On the Hadamard transform of monotone Boolean functions

Charles Celerier, David Joyner, Caroline Melles, David Phillips*

June 7, 2012

Abstract

Let $f : GF(2)^n \to GF(2)$ be a monotone Boolean function. Associated to f is the Cayley graph X whose vertices correspond to points of $GF(2)$ and whose edges correspond to pairs of vectors (v, w) whose sum is in the support of f. The spectrum of X (the set of eigenvalues of its adjacency matrix) can be computed in terms of the Hadamard transform of f. We show that if f is atomic, the adjacency matrix of X is singular if and only if the support of f has an even number of elements. We ask whether it is true that for every even monotone function the adjacency matrix of the Cayley graph must be singular. We give an example in dimension $n = 6$ to show that the answer to this question is no. We use Sage to compute some examples of monotone Boolean functions, their Cayley graphs, and the graph spectra. We include some interesting characterizations of monotone functions. We give some conditions on a monotone function that imply that the function is not bent. Finally, we ask whether it is true that no even monotone function is bent.

1 Introduction

We begin with notation and by recalling some background from [Sta07], [BC99].

*USNA, Mathematics Department; email: charles.celerier@gmail.com, wdj@usna.edu (corresponding author), cgg@usna.edu, dphillip@usna.edu

For a given positive integer n we may identify a Boolean function

$$f : GF(2)^n \to GF(2),$$

with its support

$$\Omega_f = \{x \in GF(2)^n \mid f(x) = 1\}.$$

For each $S \subset GF(2)^n$, let $\overline{S}$ denote the set of complements $\overline{x} = x + (1, \ldots, 1) \in GF(2)^n$, for $x \in S$, and let $\overline{f} = f + 1$ denote the complementary Boolean function. Note that

$$\Omega_f^c = \Omega_{\overline{f}},$$

where S^c denotes the complement of S in $GF(2)^r$ Let

$$\omega = |\Omega_f|$$

denote the cardinality of the support. We call a Boolean function *even* (resp., *odd*) if ω_f is even (resp., odd). We may identify a vector in $GF(2)^n$ with its support, or, if it is more convenient, with the corresponding integer in $\{0, 1, \ldots, 2^n - 1\}$. Let

$$b : \{0, 1, \ldots, 2^n - 1\} \to GF(2)^n$$

be the binary representation ordered with least significant bit last (so that, for example, $b(1) = (0, \ldots, 0, 1) \in GF(2)^n$). For convenience, we index vectors starting at 0, i.e., so a vector $x \in GF(2)^3$ has components x_0, x_1, and x_2.

Let H_n denote the $2^n \times 2^n$ Hadamard matrix defined by $(H_n)_{i,j} = (-1)^{b(i)\cdot b(j)}$, for each i, j such that $0 \leq i, j \leq n - 1$. Inductively, these can be defined by

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}, \qquad n > 1.$$

The *Hadamard transform* of f is defined to be the vector in $\mathbb{R}^{2^n}$ whose kth component is

$$(\mathcal{H}f)(k) = \sum_{i \in \{0,1,\ldots,2^n-1\}} (-1)^{b(i)\cdot b(k) + f(b(i))} = (H_n(-1)^f)_k,$$

where we define $(-1)^f$ as the column vector where the ith component is

$$(-1)^f_i = (-1)^{f(b(i))},$$

for $i = 0, \ldots, 2^n - 1$. We define a Boolean function $f : GF(2)^n \to GF(2)$ to be *bent* if the absolute value of each component of its Hadamard transform is $2^{n/2}$. Clearly, since each component of the Hadamard transform must be an integer, there are no bent functions when n is odd.

DP: Please review the definition

Example 1 (a bent, odd function)**.** *Let $f : GF(2)^2 \to GF(2)$ be defined as $f(x_1, x_2) = x_1x_2$. Then $\Omega_f = \{(1,1)\}$ so $\omega = 1$ and f is odd. Also, f is bent because*

$$(-1)^f = \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}$$

and so

$$\mathcal{H}f = H_2(-1)^f = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 2 \\ -2 \end{pmatrix}.$$

{example:3vars}

Example 2. *A Boolean function of three variables cannot be bent. Let f be defined by:*

x_1	*0*	*0*	*0*	*0*	*1*	*1*	*1*	*1*
x_2	*0*	*0*	*1*	*1*	*0*	*0*	*1*	*1*
x_3	*0*	*1*	*0*	*1*	*0*	*1*	*0*	*1*
$(-1)^f$	*1*	*-1*	*1*	*-1*	*1*	*-1*	*1*	*-1*
$\mathcal{H}f$	*0*	*8*	*0*	*0*	*0*	*0*	*0*	*0*

This function is even because

$$\Omega_f = \{(0,0,1), (0,1,1), (1,0,1), (1,1,1)\}, \quad \textit{so} \quad \omega = 4.$$

{example:4vars}

Example 3. *A Boolean function of four variables:*

x_1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
x_2	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_3	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_4	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$(-1)^f$	1	1	1	1	1	1	1	-1	1	1	1	-1	-1	-1	-1	-1
$\mathcal{H}f$	4	4	4	-4	8	0	0	0	8	0	0	0	-4	-4	-4	4

In this example, the function is even and $\omega = 6$.

CGM: Changed f to $(-1)^f$.6/4/12

For any two $x, y \in GF(2)^n$, let $d(x, y)$ denote the *Hamming metric*:

$$d(x, y) = |\{0 \leq i \leq n-1 \mid x_i \neq y_i\}|. \tag{1}$$

We define the *weight* wt of x to be the number of non-zero coordinates of x, so $d(x, y) = \mathrm{wt}(x - y)$.

Example 4. *We use Sage to look at the example of*

$$f(x_0, x_1, x_2, x_3) = x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_0x_2 + x_1x_2x_3 + x_1x_2 + x_2x_3.$$

First, we attach the file `afsr.sage` *available from Celerier [Cel], then run the following commands.*

Sage

```
sage: from sage.crypto.boolean_function import *
sage: R.<x0, x1, x2, x3> = BooleanPolynomialRing(4)
sage: f = BooleanFunction(x0*x1*x2 + x0*x1*x3 + x0*x2*x3 + x0*x2 +
x1*x2*x3 + x1*x2 + x2*x3)
sage: g = BooleanFunction([0,0,0,0,0,1,1,1,0,0,0,1,1,1,1,1])
sage: g.is_bent()
False
sage: is_monotone(g)
True
sage: g.truth_table(format='int')
(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)
sage: f.truth_table(format='int')
(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)
sage: g.algebraic_normal_form()
x0*x1*x2 + x0*x1*x3 + x0*x2*x3 + x0*x2 + x1*x2*x3 + x1*x2 + x2*x3
sage: f.algebraic_normal_form()
x0*x1*x2 + x0*x1*x3 + x0*x2*x3 + x0*x2 + x1*x2*x3 + x1*x2 + x2*x3
```

This shows how to construct Boolean functions in Sage using the `sage.crypto` *module. The only command from* `afsr.sage` *is the* `is_monotone` *function*[1].

[1] Monotonicity is defined in §3 below.

We then show that, in spite of f and g being constructed in different ways, they have the same values ("truth table") and have the same algebraic normal form[2]*.*

2 The Cayley graph

Let $X = (V, E)$ be the *Cayley graph* of f:

$$V = GF(2)^n, \qquad E = \{(v, w) \in V \times V \mid f(v + w) = 1\}.$$

We shall assume throughout and without further mention that

$$f(0) \neq 1,$$

so X has no loops. In this case, X is an ω-regular graph having r connected components, where

$$r = |GF(2)^n / \mathrm{Span}(\Omega_f)|.$$

For each vertex $v \in V$, the set of neighbors $N(v)$ of v is given by

$$N(v) = v + \Omega_f,$$

where v is regarded as a vector and the addition is induced by the usual vector addition in $GF(2)^n$. Let $A = (A_{ij})$ be the $2^n \times 2^n$ adjacency matrix of X, so

$$A_{ij} = f(b(i) + b(j)), \qquad 0 \leq i, j \leq 2^n - 1.$$

{example:3vars-gra

Example 5. *Here are some Sage commands to help visualize the Boolean function f of three variables in Example 2:*

Sage

```
sage: flist = [0,1,0,1,0,1,0,1]
sage: V = GF(2)^3
sage: Vlist = V.list()
sage: f = lambda x: GF(2)(flist[Vlist.index(x)])
sage: X = boolean_cayley_graph(f, 3)
sage: X.adjacency_matrix()
[0 1 0 1 0 1 0 1]
[1 0 1 0 1 0 1 0]
[0 1 0 1 0 1 0 1]
```

[2] The ANF is discussed, for example, in [Cel12].

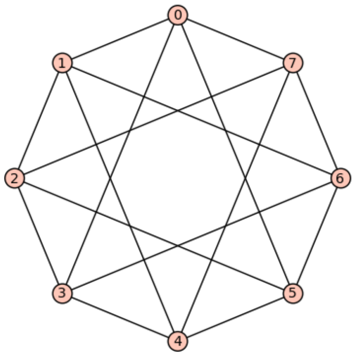

Figure 1: The Cayley graph of the Boolean function of three variables from Example 2. (The vertices are ordered as in the Example.)

{fig:monotone-bool

```
    [1 0 1 0 1 0 1 0]
    [0 1 0 1 0 1 0 1]
    [1 0 1 0 1 0 1 0]
    [0 1 0 1 0 1 0 1]
    [1 0 1 0 1 0 1 0]
    sage: X.spectrum()
    sage: X.show(layout="circular")
```

The last command gives rise to the Cayley graph X of f shown in Figure 1. The adjacency matrix A of X is given by

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

and the graph spectrum by

$$\{-4, 0, 0, 0, 0, 0, 0, 4\}.$$

{example:4vars-gra

Example 6. *For the Boolean function of four variables in Example 3, the Cayley graph is given in Figure 2. The adjacency matrix A of the graph is*

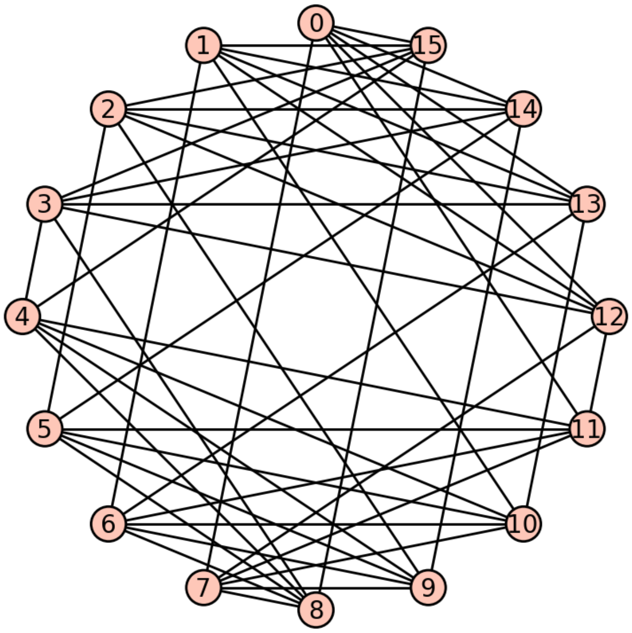

Figure 2: The Cayley graph of the Boolean function of four variables from Example 3. (The vertices are ordered as in the Example.) {fig:monotone-bool

$$A = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

and the graph spectrum is

$$\{-4,-4,-2,-2,-2,0,0,0,0,0,0,2,2,2,2,6\}.$$

These may be computed using Sage commands, as in the last example.

CGM: I rewrote the following section, changing notation and adding some subscripts.6/4/12

We wish to relate the spectrum of the Cayley graph X (the eigenvalues of the adjacency matrix A) to the Hadamard transform $\mathcal{H}f = H_n(-1)^f$. Recall that $(-1)^f$ is defined to be the column vector whose ith component is $((-1)^f)_i = (-1)^{f_i}$, where $f_i = f(b(i))$ for $i = 0, 1, ..., 2^n - 1$. Note that f and $(-1)^f$ are related by the equation

$$f = \frac{1}{2}(e - (-1)^f),$$

where $e = (1, 1, ..., 1)$. For $k = 0, 1, ..., 2^n - 1$, let $w_k \in \{\pm 1\}^{2^n}$ be the column vector whose ith component is

$$(w_k)_i = (-1)^{b(k)\cdot b(i)}.$$

Each vector w_k is an eigenvector of A, since for each i,

$$\begin{aligned}
(Aw_k)_i &= \sum_{j=0}^{2^n-1} f(b(i)+b(j))(-1)^{b(k)\cdot b(j)} \\
&= (-1)^{b(k)\cdot b(i)} \sum_{j=0}^{2^n-1} (-1)^{b(k)\cdot(b(i)+b(j))} f(b(i)+b(j)) \\
&= (w_k)_i \sum_{l=0}^{2^n-1} (-1)^{b(k)\cdot b(l)} f(b(l)) \\
&= (w_k)_i \sum_{l=0}^{2^n-1} (H_n)_{k,l} f_l \\
&= (w_k)_i (H_n f)_k \qquad (2) \quad \texttt{\{eq:w1\}} \\
&= (w_k)_i (H_n \frac{1}{2}(e - (-1)^f))_k \\
&= (w_k)_i \frac{1}{2}(H_n e - \mathcal{H}f)_k. \qquad (3) \quad \texttt{\{eq:w2\}}
\end{aligned}$$

Then Equation (2) proves that w_k is an eigenvector of A having eigenvalue $\lambda_k = (H_n f)_k$, where H_n is the nth Hadamard matrix, and Equation (3) demonstrates the affine relationship $\lambda_k = \frac{1}{2}(H_n e - \mathcal{H} f)_k$ between the spectrum of X and the Hadamard transform. Therefore, the spectrum of X,

$$\mathrm{Spectrum}(X) = \{\lambda_k \mid 0 \leq k \leq 2^n - 1\},$$

is explicitly computable as an expression in terms of f.

There is another useful expression for λ_k. Let Ω_f^* be the $\omega \times n$ matrix whose column vectors are the elements of Ω_f:

$$\Omega_f^* = \left(\begin{array}{c} y_1 \dots y_\omega \end{array} \right), \qquad \Omega_f = \{y_1, \dots, y_\omega\}.$$

Then, for $k \in \{0, \dots, 2^n - 1\}$,

$$\begin{aligned} \lambda_k &= \sum_{y \in GF(2)^n} (-1)^{b(k) \cdot y} f(y) \\ &= \sum_{y \in \Omega_f} (-1)^{b(k) \cdot y} \\ &= \sum_{y \in \Omega_f} (1 - 2(b(k) \cdot y \mod 2)) \\ &= \omega - 2\mathrm{wt}\left(\left(b(k)^\top \Omega_f^* \right) \mod 2 \right), \end{aligned}$$

This tells us that an integer m belongs to Spectrum(X) if and only if there is an $x \in GF(2)^n$ such that the number of $y \in \Omega_f$ which are not orthogonal mod 2 to x in $GF(2)^n$ is $\frac{m-\omega}{2}$.

CGM: Changed row to column vectors in Ω_f^* and changed last sentence to not orthogonal mod 2. 6/6/12

3 Monotone functions

Define a partial order $\leq$ on $GF(2)^n$ as follows: for each $v, w \in GF(2)^n$, we say

$$v \leq w$$

whenever we have $v_1 \leq w_1$, $v_2 \leq w_2$, ..., $v_n \leq w_n$. A Boolean function is called *monotone* (increasing) if whenever we have $v \leq w$ then we also have $f(v) \leq f(w)$. Examples 2 and 3 above are monotone.

CGM: Added note regarding ex.s 2 and 3. 6/6/12

Note that if f and g are monotone then (a) $f + g + fg$ is also monotone, and (b) $\overline{\Omega_f} \cap \overline{\Omega_g} = \overline{\Omega_{fg}}$. (Equivalently, if f and g are monotone *decreasing* then so is fg, and moreover we have $\Omega_f \cap \Omega_g = \Omega_{fg}$.)

There are some interesting characterizations of monotone functions.

- For $f : GF(2)^n \to GF(2)$ any Boolean function of n variables, let

$$f_0(x_1, \ldots, x_{n-1}) = f(0, x_1, \ldots, x_{n-1}),$$
$$f_1(x_1, \ldots, x_{n-1}) = f(1, x_1, \ldots, x_{n-1}).$$

  The function f is monotone if and only if (a) both of the subfunctions f_0 and f_1 are monotone and (b) $\Omega_{f_0} \subset \Omega_{f_1}$.

- For a given positive integer n and our partial ordering, the *Hasse diagram*, D_n, is the directed graph with a vertex for each vector in $GF(2)^n$ and for which (v, w) is an edge if $v \leq w$ and $wt(w) = wt(v) + 1$ (see Example 10). We define a *closure* of a directed graph $G = (V, E)$ to be a set of nodes without any outgoing edges, i.e., a set of nodes, $C \subseteq G$, with the property that if $i \in C$ and $(i, j) \in E$, then $j \in C$. We can then count the number of monotone functions on n variables by counting the number of closures on D_n.[3] Closures on directed graphs have several applications, e.g., in defense [Orl87], mining [Joh68, HC00, BZ10], and shipping [Rhy70].

Theorem 7. *For all positive integers n, the set of closures on D_n are in one-to-one correspondence with the set of monotone functions on $GF(2)^n$.*

Proof. Let n be a given positive integer and consider the set of monotone functions on $GF(2)^n$. We claim that the relation mapping Boolean functions on $GF(2)^n$ to their support defines a one-to-one correspondence from monotone functions to closures on D_n. Note that such a relation is a function from Boolean functions to subsets of $GF(2)^n$, i.e., subsets of vertices in D_n. We claim that the support of a monotone

[3] We believe this is a known result, but are not able to find a previous reference.

Boolean function is a closure on D_n. Let f be a given monotone Boolean function on $GF(2)^n$. For given vertices $v, w \in GF(2)^n$, suppose that $v \in \Omega_f$ and that (v, w) is an edge in D_n. Then, $w_i = v_i + 1$ for exactly one $i \in \{0, \ldots, 2^n - 1\}$ and $w_j = v_i$ for all $j \in \{0, \ldots, 2^n - 1\} \setminus \{i\}$, i.e., $v < w$. Then, because $v \in \Omega_f$ and f is monotone, $1 = f(v) \leq f(w)$ so $w \in \Omega_f$. Thus, Ω_f is a closure in D_n.

To see that the support is injective, note that two different Boolean functions have different supports. To see that the support is surjective, let $C \subseteq GF(2)^n$ be a given closure in D_n and define f_C as the function with C as a set of support vectors, i.e., for all $v \in C$, $f_C(v) = 1$. We claim that f_C is monotone. Let $v, w \in GF(2)^n$ be given where $v \leq w$ and $v \neq w$. If $f_C(v) = 0$ then $f_C(v) \leq f_C(w)$, trivially, so assume that $f_C(v) = 1$, i.e., $v \in C$. Note that if $v \leq w$ and $v \neq w$ then for some positive integer k, there are k components where v has a zero and w has a one. For $i \in \{0, \ldots, 2^n - 1\}$, let e_i denote the vector with one in component i and zero in all other components. Then there is a set $\{i_1, \ldots, i_k\} \subset \{0, \ldots, 2^n - 1\}$ where $w = v + \sum_{j=1}^{k} e_j$. For $\ell \in \{0, \ldots, k\}$, let $u_\ell = v + \sum_{j=1}^{\ell} e_j$. By the definition of the Hesse diagram, for $\ell \in \{0, \ldots, k-1\}$, $(v_\ell, v_{\ell+1})$ are edges in D_n. Then, as $v = v_0 \in C$, by the closure property, $v_\ell \in C$ for all $\ell \in \{0, \ldots, k\}$, so, in particular, $f_C(w) = f_C(v_k) = 1 \geq f_C(v)$.

□

- The set $\{\mathrm{supp}(v) \mid \overline{v} \in \Omega_f\}$ is an ideal[4] of $\{0, 1, \ldots, n-1\}$ (see, for example, Kleitman [Kle69]).

For each $v \in GF(2)^n$, define a monotone function $f = f_v$ to be *atomic based on* v if its support consists of all vectors greater than v, i.e., if

$$\Omega_f = \{x \in GF(2)^n \mid v \leq x\},$$

where $\leq$ is the partial order defined above. We call f *atomic* if there is some $v \neq 0$ such that f is atomic based on v. Note that Example 2 is monotone and atomic based on $(0, 0, 1)$ while Example 3 is monotone but not atomic.

[4] An *ideal* in a set U is a collection I of subsets of U such that $B \in I$ and $A \subset B$ implies $A \in I$.

CGM: Changed Ex 2 not atomic to Ex 2 is atomic. 6/6/12

{def:leastsupport}

Definition 8. Let $f : GF(2)^n \to GF(2)$ any monotone function. We say that $\Gamma \subset GF(2)^n$ forms a set of vectors of *least support* for f if Γ consists of all vectors in Ω_f which are smallest in the partial ordering $\leq$ on $GF(2)^n$.

For example, the set of vectors of least support for Example 3 is $\Gamma = \{(0,1,1,1),(1,0,1,1),(1,1,0,0)\}$.

CGM: Added this ref to Example 3. 6/6/12

A monotone function is atomic if and only if it has only one vector in its set of least supports. Here is an interesting group-theoretical characterization of atomic monotone functions.

{prop:atomic-subsp

Proposition 9. *Let f be a Boolean monotone function which is not a constant function. Then f has atomic support if and only if the set of complements $\overline{\Omega_f}$ is a subspace of $GF(2)^n$.*

Proof. Suppose that f has atomic support based on v. Then $v \leq w$ for all $w \in \Omega_f$. Then $\overline{w} \leq \overline{v}$ for all $\overline{w} \in \overline{\Omega_f}$. If $\overline{w_1}$ and $\overline{w_2}$ are in $\overline{\Omega_f}$ then $\overline{w_1}+\overline{w_2} \leq \overline{v}$. Indeed, consider the ith component of $\overline{v}$: if it is 0 then the ith components of $\overline{w_1}$ and $\overline{w_2}$ must be 0, and if it is 1 then it is impossible for the ith component of the sum to be any larger. Therefore $\overline{\Omega_f}$ is a subspace.

Conversely, suppose that $\overline{\Omega_f}$ is a proper subspace of $GF(2)^n$ and let x be any element of $\overline{\Omega_f}$.

Next, we claim that if $x \in \overline{\Omega_f}$ and if $y \leq x$, then $y \in \overline{\Omega_f}$. But $y \leq x$ if and only if $\overline{y} \geq \overline{x}$. Because f is monotone, $\overline{y} \in \Omega_f$, proving the claim.

Now let z be any element of maximal weight in $\overline{\Omega_f}$. Let h be the weight of z. Since f is monotone, there must be at least h weight 1 vectors in $\overline{\Omega_f}$, by the previous claim. Suppose there is a vector $y \in \overline{\Omega_f}$ such that y is not less than or equal to z. Then there must be at least $h+1$ (distinct) weight 1 vectors in $\overline{\Omega_f}$. Their sum must also be in $\overline{\Omega_f}$, so z is not a maximal weight element of $\overline{\Omega_f}$. Therefore $\overline{\Omega_f}$ consists of all elements y of $GF(2)^n$ such that $y \leq z$ and Ω_f consists of all elements w such that $w \geq \overline{z}$ (namely all the complements of those y's). Therefore Ω_f is atomic based on $\overline{z}$. □

{example:digraph}

Example 10. *Here is an example of a monotone function whose least support vectors are given by*

$$\Gamma = \{(1,0,0,0),(0,1,1,0),(0,1,0,1),(0,0,1,1)\} \subset GF(2)^n.$$

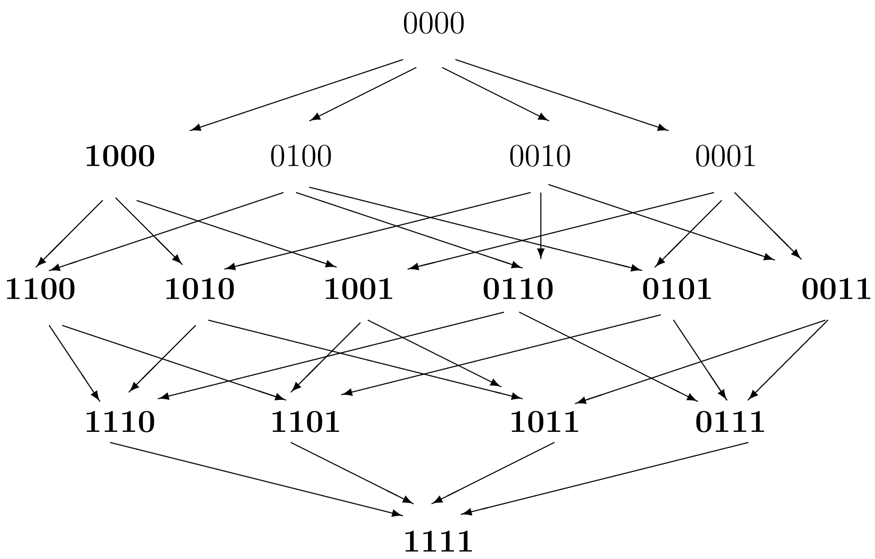

Figure 3: **Bold font** means the Boolean function takes the value 1 at that point in $GF(2)^4$. Regular font means the function is 0. This is another way of drawing the Hasse diagram for the four-dimensional unit hypercube.

This example has the property that the function $f(x_0, x_1, x_2, x_3)$ is even (i.e., the support Ω_f has an even number of elements), yet the subfunctions $f(x_0, 0, x_1, x_2)$, $f(x_0, x_1, 0, x_2)$, $f(x_0, x_1, x_2, 0)$ are all odd, but $f(0, x_0, x_1, x_2)$ is even.

Here is a compact algebraic form that these monotone functions must take. We use the multinomial notation $x^v = x_1^{v_1} x_2^{v_2} ... x_n^{v_n}$.

DP: I stopped editing here (outside of moving Caroline's example to this section) as I was not sure what x^v is when x is a vector. Is this defined somewhere? CGM: added explanation of x^v 6/6/12

{theorem:compact-a

Theorem 11. *Let f be a monotone function whose least support vectors are given by $\Gamma \subset GF(2)^n$. Then*

$$f(x) = 1 + \prod_{v \in \Gamma} (x^v + 1).$$

Proof. For $y \in GF(2)^n$, let

$$g(y) = 1 + \prod_{v\in\Gamma}(x^v + 1).$$

Let

$$S_y = \{v \in \Gamma \mid v \leq y\}.$$

Case 1: $S_y = \emptyset$. In this case, y does not meet the support of f, since f is monotone. Moreover, we have

$$g(y) = 1 + (0+1)\cdot \dots \cdot (0+1) = 0.$$

Therefore, $f(y) = 0 = g(y)$, as desired.
Case 2: $S_y \neq \emptyset$. Let $m = |S_y|$. In this case, there are 2^m terms in $\prod_{v\in S_y}(y^v + 1)$, all of which are non-zero. Therefore, $f(y) = 1 = g(y)$, as desired.
□

Let us regard $f(x) = 1 + \prod_{v\in\Gamma}(x^v + 1)$ as being integer-valued. For all non-zero $y \in GF(2)^n$, the Hadamard transform of f has the following expression:

$$(\mathcal{H}f)(y) = \sum_{x\in\Omega_f}(-1)^{y\cdot x} = \sum_{\substack{x \\ \text{supp}(v)\subseteq \text{supp}(x) \\ \text{some } v\in\Gamma}}(-1)^{y\cdot x}.$$

This last expression for the Hadamard transform may help answer the following question: For which monotone functions (if any) is the graph X singular?

CGM: I don't understand the above, starting with Let us regard ... ending with Hadamard transform. 1. The expression for $\mathcal{H}f$ doesn't agree with our new definition. 2. I don't see how Theorem 10 is being used. 3. I think we want to look at λ_k instead of $\mathcal{H}f(k)$. 4. I don't see how y nonzero is being used. I propose the following. 6/6/12

The kth element λ_k of the spectrum of the Cayley graph X is given by

$$\begin{aligned}\lambda_k &= \sum_{x\in\Omega_f}(-1)^{b(k)\cdot x} \\ &= \sum_{\substack{x \\ \mathrm{supp}(v)\subseteq\mathrm{supp}(x) \\ \text{some } v\in\Gamma}} (-1)^{b(k)\cdot x}.\end{aligned}$$

This last expression for the elements of the spectrum of X may help answer the following question: For which monotone functions (if any) is the graph X singular? In other words, if f is monotone, we want to characterize when $0 \in \mathrm{Spectrum}(X)$. We can answer this question in some special cases. For example, the following result addresses the special case of atomic monotone functions.

Theorem 12. *Let f be a Boolean atomic monotone function. The associated Cayley graph is singular if and only if ω is even.*

Proof. First, note that if ω is odd then $(\mathcal{H}f)(y) \neq 0$ for all $y \in GF(2)^n$ for parity reasons. (This is true for all Boolean functions f and does not even require f to be monotone.) Therefore, we may assume ω is even.

We must show that, for some $x \in GF(2)^n$, half the vectors in Ω_f are orthogonal to x and half are not. Assume $f = f_v$ is atomic based on v, let $M \subset \{1, 2, \dots, n\}$ denote the support of v and let $m = |M|$. Consider the image of Ω_f under the projection map

$$p = p_M : GF(2)^n \to GF(2)^{n-m},$$

given by puncturing all coordinates indexed by an element of M,

$$p(\Omega_f) \subset GF(2)^{n-m}.$$

Since f is monotone based on v, this subset is actually "everything":

$$p(\Omega_f) = GF(2)^{n-m}.$$

Pick any $x \in GF(2)^n$ whose support CGM: 6/6/12 is not contained in the support of v. This is possible as long as v is not the all-ones vector, $v \neq (1, \dots, 1) \in GF(2)^n$. (The case of $f = f_v$ where $v = (1, \dots, 1) \in GF(2)^n$

cannot arise since we assumed ω is even.) Note $x \in \overline{\Omega_f}$. Since $\overline{\Omega_f}$ is a subspace, by the previous proposition, it is orthogonal to half the vectors in $\overline{\Omega_f}$ and not orthogonal to the other half. Thus, since ω is even, the same orthogonality property holds if we replace $\overline{\Omega_f}$ by Ω_f. □

Recall that a strongly regular graph is a regular graph (V, E) with vertices V and common degree c for which there are also integers d and e such that:

- every two adjacent vertices have d common neighbors,
- every two non-adjacent vertices have e common neighbors.

Proposition 13. *Let $f : GF(2)^n \to GF(2)$ denote a monotone function for which $v \in \Omega_f$ implies $\mathrm{wt}(v) > n/2$. Then f is not bent.*

Proof. Suppose not. Let Γ denote the Cayley graph of f, so (since we are assuming f is bent) Γ is strongly regular having parameters d, e with $d = e$ (where d, e denote the number of common neighbors in the adjacent, non-adjacent cases). For any vertex v in Γ, let $N(v)$ denote the neighbors (i.e., adjacent vertices) of v. Strongly regular implies that the cardinality

$$|N(v) \cap N(0)|$$

is independent of which vertex $v \in \Gamma$ we select. (Here 0 denotes the vertex $0 \in GF(2)^n$.) Let $v \in \Omega_f$ be a vector having lowest weight and let $j = (1, \ldots, 1) \in GF(2)^n$. Then

$$|N(v) \cap N(0)| = |N(j) \cap N(0)| = |\overline{\Omega_f} \cap \Omega_f| = 0.$$

This implies $d = e = 0$, which is a contradiction (this equality, in turn, implies $\Omega_f = \emptyset$ by page 2 in Stanica [Sta07]). □

Let f be any even monotone function of 4 variables. By an exhaustive search using Sage, it can be verified that such an f has the property that there is some Walsh coefficient that is zero. CGM: We have not defined Walsh coefficient and I haven't found a good definition on the internet. I suggest just calling this an element of the spectrum. 6/6/12 In other words, its Cayley graph is singular in the sense that it has 0 as an eigenvalue. In particular, such a monotone function cannot be bent.

This suggests two questions:

- Is it true that for every even monotone function, the associated Cayley graph X is singular?
- Is it true that no even monotone function is bent?

The answer to the first question is no. In fact, Example 15 below gives a counterexample in dimension 6. The second question is, as far as we know, open.

4 Derived Boolean functions

Let f be a monotone Boolean function on $GF(2)^n$. We define a new "derived" Boolean function F on $GF(2)^r$ as follows. Let $v_1, \dots , v_r$ be the least supports of f. Let A_i be the atomic set generated by v_i, i.e., A_i consists of all vectors v in $GF(2)^r$ such that $v \geq v_i$. For $x \neq (0, 0, ..., 0)$ in $GF(2)^r$, let A_x be the intersection of all A_i such that i is in the support of x. For example, if $x = (1, 1, 0, ..., 0)$, then $A_x = A_1 \cap A_2$. If $x = (0, 0, ..., 0)$, A_x is is defined to be all of $GF(2)^r$. Now we define $F(x) = 0$ if $|A_x|$ is even and $F(x) = 1$ if $|A_x|$ is odd.

Notice that $|A_x|$ is always a power of 2, so $F(x) = 1$ if and only if $|A_x| = 1$, i.e., if and only if the set A_x consists of the vector of all 1's. If $|A_x| = 1$ then $A_y = 1$ for any $y \geq x$ since by definition, $(1, 1, ..., 1) \in A_y \subset A_x$. Therefore the derived function F is also a monotone Boolean function. Note that F may be identically 0, even though we have assumed that f is not.

Example 14. *If F is the zero function then the adjacency matrix of f has 0 as an eigenvalue. To see this, we first note that each intersection of atomic sets is atomic (as a corollary of Proposition 9). (In fact, if A is atomic based on v and B is atomic based on w, then $A \cap B$ is atomic based on u, where the support of u is the union of the supports of v and w.) Also, each atomic set with more than one element has an equal number of vectors of even and odd weights. For any set S of vectors in $GF(2)^r$, let S^- be the vectors in S with odd weight and let S^+ be the set of vectors in S with even weight. Then $|A_x^+| = |A_x^-|$ for all x if F is the zero function. The support of f is $\Omega_f = \cup_i A_i$. Using the formula for the cardinality of a union of sets,*

$$\begin{aligned}|A_1^+ \cup A_2^+ \cup ... \cup A_r^+| &= \sum_{i=1}^{r} |A_i^+| - \sum_{i \neq j} |A_i^+ \cap A_j^+| \\ &+ \sum_{i,j,k \text{ distinct}} |A_i^+ \cap A_j^+ \cap A_k^+| - \\ &\cdots + (-1)^{r-1}|A_1^+ \cap A_2^+ \cap ... \cap A_r^+| \\ &= |A_1^- \cup A_2^- \cup ... \cup A_r^-|\end{aligned}$$

so that the number of even and odd weight vectors in $\Omega_f = \cup_i A_i$ must be equal if F is the zero function. Note that the vectors in Ω_f which are orthogonal to $(1, 1, ..., 1)$ are exactly the even weight vectors. Now we apply the criterion of section 2 with $m = 0$ and $x = (1, 1, ..., 1)$. This tells us that 0 belongs to the spectrum of the graph of f because the number of vectors in Ω_f which are orthogonal to $(1, 1, ..., 1)$ is $\omega/2$.

Note that this construction can be generalized to any finite collection of nonempty sets A_i in $GF(2)^n$ by taking $F(x) = |\Omega \cap A_x| \bmod 2$, but the resulting Boolean function F is not necessarily monotone. For example, if A_i consists of all vectors whose ith component is 0, then the value of F on the vector e_i whose ith component is 1 and whose other components are 0 tells us whether the subfunction $f|_{x_i=0}$ is even or odd.

Constructing a function $g : GF(2)^r \to \mathbb{Z}$ with $g(x) = |A_x|$ (i.e., the actual cardinality, not the cardinality mod 2) provides some useful counting arguments, as shown below, which can help rule out certain integers as eigenvalues of the spectrum of the Cayley graph of f.

Consider an atomic set A based on a vector v. If x is a vector in $GF(2)^n$ with support contained in the support of v, then $x \cdot y = x \cdot v$ for all $y \in A$. Otherwise, if the support of x is not contained in the support of v, x is orthogonal to exactly half the vectors in A. Using this fact we can construct, by some simple counting arguments, examples of monotone Boolean functions whose Cayley graphs cannot have 0 in their spectra.

For example, suppose that f is a monotone Boolean function on $GF(2)^n$ such that the least support of f consists of vectors v_1, v_2, and v_3 with $|A_1| = |A_2| = |A_3| = 4$ and $|A_i \cap A_j| = 1$ for $i \neq j$. Then $|\Omega_f| = 10$. Let $\mathbf{1} = (\mathbf{1}, \mathbf{1}, ..., \mathbf{1})$. For any x in $GF(2)^n$, the number of vectors y in A_i such that $x \cdot y = x \cdot 1$ is either 2 or 4. Therefore the total number of vectors y in $\Omega_f = A_1 \cup A_2 \cup A_3$ such that $x \cdot y = x \cdot 1$ is one of 4, 6, 8, or 10. This means that the number of vectors in Ω_f which are orthogonal to x cannot be $\omega/2 = 5$ for any x in $GF(2)^n$. Therefore the Cayley graph of f cannot have 0 in its spectrum.

We show now in Example 15 an explicit construction of an even, monotone boolean function for which 0 is not an eigenvalue.

{ex:caroline}

Example 15. *Let $n = 6$ and CGM: 6/6/12 let f be the monotone function whose set of vectors of least support is*

$$\Gamma = \{(1, 1, 1, 1, 0, 0), (1, 1, 0, 0, 1, 1), (0, 0, 1, 1, 1, 1)\}.$$

Using Theorem 11, we obtain the compact algebraic form

$$f(x_0, x_1, x_2, x_3, x_4, x_5) = x_0x_1x_2x_3 + x_0x_1x_4x_5 + x_2x_3x_4x_5.$$

This function is monotone yet has no vanishing Walsh coefficients. CGM: Same comment as above - haven't defined Walsh coefficient. 6/6/12/ As with the previous examples, we attach the file `afsr.sage` *available from Celerier [Cel], then run the following commands.*

Sage

```
sage: V = GF(2)^(6)
sage: L = [V([1,1,0,0,1,1]),V([0,0,1,1,1,1]), V([1,1,1,1,0,0])]
sage: f = monotone_from_support(L)
sage: is_monotone(f)
True
```

These commands simply construct a Bolean function f whose least support are the vectors in `L`*. Next, we compute the Hadamard transform of this using both the method built into Sage's* `sage.crypto` *module, and the function in* `afsr.sage`*.*

Sage

```
sage: f.walsh_hadamard_transform()
(-44, -12, -12, 12, -12, 4, 4, -4, -12, 4, 4, -4, 12, -4, -4, 4, -12, 4, 4, -4, 4, 4, 4, -4,
4, 4, 4, -4, -4, -4, -4, 4, -12, 4, 4, -4, 4, 4, 4, -4, 4, 4, 4, -4, -4, -4, -4, 4, 12,
-4, -4, 4, -4, -4, -4, 4, -4, -4, -4, 4, 4, 4, 4, -4)
sage: f.algebraic_normal_form()
x0*x1*x2*x3 + x0*x1*x4*x5 + x2*x3*x4*x5
sage: x0,x1,x2,x3,x4,x5 = var("x0,x1,x2,x3,x4,x5")
sage: g = x0*x1*x2*x3 + x0*x1*x4*x5 + x2*x3*x4*x5
sage: Omega = [v for v in V if g(x0=v[0], x1=v[1], x2=v[2], x3=v[3], x4=v[4], x5=v[5])<>0]
sage: len(Omega)
10
sage: g = lambda x: x[0]*x[1]*x[2]*x[3] + x[0]*x[1]*x[4]*x[5] + x[2]*x[3]*x[4]*x[5]
sage: [walsh_transform(g,a) for a in V]
[44, 12, 12, -12, 12, -4, -4, 4, 12, -4, -4, 4, -12, 4, 4, -4, 12, -4,-4, 4, -4, -4, -4, 4,
-4, -4, -4, 4, 4, 4, 4, -4, 12, -4, -4, 4, -4, -4, -4, 4, -4, -4, -4, 4, 4, 4, 4, -4, -12,
4, 4, -4, 4, 4, 4, -4, 4, 4, 4, -4, -4, -4, -4, 4]
```

(Note: the Walsh transform method in the `BooleanFunction` *class in Sage is off by a sign from the standard definition.) This verifies that there are no values of the Walsh transform which are* 0. *CGM: Haven't said what Walsh transform is. Need to relate these to elements of the spectrum. 6/6/12*

References

[BC99] A. Bernasconi and B. Codenotti. Spectral analysis of Boolean functions as a graph eigenvalue problem. *Computers, IEEE Transactions on*, 48(3):345–351, 1999.

[BZ10] D. Bienstock and M. Zuckerberg. Solving lp relaxations of large-scale precedence constrained problems. *Integer Programming and Combinatorial Optimization*, pages 1–14, 2010.

[Cel] C. Celerier. github repository. `https://github.com/celerier/oslo/`.

[Cel12] C. Celerier. Feedback with carry shift-registers and bent functions, 2012. USNA Honors Thesis.

[HC00] D.S. Hochbaum and A. Chen. Performance analysis and best implementations of old and new algorithms for the open-pit mining problem. *Operations Research*, pages 894–914, 2000.

[Joh68] T.B. Johnson. Optimum open pit mine production scheduling. Technical report, DTIC Document, 1968.

[Kle69] D. Kleitman. On Dedekind's problem: the number of monotone Boolean functions. In *Proc. Amer. Math. Soc*, volume 21, pages 677–682, 1969.

[Orl87] D. Orlin. Optimal weapons allocation against layered defenses. *Naval Research Logistics (NRL)*, 34(5):605–617, 1987.

[Rhy70] JMW Rhys. A selection problem of shared fixed costs and network flows. *Management Science*, pages 200–207, 1970.

[Sta07] P. Stanica. Graph eigenvalues and Walsh spectrum of Boolean functions. *Integers: Electronic Journal Of Combinatorial Number Theory*, 7(2):A32, 2007.