Quelques applications de la méthode isoperimétrique

Oriol Serra

Univ. Politècnica de Catalunya
Barcelona

Journée en Hommage à Yahya ould Hamidoune

The sumset problem

The estimation of cardinality of sumsets is a central tool in several problems. Yahya used this approach, among others, in

- Network reliability.
- Cacceta–Häggkvist conjecture.
- ZeroSum problems.
- Distinct sums.
- Complete sets.
- Frobenius problem.
- Sum–free sets.
- Additive basis.
- Diagonal forms.
- Dicks–Ivanov conjecture.
- Pollard theorem.
- and...Estimation of cardinality of sumsets.

A driving idea: the isoperimetric method

- $\Gamma \subset V \times V$ a relation (graph=directed graph=relation; undirected=symmetric; with loops=reflexive).
- $\Gamma(X)$: neighborhood of X.
- $\partial(X) = \Gamma(X) \setminus X$: boundary of X.

The isoperimetric problem: lower bounds of $|\partial X|$ in terms of $|X|$.

- $\kappa(X) = \min\{|\partial X| : X \subset V, \min\{|X|, |V \setminus \Gamma(X)|\} > 0\}$.
- F fragment if $|\partial F| = \kappa(X)$.
- $\mu(\Gamma)$ cardinality of smallest fragment.
- Atom: fragment of minimal cardinality.

Theorem (Hamidoune, 1977)

Let Γ be a reflexive relation with a transitive automorphism group. Suppose that $\mu(\Gamma) \leq \mu(\Gamma^{-1})$. Then the atoms form a set of blocks of imprimitivity.
In particular, the atom of a Cayley graph containing the unity is a subgroup.

Early applications

Theorem (Olson, 1976)

Let G be a group and $A, B \subset G$. We have

$$|AB| \geq \min\{|AK|, |A| + |B|/2\},$$

where $K = \langle BB^{-1} \rangle$.

- $|AB| = \Gamma(A)$ in $\Gamma = Cay(G, B)$ (with $1 \in B$).
- $|AB| - |A| \geq \kappa(\Gamma)$ unless $AB = AK$.
- U atom is a subgroup: $|AB| - |A| \geq |UB| - |U| \geq |UB|/2 \geq |B|/2$ (B is not contained in U.)

- The bound is tight and the extremal examples are given.
- Analogous argument shows that $\kappa(\Gamma) \geq r/2$ for vertex transitive graphs with degree r.
- Applies to infinite vertex transitive graphs.

Early applications

Theorem

In a connected arc–transitive graph the edge–connectivity equals the degree.

- Suppose that an atom U has $|U| > 1$.
- $\Gamma[U]$ has inner arcs.
- The automorphism sending an inner arc to a boundary arc contradicts atoms being blocks of imprimitivity.

Erdős –Heilbronn on subset sums

G abelian group with order n.

- Set of subset sums of $S \subset G$: $\Sigma(S) = \{\Sigma_{x\in T} x : T \subset S\}$.
- $S = \{a_1, \ldots, a_k\}$, $\Sigma(S) = \{0, a_1\} + \cdots \{0, a_t\}$
- Olson constant $Ol(G) = \min\{t : 0 \in \Sigma(S), \forall S \in \binom{G}{t}\}$.

Conjecture (Erdős–Heilbronn, 1964)

$Ol(G) \leq cn^{1/2}$.

- If $G = \mathbb{Z}/p\mathbb{Z}$ a zero subsetsum free is $1, 2, \ldots, \sqrt{2p}$
- Szeméredi (1970): proves the conjecture. (Erdős: $c = \sqrt{2}$).
- Olson (1975): $Ol(G) \leq 2\sqrt{n}$.
- Hamidoune and Zémor (1996): $Ol(\mathbb{Z}/p\mathbb{Z}) \leq \sqrt{2p} + \ln p$ (p prime) and $Ol(G) \leq \sqrt{2n} + O(n^{1/3} \ln n)$.
- Nguyen, Szeméredi, Vu (2008): $Ol(G) = \sqrt{2p}$ (for sufficiently large prime p.)
- Balandraud (2009): $Ol(\mathbb{Z}/p\mathbb{Z}) = \max\{k : k(k+1)/2 < p\}$ (Selfridge conjecture)

Complete sets and Diderrich conjecture

G abelian group with order n.

- $S \subset G$, $\Sigma(G) = \{\Sigma_{x \in T} x : T \subset S\}$.
- S is complete if $\Sigma(S) = G$.
- critical number $c(G) = \min\{t : \Sigma(S) = G, \forall S \in \binom{G}{t}\}$.

For p prime,

- Erdős–Heilbronn (1964) $c(G) \leq \sqrt{54p}$.
- Dias da Silva, Hamidoune (1994): $c(G) \leq \sqrt{4p-7} + 1$ (tight).
- Diderrich (1975) If $n = pq$, $p \leq q$, $q + p - 2 \leq c(G) \leq q + p - 1$ (both tight).

Complete sets and Diderrich conjecture

G abelian group with order n.

- $S \subset G$, $\Sigma(G) = \{\Sigma_{x \in T} x : T \subset S\}$.
- S is complete if $\Sigma(S) = G$.
- critical number $c(G) = \min\{t : \ \Sigma(S) = G, \ \forall S \in \binom{G}{t}\}$.

Conjecture (Diderrich (1975))

If n/p is not a prime then $c(G) = (n/p) + p - 2$. (p smallest divisor of n)

- Gao (1999): proof for large primes.
- Lipkin (1999): asymptotic proof.
- Hamidoune, Lladó, S. (1999): proof for $p = 3$.
- Gao, Hamidoune (1999): proof of Diderrich conjecture.
- Gao, Hamidoune, Lladó, S. (2001): Characterization of extremal sets well beyond the critical value:
  There are a subgroup H of order n/p and $y \notin H$ such that

$$(H \setminus 0) \subset S \text{ and } S \subset H \cup (y + H) \cup (-y + H).$$

Complete sets and Diderrich conjecture

G abelian group with order n.

- $S \subset G$, $\Sigma(G) = \{\Sigma_{x \in T} x : T \subset S\}$.
- S is complete if $\Sigma(S) = G$.
- critical number $c(G) = \min\{t : \ \Sigma(S) = G, \ \forall S \in \binom{G}{t}\}$.

- Vu (2007): If $S \subset \mathbb{Z}_n^*$ then S is complete for $|S| \geq c\sqrt{n}$.
- Hamidoune, Lladó, S. (2008): If $S \subset \mathbb{Z}_n^*$ then S is complete for $|S| \geq 2\sqrt{n-4} + 1$.

Use Chowla's theorem: If $A \subset \mathbb{Z}_n$ and $(B \setminus \{0\}) \subset \mathbb{Z}_n^*$ then $|A + B| \geq \min\{n, |A| + |B| - 1\}$ (and the Erdős average technique.)

A generalized Cauchy–Davenport inequality

M acyclic semigroup (associative law with identity): $xy = 1$ implies $x = y = 1$ and $xy = x$ implies $y = 1$.
Examples: Subsets or sequences of nonnegative integers with addition: $\mathcal{A}, B$ families of subsets,

$$\mathcal{A} + \mathcal{B} = \{A + B : A \in \mathcal{A}, B \in \mathcal{B}\}.$$

Theorem (Cilleruelo, Hamidoune, S. (2010))

Let $\mathcal{A}, B$ be two families of subsets: the Cauchy–Davenport inequality

$$|\mathcal{A} + \mathcal{B}| \geq |\mathcal{A}| + |\mathcal{B}| - 1,$$

holds if and only if one of the families is a chain in the poset $A < B$ iff $\min(A) < \min(B)$ or $\min(A) = \min(B)$ and $\max(A) < \max(B)$.

Uses the theory of atoms in the more abstract context of acyclic semigroups (and its graphs).

A theorem of Pollard

- G a group, $A, B \subset G$.
- $N_i(A, B)$ set of elements in AB with at least i representations.

Theorem (Pollard (1974))

Let $A, B \subset \mathbb{Z}_p$. If $t \leq \min\{|A|, |B|\}$ then

$$\sum_{i \leq t} |N_i(A, B)| \geq t \min\{p, |A| + |B| - t\}.$$

In connection with the Hanna Neuman conjecture, the following was proved:

Theorem (Dicks, Ivanov (2008))

Let A, B subsets of a group G, $\min\{|A|, |B|\} \geq 2$. Let $h \geq 3$ the smallest size of a subgroup of G.

$$|N_1(A, B)| + |N_2(A, B)| \geq 2 \min\{h, |A| + |B| - 2\}.$$

A theorem of Pollard

- G a group, $A, B \subset G$.
- $N_i(A, B)$ set of elements in AB with at least i representations.

Conjecture (Dicks, Ivanov (2008))

One of the following conditions holds:

(i) $|N_1(A, B)| + |N_2(A, B)| \geq 2(|A| + |B| - 2)$,

(ii) $N_2(A, B)$ *contains a left coset with cardinality* ≥ 3.

- Grynkiewicz (2010): Proof for the abelian case (with stronger conclussion).
- Hamidoune, S. (unpublished): Proof for the abelian case, extension to $N_t(A, B)$ and proof of the conjecture if $1 \neq A \cap B$ and $A \neq AB \neq B$.

A question of Tao

- G (nonabelian) group.
- $X \subset G$ finite subset.

Proposition (Weak Kneser theorem (Freiman, 1973; Tao, 2009))

If $|X^{-1}X|, |XX^{-1}| \leq c|X|$ *and* $1 \leq c \leq (1+\sqrt{5})/2$ *then* X *is contained in a (small) number* $\alpha(c)$ *of cosets of some finite subgroup.*

'It looks like one should be able to get a bit more structural information on than is given by the above conclusion, and I doubt the golden ratio is sharp either (the correct threshold should be 2, in analogy with the commutative Kneser theorem' (Terence Tao)

A question of Tao

- G (nonabelian) group.
- $X \subset G$ finite subset.

Theorem (Hamidoune (2010))

- *If*
$$|S^{-1}S| \le 2|S| - 2$$
then $S^{-1}S$ contains all but at most one right H–cosets it intersects.
- *If*
$$|S^2| \le (2 - (1/k))|S|,$$
where $k \le |S|$, then S can be covered by at most $(k-1)$ cosets of some subgroup H and $|S| > (k-2)|H|$.
- *If*
$$|S^{-1}S| \le \min\{G, 5/3|S|\},$$
then there is a normal subgroup K such that $S^{-1}S$ is K–periodic and contained in at most six K–cosets.

Tag Archive

You are currently browsing the tag archive for the 'Yahya Ould Hamidoune' tag.

Hamidoune's Freiman-Kneser theorem for nonabelian groups

12 March, 2011 in expository, math.CO, obituary | Tags: additive combinatorics, Freiman's theorem, Kneser's theorem, tom sanders, Yahya Ould Hamidoune | by Terence Tao | 9 comments

A few days ago, I received the sad news that Yahya Ould Hamidoune had recently died. Hamidoune worked in additive combinatorics, and had recently solved a question on noncommutative Freiman-Kneser theorems posed by myself on this blog last year. Namely, Hamidoune showed

Theorem 1 (Noncommutative Freiman-Kneser theorem for small doubling) Let $0 < \epsilon \leq 1$, and let $S \subset G$ be a finite non-empty subset of a multiplicative group G such that $|A \cdot S| \leq (2-\epsilon)|S|$ for some finite set A of cardinality $|A|$ at least $|S|$, where $A \cdot S := \{as : a \in A, s \in S\}$ is the product set of A and S. Then there exists a finite subgroup H of G with cardinality $|H| \leq C(\epsilon)|S|$, such that S is covered by at most $C'(\epsilon)$ right-cosets $H \cdot x$ of H, where $c(\epsilon), C(\epsilon) > 0$ depend only on ϵ.

Ongoing projects

- Dicks–Ivanov conjecture.
- Freiman $3k - 4$ for nonabelian torsion–free.
- Sums of dilates: the nonprime case.
- Beyond Kemperman.
- ...
- and the Mauritania school.

> Ceux qui aiment les maths ne sont jamais seuls.
>
> (Yahya)