Expander Graphs and their Applications*
Lecture 12: Cayley graph expanders

Notes taken by Eyal Rozenman

March 2002

Summary: We describe ideas leading to an elementary construction of Cayley graphs which are expanders with relatively small degree.

A set of elements S in a group H is a *generating set* if every element of $h \in H$ can be written as $h = s_1 \cdot s_2 \ldots \cdot s_k$ with $s_i \in S$.

Definition 1. The *Cayley graph* $C(H, S)$ of a group H and a generating set S is a graph whose vertices are the elements of H, and where (g, h) is an edge if $g \cdot s = h$ for some $s \in S$.

This generally defines a directed graph. If the set of generators S is *symmetric* - i.e. $s \in S$ iff $s^{-1} \in S$, then (g, h) is an edge iff (h, g) is, and we have an undirected graph. It is a regular graph of degree $|S|$.

Example 2.

- The additive cyclic group $C_d = \mathbb{Z}/d\mathbb{Z}$ with generators $S = \{+1, -1\}$ is the cycle on d vertices.
- The additive group of the vector space $(F_2)^d$ over the field with two elements is generated by the standard basis vectors $e_1 = (1, 0, \ldots, 0), e_2, \ldots, e_d$. The Cayley graph is the discrete cube - a d-regular graph.

Consider the following construction, resulting in the graph depicted in figure 1. The degree of the discrete cube is equal to the number of vertices in the d-cycle, so we can form a zigzag product of the two. Let's look at the simpler replacement product. In this product we replace every vertex of $(F_2)^d$ by a cloud of d vertices representing C_d. On each cloud we preserve the edges of the original C_d. We also connect each vertex in the cloud to one of the d neighbors of the cloud in F_2^d. For example, let's connect vertex (v, h) to $(v + e_h, h)$. Like the zigzag construction, this product is an expander if the original two graphs are expanders.

We started with two Cayley graphs and created a third graph by a graph-theoretic construction. Is the resulting graph also a Cayley graph of some group? The answer is yes. It's the *semidirect product* of C_d and F_2^d. To define this product we shall need (alas) some more definitions:

Definition 3. An *action* of a group B on a group A is a group homomorphism $\phi : B \to Aut(A)$. In other words, each element $b \in B$ corresponds to an automorphism ϕ_b of A, and we demand that $\phi_{b_1 \cdot b_2} = \phi_{b_1}\phi_{b_2}$.

Definition 4. Suppose a group B acts on a group A. The *semidirect product* $A \rtimes B$ is a group whose elements are pairs (a, b) where $a \in A$ and $b \in B$. We define

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot \phi_{b_1}(a_2), b_1 \cdot b_2).$$

Example 5.

- The direct product of two groups $A \times B$ is a special case of a semidirect product where ϕ_b is the identity automorphism of A for all $b \in B$. In this case $(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$.

* Lecture Notes for a course given by Nati Linial and Avi Wigderson at the Hebrew University, Israel.

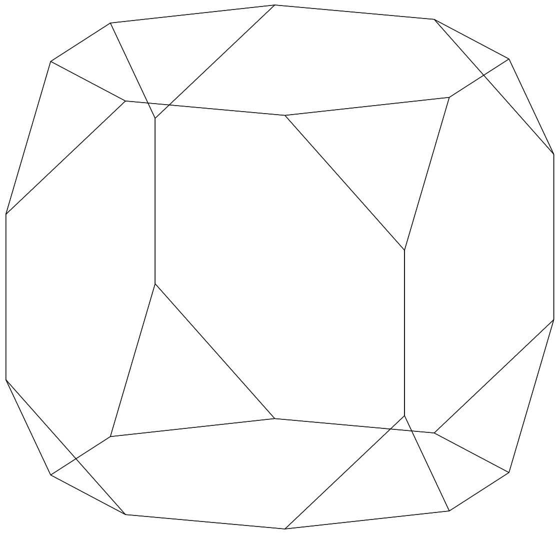

Figure 1: *A Cayley graph of $F_2^3 \rtimes C_3$*

- We have an action of C_d on F_2^d: the element $h \in C_d$ cyclically permutes the coordinates of F_2^d by h places. We can thus define $F_2^d \rtimes C_d$.

It turns out that under certain conditions there is a close relation between the semidirect product of groups and the replacement product of their Cayley graphs. Suppose a group B acts on a group A. The *orbit* of an element $a \in A$ under the action of B is the set $\{\phi_b(a) | b \in B\}$. For example, the orbit of $v \in F_2^d$ under the action of C_d is the set of all cyclic shifts of v

Claim 6. *Suppose we have two groups A, B with sets of generators S_A, S_B, such that $|B| = |S_A|$. Further, suppose that B acts on A in such a way that S_A is the orbit of one of the elements $x \in S_A$. Then $S := (1, S_B) \cup \{(x, 1)\}$ generates $A \rtimes B$, and $C(A \rtimes B, S)$ is a replacement product of $C(A, S_A)$ and $C(B, S_B)$.*

Proof. To see that S indeed generates $A \rtimes B$ notice that the elements $(S_A, 1) \cup (1, S_B)$ generate it. Now observe that $(1, b) \cdot (x, 1) \cdot (1, b^{-1}) = (\phi_b(x), 1)$, so we can indeed generate all of $(S_A, 1)$ starting with $(x, 1)$, so $(1, S_B) \cup \{(x, 1)\}$ is generating. Look at $C(A \rtimes B, S)$. It consists of clouds of the elements of B, with the graph of $C(B, S_B)$ on them, since $(a, b) \cdot (1, s_b) = (a, b \cdot s_b)$. Between clouds we have edges like $(a, b) \cdot (x, 1) = (a \cdot \phi_b(x), b)$. So the cloud of the element a is indeed connected by one edge to each of the clouds of the neighbors of a in the graph $C(A, S_A)$, and this is a replacement product. $\square$

Exercise 7. Under the assumptions of the claim, we can also describe the zigzag product of two Cayley graphs as a Cayley graph on $A \rtimes B$. Which generating set do we need?

Example 8. Look at F_2^3 and C_3 with the generators used above. In the Cayley graph of $F_2^3 \rtimes C_3$ with generators as in the claim, the neighbors of the cloud of $v = (1, 0, 0) \in F_2^3$ are:

$$\begin{aligned}
(v, 0) \cdot (e_0, 0) &= (v + e_0, 0) \\
(v, 1) \cdot (e_0, 0) &= (v + e_1, 1) \\
(v, 2) \cdot (e_0, 0) &= (v + e_2, 2)
\end{aligned}$$

And this is indeed a replacement product.

Recall that a replacement product of two expander graphs is again an expander. So we can try to make an expander graph which is also a Cayley graph using the semidirect product. As a starter, we look for generators for F_2^d that make it an expander. Since this is an abelian group, then for every set of generators the eigenvectors of the graph are the Fourier basis - which are vectors of the type $f_y(x) = (-1)^{<x,y>}$. For the standard basis $e_1, \ldots e_d$ the eigenvalues are

$$\sum_i f_y(e_i) = \sum_i (-1)^{<e_i,y>} = d - 2|y|$$

Where $|y|$ is the Hamming weight of the binary vector y. So $\lambda_1 = d, \lambda_2 = d - 2$. The second normalized eigenvalue is $(d-2)/d$ and obviously, this is not a good expander. How do we find another set of generators which does give an expander? Suppose we have a set $S = \{v_1, v_2, \ldots, v_r\}$ of generators. Write an $|S| \times d$ matrix A whose rows are the elements of S. To be an expander, we need to satisfy, for every $y \neq 0$

$$\sum_i f_y(v_i) = \sum_i (-1)^{<v_i,y>} \leq c \cdot |S|$$

for some constant $c < 1$, independent of d. This means that the vectors Ax (with $x \neq 0$) don't have too much difference between the numbers of 0's and 1's. In particular, each word must have a sufficient number of 1's. In short - a good expander in this case gives an error correcting code. Using this intuition, one would try a random $2d \times d$ matrix A, which we know gives a good code, and indeed

Claim 9. *For a random $2d \times d$ binary matrix, almost surely $2d \cdot \delta < |Ax| < 2d \cdot (1-\delta)$ for all nonzero x (for some constant $\delta > 0$).*

So we have an expander. With two "small" flaws: (a) It's not explicit, and (b) The degree is too large. To get rid of flaw (b) we want not just an arbitrary set of generating vectors. We want the generators to be one orbit under the action of C_n, for example. Luckily, this also turns out to work

Claim 10. *Pick two random vectors $u, v \in F_2^d$. Consider the matrix A generated by the orbits of u and v under the action of C_d, that is, the $2d \times d$ matrix of the cyclic shifts of u and v. Then A (a.s.) satisfies $2d \cdot \delta < |Ax| < 2d \cdot (1-\delta)$ for all nonzero x (for some constant $\delta > 0$).*

So now, by using a semidirect product with C_d we get an expander. The only difference is that we used two orbits, instead of one as in claim 6.

Exercise 11. Claim 6 still holds when S_A is a union of k orbits under the action of B. The Cayley graph of the semidirect will have $|S_B| + k$ generators.

We can now use this idea to give a counterexample to

Conjecture 12. *If a group sequence G_n is an expander with one set of generators S_n of bounded size then it is also an expander with any other set of generators U_n of bounded size.*

Recall that we have two matrices that (with their inverses) make $SL_2(F_p)$ an expander. $SL_2(p)$ acts on the $p+1$ elements of the projective plane over F_p, so just as we did with C_d we can form the semidirect product $F_2^{p+1} \rtimes SL_2(p)$. It also turns out that there are two orbits of SL_2 that make F_2^{p+1} an expander (random orbits will do). So the semidirect product is an expander with 4 generators, for every p. On the other hand, we have another set of generators for which F_2^{p+1} is not an expander - the standard basis. This gives a set of 3 generators for $F_2^{p+1} \rtimes SL_2(p)$ which is not an expander (recall that the replacement product is never a better expander than its components).

Can we iterate the semidirect product construction to get a sequence of Cayley expander graphs the same way we did with the zigzag product? For a group G let $F_p[G]$ be the group ring over F_p. we would like to make the additive group an expander using a constant number of orbits under the action of G. If we could do that in general, we could define a sequence iteratively by $G_{i+1} = F_{p_i}[G_i] \rtimes G_i$. This is indeed possible with a proper choice of p_i and G_1:

Theorem 13. *$\lambda_2(C(G_n, S_n)) \leq 1/2$ and $S_n \leq log^{(n/2)}|G_n|$ where $log^{(n/2)}$ is the iterated logarithm.*

This is the (almost) best construction of this type we can hope to get using this construction, since the group G_n is a solvable group with solvability index at most n (as G_{n-1} is a normal subgroup with abelian quotient $F_{p_{n-1}}[G_{n-1}]$). In this case it is known that any generating set which gives $\lambda_2 \leq 1/2$ has cardinality at least $log^{(n)}|G_n|$

The property we need to make $F_p[G]$ an expander with a constant number of orbits is

Theorem 14. *Let $d_1, d_2, \ldots, d_t$ be the dimensions of the irreducible representations of G. if $|\{i : d_i < r\}| < c^r$ for all integer r and some constant c, then there is a constant number of orbits of $F_p[G]$ that make it an expander.*

Miraculously, $F_p[G]$ inherits this property if G is a **monomial group**, which means all its irreducible representations are induced from one-dimensional representations of subsets of G. Furthermore, $F_p[G]$ is also monomial! Even better, we can find the generating orbits explicitly. This gives a sequence of explicit Cayley graphs which are expanders with an "almost constant" number of generators.