An Explicit Construction of Quantum Expanders

Avraham Ben-Aroya ∗ Oded Schwartz † Amnon Ta-Shma ‡

Abstract

Quantum expanders are a natural generalization of classical expanders. These objects were introduced and studied by [1, 3, 4]. In this note we show how to construct explicit, constant-degree quantum expanders. The construction is essentially the classical Zig-Zag expander construction of [5], applied to quantum expanders.

1 Introduction

Classical expanders are graphs of low degree and high connectivity. One way to measure the expansion of a graph is through the second eigenvalue of its adjacency matrix. This paper investigates the quantum counterpart of these objects, defined as follows. For a linear space $V$ we denote by $L(V)$ the space of linear operators from $V$ to itself.

Definition 1.1. We say an admissible superoperator $G : L(V) \to L(V)$ is $D$-regular if $G = \frac{1}{D} \sum_d G_d$, and for each $d \in [D]$, $G_d(X) = U_d X U_d^\dagger$ for some unitary transformation $U_d$ over $V$.

Definition 1.2. An admissible superoperator $G : L(V) \to L(V)$ is a $(N, D, \lambda)$ quantum expander if $\dim(V) = N$, $G$ is $D$-regular and:

- $G(\hat{I}) = \hat{I}$, where $\hat{I}$ denotes the completely-mixed state.

- For any $\rho \in L(V)$ that is orthogonal to $\hat{I}$ (with respect to the Hilbert-Schmidt inner product, i.e. $\text{Tr}(\rho \hat{I}) = 0$) it holds that $\| G(A) \| \leq \lambda \| A \|$ (where $\| X \| = \sqrt{\text{Tr}(XX^\dagger)}$).

A quantum expander is explicit if $G$ can be implemented by a quantum circuit of size polynomial in $\log(N)$.

The notion of quantum expanders was introduced and studied by [1, 3, 4]. These papers gave several constructions and applications of these objects. The disadvantage of all the constructions given by these papers is that each construction is either constant-degree or explicit, but not both. In this paper we show how to construct explicit quantum expanders of constant-degree. Our construction is an easy generalization of the Zig-Zag expander construction given in [5].

∗Schools of Computer Science, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv 69978, Israel. Email: abrahambe@post.tau.ac.il.
†School of Computer Science, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel. Email: odedsc@tau.ac.il.
‡School of Computer Science, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel. Email: amnon@tau.ac.il.
2 Preliminaries

We denote by $\mathcal{H}_N$ the Hilbert space of dimension $N$.

For a linear space $\mathcal{V}$, we denote by $L(\mathcal{V})$ the space of linear operators from $\mathcal{V}$ to itself. We use the Hilbert-Schmidt inner product on this space, i.e. for $X, Y \in L(\mathcal{V})$ their inner product is $\langle X, Y \rangle = \text{Tr}(XY^\dagger)$. The inner product gives rise to a norm $\|X\| = \sqrt{\langle X, X \rangle} = \sqrt{\sum s_i(X)^2}$, where $\{s_i(X)\}$ are the singular values of $X$. Throughout the paper this is the only norm we use.

We also denote by $U(\mathcal{V})$ the set of all unitary operators on $\mathcal{V}$, and by $T(\mathcal{V})$ the space of superoperators on $\mathcal{V}$ (i.e. $T(\mathcal{V}) = L(L(\mathcal{V}))$).

Finally, we denote by $I$ the identity operator normalized such that $\text{Tr}(I) = 1$. That is, $I$ denotes the completely mixed state (on the appropriate space).

3 Explicit constant-degree quantum expanders

3.1 The basic operations

The construction uses as building blocks the following operations:

- **Squaring**: For a superoperator $G \in T(\mathcal{V})$ we denote by $G^2$ the superoperator given by $G^2(X) = G(G(X))$ for any $X \in L(\mathcal{V})$.

- **Tensoring**: For superoperators $G_1 \in T(\mathcal{V}_1)$ and $G_2 \in T(\mathcal{V}_2)$ we denote by $G_1 \otimes G_2$ the superoperator given by $(G_1 \otimes G_2)(X \otimes Y) = G_1(X) \otimes G_2(Y)$ for any $X \in L(\mathcal{V}_1), Y \in L(\mathcal{V}_2)$.

- **Zig-Zag product**: For superoperators $G_1 \in T(\mathcal{V}_1)$ and $G_2 \in T(\mathcal{V}_2)$ we denote by $G_1 \oplus G_2$ their Zig-Zag product. A formal definition of this is given in Section 4. The only requirement is that $G_1$ is dim(\mathcal{V}_2)-regular.

**Proposition 3.1.** If $G$ is a $(N, D, \lambda)$ quantum expander then $G^2$ is a $(N, D^2, \lambda^2)$ quantum expander. If $G$ is explicit then so is $G^2$.

**Proposition 3.2.** If $G_1$ is a $(N_1, D_1, \lambda_1)$ quantum expander and $G_2$ is a $(N_2, D_2, \lambda_2)$ quantum expander then $G_1 \otimes G_2$ is a $(N_1 \cdot N_2, D_1 \cdot D_2, \max(\lambda_1, \lambda_2))$ quantum expander. If $G_1$ and $G_2$ are explicit then so is $G_1 \otimes G_2$.

The proofs of Propositions 3.1 and 3.2 are trivial. The proof of Theorem 1 is given in Section 4.

3.2 The construction

The construction starts with some constant-degree quantum expander, and iteratively increases its size via alternating operations of squaring, tensoring and Zig-Zag products. The tensoring is used to square the dimension of the superoperator. Then a squaring operation improves the second eigenvalue. Finally, the Zig-Zag product reduces the degree, without deteriorating the second eigenvalue too much.
Suppose $H$ is a $(D^8, D, \lambda)$ quantum expander. We define a series of superoperators as follows. The first two superoperators are $G_1 = H^2$ and $G_2 = H \otimes H$. For every $t > 2$ we define

$$G_t = \left( G_{\left[\frac{t+1}{2}\right]} \otimes G_{\left[\frac{t-1}{2}\right]} \right)^2 \otimes H.$$ 

**Theorem 2.** For every $t > 0$, $G_t$ is an explicit $(D^{8^t}, D^2, \lambda_t)$ quantum expander with $\lambda_t = \lambda + O(\lambda^2)$.

The proof of this Theorem for classical expanders was given in [3]. The proof only relies on the properties of the basic operations. Proposition 3.1, Proposition 3.2 and Theorem 1 assure the required properties of the basic operations are satisfied in the quantum case as well. Hence, the proof of this theorem is identical to the one in [5] (Theorem 3.3) and we omit it.

### 3.3 The base superoperator

Theorem 2 relies on the existence of a good base superoperator $H$. In the classical setting, the probabilistic method assures us that a good base graph exists, and so we can use an exhaustive search to find one. The quantum setting exhibits a similar phenomena:

**Theorem 3.** ($[2]$) There exists a $D_0$ such that for every $D > D_0$ there exist a $(D^8, D, \lambda)$ quantum expander for $\lambda = \frac{4 \sqrt{D - 1}}{D}$.

We will use an exhaustive search to find such a quantum expander. To do this we first need to transform the searched domain from a continuous space to a discrete one. We do this by using a net of unitary matrices, $S \subset U(\mathcal{H}_{D^8})$. $S$ has the property that for any unitary matrix $U \in U(\mathcal{H}_{D^8})$ there exists some $V_U \in S$ such that

$$\sup_{\|X\|=1} \left\| UXU^\dagger - V_U XV_U^\dagger \right\| \leq \lambda.$$ 

It is not hard to verify that indeed such $S$ exists, with size depending only on $D$ and $\lambda$. Moreover, we can find such a set in time depending only on $D$ and $\lambda$.

Suppose $G$ is a $(D^8, D, \lambda)$ quantum expander, $G(X) = \frac{1}{D} \sum_{i=1}^{D} U_i X U_i^\dagger$. We denote by $G'$ the superoperator $G'(X) = \frac{1}{D} \sum_{i=1}^{D} V_U X V_U^\dagger$. Let $X \in L(\mathcal{H}_{D^8})$ be orthogonal to $I$. Then:

$$\| G'(X) \| = \left\| \frac{1}{D} \sum_{i=1}^{D} V_i X V_i^\dagger \right\| \leq \left\| \frac{1}{D} \sum_{i=1}^{D} U_i X U_i^\dagger \right\| + \frac{1}{D} \sum_{i=1}^{D} \left\| U_i X U_i^\dagger - V_i X V_i^\dagger \right\| \leq \| G(X) \| + \lambda \| X \| \leq 2\lambda \| X \|.$$ 

Hence, $G'$ is a $(D^8, D, \frac{8(\sqrt{D} - 1)}{D})$ quantum expander. This implies that we can find a good base superoperator in time which depends only on $D$ and $\lambda$.

---

1. [3] actually shows that for any $D$ there exist a $(D^8, D, (1 + O(D^{-16/15} \log D)) \frac{2 \sqrt{D - 1}}{D})$ quantum expander.
2. One way to see this is using the Solovay-Kitaev theorem (see, e.g., [2]). The theorem assures us that, for example, the set of all the quantum circuits of length $O(\log^4 \epsilon^{-1})$ generated only by Hadamard and Toffoli gates give an $\epsilon$-net of unitaries. The accuracy of the net is measured differently in the Solovay-Kitaev theorem, but it can be verified that the accuracy measure we use here is roughly equivalent.
3. We can actually get an eigenvalue bound of $(1 + \epsilon) \frac{2 \sqrt{D - 1}}{D}$ for an arbitrary small $\epsilon$ on the expense of increasing $D_0$. 

---

3
4 The Zig-Zag product

Suppose \( G_1, G_2 \) are two superoperators, \( G_i \in T(\mathcal{H}_{N_i}) \), and \( G_i \) is a \((N_i, D_i, \lambda_i)\) quantum expander. We further assume that \( N_2 = D_1 \). \( G_1 \) is \( D_1\)-regular and so it can be expressed as \( G_1(X) = \frac{1}{D_1} \sum_d U_d X U_d^\dagger \)
for some unitaries \( U_d \in U(\mathcal{H}_{N_1}) \). We lift the ensemble \( \{U_d\} \) to a superoperator \( \hat{U} \in L(\mathcal{H}_{N_1} \otimes \mathcal{H}_{D_1}) \)
defined by:

\[
\hat{U}(|a\rangle \otimes |b\rangle) = U_b |a\rangle \otimes |b\rangle,
\]
and we define \( \hat{G}_1 \in T(\mathcal{H}_{N_1} \otimes \mathcal{H}_{D_1}) \) by \( \hat{G}_1(X) = \hat{U} X \hat{U}^\dagger \).

**Definition 4.1.** Let \( G_1, G_2 \) be as above. The Zig-Zag product,\( G_1 \otimes G_2 \in T(\mathcal{H}_{N_1} \otimes \mathcal{H}_{D_1}) \), is defined to be \( (G_1 \otimes G_2)X = (I \otimes G_2) \hat{G}_1(I \otimes G_2^\dagger)X \).

We claim:

**Proposition 4.2.** For any \( X, Y \in L(\mathcal{H}_{N_1} \otimes \mathcal{H}_{D_1}) \) such that \( X \) is orthogonal to the identity operator we have:

\[
| \langle G_1 \otimes G_2 X , Y \rangle | \leq f(\lambda_1, \lambda_2) \| X \| \cdot \| Y \|
\]

where \( f(\lambda_1, \lambda_2) = \lambda_1 + \lambda_2 + \lambda_2^2 \).

And as a direct corollary we get:

**Theorem 1.** If \( G_1 \) is a \((N_1, D_1, \lambda_1)\) quantum expander and \( G_2 \) is a \((D_1, D_2, \lambda_2)\) quantum expander then \( G_1 \otimes G_2 \) is a \((N_1 \cdot D_1, D_2^2, \lambda_1 + \lambda_2 + \lambda_2^2)\) quantum expander. If \( G_1 \) and \( G_2 \) are explicit then so is \( G_1 \otimes G_2 \).

**Proof:** Let \( X \) be orthogonal to \( I \) and let \( Y = (G_1 \otimes G_2)X \). By Proposition 4.2 \( \| Y \|^2 \leq f(\lambda_1, \lambda_2) \| X \| \cdot \| Y \|. \) Equivalently, \( \| (G_1 \otimes G_2)X \| \leq f(\lambda_1, \lambda_2) \| X \| \) as required.

The explicitness of \( G_1 \otimes G_2 \) is immediate from the definition of the Zig-Zag product.

We now turn to the proof of Proposition 4.2. We adapt the proof given in [5] for the classical case to the quantum setting. For that we need to work with linear operators instead of working with vectors. Consequently, we replace the vector inner-product used in the classical proof with the Hilbert-Schmidt inner product on linear operators, and replace the Euclidean norm on vectors, with the \( \text{Tr}(XX^\dagger) \) norm on linear operators. Interestingly, the same proof carries over to this generalized setting. One can get the proof below by simply going over the proof in [5] and doing the above translation. We provide the details here for completeness.

**Proof of Proposition 4.2** We first decompose the space \( L(\mathcal{H}_{N_1} \otimes \mathcal{H}_{D_1}) \) to

\[
W^\| = \text{Span} \left\{ \sigma \otimes I \mid \sigma \in L(\mathcal{H}_{N_1}) \right\} \text{ and,} \\
W^\perp = \text{Span} \left\{ \sigma \otimes \tau \mid \sigma \in L(\mathcal{H}_{N_1}) , \tau \in L(\mathcal{H}_{D_1}) , \langle \tau, I \rangle = 0 \right\}.
\]
Decompose $X$ to $X = X^\parallel + X^\perp$, where $X^\parallel \in W^\parallel$ and $X^\perp \in W^\perp$, and similarly $Y = Y^\parallel + Y^\perp$. By definition,

$$\langle G_1 \otimes G_2 X, Y \rangle = |\langle (I \otimes G_2) \hat{G}_1(I \otimes G_1^\dagger) X, Y \rangle| = |\langle \hat{G}_1(I \otimes G_2)(X^\parallel + X^\perp), (I \otimes G_2)(Y^\parallel + Y^\perp) \rangle|.$$ 

Opening to the four terms and pushing the absolute value inside, we see that

$$\langle G_1 \otimes G_2 X, Y \rangle \leq |\langle \hat{G}_1(I \otimes G_2)X^\parallel, (I \otimes G_2)Y^\parallel \rangle| + |\langle \hat{G}_1(I \otimes G_2)X^\perp, (I \otimes G_2)Y^\perp \rangle| + |\langle \hat{G}_1X^\parallel, (I \otimes G_2)Y^\parallel \rangle| + |\langle \hat{G}_1X^\perp, (I \otimes G_2)Y^\perp \rangle|$$

Where the last equality is due to the fact that $I \otimes G_2$ is identity over $W^\parallel$ (since $G_2(\tilde{I}) = \tilde{I}$). In the last three terms we have $I \otimes G_2$ acting on an operator from $W^\perp$. As expected, when this happen the quantum expander $G_2$ shrinks the operator. Formally,

**Claim 4.3.** For any $Z \in W^\perp$ we have $\| (I \otimes G_2)Z \| \leq \lambda_2 \| Z \|$.

We defer the proof for later. Having the claim we see that, e.g., $\| \langle \hat{G}_1X^\parallel, (I \otimes G_2)Y^\parallel \rangle \| \leq \| \hat{G}_1X^\parallel \| \| (I \otimes G_2)Y^\parallel \| \leq \lambda_2 \| X^\parallel \| \| Y^\parallel \|$. Similarly, $\| \langle \hat{G}_1(I \otimes G_2)X^\perp, Y^\parallel \rangle \| \leq \lambda_2 \| X^\perp \| \| Y^\parallel \|$. and $\| \langle \hat{G}_1(I \otimes G_2)X^\parallel, (I \otimes G_2)Y^\perp \rangle \| \leq \lambda_2^2 \| X^\parallel \| \| Y^\perp \|$

To bound the first term, we notice that on inputs from $W^\parallel$ the operator $\hat{G}_1$ mimics the operation of $G_1$ with a random seed. Formally,

**Claim 4.4.** For any $A \in W^\parallel$ orthogonal to the identity operator and any $B \in W^\parallel$ we have $|\langle \hat{G}_1A, B \rangle| \leq \lambda_1 \| A \| \cdot \| B \|$.

We again defer the proof for later. Having the claim we see that $|\langle \hat{G}_1X^\parallel, Y^\parallel \rangle| \leq \lambda_1 \| X^\parallel \| \cdot \| Y^\parallel \|$. Denoting $p_i = \| \rho_i \| / \| \rho_i \|$ and $q_i = \| \rho_i^\perp \| / \| \rho_i \|$ (for $i = 1, 2$, $\rho_1 = X$ and $\rho_2 = Y$) we see that $p_i^2 + q_i^2 = 1$, and,

$$|\langle (G_1 \otimes G_2) X, Y \rangle| \leq (p_1^2 + p_2^2 \lambda_1 + p_1q_2 \lambda_2 + p_2q_1 \lambda_2 + q_1q_2 \lambda_2^2) \| X \| \cdot \| Y \|$$

Elementary calculus now shows that this is bounded by $f(\lambda_1, \lambda_2) \| X \| \cdot \| Y \|$.  

We still have to prove the two claims:

**Proof of Claim 4.3.** $Z$ can be written as $Z = \sum_i \sigma_i \otimes \tau_i$, where each $\tau_i$ is perpendicular to $\tilde{I}$ and $\{\sigma_i\}$ is an orthogonal set. Hence,

$$\| (I \otimes G_2) Z \| = \left\| \sum_i \sigma_i \otimes G_2(\tau_i) \right\| \leq \sum_i \| \sigma_i \otimes G_2(\tau_i) \| \leq \sum_i \lambda_2 \| \sigma_i \otimes \tau_i \| = \lambda_2 \| Z \|.$$

$\blacksquare$
And,

**Proof of Claim 4.4** Since \( A, B \in W || \), they can be written as

\[
A = \sigma \otimes \tilde{I} = \frac{1}{D_1} \sum_i \sigma \otimes |i\rangle\langle i| \\
B = \eta \otimes \tilde{I} = \frac{1}{D_1} \sum_i \eta \otimes |i\rangle\langle i|.
\]

Moreover, since \( A \) is perpendicular to the identity operator, it follows that \( \sigma \) is perpendicular to the identity operator on the space \( L(\mathcal{H}_{N_1}) \). This means that applying \( G_1 \) on \( \sigma \) will shrink it by at least a factor of \( \lambda_1 \).

Considering the inner product

\[
| \langle \hat{G}_1 A, B \rangle | = \frac{1}{D_1^2} \left| \sum_{i,j} \text{Tr} \left( (U_i \sigma U_i^\dagger) \otimes |i\rangle\langle i| \right) \right|
\]

\[
= \frac{1}{D_1^2} \left| \sum_{i,j} \text{Tr} \left( (U_i \sigma U_i^\dagger \eta^\dagger) \otimes |i\rangle\langle j| \right) \right|
\]

\[
= \frac{1}{D_1^2} \left| \sum_i \text{Tr} \left( (U_i \sigma U_i^\dagger \eta^\dagger) \otimes |i\rangle\langle i| \right) \right|
\]

\[
= \frac{1}{D_1^2} \left| \sum_i \text{Tr} \left( U_i \sigma U_i^\dagger \eta^\dagger \right) \right|
\]

\[
= \frac{1}{D_1} \left| \text{Tr} \left( \left( \frac{1}{D_1} \sum_i U_i \sigma U_i^\dagger \right) \eta^\dagger \right) \right|
\]

\[
= \frac{1}{D_1} |\langle G_1(\sigma), \eta \rangle| \leq \frac{\lambda_1}{D_1} \| \sigma \| \cdot \| \eta \| = \lambda_1 \| A \| \cdot \| B \|,
\]

where the inequality follows from the expansion property of \( G_1 \) (and Cauchy-Schwartz).

**References**

[1] A. Ben-Aroya and A. Ta-Shma. Quantum expanders and the quantum entropy difference problem. arXiv:quant-ph/0702129.

[2] C. M. Dawson and M. A. Nielsen. The Solovay-Kitaev algorithm. *Quantum Information & Computation, 6*(1):81–95, 2006.

[3] M. B. Hastings. Entropy and entanglement in quantum ground states. *Phys. Rev. B, 76*(3):035114, 2007.

[4] M. B. Hastings. Random unitaries give quantum expanders. Technical report, arXiv:0706.0556, 2007.
[5] O. Reingold, S. Vadhan, and A. Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders. *Ann. of Math.*, 155(1):157–187, 2002.