Polyphase alternating codes

Markku Markkanen\textsuperscript{1} and Juha Vierinen\textsuperscript{2}

\textsuperscript{1} Eigenor Corporation \textsuperscript{2} Sodankylä Geophysical Observatory

Abstract. This work introduces a method for constructing polyphase alternating codes in which the length of a code transmission cycle can be $p^m$ or $p - 1$, where $p$ is a prime number and $m$ is a positive integer. The relevant properties leading to the construction alternating codes and the algorithm for generating alternating codes is described. Examples of all practical and some not that practical polyphase code lengths are given.

1 Introduction

Alternating codes (\cite{Lehtinen1986}) are widely used in incoherent scatter radar measurements and their properties are well known. Currently, the only so called type 1 code lengths are powers of two, which sometimes causes inflexibility when designing radar experiments. With this in mind, \cite{Sulzer1993} proposed a new type of alternating codes (type 2) that made it possible to use other code lengths. These codes also produce unambiguous back-scatter autocorrelation function estimates of the target. But there does not exist a search strategy efficient enough for finding longer type 2 codes. To best of our knowledge, the longest type 2 alternating code length is 14, which is not necessarily large enough for all applications.

In this paper we generalize previous work \cite{Markkanen1997} and apply it to polyphase codes, i.e., codes that are phase coded with two or more different phases. We have identified two different types of polyphase alternating codes. The first type includes codes that have $p$ phases and code lengths of $p^m$, where $p$ is a prime number and $m$ is a positive integer. The other class contains codes with $p - 1$ phases and code length $p - 1$. The number of codes in these kinds of alternating code sets is the same as the number of bauds in a code. The first 50 alternating code lengths are shown in Fig. 1.

This paper concentrates on polyphase alternating codes satisfying the so called weak condition. Strong codes can be generated from weak codes using the method described by \cite{Sulzer1989}. This method also works for the polyphase alternating codes presented in this work. To create an alternating code set satisfying the strong condition, the code set is duplicated. For each code in the duplicated part, bauds with even indices are multiplied by $-1$.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{alternating_code_lengths.png}
\caption{First 50 alternating code lengths, solid black circles represent known binary phase alternating codes, open circles represent new polyphase alternating code lengths.}
\end{figure}
2 Construction of $p$-nary alternating codes

By a $p$-nary radar pulse we mean a phase modulated pulse, where the complex phases of bauds belong to set $E_p = \{1, \alpha, \ldots, \alpha^{p-1}\}$, where $\alpha = e^{2\pi i/p}$. In what follows, $p$ is a prime number unless otherwise stated. A $p$-nary alternating code of length $n$ is a set of sequences $A_0 = (a_0, 0, \ldots, a_0, n-1), \ldots, A_n = (a_{n-1}, 0, \ldots, a_{n-1}, n-1)$ of $p$-nary pulses satisfying the natural extension of the weak condition given in [Lehtinen 1986] for binary codes:

**Condition 1.** For each $i, i', j$ and $j'$ where $j-i = j'-i'$, $i \neq j$, and $i \neq i'$.

$$\sum_{k=0}^{n} a_{k,i}a_{k,j}a_{k,i'}a_{k,j'} = 0$$

Let us denote by $M$ the operator, which shifts the elements of a sequence cyclically by one, that is

$$M(a_0, \ldots, a_{n-1}) = (a_1, \ldots, a_{n-1}, a_0).$$

Let $A = (a_0, \ldots, a_{n-1})$ be a $p$-nary sequence and let us denote by $U$ the unit sequence $U = (1, 1, \ldots, 1)$. By multiplication of two sequences we mean pointwise multiplication of them and will denote it by $\otimes$. Similarly we will mean by conjugate of $A$ the pointwise complex conjugate of $A$ and denote it by $\overline{A}$. Then $A \otimes \overline{A} = U$, because $|a_i| = 1$ for all $i$.

Let us denote by $C$ the set of sequences $A, MA, \ldots, M^{n-1}A, U$. Here $M^i$ means $i$ repeated cyclical shift operations. We will show that when $A$ satisfies the following two conditions, $C$ will constitute a $p$-nary alternating code set:

**Condition 2.** All the sequences of $C$ are different.

**Condition 3.** Multiplying all the sequences of $C$ by a fixed one of it permutes $C$.

To prove this, we need the following properties of the sequences satisfying conditions 2 and 3:

**Property 1.** The sum $s$ of elements of $A$ is $-1$.

This can be seen by considering the sequence $S = A + MA + \cdots + M^{n-1}A + U$, which equals $(s+1)U$ (the sequences $A, \ldots, M^{n-1}A$ contain in each location all the elements of $A$ in some cyclic order). Because by condition 3 multiplication by $A$ permutes the terms of $S$, $A \otimes S = S$, and because $A \otimes U = A$, it follows that

$$(s+1)A = (s+1)U.$$

Now condition 2 requires that $A \neq U$. Thus $s + 1 = 0$ and $s = -1$.

Notice that in the case of $p = 2$, when $E_p = \{1, -1\}$, it follows from property 1 that $n$ is odd.

**Property 2.** There exists $s_i$ so that $M^iA = M^{i+s_i}A$ for all $i$.

By condition 3 there is $s_0$ so that $A \otimes M^{s_0}A = U$, that is, $M^{s_0}A = \overline{A}$. Then

$$M^iA = M^i\overline{A} = M^iM^{s_0}A = M^{i+s_0}A,$$

for any $i$.

Let as denote by $A^i$ the sequence formed by taking the the $i$th elements of sequences $A_0, \ldots, A_{n-1}$. Condition 3 is then the requirement that sum of elements of sequence $D = A^i \otimes A^i$ equals $U$ (coming from $A_n = U$) is 0, that is sum of elements of $D$ is $-1$.

Now $A^i = M^iA$ and thus

$$D = M^iA \otimes M^i\overline{A} = M^iA \otimes M^i\overline{A}.$$
3 Construction of sequence A

Instead of set $E_p$ we will consider the set $\mathbb{Z}_p = \{0, \ldots, p - 1\} \mod p$ of possible exponents of $\alpha$. Instead of sequences with elements in $E_p$ we then have vectors in vector space $\mathbb{Z}_p^n$, multiplication of sequences corresponds to addition, multiplication by complex conjugate corresponds to subtraction and $U$ is replaced by 0-vector $0 \in \mathbb{Z}_p^n$. The operator $M$ corresponds to a linear operator mapping each base vector of $\mathbb{Z}_p^n$, to the previous one, except the first one, which is mapped to the last one.

Let us thus have a vector $A = (a_0, \ldots, a_{n-1}) \in \mathbb{Z}_p^n$ and set $C = \{A, MA, \ldots, M^{n-1}A, 0\} \subset \mathbb{Z}_p^n$. Conditions 2 and 3 then correspond to the following conditions:

**Condition 3a.** All the vectors in $C$ are different.

**Condition 3a.** Adding a fixed vector of $C$ to all vectors belonging to it permutes $C$.

The sum of any two vectors in $C$ belong to $C$ by condition 3a. In fact, when condition 2a is satisfied, condition 3a is equivalent to the condition that sum of any two vectors in $C$ belong to $C$, because addition of a fixed vector is then bijection. Because for any $B \in C$ also $2B = B + B \in C$ and similarly for any $k \in \mathbb{Z}_p$ by induction, it follows that $C$ is a vector subspace of $\mathbb{Z}_p^n$. If $\dim(C) = m$, number of vectors in $C$ is $p^m$, and thus $n = p^m - 1$.

Let us now consider in $\mathbb{Z}_p$ a $m^{th}$-order difference equation

$$x_{i+m} = b_{m-1}x_{i+m-1} + \ldots + b_0x_i, \quad i = 0, \ldots,$$

with $b_0, \ldots, b_{m-1} \in \mathbb{Z}_p$. Because there is only a finite number of different $m$-tuples of elements of $\mathbb{Z}_p$, any sequence, which is solution of (2), is periodic (possible beginning with a non-periodic part if $b_0 = 0$). Let us suppose that (2) has a solution $A' = \{a_i\}_{i=0}^\infty$ with period $n = p^m - 1$. Then the vector $A = (a_0, \ldots, a_{n-1}) \in \mathbb{Z}_p^n$ satisfies conditions 2a and 3a.

Periodic part of $A'$ contains all $p^m - 1$ different non-zero $m$-tuples, and so $A'$ can’t have non-periodic part. Then $a_n = a_0, a_{n+1} = a_1, \ldots$ and the $m$-tuples $(a_0, \ldots, a_{m-1}), (a_1, \ldots, a_m), \ldots, (a_{m-1}, \ldots, a_{m+n-2}), (0, \ldots, 0)$, which are the starts of vectors $A, MA, \ldots, M^{n-1}A, 0$ are all the $p^m$ different $m$-tuples of $\mathbb{Z}_p$, proving condition 1a. If $B_1, B_2 \in C$, there is $B_3 \in C$ such that the first $m$ elements of $B_1 + B_2$ are equal to the first $m$ elements of $B_3$. Because $B_1 + B_2$ is also a solution of (2), it follows that $B_1 + B_2 = B_3$, proving condition 2a.

Notice that we can choose as our $A$ any nonzero vector of $C$, e.g., one starting with $m - 1$ zeros followed by $1$.

Thus, in order to satisfy the original condition for alternating codes, it is sufficient that the following condition is satisfied:

**Condition 4.** The $m^{th}$ order difference equation in $\mathbb{Z}_p$ has a period $p^m - 1$.

4 The number of $p^m$-type alternating codes

If all the roots of polynomial $Q(x) = x^n - b_{n-1}x^{n-1} - \ldots - b_0$ are different, the general solution of the difference equation (2) is

$$x_i = c_1\alpha_1^i + \ldots + c_m\alpha_m^i, \quad i = 0, \ldots,$$

where $\alpha_1, \ldots, \alpha_m$ are the roots of $Q(x)$ and $c_1, \ldots, c_m$ are arbitrary coefficients. If $Q(x)$ is irreducible in $\mathbb{Z}_p[x]$ and there is no integer $d$ smaller than $n$ such that $Q(x)$ divides $x^d - 1$, the roots of $Q(x)$ are different and the period of all sequences $\{1, \alpha_1, \alpha_2^2, \ldots\}$ is $n$, and so is then also the period of sequence $\{x_0, x_1, \ldots\}$. Thus each $m$-degree polynomial $Q(x) \in \mathbb{Z}_p[x]$ satisfying the above mentioned conditions determines a $p$-nary alternating code, and it is easy to see that different $Q$’s determine different codes by comparing for all locations of 1, the elements following $m$-tuple $(0, 0, 1, 0, \ldots, 0)$ in the solutions of corresponding difference equations.

It is possible to show (e.g., [Lidl and Niederreiter 1997], p. 85) that the number of different polynomials $N_c$ satisfying the above mentioned conditions is

$$N_c = \frac{\varphi(p^m - 1)}{m}.$$

Here $\varphi(i)$ is the Euler $\varphi$-function, which is the number of integers smaller than $i$ which do not have a common factor with $i$. It can also be shown that there are no other sets $C$ satisfying conditions 1a and 2a, so the number $N_c$ given above is the number of different alternating codes satisfying those conditions. This means especially that for any prime number $p$ and any positive integer $m$ there exist $p$-nary alternating codes of length $p^m$.

5 $p$-nary alternating codes of length $p$

We will now look more closely at the case $m = 1$. In this case the difference equation is simply

$$x_{i+1} = b_0x_i, \quad b_0 \in \mathbb{Z}_p, \quad i = 0, 1, \ldots$$

and if we choose $x_0 = 1$, it’s solution is $x_i = b_0^i \mod p$.

We get thus a suitable $A$, if and only if all the numbers $b_0, b_0, \ldots, b_0^{p-2} \mod p$ are different, that is, if $b_0$ is the generator of the cyclic multiplicative group $\mathbb{Z}_p^*$. As an example, let us have a look at primes 3 and 5. The only generator of $\mathbb{Z}_5^*$ is $b_0 = 2$, giving the set of exponent sequences

$$C = \{(1, 2, 1), (2, 1, 2), (0, 0, 0)\},$$

for the base element $\alpha = e^{2\pi i/3}$. For $\mathbb{Z}_7^*$ there are two generators $b_0 = 2, 3$, giving the sets
For the “dual” sequence $A'$ with indices $1, b_0, \ldots, b_0^{p-2}$ and corresponding values $0, 1, \ldots, p-2$ this means that all differences $(\mod p - 1)$ of values of elements of $A'$ with fixed difference $(\mod p)$ of indices are different.

But this is again stronger than the condition for $(p-1)$-nary alternating codes: all differences $(\mod p - 1)$ of values of elements of $A'$ with fixed difference of indices are different, and thus the sequence $A'$ defines a $(p-1)$-nary alternating code of length $p-1$!

**Example:** dual 7-nary and 6-nary sequences:
When $p = 7$ and $b_0 = 3$, we have the following situation:

$\mathbb{Z}_7$

| Index | 0 | 1 | 2 | 3 | 4 | 5 |
|-------|---|---|---|---|---|---|

$\mathbb{Z}_6$

| Index | 0 | 1 | 2 | 3 | 4 | 5 |
|-------|---|---|---|---|---|---|

This gives sequence $\{1, 3, 2, 6, 4, 5, 1\}$ defining a 7-nary alternating code and sequence $\{0, 2, 1, 4, 5, 3\}$ defining a 6-nary alternating code.

It can be noted that whereas in $p$-nary codes the first and last columns are identical and the constant column of $F_p$ is not in the code, in $(p-1)$-nary codes all the columns of $F_{p-1}$ are in the code once.

The number of $p$-nary alternating codes of length $p$ is $\varphi(p-1)$ and one could think that it is also the number of $(p-1)$-nary alternating codes of length $p-1$. However, this is not the case, instead different $p$-nary codes give only different sequences of the same $(p-1)$-nary code, and thus the construction presented here gives only one $(p-1)$-nary alternating code for each prime $p$. This can be seen by noticing that if $b_0$ and $b_1$ are generators of $\mathbb{Z}_p^*$, there is $k_0$ such that $b_0 = b_1^{k_0}$. If then $A = \{a_1, a_2, \ldots\}$ and $A' = \{a_1', a_2', \ldots\}$ are dual sequences of $\{1, b_0, \ldots\}$ and $\{1, b_1, \ldots\}$, $a_{i'}^{b_0} = a_i^{b_0} = k_0k = k_0a_{i'}$, meaning that $A' = k_0A$.

### 6 Algorithm for generating $p^m$-length alternating codes

Finding alternating codes is a fairly simple computation that involves going through all possible $m$-tuples $b = (b_0, \ldots, b_{m-1})$ with elements in $\mathbb{Z}_p$. This involves going through only $p^m$ alternatives. For each $b$, we check if the corresponding $m$'th order difference equation (2) has a period of $p^m - 1$ (notice that the equation is calculated in modulo $p$ arithmetic). If this is true, then the difference equation with coefficients $b$ is a generator for an alternating code set, which can then be defined as

$$A_j = \{a_j, a_{j+p}, \ldots, a_{j+p^{m-1}}\}, \quad j \in 1, \ldots, p^m - 1,$$

$A_j = \{1, 1, \ldots, 1\}$,

where $\alpha = e^{2\pi i / p}$ and $x_j$ are the values of the generating difference equation (2), using initial values $x_1, \ldots, x_{m-1} = 0$ and $x_m = 1$.
Fig. 2. The phases of a 25 baud alternating code. The cyclic nature of the code can be easily seen. One can also see property 2 which states that each code is conjugate symmetric.

To generate a \((p - 1)\)-nary code, one first generates the corresponding \(p\)-nary code and then forms the code group using the transformation described in Sect. 5.

Table 1 lists alternating codes up to code length 366, only one code per code length is listed. The codes are expressed in terms of number of phases \(p\), generating coefficients \(b = (b_0, ..., b_{m-1})\) and code length. As an example, a 25 baud alternating code set is shown as phases in Fig. 2. A program for generating weak and strong polyphase alternating codes is available at request from the authors.

7 Discussion

It is also possible to use truncated polyphase alternating codes in a similar manner as binary phase alternating codes, in order to have smaller number of scans.

Like binary alternating codes, also general \(p\)-nary codes made in this way have the worst possible covariance structure, and need randomization as described by Lehtinen et al. (1997). The covariance structures of \((p - 1)\)-nary codes have not been studied yet.

We have also done a complete search of codes with columns from \(F_p\) for all numbers up to \(p = 15\). For numbers followed by a prime there is indeed an unique code. On the other hand, for the numbers 8, 9, 14 and 15 there are no alternating code sets. These are the first composite numbers not followed by a prime. This small search hints to the possibility that there are no \(p\)-nary alternating codes of length \(p\) formed from \(F_p\), except when \(p\) or \(p + 1\) is a prime.

8 Conclusions

Signal processing hardware today can easily generate arbitrary waveforms, this includes the polyphase codes presented in this paper. Because these codes also have a constant amplitude, there is no transmission power trade-off compared to binary phase codes. It should be pretty straightforward to modify existing correlators to use these new codes. The main benefit of polyphase alternating codes is the larger set of code lengths compared to binary phase codes.

Acknowledgements. Support for J. Vierinen was provided by the Academy of Finland (application number 213476, Finnish Programme for Centres of Excellence in Research 2006-1011).

References

Lehtinen, M.: Statistical theory of incoherent scatter measurements, EISCAT Tech. Note 86/45, 1986.
Lehtinen, M. S., Huuskonen, A., and Markkanen, M.: Randomization of alternating codes: Improving incoherent scatter measurements by reducing correlations of gated ACF estimates, Radio Science, 32, 1997.
Lidl, R. and Niederreiter, H.: Finite Fields, 2nd ed., Cambridge University Press, 1997.
Markkanen, M. and Nygrén, T.: Long alternating codes: 2. Practical search method, Radio Science, 32, 1997.
Sulzer, M. P.: Recent incoherent scatter techniques, Adv. Space Res, 9, 1989.
Sulzer, M. P.: A new type of alternating code for incoherent scatter measurements, Radio Science, 28, 1993.
Table 1. Alternating codes with lengths up to 366, only one code for each number of phases. The number of phases is denoted by $N_p$, the number of different code sets $N_c$ and the generator coefficients are denoted by $b$. The $(p - 1)$-nary codes are generated from the next consecutive prime.