SNEVILY'S CONJECTURE

by

Bodan Arsovski

ST CATHERINE'S COLLEGE, OXFORD

Motivation

Many questions in additive combinatorics relate the sizes of

$$A \text{ and } B, \text{ subsets of a group } G$$

with the size of

$$A + B, \text{ the set } \{a + b \,|\, a \in A \text{ and } b \in B\}.$$

Motivation

A central example:

Cauchy–Davenport Theorem (1813)

If $G = F_p$, then

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

There are many extensions of this theorem, and it can be proven in at least 3 different ways.

Motivation

A central example:

Cauchy–Davenport Theorem (1813)

If $G = F_p$, then

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

There are many extensions of this theorem, and it can be proven in at least 3 different ways.

Motivation

The bound is best possible in general.

However, if A and B are of size k each, then the sum $a + b$ can be formed in k^2 ways, so the bound is relatively weak.

A natural question to ask is: although we cannot strengthen the right side, perhaps we can strengthen the left side?

In other words, perhaps we can bound *special subsets of* $A + B$ in terms of $|A|$ and $|B|$?

For example, what if we decide only to consider the sums $a + b$ such that $a \neq b$?

Motivation

The bound is best possible in general.

However, if A and B are of size k each, then the sum $a + b$ can be formed in k^2 ways, so the bound is relatively weak.

A natural question to ask is: although we cannot strengthen the right side, perhaps we can strengthen the left side?

In other words, perhaps we can bound *special subsets of* $A + B$ in terms of $|A|$ and $|B|$?

For example, what if we decide only to consider the sums $a + b$ such that $a \neq b$?

Motivation

This question turns out to be quite difficult, even though there are still $k^2 - k$ ways to form the sum $a + b$.

Erdös–Heilbronn Conjecture (1964, first proved 1994)

If $G = F_p$, then the size of

$$\{a + b \,|\, a \in A \text{ and } b \in B \text{ and } a \neq b\}$$

is at least

$$\min\{|A| + |B| - 3, p\}.$$

Motivation

Therefore, interesting questions arise from considering subsets of $A + B$.

A natural follow-up question is of considering a *least possible* subset of $A + B$:

Question.

If G is a finite abelian group, if A and B are subsets of G, each of size k, is there a bijection $\rho : A \to B$ such that

$$|\{a + \rho(a) \mid a \in A\}| \geq k?$$

This is false as stated if G contains $\mathbb{Z}/(2)$, which leads to the following conjecture.

Motivation

Therefore, interesting questions arise from considering subsets of $A + B$.

A natural follow-up question is of considering a *least possible* subset of $A + B$:

Question.

If G is a finite abelian group, if A and B are subsets of G, each of size k, is there a bijection $\rho : A \to B$ such that

$$|\{a + \rho(a) \mid a \in A\}| \geq k?$$

This is false as stated if G contains $\mathbb{Z}/(2)$, which leads to the following conjecture.

Snevily's Conjecture (1999)

Abelian group G of odd size.

Subsets $\{a_1, \ldots, a_k\}$ and $\{b_1, \ldots, b_k\}$ of G.

Does there exist a permutation π such that

$$a_1 + b_{\pi(1)}, \ldots, a_k + b_{\pi(k)}$$

are pairwise distinct?

How Much Is Known?

a proof for cyclic groups of prime order. [Alon, 2000]
(embedding the group as the additive group of F_p)

a proof for all cyclic groups.
[Dasgupta, Károlyi, Serra, Szegedy, 2001]
(embedding the group as a subgroup of $\mathbb{C}^\times$)

a proof for all groups. [Arsovski, 2009]
(working with the dual group of homomorphisms into $F^\times$
for a suitable field F of characteristic 2)

How Much Is Known?

a proof for cyclic groups of prime order. [Alon, 2000]
(embedding the group as the additive group of F_p)

a proof for all cyclic groups.
[Dasgupta, Károlyi, Serra, Szegedy, 2001]
(embedding the group as a subgroup of $\mathbb{C}^\times$)

a proof for all groups. [Arsovski, 2009]
(working with the dual group of homomorphisms into $F^\times$
for a suitable field F of characteristic 2)

How Much Is Known?

a proof for cyclic groups of prime order. [Alon, 2000]

(embedding the group as the additive group of F_p)

a proof for all cyclic groups.

[Dasgupta, Károlyi, Serra, Szegedy, 2001]

(embedding the group as a subgroup of $\mathbb{C}^\times$)

a proof for all groups. [Arsovski, 2009]

(working with the dual group of homomorphisms into $F^\times$

for a suitable field F of characteristic 2)

How Much Is Known?

a proof for cyclic groups of prime order. [Alon, 2000]

(embedding the group as the additive group of F_p)

a proof for all cyclic groups.

[Dasgupta, Károlyi, Serra, Szegedy, 2001]

(embedding the group as a subgroup of $\mathbb{C}^\times$)

a proof for all groups. [Arsovski, 2009]

(working with the dual group of homomorphisms into $F^\times$ for a suitable field F of characteristic 2)

The Proof

Basic linear algebra

Plan of The Proof

Instead of just G, consider also $\mathrm{Hom}(G, F^\times)$, which is isomorphic to G under suitable conditions.

The set $\mathrm{Hom}(G, F^\times)$ is linearly independent. (Dedekind)

So any map φ can be written as a linear combination of homomorphisms $G \to F^\times$.

Algebraic manipulations which involve the fact that any general φ has a sort of multiplicative structure by above.

Plan of The Proof

Instead of just G, consider also $\mathrm{Hom}(G, F^\times)$, which is isomorphic to G under suitable conditions.

The set $\mathrm{Hom}(G, F^\times)$ is linearly independent. (Dedekind)

So any map φ can be written as a linear combination of homomorphisms $G \to F^\times$.

Algebraic manipulations which involve the fact that any general φ has a sort of multiplicative structure by above.

Plan of The Proof

Instead of just G, consider also $\mathrm{Hom}(G, F^\times)$, which is isomorphic to G under suitable conditions.

The set $\mathrm{Hom}(G, F^\times)$ is linearly independent. (Dedekind)

So any map φ can be written as a linear combination of homomorphisms $G \to F^\times$.

Algebraic manipulations which involve the fact that any general φ has a sort of multiplicative structure by above.

Plan of The Proof

Instead of just G, consider also $\mathrm{Hom}(G, F^\times)$, which is isomorphic to G under suitable conditions.

The set $\mathrm{Hom}(G, F^\times)$ is linearly independent. (Dedekind)

So any map φ can be written as a linear combination of homomorphisms $G \to F^\times$.

Algebraic manipulations which involve the fact that any general φ has a sort of multiplicative structure by above.

Theorem (Dedekind)

If G is a group and F is a field, the set of homomorphisms $\chi_\alpha : G \to F^\times$ is linearly independent.

Proof. Assume dependency $a_1\chi_1 + \cdots + a_s\chi_s = 0$ with minimal s. As $\chi_1 \neq \chi_2$ then $\chi_1(g) \neq \chi_2(g)$ for some g. Multiply $\Sigma a_i\chi_i(x) = 0$ by $\chi_1(g)$, and then subtract $\Sigma a_i\chi_i(xg) = \Sigma a_i\chi_i(x)\chi_i(g) = 0$ to get

$$\sum_{j\geq 2} a_j\chi_j(x)(\chi_1(g) - \chi_j(g)) = 0,$$

contradicting minimality of s. □

Theorem (Dedekind)

If G is a group and F is a field, the set of homomorphisms $\chi_\alpha : G \to F^\times$ is linearly independent.

Proof. Assume dependency $a_1\chi_1 + \cdots + a_s\chi_s = 0$ with minimal s. As $\chi_1 \neq \chi_2$ then $\chi_1(g) \neq \chi_2(g)$ for some g.

Multiply $\Sigma a_i\chi_i(x) = 0$ by $\chi_1(g)$, and then subtract $\Sigma a_i\chi_i(xg) = \Sigma a_i\chi_i(x)\chi_i(g) = 0$ to get

$$\sum_{j\geq 2} a_j\chi_j(x)(\chi_1(g) - \chi_j(g)) = 0,$$

contradicting minimality of s. □

Theorem (Dedekind)

If G is a group and F is a field, the set of homomorphisms $\chi_\alpha : G \to F^\times$ is linearly independent.

Proof. Assume dependency $a_1\chi_1 + \cdots + a_s\chi_s = 0$ with minimal s. As $\chi_1 \neq \chi_2$ then $\chi_1(g) \neq \chi_2(g)$ for some g. Multiply $\Sigma a_i\chi_i(x) = 0$ by $\chi_1(g)$, and then subtract $\Sigma a_i\chi_i(xg) = \Sigma a_i\chi_i(x)\chi_i(g) = 0$ to get

$$\sum_{j\geq 2} a_j\chi_j(x)(\chi_1(g) - \chi_j(g)) = 0,$$

contradicting minimality of s. □

Corollary.

If G a finite abelian group of size m and F a finite field such that m divides $|F^\times|$, then $\mathrm{Hom}(G, F^\times)$ *spans the space of maps from G to F.*

Proof. In this case $\mathrm{Hom}(G, F^\times)$ is isomorphic to G so there are exactly as many homomorphisms $G \to F^\times$ as we would expect in a basis. □

Lemma.

Given $k \times k$ array of elements $g_{ij} \in G$.

Any two in the same row or column are distinct.

If F is a field with more than k elements, then there exists a function $\varphi : G \to F$ such that

$$\det \|\varphi(g_{ij})\| \neq 0$$

Proof. Induction on k. The case $k = 1$ is trivial. If $k > 1$, suppose g appears as an entry. The determinant of the array is a polynomial in $\varphi(g)$, of degree at most $k < |F|$, with leading coefficient the determinant of a submatrix of $(\varphi(g_{ij}))$. By the induction hypothesis, φ can be defined on $G \backslash \{g\}$ in a way that this coefficient is nonzero. The polynomial in $\varphi(g)$, obtained in this way, is not the zero polynomial, and has degree at most $k < |F|$. Therefore, $\varphi(g)$ can be assigned a value from F in a way that this polynomial does not vanish. $\square$

Proof. Induction on k. The case $k = 1$ is trivial. If $k > 1$, suppose g appears as an entry. The determinant of the array is a polynomial in $\varphi(g)$, of degree at most $k < |F|$, with leading coefficient the determinant of a submatrix of $(\varphi(g_{ij}))$. By the induction hypothesis, φ can be defined on $G \backslash \{g\}$ in a way that this coefficient is nonzero. The polynomial in $\varphi(g)$, obtained in this way, is not the zero polynomial, and has degree at most $k < |F|$. Therefore, $\varphi(g)$ can be assigned a value from F in a way that this polynomial does not vanish. $\square$

Proof. Induction on k. The case $k = 1$ is trivial. If $k > 1$, suppose g appears as an entry. The determinant of the array is a polynomial in $\varphi(g)$, of degree at most $k < |F|$, with leading coefficient the determinant of a submatrix of $(\varphi(g_{ij}))$. By the induction hypothesis, φ can be defined on $G \backslash \{g\}$ in a way that this coefficient is nonzero. The polynomial in $\varphi(g)$, obtained in this way, is not the zero polynomial, and has degree at most $k < |F|$. Therefore, $\varphi(g)$ can be assigned a value from F in a way that this polynomial does not vanish. $\square$

Proof. Induction on k. The case $k = 1$ is trivial. If $k > 1$, suppose g appears as an entry. The determinant of the array is a polynomial in $\varphi(g)$, of degree at most $k < |F|$, with leading coefficient the determinant of a submatrix of $(\varphi(g_{ij}))$. By the induction hypothesis, φ can be defined on $G \backslash \{g\}$ in a way that this coefficient is nonzero. The polynomial in $\varphi(g)$, obtained in this way, is not the zero polynomial, and has degree at most $k < |F|$. Therefore, $\varphi(g)$ can be assigned a value from F in a way that this polynomial does not vanish. $\square$

Proof. Induction on k. The case $k = 1$ is trivial. If $k > 1$, suppose g appears as an entry. The determinant of the array is a polynomial in $\varphi(g)$, of degree at most $k < |F|$, with leading coefficient the determinant of a submatrix of $(\varphi(g_{ij}))$. By the induction hypothesis, φ can be defined on $G \backslash \{g\}$ in a way that this coefficient is nonzero. The polynomial in $\varphi(g)$, obtained in this way, is not the zero polynomial, and has degree at most $k < |F|$. Therefore, $\varphi(g)$ can be assigned a value from F in a way that this polynomial does not vanish. $\square$

Corollary.

If $\{a_1, \ldots, a_k\}$ and $\{b_1, \ldots, b_k\}$ are subsets of a group G.

If F is a field with more than k elements.

Then there exists a function $\varphi : G \to F$ such that

$$\det \|\varphi(a_i + b_j)\| \neq 0$$

Let G be an abelian group of odd size m.

Let F be a finite field of characteristic 2 and size q such that $m \mid q-1$, so that $q > m$. For example, take $q = 2^{\phi(m)}$.

We know that there is a map $\varphi : G \to F$ such that $\det \|\varphi(a_i + b_j)\| \neq 0$.

We also know that the set of all homomorphisms $\varphi_1, \ldots, \varphi_m : G \to F^\times$ spans the space of maps from G to F.

Therefore, there are elements $\lambda_1, \ldots, \lambda_m \in F$ such that

$$\varphi = \lambda_1 \varphi_1 + \cdots + \lambda_m \varphi_m$$

Let G be an abelian group of odd size m.

Let F be a finite field of characteristic 2 and size q such that $m \mid q-1$, so that $q > m$. For example, take $q = 2^{\phi(m)}$.

We know that there is a map $\varphi : G \to F$ such that $\det \|\varphi(a_i + b_j)\| \neq 0$.

We also know that the set of all homomorphisms $\varphi_1, \ldots, \varphi_m : G \to F^\times$ spans the space of maps from G to F.

Therefore, there are elements $\lambda_1, \ldots, \lambda_m \in F$ such that

$$\varphi = \lambda_1 \varphi_1 + \cdots + \lambda_m \varphi_m$$

Let G be an abelian group of odd size m.

Let F be a finite field of characteristic 2 and size q such that $m \mid q-1$, so that $q > m$. For example, take $q = 2^{\phi(m)}$.

We know that there is a map $\varphi : G \to F$ such that $\det \|\varphi(a_i + b_j)\| \neq 0$.

We also know that the set of all homomorphisms $\varphi_1, \ldots, \varphi_m : G \to F^\times$ spans the space of maps from G to F.

Therefore, there are elements $\lambda_1, \ldots, \lambda_m \in F$ such that

$$\varphi = \lambda_1 \varphi_1 + \cdots + \lambda_m \varphi_m$$

Let G be an abelian group of odd size m.

Let F be a finite field of characteristic 2 and size q such that $m \mid q-1$, so that $q > m$. For example, take $q = 2^{\phi(m)}$.

We know that there is a map $\varphi : G \to F$ such that $\det \|\varphi(a_i + b_j)\| \neq 0$.

We also know that the set of all homomorphisms $\varphi_1, \ldots, \varphi_m : G \to F^\times$ spans the space of maps from G to F.

Therefore, there are elements $\lambda_1, \ldots, \lambda_m \in F$ such that

$$\varphi = \lambda_1 \varphi_1 + \cdots + \lambda_m \varphi_m$$

The determinant is a multilinear map, so

$$\det \|\varphi(a_i + b_j)\| = \sum_{s_1,\ldots,s_k=1}^{m} \left(\prod_{i=1}^{k} \lambda_{s_i} \right) \det \|\varphi_{s_i}(a_i + b_j)\|$$

If two among the indices $s_1, \ldots, s_k$ are equal then the two corresponding rows of the matrix $\|\varphi_{s_i}(a_i + b_j)\|$ are proportional, so the determinant vanishes. So

$$\sum_{s_1,\ldots,s_k=1}^{m} \left(\prod_{i=1}^{k} \lambda_{s_i} \right) \det \|\varphi_{s_i}(a_i + b_j)\| =$$

$$\sum_{1 \le s_1 < \cdots < s_k \le m} \left(\prod_{i=1}^{k} \lambda_{s_i} \right) \left(\sum_{\pi \in S_k} \det \left\| \varphi_{s_{\pi(i)}}(a_i + b_j) \right\| \right)$$

The determinant is a multilinear map, so

$$\det \|\varphi(a_i + b_j)\| = \sum_{s_1,\ldots,s_k=1}^{m} \left(\prod_{i=1}^{k} \lambda_{s_i} \right) \det \|\varphi_{s_i}(a_i + b_j)\|$$

If two among the indices $s_1, \ldots, s_k$ are equal then the two corresponding rows of the matrix $\|\varphi_{s_i}(a_i + b_j)\|$ are proportional, so the determinant vanishes. So

$$\sum_{s_1,\ldots,s_k=1}^{m} \left(\prod_{i=1}^{k} \lambda_{s_i} \right) \det \|\varphi_{s_i}(a_i + b_j)\| =$$

$$\sum_{1 \le s_1 < \cdots < s_k \le m} \left(\prod_{i=1}^{k} \lambda_{s_i} \right) \left(\sum_{\pi \in S_k} \det \left\| \varphi_{s_{\pi(i)}}(a_i + b_j) \right\| \right)$$

$$\sum_{s_1,\ldots,s_k=1}^{m} \left(\prod_{i=1}^{k} \lambda_{s_i} \right) \det \|\varphi_{s_i}(a_i + b_j)\| =$$

$$\sum_{1 \le s_1 < \cdots < s_k \le m} \left(\prod_{i=1}^{k} \lambda_{s_i} \right) \left(\sum_{\pi \in S_k} \det \left\| \varphi_{s_{\pi(i)}}(a_i + b_j) \right\| \right)$$

But the whole thing on the right is nonzero.

Which means that, for some k-tuple $s_1, \ldots, s_k$, the sum

$$\sum_{\pi \in S_k} \det \left\| \varphi_{s_{\pi(i)}}(a_i + b_j) \right\| \neq 0$$

$$
\begin{aligned}
0 \neq & \sum_{\pi \in S_k} \det \left\| \varphi_{s_{\pi(i)}}(a_i + b_j) \right\| \\
= & \sum_{\pi \in S_k} \left(\sum_{\tau \in S_k} \prod_{i=1}^{k} \varphi_{s_{\pi(i)}}(a_i + b_{\tau(i)}) \right) \\
= & \sum_{\pi \in S_k} \left(\sum_{\tau \in S_k} \prod_{i=1}^{k} \varphi_{s_i}(a_{\pi^{-1}(i)} + b_{\tau(\pi^{-1}(i))}) \right) \\
= & \sum_{\tau \in S_k} \left(\sum_{\pi \in S_k} \prod_{i=1}^{k} \varphi_{s_i}(a_{\pi(i)} + b_{\tau(\pi(i))}) \right) \\
= & \sum_{\tau \in S_k} \det \left\| \varphi_{s_i}(a_j + b_{\tau(j)}) \right\| \neq 0
\end{aligned}
$$

Since

$$\sum_{\tau \in S_k} \det \left\| \varphi_{s_i}(a_j + b_{\tau(j)}) \right\| \neq 0$$

it follows that, for some τ,

$$\det \left\| \varphi_{s_i}(a_j + b_{\tau(j)}) \right\| \neq 0$$

So in particular the columns are different.

So the numbers $a_j + b_{\tau(j)}$ are different. $\square$

Since

$$\sum_{\tau \in S_k} \det \left\| \varphi_{s_i}(a_j + b_{\tau(j)}) \right\| \neq 0$$

it follows that, for some τ,

$$\det \left\| \varphi_{s_i}(a_j + b_{\tau(j)}) \right\| \neq 0$$

So in particular the columns are different.

So the numbers $a_j + b_{\tau(j)}$ are different. $\square$

Remarks

The proof needs that F be of characteristic 2, since the change of variable in the algebraic manipulations works only if we ignore signs.

Since $F^\times$ is cyclic, and so $\mathrm{Hom}(G, F^\times)$ is isomorphic of G if and only if the exponent of G divides $|F^\times|$, it is crucial in the proof that this exponent is odd, and therefore that G has odd size.

In fact, Snevily's conjecture is not true if G has even size, since it is not true for $\mathbb{Z}/(2)$.

Questions

It seems that even-sized subgroups are the only obstruction, and the answer to the following question is unknown.

Question 1. If G is a finite abelian group. If A and B are subsets of G, each of size k. If neither A nor B is a translate of an even-sized subgroup of G. Then there exists a bijection $\rho : A \to B$ such that all the numbers $a + \rho(a)$ are different. (Open problem garden)

Question 2. What can we say about non-commutative G? (Snevily, personal communication)

Questions

It seems that even-sized subgroups are the only obstruction, and the answer to the following question is unknown.

Question 1. If G is a finite abelian group. If A and B are subsets of G, each of size k. If neither A nor B is a translate of an even-sized subgroup of G. Then there exists a bijection $\rho : A \to B$ such that all the numbers $a + \rho(a)$ are different. (Open problem garden)

Question 2. What can we say about non-commutative G? (Snevily, personal communication)

- N. Alon, *Additive Latin transversals,* Israel Journal of Mathematics **117** (2000), *125–130*
- S. Dasgupta, Gy. Károlyi, O. Serra, B. Szegedy, *Transversals of additive Latin squares,* Israel Journal of Mathematics, **126** (2001), *17–28*
- B. Arsovski, *A proof of Snevily's conjecture,* Israel Journal of Mathematics, *to appear*
- H. Snevily, *Unsolved Problems: The Cayley Addition Table of $\mathbb{Z}/n\mathbb{Z}$,* American Mathematical Monthly **106** (1999), #6, *584–585*