Average degree of graph powers

Matt DeVos

This article will eventually turn to a very basic question in graph theory. However, we shall begin with our motivation, which comes from the world of additive number theory.

1 Groups

Let Γ be an abelian group (written additively). For two sets $A, B \subseteq \Gamma$ we define

$$A + B = \{a + b \mid \ a \in A \text{ and } b \in B\}$$

and we call such a set a sumset. One of the central problems in additive combinatorics is understanding the structure of finite sets A for which the sumset $A + A$ is small. Let's begin with an easy case where our group is the integers.

Observation 1.1. *If $A \subseteq \mathbb{Z}$ is finite and nonempty, then $|A + A| \geq 2|A| - 1$. Moreover, if this bound is met with equality, then A is an arithmetic progression.*

Proof. Let $A = \{a_1, a_2, \ldots, a_n\}$ where $a_1 < a_2 \ldots < a_n$. Then we may exhibit $2n-1$ distinct members of the sumset $A + A$ as follows

$$a_1 + a_1 < a_1 + a_2 < \ldots a_1 + a_n < a_2 + a_n \ldots < a_n + a_n.$$

This gives us the desired bound.

Now we investigate the case where our set A hits this bound with equality. Generalizing the above procedure, we can construct a list of $2n-1$ distinct members of $A + A$ by starting with $a_1 + a_1$ and moving to $a_n + a_n$ by increasing the index of either the left or right term by one at each stage. If $|A + A| = 2n - 1$ then we must get the same list of integers however we do this. Since the k^{th} term in such a list could be either $a_1 + a_{k+1}$ or $a_2 + a_k$ it follows that every $1 \leq k < n$ must satisfy $a_2 - a_1 = a_{k+1} - a_k$. Therefore, A is an arithmetic progression. □

Now we shall turn our attention from the integers to the group $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ in the case when p is prime. Here there is a new reason why the set $A + A$ might be small relative to

A, namely A could be all, or almost all of the group. The following famous theorem asserts that in this group we either get the same bound we had for the integers, or $A + A = \mathbb{Z}_p$.[1]

Theorem 1.2 (Cauchy-Davenport)**.** *Let p be prime and let $A \subseteq \mathbb{Z}_p$ be nonempty. Then we have*

$$|A + A| \geq \min\{p, 2|A| - 1\}.$$

There is an also a characterization of the sets $A \subseteq \mathbb{Z}_p$ for which $|A + A| < 2|A|$ due to Vosper.[2]

Theorem 1.3 (Vosper)**.** *Let p be prime, let $A \subseteq \mathbb{Z}_p$ is nonempty, and assume $|A+A| < 2|A|$. Then one of the following holds:*

1. *A is an arithmetic progression.*
2. *$|A + A| \geq p - 1$.*

There are similar results which hold in more general contexts, such as the following result which we do not state precisely. Here we have switched to multiplicative notation for the group Γ since this is the common convention when working with groups which are permitted to be nonabelian. So $A \cdot A = \{a \cdot a' \mid a, a' \in A\}$.

Theorem 1.4 (D.)**.** *Let A be a finite generating set of the multiplicative group Γ and assume $1 \in A$. If $|A \cdot A| < 2|A|$ then one of the following holds*

1. *Γ has a normal subgroup K so that Γ/K is either cyclic or dihedral.*
2. *There exists a proper coset K so that $\Gamma \setminus K \subseteq A \cdot A$.*

In fact, there are very wide sweeping generalizations of these results which concern sets A for which $|A \cdot A| < c|A|$ for a fixed constant c. There are structure theorems here due to Green-Ruzsa for abelian groups and due to Breulliard-Green-Tao for arbitrary groups which yield profound insights into the nature of these groups. We will not pursue this direction, but shall instead try to take some of the behaviour we see here and prove that similar things happen without all of the structure of a group.

2 Graphs

Assume now that Γ is a multiplicative group and let $A \subseteq \Gamma$. The Cayley Graph $Cayley(\Gamma, A)$ is a directed graph with vertex set Γ and an edge (x, y) whenever $y \in xA$. So, in words,

[1] In fact, this theorem has a more general form which involves sumsets of the form $A + B$.

[2] As with Cauchy-Davenport, Vosper's theorem applies more generally to sets A, B with $|A+B| < |A|+|B|$.

there is an edge from x to y if you can get from x to y my multiplying on the right by some element in A. Let $g \in \Gamma$ and consider the bijection of Γ given by the rule $x \to gx$. It follows immediately from our definition that this map sends directed edges to directed edges, so this gives an automorphism of our digraph. Since there is such an automorphism sending any vertex to any to any other vertex, every Cayley graph is vertex transitive.

One convenient property of Cayley graphs is that they permit us to analyze questions about small product sets using graphs. Indeed, for $Cayley(\Gamma, A)$ the size of A is precisely the degree of this regular digraph, and the size of the set $A \cdot A$ is precisely the number of vertices reachable from a given fixed vertex x by taking two (directed) steps. This gives us hope of following the theme of the previous section in a more general setting of digraphs instead of Cayley graphs. There are many nice questions in this realm which are unsolved. Here is one of my favourite.

Conjecture 2.1. *Let G be a simple d-regular digraph (all indegrees and outdegrees equal to d) with no directed cycles of length 1 or 2. Then there exists a vertex $x \in V(G)$ so that x can reach at least $2d$ vertices by a forward path of length 1 or 2.*

If true the above would resolve a very special case of the following very famous unsolved problem. (Namely the case when G is regular and $k = 3$).

Conjecture 2.2 (Caccetta-Häggkvist)**.** *Let k be a positive integer and let G be a simple n-vertex digraph. If every vertex in G has outdegree at least n/k, then G has a directed cycle of length at most k.*

As is common in graph theory, digraphs are awfully tricky and undirected graphs behave better. The following theorem is a related success for undirected graphs. Here the graph G^k denotes the simple graph with vertex set $V(G)$ and two vertices u, v adjacent in G^k if they have distance at most k in G.

Theorem 2.3 (D., Thomassé)**.** *If G is a simple connected graph of minimum degree d and diameter at least 3, then the average degree of G^3 is at least $\frac{7}{4}d$.*

A proof can be found in our paper on the Arxiv.