A generalisation of bent vectors for Butson Hadamard matrices

Ronan Egan
Dublin City University

Joint work with:

- José Andrés Armario - Universidad de Sevilla
- Hadi Kharaghani - University of Lethbridge
- Padraig Ó Catháin - Dublin City University

Hadamard matrices

Theorem (Hadamard, 1893)

An $n \times n$ matrix H with complex entries of modulus no greater than 1 satisfies

$$|\det(H)| \leq n^{n/2}.$$

A matrix attaining this bound is a (complex) ***Hadamard matrix***.

If the entries of H are restricted to the k^{th} roots of unity for some integer k, then H is called a ***Butson*** matrix, and the set of such matrices is denoted $\mathrm{BH}(n, k)$.

The orthogonality property can be expressed by the matrix equation

$$HH^* = nI_n.$$

The eigenvalues of $\frac{1}{\sqrt{n}}H$ all have norm 1.

Typically, even if the entries of H are, these eigenvalues are not roots of unity.

Similarly, the eigenvectors need not have root of unity entries (or entries of equal norm), but it is possible, and there are multiple applications of such vectors.

Definition

Let $H \in \mathrm{BH}(n,k)$, and let $\mathbf{x}$ be a vector of length n with entries in $\langle \zeta_k \rangle$. We say that $\mathbf{x}$ is H-***bent*** if and only if

$$H\mathbf{x} = \sqrt{n}\mathbf{y}\,,$$

where all entries of $\mathbf{y}$ are complex numbers of norm 1.

Further, $\mathbf{x}$ is ***self-dual*** H-***bent*** if $\mathbf{y} = \mathbf{x}$ and ***conjugate self-dual*** if $\mathbf{y} = \overline{\mathbf{x}}$.

Aside: Another generalization of this self-dual property relates the entries of $\mathbf{y}$ to the entries of $\mathbf{x}$ by a Galois automorphism $z \mapsto z^\ell$ for some ℓ coprime to k, this is work done with some other authors.

Some motivation

It has been shown that there exist Butson-Hadamard matrices which admit ***conjugate*** self-dual bent vectors but ***do not*** admit self-dual bent vectors.

We can explicitly construct large families of matrices admitting conjugate self-dual bent vectors, and the vectors themselves.

Existence conditions stemming from algebraic number theory relate to different problems.

We present an application of conjugate self-dual bent vectors to the covering radius of certain non-linear codes generalising the Reed Muller codes.

Some notation and definitions

$\zeta_k = e^{\frac{2\pi i}{k}}$ will always denote a primitive k^{th} root of unity and $\langle \zeta_k \rangle$ the set of all k^{th} roots.

$F(C_n) = [\zeta_n^{ij}]_{0 \leq i,j \leq n-1} \in \mathrm{BH}(n, n)$ is $n \times n$ Fourier matrix.

The character tables of elementary abelian groups of odd order, $F(C_p^m) = \otimes^m F(C_p)$ are sometimes called ***generalised Sylvester matrices***.

A function $f : C_k^m \to C_k$ is naturally identified with the vector $\mathbf{x} = [\zeta_k^{f(a)}]_{a \in C_k^m}^\top$.

An example [Kumar, Scholtz, Welch '85]

Let k be an integer and $m = 2t$ be an even integer. Define $f : \mathbb{Z}_k^m \to \mathbb{Z}_k$ by

$$f(x_1, \ldots, x_{2t}) = x_1 x_{t+1} + \ldots + x_t x_{2t} \,.$$

Let $\mathbf{x}$ be the C_k^m-indexed vector with $x_c = \zeta_k^{f(c)}$. Then $F(C_k^m)\mathbf{x} = k^{m/2}\overline{\mathbf{x}}$. In other words, $\mathbf{x}$ is conjugate self-dual $F(C_k^m)$-bent.

Nonexistence when $k = 3$

Proposition

Suppose that $H \in \mathrm{BH}(n, 3)$ and that $\mathbf{x}$ is H-bent. If there exists an index i such that $(H\mathbf{x})_i \in \sqrt{n}\langle\zeta_3\rangle$ then $n = 9m^2$ for integer m.

Proof sketch: By hypothesis $(H\mathbf{x})_i$ has the form

$$s_0 + s_1\zeta_3 + s_2\zeta_3^2 = \sqrt{n}\,\zeta_3^j$$

where $s_0 + s_1 + s_2 = n$ and $j \in 0, 1, 2$.

Use that $\zeta_3 + \zeta_3^2 = -1$, and rearrange to

$$(s_1 - s_0)\zeta_3 + (s_2 - s_0)\zeta_3^2 = \sqrt{n}\,\zeta_3^j\,.$$

Determine that the solutions are $s_0 = \dfrac{n \pm \sqrt{n}}{3}$. □

Algebraic number theory

The elements of the ring

$$\mathbb{Z}[\zeta_k] = \left\{ \sum_{j=0}^{k-1} b_j \zeta_k^j : \ b_j \in \mathbb{Z} \right\}$$

are called ***cyclotomic integers***.

Every proper ideal of $\mathbb{Z}[\zeta_k]$ can be uniquely factorized into a product of finitely many prime ideals. The principal ideal of $\mathbb{Z}[\zeta_k]$ generated by $a \in \mathbb{Z}[\zeta_k]$ is denoted by $a\mathbb{Z}[\zeta_k]$.

A prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\zeta_k]$ appears in the factorization of $a\mathbb{Z}[\zeta_k]$ if and only if $a \in \mathfrak{p}$.

We say that p is ***ramified*** in $\mathbb{Z}[\zeta_k]$ if a proper power of a prime ideal divides $p\mathbb{Z}[\zeta_k]$, and unramified otherwise.

Algebraic number theory

For any composite number $k = p^r m$ with m coprime to p, we let $k_p = p^r$ be the p-part of k.

Definition

The prime p is ***self-conjugate*** modulo k if and only if there exists an integer j such that $p^j \equiv -1 \mod k/k_p$. More generally, for integers n and k, we say that n is *self-conjugate* modulo k if all prime divisors p of n are self-conjugate modulo k/k_p.

Algebraic number theory

Theorem (Ireland, Rosen)

Let p be a rational prime, and let ϕ be the Euler totient function. Let f be the least positive integer such that $p^f \equiv 1 \mod (k/k_p)$ and define g by $fg = \phi(k/k_p)$. The factorisation of p in $\mathbb{Z}[\zeta_k]$ is as follows:

$$p\mathbb{Z}[\zeta_k] = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^{\phi(k_p)}$$

where the $\mathfrak{p}_i$ are distinct prime ideals of $\mathbb{Z}[\zeta_k]$. In particular, an odd prime p is ramified in $\mathbb{Z}[\zeta_k]$ precisely when $p \mid k$, and 2 is ramified when $4 \mid k$.

Algebraic number theory

Theorem (Beth, Jungnickle, Lens)

Let $\mathfrak{p}$ be a prime ideal over the rational prime p, and let $m = k/k_p$ for integer k. A field automorphism $\sigma \in Gal_k$ fixes $\mathfrak{p}$ if and only if $\sigma(\zeta_m) = \zeta_m^{p^j}$ for some integer j. In particular, $\mathfrak{p}$ is fixed by complex conjugation if and only if $\sigma^*(\zeta_m) = \zeta_m^{p^j}$ for some integer j.

An example using these tools

Consider the ideal $5\mathbb{Z}[\zeta_{13}]$, which is unramified and a product of three prime ideals by IR, each fixed by complex conjugation by BJL since $5^2 \equiv -1 \mod 13$. Let $\mathfrak{p}$ be a prime ideal dividing $5\mathbb{Z}[\zeta_{13}]$.

In the norm equation $xx^* = 5^{2t+1}$, the right hand side is divisible by an odd power of $\mathfrak{p} \mid 5$, while the left side must be divisible by an even power.

Hence no such x exists. One concludes that there are no matrix solutions of $MM^* = 5I_n$ with entries in $\mathbb{Z}[\zeta_{13}]$.

More generally...

Suppose that p is self-conjugate modulo k, that p divides n and that there exists $H \in \mathrm{BH}(n,k)$. Let $\mathfrak{p}_i$ be the prime ideals above p fixed by complex conjugation, where $1 \leq i \leq g$.

Denote by x the determinant of H. Then $xx^* = n^n$. Since $\mathfrak{p}_i$ is a prime ideal which divides n, it divides one of x and x^*. But if $\mathfrak{p}$ divides x then $\mathfrak{p}^*$ divides x^* and since $\mathfrak{p}_i^* = \mathfrak{p}_i$ we conclude that $\mathfrak{p}_i^2$ divides n. Since the conclusion holds for every $\mathfrak{p}_i$, it follows that p divides n^n to an even power.

Theorem

Suppose that k is an integer, that $\mathbf{x}$ is H-bent for $H \in \mathrm{BH}(n,k)$. If $k_p = 1$, and $n_p > 1$ and p is self-conjugate modulo k then n_p is a square.

Take the prime ideal factorisation of both side of $(H\mathbf{x})_j(H\mathbf{x})_j^* = n$. The rest is similar.

Corollary

Suppose that $k \equiv 2 \mod 4$ and that $\mathbf{x}$ is H-bent for $H \in \mathrm{BH}(n,k)$. If 2 is self-conjugate modulo k then n_2 is a square.

Theorem

Let $H \in \mathrm{BH}(n,k)$ and let $\mathbf{x}$ be H-bent with entries in $\langle \zeta_k \rangle$, and let $\mathbf{y} = \frac{1}{\sqrt{n}} H\mathbf{x}$. If n is self-conjugate modulo k, then every entry of $\mathbf{y}$ belongs to $\langle \zeta_{2k} \rangle$ if k is even and $\langle \zeta_{4k} \rangle$ if k is odd.

$$y_i y_i^* = \left(\sum_{j=1}^{n} h_{ij} x_j \right) \sigma^* \left(\sum_{j=1}^{n} h_{ij} x_j \right) = n.$$

We have the following equality of ideals:

$$y_i^2 \mathbb{Z}[\zeta_k] = n\mathbb{Z}[\zeta_k]\,.$$

Two principal ideals are equal if and only if they differ by a unit. The only units in $\mathbb{Z}[\zeta_k]$ are roots of unity and hence $y_i^2 \zeta_k^j = n$ for some j.

It follows that $\sqrt{y_i^2/n} = \pm\zeta_{2k}^j$ is also a root of unity, since its square is $\pm\zeta_k^j$.

A slight detour

Theorem

Suppose that $\mathbf{x}$ *is* $F(C_n)$*-bent. Then* $H = [\boldsymbol{x}_{i-j}]_{0 \le i,j \le n-1}$ *is a circulant Hadamard matrix, where indices are interpreted modulo* n*.*

Corollary

There does not exist a real circulant Hadamard matrix of order $n = 4p^2$ *for any prime* $p \equiv 3 \mod 8$*.*

Proof sketch

Observe that $4p^2$ is self-conjugate modulo $4p^2$.

An eigenvalue $\lambda = (H\mathbf{x})_1$, where $\mathbf{x}$ is any column of $F(C_n)$ is $2p$ times a root of unity.

If all of the eigenvalues are roots of unity, then there exists a positive integer m such that $\left(\frac{H}{2p}\right)^m = I_n$, contradicting a result of Craigen and Kharaghani.

Constructions

Lemma

If $\mathbf{x}$ *and* $\mathbf{y}$ *are conjugate self-dual* H*-bent and* K*-bent respectively, for* $H \in \mathrm{BH}(n,k)$ *and* $K \in \mathrm{BH}(m,k)$*, then* $\mathbf{x} \otimes \mathbf{y}$ *is conjugate self-dual* $(H \otimes K)$*-bent.*

Define Φ to be the vectorisation map, i.e. $\Phi(H) = \mathbf{x}$ with $x_{(i-1)n+j} = h_{i,j}$.

Proposition

Let A, B, M be $n \times n$ matrices. Then $(A \otimes B)^* \Phi(M) = \Phi(A^* \ M \ \overline{B})$.

Corollary

1. *If H is Hadamard then the vector $\Phi(H)$ is conjugate self-dual $(H^* \otimes H^*)$-bent.*
2. *If H and M are commuting Hadamard matrices then $\Phi(M)$ is self-dual $(H \otimes \overline{H})$-bent.*
3. *If H and M are amicable Hadamard matrices, that is $HM^* = MH^*$, then $\Phi(M)$ is conjugate self-dual $(H \otimes H^\top)$-bent if M is symmetric.*

Building with Bush matrices

Definition (Bush, 71)

A matrix $H \in \mathrm{BH}(n^2, k)$ is of ***Bush-type*** if it may be subdivided into $n \times n$ blocks H_{ij} such that $JH_{ij} = H_{ij}J = \delta_{i,j} nJ$, for all $1 \leq i, j \leq n$, where J is the $n \times n$ matrix of all ones.

Proposition

If $H \in \mathrm{BH}(4m^2, 4)$ is of Bush-type, then there are at least 2^{2m} self-dual H-bent vectors, and at least 2^{2m} conjugate self-dual $(-H)$-bent vectors.

Let $\mathbf{1}$ be the all-one vector of length $2m$, and let $u_k \in \{\pm\zeta_4\}$ be arbitrary. Any vector $\mathbf{x}^\top = (u_1\mathbf{1}, \ldots, u_{2m}\mathbf{1})$, is both self-dual H-bent and conjugate self-dual $(-H)$-bent.

Building with Bush matrices

Proposition

Let k be odd and let H be a Bush-type $\mathrm{BH}(n^2, k)$, then there exist k^n matrices in $\mathrm{BH}(n^2, k)$, each admitting a self-dual and a conjugate self-dual bent vector.

Let $H = [H_{ij}]$ and

$$H' = [H'_{ij}] = \begin{cases} H_{ij} & i \neq j \\ \zeta_k^{u_i} H_{ij} & i = j, \end{cases}$$

where $u_i \in \mathbb{Z}_k$ for each i. Then H' is a $\mathrm{BH}(n^2, k)$ and the vector $\mathbf{x}$ defined by $\mathbf{x}^\top = (\zeta_k^{u_1\alpha}\mathbf{1}, \ldots, \zeta_k^{u_n\alpha}\mathbf{1})$ is self-dual H'-bent when $\alpha = \frac{k+1}{2}$, and is conjugate self-dual H'-bent when $\alpha = \frac{k-1}{2}$.

Conjugate self-bent vectors

We want to construct pairs of matrices M and N such that $MN = p\overline{N}$ in dimension p^2 for an odd prime p.

Lemma

Denote by r_a the a^{th} row of $F(C_p)$ for $0 \leq a \leq p-1$, and let $R_a = r_a^* r_a$ be the outer product. The following hold:

1. *Rank 1 projectors: R_a is rank 1, and satisfies $R_a^2 = pR_a$ for $0 \leq a \leq p-1$.*
2. *Hermitian: $R_a^* = R_a$, for each a. Furthermore, $R_a^\top = R_{p-a}$.*
3. *Orthogonal: $R_a R_b = 0$, $a \neq b$.*
4. *Basis: $\sum_0^{p-1} R_a^2 = p^2 I_p$.*

Proposition

Let B_a be the block-circulant matrix having $[R_0, R_a, R_{2a}, \ldots, R_{(p-1)a}]$ as its first row, with indices interpreted modulo p. For $a = 1, 2, \ldots, p-1$, the matrix B_a is a symmetric Bush-type Butson Hadamard matrix $\mathrm{BH}(p^2, p)$. Furthermore, $\overline{B_a} = B_{p-a}$ and $B_a B_{(p-2)a} = pB_{2a} = p\overline{B}_{(p-2)a}$.

As a consequence, for any prime $p \geq 3$ and any choice of $a \in \{1, \ldots, p-1\}$ the columns of $B_{(p-2)a}$ are conjugate self-dual B_a-bent vectors.

An application to codes

The ***covering radius*** of a $\mathbb{Z}_k$-code C of length n is defined by the formula

$$r(C) = \max_{\mathbf{x} \in \mathbb{Z}_k^n} \min_{\mathbf{y} \in C} d(\mathbf{x}, \mathbf{y}).$$

Definition

Let $H \in \mathrm{BH}(n, k)$. We denote by R_H the $\mathbb{Z}_k$-code of length n consisting of the rows of $L(H)$, and we denote by C_H the $\mathbb{Z}_k$-code defined as $C_H = \cup_{\alpha \in \mathbb{Z}_k}(R_H + \alpha \mathbf{1})$. The code C_H over $\mathbb{Z}_k$ is called a ***Butson Hadamard code*** (briefly, BH-code).

The ***nonlinearity*** of a function $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ is the Hamming distance between f and $R_q(1, m)$, the first order generalised Reed-Muller code. Thus the maximal non-linearity of a function $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ is equal to the covering radius of $R_q(1, m)$, this quantity is denoted $\rho_q(m)$.

Theorem (Leducq, 13)

Let $H \in \mathrm{BH}(n, q)$ where q is an odd prime. Then

$$r(C_H) \leq \frac{q-1}{q} n - \frac{1}{q}\sqrt{n}\,.$$

Lemma

Let $\mathbf{v}, \mathbf{w} \in \langle \zeta_3 \rangle^n$. *Then* $d(L(\mathbf{v}), L(\mathbf{w})) = 2/3\Big(n - \mathcal{R}(\langle \mathbf{v}, \mathbf{w} \rangle)\Big)$.

Theorem

Suppose that $H \in BH(n, 3)$ *admits a bent vector. Then*

$$\frac{2}{3}n - \frac{2}{3}\sqrt{n} \leq r(C_H) \leq \frac{2}{3}n - \frac{1}{3}\sqrt{n}.$$

A shameless plug