Expanding Graphs and Property (T)

Horace Fusco

November 2022

1 Expanding Graphs

In theoretical computer science, graph of various sorts can be used to model algorithms, and understanding properties of the graphs in question can sometimes yield useful information about run-time bounds. One type of graph of particular interest is called an expanding graph, whose properties we'll spend the rest of this section exploring. One of the many interesting features of expanding graphs is the difficulty, given a relatively simple definition, in constructing them. Aside from a handful of trivial examples, concrete families of expanding graphs are few and far between. As it turns out, for these graphs to be of any use to computer scientists, they need an explicit construction. One surprisingly efficient way of doing this involves taking a tour through geometric group theory, devising a group theoretic property, and then concluding that the Cayley graphs of certain finite groups with this property will have the desired graph structure. This will give us exactly what we since we can algorithmically construct the Cayley graph of a finite group.

Roughly speaking, expanders are graphs which are simultaneously both sparse and highly connected in a certain sense. We will concern ourselves with k-regular graphs (for which every vertex has k neighbors), since this simplifies our proofs and generalizing these results to all graphs is, apparently, not hard. Throughout we say that G is a finite, k-regular graph, with vertex set $V(G)$ and edge set $E(G)$. For some set $A \subseteq V(G)$, we denote by $\partial(A)$ the so called boundary of A, $\partial(A) = \{y \in V(G) : d(y, A) = 1\}$ where d is the usual graph metric.

Definition 1. A finite k-regular graph G with vertex set of size n is called an (n, k, c)-expander if for every subset $A \subseteq V(G)$,

$$|\partial(A)| \geq c\left(1 - \frac{|A|}{n}\right)|A|$$

To unpack this definition slightly, we can rephrase the above restriction as $|\partial(A)| \geq c\,|B|\,|A|/n$, where B is subgraph induced on the vertex compliment of A. One way of interpreting this is to say note that we are requiring the neighborhood of the set A to comprise at least as high a fraction of the remaining graph, up to some fixed constant multiple, as the set A comprises of the original graph. Or, most loosely, we want the neighborhood of A to be quite big provided that A isn't already too big. We can observe immediately that every finite graph is an expander for some sufficiently small $c > 0$, which gives us a family of relatively insignificant examples. We also note that the complete graph on n vertices is an $(n, n-1, 1)$-expander, but this graph is too dense to be useful. The notion becomes more interesting when we consider a family of graphs which are uniformly (n, k, c)-expanders for a fixed k and c as $n \to \infty$. We will now begin a detour into group theory to prove a method for constructing expander graphs.

2 Property T

2.1 Hilbert Spaces and Group Representations

Alas we'll need to introduce a few general terms before being able to define the group theoretic structure that will prove relevant in our discussion of expanding graphs. We've written this section to include minimal new terminology so many of the ideas expressed here have a more concise presentation, for which we encourage the interested reader to consult [1]. The first idea which will play in our general discussion is the notion that you can equip a group with additional topological structure.

Definition 2. A topological group G is a group with a topology such that the maps defining group multiplication (product map) and inversion (inverse map), given by

$$(g,h) \mapsto gh \qquad (G \times G \to G)$$
$$g \mapsto g^{-1} \qquad (G \to G)$$

are continuous maps. Here we give $G \times G$ the usual product topology. A locally compact group is a topological group such that every point is contained in a compact subset.

The notion of a topological group won't feature too prominently in our discussion, other than allowing us to state property (T) in its true form, but nonetheless it is instructive to see a few examples of topological groups, since the practical meaning of the idea is not as mysterious as the definition may suggest. We can make any group a topological group by giving it the discrete topology, but in this case the topology contributes nothing to our understanding of the group. One heuristic way of thinking about topological groups, as they are often seen in practice, is thinking about groups that act on geometric objects in a continuous way. Two examples are the familiar $\mathbb{R}$ under addition, and the circle group, $\mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}$.

We now turn towards the question of representing a group, which will be essential in our discussion of Property (T). We have already seen how a group acting on a space can be viewed as a homomorphism from that group into the group of symmetries on the space. We can alter this idea slightly to produce what's known as a group representation. In some sense the symmetries of a vector space are the linear transformations on that space, which form a group with composition. A group representation is a homomorphism from a group G into the set of linear transformations on some vector space V. In general this gives a powerful tool to study groups since it allows us to use linear algebra, which opens the door to a world of abstract and computational techniques. In our specific case we will barely scratch the surface of representation theory, only covering what's necessary to understand the definition of property (T). We will now make this idea more formal and more specific.

Definition 3. A Hilbert space, H, is a vector space over $\mathbb{C}$, complete with respect to an inner product map $\langle \ , \ \rangle : H \times H \to \mathbb{C}$ that satisfies the following properties:

1. (Symmetic) $\langle x, y \rangle = \overline{\langle y, x \rangle}$.
2. (Linear) $\langle c_1 x_1 + c_z x_2, y \rangle = c_1 \langle x_1, y \rangle + c_2 \langle x_2, y \rangle$ for $c_1, c_2 \in \mathbb{C}$.
3. (Positive-definite) $\langle x, x \rangle \geq 0$ and $\langle x, x \rangle = 0 \iff x = 0$.

Taking symmetry and linearity together, we also get linearity in the second argument of the inner product. We note that the inner product gives us a norm $\|x\| = \sqrt{\langle x, x \rangle}$, which gives us a metric (conversely, if we have a norm that satisfies the parallelogram equality, it implies an inner product). As part of this definition we must stipulate that H is complete with respect to the metric induced by the norm, which means that every sequence which is Cauchy with respect to the norm (in the usual real analytic sense), converges to a limit point in the space. Discussing completeness in detail here would take us too far afield, but this assumption lingers in the background and will sometimes pose serious problems if you forget about it. Moving back to the task at hand, for our purposes the vector spaces in our representations will be Hilbert spaces, and the transformations of interest will be unitary operators.

Definition 4. A unitary operator on H is a surjective linear transformation $T : H \to H$ that sends bounded sets to bounded sets and has the inner product preserving property,

$$\langle Tx, Ty \rangle = \langle x, y \rangle.$$

By convention the image of $x \in H$ under T is denoted Tx. The set of unitary operators on H is denoted $U(H)$ and forms a group under composition. The reader can also verify that unitary operators are norm preserving, in other words unitary operators are isometries on a Hilbert space! One important class of unitary operator on the Hilbert space $\mathbb{R}^3$ is the group of rotations, $SO(3)$. We are inching ever closer to being able to define property (T), which describes the way groups can be represented via homomorphisms into $U(H)$.

Definition 5. A unitary representation of a group G is a pair (H, ρ) where ρ is a homomorphism $\rho : G \to U(H)$ for some Hilbert space H. Each Hilbert space accommodates a trivial representation (H, ρ_0) where $\rho_0 : G \to U(H)$ sends every group element to the identity transformation. On the other hand, a unitary representation (H, ρ) is called essentially nontrivial if for every nonzero vector $v \in H$, we have some $g \in G$ where $\rho(g)v \neq v$.

In our definition of Property (T) we will be concerned with unitary, essentially nontrivial representations. To rephrase the above definition, a representation $\rho : G \to U(H)$ is essentially nontrivial if there are no one-dimensional subrepresentation. We are now ready to state the definition of property (T). There are many equivalent definitions of this property, but we have chosen to state the one that requires minimal background structure and will be most immediately useful for the construction of expander graphs.

Definition 6 (Definition 3.1.3 in [1])**.** A Group G has property T if there exist an $\epsilon > 0$ and a compact subset K of G such that for every unitary, essentially nontrivial representation (H, ρ) of G and every vector $v \in H$ of unit norm, we have $\|\rho(k)v - v\| > \epsilon$ for some $k \in K$.

This definition essentially stipulates that G has a compact subset K such that no matter how G is represented (as long as that representation is unitary and essentially nontrivial), every vector in the corresponding Hilbert space gets nudged sufficiently much by the transformation $\rho(k)$ given by some element $k \in K$. The discussion in the rest of this section is not essential for the construction of expanders, and the reader is encouraged to skip to the next section for that result, but we will include here a slightly deeper discussion of the definition of property (T), because I find that phrasing it in a slightly different way, although useless for the purposes of proving our main theorem, is very helpful in gaining intuition for the property.

Definition 7. Let $\rho : G \to U(H)$ be an essentially nontrivial, unitary representation, and let Q be some subset $Q \subseteq G$ and $\epsilon > 0$.

- A vector $h \in H$ is called (Q, ϵ)-invariant if

$$\sup_{g \in Q} \|\rho(g)h - h\| < \epsilon \|h\|$$

- The representation (H, ρ) is said to *almost have invariant vectors* if it has nonzero (Q, ϵ)-invariant vectors for every *compact* subset $Q \subseteq G$ and every $\epsilon > 0$.

- The representation (H, ρ) is said to *have invariant vectors* if there is some nonzero $h \in H$ such that $\rho(g)h = h$ for all $g \in G$.

The last item in this definition is the most straightforward: to have invariant vectors means there is some vector that is preserved by every transformation in $\rho(G)$. This contextualizes the second item in the definition, which is a sort of consolation for not quite having nonzero G-invariant vectors. To almost have invariant vectors means that for every compact set in G, there is a vector that is only nudged by an arbitrarily small amount by transformations coming from elements in that set. Think of this as analogous to the way that, in calculus, functions are often defined to have properties on every compact set, instead of on all of $\mathbb{R}$, and often this is good enough. In fact, consider the function space $L^2(\mathbb{R})$, the space of functions $f : \mathbb{R} \to \mathbb{R}$ with $\int_{-\infty}^{\infty} |f(x)|^2 \, dx < \infty$. It turns out $L^2(\mathbb{R})$ is a Hilbert space with norm given by the square root of the latter integral (try to guess what the inner product looks like, and prove that this indeed yields a Hilbert space), and that the representation $\lambda : \mathbb{R} \to U(L^2(\mathbb{R}))$ given by translations almost has invariant vectors. Indeed take some compact subset $Q \subseteq \mathbb{R}$ and $\epsilon > 0$. Compact subsets of $\mathbb{R}$ are bounded so there is some N such that $|t| < N$ for all $t \in Q$. Now let $M = \ 2N/\epsilon^2$ and χ be the characteristic function of the interval $[0, M]$, and define $h := \frac{h}{\sqrt{M}}$, a simple geometric argument shows that that for every $t \in Q$,

$$\|\lambda(t)h - h\|^2 = \frac{2\,|t|}{M} < \frac{2N}{M} = \epsilon^2.$$

We can now formulate property (T) in a slightly different way.

Definition 8.

(i) For a topological group G, a subset $K \subseteq G$ is called a Kazhdan set if there is some $\epsilon > 0$ such that every unitary, essentially nontrivial representation of G which has a (K, ϵ)-invariant vector also has a nonzero G-invariant vector.

(ii) The group G has property (T) if G has a compact Kazhdan set.

This is actually a morally weaker definition than the one we are using. The primary definition in this paper is sufficient to ensure a group has property (T) by giving a pair (K, ϵ) as above, and insisting that there are no (K, ϵ)-invariant vectors, so we don't need to worry about G-invariant vectors at all. To conclude the section, we will list some groups that do and don't have property (T). Unfortunately the proofs of these facts are all quite involved, so we will not explore them here, but suffice it to say that there are well-understood groups with property (T), with which the construction proved in the next section can proceed.

Proposition 1.

- ***Groups with Property*** (T)
  - *Compact tolological groups.*
  - *The additive group of p-adic integers.*
  - *Simple real Lie groups of rank at least two.*
  - $SL_3(\mathbb{R})$
- ***Groups without Property*** (T)
  - *The additive groups $\mathbb{R}$ and $\mathbb{Z}$.*
  - $SL_2(\mathbb{R})$*.*
  - *Free groups.*

2.2 An Explicit Construction of Expanders

In this section we will give a construction of a family of expanding graphs, which will end up being the Cayley graphs of a family of finite groups. It is worth noting here the fact that we are using a property of infinite groups, property (T), to construct a family of finite graphs, a small philosophical point that adds to the beauty of this construction. First we will prove the following technical proposition, which states that in our application we can use a generating set as the compact subset in the definition of property (T).

Proposition 2. *If G is a finitely generated discrete group with property (T), then for every generating set S there exists an $\epsilon > 0$ such that for every unitary, essentially nontrivial representation (H, ρ) and for every $v \in H$, there exists $s \in S$ such that $\|\rho(s)v - v\| > \epsilon \|v\|$.*

Take some essentially nontrivial, unitary representation (H, ρ). If G has property T then there exists a (necessarily finite) compact subset $K \subseteq G$ with some $k \in K$ and some $\epsilon > 0$ such that $\|\rho(k)u - u\| > \epsilon$ for every $u \in H$ of unit norm. For an arbitrary nonzero vector $v \in H$ we can write

$$\|\rho(k)v - v\| = \|v\| \left\| \rho(k)\frac{v}{\|v\|} - \frac{v}{\|v\|} \right\| > \|v\| \epsilon,$$

since $\frac{v}{\|v\|}$ has unit norm. This is because $\rho(k)$ is unitary and thus norm preserving. Now fix ϵ' and suppose that for every $s \in S$, we had $\|\rho(s)v - v\| \leq \epsilon' \|v\|$ for some $v \in H$. Since K is finite we can say that the word length of every element $k \in K$ over S is at most l. Thus $\rho(k) = \rho(s_1) \cdots \rho(s_l)$, where some s_i may be the identity. We can now apply the triangle inequality to bound $\|\rho(k)v - v\|$. Since $\rho(k)$ is a unitary linear transformation, and since $s_l^{-1} \in S$ then by assumption $\left\|v - \rho(s_l^{-1})v\right\| \leq \epsilon' \|v\|$, and so we have

$$\|\rho(s_1 \cdots s_l)v - \rho(s_1 \cdots s_{l-1})v\| = \left\|\rho(k)\left(v - \rho(s_l^{-1})v\right)\right\| \leq \epsilon' \|v\| = \epsilon' \|v\|.$$

By the same argument we have $\|\rho(s_1 \cdots s_{l-1})v - \rho(s_1 \cdots s_{l-2})v\| \leq \epsilon' \|v\|$ and proceeding in this way we eventually have $\|\rho(s_1 s_2)v - \rho(s_1)v\| \leq \epsilon' \|v\|$ and then $\|\rho(s_1)v - v\| \leq \epsilon' \|v\|$, so by the triangle inequality we have $\|\rho(k)v - v\| \leq l\epsilon' \|v\|$ for all $k \in K$. Now if we can make ϵ' arbitrarily small, then we can make it small enough to contradict the assumption that $\|\rho(k)v - v\| > \epsilon \|v\|$, so there must be some $\epsilon' > 0$ such that the proposition is true.

We are now ready to use the results above to give way of constructing expanding graphs from groups with property (T). This transfers the task of exhibiting graphs with this property to the somewhat easier (though still not easy) task of exhibiting groups with property (T). Let G be a finitely generated group with property (T). Let $\mathcal{L}$ be a family of finite index normal subgroups, and let S be a finite generating set with $S^{-1} = S$.

Theorem 1 (Proposition 3.3.1 in [1])**.** *The family of Cayley graphs of the finite groups G/N for $N \in \mathcal{L}$ with respect to the generating set S is a family of $(|G/N|, |S|, c)$-expanders.*

We define a Hilbert space H as the set of complex valued functions on the finite set $G' = G/N$ with norm $\|f\|^2 = \sum_{x \in G'} |f(x)|^2$. To specify a representation $\rho : G \to U(H)$, we will let $\rho(g)$ be the transformation on H that sends $f(x)$ to $f(gx)$. There are several things that need to be checked: that the transformation $\rho(g)$ is a linear transformation, that it is unitary, and that ρ is a homomorphism. The last item can be seen by viewing ρ as a group action of G on H, the first two can be seen by noting that multiplication by any $g \in G$ simply permutes the elements of $G' = G/N$.

The representation $\rho : G \to U(H)$ is not essentially nontrivial, but the action of G on G' by multiplication is transitive, so the only functions in H which are G invariant, i.e. for which $\rho(g)f = f$ for all $g \in G$, are the constant functions. These G invariant functions generate G invariant subspaces, so if we wish to restrict our representation to an essentially nontrivial representation, we must eliminate them. Thus we can take the G invariant subspace $H_0 = \{f \in H : \sum_{x \in G'} f(x) = 0\}$, forcing the only constant function to be the zero element.

Now we can use the fact that G has property (T) to invoke the proposition above, giving that there exists an $\epsilon > 0$ which is not dependent on N such that for every $f \in H_0$, $\|\rho(s)f - f\| > \epsilon \|f\|$ for some $s \in S$. Let $A \subseteq G'$ be some subset of size a and B be its complement of size $b = n - a$. We can now define a function $f \in H_0$ as follows

$$f(x) = \begin{cases} b & \text{if } x \in A \\ -a & \text{if } x \in B. \end{cases}$$

Then we have

$$\|f\|^2 = ab^2 + ba^2 = (a+b)ab.$$

We also have that for $s \in S$,

$$\|\rho(s)f - f\|^2 = (a+b)^2 N_s,$$

where we define $N_s = |\{g \in G' : x \in A \text{ and } xs \in B \text{ or } x \in B \text{ and } xs \in A\}|$. In other words N_s counts the number of edges between A and a vertex in its neighborhood for which a specific generator $s \in S$ is responsible. Note that N_s also gives us a lower bound on the number of neighbors in $\partial(A)$,

$$|\partial A| \geq \frac{1}{2} N_s,$$

since each edge is caused by some generator, and N_s over counts the contribution of each generator at most twice for degree two generators. We have the equality above for $\|\rho(s)f - f\|^2$ because $\rho(s)f$ takes the same values as f on vertices $g \in G'$ which are not swapped between A and its neighborhood, and takes alternate value on vertices which are. Using the conclusion we derived from the fact that G has property (T), there exists $s \in S$ such that, recalling that $n = a + b$, we have

$$|\partial A| \geq \frac{1}{2} N_s = \frac{\|\rho(s)f - f\|^2}{2n^2} \geq \frac{\epsilon^2 \|f\|^2}{2n^2} = \epsilon^s \frac{ab}{2n} = \frac{\epsilon^2}{2} \left(1 - \frac{|A|}{n}\right) |A|.$$

This exactly shows that the Cayley graphs of $G' = G/N$ are expanders for any $c \geq \frac{\epsilon^2}{2}$.

References

[1] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Birkhauser Verlag, 1993.

[2] B. Bekka, P. de la Harpe and A. Valette, *Kazhdan's Property (T)*, 2007.