Quantum expanders from any classical Cayley graph expander

Aram Harrow (Bristol)

QIP “08”

19 Dec 2007

arXiv:0709.1142
Main result.

Definitions.

Proof of main result.

Applying the recipe: examples of quantum Cayley graph expanders.

Related work.

Coming attractions: tensor product expanders and k-designs.
The result

Given:

1. A classical Cayley graph expander on a group $G$ with gap $1 - \lambda_2$ and degree $d$.

2. An irrep $\mu(g)$ of $G$ with dimension $N$.

3. An efficient method of implementing $\mu(g)$ (such as a QFT on $G$).

We have:

An efficient quantum expander with dimension $N$, degree $d$ and gap $\geq 1 - \lambda_2$. 
Definition: Cayley graph

Cayley graph:

1. Given by a group $G$ and a generating set $D$. $d = |D|$
2. Vertices are elements of $G$.
3. Neighbours of $g \in G$ are $\{xg : x \in D\}$. Graph is $d$-regular.
Example: cyclic group

\[ G = \mathbb{Z}_6 \]
\[ D = \{2, 3\} \]

\[
W = \frac{1}{|D|} \sum_{x \in D} L_x = \frac{1}{2} \begin{pmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0
\end{pmatrix}
\]
**Definition: expander**

(Classical) expander graph.
Really a family of graphs with $N \to \infty$ vertices and degree $d=O(1)$.

**Combinatorial definition**: Any not-too-big subset of vertices has lots of neighbours.

**Spectral definition**: The random walk matrix on the graph has second-largest eigenvalue $\lambda_2 = 1 - \Omega(1)$.

---

**Quantum expander**: Spectral definition only.

A family of quantum operations $\mathcal{E}$ acting on an $N$-dim system.
$d=O(1)$ Kraus operators.
(Typically proportional to unitaries, so $\mathcal{E}(I/N) = I/N$.)

**Spectral gap**: As a linear operator on density matrices, $\lambda_2(\mathcal{E}) = 1 - \Omega(1)$. 
**Representation theory defs**

**Irrep**: $\mu$ is a map from $G$ to operators on $V_\mu$ such that $V_\mu$ has no non-trivial $\mu$-invariant subspace.

Efficiently implementing $\mu(g)$ means taking time $\text{poly}(\log N)$ to apply $\mu(g)$ to a $\log N$ - qubit register. $N := d_\mu = \dim V_\mu$.

**Quantum Fourier Transform**: $U_{\text{QFT}}$

Implements isomorphism $\mathbb{C}[G] \cong \bigoplus_{\mu} V_\mu \otimes V_\mu^*$

$L_x$ is the left-multiplication operator: $L_x|g\rangle = |xg\rangle$

Then $U_{\text{QFT}}L_xU_{\text{QFT}}^\dagger = \sum_{\mu \in \hat{G}} |\mu\rangle\langle \mu| \otimes \mu(x) \otimes I_{d_\mu}$.

So, if $U_{\text{QFT}}$ and $L_x$ can be implemented efficiently, then so can $\mu(x)$. (Assuming that poly($\log |G|$) is the same as poly($\log d_\mu$).)
spectra of Cayley graphs

The walk operator is

$$W = \frac{1}{|D|} \sum_{x \in D} L_x .$$

The (normalised) stationary distribution is

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

In the Fourier basis

The walk operator is

$$\sum_{\mu} |\mu\rangle\langle\mu| \otimes \frac{1}{|D|} \sum_{x \in D} \mu(x) \otimes I_{d_\mu} .$$

The stationary distribution is

$$|\mu=\text{trivial}\rangle \otimes 10 \otimes 10 .$$

The second largest eigenvalue is

$$\lambda_2(W) = \max_{\mu \neq \text{trivial}} \left\| \frac{1}{|D|} \sum_{x \in D} \mu(x) \right\|_\infty .$$
Example: cyclic group

\[ G = \mathbb{Z}_6 \]
\[ D = \{2,3\}. \]

Fourier basis:
\[ \mu_k(x) = \omega^{kx} \]
\[ \omega = e^{2\pi i/6} \]

\[ W = \frac{1}{|D|} \sum_{x \in D} \sum_{k \in \{0,1,2,3,4,5\}} \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \]

Warning!
Abelian groups can’t have \( O(1) \) degree, \( \Omega(1) \) gap.
### Example: symmetric group

\( G = S_3 \)

\( D = \{(12), (123)\} \)

| \( \mu \)       | \( \frac{1}{|D|} \sum_{x \in D} \mu(x) \) |
|------------------|------------------------------------------|
| trivial          | 1                                        |
| sign             | 0                                        |
| 2-dim            | \( \frac{1}{4} \left( \begin{array}{cc} -1 + i\sqrt{3} & 2 \\ 2 & -1 - i\sqrt{3} \end{array} \right) \) |

\( \lambda_2 = \frac{1}{2} \)
The quantum expander construction

Given a classical Cayley graph with generators $D \subset G$

and given an irrep $\mu$;

the quantum expander is:

$$\mathcal{E}(\rho) = \frac{1}{|D|} \sum_{x \in D} \mu(x) \rho \mu(x)^\dagger$$

# Kraus operators = $|D|$ = degree of classical expander

$\mathcal{E}$ is efficient if $\mu(x)$ is efficient.

It remains to show that $\lambda_2(\mathcal{E}) \leq \lambda_2(W)$. 
Analysis of quantum expander

$$\mathcal{E}(\rho) = \frac{1}{|D|} \sum_{x \in D} \mu(x) \rho \mu(x)^\dagger$$

As a linear operator (instead of a super-operator), this is:

$$\hat{\mathcal{E}} = \frac{1}{|D|} \sum_{x \in D} \mu(x) \otimes \mu(x)^*$$

We want $\lambda_2(\hat{\mathcal{E}})$.

Now the inevitable representation theory:

$\mu \otimes \mu^*$ is a reducible representation of $G$, and can be decomposed into irreps. If $\nu$ appears with multiplicity $m_\nu$, then

$$\mu(x) \otimes \mu(x)^* \cong \sum_{\nu} |\nu\rangle \langle \nu| \otimes \nu(x) \otimes I_{m_\nu}$$

AND! Schur’s Lemma says $m_{\text{trivial}} = 1$. 
Analysis of quantum expander

\[ \hat{\mathcal{E}} = \frac{1}{|D|} \sum_{x \in D} \mu(x) \otimes \mu(x)^* \]

\[ \cong \sum_{\nu} |\nu\rangle\langle\nu| \otimes \left( \frac{1}{|D|} \sum_{x \in D} \nu(x) \right) \otimes I_{m_\nu} \]

\( m_{\text{trivial}} = 1 \) corresponds to \( \lambda_1 = 1 \).

The second largest eigenvalue is

\[ \lambda_2(\hat{\mathcal{E}}) = \max_{\nu \neq \text{trivial}} \left\| \frac{1}{|D|} \sum_{x \in D} \nu(x) \right\|_{\infty} \]

\[ \leq \max_{\nu \neq \text{trivial}} \left\| \frac{1}{|D|} \sum_{x \in D} \nu(x) \right\|_{\infty} = \lambda_2(W) \]

Q.E.D.
Applying the recipe

Recall: We want run-time to be $\text{poly}(\log d_\mu)$, but implementing $\mu$ using a QFT usually requires $\text{poly}(\log |G|)$ time. This works when $d_\mu$ is sufficiently large.

**PSL(2, $\mathbb{F}_q$):** The LPS expander. $d=6, \lambda_2 = \sqrt{5} / 3$.
Irreps are large, but no efficient QFT is known. **DOESN'T WORK**

**SU(2):** Another LPS expander. $d=6, \lambda_2 = \sqrt{5} / 3$.
Irreps are large, but no efficient QFT is known. quant-ph/0407140 claims to implement $\mu(x)$ in time $\text{poly}(\log d_\mu)$, but the algorithm is incomplete. **DOESN'T WORK**
Applying the recipe

\( S_n \): The Kassabov expander. \( d=O(1), \lambda_2 = 1-\Omega(1) \)
Irreps are large: \( \log d_\mu \approx (\log |S_n|) / 2 \)
QFT runs in \( \text{poly}(\log |S_n|) = \text{poly}(n) \).

\( S_{N+1} \): The Kassabov expander. \( d=O(1), \lambda_2 = 1-\Omega(1) \)
There is an \( N \)-dimensional irrep that can be directly implemented in time \( \text{poly}(\log N) \).

\( H \uparrow H \uparrow \ldots \): zig-zag product [Rozenman-Shalev-Wigderson]
\( |H| = O(1). H=[H,H] \).
Has large irreps and efficient QFT.

\( \text{Aff}(2, F_q) \): Margulis expander. \( d=8, \lambda_2 \leq 5\sqrt{2} / 8 \).
No efficient QFT but one irrep can be efficiently constructed. [Eisert-Gross; 0710.0651]

Related work

**quantum zig-zag product:**
[Ben-Aroya, Schwartz, Ta-Shma; 0709.0911]
Not the same as applying my construction to the classical zig-zag product.

Another QFT-based construction:
[Ben-Aroya, Ta-Shma; 0702129]
Not yet known to be efficient.

**Quantum Margulis expanders**
[Eisert-Gross; 0710.0651]
Also yields efficient constant-gap, constant-degree expanders for any dimension.
Coming attractions!

expander

approx. 1-design
\{p_i, U_i\} s.t.

\[ \sum_i p_i U_i \rho U_i^\dagger \approx \int dU \ U \rho U^\dagger \]

approx. k-design
\{p_i, U_i\} s.t.

\[ \sum_i p_i U_i \otimes^k \rho(U_i^\dagger) \otimes^k \approx \int dU \ U \otimes^k \rho(U^\dagger) \otimes^k \]

k-tensor product expander

with M. Hastings: random unitaries are tensor product expanders.

with R. Low: random circuits are tensor product expanders. (we think)
THANKS