Inverse theorems: very small sumsets

John Griesmer

Colorado School of Mines

jtgriesmer@gmail.com

University of Mississippi Number Theory Seminar
30 March 2022

Overview

1. Sumsets and the Cauchy-Davenport inequality
2. Inverse Theorems: Vosper, Kneser, Kemperman, and friends
3. General LCA groups: newer results
4. Lack of structure in $A+A$ for $|A| \approx \frac{1}{2}|G|$
5. Main tool: the e-transform

Let G be an abelian group and $A, B \subset G$. The sumset of A and B is

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

If $A = \{1, 4, 5\}$ and $B = \{0, 10, 100, 1000\}$, then

$$A + B = \{1, 4, 5, 11, 14, 15, 101, 104, 105, 1001, 1004, 1005\}$$

Here $|A + B| = |A||B|$.

If $C = \{3, 5, 7\}$ and $D = \{2, 4, 6, 8\}$ then

$$C + D = \{5, 7, 9, 11, 13, 15\}$$

Here $|C + D| = |C| + |D| - 1$.

Theorem

If $A, B \subset \mathbb{Z}$, then $|A| + |B| - 1 \leq |A + B| \leq |A||B|$.

Proof that $|A|+|B|-1 \leq |A+B|$ in $\mathbb{Z}$.

Write $A=\{a_1<a_2<\cdots<a_n\}$, $B=\{b_1<b_2<\cdots<b_m\}$
Then

$$\{a_1+b_1<a_2+b_1<\cdots<a_n+b_1<a_n+b_2<\cdots<a_n+b_m\}\subset A+B$$

Counting indices on the left reveals $|A|+|B|-1 \leq |A+B|$. $\square$

Pairs of sets A and B where equality occurs are highly structured:

Proposition

If $A, B \subset \mathbb{Z}$ and $|A+B| = |A|+|B|-1$, then $|A|=1$ or $|B|=1$ or A and B are arithmetic progressions with the same common difference:

$$A=\{a, a+d, a+2d, \ldots, a+(n-1)d\}$$
$$B=\{b, b+d, b+2d, \ldots, b+(m-1)d\}$$

Now let G be a finite abelian group. If H is a subgroup of G and B is a union of cosets of H, then $H+B=B$, so we now only have

$$|A+B| \geq \max\{|A|,|B|\}.$$

You can do better, especially in groups with few subgroups.

Theorem (Cauchy-Davenport)

If p is prime and $A, B \subset \mathbb{Z}/p\mathbb{Z}$, then $|A+B| \geq \min\{p, |A|+|B|-1\}$.

Examples where the bound is met:

(i) if $|A|+|B|>p$, then $A+B=\mathbb{Z}/p\mathbb{Z}$.

(ii) if $|A|+|B|=p$ and $A \cap B=\varnothing$, then $0 \notin A+(-B)$, so $|A+(-B)|=p-1$

(iii) if $|A|+|B| \leq p$ and A and B are arithmetic progressions with the same common difference.

(iv) if $|A|=1$ or $|B|=1$

Theorem (Vosper, [Vos56b],[Vos56a])

Let p be prime and $A, B \subset \mathbb{Z}/p\mathbb{Z}$ satisfy

$$|A + B| = |A| + |B| - 1 < p - 1.$$

Then $|A| = 1$ or $|B| = 1$, or

A and B are arithmetic progressions with the same common difference.

Can this classification be extended to other groups?

Yes. Such generalizations form a small portion of the inverse theorems in additive combinatorics.

Topological groups

A group G together with a topology is a *topological group* if the group operation $(x, y) \mapsto xy$ from $G \times G \to G$ is continuous and the inversion operation $x \mapsto x^{-1}$ is continuous.

"Locally compact" means there is a nonempty open neighborhood of the identity with compact closure.

Examples:

1. $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. A connected compact abelian group.
2. $\mathbb{T}^d$ for some $d \in \mathbb{N}$. Connected and compact.
3. $\mathbb{T}^2 \times \mathbb{Z}/15\mathbb{Z}$. Disconnected, compact. Has some proper open subgroups: $\mathbb{T}^2 \times \{0\}$, $\mathbb{T}^2 \times \{0, 5, 10\}$, etc.
4. p-adic integers

In this talk: focus on finite abelian groups and $\mathbb{T}^d \times F$, where $d \in \mathbb{N}$ and F is a finite abelian group.

Non-examples: $\mathbb{Q}$, infinite dimensional vector spaces, with any reasonable vector space topology (norm, weak, etc.)

Every compact abelian group G has a unique translation invariant Borel probability measure m_G, called Haar measure.

For locally compact, noncompact groups, $m_G(G) = \infty$, and we get uniqueness up to a constant multiple.

For finite groups Haar measure $=$ normalized counting measure.

On $\mathbb{T}^d \times F$ Haar measure is the product of normalized Lebesgue measure with normalized counting measure.

Very small sumsets: what is known about $m(A+B) \le m(A)+m(B)$ when $m(A), m(B) > 0$ in a locally compact abelian group?

Answer: everything.

M. Kneser [Kne56]: *Summenmengen in lokalkompakten abelschen Gruppen*

> reduces $m(A+B) < m(A)+m(B)$ to the same problem in finite abelian groups.
>
> classifies $m(A+B) = m(A)+m(B)$ in connected abelian groups

Kemperman [Kem60]: classifies $|A+B| < |A|+|B|$ in abel. gps.

Grynkiewicz [Gry09]: classifies $|A+B| = |A|+|B|$ in abel. gps.

Griesmer [Gri14]: classifies $m(A+B) = m(A)+m(B)$ in cpt. abel. gps.

Combining these five results yields a complete classification.
It's unpleasant to state due to sporadic examples and iterations.

Kneser's Satz 1

Definition

If $C \subset G$, the stabilizer of C is the group $H(C) := \{g \in G : g + C = C\}$.

Theorem ([Kne56], Satz 1)

If G is a locally compact abelian group and $A, B \subset G$ satisfy $m(A+B) < m(A) + m(B)$, then the stabilizer $H := H(A+B)$ of $A+B$ is compact and open and satisfies

$$m(A+B) = m(A+H) + m(B+H) - m(H). \tag{1}$$

In particular, $A+B$ is a union of cosets of H.

This reduces the study of $m(A+B) < m(A) + m(B)$ in LCA groups to the study of $|A+B| < |A| + |B|$ in finite groups. (Reduction is not obvious)

Connected groups have no proper open subgroups, so the following is an immediate corollary of Kneser's Satz 1:

Corollary

If G is a connected locally compact abelian group and $A, B \subset G$, then $m(A+B) \geq \min\{m(A)+m(B), m(G)\}$.

This extends work of MacBeath [Mac61], Shields [Shi55], Raikov [Rai40], and others in $\mathbb{T}^d$.

Kneser also classified all pairs where equality occurs in a connected compact group.

Definition

An interval in $\mathbb{T}$ is a set $[a, b] + \mathbb{Z}$, where $a \leq b \leq a+1 \in \mathbb{R}$.

Then $m(I) =$ length of I.

If I, J are intervals then $m(I+J) = \min\{m(I)+m(J), 1\}$.

All examples where $m(A), m(B) > 0$ and $m(A+B) = m(A)+m(B) < 1$ in connected groups come from intervals.

Lifting intervals to other groups

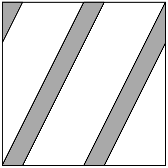
Definition

If $\pi : G \to \mathbb{T}$ is a continuous surjective homomorphism and $I \subset \mathbb{T}$ is an interval, we say $\tilde{I} := \pi^{-1}I$ is a Bohr interval in G.

If $\tilde{I} = \pi^{-1}I$ and $\tilde{J} = \pi^{-1}J$ are Bohr intervals defined with the same π, we say that $\tilde{I}$ and $\tilde{J}$ are parallel Bohr intervals.

Example in $G = \mathbb{T}^2$:

$$\pi : \mathbb{T}^2 \to \mathbb{T}, \quad \pi(x,y) = 2x - y$$
$$I = [0, 1/4] \subset \mathbb{T}$$
$$\tilde{I} = \pi^{-1}I = \{(x,y) : 2x - y \in [0, 1/4]\}$$



Small sumsets: if A and B are parallel Bohr intervals with $m(A) + m(B) < 1$, then $m(A+B) = m(A) + m(B)$.

Reason: Homomorphisms preserve Haar measure.

Theorem ([Kne56], Satz 2)

If G is a connected compact abelian group and $A, B \subset G$ satisfy $m(A) > 0$, $m(B) > 0$, and $m(A+B) = m(A) + m(B) < 1$, then there are parallel Bohr intervals $\tilde{I}, \tilde{J} \subset G$ such that $m(A) = m(\tilde{I})$, $m(B) = m(\tilde{J})$, and $A \subset \tilde{I}$ and $B \subset \tilde{J}$.

Corollary

If G is a connected compact abelian group, $A, B \subset G$ have positive measure, and $m(A+B) \leq m(A) + m(B)$, then $A+B$ contains a Bohr interval.

In general: if $m(A+B) \leq m(A) + m(B)$, then $A+B$ contains (up to measure 0, in some rare cases) highly structured subsets: either a coset of an open subgroup, or a Bohr interval.
Do results persist when the right hand side of $m(A+B) \leq m(A) + m(B)$ is relaxed slightly?
Yes, but with additional (some may say "artificial") hypotheses.

Theorem ("Approximate Satz 2" – [Tao18])

Let $\varepsilon > 0$. Then there exists $\delta > 0$ such that for every compact connected abelian group and every pair of sets $A, B \subset G$ such that $m(A), m(B) > \varepsilon$, $m(A) + m(B) < 1 - \varepsilon$, and

$$m(A + B) \leq m(A) + m(B) + \delta$$

there are parallel Bohr intervals $\tilde{I}, \tilde{J} \subset G$ such that

$$m(\tilde{I}) < m(A) + \varepsilon, \quad m(\tilde{J}) < m(B) + \varepsilon, \quad \text{and } A \subset \tilde{I}, B \subset \tilde{J}.$$

Applied recently by Tao and Teräväinen [TT19] to study Liouville function. Proof uses nonstandard analysis-ish arguments. Not really quantitative.

Theorem ([Gri19])

Same hypothesis as above, but with (possibly) disconnected G. Then there are sets $A', B' \subset G$ with $m(A \triangle A') + m(B \triangle B') \leq \varepsilon$ and $m(A' + B') \leq m(A') + m(B')$.

Proof uses ultraproducts. Utterly non-quantitative.

Natural questions

[Tao18] and [Gri19] study $m(A+B) < m(A) + m(B) + \delta$, assuming $m(A), m(B) > \varepsilon$ and $m(A) + m(B) < 1 - \varepsilon$.

Question

Can the dependence of δ on ε be specified? (Like $\delta = \varepsilon/100$ for $\varepsilon < 1/10$)

There are many quantitative results in specific groups.

Freiman: if $A \subset \mathbb{Z}/p\mathbb{Z}$, $|A| < p/35$, and $|A+A| < 2.4|A|$, then A is contained in an arithmetic progression of cardinality not too much larger than A. See [Nat96] for a proof.

[Lev22] is a recent breakthrough for general finite groups.

These kinds of results tend to use some harmonic analysis.

Nonabelian groups

[Kem64] extends Kneser's Satz 1 to study pairs A, B satisfying $m(AB) < m(A) + m(B)$ in a unimodular locally compact group.

The key equation $m(AB) = m(AH) + m(BH) - m(H)$ no longer holds.

Matt DeVos [DeV13] classified pairs $A, B \subset G$ satisfying $|AB| < |A| + |B|$ for arbitrary discrete groups.

A general classification for $m(AB) = m(A) + m(B)$ in an arbitrary compact group seems out of reach.

Björklund [Bjö17] classified pairs in compact topological groups with abelian identity component (and some minor additional hypotheses) where $m(AB) = m(A) + m(B)$.

Conjecture 5.1 of [Tao18]

Let G be a compact group with Haar probability measure m. For all $\varepsilon > 0$, there is a $\delta > 0$ such that if $A, B \subset G$ have $m(A), m(B) > \varepsilon$ and $m(AB) < m(A) + m(B) + \delta$, then there are $A', B' \subset G$ with $m(A \triangle A') + m(B \triangle B') \leq m(A) + m(B)$.

[Gri19] resolved the case where G is abelian.

There is recent work toward understanding very small sumsets in general locally compact groups:

[AJTZ21], [JT21], [JT20], [JTZ21]

(Jinpeng An, Yifan Jing, Chieu-Minh Tran, Ruixiang Zhang)

To motivate the next question, consider the following rhetorical questions.

Question

Let $G = \mathbb{T}^2$, and $A, B \subset G$ have $m(A) = m(B) = \frac{1}{2} - \varepsilon$ (think $\varepsilon = 10^{-100}$). Must $A + B$ contain a Bohr interval?

Answer: no – Bourgain (folklore, answering a question of Katznelson).

Question

Let G be a finite group and $|A| = |B| = (\frac{1}{2} - \varepsilon)|G|$. Must $A + B$ contain a coset of a large subgroup, or a long arithmetic progression?

Answer: no – Example 9.4 of Ben Green's *finite field models in additive combinatorics.*

These examples are instances of Ruzsa's famous *niveau set* construction.
Difference sets and the Bohr topology (link to Ruzsa's 1985 preprint)

The only known examples of large sets whose sumsets are unstructured in the way we're considering in this talk.

Julia Wolf's *Structure of popular difference sets* has a very nice exposition.

Lemma (Ruzsa's niveau sets in $\mathbb{F}_2^n$)

Fix $k \in \mathbb{N}$ and $\varepsilon > 0$. Then for all sufficiently large n, there is a set $A \subset \mathbb{F}_2^n$ such that

(i) $|A| > \left(\frac{1}{2} - \frac{\varepsilon}{2}\right)2^n$

(ii) $|A + A| < (2 + \varepsilon)|A|$

(iii) *$A + A$ does not contain a coset of a subgroup of index at most k.*

Proof: write $\mathbf{x} \in \mathbb{F}_2^n$ as strings of 0s and 1s: $\mathbf{x} = (x_1, \ldots, x_n)$.

$$\text{Let } A = \{\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n : \#\{i : x_i = 1\} > \frac{n}{2} + n^{1/3}\}$$

(i) Central Limit Theorem implies $|A| > \left(\frac{1}{2} - \frac{\varepsilon}{2}\right)2^n$ for large n

(ii) Follows from (i) and $|\mathbb{F}_2^n| = 2^n$.

(iii) We will show that

(iii.1) $C := \mathbb{F}_2^n \setminus (A + A)$ has nonempty intersection with every coset of every subgroup of index $2^{n^{1/3}}$. (Continue on next slide)

$$\text{Let } A = \{\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n : \#\{i : x_i = 1\} > \frac{n}{2} + n^{1/3}\}$$

(i) Central Limit Theorem implies $|A| > \left(\frac{1}{2} - \varepsilon\right)2^n$ for large n
(ii) Follows from (i) and $|\mathbb{F}_2^n| = 2^n$.
(iii) We will show that
(iii.1) $C := \mathbb{F}_2^n \setminus (A + A)$ has nonempty intersection with every coset of every subgroup of index $2^{n^{1/3}}$.
To do so, we claim that C contains the following set:

$$S_{n^{1/3}} := \{(x_1, \ldots, x_n) : \#\{i : x_i = 1\} > n^{1/3}\}$$

To see that $S_{n^{1/3}} \subset C$, we show that for all $\mathbf{x}, \mathbf{y} \in A$, the number of 1s in $\mathbf{x} - \mathbf{y}$ is at most $n^{1/3}$. This is because $\mathbf{x}$ and $\mathbf{y}$ must have at least $n^{1/3}$ entries $= 1$ in common.
It is "not hard" to check that $S_{n^{1/3}}$ has nonempty intersection with every coset of every subgroup of index at most $2^{n^{1/3}}$ (i.e. every subspace of dimension at least $\lfloor n^{1/3} \rfloor$).

Ruzsa constructed niveau sets in $\mathbb{Z}$, but the same idea works in any compact group. Use values of uncorrelated trig. polynomials instead of coordinates in $\mathbb{F}_2^n$.

Most known examples of sumsets lacking structure are based on this idea. Do these exhaust all possibilities?

Question

Is every example of a set $A \subset \mathbb{F}_2^n$ where $|A| \approx \frac{1}{2}|\mathbb{F}_2^n|$ and $A + A$ contains no coset of a large subgroup basically one of the sets constructed on the preceding two slides?

To be specific: Let

$A_{n,k} := \{\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n : \#\{i : x_i = 1\} > \frac{n}{2} + k\}$.

Let $d = d(n)$ go to infinity with n.

Fix $\varepsilon > 0$ and suppose $B_n \subset \mathbb{F}_2^n$ satisfies $|B_n| > (\frac{1}{2} - \frac{1}{d(n)})|\mathbb{F}_2^n|$ and $B_n + B_n$ does not contain a coset of a subgroup of index $d(n)$. Does there exist an isomorphism $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that $|B_n \triangle \phi^{-1} A_{n,k}| = o(2^n)$.

Main technique for abelian groups: Dyson e-transform

If $A, B \subset G$ and $e \in G$, form a new pair of sets

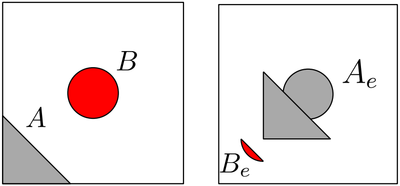
$$A_e = (A + e) \cup B, \quad B_e = A \cap (B - e)$$

Then

(i) $A_e + B_e \subset A + B$

(ii) $m(A_e) + m(B_e) = m(A) + m(B)$

Assuming $A + B$ is as small as possible, the e-transform allows you to find another pair A_e, B_e with $A_e + B_e \subset A + B$ and *smaller* B. So in finite groups you can do induction on the cardinality of B.



e-transform in $\mathbb{T}^2$ with $e = (0.25, 0.25)$

Lemma (e-transforms to shrink B in connected groups)

Suppose G is a connected compact abelian group and $m(A), m(B) > 0$ and $m(A) + m(B) < 1$ (NO HYPOTHESIS on $A + B$ here)
Then there is a sequence of pairs
$(A, B) = (A^{(1)}, B^{(1)}), (A^{(2)}, B^{(2)}), \ldots,$ *so that*

(i) $(A^{(n+1)}, B^{(n+1)})$ *is an e-transform of* $(A^{(n)}, B^{(n)})$

(ii) $m(B^{(n)}) \neq 0$, *and* $\lim_{n\to\infty} m(B^{(n)}) = 0$.

Proof uses an averaging argument and connectedness of G:
Note: $m(A^{(n)})$ can never exceed $m(A) + m(B)$.
$p(x) := m(A \cap (B - x))$ is continuous,
Fubini implies $\int m(A \cap (B - x))\, dm(x) = m(A)m(B)$.
So avg val of $m(A^{(n)} \cap (B^{(n)} - x))$ is $\leq cm(B)$, where $c \leq m(A) + m(B)$
So there is at least one x where $p(x) \leq cm(B)$, where $c < 1$ is INDEPENDENT of n. Also $p(x) > 0$ for some x.
Connectedness of G and continuity of p then provide an x where $p(x) < cm(B)$. This x is the e we use to form $(A^{(n+1)}, B^{(n+1)})$.

References I

- Jinpeng An, Yifan Jing, Chieu-Minh Tran, and Ruixiang Zhang, *On the small measure expansion phenomenon in connected noncompact nonabelian groups*, arXiv e-prints (2021), arXiv:2111.05236.
- Michael Björklund, *Small product sets in compact groups*, Fund. Math. **238** (2017), no. 1, 1–27. MR 3661726
- Matt DeVos, *The Structure of Critical Product Sets*, arXiv e-prints (2013), arXiv:1301.0096.
- John T. Griesmer, *An inverse theorem: when the measure of the sumset is the sum of the measures in a locally compact abelian group*, Trans. Amer. Math. Soc. **366** (2014), no. 4, 1797–1827. MR 3152713
- ______, *Semicontinuity of structure for small sumsets in compact abelian groups*, Discrete Anal. (2019), Paper No. 18, 46. MR 4042161

References II

David J. Grynkiewicz, *A step beyond Kemperman's structure theorem*, Mathematika **55** (2009), no. 1-2, 67–114. MR 2573603

Yifan Jing and Chieu-Minh Tran, *Minimal and nearly minimal measure expansions in connected unimodular groups*, arXiv e-prints (2020), arXiv:2006.01824.

______, *A Cauchy-Davenport theorem for locally compact groups*, arXiv e-prints (2021), arXiv:2106.02924.

Yifan Jing, Chieu-Minh Tran, and Ruixiang Zhang, *A nonabelian Brunn-Minkowski inequality*, arXiv e-prints (2021), arXiv:2101.07782.

J. H. B. Kemperman, *On small sumsets in an abelian group*, Acta Math. **103** (1960), 63–88. MR 110747

______, *On products of sets in a locally compact group*, Fund. Math. **56** (1964), 51–68. MR 202913

References III

- Martin Kneser, *Summenmengen in lokalkompakten abelschen Gruppen*, Math. Z. **66** (1956), 88–110. MR 81438

- Vsevolod F. Lev, *Small doubling in groups with moderate torsion*, SIAM J. Discrete Math. **36** (2022), no. 1, 315–335. MR 4372644

- A. M. MacBeath, *On measure of sumsets. III. The continuous $(\alpha + \beta)$-theorem*, Proc. Edinburgh Math. Soc. (2) **12** (1960/61), 209–211. MR 138716

- Melvyn B. Nathanson, *Additive number theory*, Graduate Texts in Mathematics, vol. 165, Springer-Verlag, New York, 1996, Inverse problems and the geometry of sumsets. MR 1477155

- D. A. Raikov, *A proof of a theorem of L. G. Schnirelmann concerning the density of the arithmetic sum of sets*, Uspekhi Matem. Nauk **7** (1940), 97–101. MR 0001775

- A. Shields, *Sur la mesure d'une somme vectorielle*, Fund. Math. **42** (1955), 57–60. MR 72201
- Terence Tao, *An inverse theorem for an inequality of Kneser*, Proc. Steklov Inst. Math. **303** (2018), no. 1, 193–219, Published in Russian in Tr. Mat. Inst. Steklova **3**03 (2018), 209–238. MR 3920221
- Terence Tao and Joni Teräväinen, *Value patterns of multiplicative functions and related sequences*, Forum Math. Sigma **7** (2019), Paper No. e33, 55. MR 4016500
- A. G. Vosper, *Addendum to "The critical pairs of subsets of a group of prime order"*, J. London Math. Soc. **31** (1956), 280–282. MR 78368
- _______, *The critical pairs of subsets of a group of prime order*, J. London Math. Soc. **31** (1956), 200–205. MR 77555