The Structure of Sidelobe-Preserving Operator Groups

GREGORY E. COXSON, Senior Member, IEEE
Olney, MD, USA

DENNIS SPELLMAN
Temple University
Philadelphia, PA, USA

This paper considers the structure of groups of operators preserving the aperiodic autocorrelation peak sidelobe level of the *m*th root of unity codes. These groups are shown to be helpful for efficient enumeration of codes by peak sidelobe level for a given *m* and given codeword length *N*. Another possible use is in narrowing the search space for the *m*th root of unity codes of a given length. 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 odd-length binary Barker codes can be discovered in a natural way by considering degeneracies of group actions. The group structure for $m > 2$ is shown to have higher complexity. Instead of a single group, there are *m* order-$4m^2$ groups, and they are no longer Abelian. The structure of these groups is identified for any $m > 2$ and any positive length *N*.

Manuscript received February 5, 2014; revised July 21, 2014; released for publication December 6, 2014.

DOI. No. 10.1109/TAES.2015.140100.

Refereeing of this contribution was handled by F. Gini.

Authors' addresses: G. E. Coxson, 17412 Cherokee Lane, Olney, MD 20832, USA, E-mail: (gcoxson@ieee.org); D. Spellman, 5147 Whitaker Lane, Philadelphia, PA 19124, USA.

I. 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, 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 entries that are mth roots of unity for some m. Polyphase codes with $m = 2$ are called binary codes; all elements are ± 1.

Binary and polyphase codes that achieve low aperiodic autocorrelation 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 [1]. 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 reliable approach is exhaustive search. Taking the search space as all mth root-of-unity 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. The search may be expedited if a method can be found that involves searching single representatives from each equivalence class. Furthermore, listing the best representatives (for some measure of sidelobe level of interest) is more efficient than listing the full set of the best codes from the search space.

Because search techniques quickly grow computationally costly, even prohibitively 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. This is possibly another opening for the use of sidelobe-preserving operator groups. For the most notable example of low-sidelobe codes, the binary Barker codes, those of odd length share a skew-symmetry 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.

The paper is organized as follows. After an introduction (section I) and notation and terminology (section II), section III discusses the motivation for examining sidelobe-preserving operator groups. Section IV will look at the group structure for the binary case. Section V will show that consideration of degeneracies in group actions for odd-length binary Barkers leads in a natural way to the uncovering of their skew-symmetry property. Section VI will exhibit the group operations for the general unimodular case, where code elements can be

drawn freely from the unit circle. Section VII will examine the mth-root-of-unity codes for $m \geq 2$, and group structure will be identified for any $m \geq 2$ and $N > 0$. Section VIII will return to the issue of exploiting the group structure in searches for low-sidelobe codes.

II. 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 element of which 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 aperiodic autocorrelation (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:

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

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

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

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,

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

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

The peak sidelobe level (PSL) 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 [2]. When $m > 2$, codes $x \in (Q_m)_N$ that achieve $\mathrm{PSL}_x = 1$ are called generalized Barker sequences [3] or polyphase Barker sequences [4].

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 hgh^{-1} (this is not to be confused with complex conjugation). The notation $[g, h]$ will mean the commutator of the two elements, or $[g, h] = g^{-1}h^{-1}gh$. Given two groups G and H, the notation $G \times H$ will mean the Cartesian product of G with H, and GH will represent a semidirect product of G and H (see, e.g., [5]).

III. 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 [1, 6, 7]). For a given length, it is useful to know the lowest achievable PSL, and some or all the codes that 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 operators for general polyphase codes. They are:

1) reversal $\bar{x}$,
2) complex conjugation x^c,
3) constant multiple transformation (CMT): Given any unit-modulus complex number α, form the product αx, and
4) progressive multiplication transformation (PMT): Given any unit-modulus complex number ρ, multiply the ith element x_i by ρ^i for i = 1, . . . , 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 $\bar{x}$,
2) negation $-x$, and
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,

$$x = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \end{bmatrix}. \tag{8}$$

Behind the efficiency of this use of representatives, there is 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 the code has a special structure, and the structure is related to "actions" of the three transformations under composition.

Skolnik [1] 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 I lists these results, along with similar figures for $N = 2$.

Interestingly, the values tabulated in [1] 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 I. 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 appears that degeneracies in the "actions" of the 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.

TABLE I
Count of Equivalence Classes

N	Best PSL	Number of Representatives for Negative & Reversal	Number of Representatives for Negation, Reversal, & 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	1021	515
24	3	1716	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

IV. 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) $g_3 = xA_N$,

TABLE II
Binary Operator Group

$\circ$	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

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

$$J_N = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}, \tag{9}$$

and A_N is the matrix

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

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 the composition of operations. The 8×8 multiplication table is shown in Table II (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 has an inverse relative to the identity, and that the associativity property holds [9]. Furthermore, G is Abelian and isomorphic to $Z_2 \times Z_2 \times Z_2$ (see [10]), 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) $g_2 \circ g_3 = g_3 \circ g_2$, and
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 m-root-of-unity codes. A group generated by sidelobe-preserving operators for some m and N will be referred to as a sidelobe-preserving operator group (or SPG).

V. 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 $y = g_{kx}$ 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 for the case of binary $\pm$ codes is that it is possible; one such algorithm was provided in Coxson et al. [11].

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 nontrivial identity (or nontrivial 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 $N > 0$; and
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: $g_2 x = \bar{x}$ fixes symmetric codes x, none of which can achieve $\mathrm{PSL}_x = 1$ for $N > 2$; and
2) g_3: $g_4 x = -\bar{x}$ 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 $0 = g_7x - x = -(\overline{xA_N} + x)$.

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):

$$0 = g_7x - x = x \begin{pmatrix} -1 & 0 & \dots & 0 & \dots & 0 & 1 \\ 0 & -1 & \dots & 0 & \dots & -1 & 0 \\ \vdots & \vdots & \dots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \dots & \vdots & \dots & \vdots & \vdots \\ 0 & -1 & \dots & 0 & \dots & -1 & 0 \\ 1 & 0 & \dots & 0 & \dots & 0 & -1 \end{pmatrix}. \tag{11}$$

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

$$x = \begin{bmatrix} z & y & -\overline{zA_{(N-1)/2}} \end{bmatrix}, \tag{12}$$

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:

$$x = \begin{bmatrix} z & y & \overline{zA_{(N-1)/2}} \end{bmatrix}, \tag{13}$$

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, [12]) and is often credited to Golay, and referred to as (Golay) skew-symmetry (see, e.g., [13]). 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 $y = g_{kx}$ for some $g_k \in \mathrm{G}$. Then $g_{6x} = x$ 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 [2]):

1) $N = 3: \begin{bmatrix} 1 & 1 & -1 \end{bmatrix}$. (15)

2) $N = 5: \begin{bmatrix} 1 & 1 & 1 & -1 & 1 \end{bmatrix}$. (16)

3) $N = 7: \begin{bmatrix} 1 & 1 & 1 & -1 & -1 & 1 & -1 \end{bmatrix}$. (17)

4) $N = 11: \begin{bmatrix} 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \end{bmatrix}$. (18)

5) $N = 13: \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \end{bmatrix}$. (19)

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. Consider applying an exhaustive search and keeping a count of the number of equivalence classes for skew-symmetric codes having different PSL values for different lengths. Table III shows the results for lengths between 3 and 15.

TABLE III
Number of Skew-Symmetric Binary Codes, $N = 3$ to 15

(N\PSL)	1	3	5	7	9	11	13	15
3	1	0	0	0	0	0	0	0
5	1	1	0	0	0	0	0	0
7	1	2	1	0	0	0	0	0
9	0	5	2	1	0	0	0	0
11	1	4	8	2	1	0	0	0
13	1	9	9	10	2	1	0	0
15	0	6	26	24	11	2	1	0

Column 1 in Table III corresponds to the Barker codes, showing that there are odd-length Barker codes for $N = 3$, 5, 7, 11, 13 but not for $N = 9$ or $N = 15$. Odd-length skew-symmetric binary codes can have only odd PSL (a nice exercise for the reader), so only columns for odd PSL are provided in Table III. One consequence of this property is 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. Examples are $N = 9$ and $N = 15$; in each case, the optimal PSL is 2, as indicated in Table I, so a search over skew-symmetric codes of length 9 or 15 will fail to turn up any optimal-PSL codes. Nonetheless, such searches will find codes with near-optimal PSL for a considerable savings in computational cost.

Table III also shows that relatively high values of PSL are represented along with low values. For instance, for $N = 13$, there are ten equivalence classes for PSL = 7, two equivalence classes for PSL = 9, and one equivalence class for PSL = 11.

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 paper. The following sections will pursue the structure of operator groups for a more general set of codes.

VI. OPERATORS FOR GENERAL UNIMODULAR CODES

It is useful to look at the sidelobe-preserving operations in the general unimodular case, where code elements may 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 for which 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 aperiodic autocorrelation 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 $\bar{x}$;
3) M_μ: multiplication by $\mu \in Q_\infty$ to give μx; and
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 $i = 1, \ldots, N$.

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.

VII. GROUP STRUCTURE FOR mth-ROOT-OF-UNITY CODES

Having considered the quite general framework of the previous section, we will now step back to the special case of mth-root-of-unity codes. Code length will be represented by integer $N > 0$. The elements of a code will now be drawn for the set of mth roots of unity for some integer $m \geq 2\{e^{2\pi i/m}, e^{4\pi i/m}, \ldots, 1\}$, where $i = \sqrt{-1}$. When $m = 2$, we have the binary $\pm$ 1 case already discussed.

The codes x are drawn from the set $(Q_m)_N$. For example, when $m = 4$, a code $x \in (Q_4)_N$ having N elements is chosen from the four-element set $\{i,-1,-i,1\}$. The case of $m = 4$ is given special attention in [14].

Not surprisingly, added complexities arise in the group structure in moving from a choice of 2 real values for each element (the binary $\pm$ 1 codes) to a choice between m mostly complex values. One of the new complications is that instead of a single group, there are now m possible groups, where the structure of the group for a given code length N depends on the congruence of N modulo m. Furthermore, the groups will be non-Abelian in general. The group order will depend on m, as $4m^2$ (see Theorem 7.3). Finally, it will no longer be possible to represent transformations in terms of matrix operations because now elementwise complex conjugation must be added as a sidelobe-preserving transformation; there is no matrix representation for the conjugation operation.

Specializing the set of operators in the previous section to the mth-root-of-unity codes yields the following list of four:

1) C: elementwise complex conjugation;
2) R: reversal $\bar{x}$;
3) M_μ: multiplication by $\mu = e^{2\pi i/m}$; and
4) P_ρ: progressive multiplication by $\rho = e^{2\pi i/m}$.

No loss of generality results from the particular choice of values for μ and ρ, since $<M_\mu>$ and $<P_\rho>$ are cyclic subgroups of size m; the other mth roots of unity are formed as powers of the generators M_μ and P_ρ. To simplify the following discussion, μ will be used for both, that is, P_ρ will be written P_μ.

Before continuing, we review some elementary group theory useful for deriving our ultimate results. We shall write groups multiplicatively. In particular, 1 shall be the group identity element, and the meaning of the symbol 1 should be clear from context. If K and H are subgroups in a group G, then the complex KH is defined to be the set of all products kh as k and h vary over K and H, respectively. Note that $1 = 1 \cdot 1$ lies in KH. However, in general, KH is not a subgroup of G. Let us say that K and H commute elementwise provided that $hk = kh$ for all $k \in K$ and $h \in H$. Elementwise commutation is a sufficient but in general unnecessary condition for the setwise commutation $KH = HK$. Nevertheless, we claim that the condition $KH = HK$ is necessary and sufficient for KH to be a subgroup of G. For necessity, suppose KH is a subgroup in G. Observe that k^{-1} and h^{-1} vary over K and H as k and h do. Moreover, $(kh)^{-1}$ varies over KH as does kh when k and h vary over K and H, respectively. Then from $(kh)^{-1} = h^{-1}k^{-1}$, we deduce $KH = HK$. For sufficiency, suppose $KH = HK$. Observe that the above argument shows that KH not only contains 1 but also is closed under taking inverses. It remains to show that KH is closed under taking products. Toward that end, we compute the product $k_1h_1 \cdot k_2h_2$, where k_1 and k_2 lie in K and h_1 and h_2 lie in H: $k_1h_1 \cdot k_2h_2 = k_1(h_1k_2)h_2$. Since h_1k_2 lies in $HK = KH$, there are

k_3 in K and h_3 in H, such that $h_1k_2 = k_3h_3$. Then

$$\begin{aligned} k_1h_1 \cdot k_2h_2 &= k_1(k_3h_3)h_2 \\ &= k_1k_3 \cdot h_3h_2, \end{aligned}$$

which lies again in KH. Thus, KH is closed under taking products and is indeed a subgroup.

We next claim that a sufficient condition for the setwise commutation $KH = HK$ is that at least one of K or H be normal in G. Indeed, suppose K is normal in G. Then from the identities $kh = h \cdot h^{-1}kh$ and $hk = hkh^{-1}h$, we deduce $KH = HK$ as, for fixed h in H, $h^{-1}kh$ and hkh^{-1} each vary over K as k does, since K is normal in G. Henceforth, we assume K normal in G so that the complex KH is a subgroup in G. If the complex exhausts G, then we say that KH is a factorization of G. Suppose that is the case, so $G = KH$ with K normal in G. In that event, every element g in G can be written in at least one way as a product kh with $k \in K$ and $h \in H$. In general, such a product representation of an element need not be unique. We claim that in the above context, a necessary and sufficient condition for the uniqueness of the product representation is that the intersection $K \cap H$ be the trivial subgroup $\{1\}$. Suppose $g \neq 1$ belongs to $K \cap H$. Then g has the two different representations $g \cdot 1$ and $1 \cdot g$ of the form kh. Then $K \cap H = \{1\}$ is a necessary condition for the uniqueness of the product representation of elements. For sufficiency assume $K \cap H = \{1\}$. Suppose $k_1h_1 = k_2h_2$, where k_1 and k_2 lie in K and h_1 and h_2 lie in H. then

$$k_2^{-1}(k_1h_1)h_1^{-1} = k_2^{-1}(k_2h_2)h_1^{-1}$$

and $k_2^{-1}k_1 = h_2h_1^{-1}$. Let g be the common value of $k_2^{-1}k_1$ and $h_2h_1^{-1}$ in G. Then, $g = k_2^{-1}k_1$ lies in K, and $g = h_2h_1^{-1}$ lies in H. So g lies in $K \cap H = \{1\}$ and $g = 1$. From $k_2^{-1}k_1 = 1$, we infer $k_1 = k_2$. From $h_2h_1^{-1} = 1$, we infer $h_2 = h_1$. Therefore the representation is unique and sufficiency is established.

DEFINITION 7.1 Let G be a group and K and H subgroups of G. If K is normal in G, $G = KH$, and $K \cap H = \{1\}$, then G is the internal semidirect product of K by H.

Note that if G is the internal semidirect product of K by H, then $|G| = |K| \cdot |H|$, since every element g in G is uniquely representable as a product kh with $k \in K$ and $h \in H$. In the event that the semidirect product G of K by H satisfies the stronger condition that K and H commute elementwise, then both K and H will be normal in G, and G will be the internal direct product of K and H.

Just as one can construct the external direct product of two groups K and H by defining a multiplication on the set $K \times H$ of ordered pairs (k, h) with $k \in K$ and $h \in H$ via

$$(k_1, h_1) \cdot (k_2, h_2) = (k_1k_2, h_1h_2),$$

one can define an external semidirect product of K by H under certain additional information. To motivate the construction, we begin with a given internal semidirect product $G = KH$ of K by H. Since K is normal in G, for each fixed h in H, the function $\alpha(h)$: $K \to K$, defined by

$$\alpha(h)(k) = hkh^{-1}$$

for all $k \in K$, is an automorphism of K. Moreover, the function

$$\alpha : H \to \mathrm{Aut}(K)$$

from H into the automorphism group $\mathrm{Aut}(K)$ is a group homomorphism. To see that, observe, for all $k \in K$ and all h_1, h_2 in H,

$$\begin{aligned} \alpha(h_1h_2)(k) &= (h_1h_2)k(h_1h_2)^{-1} \\ &= h_1h_2kh_2^{-1}h_1^{-1} \\ &= h_1(h_2kh_2^{-1})h_1^{-1} \\ &= \alpha(h_1)(\alpha(h_2)(k)) \\ &= (\alpha(h_1) \cdot \alpha(h_2))(k). \end{aligned}$$

Let us compute the product of two elements $k_1h_1 \cdot k_2h_2$, where k_1 and k_2 lie in K and h_1 and h_2 lie in H:

$$\begin{aligned} k_1h_1 \cdot k_2h_2 &= k_1h_1k_2(h_1^{-1}h_1)h_2 \\ &= (k_1 \cdot h_1k_2h_1^{-1}) \cdot (h_1h_2) \\ &= (k_1\alpha(h_1)(k_2)) \cdot (h_1h_2). \end{aligned}$$

Note that $k_1\alpha(h_1)(k_2)$ lies in K, and h_1h_2 lies in H.

DEFINITION 7.2 Given groups K and H and a group homomorphism α from H into the automorphism group $\mathrm{Aut}(K)$ of K, the group $K \rtimes_\alpha H$ consisting of the ordered pairs (k, h) with $k \in K$ and $h \in H$ and having multiplication defined by

$$(k_1, h_1) \cdot (k_2, h_2) = (k_1\alpha(h_1)(k_2), h_1, h_2)$$

is the external semidirect product of K by H modulo α.

Just as one can prove that the internal direct product of K and H is isomorphic to the external direct product of K and H, one can prove that the internal semidirect product of K by H is isomorphic to the external semidirect product $K \rtimes_\alpha H$ when α is given by $\alpha(h)(k) = hkh^{-1}$. This concludes our review of elementary group theory.

Fix an integer $N > 0$ representing code length and an integer $m \geq 2$ specifying the possible values for code elements. Then, a complete list of generator relations for the group $<C, R, M_\mu, P_\mu>$ is found to be

1) $C^2 = R^2 = 1$.
2) $M_\mu^m = P_\mu^m = 1$.
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) $RP_\mu = M_\mu^{N+1}P_\mu^{-1}R$.

Note that the last of these relations depends on N, and in particular, the value of N modulo m. Hence, there are m different sets of relations, yielding m possibly different groups.

Let us now fix m and N. Further, to simplify notation, we suppress the expression depending on $\mu = e^{2\pi i/m}$ and write M and P for M_μ and P_μ, respectively. Let us formally define Γ to be the group generated by the symbols C, R, M, and P subject to the defining relations (1) through (8), noting that relations (1) and (2) actually represent two relations each. Note that the defining relations (5) through (8) allow us to move any element of the subgroup $<C, R>$ to the right of any element of the subgroup $<M, P>$. Furthermore, the relations (3) and (4) guarantee that each of the subgroups $<C, R>$ and $<M, P>$ is Abelian. It follows that every element of Γ may be written in at least one way as $M^{e(M)}P^{e(P)}C^{e(C)}R^{e(R)}$. Moreover, it follows from (2) that M and P have order dividing m, and it follows from (1) that C and R have order dividing 2. Thus, we may take

$$0 \leq e(M), e(P) < m$$

and

$$0 \leq e(C), e(R) < 2.$$

It follows that Γ has at most $4m^2$ elements. Our main result will be that Γ has a semidirect product decomposition. More precisely, we shall show that $<M, P>$ is isomorphic to the direct product of two groups, each cyclic of order m, $<C, R>$ is isomorphic to the direct product of two groups, each cyclic of order 2, and Γ is a semidirect product of $<M, P>$ by $<C, R>$. In particular, it will follow that Γ has order exactly $4m^2$.

To that end, we examine possible automorphisms of the direct product of two groups cyclid of order m. We take a brief excursion into linear algebra. Suppose V is a finite dimensional vector space over a field k. Once we fix and order a basis for V, every linear transformation $\alpha: V \to V$ is uniquely representable by an $n \times n$ matrix, where n is the dimension of V. Assuming the ordered basis given and identifying α with its matrix, α will be a linear automorphism if and only if its determinant is nonzero. Under certain additional hypotheses on V, the above will in large measure carry over when the conditions are relaxed in k assuming only that k is a commutative ring with multiplicative identity $1 \neq 0$. Call a nonzero element u of such k a unit in k provided it has a multiplicative inverse u^{-1} in k. Call a vector space V over k a free k-module of (finite) rank n provided it has a basis with n elements (see [15]). Fix and order such a basis. Once this is done, every k-module homomorphism $\alpha: V \to V$ is uniquely determined by an $n \times n$ matrix with entries in k. Such an α will be an automorphism provided its determinant is a unit in k.

Now let V be a free rank-2 module over the ring of integers modulo m with basis

$$\{\bar{M}, \bar{P}\} = \left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right\}.$$

Let $< \bar{C}, \bar{R} >$ be the internal direct product of two groups $< \bar{C} >$ and $< \bar{R} >$, each cyclic of order 2. Observe that V, viewed as an Abelian group, is the internal direct product of two groups $< \bar{M} >$ and $< \bar{P} >$, each cyclic of order m.

We propose to define a function

$$\alpha :< \bar{C}, \bar{R} > \to \text{Aut}(V).$$

We define α on the generators $\bar{C}$ and $\bar{R}$ and will observe that the defining relations $\bar{C}^2 = \bar{R}^2 = 1$ and $\bar{C}\bar{R} = \bar{R}\bar{C}$ are preserved so that α extends to a group homomorphism. Explicitly, α sends $\bar{C}$ to the automorphism

$$\begin{bmatrix}x\\y\end{bmatrix} \to \begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix},$$

and α sends $\bar{R}$ to the automorphism

$$\begin{bmatrix}x\\y\end{bmatrix} \to \begin{bmatrix}1 & N+1\\0 & -1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}.$$

With these data, we construct the external semidirect product $< \bar{M}, \bar{P} > \rtimes_\alpha < \bar{C}, \bar{R} >$. Now the map on the generators M, P, C, and R of Γ into $< \bar{M}, \bar{P} > \rtimes_\alpha < \bar{C}, \bar{R} >$ given by

$$\begin{aligned} M &\to \bar{M},\\ P &\to \bar{P},\\ C &\to \bar{C},\\ R &\to \bar{R}, \end{aligned}$$

preserves the relations (1) through (8) so they extend to a homomorphism from Γ into $< \bar{M}, \bar{P} > \rtimes_\alpha < \bar{C}, \bar{R} >$. The image of the homomorphism must be the entire group, since it contains the generators $\bar{M}$, $\bar{P}$, $\bar{C}$, and $\bar{R}$. Thus, Γ of order at most $4m^2$ has a homomorphism image of order exactly $4m^2$. From this, it follows that Γ has order exactly $4m^2$ and must, in fact, be isomorphic with the semidirect product $< \bar{M}, \bar{P} > \rtimes_\alpha < \bar{C}, \bar{R} >$.

We have proven:

THEOREM 7.3 For any fixed integer $N > 0$, and any fixed integer $m \geq 2$, the set of four operators $\{M, P, C, R\}$ generates a semidirect product of a group $<M, P>$, which is the direct product of two groups $<M>$ and $<P>$, each cyclic of order m, by a group $<C, R>$, which is the direct product of two groups $<C>$ and $<R>$, each cyclic of order 2. In particular, $<M, P, C, R>$ has order $4m^2$.

A. Example

We show how to compute a product in Γ. Let $m = 4$ and $N = 10$. Then $\mu = e^{2\pi i/4}$. Consider the elements MP^2C and M^3CR. Their product is

$$\begin{aligned} MP^2C \cdot M^3CR &= MP^2\alpha(C)(M^3) \cdot CCR\\ &= MP^2M^{-3}C^2R\\ &= M^{-2}P^2R\\ &= M^2P^2R. \end{aligned}$$

Here we used the facts that conjugation by C is effected by

$$\begin{bmatrix}x\\y\end{bmatrix} \to \begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix},$$

C has order 2, M and P commute, and the exponents on M may be taken modulo 4.

VIII. LEVERAGING SIDELOBE-PRESERVER EQUIVALENCE CLASSES FOR EFFICIENCIES

There are at least two ways to make use of sidelobe-preserving group structure, for mth-root-of-unity codes for a given m and length N. One is efficient representation of low-sidelobe codes. The second is in exhaustive search for low-sidelobe codes. In either case, the idea is to list or check a single representative of each optimal-sidelobe equivalence class rather than every code in the search space. In the case of code searches, this approach should be combined with other efficiencies to achieve the best advantage for typically quite computationally demanding search tasks.

It is straightforward to identify a limit on achievable improvement in efficiency. The entire space of codes for a given N and m is m^N, and the maximum size of an equivalence class is $4m^2$. Hence, it is possible to shorten the list of codes, or to narrow the search space, by no more than a factor of $(1/4)m^{N-2}$. This factor corresponds to the case where every equivalence class has the maximum size of $4m^2$. Consider the quad-phase case, $m = 4$, giving a rule-of-thumb narrowing factor of $4m^2 = 64$. For $N = 10$, this would mean that 17 384 representative codes would need to be checked instead of 1 048 576. To determine the true number for a given case requires determining the exact number of equivalence classes.

For a given m and N, there will inevitably exist "degenerate" equivalence classes of size less than $4m^2$, containing codes of special structure. In the binary case, the fraction of codes that would need to be checked, or listed, is roughly 3/8, rather than 1/8 [11].

Work remains in studying equivalence class size distribution for given m and N. Furthermore, it would be useful for a given m and N to have an approach for generating single representatives of each equivalence class; this would help expedite exhaustive searches. An example of such a method for binary codes is given in [11]. Such an approach has yet to be found for nonbinary mth-root-of-unity codes.

IX. CONCLUSIONS

This paper considers the structure of groups of peak-sidelobe-preserving operators for the aperiodic autocorrelation of mth-root-of-unity 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 odd-length binary Barker codes can be discovered in a natural way from considering degeneracies in group actions.

Next the group structure is considered for the case of mth-root-of unity codes, a special case of the unimodular codes, for $m \geq 2$. The binary codes correspond to $m = 2$. When $m > 2$, there are m groups rather than one, and the group order is $4m^2$. Furthermore, the groups are not Abelian in general. Nevertheless the structure is identified for any $m \geq 2$ and code length $N > 0$. Future work will focus on studying group action degeneracies as a way to uncover new classes of low-sidelobe unimodular codes.

ACKNOWLEDGMENT

The authors would like to thank I. Martin Isaacs (Department of Mathematics, University of Wisconsin at Madison), David Joyner (Department of Mathematics, United States Naval Academy), and Chris Monsour (Travellers Insurance) for their help.

REFERENCES

[1] Skolnik, M.
Radar Handbook (2nd ed.). New York: McGraw-Hill, 1990.

[2] Barker, R. H.
Group synchronization of binary digital systems.
In *Communications Theory*, W. Jackson, Ed. London: Academic Press, 1953, pp. 273–287.

[3] Golomb, S., and Scholtz, R.
Generalized Barker sequences (transformations with correlation function unaltered, changing generalized Barker sequences).
IEEE Transactions on Information Theory, **11** (Oct. 1965), 533–537.

[4] Friese, M., and Zottman, H.
Polyphase Barker sequences up to length 31.
Electronics Letters, **30**, 23 (Nov. 1994), 1930–1931.

[5] Carter, N.
Visual Group Theory. Washington, DC: MAA Press, 2009.

[6] Levanon, N., and Mozeson, E.
Radar Signals. New York: Wiley, 2005.

[7] Pless, V. S., and Huffman, W. C. (Eds.)
Handbook of Coding Theory. North-Holland Mathematical Library, Amsterdam, The Netherlands: Elsevier Publishing Co., 1998.

[8] Golomb, S., and Win, M. Z.
Recent results on polyphase sequences.
IEEE Transactions on Information Theory, **44**, 2 (Mar. 1999), 817–824.

[9] Herstein, I. N.
Topics in Algebra (2nd ed.). New York: Wiley, 1975.

[10] Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A., and Wilson, R. A.
Atlas of Finite Groups. Oxford, United Kingdom: Clarendon Press, 1985.

[11] Coxson, G. E., Cohen, M. N., and Hirschel, A.
New results on minimum-PSL binary codes.
In *Proceedings of the 2001 IEEE National Radar Conference*, Atlanta, GA, May 2001, 153–156.

[12] Turyn, R. J., and Storer, J.
On binary sequences.
Proceedings of the American Mathematical Society, **12** (1961), 394–399.

[13] Militzer, B., Zamparelli, M., and Beule, D.
Evolutionary search for low autocorrelated binary sequences.
IEEE Transactions on Evolutionary Computation, **2**, 1 (1998), 34–39.

[14] Coxson, G. E.
The structure of sidelobe preserving operator groups.
In *Excursions in Harmonic Analysis*, Vol. 1. Birhauser, K. New York, 2001.

[15] Govorov, V. E.
Free module.
In M. Hazewinkel, Ed. *Encyclopaedia of Mathematics.* Vol. 4, Dordrecht, The Netherlands: Springer Verlag, 2001.

Greg Coxson has an M.A. degree in mathematics (1987) and a Ph.D. degree in electrical engineering (1993), both from the University of Wisconsin at Madison. He is a radar engineer who has worked at several radar houses, including the Radar Division of the Naval Research Laboratory (Washington, DC), Technology Service Corporation (Silver Spring, MD), Lockheed Martin (Moorestown, NJ), and Hughes Radar Systems (El Segundo, CA). He also worked in military operations research at the Center for Naval Analysis (Alexandria, VA), his first job after graduation from the University of Virginia.

Dennis Spellman received his Ph.D. degree in mathematics in 1971, working under Wilhelm Magnus in Group Theory at New York University's Courant Institute of Mathematical Sciences. He is the author or coauthor of over 30 research papers. Working with Seymour Lipschutz, he has revised Murray Spiegel's *Schaums Outline on Vector Analysis*; moreover, working with Seymour Lipschutz and John Schuller, he has revised Murray Spiegel's *Schaums Outline on Complex Variables*. Most recently, he is coauthor with Benjamin Fine, Anthony M. Gaglione, Gerhard Rosenberger, and Alexei G. Myasnikov of *The Elementary Theory of Groups*, published by DeGruyter.