10 Sumsets and Connectivity of Symmetric Graphs

The goal of this section is to paint a bridge between the study of small sumsets and the study of connectivity of symmetric graphs. This is a simple and useful connection which we will describe after we establish a few important definitions and conventions. For simplicity, we will restrict to the case of finite groups for this section, although we will permit nonabelian groups. Thus, we now fix a finite multiplicative group G.

Group Actions

We will let our groups act on the right. If G acts on a set X, and $x \in X$, $g \in G$, we let xg denote the image of x under the action of g. Similarly, if $Y \subseteq X$ we let $Yg = \{yg : y \in Y\}$. We let $G_x = \{g \in G : xg = x\} \leq G$ and we call this set the *stabilizer* of x (in G). A subset $B \subseteq X$ is a *block of imprimitivity* if $Bg \cap B = \emptyset$ or $Bg = B$ for every $g \in G$. The set of images of B under G, $\{Bg : g \in G\}$ is a partition of G (check!) called a *system of imprimitivity.*

Coset Representations

Assume now that G acts transitively on X (so for every $x, y \in X$ there exists $g \in G$ with $xg = y$). Then the action of G on X may be represented by right cosets in a manner we now describe. Choose a base point $x \in X$ and associate each $y \in X$ with the set $\{g \in G : xg = y\}$. If $G_x = H$ and $xg = y$, then the set of points associated with y is equal to Hg (check!) and we shall denote this set by H^y. Now every point is associated with a right H-coset, and the action of G on X corresponds to right multiplication on these H-cosets. In other words, if $y, z \in X$ and $g \in G$, then $yg = z$ if and only if $(H^y)g = H^z$ (check!).

Transitive Graphs

Throughout this section, we will consider only simple graphs, so we permit loops, but we shall forbid parallel edges. If Γ is a graph, then we let $Aut(\Gamma)$ denote the set of all automorphisms of Γ (bijections from $V(G) \to V(G)$ which preserve incidence). So $Aut(\Gamma)$ acts on $V(\Gamma)$ and $E(\Gamma)$, and we say that Γ is *vertex transitive* if the first of these actions is transitive and *edge transitive* if the second is transitive. If Γ is a vertex transitive graph, then every vertex has the same degree, and we call this common number the *degree* of Γ and denote it by $deg(\Gamma)$. A group G acting on Γ may be viewed either as a homomorphism $G \to Aut(\Gamma)$ or just as an action of G on $V(\Gamma)$ which preserves incidence.

Cayley Graphs

If $A \subseteq G$, the *Cayley digraph on G generated by A*, denoted $\mathcal{C}(G, A)$ has vertex set G and has an edge from x to y if and only if $y \in Ax$ (you can get from x to y by left-multiplying by some element of A). It is immediate from this definition that G acts transitively on $\mathcal{C}(G, A)$ by right multiplication ($xg = x \cdot g$).

Graph Connectivity

Next we will introduce some connectivity parameters for graphs. First let Γ be a (undirected) graph and let $Y \subseteq V(\Gamma)$. We let $\partial(Y) = \{x \in V(\Gamma)\backslash Y : (y, x) \in E(\Gamma) \text{ for some } y \in Y\}$ and we let $\delta(Y) = \{e \in E(\Gamma) : e \text{ has exactly one end in } Y\}$. The *edge-connectivity* of Γ is the minimum of $|\delta(Y)|$ over all $\emptyset \subset Y \subset V(\Gamma)$. The *vertex-connectivity* of Γ is the minimum of $|\partial(Y)|$ over all $\emptyset \neq Y \subseteq V(\Gamma)$ with $Y \cup \partial(Y) \neq V(G)$. Similarly, if Γ is a digraph and $Y \subseteq V(\Gamma)$ we let $\partial^+(Y) = \{x \in V(\Gamma) \setminus Y : (y, x) \in E(\Gamma) \text{ for some } y \in Y\}$. The *strong connectivity* of Γ is the minimum of $|\partial^+(Y)|$ over all $\emptyset \neq Y \subseteq V(\Gamma)$ for which $Y \cup \partial^+(Y) \neq V(\Gamma)$.

With this in place, we are finally ready to discuss the connection between vertex transitive graphs and sumsets - well, actually product sets, since we have switched to multiplicative notation. Let $A, B \subseteq G$ and assume that $1 \in A$. Let $\Gamma = \mathcal{C}(G, A)$. Now consider the product set AB. By assumption, $1 \in A$ so $B \subseteq AB$. Further, $AB \setminus B = \partial^+_\Gamma(B)$. In particular, the pair A, B is critical (recall that this means $|AB| < |A| + |B|$) if and only if $|\partial^+(B)| < |A| = deg(\Gamma)$. So, if we fix a particular set $A \subseteq G$ with $1 \in A$, studying those $B \subseteq G$ for which A, B is critical is equivalent to finding those subsets of vertices in our Cayley graph $\mathcal{C}(G, A)$ which have out-boundary smaller than the degree. By way of this connection, we now have the following reformulation of the Cauchy-Davenport Theorem.

Theorem 10.1 (Cauchy-Davenport) *Let Γ be a loopless Cayley graph on $\mathbb{Z}_p$ for a prime p. Then $\kappa(\Gamma) = deg(\Gamma)$.*

Proof of Equivalence: To prove the Cauchy-Davenport theorem, it suffices (by shifting) to consider only those pairs $A, B \subseteq \mathbb{Z}_p$ with $0 \in A$. Thus, we let $A, B \subseteq \mathbb{Z}_p$ satisfy $0 \in A$ and set $\Gamma = \mathcal{C}(\mathbb{Z}_p, A \setminus \{0\})$. Now we have the following chain of equivalent equations.

$$\begin{aligned} |A + B| &\geq \min\{p, |A| + |B| - 1\} \\ |B \cup \partial^+_\Gamma(B)| &\geq \min\{p, |A| + |B| - 1\} \\ |\partial^+_\Gamma(B)| \geq deg(\Gamma) \quad &\text{or} \quad A \cup \partial^+_\Gamma(B) = V(\Gamma) \end{aligned}$$

Our equivalence follows immediately from this. $\square$

Indeed, it is natural to suspect that a (finite) graph which is vertex transitive should be well connected, and this intuition has led to a number of nice results. The first of these we give here is a theorem of Mader on edge-connectivity. The key tool in the proof is the same as the key tool used in the proof of Cauchy-Davenport, an uncrossing (intersection/union) argument. Here the key property is as follows. If $X, Y \subseteq V(\Gamma)$, then $|\delta(X \cap Y)| + |\delta(X \cup Y)| \leq |\delta(X)| + |\delta(Y)|$ (check!).

Theorem 10.2 (Mader) *If Γ is a finite connected vertex transitive graph, then its edge-connectivity is equal to its degree.*

Proof: Since every vertex x has $|\delta(\{x\})| = deg(\Gamma)$, it suffices to show that the connectivity of Γ is at least $deg(\Gamma)$. Choose a subset $\emptyset \neq X \subset V(\Gamma)$ so that

(i) $|\delta(X)|$ is minimum

(ii) $|X|$ is minimum (subject to (i)).

Note that since $\delta(X) = \delta(V(\Gamma) \setminus X)$ part (ii) of our assumptions implies that $|X| \leq \frac{1}{2}|V(\Gamma)|$. Suppose there is an automorphism $\phi \in Aut(\Gamma)$ for which $\emptyset \neq \phi(X) \cap X \neq X$. Then by our uncrossing argument

$$|\delta(X \cup \phi(X)| + |\delta(X \cap \phi(X))| \leq |\delta(X)| + |\delta(\phi(X))| = 2|\delta(X)|.$$

If $|\delta(X \cup \phi(X))| < |\delta(X)|$ then (since $X \cup \phi(X) \neq V(\Gamma)$) the set $X \cup \phi(X)$ contradicts our choice of X for (i). Otherwise the above inequality implies that $|\delta(X \cap \phi(X))| \leq |\delta(X)|$, but then $X \cap \phi(X)$ contradicts our choice of X for (i) or (ii). It follows that X is a block of imprimitivity. Since Γ is vertex transitive, there must exist $a, b \in \mathbb{N}$ so that every vertex in X has a neighbors in X and b neighbors outside X. Note that $b > 0$ and that $a + b = deg(\Gamma)$. Now we have

$$|\delta(X)| = b|X| \geq b(a+1) = ba + b \geq a + b = deg(\Gamma)$$

Thus Γ has edge-connectivity equal to its degree as desired. $\square$

There is a similar uncrossing argument which can be used to treat vertex connectivity. This program was initially followed by Mader and Watkins for graphs, and later by Hamidoune for directed graphs. A nice description of it can be found in the book Algebraic Graph

Theory by Godsil and Royle. Our treatment here will be a little more general with an eye toward some upcoming results. We begin with some further definitions.

Duets

A *G-duet* $\Delta = (X, Y)$ is a bipartite graph with bipartition (X, Y) together with transitive actions of G on X and on Y which preserve adjacency (so if $x \in X$, $y \in Y$, and $g \in G$, then $x \sim y$ if and only if $xg \sim yg$). As with graphs, we have a natural duet arising from a subset of G. If $A \subseteq G$, we define the *Cayley Duet*, denoted $\mathcal{C}D(G, A)$ to be the duet with vertex set consisting of two copies of G, say G and G', bipartition (G, G') and an edge (a, b') from a to b' if and only if $b \in Aa$. If Γ is a vertex transitive graph, then there is a natural $Aut(\Gamma)$-duet associated with Γ obtained by taking two copies of the vertex set $V(\Gamma)$, say V and V' and defining incidence by the rule $(u, v) \in V \times V'$ satisfy $u \sim v'$ if and only if either $u = v$ or $(u, v) \in E(\Gamma)$. Indeed, we will view duets as objects which live somewhere in between subsets of groups and vertex transitive graphs.

Representing Duets

Next we will describe a natural representation of a general G-duet $\Delta = (X, Y)$. Choose base points $x_0 \in X$ and $y_0 \in Y$, let $H = G_{x_0}$ and $K = G_{y_0}$ and consider the right coset representation of G on X and Y with base points x_0 and y_0. For every $x \in X$ let H^x be the right H-coset associated with x and for every $y \in Y$ let K^y be the right K-coset associated with y. Now let $A = \cup_{y \in \partial(x_0)} K^y$ and note that $KA = A$. Furthermore, since $H = G_{x_0}$ right multiplication by an element of H must send the set $\partial(x_0)$ back to itself, and it follows that $AH = A$.

Now, a point $y \in Y$ satisfies $x_0 \sim y$ if and only if $K^y \subseteq A$. Next we will show that our transitivity bootstraps this to a more general rule for determining adjacency. Let $x \in X$ and $y \in Y$ and choose $g \in G$ so that $x_0 g = x$. Then we have

$$\begin{aligned} x \sim y &\iff xg^{-1} \sim yg^{-1} \\ &\iff x_0 \sim yg^{-1} \\ &\iff K^y g^{-1} \subseteq A \\ &\iff K^y \subseteq Ag \\ &\iff K^y \subseteq AH^x \end{aligned}$$

Thus we see that $x \sim y$ if and only if $K^y \subseteq AH^x$ or equivalently $H^x \subseteq A^{-1}K^y$. Indeed, this gives our general duet the feel of a Cayley duet, as the set A completely determines adjacency. This representation leads us to the following proposition of Sabidussi.

Proposition 10.3 (Sabidussi) *If Γ is a vertex transitive directed graph, then it may be obtained from a Cayley graph by identifying clones (vertices with identical neighborhoods).*

Proof: Let Δ be the $G = Aut(\Gamma)$-duet associated with Γ. Choose a base point $v_0 \in V$ and consider the natural coset representation of Δ with base points consisting of both copies of v_0. Let $H = G_{v_0}$ and let A be the subset of G associated with this representation as above. Now, both copies of a vertex v are associated with the same right H-coset, which we shall denote H^v. It then follows that $(u, v) \in E(\Gamma)$ if and only if $H^v \subseteq AH^u$. Now let Γ° be the Cayley digraph $\mathcal{C}(G, A)$. It follows from the fact that $HAH = A$ that any two points in the same right H-coset are clones (check!), and Γ may be obtained from Γ° by identifying these clones. $\square$

It is worth noting that changing base points will only change K and H by conjugation and has no effect on $|A|$. Therefore, we may define the *weight* of Δ to be $w(\Delta) = |A|$, the *weight* of a set $B \subseteq X$, to be $w(B) = |B| \cdot |H|$ and the *weight* of a subset $B \subseteq Y$ to be $w(B) = |B| \cdot |K|$. The following observation follows immediately from these definitions.

Observation 10.4

$w(\Delta) = w(\partial(u))$ *for any* $u \in X \cup Y$.

$w(\Delta)$ *is a multiple of* $w(u)$ *for every* $u \in X \cup Y$.

If $k \in \mathbb{N}$, we call a set $B \subseteq X$ or $B \subseteq Y$ *k-critical* if $w(\partial B) + k = w(B) + w(\Delta)$. The reader should note that if Δ is a Cayley duet generated by A with bipartition (G, G'), then a set $B \subseteq G$ is *k-critical* for $k \in \mathbb{N}$ if $|AB| + k = |A| + |B|$, and *critical* if it is k-critical for some $k > 0$, so this aligns with our earlier notation. We say that $B \subseteq X$ ($B \subseteq Y$) is *nontrivially critical* if it is critical and $\partial B \neq Y$ ($\partial B \neq X$). We define $\kappa(\Delta)$ to be the largest integer k so that Δ contains a nontrivial k-critical set. Note that if Δ is not complete (at least one edge is missing), then $\kappa(\Delta) > 0$ since every singleton is nontrivially critical.

The reader may feel at this point that we have now gone through many steps to define an object, namely duets, which are little more than a particular subset of a group. While it is true that every duet arises in this manner, our graph-theoretic formulation will prove a helpful tool for visualization. For instance, we see subsets of our group playing several different roles.

Next we prove a theorem for duets which is the natural analogue of a theorem proved for groups by Mann and generalized to directed graphs by Hamidoune. Indeed the proof is also just like our earlier proof of Mader's theorem.

Theorem 10.5 *Let $\Delta = (X, Y)$ be a finite incomplete G-duet with bipartition (X, Y). Then there exists a block of imprimitivity $B \subseteq X$ or $B \subseteq Y$ so that B is $\kappa(\Delta)$-critical.*

Proof: Let $k = \kappa(\Delta)$ and choose a set $B \subseteq X$ or $B \subseteq Y$ so that

(i) B is nontrivally k-critical

(ii) $w(B)$ is minimum (subject to (i)).

We shall assume (without loss) that $X \subseteq B$. Set $C = Y \setminus \partial B$, so $w(C) = |G| - w(\partial B)$ and note that

$$\begin{aligned} w(\partial C) &\leq |G| - w(B) \\ &= w(C) + w(\partial B) - w(B) \\ &= w(C) + w(\Delta) - k \end{aligned}$$

Thus, C is also k-critical, and it follows from (ii) that $w(B) \leq w(C)$. Suppose there exists $g \in G$ so that $\emptyset \neq B \cap Bg \neq B$. Choose $u \in B \cap Bg$. Now we have

$$w(C) + w(Cg) \geq w(B) + w(C) > |G| - w(\Delta) = w(Y) - w(\partial(u)),$$

but both C and Cg are subsets of $Y \setminus \partial(u)$, so it follows that $C \cap Cg \neq \emptyset$. Now we have

$$w(\partial(B \cap Bg)) + w(\partial(B \cup Bg)) \leq w(\partial(B)) + w(\partial(Bg))$$

Since $B \cap Bg \neq \emptyset$ and $\partial(B \cup Bg) \neq Y$ it then follows that both $B \cap Bg$ and $B \cup Bg$ are nontrivially k-critical. But then $B \cap Bg$ contradicts our choice of B for (ii). Thus, B is a block of imprimitivity, and our proof is complete. □

Corollary 10.6 (Hamidoune) *If Γ is a vertex transitive directed graph which is not complete, then there exists a block of imprimitivity $B \subseteq V(\Gamma)$ so that either $\partial^+(B)$ or $\partial^-(B)$ is a minimum size vertex cut.*

Proof: Let Δ be the $Aut(\Gamma)$-duet associated with Γ. Then minimum size vertex cuts in Γ correspond exactly to nontrivial maximally critical sets in Δ and the result follows. $\square$

Corollary 10.7 (Hamidoune) *If Γ is a finite connected vertex transitive digraph with degree d, then Γ is $\frac{1}{2}(d+1)$-connected.*

Proof: Assume that Γ is not complete and let k be its connectivity. By the above corollary, we may choose a block of imprimitivity $B \subseteq V(\Gamma)$ so that either $|\partial^+(B)| = k$ or $|\partial^-(B)| = k$ - and we shall assume the former. Now consider the associated duet Δ and the system of imprimitivity on the left generated by B. We obtain a new duet Δ' by identifying these blocks of imprimitivity. By our earlier observation, we may choose $s \in \mathbb{N}$ so that $w(\Delta') = sw_{\Delta'}(B)$. If $s = 1$, then every point on the right of Δ' is incident with a single point on the left, and we have a contradiction to the assumption that Γ is connected. Thus, $s \geq 2$ and we have $w_\Delta(\partial_\Delta B) = w_{\Delta'}(\partial_{\Delta'} B) = sw_{\Delta'}(B) = sw_\Delta(B)$. Since every point in Δ has the same weight, it follows that $|\partial_\Delta B| = s|B|$. Putting this together, we find

$$\begin{aligned} k &= |\partial_\Delta B| - |B| \\ &= \tfrac{s-1}{s}|\partial_\Delta B| \\ &\geq \tfrac{s-1}{s}(d+1) \\ &\geq \tfrac{1}{2}(d+1) \end{aligned}$$

which completes the proof. $\square$

A similar result relating connectivity and degree of vertex transitive digraphs can also be obtained from Lemma 10.6. This result was originally discovered by Mader and independently Watkins, and we include it here without proof.

Corollary 10.8 (Mader, Watkins) *A finite vertex transitive graph with degree d is $\geq \frac{2}{3}(d+1)$-connected.*