**An Orthogonality Graph**

Chris Godsil

Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario
Canada N2L 3G1

## 1. An Orthogonality Graph

Let $\Omega(n)$ denote the graph with the $2^n$ $(\pm 1)$-vectors of length $n$ as its vertices, where vectors $x$ and $y$ are adjacent if and only if they are orthogonal. Let $x \circ y$ denote the Schur product of two vectors of the same length. Note that $x^T y = \mathbf{1}^T (x \circ y)$.

The graph $\Omega(n)$ has a comparatively large automorphism group. If $a$, $x$ and $y$ are three vertices in it, then

$$(a \circ x)^T (a \circ y) = \mathbf{1}^T ((a \circ x) \circ (a \circ y)) = \mathbf{1}^T (x \circ y) = x^T y$$

and therefore the map

$$\tau_a : x \mapsto a \circ x, \qquad x \in V(\Omega(n))$$

is an automorphism of $\Omega(n)$. The autmorphisms $\tau_a$ form an abelian group $T$ with exponent two that acts regularly on the vertices of $\Omega(n)$. (Hence this graph is a Cayley graph for $T$.) We will call $T$ the group of *translations* of $\Omega(n)$. If $\sigma \in \mathrm{Sym}(n)$ and $x \in V(\Omega(n)$, define $x^\sigma$ by

$$(x^\sigma)_i = x_{i^\sigma}.$$

Then the map $x \mapsto x^\sigma$ is an automorphism of $\Omega(n)$ that fixes the vector $\mathbf{1}$.

If $x \in V(\Omega(n))$ then $-x \in V(\Omega(n))$ and these two vectors have the same neighbourhood. The neighbourhood of $\mathbf{1}$ consists of the vectors $y$ such that $\mathbf{1}^T y = 0$. It follows that if $n$ is odd then $\Omega(n)$ is the empty graph on $2^n$ vertices.

Our aim now is to study the chromatic number of $\Omega(n)$. We begin by eliminating two easy cases. Suppose $n \cong 2$ (modulo 4). We say that a vertex of $\Omega(n)$ is *even* if the number of negative entries is even, otherwise we call it *odd*. If $x$ is an even vertex then $\mathbf{1}^T x \neq 0$. If $x$ and $y$ are both even or both odd then $x \circ y$ is even, from which we see that the neighbours of an even vertex must all be odd. We conclude that, if $n \cong 2$ (modulo 4), then $\Omega(n)$ is bipartite.

Henceforth we assume that $n$ is divisible by four. A clique in $\Omega(n)$ is an orthogonal set of vectors, and therefore is linearly independent. This implies that $\omega(\Omega(n)) \leq n$. It is immediate that cliques of size $n$ correspond to $n \times n$ $(\pm 1)$-matrices $H$ such that

$$H^T H = nI;$$

$(\pm 1)$-matrices satisfying this condition are known as *Hadamard matrices*. From what we have already seen, such matrices can only exist if $n = 2$ or if four divides $n$. The smallest example is

$$S = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

If $H$ and $K$ are Hadamard matrices then so is their Kronecker product $H \otimes K$. Therefore Hadamard matrices exist whenever $n$ is a power of two.

**1.1 Lemma.** *If $K_n$ is a retract of $\Omega(n)$ then $n$ is a power of two.*

*Proof.* If $K_n$ is a retract of $\Omega(n)$ the $K_n$ must be the core of $\Omega(n)$. Since $\Omega(n)$ is vertex transitive, this implies that $n$ divides $|V(\Omega(n))|$. □

It is believed that that there exist Hadamard matrices of order $n$ whenever is a multiple of four and, as Jones and Sunder remark, the smallest value $n$ for which existence is unknown is "fairly large".

In a deep and important paper, Frankl and Rŏdl have proved that whenever $n$ is a sufficiently large power of two, $\chi(\Omega(n)) > n$. People working in quantum computing wish to know the precise meaning of "sufficiently large". It is easy to verify that $\chi(\Omega(4)) = 4$ and Gordon Royle has verified that $\chi(\Omega(8)) = 8$.

## 2. Eigenvalues

If $X$ is regular, there is a bound on $\alpha(X)$ in terms of the eigenvalues of $X$. This bound does not settle our quantum computational problem, but could conceivably still be useful. So we will determine the eigenvalues of $\Omega(n)$.

This involves some group theory. Let $A$ be an abelian group. A *character* of $A$ is a homomorphism $\varphi$ from $A$ to the non-zero complex numbers. Thus, if $g$ and $h$ belong to $A$ then $\varphi(gh) = \varphi(g)\varphi(h)$. It follows that $\varphi(e) = 1$ and $\varphi(g^{-1}) = \varphi(g)^{-1}$. If $A$ is finite, which is the only case of interest to us, then each element of $A$ has finite order. If $g \in A$ and $g^k = e$ then $\varphi(g)^k = 1$, whence the image of $\varphi$ consists of roots of unity. Further, $\varphi(g^{-1}) = \overline{\varphi(g)}$. The function that takes each element of $A$ to 1 is called the *trivial character* of $A$. If $\varphi$ and $\rho$ are characters of $A$ then their product $\varphi\rho$ is again a character. (Here $\varphi\rho$ maps $g$ in $S$ to $\varphi(g)\rho(g)$.) If $\varphi$ and $\rho$ are characters of $A$ we define

$$\langle \varphi, \rho \rangle := \sum_{g \in A} \overline{\varphi(g)}\rho(g).$$

This is an inner product. It will often be convenient to view a character on $A$ as a vector indexed by the elements of $A$.

**2.1 Lemma.** *If $\varphi$ is a non-trivial character on the finite abelian group $A$, then $\langle \mathbf{1}, \varphi \rangle = 0$.*

*Proof.* Suppose $\varphi$ is non-trivial and that $\varphi(g) \neq 1$. Assume that $g$ has order $k$. If $\varphi(g) = z$ then $z$ is a non-trivial complex $k$-th root of 1. So

$$\sum_{r=0}^{k-1} z^r = 0.$$

Consequently, if $a \in A$, then

$$\sum_{r=0}^{k-1} \varphi(ag^r) = \sum_{r=0}^{k-1} \varphi(a)\varphi(g^r) = \varphi(a) \sum_{r=0}^{k-1} z^r = 0.$$

Therefore the sum of $\varphi$ over a coset of the cyclic subgroup generated by $g$ is zero, and the lemma follows. $\square$

If $T$ is the group of the last section and $S \subseteq \{1, \dots, n\}$, the map $\psi_S$ defined by

$$\psi_S(a) = \prod_{i \in S} a_i$$

is easily shown to be a character of $T$, taking values in $\{-1, 1\}$. This gives us a set of $2^n$ characters of $T$. If $\Delta$ denotes the symmetric difference of subsets, then

$$\psi_R \psi_S = \psi_{R \Delta S}.$$

Therefore $R \neq S$, the characters $\psi_R$ and $\psi_S$ are pairwise orthogonal. Thus we have a set of $2^n$ pairwise orthogonal characters. (In fact, a finite abelian group $G$ always has $|G|$ distinct characters, but we do not stop to prove this.)

**2.2 Theorem.** *Suppose $X$ is a Cayley graph for the abelian group $G$ and $C$ is the connection set of $X$. If $\varphi$ is a character of $G$ then it is an eigenvector of $A(X)$, with eigenvalue $\sum_{g \in C} \varphi(g)$.*

*Proof.* Let $A$ denote the adjacency matrix of $X$. If $g \in V(X) = G$ then

$$\sum_{h \sim g} \varphi(h) = \sum_{c \in C} \varphi(cg) \sum_{c \in C} \varphi(c)\varphi(g) = \varphi(g) \sum_{c \in C} \varphi(c). \qquad \square$$

If $C \subseteq G$, it is convenient to denote $\sum_{g \in C} \varphi(g)$ by $\varphi(C)$. Thus we can paraphrase the theorem by stating that a character $\varphi$ of $G$ is an eigenvector for $X$ with eigenvalue $\varphi(C)$. Note the eigenvectors corresponding to distinct characters are orthogonal (with respect to the Hermitian inner product).

## 3. Eigenvalues of $\Omega(n)$

The graph $\Omega(n)$ is a Cayley graph relative to the group $T$ of translations. The identity element of $T$ is the vector $\mathbf{1}$, and the connection set $C$ is the set of $(\pm 1)$-vectors orthogonal to $\mathbf{1}$. If $S \subseteq \{1, \dots, n\}$ then

$$\psi_S(C) = \sum_{A \subseteq \{1, \dots, n\},\ |A| = n/2} (-1)^{|S \cap A|}.$$

Assume $n = 2m$. If $S = \emptyset$ then $\psi_S$ has eigenvalue $\binom{2m}{m}$, as expected.

Now suppose that $|S| = 1$. Then we can partition the above sum into the sets $A$ that contain $S$, and those that do not. In this case the eigenvalue of $\psi(S)$ is

$$\binom{2m-1}{m} - \binom{2m-1}{m-1} = 0.$$

Continuing in this vein, we find that if $|S| = r$ then the eigenvalue of $\psi_S$ is

$$\sum_{i=0}^{r} (-1)^i \binom{r}{i} \binom{2m-r}{m-i}.$$

It is not hard to verify that this is zero if $r$ is odd. The following is true though:

**3.1 Theorem.** *Suppose $n = 2m$. If $i \in \{1, \dots, n\}$ then*

$$\frac{2^m}{m!}(i-1)(i-3)\cdots(i-2m+1)$$

*is an eigenvalue of $\Omega(n)$.* □

Denote the value of the eigenvalue associated with $i$ by $\lambda_i$. We can also give the multiplicities of the eigenvalues. Observe that if $i$ is odd, then $\lambda_i = 0$. The multiplicity of zero is $2^{n-1}$.

If $n \cong 2 \pmod 4$ then $\lambda_i$ takes distinct values on distinct even integers, and the multiplicity of $\lambda_i$ is $\binom{n}{i}$. (We have $\lambda_{n-2j} = (-1)^j \lambda_{2j}$.)

If $n$ is divisible by 4, then $\lambda_{n-2j} = \lambda_{2j}$. If $2j < n/2$ then $\lambda_{2j}$ has multiplicity $2\binom{n}{2j}$, while $\lambda_{n/2}$ has multiplicity $\binom{n}{n/2}$.

We recall the following.

**3.2 Lemma.** *Let $X$ be a regular graph on $n$ vertices with valency $k$ and least eigenvalue $\tau$. Then*

$$\alpha(X) \leq \frac{n(-\tau)}{k-\tau}.$$

In terms of Theorem 3.1, the valency $k$ of $\Omega(n)$ is $\lambda_0$, and its least eigenvalue $\tau$ is $\lambda_2$. We have

$$\frac{k}{-\tau} = -\frac{1 \cdots 3 \cdot 2m-1}{(-1)1 \cdot 3 \dots 2m-3} = 2m-1.$$

Therefore if $n$ is divisible by 4, then

$$\alpha(\Omega(n)) \leq \frac{2^n}{n}$$

and consequently

$$\chi(\Omega(n)) \geq n.$$

If equality holds then $n$ must divide $2^n$, as we have already seen.