A note on the elementary HDX construction of Kaufman-Oppenheim*

Prahladh Harsha[†] Ramprasad Saptharishi[†]
December 23, 2019

Abstract

In this note, we give a self-contained and elementary proof of the elementary construction of spectral high-dimensional expanders using elementary matrices due to Kaufman and Oppenheim [*Proc.* 50th ACM Symp. on Theory of Computing (STOC), 2018].

1 Introduction

In the last few years, there has been a surge of activity related to high-dimensional expanders (HDXs). Loosely speaking, high-dimensional expanders are a high-dimensional generalization of classical graph expanders. Depending on which definition of graph expansion is generalized, there are several different (and unfortunately, many a time mutually inequivalent) definitions of HDXs. For the purpose of this note, we will restrict ourselves to the spectral definition of HDXs (see Definition 2.5). Lubotzky, Samuels and Vishne [LSV05a, LSV05b] constructed high-dimensional analgoues of the Ramanujan expanders of Lubotzky, Philips and Sarnak [LPS88], which they termed Ramanujan complexes. These Ramanujan complexes have several desirable properties and gave rise to the first construction of constant degree spectral HDXs. The Ramanujan graphs have the nice property that they are simple to describe, however their proof of expansion is extremely involved. The Ramanujan complexes, on the other hand, are both non-trivial to describe as well as to prove their high-dimensional expansion property. Subsequently Kaufman and Oppenheim [KO18] gave an extremely elegant and elementary construction of spectral HDXs using elementary matrices. Despite their construction being elementary and simple, the proof of expansion, though straightforward, requires some knowledge of some representation theory of the specific groups involved in the construction. The purpose of this exposition is to give an alternate elementary proof of the expansion of the Kaufman-Oppenheim HDX construction.

The underlying graph of a HDX (even a onesided spectral HDX) is a two-sided spectral expander. Thus, this construction has the added advantage that it yields an elementary construction (accompanied with a simple proof) of a standard two-sided spectral expander (though not an optimal one).

^{*}This work was done when the authors were visiting the Simons Institute for Theory of Computing, Berkeley to participate in the summer cluster on Error-Correcting Codes and High Dimensional Expanders 2019..

[†]Tata Institute of Fundamental Research, INDIA. email: {prahladh,ramprasad}@tifr.res.in. Research of the authors supported by the Department of Atomic Energy, Government of India, under project no. 12-R&D-TFR-5.01-0500. Research of the first and second authors supported in part by the Swarnajayanti and Ramanujan Fellowships respectively.

2 Preliminaries

We begin by recalling what a simplicial complex is.

Definition 2.1 (Simplicial complex). A simplicial complex X over a finite set U is a collection of subsets of U with the property that if $S \in X$ then any $T \subseteq S$ is also in X.

- For all $i \ge -1$, define $X(i) := \{S \in X : |S| = i+1\}$ Thus, if X is non-empty, then $X(-1) = \{\emptyset\}$.
- The elements of X are called simplices or faces. The elements of X(0), X(1) and X(2) are usually referred to as vertices, edges and triangles respectively.
- The graph defined by X(0) and X(1) is called the 1-skeleton of the complex. More generally, for any $1 \le k \le d$, the d-skeleton of the complex X is the sub-complex $X(-1) \cup X(0) \cup X(1) \cup \cdots \cup X(k)$.
- The dimension of the simplicial complex X defined as the largest d such that X(d) (which consists of faces of size d+1) is non-empty.
- The simplicial complex is said to be pure if every face is contained in some face in X(d), where $d = \dim(X)$.
- For a face $S \in X$, the link of S, denoted by X_S , is the simplicial complex defined as

$$X_S := \{T \setminus S : T \in X, S \subseteq T\}.$$

Thus, a graph G = (V, E) is just a simplicial complex G of dimension one with G(0) = V and G(1) = E. We will deal with *weighted* pure simplicial complexes where the weight function satisfies a certain *balance* condition.

Definition 2.2 (weighted pure simplicial complexes). Given a d-dimensional pure simplicial complex X and an associated weight function $w: X \to \mathbb{R}_{\geq 0}$, we say the weight function is balanced if the following two conditions are satisfied.

$$(2.3) \qquad \sum_{\sigma \in X(d)} w(\sigma) = 1 \; ; \qquad \qquad w(\sigma) = \frac{1}{(i+2)} \sum_{\tau \in X(i+1), \tau \supset \sigma} w(\tau), \; \textit{for all } i < d \; \textit{and} \; \sigma \in X(i).$$

A weighted simplicial complex (X, w) is a pure simplical complex accompanied with a balanced weight function w. If no weight function is specified, then we work with the balanced weight function w induced by the uniform distribution on the set X(d) of top faces.

For a face $S \in X$, the balanced weight function w_S associated with the link X_S is the restricted weight function, suitable normalized, more precisely $w_S := w|_{X_S}/w(S)$.

Condition (2.3) states that the weight function can be interpreted as a family of joint distributions $(w|_{X(-1)},\ldots,w|_{X(d)})$ where $w|_{X(i)}$ is a probability distribution on X(i). The distribution $w|_{X(d)}$ is specified by the first condition in (2.3) while the second condition implies that the weight distribution $w|_{X(i)}$ is the distribution on X(i) obtained by picking a random $\tau \in X(d)$ according to $w|_{X(d)}$ and then removing (d-i) elements uniformly at random.

We now recall the classical definition of what it means for a graph to be a spectral expander.

Definition 2.4 (spectral expander). Given an undirected weighted graph G = (V, E, w) on n vertices, let A_G be its normalized adjacency matrix given as follows:

$$A_G(u,v) := egin{cases} rac{w(u,v)}{w(u)} & \textit{if } \{u,v\} \in E, \ 0 & \textit{otherwise}. \end{cases}$$

Let $1 = \lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_n \ge -1$ be the n eigenvalues of A_G with multiplicities in non-increasing order¹. We denote the second largest eigenvalue of G as $\lambda(G)$.

G is said to be a λ -spectral expander if $\max\{\lambda_2, |\lambda_n|\} \leq \lambda$.

G is said to be a λ -onesided-spectral expander if $\lambda_2 \leq \lambda$.

This spectral definition of expanders is generalized to higher dimensional simplicial complexes as follows.

 \Diamond

Definition 2.5 (λ -spectral HDX). A weighted simplicial complex (X, w) of dimension $d \geq 1$ is said to be a λ -spectral HDX² if for every $-1 \leq i \leq d-2$ and $s \in X(i)$, the weighted 1-skeleton of the link (X_s, w_s) is a λ -spectral expander.

A weighted simplicial complex (X, w) of dimension $d \ge 1$ is said to be a λ -onesided spectral HDX if for every $-1 \le i \le d-2$ and $s \in X(i)$, the weighted 1-skeleton of the link (X_s, w_s) is a λ -onesided-spectral expander. \Diamond

Using Garland's technique [Gar73], Oppenheim [Opp18] showed that if the 1-skeleton all the links are connected, then a spectral gap at dimension (d-2) descends to all lower levels.

Descent Theorem 2.6 ([Opp18]). *Suppose* (X, w) *is a d-dimensional weighted simplicial complex with the following properties.*

- For all $s \in X(d-2)$, the link (X_s, w_s) is a λ -(onesided)-spectral expander.
- *The* 1-*skeleton of every link is connected.*

Then,
$$(X, w)$$
 is a $\left(\frac{\lambda}{1-(d-1)\lambda}\right)$ -(onesided)-spectral HDX.

Thus to prove that a given simplicial complex, it suffices to show that the 1-skeleton of all links are connected and a spectral gap at the top level. For the sake of completeness, we give a proof of the Descent Theorem 2.6 in Appendix A which includes a descent theorem for the least eigenvalue as well.

3 Coset complexes

In this section, we construct certain special simplicial complexes based on a group and its subgroups, that are called *coset complexes*. For a basic primer on group theory, see Appendix B

Definition 3.1 (coset complex). Let G be a group and let K_1, \ldots, K_d be d subgroups of G. The coset complex $\mathcal{X}(G, \{K_1, \ldots, K_d\})$ is a (d-1)-dimensional simplicial complex defined as follows:

• The vertices, $\mathcal{X}(0)$, consists of cosets of K_1, \ldots, K_d and we shall say cosets of K_i are of type i.

¹By the balance condition, w satisfies $w(v) = \sum_{\{u,v\} \in E} w(u,v)$. The matrix A_G is self-adjoint with respect to the inner product $\langle f,g\rangle_w := \mathbb{E}_{v \sim w}[f(v)g(v)]$ since $\langle f,Ag\rangle_w = \langle Af,g\rangle_w = \mathbb{E}_{\{u,v\}\sim w}[f(u)g(v)]$. Hence, A_G has n real eigenvalues which can be obtained using the Courant-Fischer Theorem A.2.

²These are sometimes also referred to as λ -link HDXs or λ -local-expanders.

• The maximal faces, $\mathcal{X}(d-1)$, consists of d-sets of cosets of different types with a non-empty intersection. That is,

$$\{g_1K_1,\ldots,g_dK_d\}\in\mathcal{X}(d-1)\Longleftrightarrow g_1K_1\cap\cdots g_dK_d\neq\emptyset.$$

An equivalent way of stating this is that $\{g_1K_1, \ldots, g_dK_d\} \in \mathcal{X}(d-1)$ if and only if there is some $g \in G$ such that $g_iK_i = gK_i$ for all i.

• The lower dimensional faces are obtained by down-closing the maximal faces. Hence, for $0 \le r \le d$, $\{g_{i_1}K_{i_1}, \ldots, g_{i_r}K_{i_r}\} \in \mathcal{X}(r-1)$ if and only if $i_j \ne i_k$ for all $j \ne k$ and

$$g_{i_1}K_{i_1}\cap\cdots\cap g_{i_r}K_{i_r}\neq\emptyset.$$

We shall call the set $\{i_1, \ldots, i_r\}$ the type of this face.

- The dimension of this complex is (d-1).
- The weight function we will use is the one induced by the uniform distribution on the top face $\mathcal{X}(d-1)$.

A simplicial complex constructed this way is *partite* in the sense that each maximal face consists of vertices of distinct types.

Connectivity:

Observation 3.2. $g_1K_1 \cap g_2K_2 \neq \emptyset$ *if and only if* $g_1^{-1}g_2 \in K_1K_2$.

Proof. (⇒) Say
$$x = g_1k_1 = g_2k_2$$
 for $k_1 \in K_1$ and $k_2 \in K_2$. Then $g_1^{-1}g_2 = g_1^{-1}x \cdot x^{-1}g_2 = k_1k_2^{-1} \in K_1K_2$. (⇐) If $g_1^{-1}g_2 = k_1k_2$ for $k_1 \in K_1$ and $k_2 \in K_2$, then $g_1k_1 = g_2k_2^{-1} \in g_1K_1 \cap g_2K_2$.

Lemma 3.3 (Criterion for connected 1-skeletons). The 1-skeleton (underlying graph) of $\mathcal{X}(G, \{K_1, \dots, K_d\})$ is connected if and only if $G = \langle K_1, \dots, K_d \rangle$.

Proof. (\Leftarrow) Since there is always an edge between gK_i and gK_j for $i \neq j$, it suffices to show that K_1 is connected to gK_1 for an arbitrary $g \in G$. Suppose, for an arbitrary element $g \in G$, we have $g = g_1 \dots g_r$ where $g_j \in K_{i_j}$ and $i_j \neq i_{j+1}$ for each j. We might wlog. assume that (a) $g_1 \in K_1$ (otherwise set $g = 1 \cdot g_1 \cdots g_r$) and (b) if $r \geq 2$, then $i_r \neq 1$ (since otherwise we might then have worked with $g' = g_1 g_2 \dots g_{r-1}$ as $gK_1 = g'g_r K_1 = g'K_1$).

Then, we get the following path connecting K_1 and gK_{i_r}

$$K_1 = g_1 K_{i_1} \to (g_1 g_2) K_{i_2} \to (g_1 g_2 g_3) K_{i_3} \to \ldots \to (g_1 \cdots g_r) K_{i_r} = g K_{i_r}.$$

Note that, due to Observation 3.2, each successive pair of cosets are connected by an edge in the simplicial complex. Now, since gK_{i_r} is adjacent to gK_1 (as $i_r \neq 1$), we have that K_1 is connected to gK_1 .

(⇒) For an arbitrary $g \in G$, since the 1-skeleton is connected we have a path

$$K_1 = g_0 K_{i_0} \to g_1 K_{i_1} \to \cdots \to g_r K_{i_r} = g K_1.$$

By Observation 3.2, for every $j=0,\ldots,r-1$, we have $g_j^{-1}g_{j+1}\in K_{i_j}K_{i_{j+1}}\in \langle K_1,\ldots,K_d\rangle$. Therefore,

$$g = (g_0^{-1}g_1) \cdot (g_1^{-1}g_2) \cdots (g_{r-1}^{-1}g_r) \in \langle K_1, \dots, K_d \rangle.$$

Structure of links of the coset complex:

For any set $S \subseteq [d]$, define the group $K_S := \bigcap_{i \in S} K_i$; let $K_\emptyset := \langle K_1, \dots, K_d \rangle$. The following lemma shows that the links of a coset complex are themselves coset complexes.

Lemma 3.4. For any $v \in \mathcal{X}(k)$ of type $S \subseteq [d]$, the link X_v is isomorphic to the simplicial complex defined by $\mathcal{X}(K_S, \{K_S \cap K_i : i \notin S\})$.

Proof. It suffices to prove this lemma for $v \in \mathcal{X}(0)$ as links of higher levels can be obtained by inductive applications of this case.

Observe that if g is any element of G, then $(g_{i_1}K_{i_1},\ldots,g_{i_r}K_{i_r}) \in \mathcal{X}(r-1)$ if and only if the tuple $(gg_{i_1}K_{i_1},\ldots,gg_{i_r}K_{i_r}) \in \mathcal{X}(r-1)$. Therefore, the link of a coset gK_i is isomorphic to the link of the coset K_i . Thus, it suffices to prove the lemma for links of the type X_{K_i} for some $i \in [d]$.

Let v be the coset K_1 , without loss of generality. The *vertices* of the link, $X_v(0)$, are cosets of K_2, \ldots, K_d that have a non-empty intersection with K_1 . Note that any non-empty intersection $g_jK_j\cap K_1$ of a cosets with K_1 is itself a coset $\tilde{g}_j(K_j\cap K_1)$ of the intersection subgroup $K_j\cap K_1$ in K_1 . Therefore, the vertices of the link $X_v(0)$ are in bijective correspondence with cosets of $\{K_j\cap K_1:j\in\{2,\ldots,d\}\}$.

The maximal faces in X that contain the coset K_1 are precisely d-sets of cosets $\{K_1, g_2K_2, \dots, g_dK_d\}$ with a non-empty intersection and hence

$$\emptyset \neq K_1 \cap g_2 K_2 \cap \cdots \cap g_d K_d = (g_2 K_2 \cap K_1) \cap \ldots (g_d K_d \cap K_1) = \tilde{g_2}(K_2 \cap K_1) \cap \ldots \cap \tilde{g_d}(K_d \cap K_1),$$

which are precisely the maximal faces of the coset complex $\mathcal{X}\left(K_1,\left\{K_j\cap K_1:j\in\{2,\ldots,d\}\right\}\right)$. This establishes the isomorphism between X_v and $\mathcal{X}\left(K_1,\left\{K_j\cap K_1:j\in\{2,\ldots,d\}\right\}\right)$.

4 A concrete instantiation

The simplicial complex of Kaufman and Oppenheim [KO18] is a specific instantiation of the above *coset complex* construction. We will need some notation to describe their group.

Notation

- Let R denote the ring $\frac{\mathbb{F}_p[t]}{\langle t^s \rangle}$. This is a ring whose elements can be identified with polynomials in $\mathbb{F}_p[t]$ of degree less than s (where addition and multiplication are performed modulo t^s). We will think of p as some fixed prime power, t a formal variable and s as a growing integer.
- For $1 \le i, j \le d$ with $i \ne j$ and an element $r \in R$, we define the $e_{i,j}(r)$ to be the $d \times d$ elementary matrix with 1's on the diagonal and r on the (i,j)-th entry.

For the sake of notational convenience, we shall abuse this notation and use $e_{i+d,j}(r)$, $e_{i,j+d}$ etc. to refer to $e_{i,j}(r)$ by wrapping around if necessary. For example, $e_{d,d+1}(r)$ refers to $e_{d,1}(r)$.

We are now ready to describe the groups in the construction.

For
$$i \in \{1, \ldots, d\}$$
, $K_i = \langle e_{j,j+1}(at+b) : a, b \in \mathbb{F}_p, j \in [d] \setminus \{i\} \rangle$. $G = \langle K_1, \ldots, K_d \rangle$

Each K_i is generated by elementary matrices that have 1's on the diagonal and an arbitrary linear polynomial in one entry of the generalised diagonal $\{(i,j): i+1=j \mod d\}$.

It so happens that the group G generated by the subgroups K_1, \ldots, K_d is $SL_d(R)$, the group of $d \times d$ matrices with entries in R whose determinant is 1 (in R). This is a non-trivial fact. All we will need is the simpler fact that |G| grows exponentially with s (for fixed p and d) while the size of the groups K_i are functions of p and d (and independent of s). This will follow from the sequence of observations and lemmas developed in the following section.

4.1 Explicit description of the groups

The following is an easy consequence of the definition of $e_{i,j}(r)$.

Observation 4.1. • Sum: *If* $i \neq j$, then $e_{i,j}(r_1) \cdot e_{i,j}(r_2) = e_{i,j}(r_1 + r_2)$.

• Product: If $i \neq j$ and $k \neq \ell$, then the commutator³ $[e_{i,j}(r_1), e_{k,\ell}(r_2)]$ behaves as follows.

$$[e_{i,j}(r_1), e_{k,\ell}(r_2)] = \begin{cases} e_{i,\ell}(r_1 r_2) & \text{if } j = k \text{ and } i \neq \ell, \\ \text{id} & \text{if } j \neq k. \end{cases}$$

Therefore, we have that

$$\left[e_{i_1,i_2}(r_1),\left[e_{i_2,i_3}(r_2),\cdots\left[e_{i_{\ell-1},i_{\ell}}(r_{\ell-1}),e_{i_{\ell},i_{\ell+1}}(r_{\ell})\right]\cdots\right]\right]=e_{i_1,i_{\ell+1}}(r_1\cdots r_{\ell})$$

and hence $e_{i,j}(r)$ can be generated for any $r \in R$. This in particular implies that |G| is at least $|p^s|$. On the other hand, the size of K_i depends only on d, p and is independent of s. The lemma below describes K_d ; the other K_i 's are just rearrangements of rows and columns in K_d .

Lemma 4.2 (Explicit description of K_d). The group $K_d = \langle e_{i,i+1}(at+b) : a,b \in \mathbb{F}_p$, $i \neq d \rangle$ consists of matrices $A = (A_{i,i})$ of the following form:

$$A_{i,j} = \begin{cases} 0 & \text{if } i > j, \\ 1 & \text{if } i = j, \\ a \text{ polynomial of degree} \le r & \text{if } j - i = r. \end{cases}$$

Therefore, we can obtain a crude bound of $|K_n| \le p^{O(d^3)}$. In fact, we can generalise the above definition to define the group $\widetilde{K_S}$ for any $S \subseteq [d]$ as follows:

$$\widetilde{K_S} := \left\langle e_{i,i+1}(at+b) : a,b \in \mathbb{F}_p, i \notin S \right\rangle.$$

These groups can also be explicitly described.

³The commutator of two elements g, h, denoted by [g, h] is defined as $g^{-1}h^{-1}gh$. (Definition B.2)

Lemma 4.3 (Explicit description of $\widetilde{K_S}$). For any $\emptyset \neq S \subseteq [d]$, group $\widetilde{K_S}$ is the set of all $d \times d$ matrices $A = (a_{ij})$ of the form

$$A_{i,j} = \begin{cases} 1 & \text{if } i = j, \\ a \text{ polynomial of degree} \leq j - k & \text{if } j \neq k \text{ and } \{k, k + 1, \dots, j - 1\}_{\text{mod } d} \cap S = \emptyset, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Any $A \in \widetilde{K_S}$ can be expressed as $A = B_1 \cdots B_m$ where each $B_r = e_{i_r,i_r+1}(\ell_r)$, for some linear polynomial ℓ_r , with $i_r \notin S$. Then,

$$A_{i,j} = \sum_{\substack{i_1, \dots, i_{m+1} \\ i_1 = i, i_{m+1} = j}} (B_1)_{i_1, i_2} (B_2)_{i_2, i_3} \cdots (B_m)_{i_m, i_{m+1}}.$$

From the structure of each B_r , any nonzero contribution from the RHS must involve either $i_{r+1} = i_r$, or $i_{r+1} = i_r + 1$ if $r \notin S$. This forces that the only entries of A that are nonzero, besides the diagonal, are at (i,j) with none of $\{i,i+1,\ldots,j\}$ in S.

In the case when $\{i, i+1, \ldots, j\} \cap S = \emptyset$, the above argument also shows that the entry $A_{i,j}$ has degree at most j-i. Furthermore, Observation 4.1 shows that $e_{i,j}(f) \in \widetilde{K_S}$ for an arbitrary polynomial f(t) of degree at most j-i. From this, we can deduce that the structure of $\widetilde{K_S}$ is exactly as claimed.

From the explicit structure of the groups, we have the following corollary.

Corollary 4.4 (Intersections of K_i 's). *For any* $S \subseteq [d]$,

$$\widetilde{K_S} = \langle e_{i,i+1}(at+b) : a,b \in \mathbb{F}_p, i \notin S \rangle = \bigcap_{i \in S} K_i = K_S$$

In other words, the group generated by the intersection of generators equals the group intersection.

The above corollary tells us that we can drop the tilde notation and use K_S for \widetilde{K}_S .

4.2 Connectivity of this complex

Lemma 4.5. *Let* $S \subset [d]$ *with* $|S| \leq d - 2$. *Then,*

$$K_S = \langle K_S \cap K_i : i \in [d] \setminus S \rangle$$
.

Proof. It is clear that K_S is a superset of the RHS. It only remains to show that the other containment also holds. To see this, consider an arbitrary generator $e_{j,j+1}(r)$ of K_S . Since $j \notin S$ and $|S| \le d-2$, there is some $i \in [d] \setminus (S \cup \{j\})$. Therefore, $e_{j,j+1}(r) \in K_S \cap K_i$ and hence is generated by the RHS. □

Combining the above lemma with Lemma 3.3 and Lemma 3.4, we have the following corollary.

Corollary 4.6. For the coset complex $\mathcal{X}(G, \{K_1, \dots, K_d\})$ defined by the above groups, the 1-skeleton of every link is connected.

5 Spectral expansion of the complex

In this section we prove that the coset complex $\mathcal{X}(G, \{K_1, ..., K_d\})$ is a good spectral HDX. The Descent Theorem 2.6 states that it suffices to show that the 1-dimensional links of faces in $\mathcal{X}(d-3)$ are good spectral expanders.

5.1 Structure of 1-dimensional links

One dimensional links of the coset complex constructed are links of $v \in \mathcal{X}(G, \{K_1, ..., K_d\})$ of size exactly (d-2) (which are elements of $\mathcal{X}(d-3)$. Any such v can be written as $\{gK_1, ..., gK_d\} \setminus \{gK_i, gK_j\}$ for $i, j \in [d]$ with $i \neq j$ and $g \in G$. Since the link of v is isomorphic to the link of $\{K_1, ..., K_d\} \setminus \{K_i, K_j\}$, we might as well assume that g = id. These happen to be of two types depending on whether i and j are consecutive or not.

Observation 5.1. Consider $v = \{K_1, ..., K_d\} \setminus \{K_i, K_j\}$ where i and j are not consecutive (i.e. $(i - j) \neq \pm 1 \mod d$). Then the 1-dimensional link of v is a complete bipartite graph.

Proof. Note that since $j \neq i + 1$, we have $[e_{i,i+1}(r_1), e_{j,j+1}(r_2)] = id$ by Observation 4.1. Hence, these two elements commute.

The link of v corresponds to the coset complex $\mathcal{X}(H, \{H_1, H_2\})$ where

$$H = K_{[d] \setminus \{i,j\}} = \langle e_{i,i+1}(at+b), e_{j,j+1}(at+b) : a, b \in \mathbb{F}_p \rangle,$$

$$H_1 = K_{[d] \setminus \{i\}} = \langle e_{i,i+1}(at+b) : a, b \in \mathbb{F}_p \rangle,$$

$$H_2 = K_{[d] \setminus \{j\}} = \langle e_{i,j+1}(at+b) : a, b \in \mathbb{F}_p \rangle.$$

Thus, the groups H_1 and H_2 commute with each other and hence any element of $h \in H$ can be written as $h = g_1 \cdot g_2$ where $g_1 \in H_1$ and $g_2 \in H_2$. Observation 3.2 implies that the resulting graph is the complete bipartite graph.

The interesting case is when $v = \{K_1, ..., K_d\} \setminus \{K_i, K_{i+1}\}$. Without loss of generality, we may focus on the link of $v = \{K_3, K_4, ..., K_d\}$. This corresponds to the coset complex $\mathcal{X}(H, \{H_1, H_2\})$ where

$$H = K_{3,4,...,d} = \langle e_{1,2}(at+b), e_{2,3}(at+b) : a, b \in \mathbb{F}_p \rangle,$$

$$H_1 = K_{2,3,4,...,d} = \langle e_{1,2}(at+b) : a, b \in \mathbb{F}_p \rangle,$$

$$H_2 = K_{1,3,4,...,d} = \langle e_{2,3}(at+b) : a, b \in \mathbb{F}_p \rangle.$$

Hence, it suffices to focus on the first three rows and columns of these matrices as the rest of them are constant. Written down explicitly,

$$H = \left\{ \begin{bmatrix} 1 & \ell_1 & Q \\ 0 & 1 & \ell_2 \\ 0 & 0 & 1 \end{bmatrix} : \begin{array}{l} \ell_1, \ell_2 \text{ are linear polynomials in } \mathbb{F}_p[t] \\ \text{and } Q \text{ is a quadratic polynomial in } \mathbb{F}_p[t] \end{array} \right\},$$

$$H_1 = \left\{ \begin{bmatrix} 1 & \ell & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : \ell \text{ is a linear polynomial in } \mathbb{F}_p[t] \right\},$$

$$H_2 = \left\{ egin{bmatrix} 1 & 0 & 0 \ 0 & 1 & \ell \ 0 & 0 & 1 \end{bmatrix} : \ell ext{ is a linear polynomial in } \mathbb{F}_p[t]
ight\}.$$

Therefore, each coset of H_1 and H_2 in H has a unique representative of the form

$$M_1(\ell,Q) := egin{bmatrix} 1 & 0 & Q \ 0 & 1 & \ell \ 0 & 0 & 1 \end{bmatrix} \quad , \quad M_2(\ell,Q) := egin{bmatrix} 1 & \ell & Q \ 0 & 1 & 0 \ 0 & 0 & 1 \end{bmatrix}$$

respectively, where ℓ is a linear polynomial and Q is a quadratic polynomial in $\mathbb{F}_p[t]$.

Lemma 5.2. For linear polynomials $\ell_1, \ell_2 \in \mathbb{F}_p[t]$ and quadratic polynomials $Q_1, Q_2 \in \mathbb{F}_p[t]$, we have that

$$M_1(\ell_1, Q_1)H_1 \cap M_2(\ell_2, Q_2)H_2 \neq \emptyset \iff \ell_1\ell_2 = Q_1 - Q_2.$$

Proof. By Observation 3.2, the cosets have a non-empty intersection if and only if

$$H_1H_2 \ni M_1(ell_1, Q_1)^{-1}M_2(\ell_2, Q_2) = \begin{bmatrix} 1 & 0 & -Q_1 \\ 0 & 1 & \ell_1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & \ell_2 & Q_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \ell_2 & Q_2 - Q_1 \\ 0 & 1 & -\ell_1 \\ 0 & 0 & 1 \end{bmatrix}$$

which happens if and only if $(\ell_2)(-\ell_1) = Q_2 - Q_1$ which is the same as $Q_1 - Q_2 = \ell_1 \ell_2$.

Therefore, the 1-dimensional link is the bipartite graph A=(U,V,E) with left and right vertices identified by pairs (ℓ,q) where ℓ and Q are linear and quadratic polynomials in $\mathbb{F}_p[t]$ respectively, with $(\ell_1,Q_1)\sim(\ell_2,Q_2)\Leftrightarrow\ell_1\ell_2=Q_1+Q_2$ (by associating $M_1(\ell,Q)$ with the tuple (ℓ,Q) on the left, and $M_2(\ell,Q)$ with the tuple (ℓ,Q) on the right).

Note that A is an undirected, p^2 -regular bipartite graph with p^5 vertices on each side. It suffices to show that A is a good expander.

5.2 A related graph

The following graph is the "lines-points" or the "affine plane" graph used by Reingold, Vadhan and Wigderson [RVW05] (as the *base graph* in construction of constant-degree expanders, using the zig-zag product). Let \mathbb{F}_q be a finite field. Consider the bipartite graph $B_q = (U', V', E')$ defined as follows:

$$U' = V' = \mathbb{F}_q \times \mathbb{F}_q$$
, $E' = \{((a,b),(c,d)) : ac = b + d\}.$

Lemma 5.3. The q-regular bipartite graph B_q is a $\frac{1}{\sqrt{q}}$ -onesided-spectral expander.

Proof. Consider the graph B_q^2 restricted to the vertices in U'. It is easy to see that

edges between
$$(a,b)$$
 and $(c,d) = \begin{cases} 1 & \text{if } a \neq c, \\ q & \text{if } a = c \text{ and } b = d, \\ 0 & \text{otherwise.} \end{cases}$

Therefore, the adjacency matrix of B_q^2 (restricted to U') can be written (under a suitable order of listing vertices)

$$qI_{q^2} + (J_q - I_q) \otimes J_q$$
 (where J_q is the $q \times q$ matrix of 1s).

Hence the unnormalized second largest eigenvalue of B_q^2 is q and hence we have that the normalized second largest eigenvalue of B_q is $1/\sqrt{q}$.

5.3 Relating the graph B_q with A

Set $q = p^3$ so that $\mathbb{F}_q = \frac{\mathbb{F}_p[y]}{\mu(y)}$ for some irreducible polynomial $\mu(y)$ of degree exactly 3. Therefore, each element in \mathbb{F}_q is expressible as $a_0 + a_1 + a_2 y^2$ for some $a_0, a_1, a_2 \in \mathbb{F}_p$. Thus, the graph $B_q = (U', V', E')$ defined above, for this setting of $q = p^3$, is a p^3 -regular bipartite graph with p^6 vertices on either side.

Let $U'' = V'' = \{(a_0 + a_1y, b_0 + b_1y + b_2y^2) : a_0, a_1, b_0, b_1, b_2 \in \mathbb{F}_p\}$, which is a subset of U' and V', respectively, of size p^5 each.

Observation 5.4. The induced subgraph of B_q on U'', V'' is exactly the graph A = (U, V, E) described earlier.

Proof. Note that $((\ell_1(y), Q_1(y)), (\ell_2(y), Q_2(y))) \in E'$ if and only if

$$\ell_1(y) \cdot \ell_2(y) = Q_1(y) + Q_2(y) \mod \mu(y).$$

However, since the above equation has degree at most 2, we have

$$\ell_1(y) \cdot \ell_2(y) = Q_1(y) + Q_2(y) \Leftrightarrow \ell_1(y) \cdot \ell_2(y) = Q_1(y) + Q_2(y) \pmod{\mu(y)},$$

and the first equation is exactly the adjacency condition of the graph A. Hence, the induced subgraph of B_q on U'', V'' is indeed the graph A.

Normally, induced subgraphs of expanders need not even be connected. However, the following lemma shows that there are some instances when we may be able to give non-trivial bounds on λ .

Lemma 5.5. Suppose X is a d-regular, undirected graph that is an induced subgraph of a D-regular graph Y. Then,

$$\lambda(X) \le \frac{D\lambda(Y)}{d}.$$

Proof. The Courant-Fischer Theorem A.2 characterization of the second largest eigenvalue tells us that $\lambda(X) = \max_{\mathbf{a} \perp \mathbf{1}_{|X|}} \frac{\mathbf{a}^T G \mathbf{a}}{d \cdot \mathbf{a}^T \mathbf{a}}$. Consider an arbitrary $\mathbf{a} \in \mathbb{R}^{|X|}$ such that $\mathbf{a} \perp \mathbf{1}_{|X|} = 0$. Since X is an induced subgraph of Y, the vector \mathbf{a} can be padded with zeroes to obtain a vector $\mathbf{b}_{\mathbf{a}} \in \mathbb{R}^{|Y|}$ such that $\mathbf{b}_{\mathbf{a}} \perp \mathbf{1}_{|Y|}$. Therefore,

$$\lambda(X) = \max_{\mathbf{a} \perp \mathbf{1}_{|X|}} \frac{\mathbf{a}^T A_X \mathbf{a}}{\mathbf{a}^T \mathbf{a}} = \frac{D}{d} \cdot \max_{\mathbf{a} \perp \mathbf{1}_{|X|}} \frac{\mathbf{b}_{\mathbf{a}}^T A_Y \mathbf{b}_{\mathbf{a}}}{\mathbf{b}_{\mathbf{a}}^T \mathbf{b}_{\mathbf{a}}} \le \frac{D}{d} \cdot \max_{\mathbf{b} \perp \mathbf{1}_{|Y|}} \frac{\mathbf{b}^T A_Y \mathbf{b}}{\mathbf{b}^T \mathbf{b}} = \frac{D\lambda(Y)}{d} .$$

Corollary 5.6. The graph A(U, V, E) corresponding to the 1-dimensional links of $\mathcal{X}(G, \{K_1, \dots, K_d\})$ is an onesided $\left(\frac{1}{\sqrt{p}}\right)$ -spectral expander.

Proof. The graph B_{p^3} is a bipartite, p^3 -regular graph with $\lambda(B_{p^3}) \leq \frac{1}{p^{3/2}}$ and A(U,V,E) is a p^2 -regular graph that is an induced subgraph of B_{p^3} . Hence, by Lemma 5.5,

$$\lambda(A) \le \frac{p^3 \cdot (1/p^{3/2})}{p^2} = \frac{1}{\sqrt{p}}.$$

The final expansion bounds

From the corollary above, we obtain the following theorem of Kaufman and Oppenheim.

Theorem 5.7 ([KO18]). For $p > (d-2)^2$, the (d-1)-dimensional coset complex $\mathcal{X}(G, \{K_1, \ldots, K_d\})$ is a $\frac{1}{\sqrt{p}-(d-2)}$ -onesided-spectral HDX.

Proof. Follows directly from Descent Theorem 2.6 that $\mathcal{X}(G, \{K_1, \dots, K_d\})$ is a γ -(onesided) local spectral expander for

$$\gamma \le \frac{1/\sqrt{p}}{1 - (d-2)(1/\sqrt{p})} = \frac{1}{\sqrt{p} - (d-2)}.$$

Constructing two-sided HDXs and standard expanders graphs: The (d-1)-dimensional coset complex $\mathcal{X}(G, \{K_1, \dots, K_d\})$ is a not a two-sided HDX as the 1-skeleton of the links of the faces in $\mathcal{X}(d-3)$ are bipartite. However, if we restrict attention to the k-skeleton of \mathcal{X} for some k < d-1 then we can bound the least eigenvalue using the descent theorem for least eigenvalue (Theorem A.4(2)). This is summarized in the following corollary.

Corollary 5.8. For $p > (d-2)^2$ and any $1 \le k < d$ the k-skeleton of the (d-1)-dimensional coset complex $\mathcal{X}(G, \{K_1, \ldots, K_d\})$ is a max $\left\{\frac{1}{\sqrt{p}-(d-2)}, \frac{1}{d-k}\right\}$ -two-sided spectral HDX.

In particular, if we set k=1 in the above corollary, we get a standard max $\left\{\frac{1}{\sqrt{p}-(d-2)}, \frac{1}{d-1}\right\}$ -two-sided spectral expander. This graph is a d-partite graph and hence its least eigenvalue is at most -1/(d-1), while the above argument shows that it is least (and hence equal to) -1/(d-1).

Thus, this not only yields an elementary construction and proof of onesided-spectral HDXs (Theorem 5.7), but also one of standard spectral expander (Corollary 5.8).

References

- [Dik19] YOTAM DIKSTEIN. Agreement Theorems and Fourier Decomposition on High Dimensional Expanders. Master's thesis, Weizmann Institute of Science, Israel, 2019.
- [Gar73] HOWARD GARLAND. *p-adic curvature and the cohomology of discrete subgroups of p-adic groups*. Ann. of Math., 97(3):375–423, 1973. doi:10.2307/1970829.
- [KO18] TALI KAUFMAN and IZHAR OPPENHEIM. Construction of new local spectral high dimensional expanders. In Proc. 50th ACM Symp. on Theory of Computing (STOC), pages 773–786. 2018. doi:10.1145/3188745.3188782.
- [LPS88] ALEXANDER LUBOTZKY, RALPH PHILLIPS, and PETER SARNAK. *Ramanujan graphs*. Combinatorica, 8(3):261–277, 1988. doi:10.1007/BF02126799.
- [LSV05a] Alexander Lubotzky, Beth Samuels, and Uzi Vishne. Explicit constructions of Ramanujan complexes of type $\tilde{A_d}$. European J. Combin., 26(6):965–âÅŞ993, 2005. doi:10.1016/j.ejc.2004.06.007.

[LSV05b] — Ramanujan complexes of type \tilde{A}_d . Israel J. Math., 149(1):267–299, 2005. doi:10.1007/BF02772543.

[Opp18] IZHAR OPPENHEIM. Local spectral expansion approach to high dimensional expanders part I: Descent of spectral gaps. Discrete Comput. Geom., 59(2):293–330, 2018. doi:10.1007/s00454-017-9948-x.

[RVW05] OMER REINGOLD, SALIL VADHAN, and AVI WIGDERSON. Entropy waves, the zig-zag graph product, and new constant-degree expanders. Annals of Math (2), 155(1):157–187, 2005. (Preliminary version in 41st FOCS, 2000). doi:10.2307/3062153.

A Proof of the Descent Theorem

For the sake of completeness, we present the proof of Descent Theorem 2.6 that asserts that proving local expansion for the maximal faces is sufficient to obtain expansion of any link. This exposition is essentially from the lecture notes by Dikstein [Dik19].

Let (X, w) be a weighted d-dimensional simplicial complex. Let $\mu_d = w|_{X(d)}$ be the distribution on the set X(d) of (d+1)-sized faces. This distribution induces distributions μ_i on X(i) in the natural way.

For two functions $f,g:X(0)\to\mathbb{R}$, define their *inner-product* $\langle f,g\rangle_X=\mathbb{E}_{u\sim\mu_0}[f(u)g(u)]$. We will drop the subscript X if it is clear from context. Note that, by the definition of μ_1 , sampling u according to μ_0 can be equivalently achieved by sampling an edge (u,v) according of μ_1 and returning one of the points. Therefore,

$$(A.1) \qquad \langle f,g\rangle_X = \underset{u\sim\mu_0}{\mathbb{E}}[f(u)g(u)] = \underset{\{u,v\}\sim\mu_1}{\mathbb{E}}[f(u)g(u)] = \underset{v\sim\mu_0}{\mathbb{E}}\underset{u\in X_n(0)}{\mathbb{E}}[f(u)g(u)] = \underset{v\sim\mu_0}{\mathbb{E}}[\langle f_v,g_v\rangle_{X_v}],$$

where $f_v, g_v : X_v(0) \to \mathbb{R}$, the restriction to the link of v.

Define the *adjacency operator* A that, on a function $f: X(0) \to \mathbb{R}$ on vertices returns another function Af on vertices defined via

$$Af(v) = \mathbb{E}_{u \sim v}[f(u)].$$

In other words, A averages f over neighbours. Furthermore, A is self-adjoint with respect to the above inner product, i.e, $\langle Af,g\rangle=\langle f,Ag\rangle$. Hence, it has n real eigenvalues and an orthonormal set of eigenvectors. Clearly $A\mathbb{1}=\mathbb{1}$; the constant 1 function is an eigenvector for this operator (in fact, it is an eigenvector corresponding to the largest eigenvalue 1). The remaining eigenvalues are characterized by the Courant-Fischer Theorem A.2.

Courant-Fischer Theorem A.2. Let $A \in \mathbb{R}^{n \times n}$ be a $n \times n$ matrix over the reals that is self-adjoint with respect to some inner product $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$. Then A has n real eigenvalues $\lambda_1 \geq \cdots \geq \lambda_n$ which have the following characterization.

$$\lambda_i = \max_{V: \dim V = i} \min_{x \in V} \frac{\langle x, Ax \rangle}{\langle x, x \rangle} = \min_{V: \dim V = n - i + 1} \max_{x \in V} \frac{\langle x, Ax \rangle}{\langle x, x \rangle}.$$

Similar to Equation A.1, we have

$$\langle Af, g \rangle_X = \underset{(u, w) \sim \mu_1}{\mathbb{E}} [f(u)g(w)] = \underset{(u, v, w) \sim \mu_2}{\mathbb{E}} [f(u)g(w)]$$

(A.3)
$$= \underset{v \sim \mu_0}{\mathbb{E}} \left[\underset{(u,w) \in X_v(1)}{\mathbb{E}} [f(u)g(w)] \right]$$
$$= \underset{v \sim \mu_0}{\mathbb{E}} \left[\langle A_v f_v, g_v \rangle_{X_v} \right]$$

where A_v denotes the adjacency operator restricted to the link X_v .

With the above notation, we can now state the theorem we wish to prove. It suffices to prove the theorem in the case of d = 3 as we can obtain Descent Theorem 2.6 by induction.

Theorem A.4. Suppose (X, w) is weighted 2-dimensional simplicial complex. Then, we have the following two implications:

- 1. Suppose the 1-skeleton of X is connected and for every vertex $v \in X(0)$, if $\langle A_v f, f \rangle \leq \lambda \langle f, f \rangle$ for all $f \colon X_v(0) \to \mathbb{R}$ with $f \perp \mathbb{1}_{X_v}$. Then, for any $g \colon X(0) \to \mathbb{R}$ with $g \perp \mathbb{1}_X$, we have $\langle Ag, g \rangle \leq \gamma \langle g, g \rangle$ where $\gamma \leq \frac{\lambda}{1-\lambda}$.
- 2. Suppose the 1-skeleton of X is non-empty and for every vertex $v \in X(0)$, if $\langle A_v f, f \rangle \geq \eta \langle f, f \rangle$ for all $f: X_v(0) \to \mathbb{R}$. Then, for any $g: X(0) \to \mathbb{R}$, we have $\langle Ag, g \rangle \geq \gamma \langle g, g \rangle$ where $\gamma \geq \frac{\eta}{1-\eta}$.

Before we see a proof of this, let us see how Descent Theorem 2.6 follows from this.

Descent Theorem A.5 (Descent Theorem 2.6 restated). Suppose (X, w) is a non-empty d-dimensional weighted simplicial complex with the following properties.

- *The* 1-*skeleton of every link is connected.*
- For all $v \in X(d-2)$, the link (X_v, w_v) is a λ -(onesided)-spectral expander. I.e., there is a $\lambda > 0$ such that, for every $v \in X(d-2)$ and every $g: X_v(0) \to \mathbb{R}$ with $g \perp 1$, we have

$$\langle A_v g, g \rangle \leq \lambda \langle g, g \rangle$$
.

Then, (X, w) is a γ -(onesided) local spectral expander for $\gamma \leq \frac{\lambda}{1 - (d - 1)\lambda}$. That is, for any $v \in X(-1) \cup \cdots \cup X(d - 2)$ and every $g : X_v(0) \to \mathbb{R}$ with $g \perp 1$, we have $\langle A_v g, g \rangle \leq \gamma \langle g, g \rangle$.

Additionally, if we also know that there is a $\eta \in [-1,0)$ such that, for every $v \in X(d-2)$ and every $g: X_v(0) \to \mathbb{R}$, we have $\langle A_v g, g \rangle \geq \eta \ \langle g, g \rangle$. Then, for any $v \in X(-1) \cup \cdots \cup X(d-2)$ and every $g: X_v(0) \to \mathbb{R}$, we have that X is a γ -(two-sided) local spectral expander with

$$\gamma \leq \max\left(\frac{\lambda}{1-(d-1)\lambda'}\left|\frac{\eta}{1-(d-1)\eta}\right|\right).$$

Proof. For any $i \le d - 2$, let

$$\lambda_i = \min_{v \in X(i)} \max_{g: X_v(0) \to \mathbb{R}} \frac{\langle A_v g, g \rangle}{\langle g, g \rangle},$$

the smallest local expansion with respect to X(i). From repeated applications of Theorem A.4,

$$\lambda_{-1} \le \frac{\lambda_0}{1 - \lambda_0} \le \frac{\lambda_1 / (1 - \lambda_1)}{1 - (\lambda_1 / (1 - \lambda_1))} = \frac{\lambda_1}{1 - 2\lambda_1} \le \dots \le \frac{\lambda_{d-2}}{1 - (d-1)\lambda_{d-2}}$$

which eventually completes the proof for onesided local spectral expansion.

For two-sided local spectral expansion, we would also have to show that all local eigenvalues are bounded away from -1. One again, let η_i be such that

$$\eta_i = \max_{v \in X(i)} \min_{\substack{g: X_v(0) \to \mathbb{R} \\ g \mid 1}} \frac{\langle A_v g, g \rangle}{\langle g, g \rangle}.$$

By repeated applications of Theorem A.4 (2), we obtain

$$\eta_{-1} \ge \frac{\eta_0}{1 - \eta_0} \ge \frac{\eta_1/(1 - \eta_1)}{1 - (\eta_1/(1 - \eta_1))} = \frac{\eta_1}{1 - 2\eta_1} \ge \dots \ge \frac{\eta_{d-2}}{1 - (d-1)\eta_{d-2}}$$

Together, we have that X is a γ -(two-sided) local spectral expander for

$$\gamma = \max\left(\frac{\lambda}{1 - (d - 1)\lambda'} \left| \frac{\eta}{1 - (d - 1)\eta} \right| \right). \quad \Box$$

Proof of Theorem A.4. Let g be an eigenvector that satisfies $\langle g,g\rangle=1$ and $g\perp \mathbb{1}_X$ that maximises (or minimises) $\langle Ag,g\rangle$, and $\gamma=\langle Ag,g\rangle$ be the extremal value. In particular, $Ag=\gamma\cdot g$. From (A.3) we have $\gamma=\langle Ag,g\rangle=\mathbb{E}_v\left[\langle A_vg_v,g_v\rangle\right]$.

Even though $g \perp \mathbb{1}_X$, the *local* component g_v need not be perpendicular to $\mathbb{1}_{X_v}$. Hence, let us write $g_v = \alpha_v \mathbb{1}_{X_v} + g_v^{\perp}$ where $g_v^{\perp} \perp \mathbb{1}_{X_v}$; we shall dropping the subscript from $\mathbb{1}_{X_v}$ for the sake of brevity as the length of the vector will be clear from context. Note that $\alpha_v = \langle g_v, \mathbb{1} \rangle = \mathbb{E}_{w \in X_v(0)}[g_v] = Ag(v)$. Therefore, $\mathbb{E}_v[\alpha_v^2] = \langle Ag, Ag \rangle = \gamma^2$.

(A.6)
$$\gamma = \langle Ag, g \rangle = \mathbb{E}_{v} \left[\langle A_{v}g_{v}, g_{v} \rangle \right] = \mathbb{E}_{v} \left[\alpha_{v}^{2} + \left\langle A_{v}g_{v}^{\perp}, g_{v}^{\perp} \right\rangle \right]$$

We shall now focus on the proof of Theorem A.4 (1). The other direction is exactly identical with the inequality flipped.

In the case of Theorem A.4 (1), where we are given $\langle A_v g_v^{\perp}, g_v^{\perp} \rangle \leq \lambda \langle g_v^{\perp}, g_v^{\perp} \rangle$ for all $v \in X(0)$, we have

$$\gamma = \mathbb{E}_{v} \left[\alpha_{v}^{2} + \left\langle A_{v} g_{v}^{\perp}, g_{v}^{\perp} \right\rangle \right] \leq \mathbb{E}_{v} \left[\alpha_{v}^{2} + \lambda \left\langle g_{v}^{\perp}, g_{v}^{\perp} \right\rangle \right]$$

$$= \mathbb{E}_{v} \left[(1 - \lambda) \alpha_{v}^{2} + \lambda \left\langle g_{v}, g_{v} \right\rangle \right]$$

$$= (1 - \lambda) \gamma^{2} + \lambda.$$

$$\implies \gamma (1 - \gamma) \leq \lambda (1 - \gamma^{2})$$

$$\implies \gamma \leq \lambda (1 + \gamma) \qquad \text{(connected, thus } \gamma < 1)$$

$$\implies \gamma \leq \frac{\lambda}{1 - \lambda}.$$

In the case of Theorem A.4 (2), where we are given $\langle A_v g_v^{\perp}, g_v^{\perp} \rangle \geq \eta \langle g_v^{\perp}, g_v^{\perp} \rangle$ for all $v \in X(0)$, the same argument yields

$$\gamma = \mathbb{E}_{v} \left[\alpha_{v}^{2} + \left\langle A_{v} g_{v}^{\perp}, g_{v}^{\perp} \right\rangle \right] \ge \mathbb{E}_{v} \left[\alpha_{v}^{2} + \eta \left\langle g_{v}^{\perp}, g_{v}^{\perp} \right\rangle \right] = (1 - \eta) \gamma^{2} + \eta$$

$$\implies \gamma \ge \frac{\eta}{1 - \eta}$$

B Primer on Group Theory

In this section, for completeness, we shall note the basic definitions and properties of group that is used in this exposition.

Definition B.1 (Groups and subgroups). *A set of elements G equipped with a binary operation* \star : $G \times G \rightarrow G$ *is said to be a* group *that satisfies the following properties:*

Associativity: For all $g_1, g_2, g_3 \in G$, we have $(g_1 \star g_2) \star g_3 = g_1 \star (g_2 \star g_3)$.

Identity: There exists an identity element $id \in G$ such that, for all $g \in G$, we have $g \star id = id \star g = g$.

Inverses: For every element $g \in G$, there is an element $g^{-1} \in G$ such that $g \star g^{-1} = g^{-1} \star g = \mathrm{id}$.

Often the binary operation \star is omitted and products just expressed as concatenation of elements.

A subset $H \subseteq G$ is said to be a subgroup of G if H the binary operation \star restricted to H satisfies the above three properties (including the fact that $h_1 \star h_2 \in H$ for all $h_1, h_2 \in H$).

Suppose H, K are subgroups of G, would often consider the product HK (or $H \star K$) which refers to the set $\{h \star k : h \in H, k \in K\}$. It is worth stressing that HK need not be a subgroup of G and the above just refers to a set of elements that can be expressed as (ordered) product of an element in H and an element in G.

For an arbitrary set S of G, we will define $\langle S \rangle$ as the smallest subgroup of G that contains the set S. This is also referred to as the *group generated* by S.

In general, the binary operation \star is order dependent. Groups where $g_1 \star g_2 = g_2 \star g_1$ for all $g_1, g_2 \in G$ is said to be a *commutative* or *Abelian* group. The following notion of *commutators* (and *commutator subgroups*) is a way to measure *how non-commutative* a group G is.

Definition B.2 (Commutators). For a pair of elements $g, h \in G$, we shall define the commutator of g, h (denoted by [g, h]) as

$$[g,h] := g^{-1}h^{-1}gh.$$

The commutator subgroup of G, denoted by [G,G] is group generated by all commutators. That is,

$$[G,G] := \langle \{[g,h] : g,h \in G\} \rangle.$$

Note that if G is Abelian, then $[G, G] = \{id\}$. As mentioned earlier, the commutator subgroup can be thought of as a way of describing how non-Abelian a group is. In fact, the commutator subgroup of G is the smallest *normal* subgroup H of G such that the *quotient* G/H is Abelian.