Quantum Information and Computation, Vol. 8, No. 8&9 (2008) 0715–0721

QUANTUM EXPANDERS FROM ANY CLASSICAL CAYLEY GRAPH EXPANDER

ARAM W. HARROW
Department of Mathematics, University of Bristol, Bristol, U.K.
a.harrow@bris.ac.uk

Received October 10, 2007
Revised February 4, 2008

We give a simple recipe for translating walks on Cayley graphs of a group G into a quantum operation on any irrep of G. Most properties of the classical walk carry over to the quantum operation: degree becomes the number of Kraus operators, the spectral gap lower-bounds the gap of the quantum operation (viewed as a linear map on density matrices), and the quantum operation is efficient whenever the classical walk and the quantum Fourier transform on G are efficient. This means that using classical constant-degree constant-gap families of Cayley expander graphs on groups such as the symmetric group, we can construct efficient families of quantum expanders.

Communicated by: R Cleve & B Terhal

1 Background

Classical expanders can be defined in either combinatorial or spectral terms, while quantum expanders usually have only a spectral definition. Quantum expanders were introduced in [1] for their application to quantum spin chains and in [2] for applications to quantum statistical zero knowledge. Here we (following [1] and [3]) define a (N, D, λ) quantum expander to be a quantum operation $\mathcal{E}$ that

- Has N-dimensional input and output.
- Has $\leq D$ Kraus operators.
- Has second-largest singular value $\leq \lambda$. Equivalently, if $\mathcal{E}(\rho) = \rho$ and $\operatorname{tr} \rho\sigma = 0$ then $\|\mathcal{E}(\sigma)\|_2 \leq \lambda \|\sigma\|_2$, where $\|X\|_2 := \sqrt{\operatorname{tr} X^\dagger X}$.

We say that N is the dimension of the expander, D its degree (by analogy with classical expanders) and $1 - \lambda$ its gap. Note that all quantum operations have at least one fixed state and thus at least one eigenvalue equal to one. The above definition is stricter than the one in [2], which demanded only that an expander increase the von Neumann entropy of a state by at most a constant amount. Finally, we say that an expander is efficient (or "explicit") if it can be implemented on a quantum computer in time poly$(\log N)$. This paper will describe a new method for constructing quantum expanders, which will in some cases yield efficient $(N, O(1), \Omega(1))$ expanders for all values of $N > 1$.

2 Previous work on efficient quantum expanders

In [4] it was shown that, just as random constant-degree graphs are likely to be expander graphs, quantum operations that apply one of a constant number of random unitaries from $U(N)$ are likely to be quantum expanders, with spectral gap approaching the optimal value as $N \to \infty$. Naturally such expanders cannot be efficiently constructed: generic elements of $U(N)$ require $\Theta(N^2)$ gates to construct[5], and if we want to produce the expander deterministically, the only proposed method[3, Sec. 3.3] does an exhaustive search over $\exp(\Omega(N))$ different unitaries. As there are $\log N$ qubits, this could potentially take time doubly-exponential in the number of qubits.

Prescriptions for potentially efficient constructions are given in [1] and [2]. Both begin with classical expanders and turn them into quantum expanders. The proposal in [1] is to start with a so-called "tensor power expander" and then to add phases. A tensor product expander is a degree D graph (V, E) where: (a) each outgoing edge is labelled $1, \ldots, D$, and (b) if G' is the graph with vertices $V \times V$ and edges given by all pairs $(e_1, e_2) \in E \times E$ such that e_1 and e_2 have the same label, then G' is an expander. Unfortunately, when Cayley graphs (see Section 4 for definition) are labeled in the natural way (with label g corresponding to multiplication by group element g) they are not tensor power expanders. It seems plausible that random constant-degree graphs would be tensor power expanders, but this has not been proven.

The approach of [2] is, like this paper, to turn classical Cayley graph expanders into quantum expanders. Its main idea is to apply a classical expander twice: first in the standard basis, and then conjugated by a sort of generalized Hadamard transform (which they call a "good basis change"), so that it acts in a conjugate basis. Unfortunately, the quantum Fourier transform is not, by itself, always enough to make a good basis change. For some groups, such as $SL(2, q)$, it is, and thus [2] obtain a quantum expander based on the classical LPS expander graph. However, it is unknown how to perform the QFT on $SL(2, q)$ efficiently (see [6] for partial progress), and so we do not know how to efficiently perform the basis change required for their construction. On the other hand, while there are groups such as S_n for which both efficient QFT's and explicit constant-degree expanders are known, none have yet been proved to satisfy the additional property needed for the QFT to be a good basis change.

Very recently, two different constructions of efficient, constant-degree quantum expanders have appeared. The first is described in[3]. Their approach is to generalize the classical zig-zag product[7] to quantum expanders, using a constant number of random unitaries[4] for the base case. Like our paper, [3] also describes a family of constant-degree, constant-gap, efficient expanders. A minor advantage of our construction is that it can be made to work for any dimension $N > 1$, while [3] requires that N be of the form D^{8t} for a positive integer t and that $D > D_0$ for a universal constant D_0.

Another efficient constant-degree expander is given in [8]. Their approach is to turn the classical Margulis expander[9] into an operation on quantum phase space. This results in quantum expanders with the same parameters as the Margulis expander (degree 8, second largest eigenvalue $\lambda \leq 2\sqrt{5}/8$) in any dimension, including even infinite dimensional systems. While their paper only describes an efficient construction for dimensions of the form $N = d^n$ for small d, their approach is easily generalized to run in time $\operatorname{poly}\log N$ for any N.

Finally, if we relax the assumption that expanders have constant degree, then efficient constructions have been described in [10,11].

3 Representation theory notation

Let G be a group (either finite or a compact Lie group), and $\hat{G}$ a complete set of inequivalent unitary irreducible representations (irreps). For an irrep $\lambda \in \hat{G}$ and a group element $g \in G$, we denote the representation matrix by $\mathbf{r}_\lambda(g)$, its dimension by d_λ and the space it acts upon by V_λ. Let U_{QFT} be the Fourier transform on G, corresponding to the isomorphism

$$\mathbb{C}[G] \cong \bigoplus_\lambda V_\lambda \otimes V_\lambda^*.$$

It is given by the explicit formula $U_{\mathrm{QFT}} = \sum_{g,\lambda,i,j} \sqrt{d_\lambda/|G|}\mathbf{r}_\lambda(g)_{i,j}|\lambda,i,j\rangle\langle g|$. Let $L_x := \sum_{g\in G}|xg\rangle\langle g|$ denote the left multiplication operator. Then in the Fourier basis, this translates into action on the first tensor factor.

$$U_{\mathrm{QFT}} L_x U_{\mathrm{QFT}}^\dagger = \sum_{\lambda\in\hat{G}} |\lambda\rangle\langle\lambda| \otimes \mathbf{r}_\lambda(x) \otimes I_{d_\lambda}. \tag{1}$$

4 Expander construction

Let G be a group with a generating set $\Gamma \subset G$. Define the Cayley graph $(G;\Gamma)$ to have vertex set G and edges (g, xg) for each $g \in G$ and each $x \in \Gamma$. We will be interested in the case when $(G;\Gamma)$ is an expander graph.

Choose any non-trivial $\lambda \in \hat{G}$. Our quantum expander is defined as follows. Let $\mathcal{E}$ be the quantum operation on V_λ given by

$$\mathcal{E}(\rho) = \frac{1}{|\Gamma|}\sum_{g\in\Gamma} \mathbf{r}_\lambda(g)\rho\,\mathbf{r}_\lambda(g)^\dagger. \tag{2}$$

This operation acts on a d_λ dimensional space by choosing a uniformly random $g \in \Gamma$ and then applying the (unitary) representation matrix $\mathbf{r}_\lambda(g)$. We will see below ways in which $\mathbf{r}_\lambda(g)$ can be implemented on a quantum computer.

I claim that

1. The degree of $\mathcal{E}$ is $\leq |\Gamma|$.
2. If (a) group multiplication in G is efficient, (b) there is a procedure for efficiently sampling from Γ, (c) the QFT on G is efficient and (d) $\log|G| \leq \mathrm{poly}(\log d_\lambda)$, then $\mathcal{E}$ can be implemented efficiently.
3. $$\lambda_2(\mathcal{E}) \leq \lambda_2(W_\Gamma). \tag{3}$$

   Here $\lambda_2(\mathcal{E})$ is the second largest singular value of $\mathcal{E}$, when interpreted as a linear map on density matrices, while $\lambda_2(W_\Gamma)$ is the second-largest singular value of the Cayley graph transition matrix:
   $$W_\Gamma = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\sum_{g\in G}|\gamma g\rangle\langle g|.$$

Thus, classical Cayley graph expanders give quantum expanders.

Proof of claims (1-3). The first claim is immediate. In the second claim, we use the fact that $\mathbf{r}_\lambda(g)$ can be applied to $|\psi\rangle \in V_\lambda$ by performing the inverse QFT on $|\lambda\rangle|\psi\rangle|0\rangle$, applying the map $|x\rangle \to |gx\rangle$, performing the QFT and keeping only the second register (see [12, Chap. 8] for details). Condition (d) is because we say the QFT on G is efficient if it runs in time $\mathrm{poly}(\log|G|)$, but we would like our expander to run in time $\mathrm{poly}(\log d_\lambda)$. Alternatively (a), (c) and (d) can be replaced by any other efficient procedure for performing $\mathbf{r}_\lambda(g)$ on a quantum computer. (See Section 5 for examples.)

The only non-trivial claim above is (3). Assuming that Γ generates G, the unique stationary state of W_Γ is the uniform distribution

$$|u\rangle := \frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle.$$

We can find the second largest eigenvalue by subtracting off a projector onto the stationary state and taking the operator norm. Thus

$$\lambda_2(W_\Gamma) = \|W_\Gamma - |u\rangle\langle u|\,\|_\infty, \tag{4}$$

where $\|M\|_\infty$ is the largest singular value of M.

Similarly, the maximally mixed state $\tau := I_{d_\lambda}/\sqrt{d_\lambda}$ is a stationary state of $\mathcal{E}$. We choose the normalization so that τ will be a unit vector with respect to the Hilbert-Schmidt inner product $\langle A, B\rangle := \operatorname{tr} A^\dagger B$. However, to analyze $\mathcal{E}$ as a linear operator, it is simpler to think of it as acting on vectors. The corresponding linear map is denoted $\hat{\mathcal{E}}$ and is defined to be

$$\hat{\mathcal{E}} := \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\mathbf{r}_\lambda(\gamma)\otimes\mathbf{r}_\lambda(\gamma)^*, \tag{5}$$

where the * denotes the entry-wise complex conjugate with respect to a basis B_λ for V_λ. Then $|\hat\tau\rangle := d_\lambda^{-1/2}\sum_{b\in B_\lambda}|b\rangle\otimes|b\rangle$ is a fixed point of $\hat{\mathcal{E}}$. Thus

$$\lambda_2(\mathcal{E}) = \|\hat{\mathcal{E}} - |\hat\tau\rangle\langle\hat\tau|\,\|_\infty. \tag{6}$$

We now use representation theory to analyze (4) and (6). First, examine (4). Since U_{QFT} is unitary, $\|W_\Gamma - |u\rangle\langle u|\,\|_\infty = \|U_{\mathrm{QFT}}W_\Gamma U_{\mathrm{QFT}}^\dagger - U_{\mathrm{QFT}}\,|u\rangle\langle u|\,U_{\mathrm{QFT}}^\dagger\|_\infty$. Since $U_{\mathrm{QFT}}|u\rangle = |\,\mathrm{trivial}\rangle$, we can use (1) to obtain

$$\lambda_2(W_\Gamma) = \|W_\Gamma - |u\rangle\langle u|\,\|_\infty = \left\|\frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\sum_{\lambda\in\hat G}|\lambda\rangle\langle\lambda|\otimes\mathbf{r}_\lambda(\gamma)\otimes I_{d_\lambda} - |\mathrm{trivial}\rangle\langle\mathrm{trivial}|\right\|_\infty \tag{7}$$

$$= \left\|\frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\sum_{\substack{\lambda\in\hat G\\ \lambda\neq\mathrm{trivial}}}|\lambda\rangle\langle\lambda|\otimes\mathbf{r}_\lambda(\gamma)\otimes I_{d_\lambda}\right\|_\infty \tag{8}$$

$$= \max_{\lambda\neq\mathrm{trivial}}\left\|\frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\mathbf{r}_\lambda(\gamma)\right\|_\infty \tag{9}$$

A similar argument applies to (6) as well. Here the first step is to decompose $V_\lambda \otimes V_\lambda^*$ into irreps of G. In general,

$$V_\lambda \otimes V_\lambda^* \cong \bigoplus_{\nu \in \hat{G}} V_\nu \otimes \mathbb{C}^{m_\nu},$$

where m_ν is the multiplicity (possibly zero) of V_ν in $V_\lambda \otimes V_\lambda^*$. Let $U_{\rm CG}$ be the unitary transform implementing the above isomorphism. Then by definition,

$$U_{\rm CG}\left(\mathbf{r}_\lambda(g) \otimes \mathbf{r}_\lambda(g)^*\right) U_{\rm CG}^\dagger = \sum_{\nu \in \hat{G}} |\nu\rangle\langle\nu| \otimes \mathbf{r}_\nu(g) \otimes I_{m_\nu}. \tag{10}$$

We can use this to analyze the spectrum of $\mathcal{E}$. In particular

$$U_{\rm CG}\hat{\mathcal{E}}U_{\rm CG}^\dagger = \sum_{\nu \in \hat{G}} |\nu\rangle\langle\nu| \otimes \left(\frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma} \mathbf{r}_\nu(\gamma)\right) \otimes I_{m_\nu}. \tag{11}$$

From Schur's Lemma, we know that $m_{\rm trivial} = 1$, corresponding to the stationary state $|\hat{\tau}\rangle$. Thus

$$\begin{aligned}
\lambda_2(\mathcal{E}) &= \|\mathcal{E} - |\hat{\tau}\rangle\langle\hat{\tau}|\,\|_\infty && (12)\\
&= \|U_{\rm CG}(\mathcal{E} - |\hat{\tau}\rangle\langle\hat{\tau}|)U_{\rm CG}^\dagger\|_\infty && (13)\\
&= \max_{\substack{m_\nu \neq 0\\ \nu\neq \text{trivial}}} \left\|\frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\mathbf{r}_\nu(\gamma)\right\|_\infty && (14)\\
&\leq \max_{\nu\neq \text{trivial}} \left\|\frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\mathbf{r}_\nu(\gamma)\right\|_\infty && (15)\\
&= \lambda_2(W_\Gamma). && (16)
\end{aligned}$$

This completes the proof □.

5 Examples of quantum expanders

If $G = S_n$ then we can use the explicit expander of [13] and the efficient QFT of [14]. The dimension $N = d_\lambda$ can be the size of any irrep of S_n, which asymptotically can be as large as $\sqrt{n!}\exp(-O(\sqrt{n}))$. Run-time is thus poly-logarithmic in the dimension, meaning polynomial in the number of qubits. However if we would like an expander on exactly N dimensions, we are not guaranteed that $n \leq \text{poly}\log(N)$ exists such that $d_\lambda = N$ for some $\lambda \in \hat{S}_n$, nor do we know how to efficiently check, for a given n, whether such a λ exists. (For completeness, we mention here that irreps of S_n are labeled by partitions $(\lambda_1, \ldots, \lambda_n)$ with $\lambda_1 + \ldots + \lambda_n = n$ and $\lambda_1 \geq \ldots \geq \lambda_n \geq 0$. Their dimension is given by $d_\lambda = n! \prod_{i<j}(\lambda_i - \lambda_j - i + j)/\prod_i(\lambda_i + n - i)!$.)

Some other Cayley graph constructions also carry over. For example, the (classical) zig-zag product can be interpreted as a Cayley graph, where the group is an iterated wreath product[15]. Additionally, the irreps of these wreath products are large (although also with possibly inconvenient dimensions) and quantum Fourier transforms on them can be performed efficiently[6]. Thus, classical zig-zag product expanders can also be used to construct efficient, constant-degree, constant-gap quantum expanders. (We remark in passing that this construction appears not to be related to the quantum zig-zag product of [3].)

If we permit approximate constructions then we can relax the assumption that G is finite. For example, if $G = SU(2)$ then several explicit expanders are known[16, 17], but no efficient circuits are yet known for the QFT. It would suffice even to be able to implement $\mathbf{r}_\lambda(g)$ in time poly-logarithimic in d_λ. This latter result is claimed by [18], but the algorithm there is missing crucial steps.

Finally, to construct expanders for any dimension $N > 1$ we can use the fact that the S_{N+1}-irrep $\lambda = (N, 1)$ has dimension N. To implement $\mathbf{r}_\lambda(\pi)$ for $\pi \in S_{N+1}$ we cannot use the QFT on S_{N+1}, since our run-time needs to be $\operatorname{poly}\log(N)$. However, we can instead embed V_λ into the $N+1$-dimensional defining representation of S_{N+1}, which is given by $\mathbf{r}_{\rm def}(\pi)|x\rangle = |\pi(x)\rangle$ for $x = 1, \ldots, N+1$. This representation is reducible and decomposes into one copy of trivial representation (spanned by $|1\rangle + \ldots + |N+1\rangle$) and one copy of the N-dimensional irrep $V_{(N,1)}$. To embed V_λ in the defining representation, we can use any $N+1$-dimensional unitary that maps $|N+1\rangle$ to $\frac{1}{\sqrt{N+1}}\sum_{x=1}^{N+1}|x\rangle$. Then performing $\mathbf{r}_{\rm def}(\pi_j)$ (for Cayley graph generator π_j) requires only that $\pi_j(x)$ be computable from j and x in time $\operatorname{poly}(\log N)$. A careful examination of the construction of [13] shows this to be the case. Thus, this technique yields constant-degree, constant-gap explicit expanders for any dimension $N > 1$. (Of course, for low enough values of N the degree will be larger than N^2 and so the resulting expander will be inferior to the trivial "expander" which applies a random generalized Pauli matrix.)

Acknowledgments

I would like to thank Avi Ben-Aroya for useful comments on the first arXiv version of this paper, Matt Hastings for many interesting conversations on this subject, and Cris Moore for pointing out [13] and crucially asking why any classical expander couldn't be turned into a quantum expander. I am also grateful to the Oza family for their kind hospitality while I did most of this work. My funding is from the Army Research Office under grant W9111NF-05-1-0294, the European Commission under Marie Curie grants ASTQIT (FP6-022194) and QAP (IST-2005-15848), and the U.K. Engineering and Physical Science Research Council through "QIP IRC."

References

1. M. B. Hastings, *Entropy and Entanglement in Quantum Ground States*, Phys. Rev. B **76** (2007), 035114, available at arXiv:cond-mat/0701055.
2. A. Ben-Aroya and A. Ta-Shma, *Quantum expanders and the quantum entropy difference problem*, 2007, arXiv:quant-ph/0702129.
3. A. Ben-Aroya, O. Schwartz, and A. Ta-Shma, *An explicit construction of quantum expanders*, 2007, arXiv:0709.0911.
4. M.B. Hastings, *Random unitaries give quantum expanders*, Phys. Rev. A **76** (2007), 032315, available at arXiv:0706.0556.
5. V.V. Shende, S.S. Bullock, and I.L. Markov, *Synthesis of quantum logic circuits*, IEEE Trans. on Computer-Aided Design **25** (2006), no. 6, 1000–1010, available at arXiv:quant-ph/0406176.
6. C. Moore, D. N. Rockmore, and A. Russell, *Generic quantum Fourier transforms*, Proc. 15th SODA, 2004, pp. 778–787, available at arXiv:quant-ph/0304064.

7. O. Reingold, S. Vadhan, and A. Wigderson, *Entropy waves, the zig-zag product and new constant-degree expanders*, Annals of Mathematics **155** (2002), no. 1, 157–187.
8. J. Eisert and D. Gross, *Quantum Margulis Expanders*, Quan. Info. & Comp. **8** (2008), no. 8-9, 0722, available at arXiv:0710.0651.
9. G.A. Margulis, *Explicit constructions of expanders*, Problemy Peredači Informacii **9** (1973), no. 4, 71–80.
10. A. Ambainis and A. Smith, *Small Pseudo-random Families of Matrices: Derandomizing Approximate Quantum Encryption.*, APPROX-RANDOM, 2004, pp. 249–260, available at arXiv: quant-ph/0404075.
11. P. Dickinson and A. Nayak, *Approximate randomization of quantum states with fewer bits of key*, Quantum Computing: Back Action 2006, 2006, pp. 18–36, DOI 10.1063/1.2400876, available at arXiv:quant-ph/0611033.
12. A.W. Harrow, *Applications of coherent classical communication and the Schur transform to quantum information theory*, Ph.D. thesis, Massachusetts Institute of Technology, 2005, arXiv: quant-ph/0512255.
13. M. Kassabov, *Symmetric groups and expanders*, Inventiones Mathematicae **170** (2007), no. 2, available at arXiv:math.GR/0505624.
14. R. Beals, *Quantum computation of Fourier transforms over symmetric groups*, Proc. 29th STOC, 1997, pp. 48–53.
15. E. Rozenman, A. Shalev, and A. Wigderson, *A new family of Cayley expanders*, Proc. 36th STOC, 2004, pp. 445–454.
16. J. Bourgain and A. Gamburd, *New results on expanders*, C. R. Acad. Sci. Paris, Ser. I **342** (2006), 717–721.
17. A. Gamburd, D. Jakobson, and P. Sarnak, *Spectra of elements in the group ring of* $SU(2)$, J. Eur. Math. Soc. **1** (1999), 51–85.
18. C. Zalka, *Implementing high dimensional unitary representations of SU(2) on a Quantum Computer*, 2004, arXiv:quant-ph/0407140.