On the quantum chromatic number of a graph

Peter J. Cameron[*] Ashley Montanaro[†] Michael W. Newman[‡]
Simone Severini[§] Andreas Winter[¶]

Submitted: Oct 31, 2006; Accepted: Sep 30, 2007; Published: Nov 28, 2007
Mathematics Subject Classification: 05C15

Abstract

We investigate the notion of quantum chromatic number of a graph, which is the minimal number of colours necessary in a protocol in which two separated provers can convince a referee that they have a colouring of the graph.

After discussing this notion from first principles, we go on to establish relations with the clique number and orthogonal representations of the graph. We also prove several general facts about this graph parameter and find large separations between the clique number and the quantum chromatic number by looking at random graphs. Finally, we show that there can be no separation between classical and quantum chromatic number if the latter is 2, nor if it is 3 in a restricted quantum model; on the other hand, we exhibit a graph on 18 vertices and 44 edges with chromatic number 5 and quantum chromatic number 4.

1 Introduction

We consider an extension of graph colouring, based on the following model. Fix some graph G and an integer c. Alice and Bob are each given a vertex of G, and are to respond with an integer in $[c] := \{0, 1, \ldots, c-1\}$. They are required to answer differently if their vertices are adjacent, and identically if their vertices are equal. They are allowed to agree on a joint strategy beforehand, which may depend on G but not on the particular vertices they are given; in particular they are not allowed to communicate in any way once they are given their vertices.

[*]School of Mathematical Sciences, Queen Mary, University of London, London E1 4NS, U.K. p.j.cameron@qmul.ac.uk

[†]Department of Computer Science, University of Bristol, Bristol BS8 1UB, U.K. montanar@cs.bris.ac.uk

[‡]School of Mathematical Sciences, Queen Mary, University of London, London E1 4NS, U.K. m.newman@qmul.ac.uk

[§]Department of Mathematics, University of York, York YO10 5DD, U.K. ss54@york.ac.uk

[¶]Department of Mathematics, University of Bristol, Bristol BS8 1TW, U.K. a.j.winter@bris.ac.uk

It is easy to see that if $\chi(G) \leq c$, then they can always succeed: they agree beforehand on a proper vertex-colouring of G, and when presented with a vertex, answer with the colour assigned to it. It is not hard to see that if they are allowed no shared resource (other than a pre-arranged strategy depending only on G), then they can succeed with certainty only when $\chi(G) \leq c$. Thus if a referee wishes to certify that Alice and Bob have a proper c-colouring of G, it suffices to check whether they respond correctly to each pair of vertices. (In particular, the referee does not explicitly check whether Alice consistently colours a particular vertex the same way each time she is given it.)

If we allow Alice and Bob to use some shared resource (that does *not* involve communication), can they consistently fool the referee?

It is straightforward to see that shared randomness does not enable them to convince the referee with certainty. However, it turns out that if we allow Alice and Bob to share an *entangled quantum state*[1] (which may depend on G but not on the particular vertices they are given) then there are graphs G for which they can succeed with $c < \chi(G)$. In other words, they can convince a referee (in the above sense) that they have properly coloured G using only $c < \chi(G)$ colours. Based on a suggestion of one of the authors (also, independently of Patrick Hayden, see [1]) we call the smallest c such that Alice and Bob can win the graph colouring game the *quantum chromatic number*.

Such a problem was first considered in [7, 5], and generalised in [24], Theorems 8.5.1-3, and [6], for Hadamard graphs: the vertices are n-bit strings, and two of them are joined by an edge if and only if their Hamming distance is $n/2$. In these references it is shown that the game can be won with $c = n$ colours. This line of investigation was carried further under the heading "pseudo-telepathy" in [12, 13, 4, 1] (informally, if the referee does not believe in quantum entanglement, then they are forced to believe that Alice and Bob are "telepathic"). Earlier work of Frankl and Rödl [11] in extremal combinatorics established that the chromatic number of the Hadamard graphs grows exponentially in n. In [14, 20] it is shown that the chromatic number is equal to n if and only if $n \in \{1, 2, 4, 8\}$.

The rest of the paper is structured as follows: in section 2 we present the model, or actually an infinite hierarchy of models for the quantum chromatic number. Then we go on to general properties of the quantum chromatic number in section 3, bounds via orthogonal representations (section 4), small number of colours (section 5), and finally random graphs (section 6), after which we conclude with a number of open questions and conjectures. In the appendix is a brief dictionary of terms and notions from quantum mechanics that are used in the paper. The reader is referred to [22] for a proper treatment.

2 Model(s)

The most general strategy for Alice and Bob to win the graph colouring game with probability 1 with c colours for a graph $G = (V, E)$ consists of an entangled state $|\psi\rangle_{AB} \in \mathbb{C}^{d\times d}$ shared between them, and two families of POVMs $(E_{v\alpha})_{\alpha=0,\ldots,c-1}$ and $(F_{v\beta})_{\beta=0,\ldots,c-1}$, indexed by the vertices $v \in V$ of the graph. The fact that they win with probability 1 is

[1]See the appendix for a definition of this and other terms relating to quantum mechanics.

expressed by the consistency condition

$$\begin{aligned} \forall v \in V \ \forall \alpha \neq \beta \quad & \langle\psi|E_{v\alpha} \otimes F_{v\beta}|\psi\rangle = 0, \\ \forall vw \in E \ \forall \alpha \quad & \langle\psi|E_{v\alpha} \otimes F_{w\alpha}|\psi\rangle = 0. \end{aligned} \tag{1}$$

Note that the dimension d bears no relationship to c, that the entangled state $|\psi\rangle$ can be anything (it may even be mixed but it is immediate that w.l.o.g. we may assume it to be pure), and the POVMs may have operators of arbitrary rank.

The smallest possible c for which Alice and Bob can convince the referee, i.e. such that eq. (1) holds, is called the *quantum chromatic number* of G and it will be denoted by $\chi_q(G)$.

Proposition 1 *To win the graph colouring game in the above setting, w.l.o.g. the state is maximally entangled, and the POVM elements are all projectors, all w.l.o.g. of the same rank.*

Proof. Without loss of generality we can assume that $|\psi\rangle$ has full Schmidt rank d since otherwise we restrict all POVMs to the supports of the respective reduced states. From eq. (1) we get, for any $v \in V$, any α and $\beta \neq \alpha$, that $E_{v\alpha} \perp \mathrm{Tr}_B\big((\mathbb{1} \otimes F_{v\beta})|\psi\rangle\langle\psi|\big)$, hence

$$\begin{aligned} E_{v\alpha} \perp \sum_{\beta\neq\alpha} & \mathrm{Tr}_B\big((\mathbb{1} \otimes F_{v\beta})|\psi\rangle\langle\psi|\big) \\ & = \mathrm{Tr}_B\big((\mathbb{1} \otimes \mathbb{1} - \mathbb{1} \otimes F_{v\alpha})|\psi\rangle\langle\psi|\big). \end{aligned}$$

From this, and because Alice needs to get outcome α with certainty if Bob gets α, we must have

$$E_{v\alpha} = \mathrm{supp}\ \mathrm{Tr}_B\big((\mathbb{1} \otimes F_{v\alpha})|\psi\rangle\langle\psi|\big).$$

By the same argument all $F_{v\beta}$ are projectors.

Now we argue that the consistency requirement for the state $|\psi\rangle$ implies that it is also true when we substitute the maximally entangled state Φ_d: in its Schmidt basis, $|\psi\rangle = \sum_i \sqrt{\lambda_i}|i\rangle|i\rangle$, and denoting $\rho = \mathrm{Tr}_B\,|\psi\rangle\langle\psi| = \sum_i \lambda_i |i\rangle\langle i| = \mathrm{Tr}_A\,|\psi\rangle\langle\psi|$, the finding of the previous paragraph can be cast as

$$\begin{aligned} E_{v\alpha} &= \mathrm{supp}\,\sqrt{\rho}\big(\overline{F_{v\alpha}}\big)\sqrt{\rho}, \\ F_{w\beta} &= \mathrm{supp}\,\sqrt{\rho}\big(\overline{E_{w\beta}}\big)\sqrt{\rho}. \end{aligned}$$

This implies however

$$E_{v\alpha}\rho E_{v\beta} = 0$$

for all v and $\alpha \neq \beta$ (where we cancelled $\sqrt{\rho}$'s left and right), and likewise for $F_{w\alpha}$, $F_{w\beta}$. But with the fact that each $E_{v\alpha}$ is a projector and that summed over α they yield the identity, this gives (for arbitrary v)

$$\rho = \sum_{\alpha,\beta} E_{v\alpha}\rho E_{v\beta} = \sum_{\alpha} E_{v\alpha}\rho E_{v\alpha},$$

from which it follows that ρ commutes with all the (Kraus) operators $E_{v\alpha}$, and likewise $F_{w\beta}$ [18]. Hence we find

$$E_{v\alpha} = \overline{F_{v\alpha}}, \quad F_{w\beta} = \overline{E_{w\beta}},$$

and that is the claim we set out to prove: we may as well assume that $|\psi\rangle$ is maximally entangled.

Finally, how to make the operators all the same rank: let $|\psi'\rangle = |\psi\rangle \otimes |\Phi_c\rangle$, and

$$E'_{v\alpha} := \sum_{i=0}^{c-1} E_{v,\alpha+i} \otimes |i\rangle\langle i|,$$
$$F'_{w\beta} := \sum_{i=0}^{c-1} F_{w,\beta+i} \otimes |i\rangle\langle i|,$$

where the colours are w.l.o.g. $\{0, \dots, c-1\}$ and the additions above are modulo c. These states and operators evidently still make for a valid quantum colouring, and also clearly all operators have now the same rank. ∎

This proposition motivates us to introduce rank-r versions of the quantum chromatic number: $\chi_q^{(r)}(G)$ is the minimum c such that Alice and Bob can win the graph colouring game for G with a maximally entangled state of rank rc, and POVMs with operators of rank r (exactly). Then it is clear that $\chi_q^{(r)}(G) \leq \chi_q^{(s)}(G)$ whenever $r \geq s$, and that $\chi_q(G) = \inf_r\{\chi_q^{(r)}(G)\}$.

The special case of rank-1 model is the following: Alice and Bob share a c-dimensional maximally entangled state

$$|\Phi_c\rangle = \frac{1}{\sqrt{c}} \sum_{i=0}^{c-1} |i\rangle_A |i\rangle_B.$$

To make their choices, they both use rank-1 von Neumann measurements, which are ordered bases $(|e_{v\alpha}\rangle)_\alpha$ and $(|f_{v\beta}\rangle)_\beta$ for all vertices v, for Alice and Bob, respectively.

Observation 1. Bob's bases are tied to Alice's by the demand of consistency: we need, for all v and α,

$$\langle e_{v\alpha}|\langle f_{v\alpha}|\Phi_c\rangle = 1/\sqrt{c},$$

which enforces

$$|f_{v\alpha}\rangle = \overline{|e_{v\alpha}\rangle}.$$

Observation 2. This means that we can translate the colouring condition into something that only concerns Alice's bases: we need, for all $vw \in E$ and all α,

$$\langle e_{v\alpha}|\langle f_{w\alpha}|\Phi_c\rangle = 0.$$

Because of

$$\langle f_{w\alpha}|\Phi_c\rangle = \frac{1}{\sqrt{c}} \overline{|f_{w\alpha}\rangle}$$

and Observation 1 this can be rewritten as

$$\forall vw \in E \text{ and } \forall \alpha \quad \langle e_{v\alpha}|e_{w\alpha}\rangle = 0. \tag{2}$$

Observation 3. It is convenient to introduce unitary matrices U_v for each vertex v, whose columns are just the vectors $|e_{v\alpha}\rangle$, $\alpha = 0, \ldots, c-1$. Then we can reformulate Alice's strategy as follows: on receiving the request for vertex v, she performs the unitary $U_v^\dagger$ on her quantum system and measures in the standard basis to get a number $\alpha \in [c]$. By Observation 1 above, Bob, for vertex w, performs the unitary $\overline{U_w}^\dagger = U_w^\top$ and measures in the standard basis to obtain $\beta \in [c]$. In the light of Observation 2, we can rewrite the colouring condition expressed in eq. (2) as:

$$\forall vw \in E \quad U_v^\dagger U_w \text{ has only zeroes on the diagonal.} \tag{3}$$

By a similar chain of arguments we can show, for the POVM constructed in the proof of proposition 1, that $F_{v\alpha} = \overline{E_{v\alpha}}$ for all vertices v and all colours α, and that hence the colouring condition can be phrased entirely in terms of Alice's operators:

$$\forall vw \in E \text{ and } \forall \alpha \quad E_{v\alpha}E_{w\alpha} = 0, \tag{4}$$

i.e. $E_{v\alpha}$ and $E_{w\alpha}$ are orthogonal.

3 General properties

We look at some basic properties of the quantum chromatic number as a graph parameter. None of these are particularly surprising; indeed the point of this section is to show that the quantum chromatic number "does the right thing", and merits being considered as a generalization of the (ordinary) chromatic number.

A *homomorphism* is a mapping from one graph to another that preserves edges. That is, a homomorphism ϕ from G to H maps vertices of G to vertices of H such that if x and y are adjacent in G then $\phi(x)$ and $\phi(y)$ are adjacent in H. We write $G \to H$ to indicate that there exists a homomorphism from G to H.

The following easy observation is a useful tool.

Proposition 2 *If $G \to H$, then $\chi_q^{(r)}(G) \leq \chi_q^{(r)}(H)$ for all r and hence $\chi_q(G) \leq \chi_q(H)$.*

Proof. Let ϕ be a homomorphism from G to H. Then any quantum colouring of H gives a quantum colouring of G by colouring the vertex x of G with the colour assigned to $\phi(x)$ in H. ∎

It is trivial to see that if (and only if) G has no edges then $\chi_q^{(r)}(G) = \chi_q(G) = 1$. With a little more effort, one sees that if $G = K_n$ then $\chi_q^{(r)}(G) = \chi_q(G) = n$. For, using proposition 1 and eq. (4), we have a set of n rank-r pairwise orthogonal operators in a space of dimension cr. We can say a little more.

Proposition 3 *$\chi_q(G) = 2$ if and only if $\chi(G) = 2$.*

Proof. If $\chi(G) = 2$, then $G \to K_2$ and $K_2 \to G$, and so by proposition 2 $\chi_q(G)$ is at most and at least 2. On the other hand, consider any quantum colouring of G with 2 colours, with orthogonal projectors $E_{v\alpha}$ for Alice, $\alpha = 0, 1$. By eq. (4), however, $E_{v\alpha} = \mathbb{1} - E_{w\alpha}$ for adjacent vertices v and w. That means, looking at a fixed colour α^*, we encounter only two different operators as we traverse the graph – these can serve as colours in a colouring as adjacent vertices will have different $E_{v\alpha^*}$. ■

The *clique number of* G, denoted by $\omega(G)$, is the size of the largest complete subgraph of G.

Proposition 4 $\omega(G) \leq \chi_q(G) \leq \chi(G)$ □

Proof. Any graph G contains $K_{\omega(G)}$ as a subgraph, hence $K_{\omega(G)} \to G$. Also $G \to K_{\chi(G)}$, by mapping each vertex to the vertex of $K_{\chi(G)}$ corresponding to its colour. The result follows by proposition 2. ■

Of course, propositions 3 and 4 remain valid if we replace χ_q with $\chi_q^{(r)}$ for any r.

Let G and H be two graphs on the same vertex set. We define the graph $G \cup H$ to be the graph whose edge set is the union of the edge sets of G and H. It is a well-known result in graph theory [21, Chap 14.1] that $\chi(G \cup H) \leq \chi(G)\chi(H)$: colour each vertex in $G \cup H$ with the ordered pair of colours it received in colourings of G and H, respectively. This idea can be extended to quantum colourings:

Proposition 5 *For any r, s, we have $\chi_q^{(rs)}(G \cup H) \leq \chi_q^{(r)}(G)\chi_q^{(s)}(H)$.*

Proof. Given rank-r and rank-s quantum colourings for G and H respectively, we obtain a rank-rs quantum colouring of $G \cup H$ by taking the tensor products of the individual POVM operators associated to the vertices. ■

As a corollary, we obtain the following, showing that a graph and its complement cannot both have small quantum chromatic number.

Proposition 6 *$\chi_q(G)\chi_q(\overline{G}) \geq n$.*

Proof. Apply proposition 5 with $H = \overline{G}$, the complement of G. ■

4 Orthogonal representations

The origin of the quantum chromatic number is in Hadamard graphs [7, 5], which are a special case of orthogonality graphs, so it is natural to consider the larger family.

An *orthogonal representation* of a graph G is a mapping ϕ from the vertices of G to the non-zero vectors of some vector space, such that if two vertices x and y are adjacent, then $\phi(x)$ and $\phi(y)$ are orthogonal.

Given a set of vectors, we define their *orthogonality graph* to be the graph having the vectors as vertices, with two vectors adjacent if and only if they are orthogonal.

Define the *orthogonal rank* of G, $\xi(G)$, as the smallest integer c such that G has an orthogonal representation in the vector space $\mathbb{C}^c$. Furthermore, let $\xi'(G)$ be the smallest integer c such that G has an orthogonal representation in the vector space $\mathbb{C}^c$ with the added restriction that the entries of each vector must have modulus one. (Note that we really only need the entries in any particular vector to have constant modulus.)

Proposition 7 $\omega(G) \leq \xi(G) \leq \chi_q^{(1)}(G) \leq \xi'(G) \leq \chi(G)$

Proof. For each integer c, let F_c be the discrete Fourier transform of order c, i.e., $[F_c]_{j,k} = \frac{1}{\sqrt{c}} e^{2\pi ijk/c}$.

Three of these inequalities are straightforward.

Given a graph with $\chi(G) = c$, colour the vertices with the rows of F. Adjacent vertices have distinct colours and hence orthogonal vectors, and thus $\xi'(G) \leq \chi(G)$. Given a graph with $\chi_q^{(1)}(G) = c$, map each vertex to the first column of its corresponding unitary matrix. By eq. (2) adjacent vertices will get mapped to orthogonal vectors, and thus $\xi(G) \leq \chi_q^{(1)}(G)$. Given a graph with $\omega(G) = c$, any orthogonal representation of it must contain c pairwise orthogonal vectors and thus $\omega(G) \leq \xi(G)$.

Finally, given a graph with $\xi'(G) = c$, map each vertex x to $\Delta_x F_c$, where Δ_x is the diagonal (unitary) matrix whose diagonal entries are the entries of x. Then $\langle x|y\rangle = 0$ implies that $(\Delta_v F_c)^\dagger(\Delta_w F_c)$ has only zeroes on the diagonal. Thus $\chi_q^{(1)} \leq \xi'$. ∎

The proof that $\chi_q^{(1)}(G) \leq \xi'(G)$ is in fact a familiar one: it is essentially the original proof of [7, 5] using F_c in place of a Hadamard matrix, or extension of [1] using more general vertices.

In fact the only properties of F_c that we need are that its columns form an orthonormal basis and the entries all have the same modulus. So the (normalized) character table of *any* Abelian group of order c will do (as will a generalized Hadamard matrix). Likewise, the only properties of the vertices that we need are that adjacent vertices are orthogonal and the entries all have the same modulus, so we need not restrict ourselves to ± 1-vectors.

The results of [7, 5] can be rephrased in our current language as follows. Given a graph G, what is the smallest integer c such that G has an orthogonal representation in $\mathbb{C}^c$ with the added restriction that all entries are ± 1? This motivates us to consider the following question: what happens if we replace "± 1" by some other subset of roots of unity?

Proposition 8 *Let p be a prime. Let G be the orthogonality graph whose vertices are the vectors of $\mathbb{C}^p$ whose entries are all p-th roots of unity. Then $\chi(G) = p$.*

Proof. We first show that G is a Cayley graph for $\mathbb{Z}_p^p$ (this is in fact well known). To each vertex a associate the mapping $\sigma_a : x \to a \circ x$, where $a \circ x$ denotes the entry-wise product of a and x. Two vertices x and y are adjacent when $\langle x|y\rangle = 0$, or equivalently when $y = \sigma_a(x)$ for some a whose entries sum to zero. Thus the connection set is the set of such a.

The fact that p is prime is relevant for the following reason. Vertices x and y are adjacent if and only if the entries of $\overline{x} \circ y$ are all distinct: this is because the entries are p-th roots of unity and there are p of them.

It is well-known that for vertex transitive graphs H (such as Cayley graphs), we have $\alpha(H)\omega(H) \leq v$, where $\alpha(H)$ is the independence number of H, i.e. the size of the largest independent set of H. We use an extension due to Godsil [15], which in our case we may state as follows: if H is a Cayley graph on v vertices for an Abelian group then $\alpha(H)\omega(H) = v$ if and only if $\chi(H) = \omega(H)$.

It is easy to see that $\omega(G) = p$: take the rows of the character table for $\mathbb{Z}_p$. So it is necessary and sufficient to find an independent set of size p^{p-1}.

The set of vertices x with $x_1 = x_2$ form an independent set of size p^{p-1}: no two of them are adjacent since for any such x and y, the first two entries of $\overline{x} \circ y$ are equal, hence the entries are not all distinct. ■

Note that in an orthogonality graph, vectors that differ by a scalar multiple are non-adjacent and have the same neighbours, so we may restrict ourselves to vectors that have first entry equal to one. (We are really dealing with 1-dimensional subspaces and not vectors.) For convenience, we use this in the next result.

Proposition 9 *Let G be the orthogonality graph defined by vectors of dimension 4 whose entries are taken from the set $\{1, i, -1, -i\}$. Then $\chi(G) = 4$.*

Proof. It is clear that $\chi(G) \geq 4$, as G contains the 4-clique

$$\{(1,1,1,1),(1,i,-1,-i),(1,-1,1,-1),(1,-i,-1,i)\}.$$

We give an explicit 4-colouring of G found by computer. Consider the set S of all 4-dimensional vectors whose first component is 1, and whose other 3 components are taken from the set $\{1, i, -1, -i\}$. A 4-colouring of the orthogonality graph on S gives a 4-colouring of G. Consider each element $s \in S$ as a 3-digit string $s' \in \{0,1,2,3\}^3$ giving the power of i in each component of s, and list the vertices of S in lexicographic order. Then a 4-colouring of the orthogonality graph on S is given by the following:

$$\begin{aligned}(&1,1,1,2,1,1,1,2,2,1,2,2,2,1,2,2,2,1,3,3,4,1,1,3,4,\\ &4,1,2,2,4,3,2,3,4,3,3,3,4,3,3,4,4,4,3,4,4,4,3,1,1,\\ &4,3,3,1,2,3,3,4,2,2,1,4,4,2).\end{aligned} \quad ■$$

Both the graphs of proposition 8 and proposition 9 satisfy $\omega = \chi$, and therefore by proposition 4 also have $\omega = \chi_q = \chi_q^{(r)} = \chi$.

It is not hard to see directly that the orthogonality graph on ± 1-vectors of dimension 2 is 2-colourable. Thus for orthogonality graphs using ± 1-vectors, in order to have $\chi_q < \chi$ we need to go to dimensions larger than 2. We now see that for d a prime or $d = 4$, using d-th roots of unity vectors forces us to go to dimensions larger than d to obtain $\chi_q < \chi$.

Finally, we derive an upper bound on the chromatic number of the orthogonality graph on $\mathbb{C}^k$ in terms of k, which gives an upper bound on $\chi(G)$ in terms of $\xi(G)$ for any graph

G by converting any orthogonal representation of G into a colouring of G. This allows us to bound the largest possible gap between $\chi(G)$ and $\chi_q^{(1)}(G)$.

Proposition 10 *For any graph G,*

$$\chi(G) \leq (1+2\sqrt{2})^{2\,\xi(G)} \leq (1+2\sqrt{2})^{2\chi_q^{(1)}(G)}.$$

Proof. To show the first inequality, we give a colouring of the orthogonality graph on $\mathbb{C}^k$, where $k = \xi(G)$. This can be produced from a set of unit vectors $V = \{|v_i\rangle\}$ such that for all unit vectors $|w\rangle \in \mathbb{C}^k$, $\||w\rangle - |v_i\rangle\|_2 < 1/\sqrt{2}$ for some i, by assigning colour i to $|w\rangle$ (if there are two or more vectors in V satisfying this inequality, picking one arbitrarily). This works because, for any two vectors $|x\rangle$, $|y\rangle$, $\langle x|y\rangle = 0 \Rightarrow 2(1-\mathrm{Re}(\langle x|y\rangle)) = \||x\rangle - |y\rangle\|_2^2 = 2$, so no two orthogonal vectors will receive the same colour. We use the argument of [16] to bound the size of such a set (which [16] calls a $1/\sqrt{2}$-net). Let $M = \{|v_i\rangle\}$ be a maximal set of unit vectors such that $\||v_i\rangle - |v_j\rangle\|_2 \geq 1/\sqrt{2}$ for all i and j and set $m = |M|$. Then M is a $1/\sqrt{2}$-net giving a m-colouring of the orthogonality graph of $\mathbb{C}^k$. Observe that, as subsets of $\mathbb{R}^{2k}$, the open balls of radius $1/(2\sqrt{2})$ about each $|v_i\rangle$ are disjoint and contained in the overall ball of radius $1 + 1/(2\sqrt{2})$. Thus $m(1/(2\sqrt{2}))^{2k} \leq (1 + 1/(2\sqrt{2}))^{2k}$. The second inequality follows from proposition 7. ■

Remark. The above result shows that the separation between $\chi(G)$ and $\chi_q^{(1)}(G)$ can be at most exponential; the results of [6, 24] on the other hand demonstrate that exponential gaps can occur, showing that this is indeed the most extreme case, up to a constant factor in the exponent.

5 Few colours

Here we investigate properties of graphs with small quantum chromatic number or small orthogonal rank. We already saw that for two colours, classical and quantum chromatic numbers coincide. It turns out that for three this is also the case, and for numbers up to 8 the quantum chromatic number stays close to the orthogonal rank.

Proposition 11 *Given a graph G, $\chi_q^{(1)}(G) = 3$ if and only if $\chi(G) = 3$.*

Proof. If $\chi(G) = 3$, we cannot have $\chi_q(G) = 2$ (nor 1 because the graph is not empty) as this would mean $\chi(G) = 2$. On the other hand, consider a rank-1 quantum colouring with 3 colours. We use the analysis in section 2 and in particular the last observation 3: we can view the quantum colouring as a family of 3×3-unitaries U_v such that eq. (3). The columns of the unitaries are just the basis vectors $|e_{v0}\rangle$, $|e_{v1}\rangle$, $|e_{v2}\rangle$. W.l.o.g. the graph is connected and for one distinguished vertex v_0 we may assume $U_{v_0} = \mathbb{1}$.

The crucial observation is that there are essentially only two unitary(!) matrices $U_v^\dagger U_w$ with zeroes on the diagonal [23]: they can only be

$$\begin{pmatrix} 0 & 0 & * \\ * & 0 & 0 \\ 0 & * & 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & * & 0 \\ 0 & 0 & * \\ * & 0 & 0 \end{pmatrix},$$

where the starred entries must be roots of unity. Starting from v_0 we hence find inductively that all U_v are, up to phase factors, permutation matrices. Just looking at the first column, we now obtain a 3-colouring of G, choosing the colour according to the row in which the nonzero entry of the column vector is. ■

Proposition 12 *Let G be a graph with an orthogonal representation in $\mathbb{R}^c$. If $c = 3, 4$ then $\chi_q^{(1)}(G) \leq 4$; if $4 < c \leq 8$ then $\chi_q^{(1)}(G) \leq 8$.*

Proof. If $c = 4, 8$ then associate every vector $v \in \mathbb{R}^4$ and $w \in \mathbb{R}^8$ to real orthogonal designs V and W of the form $OD\,(4; 1, \ldots, 1)$ and $OD\,(8; 1, \ldots, 1)$, respectively. For example, every vector $v \in \mathbb{R}^4$ is associated to a real-orthogonal matrix

$$V = \begin{pmatrix} v_1 & v_2 & v_3 & v_4 \\ -v_2 & v_1 & -v_4 & v_3 \\ -v_3 & v_4 & v_1 & -v_2 \\ -v_4 & -v_3 & v_2 & v_1 \end{pmatrix}.$$

If $v \in \mathbb{R}^c$ and $c = 3$ or $4 < c \leq 8$ then concatenate a zero-vector of length 1 or $8 - c$ to v, respectively, and proceed as above. ■

Remark. The above construction works based on the fact that in dimensions 4 and 8 there exist division algebras (Hamilton quaternions and Cayley octonions); namely, the generating orthogonal units $1, i, j, k, \ldots$ have the property that multiplication by one of them turns every vector into an orthogonal one. Unfortunately they exist only in dimensions 1, 2, 4 and 8, cf. [10].

Example. We now give an example of a fairly small graph G (18 vertices and 44 edges) which has quantum chromatic number [actually even $\chi_q^{(1)}(G)$] equal to 4, but chromatic number 5. Label the vertices with integers $1 \ldots 18$; then

$$\begin{aligned} E = \{&(1,2), (1,3), (1,11), (1,12), (1,16), (2,3), (2,4), \\ &(2,13), (3,4), (3,13), (4,5), (4,6), (4,10), (4,17), \\ &(5,6), (5,7), (5,14), (6,7), (6,14), (7,8), (7,9), \\ &(7,16), (8,9), (8,10), (8,13), (9,10), (9,13), (10,11), \\ &(10,12), (10,17), (11,12), (11,14), (12,14), (13,14), \\ &(13,15), (13,18), (14,15), (14,18), (15,16), (15,17), \\ &(15,18), (16,17), (16,18), (17,18)\} \end{aligned}$$

The graph may be visualised as consisting of two components connected to each other by 8 additional edges: a 4-regular graph on vertices $1 - 14$ [augmented by two edges $(4, 10)$ and $(13, 14)$], and a 4-clique on vertices $15 - 18$, see Fig. 5. The following list of vectors gives an orthogonal representation of G in $\mathbb{R}^4$, which by Proposition 12 gives a quantum colouring with 4 colours:

$$\begin{aligned} \{&(0,0,1,-1), (1,0,0,0), (0,1,1,1), (0,1,0,-1), (0,0,1,0), \\ &(1,1,0,1), (1,-1,0,0), (0,0,0,1), (1,1,1,0), (1,0,-1,0), \\ &(0,1,0,0), (1,0,1,1), (0,1,-1,0), (1,0,0,-1), (1,1,1,1), \\ &(1,1,-1,-1), (1,-1,1,-1), (1,-1,-1,1)\} \end{aligned}$$

Because G contains a 4-clique, $\chi_q(G)$ cannot, on the other hand, be smaller than 4.

It may be verified as follows that G cannot be 4-coloured. Assume w.l.o.g. that vertices 15-18 are coloured $1, 2, 3, 4$ respectively. Then vertices 13 and 14 must divide colours 2 and 3 between them; and for a valid 4-colouring, none of the triplets $(1, 4, 13)$, $(1, 10, 14)$, $(4, 7, 14)$, $(7, 10, 13)$ may consist of 3 distinct colours. Using this, it is straightforward to try all the possible colourings of vertex 7 and see that each leads to vertices 4 and 10 being assigned the same colour.

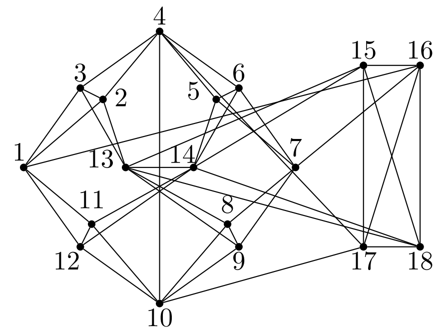

Figure 1: A graph G with $\chi_q(G) = \chi_q^{(1)}(G) = 4$, but $\chi(G) = 5$.

This graph is much smaller and uses fewer colours than the smallest specimen previously known exhibiting a separation between classical and quantum chromatic numbers: in [1] a graph on 1609 vertices is described with $\chi(G) \geq 13$ and $\chi_q(G) = 12$.

6 Random graph properties

Now we show, in contrast to all previous constructions separating classical and quantum chromatic number, that the clique number and the quantum chromatic number (in the rank-1 model) are generically exponentially separated. We use the customary notation $\mathcal{G}(n,p)$ for the family of graphs on n vertices with all edges drawn independently with probability p.

Proposition 13 *For a random graph $G \in \mathcal{G}(n,p)$, and $\epsilon > 0$,*

$$\omega(G) \leq (1+\epsilon)\frac{2\log n}{\log 1/p},$$
$$\chi_q^{(1)}(G) \geq (1-\epsilon)c(p)\sqrt{n},$$

almost surely, with some constant $c(p)$ depending on p.

Proof. The statement on the clique number is Bollobás' classic result [3] (we actually use a slightly weaker version).

The statement on $\chi_q^{(1)}(G)$ follows from that quantity being lower bounded by $\xi(G)$, which is lower bounded by the Lovász theta function [19] of the complement graph $\overline{G}$, whose random graph behaviour has been worked out by Juhasz [17]. ■

Remark. From proposition 5 we know that for any graph G, $\chi_q(G)\chi_q(\overline{G}) \geq \chi_q(K_n) = n$, hence at least one of G and $\overline{G}$ has quantum chromatic number $\geq \sqrt{n}$. Assume that $G \in \mathcal{G}(n, 1/2)$; then also $\overline{G} \in \mathcal{G}(n, 1/2)$ and both G and $\overline{G}$ are likely to have clique number only $2\log n + o(\log n)$. That means that we get an abundance of graphs for which the quantum chromatic number is exponentially larger than the clique number; asymptotically at least half of all graphs have this property. It would be interesting to see if the gap between $\omega(G)$ and $\chi_q(G)$ cannot be larger than exponential, in extension of proposition 10.

7 Conclusions & conjectures

We have studied the quantum chromatic number, the minimal number of colours required for two independent provers to win the graph colouring game if they are allowed entanglement, from first principles, and as a general graph property, beyond the immediate interest of quantum advantage exhibited in pseudo-telepathy.

We discovered a number of relations of this graph quantity to other, known, quantities such as chromatic number, clique number, orthogonal representations and the Lovász theta. We also found several separations between the quantum chromatic numbers and these quantities, but had to leave open a number of important questions.

One of them is the fundamental one: whether the graph colouring game can always be won with minimal c and a rank-1 measurement, in other words, whether $\chi_q^{(1)}(G) = \chi_q(G)$ for all graphs G. This has bearing on the decidability of the quantum chromatic number: the problem if $\chi_q^{(r)}(G) \leq c$ is decidable because it boils down to solving the set of quadratic equations (1) over the reals in a space of dimension cr, for which there exist exact algorithms based on extensions of the Gröbner basis technique [2]. However, $\chi_q(G) = \inf_r \chi_q^{(r)}(G)$ is not decidable in such an easy way. It should be possible to prove at least an upper bound on r that is sufficient to attain the limit. In that case, it would make sense to ask about the complexity of computing $\chi_q(G)$, in particular whether it is NP-hard, as is computing the chromatic number $\chi(G)$.

Similarly, we found an exponential upper bound on $\chi(G)$ in terms of $\chi_q^{(1)}(G)$, but not in terms of $\chi_q(G)$. In particular, it is still open whether there exists an (infinite) graph G with $\chi(G) = \infty$ and finite $\chi_q(G)$.

Related to the question of whether $\chi_q^{(1)}(G) = \chi_q(G)$ is the question of separating $\xi(G)$ and $\xi'(G)$. If in fact these two parameters are equal for all graphs, then the rank-1 quantum chromatic number is exactly the minimum dimension for which the graph has an orthogonal representation.

An interesting question arises in the random graph setting: what is the likely quantum chromatic number of $G \in \mathcal{G}(n,p)$? Conjecture: random graphs have $\chi(G) = \chi_q(G)$ almost surely. Recalling that $\chi(G) \sim \frac{n \log \frac{1}{1-p}}{2 \log n}$ with high probability [3], it may be possible to show by an easier approach that for all $\epsilon > 0$, $\chi_q^{(1)}(G) \geq (1-\epsilon)\frac{n \log \frac{1}{1-p}}{2 \log n}$ almost surely. Namely, one would have to show that the consistency equations (2) have, with high probability, no solution for $c = \left\lfloor (1-\epsilon)\frac{n \log \frac{1}{1-p}}{2 \log n} \right\rfloor$ colours.

Finally, an easier but still fascinating problem would be to find the smallest graph (and the smallest number of colours) exhibiting a separation between classical and quantum chromatic number. The graph G shown in Figure 5 has $\chi_q^{(1)}(G) = 4$ and $\chi(G) = 5$. By proposition 11, this is the minimum value of $\chi_q^{(1)}$ that can achieve such a separation. However, a graph showing a separation with a smaller number of vertices might exist, as might a graph with $\chi_q(G) = 3$, $\chi(G) > 3$.

A Notation and terminology

We introduce here the main terms and notions from the quantum mechanics used in the paper.

A quantum mechanical system S is axiomatically associated to a complex Hilbert space $\mathcal{H} \cong \mathbb{C}^n$, in which the inner product is written $\langle \cdot | \cdot \rangle$. Here, n is the *dimension* of S. Note that by physics convention the inner product is linear in the second argument and conjugate-linear in the first – opposite to the convention mostly used in mathematical literature. In physical terms, the dimension represents the maximum number of different classical configurations that can be observed by performing a measurement on the state of S. When S is completely isolated from the environment, its state is a unit vector $|\psi\rangle \in \mathcal{H}$ (where ψ is simply a label) modulo global scalar phase, or, equivalently, a matrix of the form $\rho_\psi = |\psi\rangle\langle\psi|$, called *density matrix*. We denote by $\langle\varphi|$ the linear functional that sends $|\psi\rangle$ to the inner product $\langle\varphi|\psi\rangle$. If S is composed of two subsystems A and B of dimension k and l, then $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \cong \mathbb{C}^k \otimes \mathbb{C}^l$, where $\otimes$ denotes the tensor product. We say that $|\psi\rangle \in \mathcal{H}$ is *entangled* if $|\psi\rangle \neq |\varphi\rangle_A \otimes |\chi\rangle_B$, for all $|\varphi\rangle_A \in \mathcal{H}_A$ and $|\chi\rangle_B \in \mathcal{H}_B$; otherwise $|\psi\rangle$ is *separable*. For $k = l$, the state $|\Psi\rangle = \frac{1}{\sqrt{k}} \sum_{i=0}^{k-1} |i\rangle|i\rangle$, where $|i\rangle$ is the i-th standard basis vector, is said to be *maximally entangled*. The time-evolution of S is induced by unitaries $U \in U(n)$: $U|\psi\rangle = |\psi(U)\rangle$. In our context, we observe S by means of POVMs. A *positive operator value measure* (for short, *POVM*) is a family $(E_i)_{i=1}^m$ of Hermitian positive semidefinite matrices, such that $\sum_{i=1}^m E_i = \mathbb{1}$, where possibly $m > n$ or $m < n$. The POVM $(E_i)_{i=1}^m$ is called *projective* if $E_i E_j = \delta_{ij} E_i$ for all i, j. The state ρ_ψ is transformed into the state $\sigma_\psi = \frac{E_i \rho_\psi E_i^\dagger}{\mathrm{tr}\left(E_i \rho_\psi E_i^\dagger\right)}$ with probability $\mathrm{tr}(E_i \rho_\psi)$, when S is observed with respect to $(E_i)_{i=1}^m$.

Acknowledgements

The authors thank Harry Buhrman, Matthias Christandl, Sean Clark, Patrick Hayden and Troy Lee for discussions on various aspects of this paper; in particular thanks to Ronald de Wolf for his kind remarks on an earlier version.

MWN is supported by NSERC Canada. SS acknowledges support by the U.K. EPSRC. AM acknowledges support by the U.K. EPSRC's "QIP IRC". AW was supported by the U.K. EPSRC's "QIP IRC" and the EC project QAP (contract no. IST-2005-15848), as well as by a University of Bristol Research Fellowship.

References

[1] D. Avis, J. Hasegawa, Y. Kikuchi and Y. Sasaki, "A quantum protocol to win the graph colouring game on all Hadamard graphs", `arXiv.org:quant-ph/0509047` (2005).

[2] S. Basu, R. Pollack and M. F. Roy, *Algorithms in Real Algebraic Geometry*, Algorithms and Computation in Mathematics, vol. 10, Springer (2006).

[3] B. Bollobás, *Random Graphs*, 2nd ed., Cambridge University Press (2001).

[4] G. Brassard, A. Broadbent and A. Tapp, "Quantum Pseudo-Telepathy", *Found. Physics*, vol. 35, no. 11, pp. 1877–1907 (2005); `arXiv.org:quant-ph/0407221`.

[5] G. Brassard, R. Cleve and A. Tapp, "Cost of Exactly Simulating Quantum Entanglement with Classical Communication", *Phys. Rev. Lett.*, vol. 83, no. 9, pp. 1874–1877 (1999).

[6] H. Buhrman, R. Cleve, J. Watrous and R. de Wolf, "Quantum Fingerprinting", *Phys. Rev. Lett.*, vol. 87, no. 16, 167902 (2001).

[7] H. Buhrman, R. Cleve and A. Wigderson, in *Proc. 30th STOC*, ACM, New York, pp. 63–68 (1998).

[8] P. J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999.

[9] R. Cleve, P. Høyer, B. Toner and J. Watrous, "Consequences and limits of nonlocal strategies", in *Proc. 19th IEEE Annual Conference on Computational Complexity*, pp. 236–249 (2004).

[10] H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, R. Remmert, *Numbers*, Springer Verlag, Graduate Texts in Mathematics (1996).

[11] P. Frankl and V. Rödl, "Forbidden Intersections", *Trans. Amer. Math. Soc.*, vol. 300, no. 1, pp. 259–286 (1987).

[12] V. Galliard and S. Wolf, "Pseudo-telepathy, entanglement, and graph colorings", in *Proc. ISIT 2002*, p. 101 (2002).

[13] V. Galliard, A. Tapp and S. Wolf, "The impossibility of pseudotelepathy without quantum entanglement", in *Proc. ISIT 2003*, p. 457 (2003).

[14] C. D. Godsil and M. W. Newman, "Colouring an Orthogonality Graph", to appear in *SIAM J. Disc. Math.*; `arXiv.org:math.CO/0509151` (2005).

[15] C. D. Godsil, "Interesting Graphs and their Colourings", `http://quoll.uwaterloo.ca/pstuff/index.html` (2003).

[16] P. Hayden, D. W. Leung, P. W. Shor, A. Winter, "Randomizing quantum states: Constructions and applications", *Commun. Math. Phys.*, vol. 250, pp. 371–391 (2004).

[17] F. Juhasz, "The asymptotic behaviour of the Lovász theta function for random graphs", *Combinatorica*, vol. 2, no. 2, pp. 153-155 (1982); A. Coja-Oghlan, "The Lovász Number of Random Graphs", *Comb. Prob. and Comput.*, vol. 14, pp. 439–465 (2005).

[18] G. Lindblad, "A general no-cloning theorem", *Lett. Math. Phys.*, vol. 47, no. 2, pp. 189–196 (1999).

[19] L. Lovasz, "On the Shannon Capacity of a Graph", *IEEE Trans. Inf. Theory*, vol. 25, no. 1, pp. 1–7 (1978).

[20] M. W. Newman, *Independent Sets and Eigenspaces*, PhD thesis, Waterloo, Canada (2005).

[21] O. Ore, "Theory of Graphs", American Mathematical Society, American Mathematical Society Colloquium Publications, Vol. XXXVIII (1962).

[22] A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers, 1993.

[23] S. Severini, "On the digraph of a unitary matrix", *SIAM J. Matrix Analysis App.*, vol. 25, no. 1, pp. 295–300 (2003).

[24] R. de Wolf, *Quantum Computing and Communication Complexity*, PhD thesis, Amsterdam (2001).