Chapter 4

Diameters of Cayley Graphs and Expander Families

Good communication networks = Messages spread quickly = Small diameters
In this chapter, we show necessary conditions for expander family related to diameters (namely logarithmic diameter), and these conditions can be further related to group structures. There is no equivalent conditions: we illustrate this in the end of the chapter by constructing an "almost" expander family example.

4.1 Expander Families have Logarithmic Diameter

Definition 4.1. Graph X, vertex v of X, non-negative integer r. Define the **closed ball** of radius r centred at v as $B_r[v]$, the **sphere** of radius r centred at v as $S_r[v]$.

$$B_r[v] = \{w \in V_X \mid \operatorname{dist}(v, w) \leq r\}$$
$$S_r[v] = \{w \in V_X \mid \operatorname{dist}(v, w) = r\}$$

Remark

- This terminology resembles that of metric spaces. Recall that dist is a metric.
- By definition, $B_r[v], S_r[v] \subset V_X$ for any r.

Lemma 4.2. $\{X_n\}$ is a sequence of d-regular graphs with $|X_n| \to \infty$ and $d \geq 3$. Then, $\operatorname{diam}(X)$ grows at least logarithmically. Equivalently, $\operatorname{diam}(X_n) = \Omega(\ln X_n)$.

Proof

- Consider the case with $\text{diam}(X) \geq 3$. Let v be a vertex of X. Suffice to show $\text{diam}(X) \geq \log_d |X|$
- Note $|S_0[v]| = 1$ and $|S_1[v]| \leq d$ (strict $<$ for loops).
- If $j \geq 2$, then for any vertex w of $S_j[v]$, at least one edge incident ot w is also incident to a vertex in $S_{j-1}[v]$. Hence, no more than $d-1$ of these edges are incident to vertices in $S_{j+1}[v]$. Thus, $|S_{j+1}[v]| \leq (d-1)|S_j[v]|$,
- Induction, $|S_j[v]| \leq d(d-1)^{j-1}$ (since $|S_1[v]| \leq d$).
- For any r, $B_r[v]$ is the disjoint union of $S_0[v], S_1[v], \ldots, S_r[v]$, thus

  $$|B_r[v]| \leq 1 + d\left(\sum_{j=0}^{r-1}(d-1)^j\right)$$

  .
- RHS is a polynomial in d of degree r, thus controlled by d^r. Claim: for $r \geq 3$, $|B_r[v]| \leq d^r$.
- Note for $r \geq 3$, $0 \leq d^2 - 3d + 1$, thus $(d-1)^3 \leq d^2(d-2)$, thus $d(d-1)^r = (d-1)^{r-3}(d-1)^3 \leq d^{r-3}d^2(d-2) = d^{r-1}(d-2)$, thus $d(d-1)^r - 2 \leq d(d-1)^r \leq d^r(d-2)$.
- Hence,

  $$|B_r[v]| \leq 1 + d\left(\sum_{j=0}^{r-1}(d-1)^j\right) = 1 + d\left[\frac{(d-1)^r - 1}{d-2}\right] \leq d^r$$

- Let $r = \text{diam}(X)$, thus $|X| = |B_r[v]| \leq d^r$, so $\text{diam}(X) \geq \log_d |X|$

Remark
Logarithmic diameter growth is the slowest possible case. Our next goal is show expander family must achieve this slowest growth case.

Lemma 4.3. Connnected finite graph X. Let $a > 1$. Suppose that for any vertex v of X, $|B_{r-1}[v]| \leq \frac{1}{2}|X|$ always implies that $|B_r[v]| \geq a^r$. Then

$$\text{diam}(X) \leq \left(\frac{2}{\ln a}\right) \ln |X|$$

Proof

- w_1, w_2 two vertices of X. Let r_1 be the smallest non-negative integer s.t. $|B_{r_1}[w_1]| > \frac{1}{2}|X|$. Such r must exist since X is connected thus having finite diameter.

- Then by assumption $|B_{r_1}[w_1]| \geq a^{r_1}$, since $r_1 - 1 < r_1$ and therefore $|B_{r_1-1}[w_1]| \leq \frac{1}{2}|X|$.
- Similarly, let r_2 be the smallest non-negative integer s.t. $|B_{r_2}[w_2]| > \frac{1}{2}|X|$, thus $|B_{r_2}[w_2]| \geq a^{r_2}$
- Note $|B_{r_1}[w_1]| + |B_{r_2}[w_2]| > |X|$, so $B_{r_1}[w_1] \cap B_{r_2}[w_2] \neq \varnothing$. Let $w_3 \in B_{r_1}[w_1] \cap B_{r_2}[w_2]$.
- Then $\operatorname{dist}(w_1, w_3) \leq r_1,\ \operatorname{dist}(w_2, w_3) \leq r_2$, so

  $$\begin{aligned}\operatorname{dist}(w_1, w_2) &\leq \operatorname{dist}(w_1, w_3) + \operatorname{dist}(w_3, w_2)\\ &\leq \log_a|B_{r_1}[w_1]| + \log_a|B_{r_2}[w_2]|\\ &\leq \left(\frac{2}{\ln a}\right)\ln|X|\end{aligned}$$

  ($B_{r_1}[w_1], B_{r_2}[w_2]$ are all subset of V_X)
- Since this holds for arbitrary w_1, w_2, done.

Proposition 4.4. *X is a connected d-regular graph. Let $C = 1 + \frac{h(X)}{d}$. Then*

$$\operatorname{diam}(X) \leq \left(\frac{2}{\ln C}\right)\ln|X|$$

Remark
If $h(X_n)$ is bounded away from 0 (hence an expander family), then $\operatorname{diam}(X_n)$ grows at most logarithmically as a function of $|X_n|$. From Lemma 4.2, we know this is the slowest growth possible.

Proof

- Let v be a vertex. Suppose $|B_{r-1}[v]| \leq \frac{1}{2}|X|$, then by definition of isoperimetric constant,

  $$|\partial B_{r-1}[v]| \geq h(X)|B_{r-1}[v]|$$

- Any edge in $\partial B_{r-1}[v]$ must be incident to a vertex in $S_r[v]$. Since X is d-regular, we have

  $$|S_r[v]| \geq \frac{\partial B_{r-1}[v]}{d} \geq \frac{h(X)}{d}|B_{r-1}[v]|$$

- Note $B_r[v]$ is the disjoint union of $B_{r-1}[v]$ and $S_r[v]$, thus

  $$|B_r[v]| = |B_{r-1}[v]| + |S_r[v]| \geq |B_{r-1}[v]| + \frac{h(X)}{d}|B_{r-1}[v]| = C|B_{r-1}[v]|.$$

- By induction, $|B_r[v]| \geq C^r$, which is implied by $|B_{r-1}[v]| \leq \frac{1}{2}|X|$. Hence, by Lemma 4.3, substitute a by C, done.

Definition 4.5. $\{X_n\}$ has logarithmic diameter if $\text{diam}(X_n) = O(\ln|X_n|)$

Corollary 4.6. Non-negative integer d. If $\{X_n\}$ is a family of d-regular expanders, then $\{X_n\}$ has logarithmic diameter.

4.2 Diameters of Cayley Graphs

Definition 4.7. Let $\{G_n\}$ be a sequence of finite groups. We say $\{G_n\}$ has logarithmic diameter if for some non-negative integer d, there exists $\{\Gamma_n\}$ s.t. $\Gamma_n \overset{s}{\subseteq} \mathrm{G}_n$ and $|\Gamma| = d$ for each n, so the sequence of Cayley graphs $\{\text{Cay}(G_n, \Gamma_n)\}$ has logarithmic diameter.

Definition 4.8. Let Γ be a set, n be a positive integer. Then a **word** of length n in Γ is an element of the Cartesian product $\Gamma \times \cdots \times \Gamma = \Gamma^n$. If $\Gamma \subset G$ for some group G and $w = (w_1, \ldots, w_n)$ is a word in Γ, then w evaluates to g in G if $g = w_1 \ldots w_n$.

Remark
Clearly, an element in G can be expressed as different words. It's also possible that for certain Γ, some elements in G cannot be expressed as any word. An example is $G = \mathbb{Z}_{10}, \ \Gamma = \{0, 2, 4, 6, 8\}$

Definition 4.9. Group G, $\Gamma \subset G$, $g \in G$ and can be expressed as a word in Γ. The **word norm** of g in Γ is the minimal length of any word in Γ that evaluates to g. By convention, identity element has word norm 0.

Proposition 4.10. Finite group G. Let Γ symmetric in G and $X = \text{Cay}(G, \Gamma)$ Then:

1 X is connected iff every element of G can be expressed as a word in Γ.

2 If $a, b \in G$ and there is a walk in X from a to b, then the distance from a to b is the word norm of $a^{-1}b$ in Γ.

3 The diameter of X equals the maximum of the word norms in Γ of elements of G.

Proof

1 Equivalent to say Γ generates G.

2
- Let $a = g_0, b = g_n$, and $(g_0, g_1, \dots, g_n)$ be a walk of length n in X from a to b.
- Let $\gamma_j = g_{j-1}^{-1} g_j$ for $j = 1, \dots, n$. Then since there is an edge from g_{j-1} to g_j, we have $\gamma_j \in \Gamma$ and $(\gamma_1, \dots, \gamma_n)$ is a word of length n in Γ that evaluates to $a^{-1}b$.
- Reversing this procedure, we see that every word of length n in Γ that evaluates to $a^{-1}b$ corresponds to a path of length n in X from a to b.
- Thus, the distance from a to b is the minimal length of all walks from a to b, which equals to the minimal length of all words hence the word norm of $a^{-1}b$.

3 Natural implication of (2).

4.3 Abelian Groups Never Yield Expander Families

Lemma 4.11. The number of solutions to the equation $a_1 + \cdots + a_n = k$, where a_i are non-negative integers, is

$$C_{n+k-1}^{k}$$

Proof
Equivalently, consider partitioning $k + n$ balls into n boxes, and each box has at least one ball. You can place $n - 1$ boards between these balls to make the partition, and there are $k + n - 1$ spaces where you can place boards.

Lemma 4.12. If $a, b \in \mathbb{N},\ b \leq a$, then

$$C_a^b \leq (a - b + 1)^b$$

Proof
Observe that if $0 < q \leq p$, then $\frac{p+1}{q+1} \leq \frac{p}{q}$. Hence

$$\frac{a}{b} \leq \frac{a-1}{b-1} \leq \cdots \leq \frac{a-b+2}{2} \leq \frac{a-b+1}{1}$$

So

$$C_a^b = \frac{a}{b} \frac{a-1}{b-1} \cdots \frac{a-b+2}{2} \frac{a-b+1}{1} \leq (a-b+1)^b$$

This bound is not sharp, but suffices for our purpose.

Proposition 4.13. No sequence of finite abelian groups has logarithmic diameter. Therefore, no sequence of abelian groups yields an expander family.

Remark
If a sequence of finite groups admits an unbounded sequence of abelian groups as quotients, then by Quotients Nonexpansion Principle, it does not yield an expander family.

Proof

- Finite abelian group G; $\Gamma \subseteq_s G$; $d = |\Gamma|$; $\gamma_1, \ldots, \gamma_d$ be the elements of Γ. Let $X = \text{Cay}(G, \Gamma)$, $k = \text{diam}(X)$ Since Γ generates G, k is finite, and every element of G can be expressed as a word in Γ of length less than k.
- Since G is abelian, we can rearrange the elements in the word, so that every element of G is of the form

  $$e^{a_0}\gamma_1^{a_1}\ldots\gamma_d^{a_d}$$

  where e is the identity and $\sum_{i=0}^{d} a_i = k$, each a_i non-negative integer. (without identity, the sum of a_i would not be constant)
- By Lemma 4.11, the number of distinct elements of this form is bounded above by C_{k+d}^{k}. Then, by Lemma 4.12, $|X| \leq C_{k+d}^{k} = C_{k+d}^{d} \leq (k+1)^d$, so $\text{diam}(X) \geq |X|^{1/d} - 1$
- For $\{X_n\}$, we have $\text{diam}(X_n) \geq |X_n|^{1/d} - 1$, but RHS is a roof function, which grows faster than logarithmic functions, done.

4.4 Diameters of Subgroups and Quotients

Diameter's version of Subgroup Nonexpansion Principle, where we connect subgroup and original with spanning subgraph.

Definition 4.14. Graph X, Y. Define composite graph of X and Y, $C(X \times Y)$, as follows.

- Vertex set: $X \times Y$
- Set of edges between (x_1, y_1) and (x_2, y_2) is the set of pairs (e_1, e_2), s.t. e_1 is an edge in X between x_1 and x_2, and e_2 is an edge in Y between y_1 and y_2.

Example
See figure 4.1.

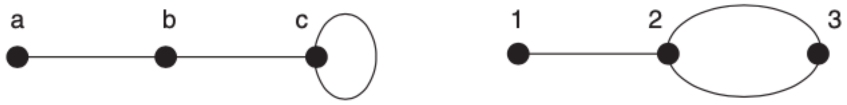

Figure 4.4 X (left) and Y (right)

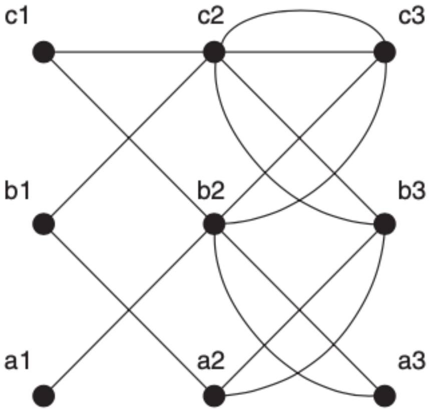

Figure 4.5 $C(X \times Y)$

Figure 4.1:

Definition 4.15. Graph X with vertex set V, edge multiset E. A spanning subgraph X' of X is a graph with vertex set V and edge set E', where $E' \subset E$.

Remark
Spanning refer to the fact that X' uses every vertex of X. Strangely, X' defined in this way must be a simple graph. Also, it's possible that X is connected while X' is not.

Lemma 4.16. Suppose X is a spanning subgraph of a finite graph Y. Then $\mathrm{diam}(X) \geq \mathrm{diam}(Y)$.

Proof
Some walk in Y may not exist in X, but any walk in X must exist in Y. So the distance between two vertices in X is no shorter than that in Y.

Lemma 4.17. Finite graphs X, Y. Then $\mathrm{diam}(C(X \times Y)) \geq \mathrm{diam}(X)$, and $\mathrm{diam}(C(X \times Y)) \geq \mathrm{diam}(Y)$

Proof
Let $x_1, x_2 \in X,\ y_1, y_2 \in Y$. A walk of length l in $C(X \times Y)$ from (x_1, y_1) to (x_2, y_2) corresponds to a walk of length l in X from x_1 to x_2. So distance in $C(X \times Y)$ is no more than that in X.

Lemma 4.18. Finite group G, $H \leq G$, T is the set of transversals, $\Gamma \subseteq_s G$. Then $\mathrm{Cay}(G, \Gamma)$ is isomorphic to a spanning subgraph of $C(\mathrm{Cay}(H, \hat{\Gamma}) \times \mathrm{Cos}(H \backslash G, \Gamma))$.

Proof
First, we identify vertices.

- Define $\phi :\ G \to H \times (H \backslash G)$, by $\phi(g) = (g(\overline{g})^{-1}, Hg)$
- For (h, Ha), we can find $\phi(h\overline{a}) = (h, Ha)$. Surjectivity done.
- Suppose $(g_1(\overline{g_1})^{-1}, Hg_1) = (g_2(\overline{g_2})^{-1}, Hg_2)$, then $Hg_1 = Hg_2$, then $\overline{g_1} = \overline{g_2}$. Since $g_1(\overline{g_1})^{-1} = g_2(\overline{g_2})^{-1}$, thus $g_1 = g_2$. Injectivity done.

Then, we identity edges. Note this is just isomorphic to one spanning subgraph, so we only need to show injectivity.

- $\gamma \in \Gamma, g \in G$. Then γ induces an edge in $\mathrm{Cay}(G, \Gamma)$ from g to $g\gamma$. The corresponding edge in $C(\mathrm{Cay}(H, \hat{\Gamma}) \times \mathrm{Cos}(H \backslash G, \Gamma))$ comes from the edge pair (e_1, e_2).
- Suppose we have two equal edge pairs (e_1, e_2) and (e_1', e_2'), then e_1, e_1' must be induced from same vertex, e_2, e_2' must be induced from same vertex, and by arguments in matching vertices, we know the corresponding edges in $\mathrm{Cay}(G, \Gamma)$ must be induced from same vertex, so these two edges are the same. Injectivity done.

Proposition 4.19. Let G, H, Γ, T be defined as above. Then

$$\begin{aligned}\operatorname{diam}(\operatorname{Cay}(G,\Gamma)) &\geq \operatorname{diam}(\operatorname{Cay}(H,\hat{\Gamma}))\\ \operatorname{diam}(\operatorname{Cay}(G,\Gamma)) &\geq \operatorname{diam}(\operatorname{Cos}(H\backslash G,\Gamma))\end{aligned}$$

Proof
$\operatorname{Cay}(G,\Gamma)$ - some spanning subgraph of $C(\operatorname{Cay}(H,\hat{\Gamma}) \times \operatorname{Cos}(H\backslash G,\Gamma))$.

Proposition 4.20. $\{G_n\}$ a sequence of finite groups. Suppose $\{G_n\}$ admits $\{H_n\}$ as a bounded-index sequence of subgroups. If $\{H_n\}$ does not have logarithmic diameter, so does $\{G_n\}$. Therefore, $\{G_n\}$ would not yield an expander family.

Remark
The Quotient Version is false. It is possible that while quotients do not have logarithmic diameter, the originals have. An example is given in section 7.

Proof

- Suppose $\{\operatorname{Cay}(G_n,\Gamma_n)\}$ has logarithmic diameter for some sets Γ_n, s.t. $|\Gamma_n|$ constant and $\Gamma_n \Subset G_n$ for all n. Let T_n be a set of transversals for H_n in G_n.
- Let M s.t. $[G_n : H_n] \leq M$ for all n. Let
$$\Lambda_n = \hat{\Gamma_n} \cup \{(M - [G_n : H_n])|\Gamma_n| \cdot e_n\}$$
- Following similar argument in Prop.2.24 and by Prop.4.19, we have
$$\begin{aligned}\operatorname{diam}(\operatorname{Cay}(H_n,\Lambda_n)) &= \operatorname{diam}(\operatorname{Cay}(H_n,\hat{\Gamma_n}))\\ &\leq \operatorname{diam}(\operatorname{Cay}(G_n,\Gamma_n))\\ &\leq C\ln|G_n| \quad \text{(Lemma 4.3)}\\ &\leq C\ln|H_n| + C\ln M \quad (|G_n| = |H_n|[G_n : H_n])\\ &\leq 2C'\ln|H_n| \quad (C\ln M \text{ must be bounded})\end{aligned}$$

  So $\{H_n\}$ has logarithmic diameter now, contradiction.

Lemma 4.21. Dihedral groups D_n do not have logarithmic diameter.

Proof
Let $H_n = \langle r\rangle \cong \mathbb{Z}_n$, thus $\{H_n\}$ do not have logarithmic diameter by Prop.4.13. Note $[D_n : H_n] = 2$ for all n, so by Prop.4.20, D_n do not have logarithmic diameter.

4.5 Solvable Groups with Bounded Derived Length

Definition 4.22. Group G. An element of the form $a^{-1}b^{-1}ab$ for some $a, b \in G$ is a **commutator**. Define G' to be the subgroup of G generated by the set of all commutators in G. G' is the **commutator subgroup** of G.

Definition 4.23. Group G. We recursively define a sequence of subgroups of G, as follows:

$$\begin{aligned} G^{(0)} &= G, \\ G^{(1)} &= G', \\ &\dots \\ G^{(k+1)} &= (G^k)' \end{aligned}$$

The group $G^{(k)}$ is the **kth derived subgroup** of G.

Remark
That is, each recursion is taking a commutator subgroup, and the 1st derived subgroup of G is exactly the commutator subgroup of G.

Definition 4.24. Group G. G is solvable with derived length 0 if G is the trivial group. G is solvable with derived length $k+1$ if G^k is nontrivial but G^{k+1} is trivial.

Remark

- G is abelian iff G is solvable with derived length 1. In this case, the only commutator is the identity.
- To say a finite group is solvable means it is "built up out of abelian pieces". The derived length is the minimum number of pieces required.

Lemma 4.25. Group G. Then:

1 $G' \lhd G$

2 If N is a normal subgroup of G, then G/N is abelian iff $G' \leq N$. That is, G' is the smallest normal subgroup with associated quotient being abelian.

Proof

1 For arbitrary $h \in G'$, $h = a^{-1}b^{-1}ab$ for $a, b \in G$. Then for any $g \in G$, $g^{-1}hg = (g^{-1}a^{-1}b^{-1})(abg) \in G'$, done.

2 (⇒)

$$\begin{aligned} G/N \text{ abelian} &\Leftrightarrow abN = baN,\ \forall a, b \in G \\ &\Leftrightarrow a^{-1}b^{-1}ab \in N\,\forall a, b \in G \\ &\Rightarrow G' \subset N \end{aligned}$$

(⇐)

$$\begin{aligned} G' \leq N &\Rightarrow G' \subset N \\ &\Rightarrow a^{-1}b^{-1}ab \in N\,\forall a, b \in G \\ &\Leftrightarrow G/N \text{ abelian} \end{aligned}$$

Proposition 4.26. $\{G_n\}$ is a sequence of finite nontrivial groups s.t. $|G_n| \to \infty$. Let k be a positive integer. Suppose that for all n, G_n is solvable with derived length $\leq k$, then $\{G_n\}$ does not yield an expander family.

Proof
Proof by induction. $k = 1$ abelian group, obvious. Suppose true for k, consider $k + 1$.

Case 1 The sequence $\{G'_n\}$ has bounded index in $\{G_n\}$.

- Note G'_n does not yield an expander family by induction hypothesis.
- Also note bounded index. Then by Subgroup Nonexpansion Principle, done.

Case 2 The sequence $|G_n/G'_n|$ is unbounded (i.e. index unbounded).

- By Lemma 4.25, G_n/G'_n always abelian, so it does not yield an expander family.
- This is an unbounded sequence of quotients. Then by Quotients Nonexpansion Principle, done.

4.6 Semidirect Product & Wreath Product

Wreath product is a special case of the semidirect product, and is essential in the construction of expander families.

Definition 4.27. Groups G, K. Homomorphism $\theta : K \to \mathrm{Aut}(G)$. Define a binary operation $\star$ on $G \times K$ by

$$(g_1, k_1) \star (g_2, k_2) = (g_1\theta_{k_1}(g_2), k_1k_2)$$

The set $G \times K$ together with $\star$, is called the semidirect product group of G and K with respect to θ, and is denoted as $G \rtimes K$ when the context of θ is unambiguous.

Remark

- Structure of this construction:

$$\begin{array}{rcl} \theta: K & \to & \mathrm{Aut}(G) \\ k & \mapsto & \theta_k \end{array} \qquad \begin{array}{c} \text{Special Case:} \\ e_K \mapsto id \end{array}$$

$$\begin{array}{rcl} \theta_k: G & \to & G \\ g & \mapsto & \theta_k(g) \end{array} \qquad \begin{array}{rcl} id: G & \to & G \\ g & \mapsto & g \end{array}$$

- Identity: (e_G, e_K)
- Inverse of (g,k): $(\theta_k^{-1}(g^{-1}), k^{-1})$
- Further simplification on notation:

$$\begin{array}{rcl} gk & \text{for} & (g,k) \\ g_1k_1g_2k_2 & \text{for} & (g_1,k_1)\star(g_2,k_2) \\ {}^kg & \text{for} & \theta_k(g) \end{array}$$

  Note ${}^{k_1k_2}g = {}^{k_1}({}^{k_2}g)$, due to homomorphism of θ

- When there is no ambiguity, we view G as a subgroup of $G \rtimes K$ by identifying $g \in G$ as (g, eG). Justification: for any group G, we always have $G \cong G \times \{e_G\}$. Similarly, view K as a subgroup of $G \rtimes K$ by identifying $k \in K$ as (e_K, k).
- In this book's context, we are implicitly treating G and K as subgroups of a larger group, so $e_K = e_G = 1$.

Lemma 4.28. $G \triangleleft G \rtimes K$, and $(G \rtimes K)/G \approx K$.

Remark
Complete notation: $G \times \{e_G\} \triangleleft G \rtimes K$, and $(G \rtimes K)/G \cong K \times \{e_K\}$
Caution: These results built on treating $e_K = e_G = 1$, i.e. G and K are subgroups of a larger group.

Proof

1 For arbitrary $(t,1)$ in G, for any $(g,k) \in G \rtimes K$,

$$\begin{aligned} (g,k)\star(t,1)\star((g,k))^{-1} &= (g\theta_k(t),k)(\theta_k^{-1}(g^{-1}),k^{-1}) \\ &= (g\theta_k(t)g^{-1},1) \in G \end{aligned}$$

Normality done.

2 LHS is the left coset of G in $G \rtimes K$, $gkG = \{(g\theta_k(t), k) \mid t \in G\}$. Note θ_k is an automorphism of G (isomorphism from G to G), thus for arbitrary $g_1, g_2 \in G$, $g_1kG = g_2kG$. That is, gkG is determined by k solely. The isomorphism is obvious.

Definition 4.29.

- Let I be a finite (index) set, and G, K be groups. Let $G^I = \oplus_{i\in I} G$ be the direct product of several copies of G, one for each element of I. Elements of G are $|I|$-tuples $(g_i)_{i\in I}$, where $g_i \in G$ for all i.
- Let θ be a homomorphism from K to S^I, where S^I is the symmetric group on I (set of all permutations of I). Later, call this as "defining θ as an action of K on I".
- Then θ induces a homomorphism, denoted as $\theta : K \to \mathrm{Aut}(G^I)$, by $k \mapsto \theta_k$, where θ_k is the permutation in S^I which corresponds to k.

Definition 4.30. The wreath product of G and K with respect to θ and I is denoted $G \wr K$ and defined as

$$G \wr K = G^I \rtimes K$$

Remark

- Wreath product is a special case of semidirect product, thus preserving all its properties. That is, $G \wr K$ is the wreath product group, $G^I \lhd G \wr K$, and $(G \wr K)/G^I \approx K$.
- Structure of this construction:

  $$\begin{array}{rcl} \theta :\ K & \to & \mathrm{Aut}(G) \\ k & \mapsto & \theta_k \end{array} \qquad \begin{array}{c} \text{Special Case:} \\ e_K \mapsto id\,\text{(no permutation)} \end{array}$$

  $$\begin{array}{rcl} \theta_k :\ G^I & \to & G^I \\ (g_i)_{i\in I} & \mapsto & (g_{\theta_k(i)})_{i\in I} \end{array} \qquad \begin{array}{rcl} id : G & \to & G \\ (g_i)_{i\in I} & \mapsto & (g_i)_{i\in I} \end{array}$$

  Note every θ_k is now a permutation on I.
- Binary operation: $((g_i^1)_{i\in I}, x) \star ((g_i^2)_{i\in I}, y) = ((g_i^1)_{i\in I}(g^2_{\theta_x(i)})_{i\in I}, xy)$
- Identity: $((e_{G_i})_{i\in I}, e_K)$
- Inverse of $((g_i)_{i\in I}, k)$: $((g^{-1}_{\theta_k^{-1}(i)})_{i\in I}, k^{-1})$, s.t.

  $$\begin{aligned} ((g_i)_{i\in I}, k) \star ((g^{-1}_{\theta_k^{-1}(i)})_{i\in I}, k^{-1}) &= ((g_i)_{i\in I}(g^{-1}_{\theta_k\theta_k^{-1}(i)})_{i\in I}, e_K) \\ &= ((g_i)_{i\in I}(g_i^{-1})_{i\in I}, e_K) \\ &= ((e_{G_i})_{i\in I}, e_K) \end{aligned}$$

4.7 Counterexample: Cube-Connected Cycle Graphs

This counterexample is motivated by following questions:

1 Is there a diameter version for Quotients Nonexpansion Principle?

2 If a sequence of finite groups has logarithmic diameter, does it necessarily yield an expander family?

3 Can an unbounded sequence of solvable groups with bounded derived length have logarithmic diameter? (a more concerete question based on 2)

The answers are no, no, and yes. The family of cube-connected cycle graphs would be the example.

We make following conventions on notation. Consider positive integer n.

- e_i denote the element of $\mathbb{Z}_2^n = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$, wiht 1 in ith place and 0 elsewhere.
- $0 = (0, \cdots, 0)$ denotes the identity of $\mathbb{Z}_2^n$

Definition 4.31.

- Define an action θ of $\mathbb{Z}_n$ on $I = \mathbb{Z}_n$ by $\theta_a(b) = a + b$. Via this action, construct the wreath product group $G_n = \mathbb{Z}_2 \wr \mathbb{Z}_n$
- Let $\Gamma_n = \{(e_n, 0), \gamma, \gamma^{-1}\} \subset G_n$, where $\gamma = (0, 1)$, $\gamma^{-1} = (0, -1)$.
- Define the cube-connected cycle graph CCC_n be the Cayley graph $\mathrm{Cay}(G_n, \Gamma_n)$.

Remark

- $G_n = \mathbb{Z}_2^n \rtimes Z_n$, the action of $\mathbb{Z}_n$ on $\mathbb{Z}_n^2$ is given by

$$
\begin{aligned}
{}^1(a_1, a_2, \ldots, a_n) &= (a_n, a_1, \ldots, a_{n-1}) \\
{}^k(a_1, a_2, \ldots, a_n) &= (a_{n-k+1}, a_{n-k+2}, \ldots, a_{n-k})
\end{aligned}
$$

  Since 1 is the generator of $\mathbb{Z}_n$. Note the identity is 0.

- Structure of this construction:

$$
\begin{array}{rcl}
\theta : \mathbb{Z}_n & \to & \mathrm{Aut}(\mathbb{Z}^{\mathbb{Z}_n}) \\
a & \mapsto & \theta_a
\end{array}
\qquad
\begin{array}{c}
\text{Special Case:} \\
0 \mapsto id\,(\text{no permutation})
\end{array}
$$

$$
\begin{array}{rcl}
\theta_a : \mathbb{Z}_n^{\mathbb{Z}_n} & \to & \mathbb{Z}_n^{\mathbb{Z}_n} \\
(g_i)_{i \in \mathbb{Z}_n} & \mapsto & (g_{i+n-a})_{i \in \mathbb{Z}_n}
\end{array}
\qquad
\begin{array}{rcl}
id : \mathbb{Z}_n^{\mathbb{Z}_n} & \to & \mathbb{Z}_n^{\mathbb{Z}_n} \\
(g_i)_{i \in \mathbb{Z}_n} & \mapsto & (g_i)_{i \in \mathbb{Z}_n}
\end{array}
$$

- Note Γ_n is symmetric, thus CCC_n is undirected. Also, $|\Gamma| = 3$, so CCC_n is 3-regular.

Example
Let $n = 3$. For simplification, denote elements of $\mathbb{Z}_2^3$ as binary strings (and follow this convention later). Then, $(e_3, 0) = (001, 0)$; $\gamma = (000, 1)$; $\gamma^{-1} = (000, -1)$. Consider (100,1). Then

$$\begin{aligned}(100, 1)(000, 1) &= (100 + 000, 1 + 1) &&= (100, 2)\\ (100, 1)(000, -1) &= (100 + 000, 1 - 1) &&= (100, 0)\\ (100, 1)(001, 0) &= (100 + 100, 1 + 0) &&= (000, 1)\end{aligned}$$

Hence (100,1) is adjacent to (100,2),(100,0), and (000,1) in CCC_3.

Remark
We express elements of $\mathbb{Z}_2^n$ as strings of n binary digits. An n-dimensional hypercube is the graph whose vertices are the elements of $\mathbb{Z}_2^n$, where two vertices are adjacent, via an edge of multiplicity one, if they differ in exactly one digit, and they are nonadjacent otherwise.

It turns out that CCC_n can be visualised as a n-dimensional hypercube, where each vertex is replaced by an n-cycle composed of elements of $\mathbb{Z}_n$ See Figure 4.2. No proof for this visualisation, since it is not the purpose.

Proposition 4.32. For all n, $\operatorname{diam}(CCC_n) \leq 4n$.

Proof

- An arbitrary element of G_n is of the form $(e_{j_1} e_{j_2} \cdots e_{j_k}, a)$ for some positive integers $j_1, \dots, j_k$ with $1 \leq j_1 < j_2 < \cdots < j_k \leq n$ and $k \leq n$ (i.e. n bites, either 1 or 0).
- By Prop.4.10, suffice to show the word norm of $(e_{j_1} e_{j_2} \cdots e_{j_k}, a) \leq 4n$.
- Let $e = (e_n, 0)$. Note for all positive integers c,

$$\begin{aligned}\gamma^c e(\gamma^{-1})^c &= (0, c)(e_n, 0)(0, -c)\\ &= (0 + {}^c e_n, c + 0)(0, -c)\\ &= ({}^c e_n, c)(0, -c)\\ &= ({}^c e_n, 0) \quad \text{0 always mapped to identity 0}\\ &= (e_c, 0)\end{aligned}$$

- Also note, $(g_1, 0)(g_2, 0) = (g_1 + \theta_0(g_2), 0) = (g_1 + g_2, 0)$, since 0 is the identity.

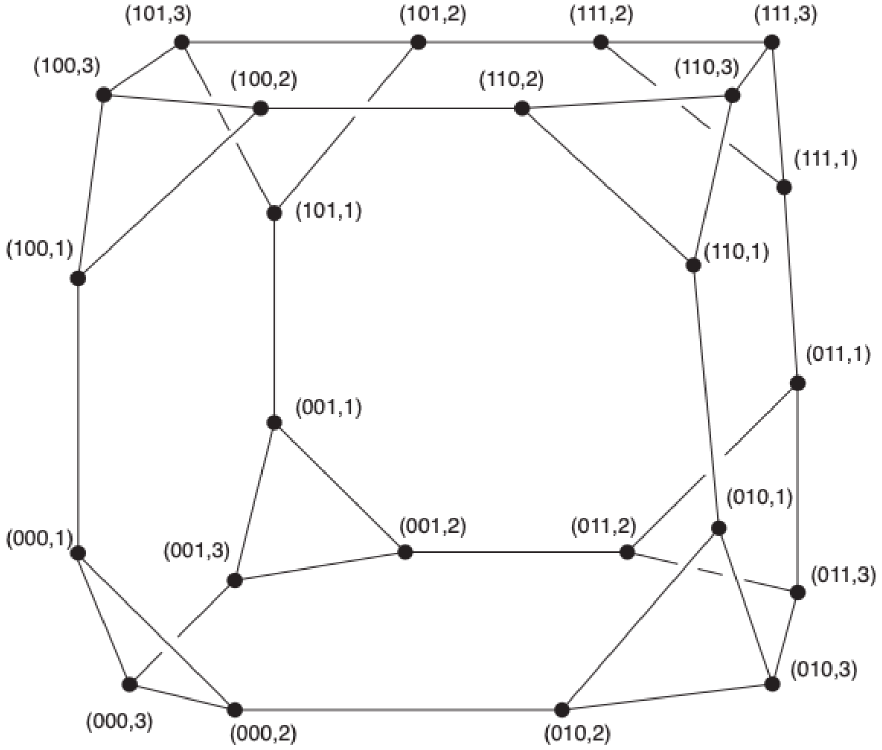

Figure 4.2: CCC_3

- Then

$$\begin{aligned}(e_{j_1}e_{j_2}\cdots e_{j_k},a) &= (e_{j_1},0)(e_{j_2},0)\dots(e_{j_k},0)(0,a)\\ &= \gamma^{j_1}e\gamma^{-j_1}\gamma^{j_2}e\gamma^{-j_2}\dots\gamma^{j_k}e\gamma^{-j_k}\gamma^{a}\\ &= \gamma^{j_1}e\gamma^{j_2-j_1}e\gamma^{j_3-j_2}\dots\gamma^{j_k-j_{k-1}}e(\gamma^{-1})^{j_k}\gamma^{a}\end{aligned}$$

  Note γ appears $j_1+(j_2-j_1)+\cdots+(j_k-j_{k-1})+a = j_k+a$ times, γ^{-1} appears j_k times, and e appears k times. So the word norm of $(e_{j_1}e_{j_2}\cdots e_{j_k},a)$ has $2j_k+a+k\le 4n$

Lemma 4.33. The sequence $\{CCC_n\}$ has logarithmic diamter.

Proof
$|G_n| = |\mathbb{Z}_2^n||\mathbb{Z}_n| = n2^n$, thus $|CCC_n| = \ln n + n\ln 2$. Let $C = 4/\ln 2$, by Prop.4.4,

$$\operatorname{diam}(CCC_n)\le 4n\le C(\ln n+n\ln 2) = C\ln|CCC_n|$$

Lemma 4.34. G_n is solvable with derived length 2. Therefore, the sequence $\{CCC_n\}$ is not an expander family.

Proof
Note G_n is not abelian as $\gamma e_n \neq e_n\gamma$, so G_n does not have derived length 1. By Lemma 4.28, $\mathbb{Z}_2^n \triangleleft G_n$, and by Lemma 4.25 G_n' is the smallest normal subgroup that is abelian, thus $G_n'\le\mathbb{Z}_2^n$. Since $\mathbb{Z}_2^n$ is the direct product of Z_2 (cyclic group of prime order), by fundamental theorem of abelian groups, $\mathbb{Z}_2^n$ is abelian, so is G_n'. Then, $G_n^{(2)} = 1$.

Remark
Now we can answer questions asked in the beginning.

1 In the proof above, we note $\mathbb{Z}_2^n\triangleleft G_n$ and $G_n/\mathbb{Z}_2^n\cong\mathbb{Z}_n$, which is a sequence of quotients. Also, as an abelian group, $\mathbb{Z}_n$ does not have logarithmic diameter. However, by Lemma 4.33, G_n does have logarithmic diameter.

2 By Lemma 4.33 and Lemma 4.34.

3 By Lemma 4.33 and Lemma 4.34.