Quantum Walks on Generalized Quadrangles

Chris Godsil*
Department of Combinatorics & Optimization
University of Waterloo
Waterloo, Canada
cgodsil@uwaterloo.ca

Krystal Guo†
Department of Mathematics
Université libre de Bruxelles
Brussels, Belgium
guo.krystal@gmail.com

Tor G. J. Myklebust
Department of Combinatorics & Optimization
University of Waterloo
Waterloo, Canada
tmyklebu@uwaterloo.ca

Submitted: Mar 2, 2016; Accepted: Oct 6, 2017; Published: Oct 20, 2017
Mathematics Subject Classifications: 05C50, 81P68

Abstract

We study the transition matrix of a quantum walk on strongly regular graphs. It is proposed by Emms, Hancock, Severini and Wilson in 2006, that the spectrum of $S^+(U^3)$, a matrix based on the amplitudes of walks in the quantum walk, distinguishes strongly regular graphs. We probabilistically compute the spectrum of the line intersection graphs of two non-isomorphic generalized quadrangles of order $(5^2, 5)$ under this matrix and thus provide strongly regular counter-examples to the conjecture.

Keywords: graph isomorphism; quantum computing; graph eigenvalues

1 Introduction

A discrete-time quantum walk is a quantum process on a graph whose state vector is governed by a matrix, called the transition matrix. In [3, 2] Emms, Severini, Wilson and Hancock propose that the quantum walk transition matrix can be used to distinguish between non-isomorphic strongly regular graphs. After experiments on a large set of

*C. Godsil gratefully acknowledges the support of the Natural Sciences and Engineering Council of Canada (NSERC), Grant No. RGPIN-9439.

†This work was done when K. Guo was a graduate student at Simon Fraser University, Burnaby, Canada, and was partially supported by NSERC.

graphs, no strongly regular graph was known to have a cospectral mate with respect to this invariant. In this paper we will compute the spectrum of $S^+(U^3)$ for two particular non-isomorphic graphs and show that they are not distinguished by the spectrum of $S^+(U^3)$.

A *discrete quantum walk* is a process on a graph X governed by a unitary matrix, U, which is called the *transition matrix*. For uv and wx arcs in the digraph of X, the transition matrix is defined to be:

$$U_{wx,uv} = \begin{cases} \frac{2}{d(v)} & \text{if } v = w \text{ and } u \neq x, \\ \frac{2}{d(v)} - 1 & \text{if } v = w \text{ and } u = x, \\ 0 & \text{otherwise.} \end{cases}$$

Let $U(X)$ and $U(H)$ be the transition matrices of quantum walks on X and H respectively. Given a matrix M, the *positive support* of M, denoted $S^+(M)$, is the matrix obtained from M as follows:

$$(S^+(M))_{i,j} = \begin{cases} 1 & \text{if } M_{i,j} > 0 \\ 0 & \text{otherwise.} \end{cases}$$

It is easy to see that if X and H are isomorphic regular graphs, then $S^+(U(X)^3)$ and $S^+(U(H)^3)$ are cospectral. For convenience, we will define $S := S^+(U(X)^3)$ and we will write S or $S^+(U^3)$ to mean $S^+(U(X)^3)$ when the context is clear. The authors of [2, 3] propose that this spectrum is also a complete invariant for strongly regular graphs; they conjecture that the spectrum of the matrix $S^+(U(X)^3)$ distinguishes strongly regular graphs. A graph X on n vertices is *strongly regular* if it is neither complete nor empty, each vertex has k neighbours, each pair of adjacent vertices has a common neighbours and each pair of non-adjacent vertices has c neighbours. The tuple (n, k, a, c) is said to be the *parameter set* of X.

In his Ph.D. thesis [12], Jamie Smith constructs an infinite family of graphs which are not distinguishable by the procedure of Emms et al. These graphs are not strongly regular but are close, in that they have diameter two and four eigenvalues. The eigenvalues of $S^+(U)$ and $S^+(U^2)$ were studied by two of the authors in [4]. Pairs of small regular (but not strongly regular) counterexamples are given in [6]. Computations in Sage [14] show that Hadamard graphs of order n are also not distinguished by the procedure of Emms et al. for $n = 4, 8, 16, 20$ and we conjecture that it is true for all n.

In this article, we give strongly regular counterexamples to the conjecture of Emms et al. by finding a pair of non-isomorphic strongly regular graphs with parameter set $(756, 130, 4, 26)$ which have the same spectrum with respect to $S^+(U^3)$. These strongly regular graphs are the line intersection graphs of the two generalized quadrangles of order $(5^2, 5)$. The line intersection graphs of the two generalized quadrangles of order $(5^2, 5)$ are not distinguished by the procedure of Emms et al.

Since the transition matrices of these graphs are 98280×98280, our computation of their minimal polynomials were done probabilistically. We then determined the eigenvalues and their multiplicities of both matrices, given the minimal polynomials.

2 Generalized quadrangles

The spectrum of $S^+(U^3)$ distinguishes strongly regular graphs for many parameter sets. In particular, the conjecture of Emms et al. was checked for the small strongly regular graphs on less than or equal to 64 vertices found in [13]. Note that the collection of strongly regular graphs in [13] is not complete for graphs up to 64 vertices; for example, the class of strongly regular graphs with parameter set $(57, 24, 11, 9)$, consisting of graphs constructed from Steiner triple systems $S(2, 3, 19)$ is missing. Nevertheless, the procedure of Emms et al. distinguishes many classes of strongly regular graphs and we are motivated to search for strongly regular graphs with more regularity.

It is known for a strongly regular graph that when the Krein bound holds with equality for the diagonal Krein parameter, the second neighbourhood of any vertex is also strongly regular. The parameter set $(756, 130, 4, 26)$ is the smallest parameter set with a pair of non-isomorphic graphs having the property of vanishing Krein parameter. See [1]. We focus on strongly regular graphs with vanishing Krein parameter since the Hadamard graphs, which were also not distinguished by the procedure of Emms. et al. are distance-regular graphs with vanishing Krein parameter.

A generalized quadrangle of order (s, t) is an incidence structure where every point lies on $s+1$ lines and every line contains $t+1$ points. We construct the *line intersection graph* of a generalized quadrangle by taking the lines to be the vertices and two lines are adjacent if they have a common point. The line intersection graph of a generalized quadrangle of order (s, t) is strongly regular with parameter set $((t + 1)(st + 1), s(t + 1), t - 1, s + 1)$. See [11] for the standard text on finite generalized quadrangles.

There are two non-isomorphic generalized quadrangles of order $(5^2, 5)$ which are known in the literature as $H(3, 5^2)$ and FTWKB(5). The description of $H(3, 5^2)$ is given in Section 3.1 of [11]. The generalized quadrangle FTWKB(5) was first discovered by Kantor in [8] and a construction as a flock generalized quadrangle can be found in Section 3.6 of [15]. The graph6 strings available upon request from the second author.

3 Eigenvalue computations

In this section, we describe our computations for the line intersection graphs of the two generalized quadrangles of order $(5^2, 5)$, namely $H(3, 5^2)$ and FTWKB(5).

We used several computer programs, implemented in C++ and using OpenMP [10] and GMP 6.1.0 [5], to do the computations described in the rest of this section:

- A program that, given an implementation of $x \mapsto Ax$ and a prime $p < 2^{31}$, generates Krylov spaces of random vectors over $GF(p)$.
- A program that, given an implementation of $x \mapsto Ax$, a prime $p < 2^{31}$ such that the minimal polynomial of A splits over $GF(p)$, and the distinct eigenvalues of A over $GF(p)$, consumes Krylov spaces and reports lower bounds on eigenspace dimensions.
- A program that, given a graph Z, computes the matrix $S^+(U^3(Z))^2$ and thereby $\mathrm{tr}(S^+(U^3(Z))^1)$, $\mathrm{tr}(S^+(U^3(Z))^2)$, $\mathrm{tr}(S^+(U^3(Z))^3)$, and $\mathrm{tr}(S^+(U^3(Z))^4)$.

- A program for enumerating all solutions to the integer system of equations and inequalities that arises later in this section.

These programs are tailored to the computation described in this section and are not general-purpose; they have been written for inputs corresponding to $H(3,5^2)$ and FTWKB(5). The programs, as well as the graph6 strings of the graphs, are publicly available on the third author's github repository[9].

If $\mathbb{F}$ is a field, A is an $n \times n$ integer matrix and $v \in \mathbb{F}^n$, then the *minimal polynomial of A on the Krylov space generated by v* is the nonzero monic polynomial ψ of least degree such that $\psi(A)v = 0$. This coincides with the minimal polynomial of the restriction of A to the Krylov subspace $\mathrm{Span}(\{v, Av, A^2v, \ldots, A^nv\})$. One can compute the vectors v, Av, A^2v, ... until a linearly dependent set is found. The first linear dependence found yields a relation of the form $A^kv + a_{k-1}A^{k-1}v + \cdots + a_0v$; the minimal polynomial of A on the Krylov space generated by v is then $x^k + a_{k-1}x^{k-1} + \cdots + a_0$.

Note that, if one chooses v uniformly at random from $\mathbb{F}^n$, then the minimal polynomial of A (on $\mathbb{F}^n$) differs from the minimal polynomial of A on the Krylov space generated by v with probability at most $n/|F|$.

A closely-related approach is Wiedemann's algorithm [16]; Wiedemann's algorithm computes, with high probability, the minimal polynomial of a matrix on the Krylov space generated by a vector when $\mathbb{F}$ is a finite field. See [7] for a probabilistic analysis of Wiedemann's algorithm.

Let X be the line intersection graph of $H(3,5^2)$ and let Y be the line intersection graph of FTWKB(5). We probabilistically compute that the minimal polynomials of both $S^+(U(X)^3)$ and $S^+(U(Y)^3)$, modulo every prime between 1999999000 and 1999999180, is as follows:

$$\begin{gathered}(x-1)(x-15)(x-125)(x-127)(x-68005)(x+25)(x+23)(x+9)\\(x^2-5426x+7128229)(x^3+799x^2+122869x-7632765).\end{gathered} \tag{1}$$

Since the minimal polynomial is square-free, $S^+(U(X)^3)$ and $S^+(U(Y)^3)$ are both diagonalizable over every finite field over which the quadratic and cubic factors of (1) split—$GF(1999999151)$ for example.

We further deterministically computed $S^+(U(X)^3)^2$ and $S^+(U(Y)^3)^2$ and obtained the following:

$$\mathrm{tr}(S^+(U(X)^3)) = \mathrm{tr}(S^+(U(Y)^3)) = 98280,$$

$$\mathrm{tr}(S^+(U(X)^3)^2) = \mathrm{tr}(S^+(U(Y)^3)^2) = 6670853280,$$

$$\mathrm{tr}(S^+(U(X)^3)^3) = \mathrm{tr}(S^+(U(Y)^3)^3) = 318986389121400,$$

and

$$\mathrm{tr}(S^+(U(X)^3)^4) = \mathrm{tr}(S^+(U(Y)^3)^4) = 21401273663621790120.$$

Let x_i be the multiplicity of the ith factor appearing in (1) as a factor of the characteristeristic polynomial of $S^+(U(X)^3)$. Since $S^+(U(X)^3)$ and $S^+(U(Y)^3)$ are both irreducible matrices with entries in $\{0,1\}$ the Perron-Frobenius theorem implies that the largest

eigenvalue in amplitude (68005) has multiplicity 1 and so $m_5 = 1$. We probabilistically compute that $m_9 = 105$ and $m_{10} = 680$; we generated 2000 random Krylov spaces modulo 1999999151 and only generated 105 eigenvectors for the 9th factor and 680 eigenvectors for the 10th factor. We get the following system of linear equations

$$\begin{aligned}
m_1 + m_2 + m_3 + m_4 + m_5 + m_6 + m_7 + m_8 + 2m_9 + 3m_{10} &= 98280\\
m_1 + 15m_2 + 125m_3 + 127m_4 + 68005m_5 - 25m_6 - 23m_7 - 9m_8 + 5426m_9 - 799m_{10} &= 98280\\
m_1 + 225m_2 + 15625m_3 + 16129m_4 + 4624680025m_5 &\\
+625m_6 + 529m_7 + 81m_8 + 15185018m_9 + 392663m_{10} &= 6670853280\\
m_1 + 3375m_2 + 1953125m_3 + 2048383m_4 + 314501365100125m_5 &\\
-15625m_6 - 12167m_7 - 729m_8 + 43716137114m_9 - 192667111m_{10} &= 318986389121400\\
m_1 + 50625m_2 + 244140625m_3 + 260144641m_4 + 21387665333634000625m_5 &\\
+390625m_6 + 279841m_7 + 6561m_8 + 128961474307442m_9 + 99596332307m_{10} &= 21401273663621790120
\end{aligned}$$

We substitute the values of m_5, m_9 and m_{10} and simplify to obtain the following linear system of 5 equations in 7 variables:

$$\begin{aligned}
59241m_1 + 17575m_7 + 72896m_8 &= 2544438125\\
-10780m_2 + 1665m_7 + 4556m_8 &= 88344500\\
8525m_3 + 570m_7 + 1088m_8 &= 74452850\\
-11172m_4 + 703m_7 + 1340m_8 &= -20869720\\
12350m_6 + 10545m_7 + 2278m_8 &= 626911750.
\end{aligned} \tag{2}$$

We deterministically computed lower bounds of the remaining multiplicities; we generated Krylov spaces at random and found 2000 linearly independent eigenvectors for each remaining eigenvalue modulo 1999999151. We obtain that $m_i \geqslant 2000$ for $i \in \{1, 2, 3, 4, 6, 7, 8\}$. Solving (2), we find only one positive integer solution satisfying this condition:

$$m_1 = 15625,\ m_2 = 2625,\ m_3 = 4914,\ m_4 = 5460,\ m_6 = 24570,\ m_7 = 27300,\ m_8 = 15625.$$

The same computations were done for $S^+(U(Y)^3)$ and the same arguments follow and so $S^+(U(X)^3)$ and $S^+(U(Y)^3)$ are cospectral.

References

[1] A. Brouwer. Parameters of strongly regular graphs. http://www.win.tue.nl/~aeb/graphs/srg/srgtab.htmlp.

[2] David Emms, Edwin R. Hancock, Simone Severini, and Richard C. Wilson. A matrix representation of graphs and its spectrum as a graph invariant. *Electron. J. Comb.*, 13:#R34, 2006.

[3] David Emms, Simone Severini, Richard C. Wilson, and Edwin R. Hancock. Coined quantum walks lift the cospectrality of graphs and trees. *Pattern Recognition*, 42(9):1988–2002, 2009.

[4] Chris Godsil and Krystal Guo. Quantum walks on regular graphs and eigenvalues. *Electron. J. Comb.*, 18:#P165, 2011.

[5] Torbjrn Granlund and the GMP development team. *GNU MP: The GNU Multiple Precision Arithmetic Library*, 6.1.0 edition, 2015. http://gmplib.org/.

[6] Guo, Krystal. Quantum walks on strongly regular graphs. Master's thesis, University of Waterloo, 2010.

[7] Gavin Harrison, Jeremy Johnson, and B. David Saunders. Probabilistic analysis of Wiedemann's algorithm for minimal polynomial computation. *ACM Commun. Comput. Algebra*, 47(3/4):118–119, January 2014.

[8] William M Kantor. Generalized quadrangles associated with $G_2(q)$. *Journal of Combinatorial Theory, Series A*, 29(2):212 – 219, 1980.

[9] Tor Myklebust. Code for spectrum computations in Guo, K.; Godsil, C.; Myklebust, T. G. J.; "Quantum walks on generalized quadrangles.". https://github.com/tmyklebu/qwalk-gq. Accessed: 2017-09-15.

[10] OpenMP Architecture Review Board. OpenMP application program interface version 3.0, May 2008.

[11] S. E. Payne and J. A. Thas. *Finite Generalized Quadrangles*. Pitman Publishing, London, 1984.

[12] Jamie Smith. *Algebraic Aspects of Multiple-Particle Quantum Walks*. PhD thesis, University of Waterloo, December 2012.

[13] T. Spence. Strongly regular graphs on at most 64 vertices. http://www.maths.gla.ac.uk/~es/srgraphs.php.

[14] W. A. Stein et al. *Sage Mathematics Software (Version 6.1.1)*. The Sage Development Team, 2014. http://www.sagemath.org.

[15] K. Thas. *Symmetry in Finite Generalized Quadrangles*. Frontiers in Mathematics. Birkhäuser Basel, 2014.

[16] Douglas H. Wiedemann. Solving sparse linear equations over finite fields. *IEEE Trans. Information Theory*, 32(1):54–62, 1986.