Derangements and Quantum Colourings

Chris Godsil
Combinatorics & Optimization
University of Waterloo

October 14, 2019

1 Introduction

These notes are meant to accompany a talk “Derangements and Quantum Colourings”. They are largely based on the following sources:


2 Colourings

A graph homomorphism from $X$ to $Y$ is a map $\varphi : V(X) \rightarrow V(Y)$ such that if $u$ and $v$ are adjacent in $X$, then $\varphi(u)$ and $\varphi(v)$ are adjacent in $Y$. We write

*Research supported by Natural Sciences and Engineering Council of Canada, Grant No. RGPIN-9439
$X \rightarrow Y$ to denote that there is a homomorphism from $X$ to $Y$. The most familiar examples are colourings: an $m$-colouring of $X$ is a homomorphism from $X$ to $K_m$. For a second class of examples, any automorphism of $X$ is a homomorphism from $X$ to itself.

We note that if $X \rightarrow Y$, then $\chi(X) \leq \chi(Y)$.

If $\varphi : X \rightarrow Y$ is a homomorphism and $y \in V(Y)$, the set

$$\varphi^{-1} := \{ x \in V(X) : \varphi(x) = y \}$$

is the fibre of $\varphi$ at $y$. Since all graphs we consider are free of loops, and fibre of a homomorphism from $X$ to $Y$ is a coclique in $X$. It follows that an $m$-colouring of $X$ determines a partition of $V(X)$ with exactly $m$ cells (where each cell is a coclique).

We choose to represent a partition $\pi$ by a characteristic matrix, this is the 01-matrix with $i$-th column equal to the characteristic vector of the $i$-th cell of $\pi$. If $M$ is the characteristic matrix of a partition, then the columns of $M$ sum to 1. If $M$ is the characteristic matrix of a colouring, each column is the characteristic vector of a coclique.

A quantum $m$-colouring of a graph $X$ is a $|V(X)| \times m$ matrix with $d \times d$ projections as entries, such that

(a) If $u \in V(X)$, then $\sum_{i=1}^{m} M_{u,i} = I_d$.

(b) If $uv \in E(X)$, then $M_{u,i}M_{v,i} = 0$ for $i = 1, \ldots, m$.

You may verify that, if $d = 1$, this is just a classical $m$-colouring. The least integer $m$ such that $X$ admits a quantum $m$-colouring is the quantum chromatic number of $X$, denoted $\chi_q(X)$. (Note that $d$ is allowed to vary.)

We have

$$\chi_q(X) \leq \chi(X).$$

It is an interesting exercise to verify that $\chi_q(X) = 2$ if and only if $\chi(X) = 2$.

2.1 Theorem. If $X$ admits a quantum $m$-colouring, then it admits a quantum $m$-colouring where all projections have the same rank. 

If the common rank is $r$, then $mr = d$.

Using the previous theorem, it is not too difficult to prove that $\chi_q(K_n) = n$. 

2
3 Orthogonality Graphs

Suppose $S$ is a subset of an inner product space, e.g., the unit vectors in $\mathbb{C}^d$. The orthogonality graph based on $S$ have vertex set $S$, and two elements of $S$ are adjacent if they are orthogonal. If the inner product space has dimension $d$, then cliques of size $d$ are orthogonal bases and the clique number of the graph is $d$. We use $S(d)$ to denote the orthogonality graphs formed from the unit vectors in $\mathbb{C}^d$. A complex vector or matrix is flat if all its entries have the same absolute value. We use $S^\flat(d)$ to denote the subgraph of $S(d)$ induced by the flat vectors. The cliques in $S^\flat(d)$ correspond to flat $d \times d$ matrices; the character table of an abelian group of order $d$ is flat and unitary (so $\omega(S^\flat(d)) = d$).

We use $S_\mathbb{R}(d)$ and $S_\mathbb{R}^\flat(d)$ to denote the real analogs of $S(d)$ and $S^\flat(d)$ (note that the latter graph is finite). These real graphs are induced subgraphs of the complex versions.

If $M$ is the characteristic matrix of an $m$-colouring of $X$, then two rows of $M$ indexed by adjacent vertices are orthogonal. This the map that sends a vertex $u$ to $e_u^T M$ is a homomorphism from $X$ to $S(m)$. If define the orthogonal rank $\xi(X)$ of $X$ to be the least integer $k$ such that there is a homomorphism from $X$ to $S(k)$. We have $\xi(X) \leq \chi(X)$.

3.1 Theorem (Gleason). If $d \geq 3$, then $\chi(S_\mathbb{R}(d)) > d$. \hfill \Box

The surprising thing about Gleason’s theorem is that is a simple consequence of an important result clarifying the nature of quantum measurements.

3.2 Theorem. Assume $n = 2^k$. We have $\omega(S_\mathbb{R}^\flat(n)) = n$. If $k \geq 4$, then $\chi(S_\mathbb{R}^\flat(n)) > n$; further $\chi(S_\mathbb{R}^\flat(n))$ increases exponentially with $n$.

Here the claim about the clique number is equivalent to the existence of Hadamard matrices of order a power of two. The claims are the chromatic number are much deeper, in particular the final claim follows from work of Frankl and Rödl.

4 Derangements

A derangement is a permutation of a set with no fixed point. If $D$ denotes the set of derangements in $\text{Sym} n$, then $D$ is closed under inverses and does
not contain the identity, so we may use $D$ as the connection set for the Cayley graph $X(\text{Sym} \ n, D)$; we denote this graph by $\mathcal{D}(n)$. We summarize some relevant properties of $\mathcal{D}(n)$.

4.1 Theorem. We have:

(a) The maximum size of a clique in $\mathcal{D}(n)$ is $n$; cliques of size $n$ correspond to $n \times n$ Latin squares.

(b) The maximum size of a coclique is $(n - 1)!$; the cocliques of size $(n - 1)!$ are cosets of the stabilizer of a point.

(c) The chromatic number of $\mathcal{D}(n)$ is $n$.

4.2 Corollary. For any graph $X$ we have $\chi(X) \leq n$ if and only if $X \rightarrow \mathcal{D}(n)$.

Two graphs $X$ and $Y$ are homomorphically equivalent if $X \rightarrow Y$ and $Y \rightarrow X$. The previous corollary may restated as the statement that $\mathcal{D}(n)$ and $K_n$ are homomorphically equivalent.

Let us represent elements of $\text{Sym} \ n$ by permutation matrices. The space of $n \times n$ complex matrices is an inner product space, with inner product

$$\langle M, N \rangle := \text{tr}(M^*N).$$

If $M$ is a permutation matrix, $M^* = M^{-1}$ and we see that if $M$ and $N$ are permutation matrices and $M^{-1}N$ represents a derangement, then $\langle M, N \rangle = 0$. Thus $\mathcal{D}(n)$ is an orthogonality graph.

5 Rank-1 Quantum Colourings and Unitary Derangements

Suppose $M$ defines a quantum $m$-colouring of $X$, where the entries of $M$ have rank one. Then the entries of $M$ must be of order $m \times m$. If $P_1, \ldots, P_m$ are the projections in row $i$ of $M$, then there are unit vectors $x_1, \ldots, x_m$ such that

$$P_r = x_r x_r^*$$
Since \( P_r P_s = 0 \) if \( r \neq s \), the vectors \( x_1, \ldots, x_m \) are pairwise orthogonal, and therefore they form the columns of a unitary matrix, \( R \) say. If \( S \) is the unitary matrix corresponding to row \( j \) of \( M \), then the condition \( M_{i,r} M_{j,r} = 0 \) holds for each \( r \) if and only the diagonal entries of \( R^* S \) are all zero. Since \( R \) and \( S \) are unitary, so is \( R^* S \).

We define a **unitary derangement** to be a unitary matrix with all diagonal entries zero. Any permutation matrix is unitary, and it is a unitary derangement if and only if the permutation it represents is a derangement. The inverse of a unitary derangement is its conjugate-transpose, and so it is again a unitary derangement. Hence we may define a Cayley graph \( UD(n) \) on the unitary group \( U(d) \), with connection set the set of unitary derangements. Note that the derangement graph \( D(n) \) is an induced subgraph of \( UD(n) \).

5.1 **Theorem.** A graph \( X \) has a rank-1 quantum \( n \)-colouring if and only if \( X \rightarrow UD(n) \). □

5.2 **Lemma.** If the matrices \( M_1, \ldots, M_n \) form a clique in \( UD(n) \), let \( M \) denote the \( n \times n \) matrix of projections with

\[
M_{i,j} = M_i e_j (M_i e_j)^*.
\]

Then \( M \) is a rank-1 quantum \( n \)-colouring of \( K_n \). □

In the context of quantum computing, rank-1 quantum \( n \)-colouring of \( K_n \) are referred as **quantum Latin squares**. (The choice of term was not motivated by any analogy to derangement graphs.) If \( L \) is an \( n \times n \) Latin square with entries from \( \{1, \ldots, n\} \) we can convert \( L \) to a quantum Latin square: if \( L_{i,j} = r \), replace the entry \( r \) by the projection \( e_r e_r^T \).

If \( z \) is a unit vector in \( \mathbb{C}^n \), then the unitary matrices \( M \) with \( i \)-th row equal to \( z \) form a coclique, for if \( Me_i = Ne_i = z \) then

\[
(M^* N)_{i,i} = e_i^T M^* N e_i = zz^* \neq 0
\]

and \( M^* N \) is not a derangement.

You may find it interesting to prove that \( \chi_q^{(1)}(X) = 3 \) if and only if \( \chi(X) = 3 \).
6 Three Homomorphisms

We use homomorphisms to relate some of the parameters at hand. One observation is in order.

6.1 Lemma. If $W$ is a flat unitary matrix and $D_1$ and $D_2$ are diagonal matrices (all of the same order), then

$$\langle D_1, W^* D_2 W \rangle = \text{tr}(D_1) \text{tr}(D_2).$$

6.2 Theorem. We have homomorphisms as follows:

$$K_n \to S^\flat(n) \to \mathcal{UD}(n) \to S(n).$$

Proof. The $n$-cliques in $S^\flat(n)$ are exactly the flat unitary matrices of order $n \times n$. This takes care of the first homomorphism.

For the second, if $z \in \mathbb{C}^n$, let $D_z$ be the diagonal matrix with

$$(D_z)_{i,i} = z_i.$$

If $z \in S^\flat(n)$, then $D_z$ is unitary and the map

$$z \mapsto D_z W$$

takes elements of $S^\flat(n)$ to unitary matrices. Consider the matrix

$$Q = (D_y W)^* D_z W.$$

We have

$$Q_{i,i} = \text{tr}(e_i e_i^T Q) = \langle e_i e_i^T, (D_y W)^* D_z W \rangle = \langle e_i e_i^T, W^* D_y^* D_z W \rangle$$

and, applying the lemma (with $D_1 = e_i e_i^T$), we deduce that

$$\langle e_i e_i^T, W^* D_y^* D_z W \rangle = \text{tr}(W^* D_y^* D_z W) = \text{tr}(D_y D_z) = \langle y, z \rangle.$$

Accordingly if $y$ and $z$ are orthogonal, then $Q$ is a derangement.

The third homomorphism is again simple. As

$$\langle M e_1, N e_1 \rangle = (M^* N)_{1,1}$$

we may use the map $M \mapsto M e_1$ as the homomorphism.

6.3 Corollary. For any graph $X$,

$$\chi(X) \geq \xi^\flat(X) \geq \chi_q^{(1)}(X) \geq \xi(X).$$
7 Separating $\chi$ and $\chi_q$

Let $q$ be an odd prime power. The vertices of the Erdős-Rényi graph $ER(q)$ are the 1-dimensional subspace of the 3-dimensional vectors over $GF(q)$; two subspaces spanned by nonzero vectors $x$ and $y$ are adjacent if $x^Ty = 0$. (Note: this is not an Erdős-Rényi random graph.) We see that $ER(q)$ has $q^2 + q + 1$ vertices and each vertex has $q + 1$ neighbours but, unfortunately perhaps, there are $q + 1$ vertices with loops on them.

The graph we use is $ER(3)$, on 13 vertices. Each vertex is represented by a vector length three with entries 0, 1 and $-1$. We normalize the vectors by assuming that the first non-zero entry is 1. Now we view these vectors as vectors over $\mathbb{R}$, and work with the orthogonality graph on these vectors. Denote it by $Y$. Clearly $\xi(Y) \leq 3$.

Cameron et al. prove the following, using properties of the quaternions.

7.1 Lemma. There is a homomorphism from $S_\mathbb{R}(4)$ into the subgraph of $UD(4)$ induced by the real orthogonal matrices.

7.2 Corollary. If $\xi_\mathbb{R}(x) \leq 4$, then $\chi_q^{(1)}(X) \leq 4$.

A direct computation shows that $\chi(Y) = 4$. Consider the cone $\hat{Y}$ over $Y$. Here $\xi_\mathbb{R}(\hat{Y}) \leq 4$, whence $\chi_q(\hat{Y}) \leq 4$. However $\chi(\hat{Y})$ must be five. Thus we have established that $\chi$ and $\chi_q$ can differ and, also, that a graph and its cone may have the same quantum chromatic number. We have not ruled out the possibility that $\chi_q(Y) = 3$, this is done in the oddities paper.

8 Derangements of Index $k$

We have seen that rank-1 colourings give rise to unitary derangements. What of rank-$k$ colourings?

A $d \times d$ projection $P$ of rank $k$ can be written as $P = UU^*$, where $U$ is $d \times k$ and its columns of are an orthonormal basis for $\text{im}(P)$. So $U^*U = I_k$. If the matrix $M$ represents a rank-$k$ quantum $m$-colouring of $X$, there are $d \times k$ matrices $U_{a,i}$ (for $a \in V(X)$ and $i = 1 \ldots, m$) such that

$$U_{a,i}^*U_{a,i} = I_k, \quad U_{a,i}U_{a,i}^* = M_{a,i}.$$
We see that if $i \neq j$, then $U^*_{a,i}U_{a,j} = 0$ and if $ab \in E(X)$, then $U^*_{a,i}U_{b,i} = 0$. Let $U$ be the matrix with $ai$-entry equal to $U_{a,i}$. Since $mk = d$, each row of $U$ is a $d \times d$ unitary matrix. If $ab \in E(X)$, then

\[(U_{a,1} \ldots U_{a,m})^* (U_{b,1} \ldots U_{b,m}) \]

is a unitary matrix of order $mk \times mk$ with $k$ diagonal blocks of zeros.

We define a unitary matrix $M$ to be a unitary derangement of index $k$ if it has order $mk \times mk$ and

\[M \circ (I_m \otimes J_k) = 0.\]

(If $k = 1$ we recover our previous derangements.) We can apply this term to permutation matrices, since they are unitary, and we will refer to them simply as derangements of index $k$. Since the set of $mk \times mk$ unitary derangements with index $k$ is closed under conjugate transpose and does not contain the identity, we can use it as the connection set for a Cayley graph for the full unitary group; if $n = km$, we denote it by $UD_k(n)$.

8.1 Theorem. Let $n = mk$. A graph $X$ has a rank-$k$ quantum $m$-colouring if and only if there is a homomorphism $X \rightarrow UD_k(n)$. \hfill $\square$

If $M$ is a unitary derangement (of index one) and $Q$ is unitary of order $k \times k$, then $M \otimes Q$ is a unitary derangement of index $k$.

9 Grassmann Graphs

The Grassmann graph $Gr(d, k)$ is the graph with the $k$-dimensional subspaces of $\mathbb{C}^d$ as vertices, with two subspaces adjacent if they are orthogonal. We may, and will, choose to represent the vertices of $Gr(d, k)$ by $d \times d$ projections of rank $k$. If $P$ and $Q$ are two such projections, then

\[\|P - Q\|^2 = \langle P - Q, P - Q \rangle = \text{tr}(P + Q - PQ - QP) = 2k - 2\langle P, Q \rangle.\]

Hence $P$ and $Q$ are at maximum distance if and only if they are orthogonal. (Since $P$ and $Q$ are positive semidefinite, $\langle P, Q \rangle \geq 0$.) Consequently we may view $Gr(d, k)$ as an analog of the Kneser graph $K_{d,k}$. Since the fractional chromatic number of a graph is determined by homomorphisms into Kneser graphs this suggests, correctly, that homomorphisms to Grassmann graphs will provide a quantum analog to fractional chromatic number.
9.1 Theorem. There is a homomorphism $UD_k(mk) \to Gr(mk,k)$.

Proof. Define

$$D = \begin{pmatrix} I_k & 0 \\ 0 & 0 \end{pmatrix}.$$ 

If $M$ is a $md \times md$ unitary matrix, then

$$MDM^*$$

represents orthogonal projection onto the column space of $MD$, i.e., onto the span of the first $k$ columns of $M$.

10 Quantum Homomorphisms

Since colourings can be usefully viewed as a special case of graph homomorphisms, it seems natural to look for quantum homomorphisms.

The definition is an extension of the definition of a quantum colouring, as it should be. A quantum homomorphism from $X$ to $Y$ is a $|V(X)| \times |V(Y)|$ matrix with entries $d \times d$ projections, such that:

(a) For each vertex $a$ of $X$, we have $\sum_{y \in V(Y)} M_{a,y} = I_d$.

(b) If $a$ and $b$ are adjacent vertices in $X$ and $y$ and $z$ are vertices in $Y$ that are not adjacent, then $M_{a,y}M_{b,z} = 0$.

You might check that, if $d = 1$, we recover the usual definition of a graph homomorphism.

It is important to note that a quantum homomorphism from $X$ to $Y$ is not a function from $V(X)$ to $V(Y)$. One symptom of this issue is that it is not obvious how we might compose quantum homomorphisms. Before discussing this, we offer a second definition of quantum homomorphism.

A measurement on $Y$ is an assignment of a $d \times d$ projection to each vertex in $Y$, such that if $P_u$ denote the projection indexed by $u$ in $V()$, then

$$\sum_{u \in V(Y)} P_u = I_d.$$ 

Given this condition, projections associated to different vertices are orthogonal. For a physicist a measurement indexed by $Y$ would be referred to
as a projective measurement, where the outcome of an actual measurement would be a vertex of $Y$. Two measurements $\{P_u\}_{u \in V(Y)}$ and $\{Q_u\}_{u \in V(Y)}$ are compatible if when $u$ and $v$ are vertices in $Y$ that are not adjacent,

$$P_u Q_v = 0.$$ 

(So $P_u Q_u = 0$ for each vertex $u$.) The vertices of the measurement graph $\mathcal{M}_d(Y)$ are the measurements on $Y$, where two measurements are adjacent if they are compatible. We have immediately:

10.1 Lemma. There is a quantum homomorphism $X \xrightarrow{q} Y$ if and only if $X \rightarrow \mathcal{M}_d(Y)$ for some $d$. \hfill $\square$

We turn to quantum composition. Assume $M$ and $N$ respectively represents quantum homomorphisms from $X$ to $Y$ and $Y$ to $Z$. We define $M \star N$ to be the matrix with rows indexed by $V(X)$, columns indexed by $V(Z)$ and with

$$(M \star N)_{x,z} = \sum_{y \in V(Y)} M_{x,y} \otimes N_{y,z}, \quad (x \in V(X), z \in V(Z)).$$

You need to verify that $M \star N$ represents a quantum homomorphism from $X$ to $Z$, and that this product is associative. (It then follows that graphs and quantum homomorphisms are the objects and arrows of a category.)