IEEE P802.11
Wireless LANs

Walsh Function Cosets and Their Properties

Date: November 3, 1997

Author: John H. Cafarella
MICRILOR, Inc.
17 Lakeside Office Park, Wakefield, MA 01880
Phone: 781-246-0103
Fax: 781:246-0157
e-Mail: JohnCafarella@worldnet.att.net

Abstract

We explore the characteristics of communications waveforms for which a pseudonoise spreading code multiplies a Walsh function as selected by the input data to be conveyed over the communications link. The group structure of Walsh functions enables the selection of direct-sequence spreading codes to be combined with Walsh functions in this orthogonal signaling technique. For any particular code selected for spreading, all possible data patterns result in a composite code which is from the same coset. The cosets can be analyzed for their properties, giving us a means for constraining aspects of the link design.

We enumerate the cosets of 16-bit spreading codes, and determine correlation properties within and between cosets which provide minimum undesired correlations. The selection of 16-bit codes offers 2048 cosets among which to search for "good" codes; for 8-bit codes there are only 16 cosets, and these do not provide codes with the properties of the 16-bit codes. Some properties derive from the number of code bits being an even power of 2.

Walsh Function Cosets and Their Properties

We explore the characteristics of communications waveforms for which a pseudonoise spreading code multiplies a Walsh function as selected by the input data to be conveyed over the communications link. The group structure of Walsh functions enables the selection of direct-sequence spreading codes to be combined with Walsh functions in this orthogonal signaling technique. For any particular code selected for spreading, all possible data patterns result in a composite code which is from the same coset. The cosets can be analyzed for their properties, giving us a means for constraining aspects of the link design. We enumerate the cosets of 16-bit spreading codes, and determine correlation properties within and between cosets which provide minimum undesired correlations. The selection of 16-bit codes offers 2048 cosets among which to search for "good" codes; for 8-bit codes there are only 16 cosets, and these do not provide codes with the properties of the 16-bit codes. Some properties derive from the number of code bits being an even power of 2.

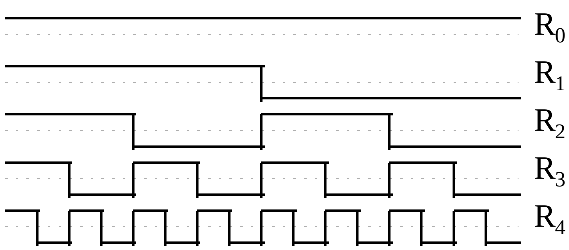

Figure 1 - Rademacher Functions.

1. Walsh Functions

Walsh functions and Rademacher functions are square-wave-like continuous-time functions with orthogonality properties analogous to sines and cosines familiar to engineers. We begin by defining the Rademacher functions, which are "squared-up" sinusoids:

$$R_N(t) = sign(\sin(2^N \pi t) \quad 0 \le t \le 1$$

The first five Rademacher functions are shown in figure 1. The Nth Rademacher function has 2^N sub-elements (bits), and each new function has a full ±1 excursion in a sub-element of the previous function. These functions are clearly orthogonal; however, since they possess odd symmetry about the origin they cannot be complete.

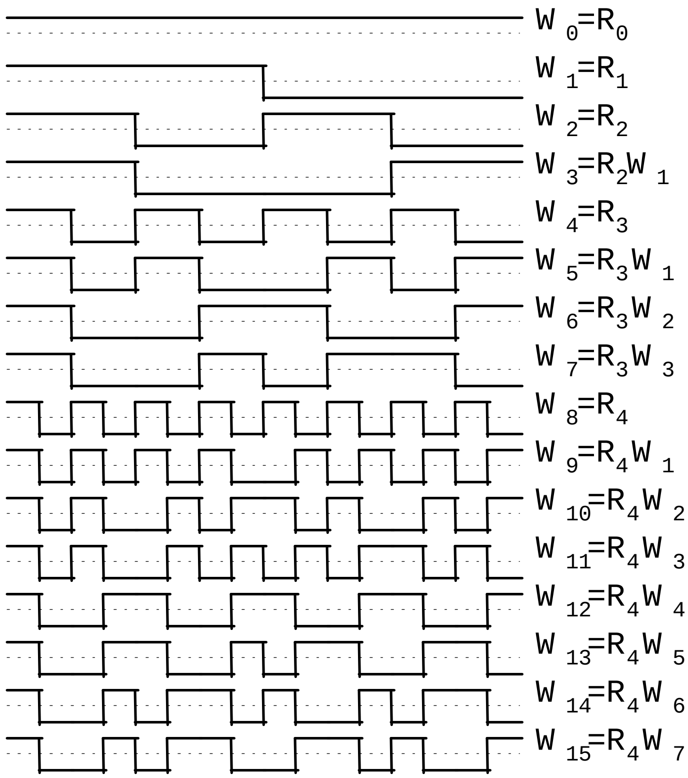

Figure 2 - Walsh functions.

The Walsh functions, constructed from products of the Rademacher functions, are the complete orthogonal set of square-wave-like functions. This construction of Walsh functions is called *dyadic ordering*; it is most convenient for mathematical manipulation. For Walsh function $W_M(t)$ the binary representation of M is used $M = \sum_{k=0} b_k 2^k$ in the product construction of Walsh functions, $b_k=\{0,1\}$.

$$W_M(t) = \prod_k R_k(t)^{b_k}$$

The first 16 Walsh functions are shown in Figure 2. The Walsh functions exhibit interesting structure. The first J Rademacher functions generate the first 2^{J-1} Walsh functions; if the J+1st Rademacher is included, then it forms a total of 2^J Walsh functions by multiplying each of the previous 2^{J-1} Walsh functions. The Walsh functions form a group; the product of any two of the 16 Walsh is another of them. This may be seen by

$$W_N(t)W_M(t) = \prod_i R_i(t)^{a_i} \prod_j R_j(t)^{b_j} = \prod_k R_k(t)^{a_k+b_k} = \prod_k R_k(t)^{c_k} = W_J(t)$$

$$W_{Nn} \equiv W_N(t)|_{t=n/N^+} \quad n = 0,1\ldots N-1$$

Thus, the index of the Walsh function produced by multiplying two other Walsh functions is obtained by bit-wise Exclusive Or (XOR) of the binary representations of their indices.[1] A direct-sequence spread-spectrum modulator converts the composite code from a sequence of binary bits {0,1} into a continuous baseband waveform with amplitude {±1}. To explore the characteristics of spreading waveforms formed by combining direct-sequence codes with Walsh functions, we consider discrete Walsh functions which are the sequences formed by sampling the Walsh functions once per sub-element.

We adopt this dual-index notation with possible suppression of the second index for convenience. Thus, W_K represents the identity of the K^{th} Walsh function. When we must consider the 16 values taken on by the sub-elements of W_K we use the second subscript W_{Kn}. The actual value and meaning of the single number W_{Kn}, for some specific K and n, are subject to the same ambiguity as is the case for spreading codes: there is an isomorphism between logic values over {0,1}, baseband amplitudes over {±1}, and carrier phase values over {0,ð}. For example, when designing digital logic, the values of both spreading codes and Walsh functions are boolean {0,1}; consideration of waveform correlation properties requires algebraic interpretation of the sub-element values {±1}. This isomorphic relationship is routinely handled in design of spread-spectrum systems, and is normally clear by context. However, for discussion purposes we must still select the specific isomorphism, that is, which of the two elements in {0,1} corresponds to which of {±1}. We select the correspondence shown. For enumerating the spreading codes and Walsh functions, we will interpret the 16-bit binary pattern of the boolean values as a binary number; selecting the correspondence between boolean 0 and +1 amplitude simply means that W_0 is at the beginning of the numerical order (0) instead of at 2^{16}-1. When we describe a Walsh function we use its Hexadecimal numerical value, since this quickly conveys the actual bit pattern if needed. With this digression concerning the discrete representation of the Walsh functions, and the meaning of the sub-element values, we now return to exploring cosets.

	π

2. Coset Decomposition

Because the Walsh functions form a proper sub-group of the 16-bit codes, it is possible use them to perform a coset decomposition. We begin with the 16 Walsh functions as the base sub-group; then, select any other 16-bit code C_1 as coset leader, and the product[2] of this with each of the Walsh functions generates a coset. For each new coset we must select as coset leader some code which has not yet appeared in any of the previous cosets. We are guaranteed by group theory that this decomposition will enumerate all codes, and that each will appear in only a single coset.

W_0	W_1	W_2	W_3	W_4	W_5	W_6	W_7	W_8	W_9	W_{10}	W_{11}	W_{12}	W_{13}	W_{14}	W_{15}
C_1	C_1W_1	C_1W_2	C_1W_3	C_1W_4	C_1W_5	C_1W_6	C_1W_7	C_1W_8	C_1W_9	C_1W_{10}	C_1W_{11}	C_1W_{12}	C_1W_{13}	C_1W_{14}	C_1W_{15}
C_2	C_2W_1	C_2W_2	C_2W_3	C_2W_4	C_2W_5	C_2W_6	C_2W_7	C_2W_8	C_2W_9	C_2W_{10}	C_2W_{11}	C_2W_{12}	C_2W_{13}	C_2W_{14}	C_2W_{15}
Etc.															

Because of this, any spreading code P_K may be selected as a coset leader multiplying $\{W_1,W_2,....W_{16}\}$ to form the coset $\{P_KW_0,P_KW_1,....P_KW_{16}\}$. Each of these is, in turn, a legitimate spreading code, and any could be selected as the coset leader with the result of re-ordering the coset. The importance of this ordering into cosets is that properties of codes within a coset, or mutual properties between codes of different cosets, may be evaluated in order to enable selection of "good" cosets for radio transmission. For example, if it were considered important for

[1] Note that this gives a trivial proof of the orthogonality of Walsh functions. All but W_0 integrate to zero; but only the product of a Walsh function with itself can produce W_0. Thus, $\int W_N(t)\, W_M(t)\, dt = d$

transmitted waveforms to have low autocorrelation side lobes, then a coset could be selected for which all members had low side lobes (by computer search). Then, no matter which member of the coset were selected for the spreading code, and no matter what the data (which Walsh function selected), then the side lobes would be bounded by the worst-case values for the coset.

To enumerate the cosets, we first limit interest to the 2^{15} codes which have leading 0s; the other half of the total 2^{16} codes are simply complements of the first half, and are not distinct since they will occur with a π flip of the carrier phase. Furthermore, the correspondence between boolean 0 and amplitude +1 results in binary interpretation of the Walsh functions having leading 0s. The 16 Walsh functions, in hexadecimal notation, are shown in the top text box at right. Because each coset has 2^4=16 members, there must be 2^{11}=2048 cosets to account for the 2^{15} codes. In hexadecimal notation, the coset leaders C_K are listed in the bottom text box at right. Each range of coset leaders contains 128 members, and there are 16 such ranges for a total of 2048 coset leaders.

0000-007F	1000-107F
0100-017F	1100-117F
0200-027F	1200-127F
0300-037F	1300-137F
0400-047F	1400-147F
0500-057F	1500-157F
0600-067F	1600-167F
0700-077F	1700-177F

3. Cosets Whose Codes Have Low Correlation Side Lobes

For many applications it is desirable to select codes having low autocorrelation and/or crosscorrelation side lobes for near-in shifts. For Walsh-Orthogonal signaling we must **find cosets for which all members satisfy whatever constraint is being imposed**. Computer search has identified several interesting sets of cosets: [3]

-Cosets with autocorrelation side lobes ≤4 over four side lobes, and ≤5 in the 5th.

0272	**0356**	**0359**	**036A**	0475	**0539**	**0563**	**0635**
064A	0652	**0653**	**065C**	0735	074A	103A	105D
114B	114D	**121D**	1228	**122E**	**1247**	1262	1272
1274	131D	1362	1412	141A	**141B**	**1427**	1441
1448	**144E**	147D	172D	**1742**			

- Cosets with autocorrelation side lobes ≤3 over the first five side lobes; call these set A.

0563	**0653**	**065C**	**114B**
1247	**1274**	**141B**	**1427**

- Cosets with cross-correlation side lobes <8 over four side lobes, and ≤9 in the 5th; call these set C.

0158	020E	0461	0737
1049	131F	1570	1626

[3] The codes appearing in bold font are "R_L" to be discussed later.

4. Cosets with Low Inter-Coset Main-Lobe Correlation

Within a coset all members have zero cross-correlation by construction. We now seek pairs of cosets for which low main-lobe cross-correlation exists **between all members of one coset and all members of the other**. We use the spreading-code coset leaders P_K identified above, but the reader should remember that any coset member also could be used. We consider two M-Orthogonal streams X_n and Y_n, independent but time-aligned.[4]

$$X_n = P_{Kn} W_{Jn}$$

$$Y_n = P_{Mn} W_{Ln}$$

The selection of the indices J and L convey four bits each, and it is desired to select the cosets (P_K and P_M) to minimize crosscorrelation between the two streams independent of the data (J and L). $Ã_{KJML}$ is given by

Since the product of any two of the 16 Walsh functions is

$$\Gamma_{KJML} = \sum_n P_{Kn} W_{Jn} P_{Mn} W_{Ln}$$

another of them, we really seek to select K and M to minimize[5]

$$\overline{\overline{\Gamma}}_{KM} = \left| \sum_n P_{Kn} P_{Mn} W_{Nn} \right|_{\max\ over\ N}$$

We define a subset R_L of the coset leaders such that we can constrain $P_K=P_M R_L$. This lets us bound the peak magnitude of

$$\overline{\overline{\Gamma}}_{KM} = \left| \sum_n R_{Ln} W_{Ln} \right|_{\max\ over\ N}$$

Hence, we can minimize the worst-case crosscorrelation between codes from coset P_K and codes from coset P_M. A computer search identified as members of the set R_L the 28 coset leaders shown in the text box at right. Interestingly, to minimize the maximum correlation, these project with equal magnitude on all the Walsh functions at ±4 units compared to a peak autocorrelation of 16 for main-lobe autocorrelation. Thus, the crosscorrelation at the is fixed at -12 dB in all channels, and this level is non-fluctuating in magnitude.6

0356	0359	0365	036A
0536	0539	0563	056C
0635	063A	0653	065C
111E	112D	114B	1178
121D	122E	1247	1274
141B	1427	144E	1472
1718	1724	1742	177E

[4] By changing coset from symbol to symbol using codes defined in this section, toleration of delay spreads larger than a symbol duration can be enhanced.

[5] As stated earlier, we have not restricted the selection of spreading codes to coset leaders, we may now recognize that P_K and P_M above may be one of the coset leaders exclusive ORed with any Walsh function, and we may also absorb those Walsh functions into W_N.

[6] This result is readily understood by recognizing the form to be minimized as a Walsh transform. Applying Parseval's theorem, minimizing the peak value requires equal dispersement of the transform over the basis functions. This is only possible if the square root of the order of the Walsh functions is an integer; that is, the number of chips per symbol must be an even power of 2.

5. Low Intra- and Inter-Coset Correlation Side Lobes

The cosets of section 3 indicated in bold are also members of the set R_L. Note that the eight best cosets A, in terms of autocorrelation side lobes, share this property. The best eight cosets C, in terms of intra-coset crosscorrelation, do not at first appear to be related to cosets R_L.

Since both sets of 8 cosets (A and C) seem interesting for various applications, we explore them further for useful relationships. We begin by forming the bit-wise XOR of the coset leaders with other coset leaders: the set A with itself, the set C with itself, and the set A with the set C. The text box on the next page shows these three 8x8 arrays of bit-wise XORs. The rows and columns are labeled with the coset leaders being used, respectively. There is clearly some structure here within the autocorrelation cosets and within the crosscorrelation cosets, but not between the two.

The XOR of the C cosets has four R_L per row (hence, column). Of interest is the fact that any coset combined with the others generates a permutation of the same set of codes.

C\C	0158	020E	0461	0737	1049	131F	1570	1626
0158	0000	**0356**	**0539**	066F	1111	**1247**	1428	**177E**
020E	**0356**	0000	066F	**0539**	**1247**	1111	**177E**	1428
0461	**0539**	066F	0000	**0356**	1428	**177E**	1111	**1247**
0737	066F	**0539**	**0356**	0000	**177E**	1428	**1247**	1111
1049	1111	**1247**	1428	**177E**	0000	**0356**	**0539**	066F
131F	**1247**	1111	**177E**	1428	**0356**	0000	066F	**0539**
1570	1428	**177E**	1111	**1247**	**0539**	066F	0000	**0356**
1626	**177E**	1428	**1247**	1111	066F	**0539**	**0356**	0000

The XOR of the A cosets has two or three R_L per row (hence, column). There is no other structure observable.

A\A	0563	0653	065C	114B	1247	1274	141B	1427
0563	0000	0330	033F	1428	**1724**	1717	**1178**	1144
0653	0330	0000	000F	**1718**	1414	**1427**	1248	**1274**
065C	033F	000F	0000	1717	**141B**	1428	**1247**	127B
114B	1428	**1718**	1717	0000	030C	033F	0550	**056C**
1247	**1724**	1414	**141B**	030C	0000	0033	**065C**	0660
1274	1717	**1427**	1428	033F	0033	0000	066F	**0653**
141B	**1178**	1248	**1247**	0550	**065C**	066F	0000	003C
1427	1144	**1274**	127B	**056C**	0660	**0653**	003C	0000

The A cosets taken with the C cosets exhibits no obvious structure.

C\A	0563	0653	065C	114B	1247	1274	141B	1427
0158	043B	070B	0704	1013	131F	132C	1543	157F
020E	076D	045D	0452	1345	1049	107A	1615	1629
0461	0102	0232	023D	152A	1626	1615	107A	1046
0737	0254	0164	016B	167C	1570	1543	132C	1310
1049	152A	161A	1615	0102	020E	023D	0452	046E
131F	167C	154C	1543	0254	0158	016B	0704	0738
1570	1013	1323	132C	043B	0737	0704	016B	0157
1626	1345	1075	107A	076D	0461	0452	023D	0201

A coset XORed with any R_L produces a coset whose codes have relatively low crosscorrelation at zero shift with codes from the original coset. We explore the set C XORed with the four R_L which showed up in the C\C portion of the previous table. We label the rows with the coset leaders of the set C, and the columns with the apparently special R_L {0356,0539,1247,177E}.

In this text box we display the matrix of XOR results. The rows have been re-ordered to exhibit more clearly the structure. Define the following sets of codes for discussion:
X={0158,0461,131F,1626}
Y={020E,0737,1049,1570}
Ã={**0539**,**1247**,**177E**}

The code **0356** XORed with the coset leaders X produce the coset leaders Y, and with the coset leaders Y produce the coset leaders X. The codes Ã XORed with any coset from X produce another coset from X; and the same is true for Ã with cosets from Y. We now have two interesting sets of four coset leaders each. This also indicates that the set of 8 cosets C has good inter-coset correlation side-lobe properties, not just intra-coset.

C	**0356**	**0539**	**1247**	**177E**
0158	020E	0461	131F	1626
0461	0737	0158	1626	131F
131F	1049	1626	0158	0461
1626	1570	131F	0461	0158
020E	0158	0737	1049	1570
0737	0461	020E	1570	1049
1049	131F	1570	020E	0737
1570	1626	1049	0737	020E