The Structure of Sidelobe-Preserving Operator Groups

Gregory E. Coxson

Abstract This chapter considers the structure of groups of operators preserving the aperiodic autocorrelation peak sidelobe level of mth root codes. These groups are shown to be helpful for efficient enumeration of codes by peak sidelobe level for a given m and given code length N. In the binary case, it is shown that there is a single Abelian group of order 8 generated by sidelobe-preserving operators. Furthermore, it is shown that shared symmetry in the binary Barker codes can be discovered in a natural way by considering degeneracies of group actions. The group structure for $m = 4$ (the quad-phase case) is shown to have higher complexity; in fact, instead of a single group, there are four groups (two pairs of isomorphic groups), and they are no longer Abelian. Group structure is identified for the cases of odd code lengths N, leaving group structure for even-length cases mostly unresolved. Moving to general mth roots codes, it is shown that results found for the quad-phase case generalize quite well. In particular, it is shown that there are $4m^2$ groups. All m groups are identified for any odd m. When m is even, the structure for odd code lengths N is identified. The group structure for m even and N even is left unresolved.

Keywords Barker code • Skew-symmetry • Autocorrelation sidelobes • Binary code • Polyphase code • Unimodular code • Group action

1 Introduction

In signal processing terminology, a code is a finite sequence of complex scalars, called code elements. A code is called unimodular if each of its elements has modulus 1 (hence unimodularity refers to the elements rather than to the code which,

G.E. Coxson (✉)
Coxson Associates, 17412 Cherokee Lane, Olney, MD 20832, USA
e-mail: gcoxson@ieee.org

T.D. Andrews et al. (eds.), *Excursions in Harmonic Analysis, Volume 1,*
Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-8376-4_16,

if it has N elements, has size $\sqrt{N}$). A subset of the unimodular codes is the set of polyphase codes, for which all elements have elements that are mth roots of unity for some n. Polyphase codes with $n = 2$ are called binary codes; all elements are ± 1.

Binary and polyphase codes that achieve low aperiodic autocorrelation (AAC) average or peak sidelobe levels are valuable for radar and communications applications. This is due to the fact that the autocorrelation function approximates the response for the matched (or North) filter for phase-coded signals [16]. The matched filter is optimal for signal-to-noise ratio, and hence can pull signals out of receiver inputs where the signal is buried in noise.

If it is desired to find the lowest peak sidelobe level for a given code length, or codes which achieve it, the most approach is exhaustive search. Taking the search space as all mth root codes for some m and some length N, it is helpful to consider a partition of this space into equivalence classes relative to a group generated by sidelobe-preserving operators. If a method can be found which involves searching single representatives from each equivalence class, the search may be expedited. Furthermore, listing the best representative (for some measure of sidelobe level of interest) is more efficient than listing the best codes from the search space.

Because search techniques quickly grow computationally costly, even prohibitive-ly so, as code length grows, it is tempting to try and identify patterns in codes that might allow the construction of codes with a good chance of providing low sidelobe levels. Here is possibly another opening for the use of sidelobe-preserving operator groups, (SPGs) may provide some help. For the most notable example of low-sidelobe codes, the binary Barker codes, those of odd length share a skew-symmetric property closely linked to degeneracies in actions of the sidelobe preserving group on these codes. Knowledge of such a symmetry can narrow the search space greatly. For example, for odd-length binary codes of length N, if, rather than searching all the codes, only skew-symmetric codes are searched, the search space is reduced from size 2^N to size $2^{(N-1)/2}$. This computational cost benefit comes at the cost of possibly missing optimal-sidelobe-level codes.

It is natural to ask whether something like skew symmetry, and its connection to a group degeneracy, can be found for non-binary codes. In order to suggest this possibility, this chapter will examine a quad-phase code with Barker-level sidelobes that satisfies a symmetry much like skew symmetry. Furthermore, it will be shown that an operator in the associated group maps this code to itself, meaning that the isometry subgroup for this code has more than one element, and hence its equivalence class degenerates under group action.

The chapter is organized as follows. After an introduction (Sect. 1) and notation and terminology (Sect. 2), Sect. 3 will discuss motivation for examining SPGs. Section 4 will look at the group structure for the binary case. Section 5 will show that consideration of degeneracies in group actions for odd-length binary Barkers leads in a naturalway to the uncovering of their skew-symmetry-property. Section 6 will then consider the group structure for the quad phase case. Finally, Sect. 7 will discuss general mth root, to which findings for the quad-phase case are found to generalize quite well.

2 Basic Notation and Terminology

Let Q_m represent the set of mth roots of unity or the set of m complex numbers z such that $z^m = 1$. For a specified value of $m \geq 2$, let

$$x = [x_1, x_2, \ldots, x_N] \tag{1}$$

denote an N-length code, each of whose elements resides in Q_m. Furthermore, let $(Q_m)_N$ mean the set of codes x with elements in Q_m that is,

$$(Q_m)_N = \{x : |x| = N, x_i \in Q_m, i = 1, \ldots, N\}. \tag{2}$$

Clearly, $|(Q_m)_N| = m^N$. For the special case of $m = 2$, the codes $x \in (Q_2)_N$ will be referred to as binary codes of length N.

The AAC sequence for an $x \in (Q_m)_N$ has length $2N - 1$ and is defined by

$$\mathrm{AAC}_x = x * \overline{x^c}, \tag{3}$$

where $*$ means acyclic convolution, $\bar{x}$ means the reversal of a code x, and x^c means elementwise complex conjugation. The elements of the AAC of x may be represented explicitly in terms of sums of pairwise products of elements of x in the following way:

$$\mathrm{AAC}_x(k) = \sum_{i=1}^{N-|k-N|} x_i x^c_{i+|k-N|} \tag{4}$$

for $k = 1, \ldots, 2N - 1$. In the binary case, the elements of x are real (either 1 or -1), so the complex conjugation operation can be ignored.

The "peak" of the autocorrelation is $\mathrm{AAC}_x(N)$. The peak is equal to N, since

$$\mathrm{AAC}_x(N) = x_1 x_1^c + \cdots + x_N x_N^c = |x|^2 = N. \tag{5}$$

Elements for indices $k \neq N$ are referred to as "sidelobes" of the autocorrelation. The autocorrelation is symmetric with respect to the peak; that is,

$$\mathrm{AAC}_x(k) = \mathrm{AAC}^c_x(2N - k) \tag{6}$$

for $k = 1, \ldots, 2N - 1$.

The "peak sidelobe level" for a code x is defined to be

$$\mathrm{PSL}_x = \max_{k \neq N} |\mathrm{AAC}_x(k)|. \tag{7}$$

The lowest achievable value of PSL_x for $x \in (Q_m)_N$ for any $m \geq 2$ and $N \geq 1$ is 1. This is because when $k = 1$ or $k = 2N-1$, the sidelobe is a $x_1 x_N$, so its modulus is 1. The binary codes x that achieve $\mathrm{PSL}_x = 1$ are called Barker codes, after the author of an early paper identifying these codes [1]. When $m > 2$, codes $x \in (Q_m)_N$ that achieve $\mathrm{PSL}_x = 1$ are called generalized Barker sequences [7] or polyphase Barker sequences [6].

Finally, some notation is needed for discussing groups and group actions. An expression of the form $< g_1, g_2, \ldots, g_k >$ will mean the group generated by the elements $g_1, \ldots, g_k$. Given a group G and two elements $g, h \in G$, the notation g^h will be shorthand for the conjugation of g by h, that is, hg^{-1} (this is not to be confused with complex conjugation). Given two groups G and H, the notation $G \times H$ will represent the Cartesian product of G with H, and GH will represent a semidirect product of G and H (see, e.g., [2]).

3 PSL-Preserving Operator Groups: Motivation

Codes with low peak sidelobe level are desired in applications such as radar and communications where match filtering is used for detection (see [11, 14, 16]). For a given length, it is useful to know the lowest achievable PSL and some or all the codes which achieve it. Although there exist some well-known construction techniques for codes with low sidelobe levels, often the lowest-PSL codes must be found by random or exhaustive searches. As code length grows, random and exhaustive searches tend to become prohibitively computationally costly.

It can be informative to know how many codes achieve these lowest, or at least relatively low, PSL values. Such enumeration efforts inevitably necessitate a decision about whether to list or enumerate all such codes or to list representatives from code equivalence classes, where the equivalence is defined relative to operations that preserve autocorrelation sidelobe level.

A sidelobe-preserving operator will be understood to mean a transformation that preserves the magnitude of every sidelobe of the autocorrelation AAC_x for each $x \in (Q_m)_N$, for some m and N. Golomb and Win [8] list four sidelobe-preserving operator, for general polyphase codes. They are:

1. Reversal $\overline{x}$
2. Complex conjugation x^c
3. Constant multiple transformation (CMT): given any unit-modulus complex number α, form the product αx
4. Progressive multiplication transformation (PMT): given any unit-modulus complex number ρ, multiply the ith element, x_i, by ρ^i for $i = 1, \ldots, N$

For N-length binary codes x (i.e., $m = 2$), involving only real quantities, the set of four transformations identified by Golomb and Win reduces to a set of three somewhat simpler transformations:

1. Reversal $\overline{x}$
2. Negation $-x$
3. Alternating-sign: multiply element x_i by $(-1)^i$, $i = 1,\ldots,N$

To illustrate the usefulness of these transformations for enumeration, suppose that for $N = 13$, there is a need to determine the lowest achievable PSL for a binary code of length N and the binary codes that achieve it. This length is small enough that an exhaustive search is practical. The simplest, most naive approach would generate each of the 2^{13} codes, compute their PSL values, and keep only those with the lowest PSL. Four codes would be found having the Barker-level PSL of 1, optimal not just for length 13 but for any length. Examination of these codes would lead to the observation that any one of the four could be found by applying various compositions of the three binary transformations listed above. Hence, rather than listing all four, it is enough to list a single representative, say [16]:

$$x = \left[\, 1\ 1\ 1\ 1\ 1\ -1\ -1\ 1\ 1\ -1\ 1\ -1\ 1 \,\right]. \tag{8}$$

Behind the efficiency of this use of representatives are an equivalence relation, and a partition of the search space into equivalence classes. Given that there are three transformations being applied in various orders, these equivalence classes would be expected to hold eight codes, in general, rather than the four found having the optimal PSL for length 13. Indeed, if all eight permutations of the binary transformations are applied to the length-13 Barker code given above, and the set of eight resulting codes are tabulated, this set can be arranged into four sets of twin codes. In other words, the size-8 equivalence class degenerates into one of size 4. This suggests that the code has special structure and the structure is related to "actions" of the three transformations under composition.

Skolnik [16] lists the lowest optimal PSL values for lengths from 3 to 40, which was the best list available in 1990, along with the number of binary codes achieving these values. Skolnik uses the term "allomorphic" for codes transformable into each other by the composition of sidelobe-preserving operations ("allo-" being the Greek root for "other" and "morph" being the Greek root for "form"). The first three columns of Table 1 list these results, along with similar figures for $N = 2$.

Interestingly, the values tabulated in [16] were developed using only two of the three binary code sidelobe-preserving operators (negation and reversal). If the third one is taken into account as well, the result is for most code lengths a reduction in the number of representative codes; the results are listed in the fourth column of Table 1. For most of the lengths, the number of representative codes is reduced by half. However, there is a small set of lengths for which the extra transformation fails to change this number; this means that for these lengths, the third transformation maps the set of minimum-PSL codes into itself. Furthermore, this set of lengths, $\{3,5,7,11,13\}$, is special in that it is the set of odd lengths for which Barker codes exist.

At the least, the behavior of sidelobe-preserving operators is useful for efficient representation of codes of interest for their low peak sidelobe levels. However, it also

Table 1 Adding a third operator changes the number of representatives

N	Best PSL	Number of representatives, for negation and reversal	Number of representatives, for negation, reversal and alternating sign
2	1	2	1
3	1	1	1
4	1	2	1
5	1	1	1
6	2	8	4
7	1	1	1
8	2	16	8
9	2	20	10
10	2	10	5
11	1	1	1
12	2	32	16
13	1	1	1
14	2	18	9
15	2	26	13
16	2	20	10
17	2	8	4
18	2	4	2
19	2	2	1
20	2	6	3
21	2	6	3
22	3	756	378
23	3	1,021	515
24	3	1,716	858
25	2	2	1
26	3	484	242
27	3	774	388
28	2	4	2
29	3	561	283
30	3	172	86
31	3	502	251
32	3	844	422
33	3	278	139
34	3	102	51
35	3	222	111
36	3	322	161
37	3	110	52
38	3	34	17
39	3	60	30
40	3	114	57

appears that degeneracies in the "actions" of compositions of these transformations can uncover structures in codes having low peak sidelobe levels. These ideas will be made more precise in the following sections.

4 Sidelobe-Preserving Operator Groups: The Binary Case

The binary case has the nice property that the sidelobe-preserving transformations can each be effected by matrix operations. Hence, consider defining

1. $g_1 = -xI_N$
2. $g_2 = xJ_N$
3. $g_3 = xA_N$

where I_N is the order-N identity matrix, J_N is the order-N matrix defined by

$$J_N = \begin{pmatrix} 0\,0 \ldots 0\,1 \\ 0\,0 \ldots 1\,0 \\ \vdots\,\vdots\;\;\vdots\;\;\vdots\,\vdots \\ 0\,1 \ldots 0\,0 \\ 1\,0 \ldots 0\,0 \end{pmatrix} \tag{9}$$

and A_N is the matrix

$$A_N = \begin{pmatrix} -1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & (-1)^{N-1} & 0 \\ 0 & 0 & \ldots & 0 & (-1)^N \end{pmatrix}. \tag{10}$$

Then g_1 and g_2 preserve the autocorrelation sequence of any binary code, as can be seen by recalling that $\mathrm{AAC}_x = x * \bar{x}$. The third operator, g_3, which switches the sign of every other element of a code x, has the effect on the autocorrelation of switching the sign of every other sidelobe. However, the magnitude of every sidelobe is preserved.

The three operators g_1, g_2, and g_3 generate a group of order 8. To see this, consider five additional operators:

1. $g_0 = I_N$
2. $g_4 = g_1 \circ g_2$
3. $g_5 = g_1 \circ g_3$
4. $g_6 = g_2 \circ g_3$
5. $g_7 = g_1 \circ g_2 \circ g_3$

where the symbol $\circ$ refers to composition of operations (Table 2). The 8×8 multiplication table is given in Table 2 (where composition is used as the multiplication operator).

These eight operations constitute a group G under composition, as can be checked by showing that the result of composing any two elements lies in the group (i.e., the closure property), that the group includes an identity, that each element

Table 2 Multiplication table for the binary operators

$\circ$	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7
g_0	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7
g_1	g_1	g_0	g_4	g_5	g_2	g_3	g_7	g_6
g_2	g_2	g_4	g_0	g_6	g_1	g_7	g_3	g_5
g_3	g_3	g_5	g_6	g_0	g_7	g_1	g_2	g_4
g_4	g_4	g_2	g_1	g_7	g_0	g_6	g_5	g_3
g_5	g_5	g_3	g_7	g_1	g_6	g_0	g_4	g_2
g_6	g_6	g_7	g_3	g_2	g_5	g_4	g_0	g_1
g_7	g_7	g_6	g_5	g_4	g_3	g_2	g_1	g_0

has an inverse relative to the identity, and that the associativity property holds [2]. Furthermore, G is Abelian, and isomorphic to $Z_2 \times Z_2 \times Z_2$ (see [3]), and indeed, $G =< g_1 > \times < g_2 > \times < g_3 >$. The group generator relations are simple ones, essentially stating that the three generators are each of order 2 and that the group multiplication is commutative:

1. $g_1 \circ g_1 = g_2 \circ g_2 = g_3 \circ g_3 = g_0$
2. $g_1 \circ g_2 = g_2 \circ g_1$
3. $g_2 \circ g_3 = g_3 \circ g_2$
4. $g_1 \circ g_3 = g_3 \circ g_1$

Note that the only time when it is important to take note of the code length N is when using matrix representation for the operators. It is notable that this same 8×8 group applies to binary codes of all lengths. On the other hand, properties of actions of the group elements on sets of codes can depend on code structure, the parity of N, and on congruence of N modulo 4, as will be shown in the next section.

The next sections will look at group structure for more general mth-root-of-unity codes. A group generated by sidelobe-preserving operators for some m and N will be referred to as a SPG.

5 Equivalence Classes, Group Actions, and the Odd-Length Barker Codes

Consider again the binary case, and the group G defined in the previous section. Furthermore, define two codes $x, y \in (Q_2)_N$ to be equivalent if $y = g_k x$ for some $g_k \in G$. This induces a partition of $(Q_2)_N$ into equivalence classes of size 8 or less.

An interesting question for computational searches is whether it is possible to generate single representatives of each equivalence class by a deterministic algorithm. The answer is that it is possible; one such algorithm was provided in Coxson et al. [4].

As indicated earlier, the odd-length Barker codes provide examples of size-4 equivalence classes. This suggests a shared symmetry that results in degenerate orbits. The theory of group actions suggests that there exists a non-trivial identity (or non-trivial identities, as is actually the case) for the odd-length Barker codes. It is an instructive exercise to find them.

The following candidates can be ruled out quickly:

1. g_1: $g_1 x = -x$ has no fixed points in $(Q_2)_N$ for any $N > 0$.
2. g_3: $g_3 x = xA_N$ has no fixed points in $(Q_2)_N$ for any $N > 0$.
3. g_5: $g_5 x = -xA_N$ has no fixed points in $(Q_2)_N$ for any $N > 0$.

Two more can be ruled out almost as quickly:

1. g_2: $g_2 x = \overline{x}$ fixes symmetric codes x, none of which can achieve $\mathrm{PSL}_x = 1$ for $N > 2$.
2. g_3: $g_4 x = -\overline{x}$ fixes some $x \in (Q_2)_N$, but only when N is even.

That leaves g_6 and g_7 as the only possibilities for nontrivial identities.

Consider first g_7. Matrix representation helps rule out possibilities for solutions to

$$0 = g_7 x - x = -(\overline{xA_N} + x).$$

Indeed, based on simple considerations in the solution of sets of linear equations, it is possible to rule out any solutions when N is even or when $N \equiv 3 \bmod 4$. However, when $N \equiv 1 \bmod 4$, one arrives at the following linear equation (making use of the matrix representation available in the binary case):

$$0 = g_7 x - x = x \begin{pmatrix} -1 & 0 & 0 & \dots 0 \dots & 0 & 0 & 1 \\ 0 & -1 & 0 & \dots 0 \dots & 0 & -1 & 0 \\ 0 & 0 & -1 & \dots 0 \dots & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \dots \vdots \dots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots 0 \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \dots \vdots \dots & \vdots & \vdots & \vdots \\ 0 & 0 & 1 & \dots 0 \dots & -1 & 0 & 0 \\ 0 & -1 & 0 & \dots 0 \dots & 0 & -1 & 0 \\ -1 & 0 & 0 & \dots 0 \dots & 0 & 0 & 1 \end{pmatrix}. \tag{11}$$

Since the matrix on the right-hand side has a zero row, and is hence singular, there exists a solution in R^N. It remains to show that there exists a solution in $(Q_2)_N$. However, the simple form of the set of equations in this case leads in a straightforward way to a set of solutions of the form

$$x = \left[z \; y \; -\overline{zA_{(N-1)/2}} \right], \tag{12}$$

where z can be chosen arbitrarily from $(Q_2)_{(N-1)/2}$ and $y \in \{1, -1\}$.

By a similar process, it is possible to conclude that g_6 has a solution only when $N \equiv 3 \bmod 4$, and the solutions are of the form

$$x = \left[z \; y \; \overline{zA_{(N-1)/2}} \right], \tag{13}$$

where z can be chosen arbitrarily from $(Q_2)_{(N-1)/2}$ and $y \in \{1, -1\}$.

This shared structure of the odd-length Barker codes is well-known (see, for instance, [17]) and is often credited to Golay and referred to as (Golay) skew symmetry (see, e.g., [12]). It is interesting, nonetheless, to rediscover this property using the theory of group actions.

Note that if x has the skew symmetry property, then any code equivalent to it is also skew-symmetric. To see this, let x and y be two members of $(Q_2)_N$ for $N \equiv 3 \bmod 4$ and let $y = g_k x$ for some $g_k \in G$. Then $g_6 x = x$ implies

$$g_6(y) = (g_6 \circ g_k)x = (g_k \circ g_6)x = (g_k)x = y. \tag{14}$$

A similar argument can be made using g_7 for $N \equiv 1 \bmod 4$.

It is easy to check that the odd-length Barker codes are skew-symmetric. Representatives of every odd-length Barker are listed here (see [16]):

1. $N = 3$:
$$\begin{bmatrix} 1 & 1 & -1 \end{bmatrix}. \tag{15}$$
2. $N = 5$:
$$\begin{bmatrix} 1 & 1 & 1 & -1 & 1 \end{bmatrix}. \tag{16}$$
3. $N = 7$:
$$\begin{bmatrix} 1 & 1 & 1 & -1 & -1 & 1 & -1 \end{bmatrix}. \tag{17}$$
4. $N = 11$:
$$\begin{bmatrix} 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \end{bmatrix}. \tag{18}$$
5. $N = 13$:
$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \end{bmatrix}. \tag{19}$$

It needs to be mentioned that while the odd-length Barker codes are skew-symmetric and achieve the lowest possible PSL, this does not mean that skew-symmetry implies low sidelobe level. If an exhaustive search is done, and a count made of the number of equivalence classes of odd-length binary skew-symmetric codes, for lengths between 3 and 25, the result is the set of tallies given in the table below.

In Table 3, notice that the number of equivalence classes for high PSL values is nearly as high as those for low sidelobe level. The reason that only even values of PSL are listed is that odd-length skew-symmetric binary codes can have only odd PSL (a nice exercise for the reader). This means that for some lengths N, in particular those where the lowest PSL is even, a search over skew-symmetric codes will not be able to find the optimal codes. Nonetheless, such searches will find codes with near-optimal PSL for a considerable savings in computational cost.

Here we see that shared structure in a very special set of codes (those having the lowest achievable peak sidelobe level) can be uncovered by studying degeneracies in group actions for a group generated by sidelobe-preserving operations. A natural question to ask is whether this is a coincidence, and furthermore, if it is not a coincidence, why this connection should exist. These questions are not going to be answered in this chapter. The following sections will pursue the structure of operator groups for a more general set of codes.

Table 3 Number of skew-symmetric binary codes, $N = 3$–25

N	1	3	5	7	9	11	13	15	17	19	21	23
3	1	0	0	0	0	0	0	0	0	0	0	0
5	1	1	0	0	0	0	0	0	0	0	0	0
7	1	2	1	0	0	0	0	0	0	0	0	0
9	0	5	2	1	0	0	0	0	0	0	0	0
11	1	4	8	2	1	0	0	0	0	0	0	0
13	1	9	9	10	2	1	0	0	0	0	0	0
15	0	6	26	24	11	2	1	0	0	0	0	0
17	0	5	45	40	23	12	2	1	0	0	0	0
19	0	4	68	82	59	27	13	2	1	0	0	0
21	0	8	68	195	115	79	30	14	2	1	0	0
23	0	9	107	270	335	154	98	33	15	2	1	0
25	0	3	128	515	552	475	201	119	36	16	2	1

6 Sidelobe-Preserving Operator Group Structure for Quad-Phase Codes

Moving from the binary case to the quad-phase case, the elements of a code $x \in (Q_4)_N$ are chosen not from the set $\{-1,1\}$ but the set $\{-1,1,i,-i\}$, where $i = \sqrt{-1}$. The longest known quad-phase code with PSL $= 1$ (i.e., a generalized Barker sequence) is the length-15 code [13]

$$x = \left[\,1\ 1\ 1\ i\ i\ 1\ {-i}\ {-i}\ i\ {-1}\ {-i}\ i\ 1\ {-1}\ 1\,\right]. \tag{20}$$

Interestingly, this code satisfies $x = -\overline{xA_{15}}$, where A_{15} is the 15×15 diagonal matrix that effects an alternating-sign transformation on the elements of x; that is, it has diagonal elements $-1,1,-1,\ldots,(-1)^{15}$. Hence, this code obeys the same symmetry as the binary Barker codes for lengths $N \equiv 1 \bmod 4$.

As will be shown, this means dealing with added complications in the sidelobe-preserving group. One of the complications is that instead of a single group, there are now four, depending on the congruence of code length N modulo 4. Furthermore, the groups have size 64 and are no longer Abelian. Finally, it will no longer be possible to represent transformations in terms of matrix operations.

Before examining this case, it is useful to look at the sidelobe-preserving operations in a more general setting, the general unimodular case where code elements can lie anywhere on the unit circle. For consistency with the notation used previously, let Q_∞ represent the unit circle and let $(Q_\infty)_N$ represent the set of N-length codes whose elements are drawn from the unit circle. Golomb and Win [8] provide a list of the sidelobe-preserving transformations for this quite general case. Let $x \in (Q_\infty)_N$. Then the following operations each preserve the magnitudes of the AAC sequence and hence the peak sidelobe level (using simpler notation than previously, to facilitate the discussions to come):

1. C: elementwise complex conjugation, x^c
2. R: reversal, $\overline{x}$
3. M_μ: multiplication by $\mu \in Q_\infty$ to give μx
4. P_ρ: progressive multiplication (or phase ramp) using $\rho \in Q_\infty$

What is meant by progressive multiplication is that element x_i is multiplied by ρ^i for $i = 1, \ldots, N$. Note that complex conjugation operation cannot be represented using matrix multiplication.

The transformations R and M_μ preserve the autocorrelation sequence, while the operations C and P_ρ preserve the magnitudes of the sidelobes (and hence the peak sidelobe level) but do not preserve the autocorrelation sequence in general.

Moving to the quad-phase case, let x be an arbitrary member of $(Q_4)_N$ for $N > 0$, and consider the following specialization of the generalized list of sidelobe-preserving operations given above:

1. C: elementwise complex conjugation
2. R: reversal, $\overline{x}$
3. M_i: multiplication by $\mu = i$
4. P_i: progressive multiplication by $\rho = i$

No loss of generality results from the particular choice of values for μ and ρ since in each case, the choice of i specifies a generator for the order-4 cyclic group containing every other possibility.

The four operators generate a group of order 64. To see this, first fix $N > 0$. Then $< R, P_i >$ (the group generated by R and P_i) is a dihedral group of order 8. Also, M_i generates a cyclic group of order 4, $< M_i >$. It follows that $< M_i, R, P_i >$ has a normal subgroup, $< M_i >$, modulo in its dihedral-8 subgroup $< R, P_i >$. Hence

$$| < M_i, R, P_i > | = (4)(8) = 32. \qquad (21)$$

Now consider the group $< M_i, R, P_i, C >$. Every element may be written $R^a P_i^b C^d M_i^e$ where $a, d \in \{0, 1\}$ and $b, c \in \{0, 1, 2, 3\}$. So

$$| < M_i, R, P_i, C > | \le (2)(2)(4)(4) = 64. \qquad (22)$$

Since C has order 2 and does not belong to $< M_i, R, P_i >$,

$$| < M_i, R, P_i, C > | \ge (2)(32) = 64. \qquad (23)$$

Therefore $G =< M_i, R, P_i, C >$ has size 64.

Let g_0 be the group identity. Then with some effort, the list of generator relations is found to be

1. $C^2 = R^2 = g_0$
2. $M_i^4 = P_i^4 = g_0$
3. $RC = CR$
4. $P_i M_i = M_i P_i$

5. $M_iR = RM_i$
6. $CM_i = M_i^{-1}C = -M_iC$
7. $CP_i = P_i^{-1}C$
8. $RP_i = M_i^{N+1}P_i^{-1}R$

Note that the last of these relation, depends on N or, more to the point, the value of N modulo 4. Hence, there are four apparently different sets of relations, yielding four possibly different groups.

To simplify the following discussions, let G_i refer to the group for $N \equiv i \bmod 4$, for $i = 0, \ldots, 3$. When the value of N is not specified, and the discussion applies to all four cases, the notation G will be used.

There exist 267 distinct groups of order 64 (see, e.g., [3]). A first hint at group structure for the four quad-phase groups results from counting the orders of group elements. In the case of G_3, the count of group elements of order 2 is 35. Fortunately, there is a single group of the 267 groups of order 64 having 35 elements of order 2, and that is the Cartesian product of two dihedral-8 groups. Hence G_3 is isomorphic to $D_8 \times D_8$. The count of order-2 elements for G_1 is also 35, suggesting that G_1 and G_3 are isomorphic.

Identification of the group structure for the two remaining cases, G_0 and G_2, is left unresolved for now.

1. 27 elements of order 2
2. 20 elements of order 4
3. 16 elements of order 8

This narrows the possible order-64 group structures to three in these two cases (see [3]).

Element order counts can sometimes be unreliable. Fortunately, it is possible to do better than order tallies. Martin Isaacs, of the Department of Mathematics at University of Wisconsin Madison, has suggested the following approach involving semidirect products and automorphisms on subgroups [10].

Let $A =< M_i, P_i >$. Since M_i and P_i have order 4 and commute, A is Abelian and isomorphic to $Z_4 \times Z_4$, where Z_4 is the integers modulo 4 with respect to addition. Next, let $U =< C, R >$. Since C and R commute and have order 2, U is noncyclic of order 4, and isomorphic to $Z_2 \times Z_2$.

Note that the intersection of U and A contains only the identity. Then $G = AU$, that is, G is the semidirect product of A with U acting on it (in other words, U normalizes A), by the following observations:

1. $CM_iC^{-1} = M_i^C = M_i^{-1}$ and $P_i^C = P_i^{-1}$ imply that C normalizes A.
2. $RM_iR^{-1} = M_i^R = M_i$ and $P_i^R = P_i^{-1}M_i^k$ where $k = N+1$ imply that R normalizes A.

Determination of the structure of G now depends on knowing what automorphisms of A are induced by conjugation by C and R.

Automorphisms of A can be represented as 2×2 matrices over Z_4. Invertibility of a matrix over Z_4 will mean the determinant is ±1 modulo 4.

Conjugation of P_i and M_i by C gives

1. $P_i^C = CP_iC^{-1} = P_i^{-1}$
2. $M_i^C = CM_iC^{-1} = M_i^{-1}$

These two relationships will be encapsulated in the matrix $-I_2$, the negative of the 2×2 identity matrix.

Similarly, conjugation of P_i and M_i by R gives $P_i^R = RP_i^{-1}R^{-1} = M_i^kP_i^{-1}$ and $M_i^C = CM_iC^{-1} = M_i$, where $k = N+1$. Conjugation of P_i twice by R gives

$$\begin{aligned} R(M_i^kP_i^{-1})R^{-1} &= (RM_i^kR^{-1})(RP_i^{-1}R^{-1} \\ &= M_i^kR(RP_i)^{-1} \\ &= M_i^kR(M_i^kP_i^{-1}R)^{-1} \\ &= M_i^kP_iM_i^{-1} \\ &= P_i. \end{aligned} \tag{24}$$

A 2×2 matrix to represent this is then

$$\begin{pmatrix} 1 & 0 \\ k & -1 \end{pmatrix}, \tag{25}$$

the square of which, modulo 4, is the identity.

The subgroup U is essentially the multiplicative group generated by the two matrices. The easiest case is for $k = N+1 \equiv 0 \bmod 4$, that is, G_3. An equivalent set of generators, then, after setting $k = 0$, is

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{26}$$

and

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{27}$$

It follows that:

1. Conjugation by C leaves M alone but inverts P.
2. Conjugation by R inverts M and leaves P alone.

Together, these imply that G_3 is isomorphic to $D_8 \times D_8$, the same conclusion arrived at from the group element order tally.

Next, if R and C are conjugated by the same invertible matrix, this simply changes the "basis" for A, leaving the group unchanged. Consider using

$$\begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}, \tag{28}$$

whose inverse modulo 4 is

$$\begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}. \tag{29}$$

Then the matrix for C is unchanged by the conjugation, but the matrix for R becomes

$$\begin{pmatrix} 1 & 0 \\ k-2 & -1 \end{pmatrix}. \tag{30}$$

It follows that the four groups fall into two pairs of isomorphic groups, with G_3 and G_1 isomorphic and G_0 and G_2 isomorphic. Furthermore, G_1 and G_3 are isomorphic to $D_8 \times D_8$, the Cartesian product of the dihedral-8 group with itself. The automorphism argument above means $G_3 =< RC, M_i > \times < R, P_i >$.

To achieve a similar identification of G_1 detailing the generators of the two dihedral-8 groups in the Cartesian product, note that the only generator relation that differs for G_3 and G_1 is the final one. Starting with the form of this last relation that holds for G_1, which is $RP_i = M_i^2 P_i^{-1} R$, observe that it may be rewritten

$$R(M_i^{-1}P_i) = (M_i^{-1}P_i)^{-1}R. \tag{31}$$

Defining a new operator, $\tilde{P}_i = M_i^{-1}P_i$, it is straightforward to check that $\tilde{P}_i$ can replace P_i wherever it appears in the list of generators relations, without affecting the validity of any of the relations. All that has changed is that the "phase ramp" starts at $-i$ rather than i; the element-to-element phase increment remains $\pi/2$. It follows that $G_1 =< RC, M_i > \times < R, M_i^{-1}P_i >$.

Consider again the generalized Barker sequence of length 15:

$$x = \begin{bmatrix} 1 & 1 & 1 & i i & 1 & -i & -i i & -1 & -i i & 1 & -1 & 1 \end{bmatrix}. \tag{32}$$

As noted earlier, this code satisfies $x = -\overline{xA_{15}}$, meaning that the composition of operators $(M_i^2) \circ R \circ (P_i^2)$ maps x to itself. Then $(M_i^2) \circ R \circ (P_i^2)$ is a group element of G_3, since the order-4 cyclic group generated by M_i is a subgroup of the dihedral group $< RC, M_i >$ and the order-4 cyclic group generated by P_i is a subgroup of the dihedral group $< R, P_i >$ (and hence $R \circ P_i^2$ is an element of $< R, P_i >$). So, as in the binary Barker case, x is a quad-phase of optimally low peak sidelobe level for which a nonidentity element of the associated SPG fixes x, causing its equivalence class to degenerate. This is due to the fact that the isometry subgroup of x contains an element other than the group identity and therefore has size 2 or greater; then, by Lagrange's orbit-stabilizer theorem [15], the equivalence class of x degenerates to size $32 = 64/2$ or smaller [5,9]. By applying combinations of operators to this code, it is easy to establish that the equivalence class must be at least size 32; hence it is exactly size 32. This example provides further anecdotal support for a link between low-peak-sidelobe codes and degeneracies in SPG group actions.

7 Generalizing from Quad-Phase to *m*th Roots of Unity

Turning from the quad-phase codes $x \in (Q_2)_N$ to the more general *m*th roots codes $x \in (Q_m)_N$ for $m \geq 3$, it will be seen that the approach used in the quad-phase case generalizes well. First, the set of sidelobe preservers becomes:

1. C: elementwise complex conjugation
2. R: reversal, $\overline{x}$
3. M_μ: multiplication by $\mu = \mathrm{e}^{i2\pi/m}$
4. P_μ: progressive multiplication by $\mu = \mathrm{e}^{i2\pi/m}$

No loss of generality results from the particular choice of values for μ. This is because with value $\mathrm{e}^{i2\pi/m}$, μ is a generator for a cyclic group of order m containing the other *m*th roots of unity. Similarly, P_μ is the generator for an order-m cyclic group of "phase ramps" (or progressive multiplication transformations), and hence contains all possible choices for this operator. These cycle groups are subgroups of the SPG or SPGs.

Two of the SPG group generators have order 2 and the other two have order m. The argument for quad-phase group order can be generalized in a natural way to give $(2)(2)(m)(m) = 4m^2$ for group order.

The set of generator relations is:

1. $C^2 = R^2 = g_0$
2. $M_\mu^m = P_\mu^m = g_0$
3. $RC = CR$
4. $P_\mu M_\mu = M_\mu P_\mu$
5. $M_\mu R = RM_\mu$
6. $CM_\mu = M_\mu^{-1}C$
7. $CP_\mu = P_\mu^{-1}C$
8. $RP_\mu = M_\mu^{N+1}P_\mu^{-1}R$

Here, as before, g_0 represents the group identity. The final relation has a different form for each of m powers of μ, implying that there are as many as m groups of order $4m^2$. Let G_i represent the SPG for $N \equiv i \bmod m$, $i = 0, 1, \ldots, m-1$.

Similar arguments as for the quad-phase case ($m = 4$) work here to conclude that $G_{m-1} =< RC, M_\mu > \times < R, P_\mu >$ (i.e., when $N+1 \equiv 0 \bmod m$). Then, turning to the case $N+1 \equiv 2 \bmod m$, it is possible to conclude that by attaching an M_μ^{-1} term to P_μ (as was done in the quad-phase case), leads to $G_1 =< RC, M_\mu > \times < R, M_\mu^{-1}P_\mu >$. This process of incrementing i by 2 and attaching an additional M_μ^{-1} can be repeated as many times as needed, allowing

$$G_{2k-1} =< RC, M_\mu > \times < R, (M_\mu^{-1})^k P_\mu >$$

for any $m-1 \geq k \geq 0$.

Now notice that whenever m is odd, every one of the m SPGs has the structure $< RC, M_\mu > \times < R, (M_\mu^{-1})^k P_\mu >$. This is because when m is odd, every one of the m SPGs is encountered in no more than m jumps, by repeatedly incrementing j by 2, starting with $j = 0$, in $N + 1 \equiv j \bmod m$. Therefore, when m is odd, every SPG is isomorphic to $D_{2m} \times D_{2m}$.

When m is even, it happens that the groups fall into two classes, those for N odd and those for N even. When N is odd,

$$G_{2k-1} =< RC, M_\mu > \times < R, (M_\mu^{-1})^k P_\mu >$$

for any $k \geq 0$, by the same argument used for m odd. Hence, G is isomorphic to $D_{2m} \times D_{2m}$ when m is even and N is odd. The group structure when m is even and N is even is left for others to resolve.

8 Conclusions

This chapter considers the structure of groups of peak-sidelobe-preserving operators for the AAC of mth root codes. These groups are shown to be helpful for efficient enumeration of codes for a given m, by peak sidelobe level. In the binary case, it is shown that the group is an Abelian group of order 8. Furthermore, it is shown that shared symmetry in the binary Barker codes can be discovered in a natural way from considering degeneracies the group actions. The group structure for $m = 4$ (the quad-phase case) is shown to have increased complexity; in fact, instead of a single group, there are four groups (two pairs of isomorphic groups). Group structure is identified for the cases of odd N. Moving to general mth roots codes, it is shown that results found for the quad-phase case generalize quite well. It is shown that there are $4m^2$ groups. All m groups are identified for any odd m. When m is even, the structure for any odd N is identified. The group structure for m even and N even is left unresolved.

Acknowledgments The author would like to acknowledge the help of I. Martin Isaacs of the University of Wisconsin at Madison, in outlining an approach for discovering the sidelobe-preserving operator group structure for quad-phase codes. In addition, Chris Monsour of Travelers Insurance, for the help with in establishing the quad-phase group order. Finally, this chapter is in memory of a friend and advisor, Larry Welch (1956–2003).

References

1. Barker, R.H.: Group synchronization of binary digital systems. In: Jackson, W. (ed.) Communications Theory, pp. 273–287. Academic, London (1953)
2. Carter, N.: Visual Group Theory. MAA Press, Washington DC (2009)

3. Conway, J.H., Curtis, R.T., Norton, S.P., Parker, R.A., Wilson, R.A.: Atlas of Finite Groups. Clarendon Press, Oxford (1985)
4. Coxson, G.E., Cohen, M.N., Hirschel, A.: New results on minimum-PSL binary codes. In: Proceedings of the 2001 IEEE National Radar Conference, pp. 153–156. Atlanta, GA (2001)
5. Dummit, D.S., Foote, R.M.: Abstract Algebra, 3rd edn. Wiley, New York (2004)
6. Friese, M., Zottman, H.: Polyphase Barker sequences up to length 31. Elect. Lett **30**(23), 1930–1931 (1994)
7. Golomb, S., Scholtz, R.: Generalized Barker sequences (transformations with correlation function unaltered, changing generalized Barker sequences. IEEE Trans. Inf. Theor. **11**, 533–537 (1965)
8. Golomb, S., Win, M.Z.: Recent results on polyphase sequences. IEEE Trans. Inf. Theor. **44**, 817–824 (1999)
9. Herstein, I.N.: Topics in Algebra, 2nd edn. Wiley, New York (1975)
10. Isaacs, I.M.: Email communication, 21 June 2006 (2006)
11. Levanon, N., Mozeson, E.: Radar Signals. Wiley, New York (2005)
12. Militzer, B., Zamparelli, M., Beule, D.: Evolutionary search for low autocorrelated binary sequences. IEEE Trans. Evol. Comput. **2**(1), 34–39 (1998)
13. Nunn, C., Coxson, G.E.: Polyphase pulse compression codes with optimal peak and integrated sidelobes. IEEE Trans. Aerosp. Electron. Syst. **45**(2), 41–47 (2009)
14. Pless, V.S., Huffman, V.S., W.C. and Brualdi, R.A., (eds.): Handbook of Coding Theory. Elsevier Publishing, Amsterdam (1998)
15. Roth, R.R.: A history of Lagrange's theorem on groups. Math. Mag. **74**(2), 99–108 (2001)
16. Skolnik, M.: Radar Handbook, 2nd edn . McGraw-Hill, New York (1990)
17. Turyn, R.J., Storer, J.: On binary sequences. Proc. Am. Math. Soc. **12**, 394–399 (1961)