Selected Problems in Additive Combinatorics

Vsevolod F. Lev

The University of Haifa

Graz, January 2015

Kneser's Theorem for Restricted Addition

Theorem (Kneser)

Suppose that A and B are finite, non-empty subsets of an abelian group. If $|A+B| < |A|+|B|-1$, then $A+B$ is periodic.

What is the analogue of Kneser's Theorem for the restricted sumset

$$A \dot{+} B := \{a+b\colon a \in A,\ b \in B,\ a \neq b\}?$$

We seek a result of the following sort:

If *($A\dot{+}B$ is small)*, then *(something very special happens)*.

Suppose for simplicity that the underlying group has no involutions.

The *($A\dot{+}B$ is small)* part: the natural bound is $|A\dot{+}B| < |A|+|B|-3$.

The *(something special happens)* part: not only is $A\dot{+}B$ periodic, but indeed we have $A\dot{+}B = A+B$!

Kneser's Theorem for Restricted Addition

Theorem (Kneser)

Suppose that A and B are finite, non-empty subsets of an abelian group. If $|A+B| < |A|+|B|-1$, then $A+B$ is periodic.

What is the analogue of Kneser's Theorem for the restricted sumset

$$A \dot{+} B := \{a+b\colon a\in A,\ b\in B,\ a\neq b\}?$$

We seek a result of the following sort:

If *($A\dot{+}B$ is small)*, then *(something very special happens)*.

Suppose for simplicity that the underlying group has no involutions.

The *($A\dot{+}B$ is small)* part: the natural bound is $|A\dot{+}B| < |A|+|B|-3$.

The *(something special happens)* part: not only is $A\dot{+}B$ periodic, but indeed we have $A\dot{+}B = A+B$!

Kneser's Theorem for Restricted Addition

Theorem (Kneser)

Suppose that A and B are finite, non-empty subsets of an abelian group. If $|A+B| < |A|+|B|-1$, then $A+B$ is periodic.

What is the analogue of Kneser's Theorem for the restricted sumset

$$A \dot{+} B := \{a+b\colon\, a \in A,\ b \in B,\ a \neq b\}?$$

We seek a result of the following sort:

If *($A\dot{+}B$ is small)*, then *(something very special happens)*.

Suppose for simplicity that the underlying group has no involutions.

The *($A\dot{+}B$ is small)* part: the natural bound is $|A\dot{+}B| < |A|+|B|-3$.

The *(something special happens)* part: not only is $A\dot{+}B$ periodic, but indeed we have $A\dot{+}B = A+B$!

Kneser's Theorem for Restricted Addition

Theorem (Kneser)

Suppose that A and B are finite, non-empty subsets of an abelian group. If $|A+B| < |A| + |B| - 1$, then $A+B$ is periodic.

What is the analogue of Kneser's Theorem for the restricted sumset

$$A \dot{+} B := \{a+b\colon\, a \in A,\ b \in B,\ a \neq b\}?$$

We seek a result of the following sort:

If *($A \dot{+} B$ is small)*, then *(something very special happens)*.

Suppose for simplicity that the underlying group has no involutions.

The *($A \dot{+} B$ is small)* part: the natural bound is $|A \dot{+} B| < |A| + |B| - 3$.

The *(something special happens)* part: not only is $A \dot{+} B$ periodic, but indeed we have $A \dot{+} B = A + B$!

Kneser's Theorem for Restricted Addition (Continued)

Conjecture (J. de Théorie des Nombres de Bordeaux 2005)

Suppose that A and B are finite, non-empty subsets of an involution-free abelian group. If $|A \dot{+} B| < |A| + |B| - 3$, then $A \dot{+} B = A + B$ (whence $A \dot{+} B$ is periodic).

- $A \dot{+} B = A + B$ implies periodicity of $A \dot{+} B$ in view of the assumption $|A \dot{+} B| < |A| + |B| - 3$, by Kneser's theorem.
- Interestingly, periodicity suffices: if one could show that $|A \dot{+} B| < |A| + |B| - 3$ implies periodicity of $A \dot{+} B$, this would give the strong form of the conjecture ($A \dot{+} B = A + B$).
- For the group $\mathbb{F}_p$, the sumset $A \dot{+} B$ is periodic iff $A \dot{+} B = \mathbb{F}_p$; hence, for the prime-order groups, the conjecture is equivalent to the Erdős-Heilbronn Conjecture.
- In the general case, the conjecture is both an analogue and a counterpart of Kneser's Theorem: if $A \dot{+} B$ is small, then it can be studied using KT.

Kneser's Theorem for Restricted Addition (Continued)

Conjecture (J. de Théorie des Nombres de Bordeaux 2005)

Suppose that A and B are finite, non-empty subsets of an involution-free abelian group. If $|A\dot{+}B| < |A| + |B| - 3$, then $A\dot{+}B = A + B$ (whence $A\dot{+}B$ is periodic).

- $A\dot{+}B = A + B$ implies periodicity of $A\dot{+}B$ in view of the assumption $|A\dot{+}B| < |A| + |B| - 3$, by Kneser's theorem.
- Interestingly, periodicity suffices: if one could show that $|A\dot{+}B| < |A| + |B| - 3$ implies periodicity of $A\dot{+}B$, this would give the strong form of the conjecture ($A\dot{+}B = A + B$).
- For the group $\mathbb{F}_p$, the sumset $A\dot{+}B$ is periodic iff $A\dot{+}B = \mathbb{F}_p$; hence, for the prime-order groups, the conjecture is equivalent to the Erdős-Heilbronn Conjecture.
- In the general case, the conjecture is both an analogue and a counterpart of Kneser's Theorem: if $A\dot{+}B$ is small, then it can be studied using KT.

Kneser's Theorem for Restricted Addition (Continued)

Conjecture (J. de Théorie des Nombres de Bordeaux 2005)

Suppose that A and B are finite, non-empty subsets of an involution-free abelian group. If $|A\dot{+}B| < |A| + |B| - 3$, then $A\dot{+}B = A + B$ (whence $A\dot{+}B$ is periodic).

- $A\dot{+}B = A + B$ implies periodicity of $A\dot{+}B$ in view of the assumption $|A\dot{+}B| < |A| + |B| - 3$, by Kneser's theorem.
- Interestingly, periodicity suffices: if one could show that $|A\dot{+}B| < |A| + |B| - 3$ implies periodicity of $A\dot{+}B$, this would give the strong form of the conjecture ($A\dot{+}B = A + B$).
- For the group $\mathbb{F}_p$, the sumset $A\dot{+}B$ is periodic iff $A\dot{+}B = \mathbb{F}_p$; hence, for the prime-order groups, the conjecture is equivalent to the Erdős-Heilbronn Conjecture.
- In the general case, the conjecture is both an analogue and a counterpart of Kneser's Theorem: if $A\dot{+}B$ is small, then it can be studied using KT.

Kneser's Theorem for Restricted Addition (Continued)

Conjecture (J. de Théorie des Nombres de Bordeaux 2005)

Suppose that A and B are finite, non-empty subsets of an involution-free abelian group. If $|A\dot{+}B| < |A| + |B| - 3$, then $A\dot{+}B = A + B$ (whence $A\dot{+}B$ is periodic).

- $A\dot{+}B = A + B$ implies periodicity of $A\dot{+}B$ in view of the assumption $|A\dot{+}B| < |A| + |B| - 3$, by Kneser's theorem.
- Interestingly, periodicity suffices: if one could show that $|A\dot{+}B| < |A| + |B| - 3$ implies periodicity of $A\dot{+}B$, this would give the strong form of the conjecture ($A\dot{+}B = A + B$).
- For the group $\mathbb{F}_p$, the sumset $A\dot{+}B$ is periodic iff $A\dot{+}B = \mathbb{F}_p$; hence, for the prime-order groups, the conjecture is equivalent to the Erdős-Heilbronn Conjecture.
- In the general case, the conjecture is both an analogue and a counterpart of Kneser's Theorem: if $A\dot{+}B$ is small, then it can be studied using KT.

Kneser's Theorem for Restricted Addition (Continued)

Conjecture (J. de Théorie des Nombres de Bordeaux 2005)

Suppose that A and B are finite, non-empty subsets of an involution-free abelian group. If $|A \dot{+} B| < |A| + |B| - 3$, then $A \dot{+} B = A + B$ (whence $A \dot{+} B$ is periodic).

- $A \dot{+} B = A + B$ implies periodicity of $A \dot{+} B$ in view of the assumption $|A \dot{+} B| < |A| + |B| - 3$, by Kneser's theorem.
- Interestingly, periodicity suffices: if one could show that $|A \dot{+} B| < |A| + |B| - 3$ implies periodicity of $A \dot{+} B$, this would give the strong form of the conjecture ($A \dot{+} B = A + B$).
- For the group $\mathbb{F}_p$, the sumset $A \dot{+} B$ is periodic iff $A \dot{+} B = \mathbb{F}_p$; hence, for the prime-order groups, the conjecture is equivalent to the Erdős-Heilbronn Conjecture.
- In the general case, the conjecture is both an analogue and a counterpart of Kneser's Theorem: if $A \dot{+} B$ is small, then it can be studied using KT.

Kneser's Theorem for Restricted Addition (Continued)

Kemperman and Scherk have shown that if there exists $c \in A + B$ with a unique representation as $c = a + b$ with $a \in A$ and $b \in B$, then $|A + B| \geq |A| + |B| - 1$.

Conjecture (Restatement 1)

Suppose that A and B are finite, non-empty subsets of an abelian group. If there exists $c \in A + B$ with a unique representation as $c = a + b$ with $a \in A$ and $b \in B$, then $|A \dot{+} B| \geq |A| + |B| - 3$.

Conjecture (Restatement 2)

Suppose that A and B are finite, non-empty subsets of an abelian group. If $|(A + B) \setminus (A \dot{+} B)| \geq 3$, then $|A \dot{+} B| \geq |A| + |B| - 3$.

- The general case reduces to that where $0 \in B \subseteq A$ and $0 \notin A \dot{+} B$.
- The conjecture is true in torsion-free groups, prime-order groups, groups of exponent 2, small-order cyclic groups (computationally).

Kneser's Theorem for Restricted Addition (Continued)

Kemperman and Scherk have shown that if there exists $c \in A + B$ with a unique representation as $c = a + b$ with $a \in A$ and $b \in B$, then $|A + B| \geq |A| + |B| - 1$.

Conjecture (Restatement 1)

Suppose that A and B are finite, non-empty subsets of an abelian group. If there exists $c \in A + B$ with a unique representation as $c = a + b$ with $a \in A$ and $b \in B$, then $|A \dot{+} B| \geq |A| + |B| - 3$.

Conjecture (Restatement 2)

Suppose that A and B are finite, non-empty subsets of an abelian group. If $|(A + B) \setminus (A \dot{+} B)| \geq 3$, then $|A \dot{+} B| \geq |A| + |B| - 3$.

- The general case reduces to that where $0 \in B \subseteq A$ and $0 \notin A \dot{+} B$.
- The conjecture is true in torsion-free groups, prime-order groups, groups of exponent 2, small-order cyclic groups (computationally).

Kneser's Theorem for Restricted Addition (Continued)

Kemperman and Scherk have shown that if there exists $c \in A + B$ with a unique representation as $c = a + b$ with $a \in A$ and $b \in B$, then $|A + B| \geq |A| + |B| - 1$.

Conjecture (Restatement 1)

Suppose that A and B are finite, non-empty subsets of an abelian group. If there exists $c \in A + B$ with a unique representation as $c = a + b$ with $a \in A$ and $b \in B$, then $|A \dot{+} B| \geq |A| + |B| - 3$.

Conjecture (Restatement 2)

Suppose that A and B are finite, non-empty subsets of an abelian group. If $|(A + B) \setminus (A \dot{+} B)| \geq 3$, then $|A \dot{+} B| \geq |A| + |B| - 3$.

- The general case reduces to that where $0 \in B \subseteq A$ and $0 \notin A \dot{+} B$.
- The conjecture is true in torsion-free groups, prime-order groups, groups of exponent 2, small-order cyclic groups (computationally).

"Small" Sets in the Freiman Isomorphism Classes

The set $\{0, 1, 2, 4, \dots, 2^{n-2}\}$ is linear (has Freiman's rank 1); as such, it is not Freiman-isomorphic to any shorter set. Is this the extremal case?

Conjecture (Konyagin-Lev, Mathematika 2000)

Any n-element set of integers is isomorphic to a subset of $[0, 2^{n-2}]$.

For sets of rank r, it is natural to seek "compact" isomorphic sets in $\mathbb{Z}^r$.

Conjecture (Konyagin-Lev, Mathematika 2000)

For any n-element integer set A of rank r, there exist integer $l_1, \dots, l_r \geq 0$ with $l_1 + \dots + l_r \leq n - r - 1$ such that A is isomorphic to a subset of the parallelepiped $[0, l_1] \times \dots \times [0, l_r] \subseteq \mathbb{Z}^r$.

Both conjectures are true in the extremal cases $r = 1$ (linear sets) and $r = n - 1$ (Sidon sets).

Grynkiewicz has some partial results on the second conjecture.

"Small" Sets in the Freiman Isomorphism Classes

The set $\{0, 1, 2, 4, \dots, 2^{n-2}\}$ is linear (has Freiman's rank 1); as such, it is not Freiman-isomorphic to any shorter set. Is this the extremal case?

Conjecture (Konyagin-Lev, Mathematika 2000)

Any n-element set of integers is isomorphic to a subset of $[0, 2^{n-2}]$.

For sets of rank r, it is natural to seek "compact" isomorphic sets in $\mathbb{Z}^r$.

Conjecture (Konyagin-Lev, Mathematika 2000)

For any n-element integer set A of rank r, there exist integer $l_1, \dots, l_r \geq 0$ with $l_1 + \dots + l_r \leq n - r - 1$ such that A is isomorphic to a subset of the parallelepiped $[0, l_1] \times \dots \times [0, l_r] \subseteq \mathbb{Z}^r$.

Both conjectures are true in the extremal cases $r = 1$ (linear sets) and $r = n - 1$ (Sidon sets).

Grynkiewicz has some partial results on the second conjecture.

Large Sum-Free Sets in $\mathbb{F}_3^n$

Any affine hyperplane in $\mathbb{F}_3^n$ which is not a *linear* hyperplane is a sum-free subset of $\mathbb{F}_3^n$ of size 3^{n-1}. Conversely, if $A \subseteq \mathbb{F}_3^n$ is sum-free, then A, $A - a$, and $A + a$ are pairwise disjoint for any fixed $a \in A$. Hence, 3^{n-1} is the largest possible size of a sum-free subset of $\mathbb{F}_3^n$.

(Notice that in a characteristic other than 3, one can have sum-free sets A with $(A - a) \cap (A + a) \neq \varnothing$ for some $a \in A$.)

What do large sum-free subsets of $\mathbb{F}_3^n$ look like?

Theorem (J. Combinatorial Theory A, 2005)

If $n \geq 3$ and $A \subseteq \mathbb{F}_3^n$ is sum-free of size $|A| > \frac{5}{27} \cdot 3^n$, then A is contained in an affine hyperplane.

The coefficient $5/27$ is best possible and cannot be replaced with a smaller number. Yet, there is a room for a significant improvement.

Large Sum-Free Sets in $\mathbb{F}_3^n$

Any affine hyperplane in $\mathbb{F}_3^n$ which is not a *linear* hyperplane is a sum-free subset of $\mathbb{F}_3^n$ of size 3^{n-1}. Conversely, if $A \subseteq \mathbb{F}_3^n$ is sum-free, then A, $A - a$, and $A + a$ are pairwise disjoint for any fixed $a \in A$. Hence, 3^{n-1} is the largest possible size of a sum-free subset of $\mathbb{F}_3^n$.

(Notice that in a characteristic other than 3, one can have sum-free sets A with $(A - a) \cap (A + a) \neq \varnothing$ for some $a \in A$.)

What do large sum-free subsets of $\mathbb{F}_3^n$ look like?

Theorem (J. Combinatorial Theory A, 2005)

If $n \geq 3$ and $A \subseteq \mathbb{F}_3^n$ is sum-free of size $|A| > \frac{5}{27} \cdot 3^n$, then A is contained in an affine hyperplane.

The coefficient $5/27$ is best possible and cannot be replaced with a smaller number. Yet, there is a room for a significant improvement.

Large Sum-Free Sets in $\mathbb{F}_3^n$

Any affine hyperplane in $\mathbb{F}_3^n$ which is not a *linear* hyperplane is a sum-free subset of $\mathbb{F}_3^n$ of size 3^{n-1}. Conversely, if $A \subseteq \mathbb{F}_3^n$ is sum-free, then A, $A-a$, and $A+a$ are pairwise disjoint for any fixed $a \in A$. Hence, 3^{n-1} is the largest possible size of a sum-free subset of $\mathbb{F}_3^n$.

(Notice that in a characteristic other than 3, one can have sum-free sets A with $(A-a) \cap (A+a) \neq \varnothing$ for some $a \in A$.)

What do large sum-free subsets of $\mathbb{F}_3^n$ look like?

Theorem (J. Combinatorial Theory A, 2005)

If $n \geq 3$ and $A \subseteq \mathbb{F}_3^n$ is sum-free of size $|A| > \frac{5}{27} \cdot 3^n$, then A is contained in an affine hyperplane.

The coefficient $5/27$ is best possible and cannot be replaced with a smaller number. Yet, there is a room for a significant improvement.

Large Sum-Free Sets in $\mathbb{F}_3^n$ (Continued)

- One can obtain sum-free sets in $\mathbb{F}_3^n$ by "lifting" sum-free sets from lower dimensions: if $m < n$ and $\varphi \colon \mathbb{F}_3^n \to \mathbb{F}_3^m$ is a surjective homomorphism, then for any sum-free set $A_0 \subseteq \mathbb{F}_3^m$, the full inverse image $A := \varphi^{-1}(A_0) \subseteq \mathbb{F}_3^n$ is sum-free and has the same density in $\mathbb{F}_3^n$ as A_0 has in $\mathbb{F}_3^m$.

  A sum-free set $A \subseteq \mathbb{F}_3^n$ can be obtained by lifting if and only if it is *periodic*.
- One can also obtain sum-free sets by removing some elements from larger sum-free sets.

Thus, of real interest are those sum-free sets which are *aperiodic* and *maximal* (by inclusion). They are "building blocks" from which all other sum-free sets can be obtained by lifting / removing elements.

How large can a maximal, aperiodic sum-free set in $\mathbb{F}_3^n$ be?

Large Sum-Free Sets in $\mathbb{F}_3^n$ (Continued)

- One can obtain sum-free sets in $\mathbb{F}_3^n$ by "lifting" sum-free sets from lower dimensions: if $m < n$ and $\varphi\colon \mathbb{F}_3^n \to \mathbb{F}_3^m$ is a surjective homomorphism, then for any sum-free set $A_0 \subseteq \mathbb{F}_3^m$, the full inverse image $A := \varphi^{-1}(A_0) \subseteq \mathbb{F}_3^n$ is sum-free and has the same density in $\mathbb{F}_3^n$ as A_0 has in $\mathbb{F}_3^m$.

  A sum-free set $A \subseteq \mathbb{F}_3^n$ can be obtained by lifting if and only if it is *periodic*.
- One can also obtain sum-free sets by removing some elements from larger sum-free sets.

Thus, of real interest are those sum-free sets which are *aperiodic* and *maximal* (by inclusion). They are "building blocks" from which all other sum-free sets can be obtained by lifting / removing elements.

How large can a maximal, aperiodic sum-free set in $\mathbb{F}_3^n$ be?

Large Sum-Free Sets in $\mathbb{F}_3^n$ (Continued)

Conjecture (J. Combinatorial Theory A, 2005)

The largest possible size of a maximal, aperiodic sum-free set in $\mathbb{F}_3^n$ is $(3^{n-1}+1)/2$.

There is an explicit construction of a maximal, aperiodic sum-free set in $\mathbb{F}_3^n$ of size $(3^{n-1}+1)/2$; the conjecture thus says that one cannot go beyond that.

Establishing this conjecture would allow one to classify all sum-free subsets of $\mathbb{F}_3^n$ of density larger than $\frac{1}{6}+\varepsilon$, for any fixed $\varepsilon > 0$.

When does $P(a-b)=0,\ a\neq b$ imply $P(0)=0$?

Suppose $A\subseteq\mathbb{F}_2^n$. Given that $P\in\mathbb{F}_2[x_1,\dots,x_n]$ vanishes on $A\dot{+}A=(A+A)\setminus\{0\}$, can we conclude that also $P(0)=0$?

Not necessarily: any function on $\mathbb{F}_2^n$ can be represented by a polynomial. What if $\deg P$ is small, while A is large?

Given $d\geq 0$, how large must $A\subseteq\mathbb{F}_2^n$ be to ensure that if $\deg P\leq d$ and $P(a+b)=0$ for all $a,b\in A,\ a\neq b$, then also $P(0)=0$?

- P constant ($d=0$): suffices to have $|A|\geq 2$ (so that $A\dot{+}A\neq\varnothing$).
- P linear ($d=1$): $|A|=2$ insufficient (take $A=\{0,e_1\}, P=x_1+1$), while $|A|\geq 3$ suffices (if $\{a,b,c\}\subseteq A$ and $P(a+b)=P(b+c)=P(c+a)=0$, then also $P(0)=0$ as $0=(a+b)+(b+c)+(c+a)$ and P is linear).
- P quadratic ($d=2$): $|A|\geq n+3$ suffices, $|A|=n+1$ is not enough (consider $A=\{0,e_1,\dots,e_n\}$, $P=1+\sum_{1\leq i\leq n}x_i+\sum_{1\leq i<j\leq n}x_ix_j$).

When does $P(a-b)=0,\ a\neq b$ imply $P(0)=0$?

Suppose $A\subseteq\mathbb{F}_2^n$. Given that $P\in\mathbb{F}_2[x_1,\dots,x_n]$ vanishes on $A\dot{+}A=(A+A)\setminus\{0\}$, can we conclude that also $P(0)=0$?

Not necessarily: any function on $\mathbb{F}_2^n$ can be represented by a polynomial. What if $\deg P$ is small, while A is large?

Given $d\geq 0$, how large must $A\subseteq\mathbb{F}_2^n$ be to ensure that if $\deg P\leq d$ and $P(a+b)=0$ for all $a,b\in A,\ a\neq b$, then also $P(0)=0$?

- P constant ($d=0$): suffices to have $|A|\geq 2$ (so that $A\dot{+}A\neq\varnothing$).
- P linear ($d=1$): $|A|=2$ insufficient (take $A=\{0,e_1\}, P=x_1+1$), while $|A|\geq 3$ suffices (if $\{a,b,c\}\subseteq A$ and $P(a+b)=P(b+c)=P(c+a)=0$, then also $P(0)=0$ as $0=(a+b)+(b+c)+(c+a)$ and P is linear).
- P quadratic ($d=2$): $|A|\geq n+3$ suffices, $|A|=n+1$ is not enough (consider $A=\{0,e_1,\dots,e_n\}$, $P=1+\sum_{1\leq i\leq n}x_i+\sum_{1\leq i<j\leq n}x_ix_j$).

When does $P(a-b)=0,\ a \neq b$ imply $P(0)=0$?

Suppose $A \subseteq \mathbb{F}_2^n$. Given that $P \in \mathbb{F}_2[x_1, \dots, x_n]$ vanishes on $A \dot{+} A = (A+A) \setminus \{0\}$, can we conclude that also $P(0)=0$?

Not necessarily: any function on $\mathbb{F}_2^n$ can be represented by a polynomial. What if $\deg P$ is small, while A is large?

Given $d \geq 0$, how large must $A \subseteq \mathbb{F}_2^n$ be to ensure that if $\deg P \leq d$ and $P(a+b)=0$ for all $a, b \in A,\ a \neq b$, then also $P(0)=0$?

- P constant ($d=0$): suffices to have $|A| \geq 2$ (so that $A \dot{+} A \neq \varnothing$).
- P linear ($d=1$): $|A|=2$ insufficient (take $A=\{0, e_1\}, P=x_1+1$), while $|A| \geq 3$ suffices (if $\{a,b,c\} \subseteq A$ and $P(a+b)=P(b+c)=P(c+a)=0$, then also $P(0)=0$ as $0=(a+b)+(b+c)+(c+a)$ and P is linear).
- P quadratic ($d=2$): $|A| \geq n+3$ suffices, $|A|=n+1$ is not enough (consider $A=\{0, e_1, \dots, e_n\}$, $P=1+\sum_{1 \leq i \leq n} x_i + \sum_{1 \leq i < j \leq n} x_i x_j$).

When does $P(a-b)=0,\ a\neq b$ imply $P(0)=0$?

Suppose $A\subseteq\mathbb{F}_2^n$. Given that $P\in\mathbb{F}_2[x_1,\dots,x_n]$ vanishes on $A\dot{+}A=(A+A)\setminus\{0\}$, can we conclude that also $P(0)=0$?

Not necessarily: any function on $\mathbb{F}_2^n$ can be represented by a polynomial. What if $\deg P$ is small, while A is large?

Given $d\geq 0$, how large must $A\subseteq\mathbb{F}_2^n$ be to ensure that if $\deg P\leq d$ and $P(a+b)=0$ for all $a,b\in A,\ a\neq b$, then also $P(0)=0$?

- P constant ($d=0$): suffices to have $|A|\geq 2$ (so that $A\dot{+}A\neq\varnothing$).
- P linear ($d=1$): $|A|=2$ insufficient (take $A=\{0,e_1\}, P=x_1+1$), while $|A|\geq 3$ suffices (if $\{a,b,c\}\subseteq A$ and $P(a+b)=P(b+c)=P(c+a)=0$, then also $P(0)=0$ as $0=(a+b)+(b+c)+(c+a)$ and P is linear).
- P quadratic ($d=2$): $|A|\geq n+3$ suffices, $|A|=n+1$ is not enough (consider $A=\{0,e_1,\dots,e_n\}$, $P=1+\sum_{1\leq i\leq n}x_i+\sum_{1\leq i<j\leq n}x_ix_j$).

When does $P(a-b)=0,\ a\neq b$ imply $P(0)=0$?

Suppose $A\subseteq\mathbb{F}_2^n$. Given that $P\in\mathbb{F}_2[x_1,\dots,x_n]$ vanishes on $A\dot{+}A=(A+A)\setminus\{0\}$, can we conclude that also $P(0)=0$?

Not necessarily: any function on $\mathbb{F}_2^n$ can be represented by a polynomial. What if $\deg P$ is small, while A is large?

Given $d\geq 0$, how large must $A\subseteq\mathbb{F}_2^n$ be to ensure that if $\deg P\leq d$ and $P(a+b)=0$ for all $a,b\in A,\ a\neq b$, then also $P(0)=0$?

- P constant ($d=0$): suffices to have $|A|\geq 2$ (so that $A\dot{+}A\neq\varnothing$).
- P linear ($d=1$): $|A|=2$ insufficient (take $A=\{0,e_1\}, P=x_1+1$), while $|A|\geq 3$ suffices (if $\{a,b,c\}\subseteq A$ and $P(a+b)=P(b+c)=P(c+a)=0$, then also $P(0)=0$ as $0=(a+b)+(b+c)+(c+a)$ and P is linear).
- P quadratic ($d=2$): $|A|\geq n+3$ suffices, $|A|=n+1$ is not enough (consider $A=\{0,e_1,\dots,e_n\}$, $P=1+\sum_{1\leq i\leq n}x_i+\sum_{1\leq i<j\leq n}x_ix_j$).

When does $P(a-b)=0,\ a\neq b$ imply $P(0)=0$?

Suppose $A\subseteq\mathbb{F}_2^n$. Given that $P\in\mathbb{F}_2[x_1,\dots,x_n]$ vanishes on $A\dot{+}A=(A+A)\setminus\{0\}$, can we conclude that also $P(0)=0$?

Not necessarily: any function on $\mathbb{F}_2^n$ can be represented by a polynomial. What if $\deg P$ is small, while A is large?

Given $d\geq 0$, how large must $A\subseteq\mathbb{F}_2^n$ be to ensure that if $\deg P\leq d$ and $P(a+b)=0$ for all $a,b\in A,\ a\neq b$, then also $P(0)=0$?

- P constant ($d=0$): suffices to have $|A|\geq 2$ (so that $A\dot{+}A\neq\varnothing$).
- P linear ($d=1$): $|A|=2$ insufficient (take $A=\{0,e_1\}, P=x_1+1$), while $|A|\geq 3$ suffices (if $\{a,b,c\}\subseteq A$ and $P(a+b)=P(b+c)=P(c+a)=0$, then also $P(0)=0$ as $0=(a+b)+(b+c)+(c+a)$ and P is linear).
- P quadratic ($d=2$): $|A|\geq n+3$ suffices, $|A|=n+1$ is not enough (consider $A=\{0,e_1,\dots,e_n\}$, $P=1+\sum_{1\leq i\leq n}x_i+\sum_{1\leq i<j\leq n}x_ix_j$).

When does $P(a-b)=0$ imply $P(0)=0$? (Continued)

For cubic polynomials the problem is wide open: it is not even clear whether $|A|$ can be polynomial in n (or must be exponential).

Problem

How large must $A \subseteq \mathbb{F}_2^n$ be to ensure that if P is a cubic polynomial in n variables over $\mathbb{F}_2$ satisfying $P(a+b)=0$ for all $a, b \in A,\ a \neq b$, then also $P(0)=0$?

Generally, for $d \geq 3$ given, how large must $A \subseteq \mathbb{F}_2^n$ be to ensure that if $P \in \mathbb{F}_2[x_1, \dots, x_n]$ is a polynomial of degree d satisfying $P(a+b)=0$ for all $a, b \in A,\ a \neq b$, then also $P(0)=0$?

Motivation: an $\mathbb{F}_2$-analogue of the “Roth' problem” by Ernie Croot. To make a progress in Ernie's problem, one needs to show that for polynomials of degree about $(0.5+\varepsilon)n$, it suffices to have, say, $|A| > 2^n/n^2$.

When does $P(a-b)=0$ imply $P(0)=0$? (Continued)

For cubic polynomials the problem is wide open: it is not even clear whether $|A|$ can be polynomial in n (or must be exponential).

Problem

How large must $A \subseteq \mathbb{F}_2^n$ be to ensure that if P is a cubic polynomial in n variables over $\mathbb{F}_2$ satisfying $P(a+b)=0$ for all $a,b \in A,\ a \neq b$, then also $P(0)=0$?

Generally, for $d \geq 3$ given, how large must $A \subseteq \mathbb{F}_2^n$ be to ensure that if $P \in \mathbb{F}_2[x_1,\dots,x_n]$ is a polynomial of degree d satisfying $P(a+b)=0$ for all $a,b \in A,\ a \neq b$, then also $P(0)=0$?

Motivation: an $\mathbb{F}_2$-analogue of the "Roth' problem" by Ernie Croot.
To make a progress in Ernie's problem, one needs to show that for polynomials of degree about $(0.5+\varepsilon)n$, it suffices to have, say, $|A| > 2^n/n^2$.

Large Doubling-Critical Sets in $\mathbb{F}_2^n$

Definition

We say that a subset A of an abelian group is doubling-critical if, for any proper subset $B \subsetneq A$, we have $2B \neq 2A$.

That is, A is doubling-critical if, for any given $a \in A$, there exists $a' \in A$ such that $a + a'$ has a unique representation in $2A$ $(= A + A)$.

- Every set A with $|A| \leq 2$ is doubling-critical. (Three-element subgroups are not doubling-critical!)
- Every Sidon set is doubling-critical.

The ideology: *small* doubling-critical sets are common, *large* doubling-critical sets are rare and must be structured.

What is the largest possible size of a doubling-critical subset of a finite abelian group G? What is the structure of large doubling-critical subsets of G?

Large Doubling-Critical Sets in $\mathbb{F}_2^n$

Definition

We say that a subset A of an abelian group is doubling-critical if, for any proper subset $B \subsetneq A$, we have $2B \neq 2A$.

That is, A is doubling-critical if, for any given $a \in A$, there exists $a' \in A$ such that $a + a'$ has a unique representation in $2A$ $(= A + A)$.

- Every set A with $|A| \leq 2$ is doubling-critical. (Three-element subgroups are not doubling-critical!)
- Every Sidon set is doubling-critical.

The ideology: *small* doubling-critical sets are common, *large* doubling-critical sets are rare and must be structured.

What is the largest possible size of a doubling-critical subset of a finite abelian group G? What is the structure of large doubling-critical subsets of G?

Large Doubling-Critical Sets in $\mathbb{F}_2^n$

Definition

We say that a subset A of an abelian group is doubling-critical if, for any proper subset $B \subsetneq A$, we have $2B \neq 2A$.

That is, A is doubling-critical if, for any given $a \in A$, there exists $a' \in A$ such that $a + a'$ has a unique representation in $2A$ $(= A + A)$.

- Every set A with $|A| \leq 2$ is doubling-critical. (Three-element subgroups are not doubling-critical!)
- Every Sidon set is doubling-critical.

The ideology: *small* doubling-critical sets are common, *large* doubling-critical sets are rare and must be structured.

What is the largest possible size of a doubling-critical subset of a finite abelian group G? What is the structure of large doubling-critical subsets of G?

Large Doubling-Critical Sets in $\mathbb{F}_2^n$ (Continued)

If A is a doubling-critical subset of a finite abelian group G, then $|A| \le \frac{1}{2}|G| + 1$. (For if $B \subset A$, $|B| > \frac{1}{2}|G|$, then $2B = 2A = G$.)

Equality is attained if $|G|$ is even: if $H < G$ with $|H| = \frac{1}{2}|G|$ and $g \in G \setminus H$, then $A := (g + H) \cup \{0\}$ is doubling-critical.

A generalization: if $S \subseteq G$ is sum-free, then $S \cup \{0\}$ is doubling-critical — and so are its translates $g + (S \cup \{0\})$.

Theorem (Grynkiewicz-Lev, SIDMA 2010)

Suppose that $A \subseteq \mathbb{F}_2^n$ is doubling critical. If $|A| > \frac{11}{36} \cdot 2^n + 3$, then

$$A = g + (S \cup \{0\})$$

with a sum-free set $S \subseteq \mathbb{F}_2^n$ and an element $g \in \mathbb{F}_2^n$.

Problem

Replace the coefficient $\frac{11}{36}$ with the best possible one.
(At least $\frac{1}{4}$ should be possible.)

Large Doubling-Critical Sets in $\mathbb{F}_2^n$ (Continued)

If A is a doubling-critical subset of a finite abelian group G, then $|A| \le \frac{1}{2}|G| + 1$. (For if $B \subset A,\ |B| > \frac{1}{2}|G|$, then $2B = 2A = G$.)

Equality is attained if $|G|$ is even: if $H < G$ with $|H| = \frac{1}{2}|G|$ and $g \in G \setminus H$, then $A := (g + H) \cup \{0\}$ is doubling-critical.

A generalization: if $S \subseteq G$ is sum-free, then $S \cup \{0\}$ is doubling-critical — and so are its translates $g + (S \cup \{0\})$.

Theorem (Grynkiewicz-Lev, SIDMA 2010)

Suppose that $A \subseteq \mathbb{F}_2^n$ is doubling critical. If $|A| > \frac{11}{36} \cdot 2^n + 3$, then

$$A = g + (S \cup \{0\})$$

with a sum-free set $S \subseteq \mathbb{F}_2^n$ and an element $g \in \mathbb{F}_2^n$.

Problem

Replace the coefficient $\frac{11}{36}$ with the best possible one. (At least $\frac{1}{4}$ should be possible.)

Large Doubling-Critical Sets in $\mathbb{F}_2^n$ (Continued)

If A is a doubling-critical subset of a finite abelian group G, then $|A| \le \frac{1}{2}|G| + 1$. (For if $B \subset A$, $|B| > \frac{1}{2}|G|$, then $2B = 2A = G$.)

Equality is attained if $|G|$ is even: if $H < G$ with $|H| = \frac{1}{2}|G|$ and $g \in G \setminus H$, then $A := (g + H) \cup \{0\}$ is doubling-critical.

A generalization: if $S \subseteq G$ is sum-free, then $S \cup \{0\}$ is doubling-critical — and so are its translates $g + (S \cup \{0\})$.

Theorem (Grynkiewicz-Lev, SIDMA 2010)

Suppose that $A \subseteq \mathbb{F}_2^n$ is doubling critical. If $|A| > \frac{11}{36} \cdot 2^n + 3$, then

$$A = g + (S \cup \{0\})$$

with a sum-free set $S \subseteq \mathbb{F}_2^n$ and an element $g \in \mathbb{F}_2^n$.

Problem

Replace the coefficient $\frac{11}{36}$ with the best possible one.
(At least $\frac{1}{4}$ should be possible.)

Large Doubling-Critical Sets in $\mathbb{F}_2^n$ (Continued)

If A is a doubling-critical subset of a finite abelian group G, then $|A| \le \frac{1}{2}|G| + 1$. (For if $B \subset A$, $|B| > \frac{1}{2}|G|$, then $2B = 2A = G$.)

Equality is attained if $|G|$ is even: if $H < G$ with $|H| = \frac{1}{2}|G|$ and $g \in G \setminus H$, then $A := (g + H) \cup \{0\}$ is doubling-critical.

A generalization: if $S \subseteq G$ is sum-free, then $S \cup \{0\}$ is doubling-critical — and so are its translates $g + (S \cup \{0\})$.

Theorem (Grynkiewicz-Lev, SIDMA 2010)

Suppose that $A \subseteq \mathbb{F}_2^n$ is doubling critical. If $|A| > \frac{11}{36} \cdot 2^n + 3$, then

$$A = g + (S \cup \{0\})$$

with a sum-free set $S \subseteq \mathbb{F}_2^n$ and an element $g \in \mathbb{F}_2^n$.

Problem

Replace the coefficient $\frac{11}{36}$ with the best possible one.
(At least $\frac{1}{4}$ should be possible.)

Large Doubling-Critical Sets in $\mathbb{F}_p$

For a prime p, let $\mathrm{DC}[\mathbb{F}_p]$ denote the family of all doubling-critical subsets of $\mathbb{F}_p$.

Since $\mathbb{F}_p$ has sum-free subsets of size $\frac{1}{3}p + O(1)$, we have

$$\frac{1}{3}p + O(1) \le \max\{|A| \colon A \in \mathrm{DC}[\mathbb{F}_p]\} \le \frac{1}{2}p + O(1),$$

and I can improve this to

$$\frac{1}{3}p + O(1) \le \max\{|A| \colon A \in \mathrm{DC}[\mathbb{F}_p]\} \le \frac{2}{5}p + O(1).$$

Problem

What is the largest possible size of a doubling-critical set in $\mathbb{F}_p$?
(It is tempting to conjecture $\frac{1}{3}p + O(1)$.)

Problem

How about *difference*-critical sets?

Large Doubling-Critical Sets in $\mathbb{F}_p$

For a prime p, let $\mathrm{DC}[\mathbb{F}_p]$ denote the family of all doubling-critical subsets of $\mathbb{F}_p$.

Since $\mathbb{F}_p$ has sum-free subsets of size $\frac{1}{3}p + O(1)$, we have

$$\frac{1}{3}p + O(1) \le \max\{|A| : A \in \mathrm{DC}[\mathbb{F}_p]\} \le \frac{1}{2}p + O(1),$$

and I can improve this to

$$\frac{1}{3}p + O(1) \le \max\{|A| : A \in \mathrm{DC}[\mathbb{F}_p]\} \le \frac{2}{5}p + O(1).$$

Problem

What is the largest possible size of a doubling-critical set in $\mathbb{F}_p$? (It is tempting to conjecture $\frac{1}{3}p + O(1)$.)

Problem

How about *difference*-critical sets?

Large Doubling-Critical Sets in $\mathbb{F}_p$

For a prime p, let $\mathrm{DC}[\mathbb{F}_p]$ denote the family of all doubling-critical subsets of $\mathbb{F}_p$.
Since $\mathbb{F}_p$ has sum-free subsets of size $\frac{1}{3}p + O(1)$, we have

$$\frac{1}{3}p + O(1) \le \max\{|A| \colon A \in \mathrm{DC}[\mathbb{F}_p]\} \le \frac{1}{2}p + O(1),$$

and I can improve this to

$$\frac{1}{3}p + O(1) \le \max\{|A| \colon A \in \mathrm{DC}[\mathbb{F}_p]\} \le \frac{2}{5}p + O(1).$$

Problem

What is the largest possible size of a doubling-critical set in $\mathbb{F}_p$?
(It is tempting to conjecture $\frac{1}{3}p + O(1)$.)

Problem

How about *difference*-critical sets?

Large Doubling-Critical Sets in $\mathbb{F}_p$

For a prime p, let $\mathrm{DC}[\mathbb{F}_p]$ denote the family of all doubling-critical subsets of $\mathbb{F}_p$.

Since $\mathbb{F}_p$ has sum-free subsets of size $\frac{1}{3}p + O(1)$, we have

$$\frac{1}{3}p + O(1) \le \max\{|A| \colon A \in \mathrm{DC}[\mathbb{F}_p]\} \le \frac{1}{2}p + O(1),$$

and I can improve this to

$$\frac{1}{3}p + O(1) \le \max\{|A| \colon A \in \mathrm{DC}[\mathbb{F}_p]\} \le \frac{2}{5}p + O(1).$$

Problem

What is the largest possible size of a doubling-critical set in $\mathbb{F}_p$?
(It is tempting to conjecture $\frac{1}{3}p + O(1)$.)

Problem

How about *difference*-critical sets?

Quadratic Residues are not a Perfect Difference Set

Sárközy conjectured that the set $\mathcal{R}_p$ of all quadratic residues modulo a (sufficiently large) prime p is not a sumset:

$$\mathcal{R}_p \neq A + B, \quad \min\{|A|, |B|\} > 1.$$

The case $B = A$ was settled by Shkredov: $\mathcal{R}_p \neq 2A$ ($p > 3,\ A \subseteq \mathbb{F}_p$).

For $B = -A$, Shkredov's method does not work: it is believed that $\mathcal{R}_p \cup \{0\} \neq A - A$, but we cannot prove this. A more tractable version:

Conjecture (Lev-Sonn)

For a prime $p > 13$, there does not exist a set $A \subseteq \mathbb{F}_p$ such that the differences $a' - a''$ ($a', a'' \in A,\ a' \neq a''$) list all elements of $\mathcal{R}_p$, and *every element is listed exactly once*.

With Jack Sonn, we have established a number of necessary conditions, and used them to show that in the range $13 < p < 10^{20}$, there are no "exceptional primes".

Quadratic Residues are not a Perfect Difference Set

Sárközy conjectured that the set $\mathcal{R}_p$ of all quadratic residues modulo a (sufficiently large) prime p is not a sumset:

$$\mathcal{R}_p \neq A + B, \quad \min\{|A|, |B|\} > 1.$$

The case $B = A$ was settled by Shkredov: $\mathcal{R}_p \neq 2A$ ($p > 3,\ A \subseteq \mathbb{F}_p$).

For $B = -A$, Shkredov's method does not work: it is believed that $\mathcal{R}_p \cup \{0\} \neq A - A$, but we cannot prove this. A more tractable version:

Conjecture (Lev-Sonn)

For a prime $p > 13$, there does not exist a set $A \subseteq \mathbb{F}_p$ such that the differences $a' - a''$ ($a', a'' \in A,\ a' \neq a''$) list all elements of $\mathcal{R}_p$, and *every element is listed exactly once*.

With Jack Sonn, we have established a number of necessary conditions, and used them to show that in the range $13 < p < 10^{20}$, there are no "exceptional primes".

Quadratic Residues are not a Perfect Difference Set

Sárközy conjectured that the set $\mathcal{R}_p$ of all quadratic residues modulo a (sufficiently large) prime p is not a sumset:

$$\mathcal{R}_p \neq A + B, \quad \min\{|A|, |B|\} > 1.$$

The case $B = A$ was settled by Shkredov: $\mathcal{R}_p \neq 2A$ ($p > 3,\ A \subseteq \mathbb{F}_p$).

For $B = -A$, Shkredov's method does not work: it is believed that $\mathcal{R}_p \cup \{0\} \neq A - A$, but we cannot prove this. A more tractable version:

Conjecture (Lev-Sonn)

For a prime $p > 13$, there does not exist a set $A \subseteq \mathbb{F}_p$ such that the differences $a' - a''$ ($a', a'' \in A,\ a' \neq a''$) list all elements of $\mathcal{R}_p$, and *every element is listed exactly once*.

With Jack Sonn, we have established a number of necessary conditions, and used them to show that in the range $13 < p < 10^{20}$, there are no "exceptional primes".

Quadratic Residues are not a Perfect Difference Set

Sárközy conjectured that the set $\mathcal{R}_p$ of all quadratic residues modulo a (sufficiently large) prime p is not a sumset:

$$\mathcal{R}_p \neq A + B, \quad \min\{|A|, |B|\} > 1.$$

The case $B = A$ was settled by Shkredov: $\mathcal{R}_p \neq 2A$ ($p > 3,\ A \subseteq \mathbb{F}_p$).

For $B = -A$, Shkredov's method does not work: it is believed that $\mathcal{R}_p \cup \{0\} \neq A - A$, but we cannot prove this. A more tractable version:

Conjecture (Lev-Sonn)

For a prime $p > 13$, there does not exist a set $A \subseteq \mathbb{F}_p$ such that the differences $a' - a''$ ($a', a'' \in A,\ a' \neq a''$) list all elements of $\mathcal{R}_p$, and *every element is listed exactly once*.

With Jack Sonn, we have established a number of necessary conditions, and used them to show that in the range $13 < p < 10^{20}$, there are no "exceptional primes".

Dense Perfect Difference Sets in $\mathbb{N}$

A set $A \subseteq \mathbb{N}$ is a *perfect difference set* if every element of $\mathbb{N}$ has a unique representation as a difference of two elements of A.

A construction: start with $A = \varnothing$ and at each step find the smallest $d \notin A - A$ and add to A two elements u and $u + d$, where u is large enough to avoid any element having two (or more) representations.

This yields a perfect difference set A with the counting function $A(x) \gg x^{1/3}$. On the other hand, for every perfect difference set $A \subseteq \mathbb{N}$ one has $A(x) \ll x^{1/2}$.

Problem (E. Journal of Combinatorics, 2004)

Do there exist perfect difference sets $A \subseteq \mathbb{N}$ with the counting function satisfying $A(x) \gg x^{1/2-\varepsilon}$? If not, how large can $\liminf_{x\to\infty} \frac{\ln A(x)}{\ln x}$ be?

(Nathanson and Cilleruelo (2008) constructed perfect difference sets $A \subseteq \mathbb{N}$ with the counting function $A(x) \gg x^{\sqrt{2}-1-o(1)}$.)

Dense Perfect Difference Sets in $\mathbb{N}$

A set $A \subseteq \mathbb{N}$ is a *perfect difference set* if every element of $\mathbb{N}$ has a unique representation as a difference of two elements of A.

A construction: start with $A = \varnothing$ and at each step find the smallest $d \notin A - A$ and add to A two elements u and $u + d$, where u is large enough to avoid any element having two (or more) representations.

This yields a perfect difference set A with the counting function $A(x) \gg x^{1/3}$. On the other hand, for every perfect difference set $A \subseteq \mathbb{N}$ one has $A(x) \ll x^{1/2}$.

Problem (E. Journal of Combinatorics, 2004)

Do there exist perfect difference sets $A \subseteq \mathbb{N}$ with the counting function satisfying $A(x) \gg x^{1/2-\varepsilon}$? If not, how large can $\liminf_{x\to\infty} \frac{\ln A(x)}{\ln x}$ be?

(Nathanson and Cilleruelo (2008) constructed perfect difference sets $A \subseteq \mathbb{N}$ with the counting function $A(x) \gg x^{\sqrt{2}-1-o(1)}$.)

Dense Perfect Difference Sets in $\mathbb{N}$

A set $A \subseteq \mathbb{N}$ is a *perfect difference set* if every element of $\mathbb{N}$ has a unique representation as a difference of two elements of A.

A construction: start with $A = \varnothing$ and at each step find the smallest $d \notin A - A$ and add to A two elements u and $u + d$, where u is large enough to avoid any element having two (or more) representations.

This yields a perfect difference set A with the counting function $A(x) \gg x^{1/3}$. On the other hand, for every perfect difference set $A \subseteq \mathbb{N}$ one has $A(x) \ll x^{1/2}$.

Problem (E. Journal of Combinatorics, 2004)

Do there exist perfect difference sets $A \subseteq \mathbb{N}$ with the counting function satisfying $A(x) \gg x^{1/2-\varepsilon}$? If not, how large can $\liminf_{x\to\infty} \frac{\ln A(x)}{\ln x}$ be?

(Nathanson and Cilleruelo (2008) constructed perfect difference sets $A \subseteq \mathbb{N}$ with the counting function $A(x) \gg x^{\sqrt{2}-1-o(1)}$.)

Flat-full Sets in $\mathbb{F}_2^n$

For integer $1 \le d \le n$, let $\gamma_d(n)$ denote the smallest size of a subset $A \subseteq \mathbb{F}_2^n$ such that for every $v \in \mathbb{F}_2^n$, there is a d-dimensional subspace $L < \mathbb{F}_2^n$ with $v + L \subseteq A \cup \{v\}$. That is, through every point $v \in \mathbb{F}_2^n$ passes a d-flat entirely contained in A, with the possible exception of v itself.

Equivalently, $\gamma_d(n)$ is the smallest possible size of a union of the form

$$\bigcup_{v \in \mathbb{F}_2^n} (v + L_v \setminus \{0\}),$$

for all families $\{L_v \colon v \in \mathbb{F}_2^n\}$ of d-subspaces.

For instance, $\gamma_1(n) = 2$, and it is easy to see that $\gamma_2(n) = \Theta(2^{n/3})$.

Theorem (Blokhuis-Lev, MJCNT 2013)

We have $2^{3n/8} \ll \gamma_3(n) \ll 2^{3n/7}$, with absolute implicit constants.

Problem

What is the true order of magnitude of $\gamma_3(n)$ as n grows?

Flat-full Sets in $\mathbb{F}_2^n$

For integer $1 \le d \le n$, let $\gamma_d(n)$ denote the smallest size of a subset $A \subseteq \mathbb{F}_2^n$ such that for every $v \in \mathbb{F}_2^n$, there is a d-dimensional subspace $L < \mathbb{F}_2^n$ with $v + L \subseteq A \cup \{v\}$. That is, through every point $v \in \mathbb{F}_2^n$ passes a d-flat entirely contained in A, with the possible exception of v itself.

Equivalently, $\gamma_d(n)$ is the smallest possible size of a union of the form

$$\bigcup_{v \in \mathbb{F}_2^n} (v + L_v \setminus \{0\}),$$

for all families $\{L_v : v \in \mathbb{F}_2^n\}$ of d-subspaces.

For instance, $\gamma_1(n) = 2$, and it is easy to see that $\gamma_2(n) = \Theta(2^{n/3})$.

Theorem (Blokhuis-Lev, MJCNT 2013)

We have $2^{3n/8} \ll \gamma_3(n) \ll 2^{3n/7}$, with absolute implicit constants.

Problem

What is the true order of magnitude of $\gamma_3(n)$ as n grows?

Flat-full Sets in $\mathbb{F}_2^n$

For integer $1 \le d \le n$, let $\gamma_d(n)$ denote the smallest size of a subset $A \subseteq \mathbb{F}_2^n$ such that for every $v \in \mathbb{F}_2^n$, there is a d-dimensional subspace $L < \mathbb{F}_2^n$ with $v + L \subseteq A \cup \{v\}$. That is, through every point $v \in \mathbb{F}_2^n$ passes a d-flat entirely contained in A, with the possible exception of v itself.

Equivalently, $\gamma_d(n)$ is the smallest possible size of a union of the form

$$\bigcup_{v \in \mathbb{F}_2^n} (v + L_v \setminus \{0\}),$$

for all families $\{L_v \colon v \in \mathbb{F}_2^n\}$ of d-subspaces.

For instance, $\gamma_1(n) = 2$, and it is easy to see that $\gamma_2(n) = \Theta(2^{n/3})$.

Theorem (Blokhuis-Lev, MJCNT 2013)

We have $2^{3n/8} \ll \gamma_3(n) \ll 2^{3n/7}$, with absolute implicit constants.

Problem

What is the true order of magnitude of $\gamma_3(n)$ as n grows?

Small Sums of Roots of Unity

In 1975, Gerry Myerson defined $f(n,q)$ to be the smallest possible sum of n roots of unity of degree q (repeated summands allowed), and obtained some estimates for q even.

For q prime and repetitions *forbidden*, we are seeking lower bounds for

$$S_A := \sum_{a\in A} e^{2\pi ia/p}, \quad A \subseteq \mathbb{F}_p$$

in terms of p and $n := |A|$.

Theorem (Konyagin-Lev, INTEGERS 2000)

For any set $A \subseteq \mathbb{F}_p$ with $n := |A| \in [3, p-1]$, we have $|S_A| > n^{-\frac{p-1}{4}}$.
On the other hand, for any $n = 2^k < p/20$, there exists $A \subseteq \mathbb{F}_p$ with $|A| = n$ such that $|S_A| < n^{-c\log p}$, with an absolute constant $c > 0$.

Problem

Narrow the gap between the estimates. (The lower bound $n^{-\frac{p-1}{4}}$ seems particularly unsatisfactory.)

Small Sums of Roots of Unity

In 1975, Gerry Myerson defined $f(n,q)$ to be the smallest possible sum of n roots of unity of degree q (repeated summands allowed), and obtained some estimates for q even.

For q prime and repetitions *forbidden*, we are seeking lower bounds for

$$S_A := \sum_{a\in A} e^{2\pi i a/p}, \quad A \subseteq \mathbb{F}_p$$

in terms of p and $n := |A|$.

Theorem (Konyagin-Lev, INTEGERS 2000)

For any set $A \subseteq \mathbb{F}_p$ with $n := |A| \in [3, p-1]$, we have $|S_A| > n^{-\frac{p-1}{4}}$.
On the other hand, for any $n = 2^k < p/20$, there exists $A \subseteq \mathbb{F}_p$ with $|A| = n$ such that $|S_A| < n^{-c\log p}$, with an absolute constant $c > 0$.

Problem

Narrow the gap between the estimates. (The lower bound $n^{-\frac{p-1}{4}}$ seems particularly unsatisfactory.)

Small Sums of Roots of Unity

In 1975, Gerry Myerson defined $f(n, q)$ to be the smallest possible sum of n roots of unity of degree q (repeated summands allowed), and obtained some estimates for q even.

For q prime and repetitions *forbidden*, we are seeking lower bounds for

$$S_A := \sum_{a \in A} e^{2\pi i a/p}, \quad A \subseteq \mathbb{F}_p$$

in terms of p and $n := |A|$.

Theorem (Konyagin-Lev, INTEGERS 2000)

For any set $A \subseteq \mathbb{F}_p$ with $n := |A| \in [3, p-1]$, we have $|S_A| > n^{-\frac{p-1}{4}}$.
On the other hand, for any $n = 2^k < p/20$, there exists $A \subseteq \mathbb{F}_p$ with $|A| = n$ such that $|S_A| < n^{-c \log p}$, with an absolute constant $c > 0$.

Problem

Narrow the gap between the estimates. (The lower bound $n^{-\frac{p-1}{4}}$ seems particularly unsatisfactory.)

Popular Differences in $\mathbb{F}_p$

For a finite subset A and an element b of an abelian group G, let

$$\Delta_A(b) := |(A+b) \setminus A|,$$

the Erdős – Heilbronn (1964) / Olson (1968) function. Basic properties:

- non-vanishing: $\Delta_A(0) = 0$, and $\Delta_A(b) \geq 1$ unless $A + b = A$;
- symmetry: $\Delta_A(-b) = \Delta_A(b)$;
- sub-additivity: $\Delta_A(b_1 + \cdots + b_k) \leq \Delta_A(b_1) + \cdots + \Delta_A(b_k)$.

In applications, one needs to know that Δ_A does not assume too many small values; that is, any $B \subseteq G$ contains some $b \in B$ with $\Delta_A(b)$ large.

Theorem (Konyagin-Lev, Israel J. Math. 2010)

For all (finite) $A \subseteq \mathbb{Z}$ and $B \subseteq \mathbb{N}$ with $|B| < c|A|/\log|A|$, there exists $b \in B$ with $\Delta_A(b) \geq |B|$.

(The logarithmic factor cannot be dropped!)

What is the $\mathbb{F}_p$-version of this result?

Popular Differences in $\mathbb{F}_p$

For a finite subset A and an element b of an abelian group G, let

$$\Delta_A(b) := |(A+b) \setminus A|,$$

the Erdős – Heilbronn (1964) / Olson (1968) function. Basic properties:

- non-vanishing: $\Delta_A(0) = 0$, and $\Delta_A(b) \geq 1$ unless $A + b = A$;
- symmetry: $\Delta_A(-b) = \Delta_A(b)$;
- sub-additivity: $\Delta_A(b_1 + \cdots + b_k) \leq \Delta_A(b_1) + \cdots + \Delta_A(b_k)$.

In applications, one needs to know that Δ_A does not assume too many small values; that is, any $B \subseteq G$ contains some $b \in B$ with $\Delta_A(b)$ large.

Theorem (Konyagin-Lev, Israel J. Math. 2010)

For all (finite) $A \subseteq \mathbb{Z}$ and $B \subseteq \mathbb{N}$ with $|B| < c|A|/\log|A|$, there exists $b \in B$ with $\Delta_A(b) \geq |B|$.

(The logarithmic factor cannot be dropped!)

What is the $\mathbb{F}_p$-version of this result?

Popular Differences in $\mathbb{F}_p$

For a finite subset A and an element b of an abelian group G, let

$$\Delta_A(b) := |(A+b) \setminus A|,$$

the Erdős – Heilbronn (1964) / Olson (1968) function. Basic properties:

- non-vanishing: $\Delta_A(0) = 0$, and $\Delta_A(b) \geq 1$ unless $A + b = A$;
- symmetry: $\Delta_A(-b) = \Delta_A(b)$;
- sub-additivity: $\Delta_A(b_1 + \cdots + b_k) \leq \Delta_A(b_1) + \cdots + \Delta_A(b_k)$.

In applications, one needs to know that Δ_A does not assume too many small values; that is, any $B \subseteq G$ contains some $b \in B$ with $\Delta_A(b)$ large.

Theorem (Konyagin-Lev, Israel J. Math. 2010)

For all (finite) $A \subseteq \mathbb{Z}$ and $B \subseteq \mathbb{N}$ with $|B| < c|A|/\log|A|$, there exists $b \in B$ with $\Delta_A(b) \geq |B|$.

(The logarithmic factor cannot be dropped!)

What is the $\mathbb{F}_p$-version of this result?

Popular Differences in $\mathbb{F}_p$

For a finite subset A and an element b of an abelian group G, let

$$\Delta_A(b) := |(A+b) \setminus A|,$$

the Erdős – Heilbronn (1964) / Olson (1968) function. Basic properties:

- non-vanishing: $\Delta_A(0) = 0$, and $\Delta_A(b) \geq 1$ unless $A + b = A$;
- symmetry: $\Delta_A(-b) = \Delta_A(b)$;
- sub-additivity: $\Delta_A(b_1 + \cdots + b_k) \leq \Delta_A(b_1) + \cdots + \Delta_A(b_k)$.

In applications, one needs to know that Δ_A does not assume too many small values; that is, any $B \subseteq G$ contains some $b \in B$ with $\Delta_A(b)$ large.

Theorem (Konyagin-Lev, Israel J. Math. 2010)

For all (finite) $A \subseteq \mathbb{Z}$ and $B \subseteq \mathbb{N}$ with $|B| < c|A|/\log|A|$, there exists $b \in B$ with $\Delta_A(b) \geq |B|$.

(The logarithmic factor cannot be dropped!)

What is the $\mathbb{F}_p$-version of this result?

Popular Differences in $\mathbb{F}_p$ (Continued)

Theorem (Lev, J. Number Theory 2011)

For all $A, B \subseteq \mathbb{F}_p$ with $B \cap (-B) = \varnothing$ and $|B| < \min\{c|A|/\log|A|, \sqrt{p/8}\}$, there exists $b \in B$ with $\Delta_A(b) \geq |B|$.

The logarithmic factor cannot be dropped, the term $\sqrt{p/8}$ seems a technical annoyance.

Problem

Determine whether the $\sqrt{p/8}$–term can be dropped.

Popular Differences in $\mathbb{F}_p$ (Continued)

Theorem (Lev, J. Number Theory 2011)

For all $A, B \subseteq \mathbb{F}_p$ with $B \cap (-B) = \varnothing$ and $|B| < \min\{c|A|/\log|A|, \sqrt{p/8}\}$, there exists $b \in B$ with $\Delta_A(b) \geq |B|$.

The logarithmic factor cannot be dropped, the term $\sqrt{p/8}$ seems a technical annoyance.

Problem

Determine whether the $\sqrt{p/8}$–term can be dropped.

Theorem

Suppose that A, B, and C are subsets of the finite abelian group G. If $A+B+C \neq G$, then

$$|A|+|B|+|C|+|A+B+C| \leq 2|G|.$$

An "Elementary" Kneser's Theorem

Theorem

Suppose that A, B, and C are subsets of the finite abelian group G. If $A + B + C \neq G$, then

$$|A| + |B| + |C| + |A + B + C| \leq 2|G|.$$

This theorem is completely equivalent to Kneser's Theorem! (Some adjustments are to be made if G is infinite.)

Besides being remarkably symmetric, this restatement avoids the notion of a *period*, absolutely vital in the standard formulation of KT.

Deducing "Elementary KT" from the "Standard KT"

Suppose that $A + B + C \neq G$. If H is the period of $A + B + C$, then

$$|G| - |H| \geq |A + B + C| \geq |A| + |B| + |C| - 2|H|$$

whence

$$|A| + |B| + |C| + |A + B + C| \leq (|G| + |H|) + (|G| - |H|) = 2|G|.$$

An "Elementary" Kneser's Theorem

Theorem

Suppose that A, B, and C are subsets of the finite abelian group G. If $A + B + C \neq G$, then

$$|A| + |B| + |C| + |A + B + C| \leq 2|G|.$$

This theorem is completely equivalent to Kneser's Theorem! (Some adjustments are to be made if G is infinite.)

Besides being remarkably symmetric, this restatement avoids the notion of a *period*, absolutely vital in the standard formulation of KT.

Deducing "Elementary KT" from the "Standard KT"

Suppose that $A + B + C \neq G$. If H is the period of $A + B + C$, then

$$|G| - |H| \geq |A + B + C| \geq |A| + |B| + |C| - 2|H|$$

whence

$$|A| + |B| + |C| + |A + B + C| \leq \big(|G| + |H|\big) + \big(|G| - |H|\big) = 2|G|.$$

An "Elementary" Kneser's Theorem (Continued)

The "Elementary Kneser's Theorem"

Suppose that A, B, and C are subsets of the finite abelian group G. If $A+B+C \neq G$, then

$$|A|+|B|+|C|+|A+B+C| \leq 2|G|.$$

Deducing "Standard KT" from the "Elementary KT"

Given $A, B \subseteq G$, let $C := -\overline{A+B}$. Then $A+B+C = G \setminus H$, where H is the period of $A+B$ (easy). Hence by the EKT,

$$2|G| \geq |A|+|B|+|\overline{A+B}|+|G \setminus H|,$$

implying

$$|A+B| \geq |A|+|B|-|H|.$$

Problem

Give the "Elementary Kneser's Theorem" an independent, simple proof (preferably not appealing to the notion of a period).

An "Elementary" Kneser's Theorem (Continued)

The "Elementary Kneser's Theorem"

Suppose that A, B, and C are subsets of the finite abelian group G. If $A + B + C \neq G$, then

$$|A| + |B| + |C| + |A + B + C| \leq 2|G|.$$

Deducing "Standard KT" from the "Elementary KT"

Given $A, B \subseteq G$, let $C := -\overline{A + B}$. Then $A + B + C = G \setminus H$, where H is the period of $A + B$ (easy). Hence by the EKT,

$$2|G| \geq |A| + |B| + |\overline{A + B}| + |G \setminus H|,$$

implying

$$|A + B| \geq |A| + |B| - |H|.$$

Problem

Give the "Elementary Kneser's Theorem" an independent, simple proof (preferably not appealing to the notion of a period).

Thank you!