settle the problem of the existence of PRUS for $(L, p) = (28, 7)$ within two weeks; a problem for which an exhaustive search of the associated search space is guaranteed to take more than three million years on a standard PC.

The rest of this paper is organized as follows. In Section II, the phase distribution of PRUS over α_p is discussed. We show that the phase values of PRUS over α_p must follow a specific difference multiset property. Furthermore, Section II presents the principal equations. Section III is devoted to the study of some special cases. A discussion on the usefulness of the principal equations as well as guidelines for an efficient construction of perfect sequences along with some examples are included in section IV. In Section V, we provide our numerical results. Finally, Section VI concludes the paper.

Notation: We use bold lowercase letters for vectors/sequences and bold uppercase letters for matrices. $(.)^T$ and $(.)^*$ denote the vector/matrix transpose and complex conjugate respectively. The symbol $\odot$ is used for the Hadamard element-wise product of two matrices. $\boldsymbol{x}^{\updownarrow}$ is a vector containing the same entries as $\boldsymbol{x}$ but in reversed order. $\mathbf{0}_n$ and $\mathbf{1}_n$ are all zero and all one vectors of length n. $\boldsymbol{e}_l^{(n)}$ is the l^{th} standard basis vector in $\mathbb{R}^n$. $\|\boldsymbol{x}\|_n$ or the l_n-norm of the vector $\boldsymbol{x}$ is defined as $(\sum_k |x(k)|^n)^{\frac{1}{n}}$ where $\{x(k)\}$ are the entries of $\boldsymbol{x}$. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ represent the set of natural, integer, real and complex numbers respectively. $\mathbb{Z}_n$ represents the set $\{0, 1, \cdots, n-1\}$. Considering the multiplicities of elements, we use the concept of multiset with the notation $[\cdot]$. Finally, p denotes a prime number throughout the paper.

II. Phase Study

In this section, we study the phase distribution of PRUS over the alphabet α_p of prime size. Let $\boldsymbol{x} = \{x_l\}_{l=0}^{L-1} = \left\{e^{j\frac{2\pi}{p}k_l}\right\}_{l=0}^{L-1}$ be an L-length PRUS over α_p. All k_l are in $\mathbb{Z}_p$ and we call them the integer phases of the sequence. The periodic autocorrelation of $\boldsymbol{x}$ at lag $u \in \mathbb{Z}_L$ is defined as

$$\begin{aligned} R_u &= \sum_{l=0}^{L-1} e^{j\frac{2\pi}{p}(k_l - k_{l+u})} \\ &= \begin{cases} L & u = 0 \\ 0 & u \in \mathbb{Z}_L - \{0\} \end{cases} \end{aligned} \quad (4)$$

where the indices of $\{k_l\}$ are used in a periodic manner (i.e. $mod\ L$). It is interesting to note that R_u is a summation of terms which are also in α_p. Theorem 1 paves the way for using this observation (see Appendix A for a short proof):

Theorem 1. *If $\sum_{k=0}^{p-1} a_k e^{j\frac{2\pi}{p}k} = 0$ for some $a_k \in \mathbb{Z}$, then all a_k must be identical.*

Corollary 1. *If there exists a PRUS of length L over α_p then $p|L$.*

Proof: Let $u \in \mathbb{Z}_L - \{0\}$. Then it follows from (4) and Theorem 1 that $R_u = m\sum_{k=0}^{p-1} e^{j\frac{2\pi}{p}k} = 0$ where $m = L/p$ must be an integer. ∎

The fact pointed out in Corollary 1 is already known in the literature, see e.g. [2]. However, it is worthwhile to comment on the more general case of PRUS of length L over α_N. From a number theory perspective, the authors of [23] study the *vanishing sums of roots-of-unity*, viz. $q_1 + q_2 + \cdots q_T = 0$ with $q_l \in \alpha_N$ (for all l), and general $N \in \mathbb{N}$. In particular, they show that if $N = p_1^{a_1} \cdots p_r^{a_r}$ (with $p_1 < \cdots < p_r$) represent the prime factorization of N then a vanishing sum of T root-of-unity numbers $\{q_l\}$ (with $q_l \in \alpha_N$) can occur only if there exist non-negative integers $\{t_k\}$ such that T can be written as $T = t_1 p_1 + \cdots + t_r p_r$. Interestingly, we can use this result in the context of PRUS. Namely, the autocorrelation sums similar to that in (4) may become zero only if L can be written as

$$L = t_1 p_1 + \cdots + t_r p_r \quad (5)$$

where $\{t_k\}$ are non-negative integers. Therefore, satisfying (5) is a necessary condition for a PRUS of length L over α_N. Considering (5), also typically known as the *Frobenius coin problem* [24]-[26], can be particularly useful for showing the non-existence of PRUS when L is rather small. On the contrary, it can be shown that if $L \geq (p_1 - 1)(p_2 - 1)$ then (5) always has a solution.

In the sequel we use the notation $L = mp$, $m \in \mathbb{N}$, for the length of PRUS over α_p.

Corollary 2. *Let $\boldsymbol{x} = \left\{e^{j\frac{2\pi}{p}k_l}\right\}_{l=0}^{mp-1}$ be a PRUS of length $L = mp$ over α_p. Then for every $s \in \mathbb{Z}_p$ and $u \in \mathbb{Z}_L - \{0\}$, there exist exactly m distinct integers $\{l\}$ such that $k_l \equiv k_{l+u} + s\ (mod\ p)$.*

Proof: We only need to observe that, according to Theorem 1, all sums in (4) for $\{R_u\}_{u \in \mathbb{Z}_L - \{0\}}$ must have exactly m terms equal to $e^{j\frac{2\pi}{p}s}$ for every $s \in \mathbb{Z}_p$. ∎

We note that in light of the above results, a general difference set structure is obtained. Let $D = [d_0, d_1, \cdots, d_{s-1}]$ be a multiset over a group G of order v. D is a (v, s, λ)-difference

[1]Some parts of this work were presented at the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2011 [22].

multiset over G iff the multiset $\Delta_D = [d_k - d_l : \ k,l \in \mathbb{Z}_s, \ k \neq l]$ contains each element of G (0 included) exactly λ times. By this definition, the multiset of integer phases $[k_0, k_1, \cdots, k_{L-1}]$ of a PRUS of length $L = mp$ over α_p is a (p, mp, m)-difference multiset. The next two definitions appear to be essential in order to continue our study.

Definition 1. *Let $\xi_0, \cdots, \xi_{t-1}$ be real numbers whose sum is a constant C. From the Cauchy-Schwarz inequality we have that*

$$\|\boldsymbol{\xi}\|_2^2 \geq \left(\mathbf{1}_t^T \boldsymbol{\xi}\right)^2 / t \tag{6}$$

where $\boldsymbol{\xi}$ is the vector with entries $\{\xi_k\}$. Therefore, $\sum_{k=0}^{t-1} \xi_k^2$ attains its minimum value when the sum is uniformly distributed over $\{\xi_k\}$. We define

$$\Gamma(C,t) \triangleq \begin{cases} C^2/t & t > 0 \\ 0 & otherwise \end{cases} \tag{7}$$

as the minimum value of the sum of squares of t real variables with sum C.

Definition 2. *We let $\boldsymbol{\Phi}_x$ be the circulant matrix made from the integer phases $\{k_l\}$ of the sequence $\boldsymbol{x}$, viz.*

$$\boldsymbol{\Phi}_x \triangleq \begin{pmatrix} k_0 & k_1 & \cdots & k_{mp-1} \\ k_{mp-1} & k_0 & \cdots & k_{mp-2} \\ \vdots & \vdots & \ddots & \vdots \\ k_1 & k_2 & \cdots & k_0 \end{pmatrix}. \tag{8}$$

For the l^{th} column of $\boldsymbol{\Phi}_x$, consider the location of the entries which are equal to k_l ($l = 0, \cdots, mp-1$). Considering these locations for all columns, we build an $mp \times mp$ equivalence matrix $\boldsymbol{\Phi}_e$ of $\boldsymbol{x}$ whose entries in the mentioned locations are 1; otherwise they are 0. We also extend the definition of $\boldsymbol{\Phi}_e$ to $\boldsymbol{\Phi}_e^{(s)}$ (with $\boldsymbol{\Phi}_e^{(0)} = \boldsymbol{\Phi}_e$), for $s \in \mathbb{Z}_p$ as follows: by finding the locations of the entries $k_{l'}$ in the l^{th} column of $\boldsymbol{\Phi}_x$ such that $k_{l'} \equiv k_l + s \ (mod\ p)$, we represent these locations in $\boldsymbol{\Phi}_e^{(s)}$ by 1, and by 0 otherwise.

There exist several construction methods for PRUS with the length $L = p$; see Section III for details. Moreover, the case of $L = p$ presents some unique properties (see below) that makes its study relevant. We also study the PRUS of length $L = mp$, $m > 1$, and present our general results in sub-section II-B below.

A. The case of $L = p$ (corresponding to $m = 1$)

Based on the above discussions, the integer phases of PRUS with length $L = p$ over α_p have a $(p, p, 1)$-difference multiset structure. Such PRUS are in close connection with prime-length binary sequences with optimal periodic correlation. A detailed discussion revealing such close relationship is provided in Appendix B. Theorem 2 studies the phase distribution of PRUS in this case.

Theorem 2. *A PRUS of length $L = p > 2$ over α_p has exactly $\frac{1}{2}(p+1)$ distinct phases. Even more precisely, such PRUS consists of a singleton and $\frac{1}{2}(p-1)$ equi-phase pairs.*

Proof: Note that due to the $(p, p, 1)$-difference multiset structure, all rows of $\boldsymbol{\Phi}_e$ (in this case) have exactly one 1 except the first row whose all entries are 1. Now let μ_k be the number of times that $e^{j\frac{2\pi}{p}k}$ (for $k \in \mathbb{Z}_p$) occurs in the sequence, and let us assume that t of $\{\mu_k\}$ are nonzero. We have

$$\sum_{k=0}^{p-1} \mu_k = p. \tag{9}$$

As discussed above, by considering the rows of $\boldsymbol{\Phi}_e$, we conclude that there are $(2p-1)$ ones in $\boldsymbol{\Phi}_e$. On the other hand, since for every integer phase $k \in \mathbb{Z}_p$ we have μ_k columns with μ_k ones in each of them, the number of ones in $\boldsymbol{\Phi}_e$ is equal to $\sum_{k=0}^{p-1} \mu_k^2$; hence

$$\sum_{k=0}^{p-1} \mu_k^2 = 2p - 1. \tag{10}$$

Since the sum of μ_k is constant, we have

$$2p - 1 = \sum_{k=0}^{p-1} \mu_k^2 \geq \Gamma(p,t) = \frac{p^2}{t}, \tag{11}$$

and as a result

$$t \geq \left\lceil \frac{p^2}{2p-1} \right\rceil = \frac{1}{2}(p+1) \tag{12}$$

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. Now let us suppose that $t \geq \frac{1}{2}(p+1) + 1 = \frac{1}{2}(p+3)$. Also let v_1 be the number of $\{\mu_k\}$ which are equal to one. Therefore

$$p = \sum_{k=0}^{p-1} \mu_k \geq v_1 + 2(t - v_1) = 2t - v_1. \tag{13}$$

Note that (13) implies $v_1 \geq 2t - p \geq 3$. This leads to a contradiction for $p = 3$ as all phases should be different; i.e. $\mu_0 = \mu_1 = \mu_2 = 1$ which yields $\sum_{k=0}^{p-1} \mu_k^2 \neq 2(3) - 1$. Next we consider the case of $p \geq 5$. Note that

$$\sum_{k=0}^{p-1} \mu_k^2 \geq v_1 + \Gamma\left(p - v_1, \frac{p+3}{2} - v_1\right). \tag{14}$$

By substituting (10) in (13) we get $v_1 \leq 3$ and as a result $v_1 = 3$. Now let $\mu_{k_*} \geq 2$ for some $k_* \in \mathbb{Z}_p$; then

$$\sum_{k=0}^{p-1} \mu_k^2 \geq 3 + \mu_{k_*}^2 + \Gamma\left(p - 3 - \mu_{k_*}^2, \frac{p+3}{2} - 4\right). \tag{15}$$

Again by substituting (10) in (15) we obtain $\mu_{k_*} \leq 3$. This shows that except for $\mu_k = 1$, the only possible values of μ_k are 2 and 3. Let us denote the number of them by v_2 and v_3, respectively. Then:

$$\begin{cases} 3 + 2v_2 + 3v_3 = p \\ 3 + 4v_2 + 9v_3 = 2p - 1 \end{cases} \tag{16}$$

which is not feasible for integer numbers v_2 and v_3. Thanks to the latter contradiction, we conclude that the number of distinct phases is equal to $t = \frac{1}{2}(p+1)$. In order to obtain a complete picture of the phase distribution of $\boldsymbol{x}$, let v_k denote the number of $\{\mu_k\}$ which are equal to k, for all $k \in \mathbb{Z}_p$.

Using the inequality in (13) we have that $v_1 \geq 2t - p \geq 1$. On the other hand,

$$\sum_{k=0}^{p-1} \mu_k^2 \geq v_1 + \Gamma\left(p - v_1, \frac{p+1}{2} - v_1\right) \tag{17}$$

which implies $v_1 \leq 1$, and as a result $v_1 = 1$. If $\mu_{k_*} \geq 2$ for some $k_* \in \mathbb{Z}_p$ then

$$\sum_{k=0}^{p-1} \mu_k^2 \geq 1 + \mu_{k_*}^2 + \Gamma\left(p - 1 - \mu_{k_*}^2, \frac{p+1}{2} - 2\right). \tag{18}$$

As before, by substituting (10) in (18) we obtain $\mu_{k_*} \leq 2$, and hence $\mu_{k_*} = 2$. This implies that $v_2 = \frac{1}{2}(p-1)$ and $v_k = 0$ for $k > 2$ which completes the proof. ∎

B. The case of $L = mp$ (general case)

As indicated earlier, the integer phases of a PRUS of length $L = mp$ over α_p build a (p, mp, m)-difference multiset, which implies that for every $u \in \mathbb{Z}_L - \{0\}$, there exist exactly m distinct integers $\{l\}$ such that $k_l = k_{l+u}$. Therefore, for an $mp \times mp$ matrix $\mathbf{\Phi}_e$ built as in Definition 2, the number of ones is equal to $mp + m(mp-1)$. Let μ_k represent the number of times that $e^{j\frac{2\pi}{p}k}$ occurs in the sequence. Then we have that

$$\sum_{k=0}^{p-1} \mu_k = mp, \tag{19}$$

$$\sum_{k=0}^{p-1} \mu_k^2 = mp + m(mp-1). \tag{20}$$

We assume t of $\{\mu_k\}$ are nonzero, which implies

$$\begin{aligned} m^2 p + m(p-1) &= \sum_{k=0}^{p-1} \mu_k^2 \\ &\geq \Gamma(mp, t) = \frac{(mp)^2}{t}, \end{aligned} \tag{21}$$

and as a result

$$t \geq \frac{mp^2}{(m+1)p - 1}. \tag{22}$$

The above lower bound shows that as m increases, a larger number of phases from α_p might be needed to build a PRUS of length $L = mp$. For sufficiently large values of m we need all phases:

Theorem 3. *For $m \geq p-1$, all phase values must be used in a PRUS.*

Proof: This is a direct consequence of the lower bound in (22). ∎

Now, for every $s \in \mathbb{Z}_p - \{0\}$ we consider the matrix $\mathbf{\Phi}_e^{(s)}$ built as in Definition 2. Based on the difference multiset property, for every $u \in \mathbb{Z}_L - \{0\}$, there exist exactly m distinct integers $\{l\}$ such that $k_{l+u} \equiv k_l + s \ (mod\ p)$. Therefore, the matrix $\mathbf{\Phi}_e^{(s)}$ has exactly m ones in each of its rows except for the first row which is all zero. This implies that $\mathbf{\Phi}_e^{(s)}$ has $m(mp-1)$ ones. On the other hand, the number of ones in $\mathbf{\Phi}_e^{(s)}$ is equal to $\sum_{k=0}^{p-1} \mu_k \mu_{k+s}$ as it equals the number of all pairs with the property $k_{l+u} \equiv k_l + s \ (mod\ p)$. Therefore, the out-of-phase correlations of the sequence $\{\mu_k\}$ are given by

$$\sum_{k=0}^{p-1} \mu_k \mu_{k+s} = m(mp-1), \qquad s \in \mathbb{Z}_p - \{0\}. \tag{23}$$

Based on (19), (20) and (23), we conclude the following.

Theorem 4. *Let $\{\mu_k\}$ denote the phase distribution of a PRUS with length $L = mp$ over α_p. If we define $r_k \triangleq \mu_k - m$, then $\{r_k\}$ satisfy the following set of **principal equations**:*

$$\begin{cases} \sum_{k=0}^{p-1} r_k = 0 \\ \sum_{k=0}^{p-1} r_k^2 = m(p-1) \\ \sum_{k=0}^{p-1} r_k r_{k+s} = -m, \qquad s \in \mathbb{Z}_p - \{0\}. \end{cases} \tag{24}$$

Solving the principal equations indicate the possible PRUS phase distributions for given L and p. It is interesting to note that if $\{r_k\}$ is a solution to (24), then $\{-r_k\}$, $\{r_{-k}\}$ and $\{r_{k+l}\}$ where $l \in \mathbb{Z}_p$ are also valid solutions to (24). In other words, the set of principal equations induces a certain type of equivalence class on its solutions. We note that the unimodular perfect sequences enjoy a similar set of equivalence properties: let $\boldsymbol{x}$ be a unimodular perfect sequence, then $\boldsymbol{x}^*$ and $e^{j\phi}\boldsymbol{x}$ (where ϕ can be chosen arbitrarily) are also unimodular perfect sequences. This shows that given a solution $\{r_k\}$ to the principal equations, the solutions $\{r_{-k}\}$ and $\{r_{k+l}\}$ do not lead to new PRUS. In contrast, the solution $\{-r_k\}$ might lead to new sequences. As an aside remark, note that the second equation of (24) can be viewed as a *sum of squares problem*, which has been widely studied for many years. More details on this aspect are deferred to Appendix C. The following discussion is devoted to a geometrical study of the problem.

Let $\boldsymbol{r}_0 = (r_0, \cdots, r_{p-1})^T$ and also let $\boldsymbol{r}_k$ represent the circularly shifted version of $\boldsymbol{r}_0$ by $k \in \mathbb{Z}_p$. The principal equations can be rephrased as follows over the vectors $\{\boldsymbol{r}_k\}$:

$$\begin{cases} \mathbf{1}_p^T \boldsymbol{r}_k = 0 \\ \|\boldsymbol{r}_k\|_2 = \sqrt{m(p-1)} \\ \boldsymbol{r}_k^T \boldsymbol{r}_l = -m, \qquad k \neq l \end{cases} \tag{25}$$

The angle between each pair of vectors $\{(\boldsymbol{r}_k, \boldsymbol{r}_l)\}_{k \neq l}$ is given by

$$\theta = \arccos\left(\frac{\boldsymbol{r}_k^T \boldsymbol{r}_l}{\|\boldsymbol{r}_k\|_2 \|\boldsymbol{r}_l\|_2}\right) = \arccos\left(\frac{-1}{p-1}\right) \tag{26}$$

Therefore, $\{\boldsymbol{r}_k\}_{k \in \mathbb{Z}_p}$, form a set of p vectors lying in a $(p-1)$-dimensional space which is the hyperplane orthogonal to $\mathbf{1}_p$ and the angle between each pair of them is the value given in (26). We further note that the structure made by connecting all vertices pointed by $\{\boldsymbol{r}_k\}$ is a known multi-dimensional object called a *regular simplex* [29]. Such structures are shown in Fig. 1 for one, two and three dimensions. The reference [29] suggests $\{\boldsymbol{e}_k^{(p)}\}$ (i.e. the standard basis) as vertices of a regular simplex of edge $\sqrt{2}$ lying in the hyperplane $\mathbf{1}_p^T \boldsymbol{x} = 1$. It can be easily verified that $\widetilde{\boldsymbol{r}}_0 = \left((p-1)\sqrt{\frac{m}{p}}, -\sqrt{\frac{m}{p}}, \cdots, -\sqrt{\frac{m}{p}}\right)^T \in \mathbb{R}^p$ together with its circularly shifted versions (denoted by $\{\widetilde{\boldsymbol{r}}_k\}$) satisfy the principal equations. It is also straightforward to verify that

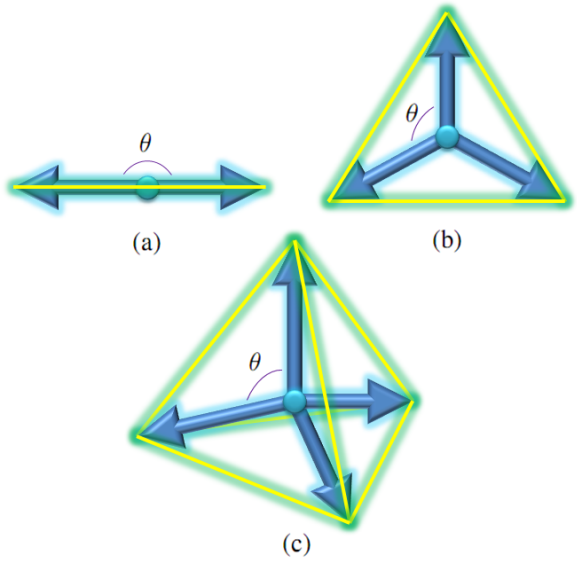


Fig. 1. (a-c) Regular simplexes in one, two and three dimensional space. In n dimensions they can be characterized with $n+1$ vectors with the same l_2-norm and also the same angle between them as described in Eq. (26).

these points can be obtained from the vectors $\{\boldsymbol{e}_k^{(p)}\}$ by a scaling and a translation. As every two regular simplexes with their center at $\mathbf{0}_p$ can be obtained from each other by a set of rotations, we can find the vectors $\{\boldsymbol{r}_k\}$ by rotations of $\{\widetilde{\boldsymbol{r}}_k\}$ such that their end lie at the integral lattice. Note that as the regular simplex made by $\{\widetilde{\boldsymbol{r}}_k\}$ is in a $(p-1)$-dimensional space, its rotation could be parametrized with $(p-2)$ angles $\psi_0, \cdots, \psi_{p-3}$ and as a result the vectors $\{\boldsymbol{r}_k\}$ could be written as a function of $\sin\psi_k$ and $\cos\psi_k$ for $k \in \mathbb{Z}_{p-2}$. Taking into consideration the fact that $\{\boldsymbol{r}_k\}$ are integral, this gives a closed form solution for m (and as a result a closed form solution for the sequence length) as well as the phase distribution. We give an example of the usage of such a geometrical approach in Section III. Nevertheless, for large values of L and p, an efficient numerical approach to tackle the principal equations is discussed in Appendix D.

III. Special Cases

This section not only considers special cases associated with the principal equations but also aims to establish the connections between the results in Section II and the existing literature on PRUS. Several special cases for m and p are discussed. The cases $m=1$ and $m=p$ are discussed because of the well-known constructions which give sequences for these values. Additionally, we study the case of $m=h^2m'$ where a solution for the principal equations can be found for length $L'=m'p$. The special cases $p=2$ and $p=3$ are also discussed to give closed form solutions for the length and phase distribution of PRUS. The case $p=3$ can be considered as an example of using the geometrical approach based on the regular simplex to solve the principal equations.

A. Special Cases of m

- $m=1$ and $m=p$: Sequences with $m=1$ (i.e. length $L=p$) can be constructed for example by Zadoff, Chu, Golomb polyphase, P3 and P4 methods [4]. These methods are all based on quadratic integer phases and it is easy to verify that all of them follow the distribution given in Section II-A. Examples of construction methods for $m=p$ (i.e. length $L=p^2$) include Frank, P1, P2 and Px methods [4]. Sequences of this length contain all phase values, see Theorem 3.
- $m=h^2m'$: Let $\{r_k^{(m')}\}$ be a solution of the principal equations for length $L'=m'p$ over α_p. Then, one can verify that $\{r_k^{(m)}\}=\{hr_k^{(m')}\}$ is a solution of the principal equations for the length $L=mp$. Interestingly, the Mow's conjecture suggests that the latter consruction of solutions for the principal equations cannot lead to new PRUS. Nevertheless, existence of such PRUS is not disproved by the principal equations.

B. Special Cases of p

- $p=2$: Solving the principal equations, viz.

$$\mu_0^2+\mu_1^2 = 2m^2+m \tag{27}$$
$$2\mu_0\mu_1 = 2m^2-m \tag{28}$$

for this case (which is the case of perfect binary sequences) yields $\mu_0 = \frac{1}{2}\left(2m \pm \sqrt{2m}\right)$ and $\mu_1 = \frac{1}{2}\left(2m \mp \sqrt{2m}\right)$. Therefore m must be of the form $2h^2$ and as a result $\mu_0 = 2h^2 \pm h$ and $\mu_1 = 2h^2 \mp h$. This enumeration of $+1$ and -1 in perfect binary sequences can be obtained also by the necessary condition (1) and is mentioned in several publications including [30].
- $p=3$: Here we use the geometrical approach discussed in Section II-B to solve the principal equations. For 3-phase perfect sequences, the $\{\boldsymbol{r}_k\}$ make a two dimensional regular simplex orthogonal to $\mathbf{1}_3$, which has 3 vectors and each two of them have an angle of $\frac{2\pi}{3}$. The structure of this regular simplex is shown in Fig. 1(b). Let $\boldsymbol{R}_{\mathbf{1}_3}$ be the unitary rotation matrix which maps $\mathbf{1}_3$ to $\sqrt{3}\boldsymbol{e}_3^{(3)}$. Also let

$$\boldsymbol{r}'_k = \sqrt{2m}\begin{pmatrix} \cos\left(\frac{2k\pi}{3}+\psi\right) \\ \sin\left(\frac{2k\pi}{3}+\psi\right) \\ 0 \end{pmatrix} \tag{29}$$

for $k \in \mathbb{Z}_3$ and $\psi \in [0, 2\pi)$. Therefore, $\boldsymbol{r}_k$ is equal to $\boldsymbol{R}_{\mathbf{1}_3}^{-1}\boldsymbol{r}'_k$ for some ψ. This implies that $\boldsymbol{r}_k \in \mathbb{Z}^3$ is of the form

$$\sqrt{2m}\begin{pmatrix} \frac{\sqrt{2}}{2}\cos\left(\frac{2k\pi}{3}+\psi\right) - \frac{\sqrt{6}}{6}\sin\left(\frac{2k\pi}{3}+\psi\right) \\ \frac{\sqrt{6}}{3}\sin\left(\frac{2k\pi}{3}+\psi\right) \\ -\frac{\sqrt{2}}{2}\cos\left(\frac{2k\pi}{3}+\psi\right) - \frac{\sqrt{6}}{6}\sin\left(\frac{2k\pi}{3}+\psi\right) \end{pmatrix}$$

for $k \in \mathbb{Z}_3$. As $\{\boldsymbol{r}_k\}$ are the circularly shifted versions of each other, it is sufficient to study one of them. For $k=0$, we infer that both $h_1 = 2\sqrt{\frac{m}{3}}\sin\psi$ (which is the second entry of $\boldsymbol{r}_0$) and $h_2 = 2\sqrt{m}\cos\psi$ (which is the difference between the first and the third entry of $\boldsymbol{r}_0$) must be integers. We conclude that $3h_1^2+h_2^2=4m$ and

$$\boldsymbol{r}_0 = \frac{1}{2}\begin{pmatrix} (h_2-h_1) \\ 2h_1 \\ -(h_2+h_1) \end{pmatrix}. \tag{30}$$

Therefore, the sequence length must be of the form

$$L = \frac{1}{4}\left(9h_1^2 + 3h_2^2\right) \tag{31}$$

while its phase distribution is given by

$$\frac{1}{4}\left(3h_1^2 + h_2^2\right)\mathbf{1}_3 + \frac{1}{2}\begin{pmatrix} (h_2 - h_1) \\ 2h_1 \\ -(h_2 + h_1) \end{pmatrix}, \tag{32}$$

for integers h_1 and h_2.

IV. PRUS: From Phase Distributions to Construction

In this section, we discuss the use of the ideas introduced earlier for an efficient search or construction of PRUS.

A. Are the Principal Equations Useful?

First we show that if $\{r_k\}$ satisfy the principal equations, then the necessary condition in (1) will be satisfied; i.e. the principal equations are more informative than (1). Let S be the sum of entries of the PRUS:

$$S \triangleq \sum_{l=0}^{mp-1} e^{j\frac{2\pi}{p}k_l} = \sum_{k=0}^{p-1} \mu_k e^{j\frac{2\pi}{p}k}. \tag{33}$$

For $\{r_k\}$ satisfying the principal equations:

$$\sum_{k=0}^{p-1} r_k r_{k+s} = \left(\sum_{k=0}^{p-1} r_k^2\right) - mp = -m, \quad s \in \mathbb{Z}_p - \{0\}. \tag{34}$$

Therefore,

$$\begin{aligned} |S|^2 &= \left|\sum_{k=0}^{p-1} \mu_k e^{j\frac{2\pi}{p}k}\right|^2 = \left|\sum_{k=0}^{p-1} r_k e^{j\frac{2\pi}{p}k}\right|^2 \\ &= \sum_{s=0}^{p-1}\left(\sum_{k=0}^{p-1} r_k r_{k+s}\right) e^{j\frac{2\pi}{p}s} = mp \end{aligned}$$

which implies the satisfaction of (1).

It is worth emphasizing that satisfaction of the principal equations is necessary but not sufficient for a PRUS. The necessity induced by the principal equations guarantees that if a sequence exists over α_p then it will have a specific length and phase distribution; particularly, the number of sequences which are needed to be checked for enummeration of PRUS of length L over α_p reduces from

$$p^L = \sum_{\{\mu_k \geq 0\}_{k=0}^{p-1}:\ \sum_{k=0}^{p-1}\mu_k = L} \binom{L}{\mu_0, \mu_1, \cdots, \mu_{p-1}} \tag{35}$$

to

$$\sum_{\{\mu_k\}_{k=0}^{p-1} \in\ \Omega} \binom{L}{\mu_0, \mu_1, \cdots, \mu_{p-1}} \tag{36}$$

where Ω represents the set of feasible phase distributions. Note that the expression (36) typically contains only a few out of $\binom{L+p-1}{p-1}$ summation terms of Eq. (35). Therefore, the principal equations can be used to show the impossibility of some lengths (in cases for which no feasible phase distribution exists) and to significantly reduce the size of search space of PRUS in general; see Section V for some numerical evidence on this aspect.

B. PRUS Construction: Guidelines and Examples

Once we have obtained the length and phase distribution of a PRUS, an efficient method for its construction (or further elimination of non-suitable cases) is needed. Hereafter, we aim to explain how a PRUS could be constructed using the $\{\mathbf{\Phi}_e^{(s)}\}$ matrices introduced in Section II. Examples of such a construction for different scenarios are also provided.

For the $\mathbf{\Phi}_e$ matrix (built based on the equality of phases) we need an all one first row and exactly m ones in any other row. On the other hand, the matrices $\{\mathbf{\Phi}_e^{(s)}\}_{s\neq 0}$ (built based on the inequality of phases) contain no ones in the first row and exactly m ones in the other rows. It is an important observation that *this condition is equivalent to the perfectness of the sequence* and as a result all we need is to check whether assigning different phases to indices in the sequence preserves this condition. Let us assume that the vector $\boldsymbol{\chi}_k = (\chi_k(0), \cdots, \chi_k(\mu_k - 1))^T$ contains the indices that are assigned to the k^{th} phase, i.e. $e^{j\frac{2\pi}{p}k}$. As an example, the configuration of the matrix $\mathbf{\Phi}_x$ and the corresponding vectors $\{\boldsymbol{\chi}_k\}$ are shown in Fig. 2 for the Frank sequence of length 9. As the $\mathbf{\Phi}_x$ matrix has a circulant structure, we can

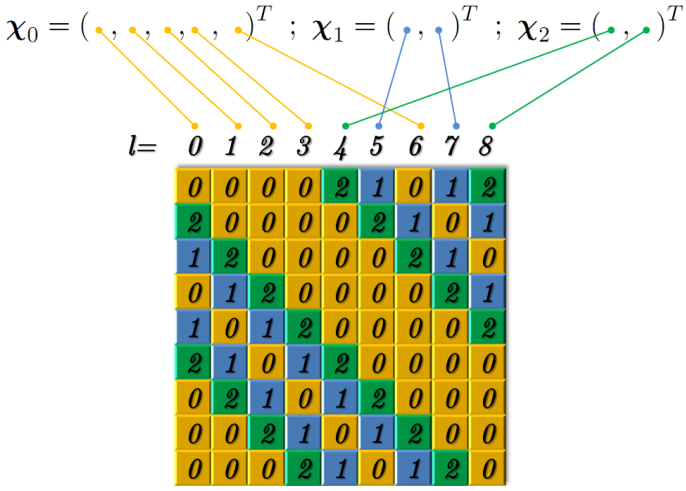


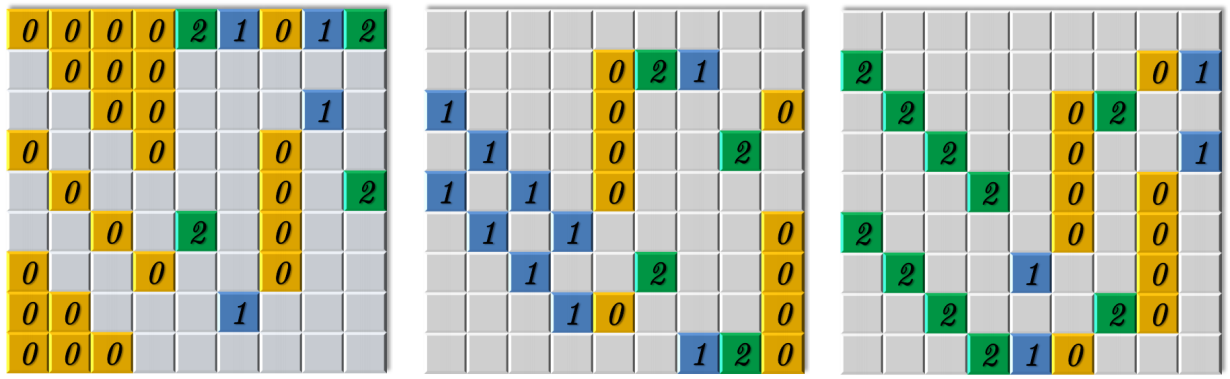
Fig. 2. Configuration of $\mathbf{\Phi}_x$ and the vectors $\{\boldsymbol{\chi}_k\}$ for the Frank sequence of length 9.

observe that rows of $\{\mathbf{\Phi}_e^{(s)}\}$ with a one in the $\chi_k(l)^{th}$ position are given by

$$(\chi_k(l) - \chi_k(1))\,\mathbf{1}_{\mu_{(k+s)}} + \boldsymbol{\chi}_{(k+s)}^{\updownarrow}. \tag{37}$$

Fig. 3 depicts the construction of the matrices $\{\mathbf{\Phi}_e^{(s)}\}$ for the Frank sequence of length 9 based on (37).

According to the above discussion, instead of the classical method based on calculation of the autocorrelation for all sequences, one can make updates of the matrices $\{\mathbf{\Phi}_e^{(s)}\}$ for each assignment of indices to phases in α_p respectively, and check whether for each assignment the number of nonzero entries in each row (except the first row) of the updated matrices $\{\mathbf{\Phi}_e^{(s)}\}$ does not exceed m. Note that since the matrices $\{\mathbf{\Phi}_e^{(s)}\}$ represent all distinct differences ($s \in \mathbb{Z}_p$ where $s = 0$ denotes the case of phase equality), they can



(a) (b) (c)

Fig. 3. (a-c) Construction of the matrices $\{\mathbf{\Phi}_e^{(s)}\}$ for the Frank sequence of length 9 and integer phase differences equal to $s = 0$ (i.e. equality of phases), 1 and 2 respectively. The positions of 1s are shown by the corresponding phases that satisfy the difference s.

be viewed as complementary binary matrices; i.e. (i) there exists no common positions for ones in the matrices $\{\mathbf{\Phi}_e^{(s)}\}$ (equivalently $\mathbf{\Phi}_e^{(s_1)} \odot \mathbf{\Phi}_e^{(s_2)}$ is an all zero matrix for any $s_1 \neq s_2$, where $s_1, s_2 \in \mathbb{Z}_p$), and (ii) the sum of matrices $\{\mathbf{\Phi}_e^{(s)}\}_{s\in\mathbb{Z}_p}$ is an all one matrix. Therefore, if by assigning all indices to elements of α_p, there still exists no row violating the above condition, then this shows that the number of ones in all rows of $\{\mathbf{\Phi}_e^{(s)}\}$ (except the first row) is equal to m.

It is important to note that by using the discussed idea, still we need to check all

$$\binom{L}{\mu_0, \mu_1, \cdots, \mu_{p-1}} \tag{38}$$

possible arrangements of entries of PRUS (with given phase distribution $\{\mu_k\}$). But the proposed method is also sensitive to unsuitable partial assignments of phases. A suitable phase arrangement is as shown in Fig. 2 corresponding to the Frank sequence of length 9. The method assigns $\boldsymbol{\chi}_0 = (0, 1, 2, 3, 6)^T$, $\boldsymbol{\chi}_1 = (5, 7)^T$ and $\boldsymbol{\chi}_2 = (4, 8)^T$ one after another and none of the matrices $\{\mathbf{\Phi}_e^{(s)}\}$ violates the above rule about the number of ones in their rows. On the other hand, there are unsuitable phase arrangements which coincide with the phase configuration of the Frank sequence. For example, suppose that the method already has assigned $\boldsymbol{\chi}_0 = (0, 1, 2, 3, 6)^T$. Now if the method assigns $\boldsymbol{\chi}_1 = (4, 5)^T$ then by updating the matrices $\{\mathbf{\Phi}_e^{(s)}\}$ (as depicted in Fig. 4), it appears that such a partial phase arrangement violates the expected number of ones in rows of $\{\mathbf{\Phi}_e^{(s)}\}$.

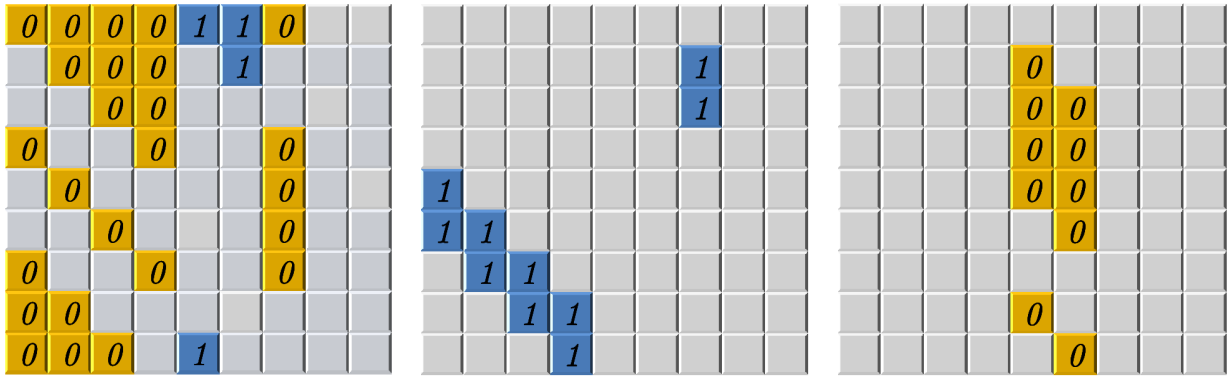
Note that by recognizing any partial assignment of phases as unsuitable, the proposed construction approach avoids testing lots of sequences and thus is considerably more efficient than the classical approach. We refer the interested reader to a further efficiency analysis of the proposed construction method in Appendix E.

V. Numerical Results

We provide several numerical results that rely on the ideas discussed in the paper. Table I presents all feasible lengths (less than or equal to 500) along with their corresponding phase distributions for $p = 5$ and 7. Using the equivalence properties of PRUS, the $\{\mu_k\}$ sequences are circularly shifted such that μ_0 take the maximum value among all $\{\mu_k\}$. The non-existence results of [2] are used to omit some cases of (L, p) wihtout solving the principal equations. Note that by providing the phase distributions we are able to significantly reduce the size of the search space in all cases. The search space cardinality reduction induced by using the principal equations is also reported in Table I.

In order to contribute to the current state-of-knowledge regarding the existence of PRUS, next we consider the unsolved cases of PRUS of length $L \leq 50$ in [2]; which are also shown in Table II. As in the previous example, the size reduction of the PRUS search space is reported when the phase distributions were derived by solving the principal equations. Nevertheless, even after using the principal equations, the size of the search spaces appears to be prohibitive for an exhaustive search. To help the interpretation of the results in Table II, and to see how expensive tackling such search problems can be, we consider the following analysis for the case $(L, p) = (28, 7)$:

- The initial size of the search space is $7^{28} \approx 4.60 \times 10^{23}$. Supposing that a standard PC can handle 5×10^9 simple math operations per second, we can see that a search for PRUS in this case would take more than
$$\frac{7^{28}}{(3600 \times 24 \times 365)(5 \times 10^9)} \text{ years} \tag{39}$$
i.e. approximately 3 *million years*.
- Using the principal equations, we reduce the size of the search space by a factor of 5.33×10^4. On the same standard PC, an exhaustive search of PRUS for $(L, p) = (28, 7)$ in this case will take more than
$$\frac{8.63 \times 10^{18}}{(3600 \times 24 \times 365)(5 \times 10^9)} \text{ years} \tag{40}$$
i.e. approximately 55 *years*.
- By employing the construction guidelines provided in



(a) (b) (c)

Fig. 4. (a-c) Updated matrices $\{\mathbf{\Phi}_e^{(s)}\}$ for an unsuitable phase arrangement which coincides with the phase configuration of the Frank sequence (integer phase differences are equal to $s = 0$, 1 and 2 for (a), (b) and (c) respectively). The positions of 1s are shown by the corresponding phases that satisfy the difference s. $\boldsymbol{\chi}_1 = (4, 5)^T$ is assigned after considering $\boldsymbol{\chi}_0 = (0, 1, 2, 3, 6)^T$ and as a result the number of 1s in the second and ninth row of (a) are more than $m = 3$.

TABLE I
ALL POSSIBLE LENGTHS (LESS THAN OR EQUAL TO 500) OF PRUS OVER α_p FOR $p = 5$ AND 7 TOGETHER WITH PHASE DISTRIBUTIONS.

p	Length (L)	Phase distributions $\{\mu_k\}_{k=0}^{p-1}$	Reduction in the size of search space induced by the principal equations ($\triangleq$ *initial size / final size*)
5	5	$(2,1,2,0,0)$ $(2,2,0,1,0)$	52.08
	25	$(6,6,6,6,1)$ $(9,4,4,4,4)$	1.60×10^3
	180	$(42,36,42,30,30)$ $(42,42,30,36,30)$	8.39×10^4
	220	$(52,46,34,46,42)$ $(52,46,46,42,34)$ $(54,42,46,36,42)$ $(54,46,42,42,36)$	6.31×10^4
	275	$(64,54,59,44,54)$ $(64,59,54,54,44)$ $(66,56,46,56,51)$ $(66,56,56,51,46)$	9.86×10^4
7	7	$(2,2,1,0,0,2,0)$	1.31×10^3
	28	$(6,6,4,2,2,6,2)$ $(7,5,5,2,5,2,2)$	5.33×10^4
	49	$(13,6,6,6,6,6,6)$ $(8,8,8,8,8,8,1)$	3.05×10^5
	56	$(11,10,10,5,10,5,5)$ $(11,11,6,11,6,6,5)$	4.55×10^5
	112	$(18,18,17,18,17,17,17)$ $(20,20,14,20,14,14,10)$ $(20,20,16,12,12,20,12)$ $(22,18,18,12,18,12,12)$ $(25,15,15,14,15,14,14)$	2.52×10^6
	196	$(30,30,30,30,30,30,16)$ $(33,33,26,33,26,26,19)$ $(37,30,30,23,30,23,23)$ $(40,26,26,26,26,26,26)$	1.02×10^7
	224	$(36,36,32,36,32,32,20)$ $(37,37,35,26,26,37,26)$ $(38,36,36,26,36,26,26)$ $(38,38,26,28,28,38,28)$ $(38,38,27,38,27,27,29)$ $(44,32,32,28,32,28,28)$	1.02×10^7
	372	$(62,62,55,62,55,55,41)$ $(62,62,62,48,62,48,48)$ $(64,64,50,64,50,50,50)$ $(71,57,57,50,57,50,50)$	8.23×10^7
	448	$(68,68,66,68,66,66,46)$ $(71,71,62,71,62,62,49)$ $(72,72,56,72,56,56,64)$ $(72,72,60,72,60,60,52)$ $(76,68,68,56,68,56,56)$ $(79,66,66,57,66,57,57)$ $(82,62,62,60,62,60,60)$	7.02×10^7

Section IV, we developed a MATLAB code[1] to search for PRUS with $(L, p) = (28, 7)$. We used two standard PCs, which dealt with the two possible phase distribtuions of the case $(L, p) = (28, 7)$ (see Table II), in parallel. Using this approach, we were able to confirm the *non-existence* of PRUS with $(L, p) = (28, 7)$ in about 2 *weeks*.

Note that due to the exponential growth in the size of search space, the questions regarding the existence of PRUS in cases for $(L, p) = (33, 11)$ and $(L, p) = (39, 13)$ remain open.

Although the study of PRUS over general root-of-unity alphabet (i.e. α_N with general $N \in \mathbb{N}$) is beyond the scope of this paper, it can be interesting to study the length/alphabet restrictions imposed by (5) and the remarks after Corollary 1. The eliminated cases of (L, N) via (5) are plotted in Fig. 5 for $2 \leq L, N \leq 100$. Interestingly, the prime values of N appear to support rather smaller numbers of lengths L than the nonprime values do. Via the results of Fig. 5 we prove the non-existence of PRUS for 3443 cases of (L, N) for $2 \leq L, N \leq 100$.

VI. CONCLUDING REMARKS

Perfect root-of-unity sequences with prime-size alphabets have been studied. The results can be summarized as follows:

[1]The MATLAB code associated with this experiment is provided online: `http://www.it.uu.se/katalog/mojso279/test-p7.rar`

TABLE II
REMAINING UNSOLVED CASES FROM [2], $L \leq 50$

p	Length (L)	Phase distributions $\{\mu_k\}_{k=0}^{p-1}$	Reduction in the size of search space induced by the principal equations ($\triangleq$ *initial size / final size*)	Final size of the search space	Existence
7	28	$(6,6,4,2,2,6,2)$ $(7,5,5,2,5,2,2)$	5.33×10^4	8.63×10^{18}	**Negative**
11	33	$(8,3,2,3,3,3,2,2,2,3,2)$	2.68×10^7	8.65×10^{26}	?
13	39	$(5,1,4,5,5,3,3,1,4,3,4,0,1)$ $(5,1,1,4,4,3,5,4,5,0,3,1,3)$ $(6,3,5,3,1,5,5,2,2,3,1,2,1)$ $(6,5,1,5,2,1,1,3,3,5,2,3,2)$	1.03×10^9	2.69×10^{34}	?

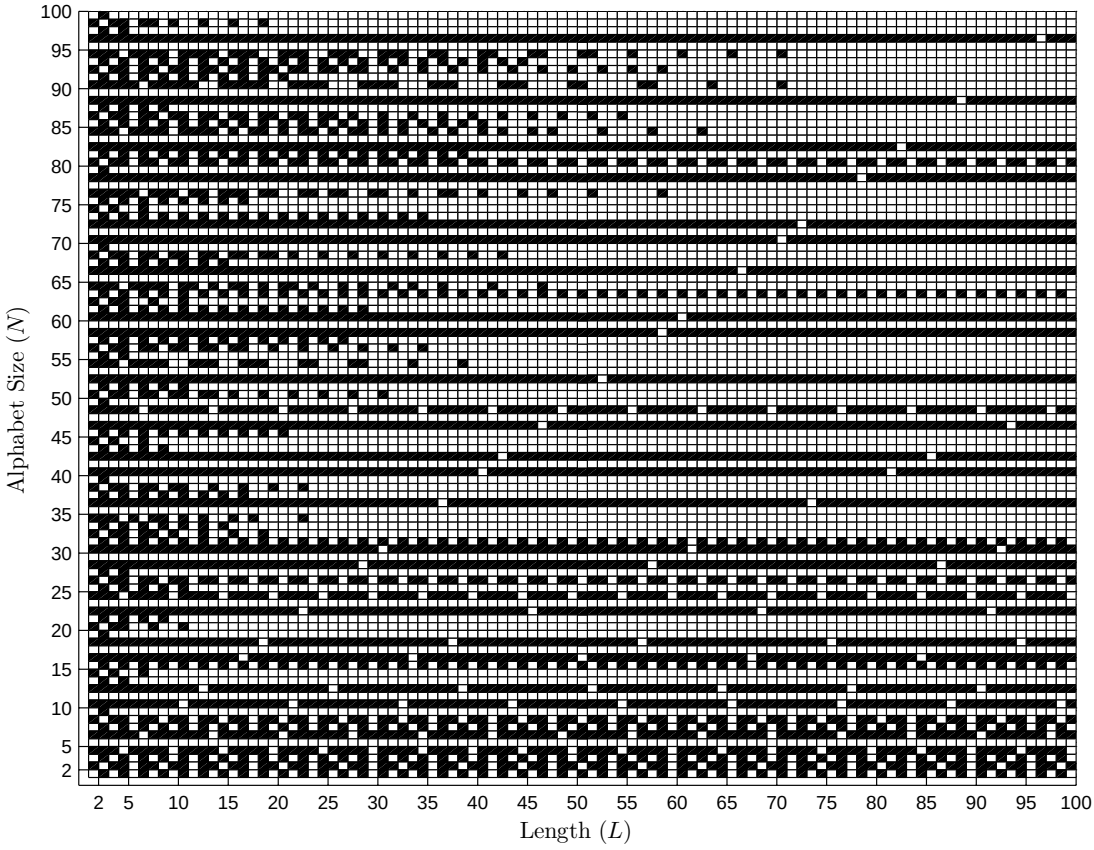


Fig. 5. The eliminated PRUS cases (represented by black squares) of (L, N) by solving (5) for $2 \leq L, N \leq 100$. The results in this figure prove the non-existence of PRUS for 3443 cases of (L, N) for $2 \leq L, N \leq 100$.

- The phase distribution of p-length PRUS over α_p was given for $p > 2$: it was shown that such sequences have $\frac{1}{2}(p+1)$ distinct phases with $\frac{1}{2}(p-1)$ of them appearing in pairs and one of them being a singleton.
- A lower bound on the number of distinct phases which must be used in a PRUS over α_p was derived. The lower bound was used to show that for PRUS of length $L \geq p(p-1)$ (i.e. $m \geq p-1$) over α_p, the sequence must use all phase values.
- Guidelines to find possible lengths (L) of PRUS over α_p were given. It was shown that integer phases of the sequence must follow a specific difference multiset property and there should exist a sequence of $\{\mu_k\}$ (introduced in Section II) satisfying the principal equations. For a possible length, the phase distribution is then given by $\{\mu_k\}_{k=0}^{p-1}$.
- A geometrical analytical method to solve the principal equations was introduced for a specific p using the regular simplex. In particular, it was shown using the geometrical approach that if there exists a perfect sequence over α_3 (i.e. a 3-phase perfect sequence), its length must be of the form $L = \frac{1}{4}\left(9h_1^2 + 3h_2^2\right)$ for $(h_1, h_2) \in \mathbb{Z}^2$ and the phase distribution of the sequence was also derived.
- The usefulness of the principal equations was discussed. Given the phase distribution, guidelines for efficient construction of PRUS (in comparison to the exhaustive

search) along with some examples were provided.
- Numerical evidence was provided to show the potential of using the principal equations and the construction guidelines of Section IV in practice. Through numerical examples, new contributions were made to the current state of knowledge regarding the existence of PRUS.

We conclude the paper with two remarks. First of all, while Theorem 1 shows that a uniform distribution of phases leads to perfect sequences, for *almost-perfect* sequences we may focus on *almost-uniform* distributions. A clear possibility here can be outlined as follows: in cases for which a perfect sequence does not exist, one can try to build sequences with a phase distribution which approximately satisfies the principal equations and approximately preserves the construction conditions for $\{\mathbf{\Phi}_e^{(s)}\}$ in Section D. Finally, we would like to emphasize the possible connections between the study of PRUS and the Szemerédi theorem and related results which study the minimal size and properties of subsets of $\mathbb{Z}_n$ containing specific length arithmetic progressions (see Appendix E). These results might be usable to further examine the existence as well as the construction for PRUS over α_p.

Appendix A
Proof of Theorem 1

We prove a more general form of the theorem by using some results from the theory of algebraic numbers and minimal polynomials: a number is called algebraic iff it is a root of a polynomial with rational coefficients. The minimal polynomial $P_{min}(x)$ of an algebraic number x_0 is the polynomial with rational coefficients, minimum degree and the leading coefficient equal to 1 which satisfies $P_{min}(x_0) = 0$. It is known [34] that the minimal polynomial of the primitive n^{th} root of unity ($e^{j\frac{2\pi}{n}}$) is of degree $d = \phi(n)$ where ϕ (the Euler's totient function) shows the number of $k \in \mathbb{Z}_n$ for which k and n are co-prime. For $n = p$, p prime, the minimal polynomial is of the unique form $\sum_{k=0}^{p-1} x^k$ [35]. We conclude that if $P(e^{j\frac{2\pi}{p}}) = 0$ for a polynomial $P(x)$ with rational coefficients and degree $d = p-1$ then $P(x)$ must be equal to $w\sum_{k=0}^{p-1} x^k$ for some rational scalar w. This implies that all coefficients of $P(x)$ must be equal, which completes the proof.

Appendix B
Connections Between PRUS of Length $L = p$ over α_p and Binary Sequences with Optimal Periodic Correlation

Let $\boldsymbol{x}$ be a PRUS of length p over α_p. Let μ_k represent the number of times for which $e^{j\frac{2\pi}{p}k}$ occurs in $\boldsymbol{x}$. It is shown in Section III-B that the distribution of $\{\mu_k\}$ is given by

$$\begin{cases} (p-1)/2, & \mu_k = 0 \\ 1, & \mu_k = 1 \\ (p-1)/2, & \mu_k = 2 \end{cases} \tag{41}$$

Since $\boldsymbol{x}$ is perfect, it has a constant magnitude of $\sqrt{p}$ in the discrete Fourier domain. Note that the value of the discrete Fourier domain, at the frequency zero, represents the sum of the sequence $\boldsymbol{x}$; hence, for $\boldsymbol{x} = \left\{e^{j\frac{2\pi}{p}k_l}\right\}_{l=0}^{p-1}$ we have that

$$\left|\sum_{l=0}^{p-1} e^{j\frac{2\pi}{p}k_l}\right| = \sqrt{p}, \tag{42}$$

or equivalently

$$\left|\sum_{k=0}^{p-1} \mu_k e^{j\frac{2\pi}{p}k}\right| = \sqrt{p}. \tag{43}$$

Now let $r_k = \mu_k - 1$. Therefore, (43) can be rewritten based on $\{r_k\}$ as

$$\left|\sum_{k=0}^{p-1} r_k e^{j\frac{2\pi}{p}k}\right| = \sqrt{p}. \tag{44}$$

The latter equality implies that

$$\sum_{k=0}^{p-1}\left(\sum_{l=0}^{p-1} r_l r_{l+k}\right) e^{j\frac{2\pi}{p}k} = p. \tag{45}$$

By applying the result of Theorem 1 to (45), we obtain:

$$\left(\sum_{l=0}^{p-1} r_l^2\right) - p = \sum_{l=0}^{p-1} r_l r_{l+1} = \cdots = \sum_{l=0}^{p-1} r_l r_{l+p-1}. \tag{46}$$

On the other hand, it is interesting to note that

$$\sum_{l=0}^{p-1} r_l^2 = \sum_{l=0}^{p-1} (\mu_l - 1)^2 = p - 1. \tag{47}$$

Therefore, the sequence $\{r_k\}$ has in-phase autocorrelation of $p-1$, and respectively, a constant out-of-phase autocorrelation of -1. Moreover, the distribution of $\{r_k\}$ is given by

$$\begin{cases} (p-1)/2, & r_k = -1 \\ 1, & r_k = 0 \\ (p-1)/2, & r_k = +1 \end{cases} \tag{48}$$

which implies that $\{r_k\}$ is a *balanced* [36] *punctured* [37] binary sequence with only one zero. Note that replacing the zero element of the sequence with $+1$ or -1 can change the out-of-phase correlation lags by 0, 2 or -2. We also note that all correlation values are congruent to the length of the sequence (i.e. p) modulo 4. Therefore, the out-of-phase correlation lags would turn to -1 for $p \equiv 3$, and to $\{1, -3\}$ for $p \equiv 1 \pmod 4$.

The discussed idea of constructing binary sequences with optimal periodic correlation from PRUS is summarized in Table III. As indicated earlier, there are several methods to construct a PRUS of length p over α_p. However, we do not limit our statements to the known construction methods as it is not yet proven that the currently known construction methods cover all possible PRUS.

Appendix C
Study of the Principal Equations in (24) using the sum of squares problem

We note that the second equality in (24) may be viewed as a sum of squares problem. This approach can be applied in particular to the case of $p = 3$. For $p = 3$, Gauss showed that a

TABLE III
CONSTRUCTION OF PRIME-LENGTH BINARY SEQUENCES WITH OPTIMAL PERIODIC CORRELATION FROM PRUS

Step 0: Consider a PRUS of length $L = p$ over α_p.
Step 1: Let μ_k represent the number of times for which $e^{j\frac{2\pi}{p}k}$ occurs in the considered PRUS. Form the sequence $r_k = \mu_k - 1$.
Step 2: Replace the only zero element in $\{r_k\}$ with $+1$ or -1.

natural number can be represented as the sum of three squares iff it is not of the form $4^k(8l-1),\ (k,l) \in \mathbb{Z}^2$ [38]. For $p > 3$, one may note that according to a theorem by Lagrange every natural number can be represented as the sum of four squares [38]. The latter result implies that every natural number can be written as sum of $p > 3$ squares. We refer the interested reader to [39]-[42] for additional information on cases $p = 5$, 7, 11, and 13.

APPENDIX D
EFFICIENT TEST METHOD FOR SPECIFIC LENGTHS

Herein we propose an efficient method for testing if a PRUS of a specific length might exist over α_p and for determining its phase distribution. This test method is useful for cases in which the length of the needed sequence is fixed or the derivation of closed form solutions of the principal equations for the sequence length and phase distribution over a desired alphabet is deemed to be expensive. Our test method is based on two approaches to reduce the size of search space for $\{r_k\}$: (i) imposing adaptive bounds on $\{r_k\}$ and (ii) assigning $\{r_k\}$ to certain classes of residues for different integer values. A preliminary bound on $\{r_k\}$ is given by the following lemma:

Lemma 1. *Let $r_0, \cdots, r_{p-1}$ be a solution to the principal equations; then*

$$|r_k| \leq (p-1)\sqrt{\frac{m}{p}}\ , \qquad k \in \mathbb{Z}_p. \tag{49}$$

Also if r_{k_*} has the maximum absolute value among all $\{r_k\}$, then

$$|r_{k_*}| \geq \left(\sqrt{p-1}\right)\sqrt{\frac{m}{p}}. \tag{50}$$

Proof: From the principal equations we have $r_k = -\sum_{l\in\mathbb{Z}_p-\{k\}} r_l$, and as a result $|r_k| \leq \sum_{l\in\mathbb{Z}_p-\{k\}} |r_l|$. Therefore,

$$\begin{aligned} m(p-1) &= \sum_{l=0}^{p-1} r_l^2 = r_k^2 + \sum_{l\in\mathbb{Z}_p-\{k\}} r_l^2 \\ &\geq r_k^2 + \Gamma\left(\sum_{l\in\mathbb{Z}_p-\{k\}} |r_l|, p-1\right) \\ &\geq r_k^2 + \Gamma\left(|r_k|, p-1\right) \\ &= \left(\frac{p}{p-1}\right) r_k^2 \end{aligned} \tag{51}$$

which yields the inequality (49). Next, note that

$$m(p-1) = \sum_{k=0}^{p-1} r_k^2 \leq p r_{k_*}^2 \tag{52}$$

which implies the inequality (50). ∎

Interestingly, similar bounds on $\{r_k\}$ could also be established in the case that some of $\{r_k\}$ are known. Let us assume that we know the values of $\{r_k\}_{k\in\mathbb{Z}_q}$ and let

$$\begin{cases} S_1 = \sum_{k=0}^{q-1} r_k \\ S_2 = \sum_{k=0}^{q-1} r_k^2 \end{cases} \tag{53}$$

Therefore, for every $k \in \mathbb{Z}_p - \mathbb{Z}_q$,

$$r_k = -S_1 - \sum_{l\in(\mathbb{Z}_p-\mathbb{Z}_q)-\{k\}} r_l \tag{54}$$

and as a result

$$\begin{aligned} m(p-1) - S_2 &= r_k^2 + \sum_{l\in(\mathbb{Z}_p-\mathbb{Z}_q)-\{k\}} r_l^2 \\ &\geq r_k^2 + \Gamma\left(r_k + S_1, p-q-1\right). \end{aligned} \tag{55}$$

The above quadratic inequality implies that such an arrangement of $\{r_k\}_{k\in\mathbb{Z}_q}$ might be possible only if

$$\frac{S_1^2}{p-q} + S_2 \leq m(p-1), \tag{56}$$

and that $\{r_k\}_{k\in\mathbb{Z}_p-\mathbb{Z}_q}$ are bounded by

$$b_\pm = \frac{-S_1 \pm \sqrt{(p-q-1)\left((p-q)(m(p-1)-S_2) - S_1^2\right)}}{(p-q)}. \tag{57}$$

These adaptive bounds help us make convenient successive selections of r_k.

In the following, we propose another useful idea to reduce the size of the search space, inspired by Minkowski-Hasse principle for quadratic forms [38]:

Minkowski-Hasse Principle. *A quadratic form*

$$Q\left(r_0, \cdots, r_{n-1}\right) = \sum_{(k,l)\in\mathbb{Z}_n^2} Q_{kl} r_k r_l \tag{58}$$

of rank n with integral coefficients represents zero over the rationals iff for any $g \in \mathbb{Z} - \{0\}$, the congruence $Q\left(r_0, \cdots, r_{n-1}\right) \equiv 0\ (mod\ g)$ has a primitive solution and in addition Q represents zero over the reals, i.e. it is indefinite.

Let

$$\begin{cases} \sum_{k=0}^{p-1} r_k \equiv 0 \\ \sum_{k=0}^{p-1} r_k^2 \equiv m(p-1) \\ \sum_{k=0}^{p-1} r_k r_{k+s} \equiv -m, \qquad s \in \mathbb{Z}_p - \{0\} \end{cases} \tag{59}$$

be a set of congruence $mod\ g \in \mathbb{N}$. Note that the second and third term of (59) are quadratic. It is also interesting to note that, as $\{r_k\}$ are bounded according to Lemma 1 and all other values are known and finite, the necessity and sufficiency of the congruence are obvious. In fact, choosing a sufficiently large g turns the congruence into an equality by adding an integral constant to r_k. The second fact we need to take into consideration is that the sum $\sum_{k=0}^{p-1} r_k,\ r_k \in \mathbb{Z}_g$, gets all the residue values in $\mathbb{Z}_g$ exactly g^{p-1} times. Therefore, by searching over all $r_k \in \mathbb{Z}_g$, the congruence set (59) must reduce the search space at least by a factor of g. Starting from a small g (say $g = 2$), we can omit at least $(g-1)/g$ of the search space elements by testing at most g^p elements. But, since many

of these elements are redundant for different g, it turns out that for sufficiently large values of g the number of newly omitted elements is less that the number of tested elements. Therefore, a combination of this method and the adaptive bounds in (57) appears to be more useful. Our proposed method can be described as follows:

- **0:** Consider the integral search space Ω bounded by the inequality (49). Without loss of generality, we assume that r_0 has the maximum value among $\{r_k\}$ and is bounded as in (50). Also let $g = 2$.
- **1:** Solve the congruence set in (59) for g. This can be done by a brute-force search over $\mathbb{Z}_g$.
- **2:** Reduce the size of Ω by omiting elements which belong to residue classes not feasible for the congruence set in (59). Let Δ_g represent the number of omitted elements. If $\Delta_g > g^p$, increase g by one and goto 1.
- **3:** Consider all possible values of r_0 in Ω and update S_1 and S_2 for each of them. By considering all $k = 1, \cdots, p-1$, respectively, do the following:
  - **3.0:** Establish the bounds $b_\pm$ as in (57).
  - **3.1:** Consider all possible r_k in Ω that follow the bounds $b_\pm$ and their absolute value is at most equal to r_0.
  - **3.2:** Update S_1 and S_2 for each r_k considered in 3.1.
- **4:** Check whether the obtained $\{r_k\}$ satisfy the third part of the principal equations (i.e. all out-of-phase correlations of $\{r_k\}$ are $-m$).

Appendix E
Further Efficiency Assessment of the Proposed Construction in Section IV-B

To explain in more detail how the proposed approach contributes an efficient construction scheme, consider the following: let $1+a_d(\boldsymbol{\chi}_k)$ be the length of the longest arithmetic progression with common difference d in $\boldsymbol{\chi}_k$. For a PRUS, we must have that

$$\sum_{k=0}^{p-1} a_d(\boldsymbol{\chi}_k) \leq m. \tag{60}$$

On the other hand, $\{a_d(\boldsymbol{\chi}_k)\}$ are not independent for different values of d as it can be checked (by construction) that

$$a_{qd}(\boldsymbol{\chi}_k) \geq \left\lfloor \frac{1}{q} a_d(\boldsymbol{\chi}_k) \right\rfloor \tag{61}$$

for every $q \in \mathbb{Z}_{a_d(\boldsymbol{\chi}_k)} - \{0\}$. This immediately shows that a large $a_d(\boldsymbol{\chi}_{k_*})$ (for a $k_* \in \mathbb{Z}_p$) limits not only $a_d(\boldsymbol{\chi}_k)$ where $k \in \mathbb{Z}_p - \{k_*\}$ but also $a_d(\boldsymbol{\chi}_k)$ for some other values of d. A preliminary result from (60) is that none of $\{\boldsymbol{\chi}_k\}$ has an arithmetic progression of length greater than $m+1$. However, the number of elements of the set $(A^\times)$ of sequences for which the assigned vectors $\boldsymbol{\chi}_0, \cdots, \boldsymbol{\chi}_l$ ($l \in \mathbb{Z}_p$) are not feasible according to (60) and (61) is significantly larger than the number of sequences for which at least one of the elements of the set $\{\boldsymbol{\chi}_0, \cdots, \boldsymbol{\chi}_l\}$ has an arithmetic progression of length greater than $m+1$. We further note that $A^\times$ is a subset of all sequences that the proposed construction approach identifies as unsuitable for PRUS before assigning all $\{\boldsymbol{\chi}_k\}_{k \in \mathbb{Z}_p}$.

Acknowledgement

The authors are grateful to Prof. Matthew Geoffrey Parker for his detailed comments on an early version of this paper.

References

[1] L. Bomer and M. Antweiler, "Perfect N-phase sequences and arrays [spread spectrum communication]," *IEEE Journal on Selected Areas in Communications*, vol. 10, no. 4, pp. 782–789, May. 1992.

[2] S. Ma and W. Ng, "On non-existence of perfect and nearly perfect sequences," *International Journal of Information and Coding Theory*, vol. 1, no. 1, pp. 15–38, 2009.

[3] E. Gabidulin, "Partial classification of sequences with perfect auto-correlation and bent functions," in *IEEE International Symposium on Information Theory*, Whistler, B.C. Canada, Sept. 1995, p. 467.

[4] N. Levanon and E. Mozeson, *Radar Signals*. New York: Wiley, 2004.

[5] H. He, J. Li, and P. Stoica, *Waveform design for active sensing systems: a computational approach*. Cambridge University Press, 2012.

[6] J. Benedetto, I. Konstantinidis, and M. Rangaswamy, "Phase-coded waveforms and their design," *IEEE Signal Processing Magazine*, vol. 26, no. 1, pp. 22–31, Jan. 2009.

[7] S. W. Golomb and G. Gong, *Signal design for good correlation: for wireless communication, cryptography, and radar*. Cambridge University Press, 2005.

[8] W. H. Mow, "A new unified construction of perfect root-of-unity sequences," in *IEEE 4th International Symposium on Spread Spectrum Techniques and Applications Proceedings*, vol. 3, Mainz, Germany, Sept. 1996, pp. 955–959.

[9] P. Fan and M. Darnell, "The synthesis of perfect sequences," in *Cryptography and Coding*, ser. Lecture Notes in Computer Science, C. Boyd, Ed. Springer Berlin / Heidelberg, 1995, vol. 1025, pp. 63–73.

[10] H. Luke, "Almost-perfect polyphase sequences with small phase alphabet," *IEEE Transactions on Information Theory*, vol. 43, no. 1, pp. 361–363, Jan. 1997.

[11] P. Fan and M. Darnell, *Sequence Design for Communications Applications*. New York: Wiley, 1996.

[12] M. Soltanalian, M. M. Naghsh, and P. Stoica, "A fast algorithm for designing complementary sets of sequences," *Signal Processing*, vol. 93, no. 7, pp. 2096–2102, 2013.

[13] M. Soltanalian and P. Stoica, "Computational design of sequences with good correlation properties," *IEEE Transactions on Signal Processing*, vol. 60, no. 5, pp. 2180–2193, 2012.

[14] P. Stoica, H. He, and J. Li, "On designing sequences with impulse-like periodic correlation," *IEEE Signal Processing Letters*, vol. 16, no. 8, pp. 703–706, Aug. 2009.

[15] ——, "New algorithms for designing unimodular sequences with good correlation properties," *IEEE Transactions on Signal Processing*, vol. 57, no. 4, pp. 1415–1425, Apr. 2009.

[16] E. Gabidulin and V. Shorin, "New families of unimodular perfect sequences of prime length based on gaussian periods," in *IEEE International Symposium on Information Theory*, Lausanne, Switzerland, 2002, p. 68.

[17] E. Gabidulin, "New perfect sequences of length $2p$," in *Proceedings of the ACCT-6*, Pskov, Russia, 1998, pp. 119–122.

[18] E. Gabidulin and V. Shorin, "Perfect sequences of length $3p$," in *IEEE International Symposium on Information Theory*, Yokohama, Japan, June 2003, p. 432.

[19] ——, "Perfect sequences of length $p_1 p_2$," in *Seventh International Symposium on Communication Theory and Applications*, Ambleside, Lake District, UK, July 2003.

[20] ——, "Unimodular perfect sequences of length p^s," *IEEE Transactions on Information Theory*, vol. 51, no. 3, pp. 1163–1166, Mar. 2005.

[21] H. Luke, "Sequences and arrays with perfect periodic correlation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 24, no. 3, pp. 287–294, May 1988.

[22] M. Soltanalian and P. Stoica, "Perfect root-of-unity codes with prime-size alphabet," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. Prague, Czech Republic: IEEE, 2011, pp. 3136–3139.

[23] T. Y. Lam and K. H. Leung, "On vanishing sums of roots of unity," *Journal of Algebra*, vol. 224, no. 1, pp. 91–109, 2000.

[24] T. Andreescu, D. Andrica, and I. Cucurezeanu, *An Introduction to Diophantine Equations: A Problem-based Approach*. Springer, 2010.

[25] A. Tripathi, "On a linear Diophantine problem of Frobenius," *Integers*, vol. 6, p. A14, 2006.

[26] J. L. R. Alfonsín, *The Diophantine Frobenius problem*. Oxford, UK: Oxford University Press, 2005.

[27] M. Buratti, "Old and new designs via difference multisets and strong difference families," *Journal of Combinatorial Designs*, vol. 7, no. 6, pp. 406–425, 1999.

[28] D. R. Stinson, *Combinatorial designs: constructions and analysis*. Springer, 2004.

[29] H. S. M. Coxeter, *Regular Polytopes*. MacMillan, 1963.

[30] H. D. Luke, L. Bomer, and M. Antweiler, "Perfect binary arrays," *Signal Processing*, vol. 17, no. 1, pp. 69–80, 1989.

[31] E. Szemerédi, "On sets of integers containing no k elements in arithmetic progression," *Acta Arithmetica*, vol. 27, pp. 299–345, 1975.

[32] W. Gowers, "A new proof of Szemerédi's theorem," *Geometric and Functional Analysis*, vol. 11, pp. 465–588, 2001.

[33] T. C. Brown and D. R. Hare, "Arithmetic progressions in sequences with bounded gaps," *Journal of Combinatorial Theory, Series A*, vol. 77, no. 2, pp. 222–227, 1997.

[34] W. Watkins and J. Zeitlin, "The minimal polynomial of $\cos(2\pi/n)$," *The American Mathematical Monthly*, vol. 100, no. 5, pp. pp. 471–474, 1993.

[35] I. Niven, *Irrational Numbers*. New York: Mathematical Association of America and Wiley, 1956.

[36] M. G. Parker, "Even length binary sequence families with low negaperiodic autocorrelation," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*. Springer, 2001, pp. 200–209.

[37] T. Jiang, X. Zhao, and L. Hou, "Perfect punctured binary sequence pairs," *Journal of Electronics (China)*, vol. 20, no. 4, pp. 285–288, 2003.

[38] Y. Manin and A. Panchishkin, *Introduction to Modern Number Theory, Encyclopaedia of Mathematical Sciences, vol.49 (2nd ed.)*. Springer-Verlag, 2005.

[39] G. Shimura, "The representation of integers as sums of squares," *American Journal of Mathematics*, vol. 124, no. 5, pp. pp. 1059–1081, 2002.

[40] S. Cooper, "Sums of five, seven and nine squares," *The Ramanujan Journal*, vol. 6, pp. 469–490, 2002.

[41] P. Barrucand and M. D. Hirschhorn, "Formulae associated with 5, 7, 9 and 11 squares," *Bulletin of the Australian Mathematical Society*, vol. 65, no. 03, pp. 503–510, 2002.

[42] S. Cooper, "On the number of representations of certain integers as sums of 11 or 13 squares," *Journal of Number Theory*, vol. 103, no. 2, pp. 135–162, 2003.