

3. PLÜNNECKE'S THEOREM AND SUMSET ESTIMATES

We begin our discussion today by investigating some nice properties of commutative graphs, which we will use to prove Plünnecke's Theorem. As usual, we follow Tao's notes (see [1]) very closely. First, let Z be an abelian group and consider a commutative graph G with vertex sets $V_0, V_1, V_2 \subseteq Z$ and edge sets $E_{0 \rightarrow 1}, E_{1 \rightarrow 2}$. Then the edge $(a \rightarrow a + b) \in E_{0 \rightarrow 1}$ induces an injection

$$f : \{(a + b \rightarrow a + b + c) \in E_{1 \rightarrow 2}\} \hookrightarrow E_{0 \rightarrow 1}$$

by setting $f((a + b \rightarrow a + b + c)) = (a \rightarrow a + c)$. The commuting square property implies that f is well-defined, i.e. that $(a \rightarrow a + c) \in E_{0 \rightarrow 1}$, and f is injective since, if $(a + b \rightarrow a + b + c')$ were another edge emanating from $a + b \in V_1$, then $f((a + b \rightarrow a + b + c)) = f((a + b \rightarrow a + b + c'))$ implies that $c = c'$ as claimed. We say that f is the **pullback map** induced by $(a \rightarrow a + b) \in E_{0 \rightarrow 1}$.

Now given a collection of edges $\{(a_i \rightarrow a_i + b_i)\}_{i=1}^n \subseteq E_{0 \rightarrow 1}$, consider the composition map defined over all edges in $E_{1 \rightarrow 2}$ starting at $a_i + b_i$ for some $1 \leq i \leq n$ by the rule

$$(a_i + b_i \rightarrow a_i + b_i + c) \mapsto (a_i \rightarrow a_i + c)$$

formed by using the pullback map induced by the edge $(a_i \rightarrow a_i + b_i)$. Suppose that we're given two edges in the domain, say $a_i + b_i \rightarrow a_i + b_i + c$ and $a_j + b_j \rightarrow a_j + b_j + c'$. If $a_i + b_i \neq a_j + b_j$ and $a_i + b_i + c \neq a_j + b_j + c'$, then we claim that this map is still injective, i.e. that the above two edges map to distinct edges in $E_{0 \rightarrow 1}$. In this case, we must have $c \neq c'$, so if $a_i = a_j$, then $a_i + c \neq a_j + c'$. Therefore the two edges $a_i \rightarrow a_i + c$ and $a_j \rightarrow a_j + c'$ are distinct, and hence the map is injective.

We have shown that if we pullback from a set of edges in $E_{1 \rightarrow 2}$ whose initial points and terminal points are distinct—for example, edges that are in disjoint paths from V_0 to V_2 —then we get a set of maps whose union is still an injection. One may also define **pushforward maps** induced by edges in $E_{1 \rightarrow 2}$, either by direct construction (as for pullback maps above) or by considering pullback maps in G^\dagger , the commutative graph formed from G by switching V_0 and V_2 and reversing edges, that is the “mirror image” of G . The fact that we get injections by pulling back and pushing forward along disjoint paths will be important in the proof of the following proposition, which immediately implies Plünnecke's Theorem:

Proposition 3.1. *Let G be a commutative graph such that $|V_1| \leq K|V_0|$ for some $K \geq 1$. Then $|G^2(A')| \leq K^2|A'|$ for some $A' \subseteq V_1$.*

Note that the particular statement in the case that $K = 1$ of Plünnecke's theorem—i.e. $A, B \subseteq Z$ and $G = G[A, B]$ —is true with $A' = A$: by Exercise 0.2, A is a union of cosets of some subgroup $H \leq Z$ and $B \subseteq H + x$ for some $x \in Z$. But then $B + B \subseteq H + H + x + x = H + (x + x)$, so Exercise 0.2 again shows that $|A + B + B| \leq |A|$. However, we need the full generality of Proposition 3.1 when $K = 1$ in order to prove the theorem for arbitrary $K \geq 1$, as we will see shortly.

Proof (of Proposition 3.1, $K = 1$). Let $s := \text{MAXFLOW}(V_0 \rightarrow V_2; G)$. Since V_1 disconnects V_0 from V_2 in G , Menger's Theorem (Exercise 2.2) implies that $s \leq |V_1| \leq |V_0|$, where the second inequality follows by assumption. By applying Menger's Theorem again, we know that there is a disconnecting set $S \subseteq V_0 \cup V_1 \cup V_2$ such that $|S| = s$. Write $S_j := S \cap V_j$.

The idea is to push S_1 into V_0 in order to form an appropriate A' . To that end, let G' be the subgraph of G whose edges $E'_{0 \rightarrow 1} \cup E'_{1 \rightarrow 2}$ consist of edges in paths

from $V'_0 := V_0 \setminus S_0$ to $V'_2 := V_2 \setminus S_2$. Since S disconnects V'_0 from V'_2 in G' , all such paths must go through S_1 . In addition, $\text{MINCUT}(V_0 \rightarrow V_2; G') = |S_1|$ since if it were any smaller, we could find a set smaller than S that disconnected V_0 from V_2 in G , contradicting the definition of s . Therefore, again by Menger's theorem, there are $|S_1|$ disjoint paths in G' . Let $W_0 \subseteq V'_0$ denote the initial points and $W_2 \subseteq V'_2$ the terminal points of these paths. Clearly $|W_0| = |S_1| = |W_2|$.

Now we note that since G is commutative, so is G' : if $(a \rightarrow a + b) \in E'_{0 \rightarrow 1}$ and $(a + b \rightarrow a + b + c) \in E'_{1 \rightarrow 2}$, then since G is commutative we know that $(a \rightarrow a + c) \in E_{0 \rightarrow 1}$ and $(a + c \rightarrow a + c + b) \in E_{1 \rightarrow 2}$. But $a \rightarrow a + c \rightarrow a + c + b$ is a path from $a \in V'_0$ to $a + b + c \in V'_2$, so its edges are in $E'_{0 \rightarrow 1}$ and $E'_{1 \rightarrow 2}$ as needed. To put this fact to use, recall from the discussion preceding the statement of the proposition that by pulling back along the $|S_1|$ disjoint paths through S_1 , we get an injection from *all the edges in $E'_{1 \rightarrow 2}$* to those edges E_{W_0} in $E'_{0 \rightarrow 1}$ that start in W_0 . Similarly, by pushing forward along these disjoint paths, we get an injection from $E'_{0 \rightarrow 1}$ to the edges E_{W_2} in $E'_{1 \rightarrow 2}$ that end in W_2 . Therefore

$$E'_{0 \rightarrow 1} \hookrightarrow E_{W_2} \subseteq E'_{1 \rightarrow 2} \hookrightarrow E_{W_0} \subseteq E'_{0 \rightarrow 1}$$

and thus all five sets are the same size.

In particular, all edges in $E'_{0 \rightarrow 1}$ start in W_0 , so we may replace S_1 with W_0 to get a set $S_0 \cup W_0 \cup S_2$ disconnecting V_0 from V_2 in G . Set $A' = V_0 \setminus (S_0 \cup W_0)$. Then $G^2(A') \subseteq S_2$ since otherwise there would be a path from V_0 to V_2 whose endpoints are neither in $S_0 \cup W_0$ nor S_2 , contradicting $|S_0 \sqcup W_0 \sqcup S_2| = s$. Finally, since $|S_0| + |W_0| + |S_2| = s \leq |V_0|$, we have

$$\begin{aligned} |G^2(A')| &\leq |S_2| \\ &\leq |V_0| - (|S_0| + |W_0|) \\ &= |A'| \end{aligned}$$

as needed. \square

Although the proof may seem a bit long-winded, I believe that it deserves this space because each time I have discussed it with others, we have gotten confused. Hopefully its length has not deterred you from digesting it.

In order to pass from $K = 1$ to the general case $K \geq 1$, we make the following definition. Let G be a commutative graph. Define the **magnification ratio** $D(G)$ by

$$D(G) := \min_{\emptyset \neq A' \subseteq V_0} \frac{|G^2(A')|}{|A'|}$$

Then Proposition 3.1 says that $|V_1|/|V_0| \leq 1$ implies that $D(G) \leq 1$. In order to finish proving Plünnecke's theorem, we must show that $|V_1|/|V_0| \leq K$ implies that $D(G) \leq K^2$ for any $K \geq 1$. In order to prove the general case, we will use the Cartesian product trick, so the following lemma will be useful:

Lemma 3.2. *If G and \tilde{G} are commutative graphs, then $D(G \times \tilde{G}) = D(G) \cdot D(\tilde{G})$.*

Before proving the lemma, we note that $D(G \times \tilde{G})$ is well-defined by Exercise 2.1. We will also require the following observation, which we leave as an exercise:

Exercise 3.1. *Given commutative graphs G and \tilde{G} and subsets $A \subseteq V_0$ and $\tilde{A} \subseteq \tilde{V}_0$,*

$$(G \times \tilde{G})^2(A \times \tilde{A}) = G^2(A) \times \tilde{G}^2(\tilde{A})$$

Proof (of Lemma 3.2). Write $d = D(G)$ and $\tilde{d} = D(\tilde{G})$. Then by the definition of magnification ratio, there are subsets $A' \subseteq V_0$ and $\tilde{A}' \subseteq \tilde{V}_0$ such that

$$|G^2(A')| = d|A'| \text{ and } |G^2(\tilde{A}')| = d|\tilde{A}'|$$

Therefore, by Exercise 3.1,

$$\begin{aligned} |(G \times \tilde{G})^2(A' \times \tilde{A}')| &= |G^2(A')| \cdot |\tilde{G}^2(\tilde{A}')| \\ &= d\tilde{d}|A'||\tilde{A}'| = d\tilde{d}|A' \times \tilde{A}'| \end{aligned}$$

So, since

$$\frac{|(G \times \tilde{G})^2(A' \times \tilde{A}')|}{|A' \times \tilde{A}'|} = d\tilde{d}$$

we have shown that $D(G \times \tilde{G}) \leq d\tilde{d}$.

It remains to show the opposite inequality, i.e. for any $U \subseteq V_0 \times \tilde{V}_0$,

$$\frac{|(G \times \tilde{G})^2(U)|}{|U|} \geq d\tilde{d}$$

To do so, we factor the set $(G \times \tilde{G})^2(U)$. First let $I_{V_0} = G[V_0, \{0\}]$ be the commutative graph whose three vertex sets are all equal to (disjoint copies of) V_0 and whose edges correspond to loops on the vertices of V_0 , that is the graph consisting of $|V_0|$ disjoint paths of length two. Similarly define $I_{\tilde{V}_2} = G[\tilde{V}_2, \{0\}]$. First I claim that

$$(9) \quad (G \times \tilde{G})^2(U) = (G \times I_{\tilde{V}_2})^2(I_{V_0} \times \tilde{G})^2(U)$$

To see this, let $z \in (G \times \tilde{G})^2(U)$. This means that there is a point $x \in U$ and edges e, e' that form a path from x to z through some $y \in V_1 \times \tilde{V}_1$. Write $z = (a + b + c, \tilde{a} + \tilde{b} + \tilde{c})$, where $x = (a, \tilde{a})$ and $y = (a + b, \tilde{a} + \tilde{b})$. Note that by exercise 3.1, $(a \rightarrow a + b + c) \in G^2(U_0)$ and $(\tilde{a} \rightarrow \tilde{a} + \tilde{b} + \tilde{c}) \in \tilde{G}^2(\tilde{U}_0)$ where $U = U_0 \times \tilde{U}_0$. Consider the path

$$(10) \quad (a, \tilde{a}) \rightarrow (a, \tilde{a} + \tilde{b} + \tilde{c}) \rightarrow (a + b + c, \tilde{a} + \tilde{b} + \tilde{c})$$

The first is an edge from U to $(I_{V_0} \times \tilde{G})^2(U)$, and the second is from $(I_{V_0} \times \tilde{G})^2$ to $(G \times I_{\tilde{V}_2})^2(I_{V_0} \times \tilde{G})^2(U)$. Therefore $(G \times \tilde{G})^2(U) \subseteq (G \times I_{\tilde{V}_2})^2(I_{V_0} \times \tilde{G})^2(U)$. To prove the other inclusion, note that we may collapse a path of the form (10) to one from U to $(G \times \tilde{G})^2(U)$, and equation (9) follows.

Now I claim that $D(I_{V_0} \times \tilde{G}) = \tilde{d}$ and $D(G \times I_{\tilde{V}_2}) = d$; this follows from Exercise 3.1, and the fact that, for example, $|I_{V_0}^2(X)| = |X|$ for any $X \subset V_0$. Therefore, by this and the above claim, we compute

$$\begin{aligned} |(G \times \tilde{G})^2(U)| &= |(G \times I_{\tilde{V}_2})^2(I_{V_0} \times \tilde{G})^2(U)| \\ &\geq D(G \times I_{\tilde{V}_2})|(I_{V_0} \times \tilde{G})^2(U)| \\ &\geq D(G \times I_{\tilde{V}_2})D(I_{V_0} \times \tilde{G})|U| \\ &= d\tilde{d}|U| \end{aligned}$$

so we are done. \square

To finish the proof of Plünnecke's theorem, we require some more notation. For any $k \in \mathbb{N}$, define $G_k := G[A, B]$ where $A = \{0\}$ and $B = \{e_1, \dots, e_k\}$ is the standard basis for $Z = \mathbb{Z}^k$. Then $|V_0| = 1$, $|V_1| = k$, and

$$D(G_k) = |G_k^2(A)| = \binom{k}{2} + k = \frac{k(k+1)}{2}$$

As before, define G_k^\dagger to be the reflected (commutative) graph of G_k , i.e. swap V_0 and V_2 and reverse all the edges. Then $|V_0^\dagger| = k(k+1)/2$, $|V_1^\dagger| = k$, and $D(G_k^\dagger) = \frac{2}{k(k+1)}$.

Proof (of Proposition 3.1). Let k be an integer between $2K - 1$ and $2K$ so that

$$\left(\frac{|V_1|}{|V_0|}\right) \frac{2}{k+1} \leq 1$$

Then for the vertex sets of $\tilde{G} := G \times G_k^\dagger$, we have

$$\begin{aligned} \frac{|\tilde{V}_1|}{|\tilde{V}_0|} &= \frac{|V_1||V_1^\dagger|}{|V_0||V_0^\dagger|} \\ &= \left(\frac{|V_1|}{|V_0|}\right) \left(\frac{k}{k(k+1)/2}\right) \leq 1 \end{aligned}$$

Therefore the case $K = 1$ applies to $G \times G_k^\dagger$, and thus $D(G \times G_k^\dagger) \leq 1$, and Lemma 3.2 yields

$$(11) \quad D(G) \leq \frac{1}{D(G_k^\dagger)} = \frac{k(k+1)}{2} \leq 10K^2$$

This is on the right track, but we have picked up a factor of 10 that we should like to get rid of. No matter; applying (11) to $G^M = G \times G \times \dots \times G$, we see (using Lemma 3.2 and the fact that $|V_1^M|/|V_0^M| = |V_1|^M/|V_0|^M \leq K^M$) that

$$D(G)^M = D(G^M) \leq 10K^{2M}$$

so $D(G) \leq 10^{1/M} K^2$ for arbitrary M , so we're done. \square

Note that for all $k > 1$, $G_k^\dagger \neq G[A, B]$ for any A, B , so we could not apply the argument above using Exercise 0.2 to the product graph \tilde{G} .

Clearly we may iterate Plünnecke's theorem to higher sums:

$$\begin{aligned} |A + B| &\leq K|A| \\ |A' + B + B| &\leq K^2|A| \\ |A'' + (B + B) + (B + B)| &\leq K^4|A| \\ |A_n + nB| &\leq K^C|A_n| \end{aligned}$$

for some absolute constant $C = C(n)$ depending only on n . By the above computations, since $m \leq n$ implies that $mB \subseteq x + nB$, we may take $C(n) = 2^{\lceil \log_2 n \rceil}$; furthermore, by modifying the proof of Proposition 3.1, it's possible to show:

Exercise 3.2. *In the above setup, show that it is possible to take $C(n) = n$.*

Furthermore, we may use these bounds plus Lemma 1.3 to see that (WLOG, $n \geq m$):

$$\begin{aligned} |nB - mB| &\leq \frac{|A_n + nB||A_n + mB|}{|A_n|} \\ &\leq \left(\frac{|A_n + nB|}{|A_n|} \right)^2 |A_n| \\ &\leq K^{2C(n)} |A_n| \leq K^{2C(n)} |A| \end{aligned}$$

This is the much-anticipated Sumset estimates, which we now record as a theorem for future reference:

Theorem 3.3 (Sumset estimates). *Let $A, B \subseteq Z$ be nonempty subsets of an abelian group Z such that $|A + B| \leq K|A|$ for some $K \geq 1$. Then*

$$|nB - mB| \leq K^{C(n,m)} |A|$$

We will use the Sumset estimates next week to show that if $F = \mathbb{Z}/p\mathbb{Z}$ has no approximate subrings, then $|A \cdot A - A \cdot A|$ is small relative to $|A|$, and the week after that we will use this to show that then $|P(A, A, \dots, A)|$ is small relative to $|A|$ for any polynomial P , which will contradict our conclusion from last time and prove that F has no approximate subrings.

References.

- [1] Terry Tao. Math 254a: Some highlights of arithmetic combinatorics, 2003.