PERFECT ROOT-OF-UNITY CODES WITH PRIME-SIZE ALPHABET

Mojtaba Soltanalian and Petre Stoica
Dept. of Information Technology, Uppsala University, Uppsala, Sweden

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

Introduction

- Root-of-unity codes and their autocorrelation lags:
  \[ x = \{x_t\}_{t=0}^{L-1} = \{e^{j2\pi t/k}\}_{t=0}^{L-1} \quad \text{L-length PRUC over } \alpha_p \]
  The periodic autocorrelation of \( x \) at lag \( u \in \mathbb{Z}_L \), is defined as
  \[ R_u = \sum_{t=0}^{L-1} x^* e^{-j\frac{2\pi u t}{L}} \]

- 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 \( \sum_{i=0}^{m-1} a_i e^{j2\pi i/k} = 0 \) for some \( a_i \in \mathbb{Z} \) and prime \( p \), then all \( a_i \) must be identical.

Corollary 1. If there exists a PRUC of length \( L \) over \( \alpha_p \), then \( pL \).

Corollary 2. Let \( x = \{e^{j2\pi t/k}\}_{t=0}^{L-1} \) be a PRUC of length \( L = mp \) over \( \alpha_p \). Then for every \( s \in \mathbb{Z}_p \) and \( v \in \mathbb{Z}_L \), there exist exactly \( m \) distinct integers \( \{l\} \) such that \( k_l \equiv k_{l+s} \mod p \).

Lower bound on the number of distinct phases in the code:
Let \( \Phi \) be the circulant matrix formed from integer phases \( \{k_l\} \) of the code
\[ \Phi = \begin{pmatrix}
  k_0 & k_1 & \cdots & k_{mp-1} \\
  k_{mp-1} & k_0 & \cdots & k_{mp-2} \\
  \vdots & \vdots & \ddots & \vdots \\
  k_1 & k_2 & \cdots & k_0
\end{pmatrix} \]

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

- If \( \mu \) represents the number of times that \( e^{j2\pi l/k} \) occurs in the sequence then \( \sum_{i=0}^{m-1} \mu_i = mp \).
- Based on Corollary 2, all rows of \( \Phi \) have exactly \( m \) ones except the first row whose all entries are one, and there are \( mp = (m-1)p \) ones in \( \Phi' \).
- On the other hand, since every integer phase \( k \in \mathbb{Z}_p \) gives \( \mu \) columns with \( \mu \) ones in each of them, the number of ones in \( \Phi' \) is equal to \( \sum_{i=0}^{m-1} \mu_i^2 \) and therefore \( \sum_{i=0}^{m-1} \mu_i^2 = mp(m-1) \).
- Now let us assume that \( t \) is the number of \( \mu \) that are nonzero. From the Cauchy-Schwarz inequality we have \( \sum_{i=0}^{m-1} \mu_i^2 \geq \frac{1}{m} \left( \sum_{i=0}^{m-1} \mu_i \right)^2 \) 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 \( s \in \mathbb{Z}_p \), let us build the \( \Phi \) matrix as follows: by finding the locations of the entries \( k_l \) in the \( l \)-th column of \( \Phi \) such that \( k_l \equiv k_{l+s} \mod p \), we represent these locations in \( \Phi \), by 1, and 0 otherwise. Based on Corollary 2, for every \( u \in \mathbb{Z}_L \), there exist exactly \( m \) distinct integers \( \{l\} \) such that \( k_{l+s} = k_{l+s} \mod p \). Therefore, the \( \Phi \) matrix has exactly \( m \) rows except for the first row which is all zero. This implies that \( \Phi \) has \( mp-1 \) ones. On the other hand, the number of ones of \( \Phi \) is equal to \( \sum_{l=0}^{mp-1} \mu_l \), as it equals the number of all pairs with the property \( k_{l+s} = k_{l+s} \mod p \). Therefore, all-out-of-phase correlations \( \sum_{l=0}^{mp-1} e^{j2\pi u(l)} \) of the \( \mu_l \) sequence are equal to \( m(mp-1) \).

- Let \( r_k = \mu_k - \mu_l \), the principal equations:
  \[ \sum_{l=0}^{mp-1} e^{j2\pi u(l)} = 0 \quad \sum_{l=0}^{mp-1} r_k e^{j2\pi u(l)} = m(mp-1) \]

Geometrical study of the principal equations:
Let \( r_0 \) be \( r_0, r_1, \ldots, r_{mp-1} \) and also let \( r_0 \) represent the circularly shifted version of \( r_0 \) by \( k \in \mathbb{Z}_p \).

The principal equations can be rephrased as follows over all vectors \( \{x_t\} \):
\[ \begin{align*}
  r_0 & = 0 \\
  r_k r_l & = m(mp-1) \\
  r_k r_{k+l} & = m(mp-1) \quad k \neq l
\end{align*} \]

The angle between each pair of vectors \( \{r_0, r_1\} \) is
\[ \theta = \arccos \left( \frac{r_0 r_1}{\|r_0\| \|r_1\|} \right) = \arccos \left( \frac{1}{p-1} \right) \]

We note that the structure made by connecting all vertices pointed by \( r_0 \) is a known multi-dimensional object called a Regular Simplex.

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

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 \( \{\mu_l\} \) make a two dimensional regular simplex orthogonal to \( 1,0 \), which has 3 vectors and each two of them have an angle of \( \frac{\pi}{3} \).

Let: \( R_0 \) be the unitary rotation matrix which maps \( 1,0,1 \) to \( \sqrt{2/3},1/\sqrt{3} \) and \( v = \sqrt{2/3} \cos (\frac{2\pi}{3} + \phi) \sin (\frac{2\pi}{3} + \phi) \) for \( k \in \mathbb{Z}_p \), \( \phi \in [0, 2\pi] \).

- \( r_0 \) is equal to \( R_0^t v \) for some \( v \)
- For \( k = 0 \), \( k_1 = 2\sqrt{3/2} \sin \phi \) (which is the second entry of \( r_0 \))
- \( k_2 = 2\sqrt{3/2} \cos \phi \) (which is the difference between the first and the third entry of \( r_0 \))

Therefore, the code length must be of the form
\[ L = \frac{1}{3} (3h_0 + 3h_1) \]
and the phase distribution is given by
\[ \frac{1}{4} \left( 3h_0 + h_1 \right) \begin{pmatrix}
  b_0 - b_1 \\
  b_2 - b_1
\end{pmatrix} + \frac{1}{2} \begin{pmatrix}
  b_0 \\
  b_2
\end{pmatrix} \]

Computational solutions:

Table 1. All possible lengths \( L \) of PRUCs over \( \alpha_p \) for \( p = 5 \) and \( 7 \) together with phase distributions.