



Abstract

In this paper, Perfect Root-of-Unity Codes (PRUCs) 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 in PRUCs over α_p is derived. We show that PRUCs of length $L \geq p(p-1)$ must use all phases in α_p . It is also shown that if there exists a PRUC of length L over α_p then p divides L . We derive equations (which we call principal equations) that give possible lengths of a PRUC over α_p together with their phase distribution.

Introduction

• Root-of-unity codes and their autocorrelation lags:

$$\bullet \mathbf{x} = \{x_l\}_{l=0}^{L-1} = \left\{ e^{j \frac{2\pi}{p} k_l} \right\}_{l=0}^{L-1} \longrightarrow L\text{-length PRUC over } \alpha_p$$

• The periodic autocorrelation of \mathbf{x} at lag $u \in \mathbb{Z}_L$ is defined as

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

• Applications:

communication systems for Frequency-Hopping Spread-Spectrum Multiple-Access (FH/SSMA), Direct-Sequence Spread-Spectrum Multiple-Access (DS/SSMA), pulse compression for continuous-wave radars, fast startup equalization and channel estimation.

• This paper considers perfect unimodular codes in finite-alphabet case.

Phase Study

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

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

$$L = mp, m \in \mathbb{N}$$

Corollary 2. Let $\mathbf{x} = \left\{ e^{j \frac{2\pi}{p} k_l} \right\}_{l=0}^{mp-1}$ be a PRUC 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 $k_l \equiv k_{l+u} + s \pmod{p}$.

• Lower bound on the number of distinct phases in the code:

Let Φ_x be the circulant matrix made from integer phases $\{k_l\}$ of the code

$$\Phi_x = \begin{pmatrix} k_0 & k_1 & \cdots & k_{mp-1} \\ k_{mp-1} & k_0 & \cdots & k_{mp-2} \\ \vdots & \vdots & \ddots & \vdots \\ k_1 & k_2 & \cdots & k_0 \end{pmatrix}$$

For the l^{th} column of Φ_x , consider the location of the entries which are equal to k_l ($l = 0, \dots, p-1$). Considering these locations for all columns, we build an $mp \times mp$ equivalence matrix Φ_e whose entries in the mentioned locations are 1; otherwise they are 0.

- If μ_k represents the number of times that $e^{j \frac{2\pi}{p} k}$ occurs in the sequence then $\sum_{k=0}^{p-1} \mu_k = mp$.
- Based on Corollary 2, all rows of Φ_e have exactly m ones except the first row whose all entries are one. \longrightarrow there are $mp + m(mp-1)$ ones in Φ_e .
- On the other hand, since every integer phase $k \in \mathbb{Z}_p$ gives μ_k columns with μ_k ones in each of them, the number of ones in Φ_e is equal to $\sum_{k=0}^{p-1} \mu_k^2$ and therefore $\sum_{k=0}^{p-1} \mu_k^2 = mp + m(mp-1)$.
- Now let us assume that t of $\{\mu_k\}$ are nonzero. From the Cauchy-Schwarz inequality we have $\sum_{k=0}^{p-1} \mu_k^2 \geq \frac{1}{t} \left(\sum_{k=0}^{p-1} \mu_k \right)^2$ and as a result $t \geq \frac{mp^2}{(m+1)p-1}$.

Corollary 3. For $m \geq p-1$, all phase values must be used in a PRUC.

The Principal Equations

Now, for every $s \in \mathbb{Z}_p - \{0\}$, let us build the Φ_e matrix¹ as follows: by finding the locations of the entries k_l in the l^{th} column of Φ_x such that $k_l \equiv k_{l+s} \pmod{p}$, we represent these locations in Φ_e by 1, and by 0 otherwise. Based on Corollary 2, for every $u \in \mathbb{Z}_L - \{0\}$, there exist exactly m distinct integers $\{l\}$ such that $k_{l+u} \equiv k_l + s \pmod{p}$. Therefore the Φ_e matrix has exactly m ones in each of its rows except for the first row which is all zero. This implies that Φ_e has $m(mp-1)$ ones. On the other hand, the number of ones in Φ_e is equal to $\sum_{k=0}^{p-1} \mu_k \mu_{k+s}$ as it equals the number of all pairs with the property $k_{l+u} \equiv k_l + s \pmod{p}$. Therefore, all out-of-phase correlations $\left\{ \sum_{k=0}^{p-1} \mu_k \mu_{k+s} \right\}_{s \in \mathbb{Z}_p - \{0\}}$ of the $\{\mu_k\}$ sequence are equal to $m(mp-1)$.

- Let $r_k = \mu_k - m$,

the principal equations:

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

• Geometrical study of the principal equations:

Let $\mathbf{r}_0 = (r_0, \dots, r_{p-1})^T$ and also let \mathbf{r}_k represent the circularly shifted version of \mathbf{r}_0 by $k \in \mathbb{Z}_p$.

The principal equations can be rephrased as follows over all vectors $\{\mathbf{r}_k\}$:

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

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

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

We note that the structure made by connecting all vertices pointed by $\{\mathbf{r}_k\}$ is a known multi-dimensional object called a *Regular Simplex*.

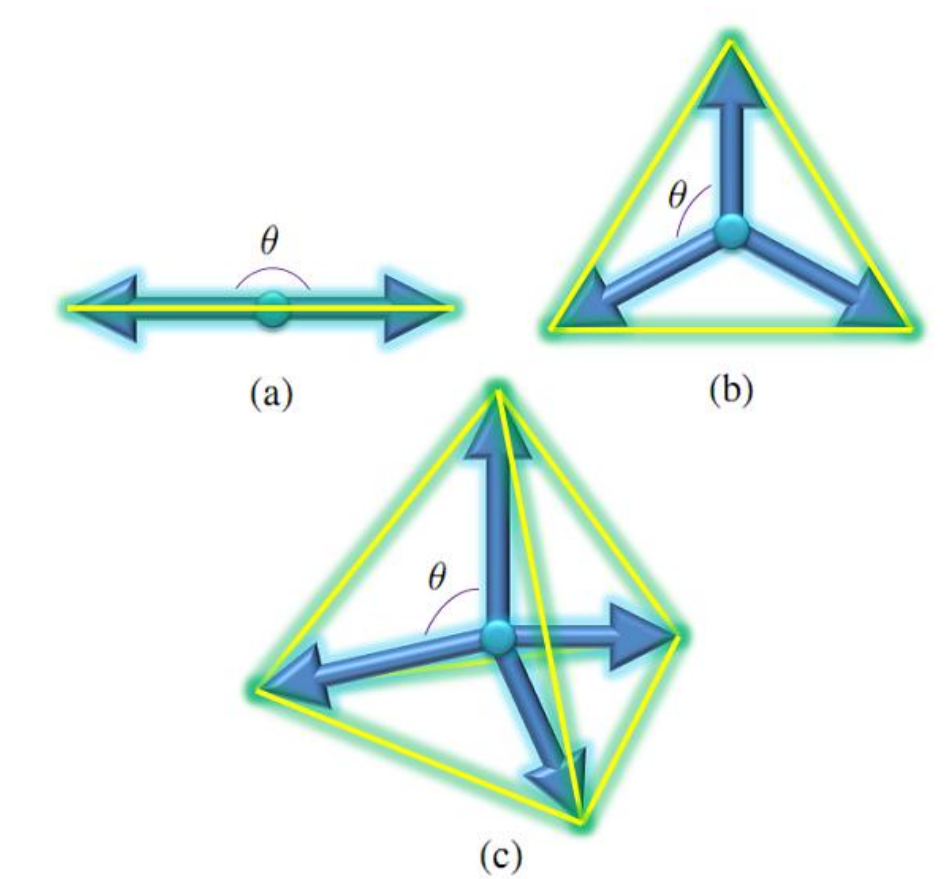


Fig. 1. (a-c) Regular Simplexes in one, two and three dimensional space. In n dimensions they can be characterized with $n+1$ vectors with the same l_2 -norm and also the same angle between them.

¹The dependency of $\{\Phi_e\}$ matrices on s is not explicitly shown for notational simplicity.

The Principal Equations: Solutions

• Analytical solutions:

As an example for using the regular simplex to solve the principal equations we study the case of $p=3$: for 3-phase perfect codes, the $\{\mathbf{r}_k\}$ make a two dimensional regular simplex orthogonal to $\mathbf{1}_3$, which has 3 vectors and each two of them have an angle of $\frac{2\pi}{3}$.

Let: \mathbf{R}_{1_3} be the unitary rotation matrix which maps $\mathbf{1}_3$ to $\sqrt{3}e_3^{(3)}$ and $\mathbf{r}'_k = \sqrt{2m} \left(\cos \left(\frac{2k\pi}{3} + \psi \right), \sin \left(\frac{2k\pi}{3} + \psi \right), 0 \right)^T$ for $k \in \mathbb{Z}_3, \psi \in [0, 2\pi)$.

\mathbf{r}_k is equal to $\mathbf{R}_{1_3}^{-1} \mathbf{r}'_k$ for some ψ

$$\mathbf{r}_k \in \mathbb{Z}^3 \text{ is of the form } \sqrt{2m} \begin{pmatrix} \frac{\sqrt{2}}{2} \cos \left(\frac{2k\pi}{3} + \psi \right) - \frac{\sqrt{6}}{6} \sin \left(\frac{2k\pi}{3} + \psi \right) \\ \frac{\sqrt{6}}{3} \sin \left(\frac{2k\pi}{3} + \psi \right) \\ -\frac{\sqrt{2}}{2} \cos \left(\frac{2k\pi}{3} + \psi \right) - \frac{\sqrt{6}}{6} \sin \left(\frac{2k\pi}{3} + \psi \right) \end{pmatrix}$$

For $k=0$,

$$\begin{cases} h_1 = 2\sqrt{\frac{m}{3}} \sin \psi \\ \text{(which is the second entry of } \mathbf{r}_0) \\ h_2 = 2\sqrt{m} \cos \psi \\ \text{(which is the difference between} \\ \text{the first and the third entry of } \mathbf{r}_0) \end{cases}$$

both must be integers.

Therefore,

the code length must be of the form

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

and the phase distribution is given by

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

• Computational solutions:

p	Length (L)	Phase distribution $\{\mu_k\}_{k=0}^{p-1}$
5	5	(2, 1, 2, 0, 0) (2, 2, 0, 1, 0)
	20	(6, 4, 6, 2, 2) (6, 6, 2, 4, 2)
	25	(6, 6, 6, 6, 1) (9, 4, 4, 4, 4)
	45	(12, 9, 12, 6, 6) (12, 12, 6, 9, 6)
	55	(16, 12, 10, 10, 7) (16, 10, 12, 7, 10)
	65	(15, 6, 10, 12, 12) (15, 12, 6, 12, 10)
7	80	(20, 16, 20, 12, 12) (20, 20, 12, 16, 12)
	100	(28, 18, 18, 18, 18) (22, 22, 22, 22, 12)
	7	(2, 2, 1, 0, 0, 2, 0)
	28	(6, 6, 4, 2, 2, 6, 2) (7, 5, 5, 2, 5, 2, 2)
	49	(13, 6, 6, 6, 6, 6, 6) (8, 8, 8, 8, 8, 8, 1)
56	(11, 10, 10, 5, 10, 5, 5) (11, 11, 6, 11, 6, 6, 5)	
63	(12, 12, 9, 6, 6, 12, 6)	
98	(17, 17, 17, 10, 17, 10, 10) (18, 18, 11, 18, 11, 11, 11)	

Table 1. All possible lengths (less than or equal to 100) of PRUCs over α_p for $p=5$ and 7 together with phase distributions.