Additive bases in groups

Thái Hoàng Lê

University of Mississippi

October 27, 2019

Additive bases in $\mathbf{N}$

- Let $(G, +)$ be an infinite commutative semigroup. If A is a subset of G, we define

$$hA = \{a_1 + \cdots + a_h : a_1, \ldots, a_h \in A\}.$$

Additive bases in $\mathbf{N}$

- Let $(G, +)$ be an infinite commutative semigroup. If A is a subset of G, we define

$$hA = \{a_1 + \cdots + a_h : a_1, \ldots, a_h \in A\}.$$

- For two sets X, Y, we write $X \sim Y$ if their symmetric difference $(X \setminus Y) \cup (Y \setminus X)$ is finite.

- We say A is a basis of order at most h if $hA \sim G$. In other words, all but finitely many elements of G can be written as a sum of exactly h elements of A.

- We say A is a basis of order at most h if $hA \sim G$. In other words, all but finitely many elements of G can be written as a sum of exactly h elements of A.

- If h is the smallest such number, we say A is a basis of order h and write

$$\mathrm{ord}_G^*(A) = h.$$

- We say A is a basis of order at most h if $hA \sim G$. In other words, all but finitely many elements of G can be written as a sum of exactly h elements of A.

- If h is the smallest such number, we say A is a basis of order h and write
$$\mathrm{ord}^*_G(A) = h.$$

- If A is not a basis, we define $\mathrm{ord}^*_G(A) = \infty$.

From specific bases...

Classical additive number theory deals with specific bases of $\mathbf{N}$ (e.g. the squares, k-th powers, the primes).

From specific bases...

Classical additive number theory deals with specific bases of **N** (e.g. the squares, *k*-th powers, the primes).

Examples:

- If $A = \{n^2 : n \geq 0\}$, then $\mathrm{ord}^*_{\mathbf{N}}(A) = 4$ (Lagrange's theorem).

From specific bases...

Classical additive number theory deals with specific bases of $\mathbf{N}$ (e.g. the squares, k-th powers, the primes).

Examples:

- If $A = \{n^2 : n \geq 0\}$, then $\mathrm{ord}^*_{\mathbf{N}}(A) = 4$ (Lagrange's theorem).
- If $A = \{n^k : n \geq 0\}$, then $\mathrm{ord}^*_{\mathbf{N}}(A) = G(k) \leq (k + o(1)) \log k$ (Waring's problem).

From specific bases...

Classical additive number theory deals with specific bases of $\mathbf{N}$ (e.g. the squares, k-th powers, the primes).

Examples:

- If $A = \{n^2 : n \geq 0\}$, then $\mathrm{ord}^*_{\mathbf{N}}(A) = 4$ (Lagrange's theorem).
- If $A = \{n^k : n \geq 0\}$, then $\mathrm{ord}^*_{\mathbf{N}}(A) = G(k) \leq (k + o(1)) \log k$ (Waring's problem).
- If A is the set of primes, then $\mathrm{ord}^*_{\mathbf{N}}(A) \leq 4$ (Goldbach's conjecture: $\mathrm{ord}^*_{\mathbf{N}}(A) = 3$).

... to generic bases.

Combinatorial number theory deals with properties of a generic basis.

... to generic bases.

Combinatorial number theory deals with properties of a generic basis.

Schnirelmann's theorem (1930): If $A \subset \mathbf{N}$ has Shnirelmann density

$$\sigma(A) := \inf_{n \in \mathbf{Z}^+} \frac{|A \cap [1, n]|}{n} > 0,$$

and $0 \in A$, then $\operatorname{ord}^*_{\mathbf{N}} A < \infty$.

Removing elements from a basis

Erdős-Graham (1980) initiated the following research direction: If we remove one element from a basis, then is the new set still a basis? If yes, then what can we say about its order?

Removing elements from a basis

Erdős-Graham (1980) initiated the following research direction: If we remove one element from a basis, then is the new set still a basis? If yes, then what can we say about its order?

The following questions have been primarily studied in $\mathbf{N}$, but they also makes sense in any semigroups G.

Let A be a basis of order $\leq h$ of G (i.e. $hA \sim G$) and $a \in A$.

1. (Erdős-Graham 1980) When is $A \setminus \{a\}$ still a basis (of a possibly different order)?

Let A be a basis of order $\leq h$ of G (i.e. $hA \sim G$) and $a \in A$.

1. (Erdős-Graham 1980) When is $A \setminus \{a\}$ still a basis (of a possibly different order)?
2. (Erdős-Graham 1980) If $A \setminus \{a\}$ is still a basis, then is its order bounded in terms of h?

Let A be a basis of order $\leq h$ of G (i.e. $hA \sim G$) and $a \in A$.

1. (Erdős-Graham 1980) When is $A \setminus \{a\}$ still a basis (of a possibly different order)?
2. (Erdős-Graham 1980) If $A \setminus \{a\}$ is still a basis, then is its order bounded in terms of h?
3. (Grekos 1982) How many "bad" elements $a \in A$ are there?

Let A be a basis of order $\leq h$ of G (i.e. $hA \sim G$) and $a \in A$.

1. (Erdős-Graham 1980) When is $A \setminus \{a\}$ still a basis (of a possibly different order)?
2. (Erdős-Graham 1980) If $A \setminus \{a\}$ is still a basis, then is its order bounded in terms of h?
3. (Grekos 1982) How many “bad” elements $a \in A$ are there?
4. (Grekos 1997) If $A \setminus \{a\}$ is still a basis, then what is the “typical” order of the new basis?

Let A be a basis of order $\leq h$ of G (i.e. $hA \sim G$) and $a \in A$.

1. (Erdős-Graham 1980) When is $A \setminus \{a\}$ still a basis (of a possibly different order)?
2. (Erdős-Graham 1980) If $A \setminus \{a\}$ is still a basis, then is its order bounded in terms of h?
3. (Grekos 1982) How many "bad" elements $a \in A$ are there?
4. (Grekos 1997) If $A \setminus \{a\}$ is still a basis, then what is the "typical" order of the new basis?
5. (Nathanson 1982) What if instead of removing an element, we remove a subset $F \subset A$ of size $k \geq 1$?

In joint works with V. Lambert and A. Plagne, and P.-Y. Bienvenu and B. Girard, we study these questions when G is a group.

In joint works with V. Lambert and A. Plagne, and P.-Y. Bienvenu and B. Girard, we study these questions when G is a group.

Why groups?

- Groups have more structures and are easier to work with.

In joint works with V. Lambert and A. Plagne, and P.-Y. Bienvenu and B. Girard, we study these questions when G is a group.

Why groups?

- Groups have more structures and are easier to work with.
- Almost all results and arguments in **N** can be repeated verbatim in **Z**.

In joint works with V. Lambert and A. Plagne, and P.-Y. Bienvenu and B. Girard, we study these questions when G is a group.

Why groups?

- Groups have more structures and are easier to work with.
- Almost all results and arguments in $\mathbf{N}$ can be repeated verbatim in $\mathbf{Z}$.
- The problem makes sense, since in any group and for any h, there exists a basis with order h.

In joint works with V. Lambert and A. Plagne, and P.-Y. Bienvenu and B. Girard, we study these questions when G is a group.

Why groups?

- Groups have more structures and are easier to work with.
- Almost all results and arguments in $\mathbf{N}$ can be repeated verbatim in $\mathbf{Z}$.
- The problem makes sense, since in any group and for any h, there exists a basis with order h.

In joint works with V. Lambert and A. Plagne, and P.-Y. Bienvenu and B. Girard, we study these questions when G is a group.

Why groups?

- Groups have more structures and are easier to work with.
- Almost all results and arguments in $\mathbf{N}$ can be repeated verbatim in $\mathbf{Z}$.
- The problem makes sense, since in any group and for any h, there exists a basis with order h.

Existing techniques are very specific to $\mathbf{N}$ (and $\mathbf{Z}$). If one wants to prove results for general groups, new ideas are required.

In joint works with V. Lambert and A. Plagne, and P.-Y. Bienvenu and B. Girard, we study these questions when G is a group.

Why groups?

- Groups have more structures and are easier to work with.
- Almost all results and arguments in $\mathbf{N}$ can be repeated verbatim in $\mathbf{Z}$.
- The problem makes sense, since in any group and for any h, there exists a basis with order h.

Existing techniques are very specific to $\mathbf{N}$ (and $\mathbf{Z}$). If one wants to prove results for general groups, new ideas are required.

From now on, G is an infinite abelian group.

The Erdős-Graham criterion

Suppose $hA \sim G$. A finite subset $F \subset A$ is said to be regular if $A \setminus F$ is still a basis, and exceptional otherwise.

The Erdős-Graham criterion

Suppose $hA \sim G$. A finite subset $F \subset A$ is said to be regular if $A \setminus F$ is still a basis, and exceptional otherwise.

In particular, an element $a \in A$ is regular if $A \setminus \{a\}$ is still a basis, and exceptional otherwise.

The Erdős-Graham criterion

Suppose $hA \sim G$. A finite subset $F \subset A$ is said to be regular if $A \setminus F$ is still a basis, and exceptional otherwise.

In particular, an element $a \in A$ is regular if $A \setminus \{a\}$ is still a basis, and exceptional otherwise.

Theorem (Erdős-Graham 1980)

Let $A \subset \mathbf{N}$ be a basis of $\mathbf{N}$ and $a \in A$. Then a is regular (i.e., $A \setminus \{a\}$ is still a basis) if and only if

$$\gcd(A \setminus \{a\} - A \setminus \{a\}) = 1.$$

Theorem (Erdős-Graham 1980)

Let A be a basis of $\mathbf{N}$ and $a \in A$. Then a is regular (i.e., $A \setminus \{a\}$ is still a basis) if and only if

$$\gcd(A \setminus \{a\} - A \setminus \{a\}) = 1.$$

Theorem (Erdős-Graham 1980)

Let A be a basis of $\mathbf{N}$ and $a \in A$. Then a is regular (i.e., $A \setminus \{a\}$ is still a basis) if and only if

$$\gcd(A \setminus \{a\} - A \setminus \{a\}) = 1.$$

Theorem (Erdős-Graham 1980)

Let A be a basis of $\mathbf{N}$ and $a \in A$. Then a is regular (i.e., $A \setminus \{a\}$ is still a basis) if and only if

$$\gcd(A \setminus \{a\} - A \setminus \{a\}) = 1.$$

Theorem (Bienvenu-Girard-L. 2019+)

Let A be a basis of G and $F \subset A$ is a finite subset. Then F is regular (i.e., $A \setminus F$ is still a basis) if and only if

$$\langle A \setminus F - A \setminus F \rangle = G.$$

Theorem (Bienvenu-Girard-L. 2019+)

Let A be a basis of G and $F \subset A$ is a finite subset. Then F is regular (i.e., $A \setminus F$ is still a basis) if and only if

$$\langle A \setminus F - A \setminus F \rangle = G.$$

Theorem (Bienvenu-Girard-L. 2019+)

Let A be a basis of G and $F \subset A$ is a finite subset. Then F is regular (i.e., $A \setminus F$ is still a basis) if and only if

$$\langle A \setminus F - A \setminus F \rangle = G.$$

Theorem (Bienvenu-Girard-L. 2019+)

Let A be a basis of G and $F \subset A$ is a finite subset. Then F is regular (i.e., $A \setminus F$ is still a basis) if and only if

$$\langle A \setminus F - A \setminus F \rangle = G.$$

- Previous results: Nash-Nathanson 1985 ($G = \mathbf{N}$, F arbitrary), Lambert-L.-Plagne 2017 (G arbitrary, $F = \{a\}$).

Theorem (Bienvenu-Girard-L. 2019+)

Let A be a basis of G and $F \subset A$ is a finite subset. Then F is regular (i.e., $A \setminus F$ is still a basis) if and only if

$$\langle A \setminus F - A \setminus F \rangle = G.$$

- Previous results: Nash-Nathanson 1985 ($G = \mathbf{N}$, F arbitrary), Lambert-L.-Plagne 2017 (G arbitrary, $F = \{a\}$).
- The "only if" direction is easy to see: Suppose for a contradiction that

$$H := \langle A \setminus F - A \setminus F \rangle \lneq G.$$

Theorem (Bienvenu-Girard-L. 2019+)

Let A be a basis of G and $F \subset A$ is a finite subset. Then F is regular (i.e., $A \setminus F$ is still a basis) if and only if

$$\langle A \setminus F - A \setminus F \rangle = G.$$

- Previous results: Nash-Nathanson 1985 ($G = \mathbf{N}$, F arbitrary), Lambert-L.-Plagne 2017 (G arbitrary, $F = \{a\}$).
- The "only if" direction is easy to see: Suppose for a contradiction that

$$H := \langle A \setminus F - A \setminus F \rangle \lneq G.$$

Theorem (Bienvenu-Girard-L. 2019+)

Let A be a basis of G and $F \subset A$ is a finite subset. Then F is regular (i.e., $A \setminus F$ is still a basis) if and only if

$$\langle A \setminus F - A \setminus F \rangle = G.$$

- Previous results: Nash-Nathanson 1985 ($G = \mathbf{N}$, F arbitrary), Lambert-L.-Plagne 2017 (G arbitrary, $F = \{a\}$).
- The "only if" direction is easy to see: Suppose for a contradiction that

  $$H := \langle A \setminus F - A \setminus F \rangle \lneq G.$$

  Then for any $a, a' \in A \setminus F$, a and a' lie in the same coset of H.

Theorem (Bienvenu-Girard-L. 2019+)

Let A be a basis of G and $F \subset A$ is a finite subset. Then F is regular (i.e., $A \setminus F$ is still a basis) if and only if

$$\langle A \setminus F - A \setminus F \rangle = G.$$

- Previous results: Nash-Nathanson 1985 ($G = \mathbf{N}$, F arbitrary), Lambert-L.-Plagne 2017 (G arbitrary, $F = \{a\}$).
- The "only if" direction is easy to see: Suppose for a contradiction that

  $$H := \langle A \setminus F - A \setminus F \rangle \lneq G.$$

  Then for any $a, a' \in A \setminus F$, a and a' lie in the same coset of H. Hence, for any s, $s(A \setminus F)$ lies in a coset of H, and $A \setminus F$ cannot be a basis of order s.

Theorem (Bienvenu-Girard-L. 2019+)

Let A be a basis of G and $F \subset A$ is a finite subset. Then F is regular (i.e., $A \setminus F$ is still a basis) if and only if

$$\langle A \setminus F - A \setminus F \rangle = G.$$

- Previous results: Nash-Nathanson 1985 ($G = \mathbf{N}$, F arbitrary), Lambert-L.-Plagne 2017 (G arbitrary, $F = \{a\}$).
- The "only if" direction is easy to see: Suppose for a contradiction that
  $$H := \langle A \setminus F - A \setminus F \rangle \lneq G.$$
  Then for any $a, a' \in A \setminus F$, a and a' lie in the same coset of H. Hence, for any s, $s(A \setminus F)$ lies in a coset of H, and $A \setminus F$ cannot be a basis of order s.
- This criterion is not true when F is infinite.

The maximum order of the new basis

Define

$$X_G(h) = \max_{hA \sim \mathbf{N}} \max\{\mathrm{ord}^*(A \setminus \{a\}) : A \setminus \{a\} \text{ is still a basis}\}.$$

The maximum order of the new basis

Define

$$X_G(h) = \max_{hA \sim \mathbf{N}} \max\{\mathrm{ord}^*(A \setminus \{a\}) : A \setminus \{a\} \text{ is still a basis}\}.$$

Erdős and Graham proved that

$$(1/4 + o(1))h^2 \leq X_{\mathbf{N}}(h) \leq (5/4 + o(1))h^2.$$

The maximum order of the new basis

Define

$$X_G(h) = \max_{hA \sim \mathbf{N}} \max\{\mathrm{ord}^*(A \setminus \{a\}) : A \setminus \{a\} \text{ is still a basis}\}.$$

Erdős and Graham proved that

$$(1/4 + o(1))h^2 \leq X_{\mathbf{N}}(h) \leq (5/4 + o(1))h^2.$$

The current best bounds are

$$(1/3 + o(1))h^2 \leq X_{\mathbf{N}}(h) \leq (1/2 + o(1))h^2.$$

and the exact asymptotic for $X_{\mathbf{N}}(h)$ is unknown.

By adapting Erdős-Graham's argument, Lambert-L.-Plagne (2017) proved that

$$X_G(h) = O_G(h^2)$$

for various groups G, including $\mathbf{R}, \mathbf{Q}, \mathbf{Z}^d, \mathbf{Z}_p$.

By adapting Erdős-Graham's argument, Lambert-L.-Plagne (2017) proved that

$$X_G(h) = O_G(h^2)$$

for various groups G, including $\mathbf{R}, \mathbf{Q}, \mathbf{Z}^d, \mathbf{Z}_p$.

We also proved that $X_G(2) \leq 5$ and $X_G(3) \leq 17$ for any G.

By adapting Erdős-Graham's argument, Lambert-L.-Plagne (2017) proved that

$$X_G(h) = O_G(h^2)$$

for various groups G, including $\mathbf{R}, \mathbf{Q}, \mathbf{Z}^d, \mathbf{Z}_p$.

We also proved that $X_G(2) \leq 5$ and $X_G(3) \leq 17$ for any G. However, it was not known if for any G and h, $X_G(h) < \infty$, not to mention if $X_G(h)$ can be bounded in terms of h alone.

By adapting Erdős-Graham's argument, Lambert-L.-Plagne (2017) proved that

$$X_G(h) = O_G(h^2)$$

for various groups G, including $\mathbf{R}, \mathbf{Q}, \mathbf{Z}^d, \mathbf{Z}_p$.

We also proved that $X_G(2) \leq 5$ and $X_G(3) \leq 17$ for any G. However, it was not known if for any G and h, $X_G(h) < \infty$, not to mention if $X_G(h)$ can be bounded in terms of h alone.

By using the notion of invariant means from functional analysis, Bienvenu-Girard-L. (2019+) prove that

By adapting Erdős-Graham's argument, Lambert-L.-Plagne (2017) proved that

$$X_G(h) = O_G(h^2)$$

for various groups G, including $\mathbf{R}, \mathbf{Q}, \mathbf{Z}^d, \mathbf{Z}_p$.

We also proved that $X_G(2) \leq 5$ and $X_G(3) \leq 17$ for any G. However, it was not known if for any G and h, $X_G(h) < \infty$, not to mention if $X_G(h)$ can be bounded in terms of h alone.

By using the notion of invariant means from functional analysis, Bienvenu-Girard-L. (2019+) prove that

Theorem

For any group G and h, we have $X_G(h) \leq h^3 - h + 1$.

By adapting Erdős-Graham's argument, Lambert-L.-Plagne (2017) proved that

$$X_G(h) = O_G(h^2)$$

for various groups G, including $\mathbf{R}, \mathbf{Q}, \mathbf{Z}^d, \mathbf{Z}_p$.

We also proved that $X_G(2) \le 5$ and $X_G(3) \le 17$ for any G. However, it was not known if for any G and h, $X_G(h) < \infty$, not to mention if $X_G(h)$ can be bounded in terms of h alone.

By using the notion of invariant means from functional analysis, Bienvenu-Girard-L. (2019+) prove that

Theorem

For any group G and h, we have $X_G(h) \le h^3 - h + 1$.

By adapting Erdős-Graham's argument, Lambert-L.-Plagne (2017) proved that

$$X_G(h) = O_G(h^2)$$

for various groups G, including $\mathbf{R}, \mathbf{Q}, \mathbf{Z}^d, \mathbf{Z}_p$.

We also proved that $X_G(2) \leq 5$ and $X_G(3) \leq 17$ for any G. However, it was not known if for any G and h, $X_G(h) < \infty$, not to mention if $X_G(h)$ can be bounded in terms of h alone.

By using the notion of invariant means from functional analysis, Bienvenu-Girard-L. (2019+) prove that

Theorem

For any group G and h, we have $X_G(h) \leq h^3 - h + 1$.

The truth may be that $X_G(h) = O(h^2)$.

An invariant mean d on G is a finitely-additive translation-invariant probability measure on G, i.e.

An invariant mean d on G is a finitely-additive translation-invariant probability measure on G, i.e.

1. if $A_1, \ldots, A_n \subset G$ are disjoint, then

$$d\left(\cup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} d(A_i),$$

An invariant mean d on G is a finitely-additive translation-invariant probability measure on G, i.e.

1. if $A_1, \ldots, A_n \subset G$ are disjoint, then

$$d\left(\cup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} d(A_i),$$

2. for all $A \subset G$ and $x \in G$, we have $d(x + A) = d(A)$,

An invariant mean d on G is a finitely-additive translation-invariant probability measure on G, i.e.

1. if $A_1, \dots, A_n \subset G$ are disjoint, then
$$d\left(\cup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} d(A_i),$$
2. for all $A \subset G$ and $x \in G$, we have $d(x + A) = d(A)$,
3. $d(G) = 1$.

An invariant mean d on G is a finitely-additive translation-invariant probability measure on G, i.e.

1. if $A_1, \ldots, A_n \subset G$ are disjoint, then
$$d\left(\cup_{i=1}^n A_i\right) = \sum_{i=1}^n d(A_i),$$
2. for all $A \subset G$ and $x \in G$, we have $d(x + A) = d(A)$,
3. $d(G) = 1$.

An invariant mean d on G is a finitely-additive translation-invariant probability measure on G, i.e.

1. if $A_1, \dots, A_n \subset G$ are disjoint, then
$$d\left(\cup_{i=1}^n A_i\right) = \sum_{i=1}^n d(A_i),$$
2. for all $A \subset G$ and $x \in G$, we have $d(x + A) = d(A)$,
3. $d(G) = 1$.

It is well known that such measures exist (in other words, all abelian groups are amenable).

An invariant mean d on G is a finitely-additive translation-invariant probability measure on G, i.e.

1. if $A_1, \ldots, A_n \subset G$ are disjoint, then

$$d\left(\cup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} d(A_i),$$

2. for all $A \subset G$ and $x \in G$, we have $d(x + A) = d(A)$,
3. $d(G) = 1$.

It is well known that such measures exist (in other words, all abelian groups are amenable).

An invariant mean d on G is a finitely-additive translation-invariant probability measure on G, i.e.

1. if $A_1, \ldots, A_n \subset G$ are disjoint, then
$$d\left(\cup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} d(A_i),$$
2. for all $A \subset G$ and $x \in G$, we have $d(x + A) = d(A)$,
3. $d(G) = 1$.

It is well known that such measures exist (in other words, all abelian groups are amenable).

However, even in $\mathbf{Z}$, the construction of an invariant mean is not explicit, and requires the axiom of choice (e.g. ultrafilters or the Hahn-Banach theorem).

Recall that

$$X_G(h) = \max_{hA \sim G} \max\{\mathrm{ord}^*(A \setminus \{a\}) : A \setminus \{a\} \text{ is still a basis}\}.$$

Recall that

$$X_G(h) = \max_{hA \sim G} \max\{\mathrm{ord}^*(A \setminus \{a\}) : A \setminus \{a\} \text{ is still a basis}\}.$$

We define

$$X_G(h,k) = \max_{hA \sim G} \max\{\mathrm{ord}^*(A \setminus F) : F \subset A, |F| = k, A \setminus F \text{ is still a basis}\}.$$

Theorem (Nash-Nathanson 1985, Nathanson 1984)

For fixed k and h $\to \infty$, we have

$$X_{\mathbf{N}}(h,k) \ll_k h^{k+1}$$

and also

$$X_{\mathbf{N}}(h,k) \gg_k h^{k+1}.$$

Again, the proof is very specific to **N**. Using invariant means, we show that

Theorem (Nash-Nathanson 1985, Nathanson 1984)

For fixed k and h $\to \infty$, we have

$$X_{\mathbf{N}}(h,k) \ll_k h^{k+1}$$

and also

$$X_{\mathbf{N}}(h,k) \gg_k h^{k+1}.$$

Again, the proof is very specific to **N**. Using invariant means, we show that

Theorem (Bienvenu-Girard-L. (2019+))

For any group G, fixed k and h $\to \infty$, we have

$$X_G(h,k) \ll_k h^{2k+1}$$

Theorem (Nash-Nathanson 1985, Nathanson 1984)

For fixed k and $h \to \infty$, we have

$$X_{\mathbf{N}}(h,k) \ll_k h^{k+1}$$

and also

$$X_{\mathbf{N}}(h,k) \gg_k h^{k+1}.$$

Again, the proof is very specific to **N**. Using invariant means, we show that

Theorem (Bienvenu-Girard-L. (2019+))

For any group G, fixed k and $h \to \infty$, we have

$$X_G(h,k) \ll_k h^{2k+1}$$

Theorem (Nash-Nathanson 1985, Nathanson 1984)

For fixed k and h $\to \infty$, we have

$$X_{\mathbf{N}}(h,k) \ll_k h^{k+1}$$

and also

$$X_{\mathbf{N}}(h,k) \gg_k h^{k+1}.$$

Again, the proof is very specific to **N**. Using invariant means, we show that

Theorem (Bienvenu-Girard-L. (2019+))

For any group G, fixed k and h $\to \infty$, we have

$$X_G(h,k) \ll_k h^{2k+1}$$

The truth may be that $X_G(h,k) \ll_k h^{k+1}$ for all groups G.

For any group G, fixed k we have

$$X_G(h,k) \ll_k h^{2k+1}$$

as $k \to \infty$.

For any group G, fixed k we have

$$X_G(h, k) \ll_k h^{2k+1}$$

as $k \to \infty$.

For a particular group G, the behavior of $X_G(h)$ and $X_G(h, k)$ may be different.

For any group G, fixed k we have

$$X_G(h,k) \ll_k h^{2k+1}$$

as $k \to \infty$.
For a particular group G, the behavior of $X_G(h)$ and $X_G(h,k)$ may be different.

- If G is σ-finite, i.e. $G = \cup_{i=1}^{\infty} G_i$, where $G_1 \subset G_2 \subset \cdots$ are finite groups, then
$$X_G(h,k) \ll_k h^{k+1}.$$

For any group G, fixed k we have

$$X_G(h,k) \ll_k h^{2k+1}$$

as $k \to \infty$.
For a particular group G, the behavior of $X_G(h)$ and $X_G(h,k)$ may be different.

- If G is σ-finite, i.e. $G = \cup_{i=1}^{\infty} G_i$, where $G_1 \subset G_2 \subset \cdots$ are finite groups, then
$$X_G(h,k) \ll_k h^{k+1}.$$
- If G has exponent ℓ (i.e. $\ell x = 0 \, \forall x \in G$), then
$$X_G(h,k) \ll_\ell \ell^{2k} h.$$

For any group G, fixed k we have

$$X_G(h,k) \ll_k h^{2k+1}$$

as $k \to \infty$.
For a particular group G, the behavior of $X_G(h)$ and $X_G(h,k)$ may be different.

- If G is σ-finite, i.e. $G = \cup_{i=1}^{\infty} G_i$, where $G_1 \subset G_2 \subset \cdots$ are finite groups, then
$$X_G(h,k) \ll_k h^{k+1}.$$
- If G has exponent ℓ (i.e. $\ell x = 0 \, \forall x \in G$), then
$$X_G(h,k) \ll_\ell \ell^{2k} h.$$
- When $k = 1$ and ℓ is a prime power, we have
$$X_G(h) \leq \ell h + O_\ell(1).$$

It is interesting to study the exact asymptotic of $X_G(h, k)$ and $X_G(h)$ for a fixed group G.

It is interesting to study the exact asymptotic of $X_G(h, k)$ and $X_G(h)$ for a fixed group G.

The only groups for which we know the exact asymptotic of $X_G(h)$ are groups having exponent 2, It is interesting to study the exact asymptotic of $X_G(h,k)$ and $X_G(h)$ for a fixed group G.

The only groups for which we know the exact asymptotic of $X_G(h)$ are groups having exponent 2, and we have

$$X_G(h) \sim 2h$$

as $h \to \infty$.

The number of exceptional elements

Recall that $a \in A$ is called exceptional if $A \setminus \{a\}$ is *not* a basis.

The number of exceptional elements

Recall that $a \in A$ is called exceptional if $A \setminus \{a\}$ is *not* a basis. It is natural to ask how many exceptional elements are there.

The number of exceptional elements

Recall that $a \in A$ is called exceptional if $A \setminus \{a\}$ is *not* a basis. It is natural to ask how many exceptional elements are there. Define

$$E_G(h) = \max_{hA \sim G} \#\,\text{exceptional elements of } A.$$

The number of exceptional elements

Recall that $a \in A$ is called exceptional if $A \setminus \{a\}$ is *not* a basis. It is natural to ask how many exceptional elements are there. Define

$$E_G(h) = \max_{hA \sim G} \#\,\text{exceptional elements of } A.$$

Theorem (Plagne 2008)

As $h \to \infty$, we have $E_{\mathbf{N}}(h) \sim 2\sqrt{\frac{h}{\log h}}$.

The number of exceptional elements

Recall that $a \in A$ is called exceptional if $A \setminus \{a\}$ is *not* a basis. It is natural to ask how many exceptional elements are there. Define

$$E_G(h) = \max_{hA \sim G} \#\,\text{exceptional elements of } A.$$

Theorem (Plagne 2008)

As $h \to \infty$, we have $E_{\mathbf{N}}(h) \sim 2\sqrt{\frac{h}{\log h}}$.

Theorem (Lambert-L.-Plagne 2017)

For any group G, we have $0 \leq E_G(h) \leq h - 1$.

The number of exceptional elements

Recall that $a \in A$ is called exceptional if $A \setminus \{a\}$ is *not* a basis. It is natural to ask how many exceptional elements are there. Define

$$E_G(h) = \max_{hA \sim G} \#\,\text{exceptional elements of } A.$$

Theorem (Plagne 2008)

As $h \to \infty$, we have $E_{\mathbf{N}}(h) \sim 2\sqrt{\frac{h}{\log h}}$.

Theorem (Lambert-L.-Plagne 2017)

For any group G, we have $0 \leq E_G(h) \leq h - 1$.

The number of exceptional elements

Recall that $a \in A$ is called exceptional if $A \setminus \{a\}$ is *not* a basis. It is natural to ask how many exceptional elements are there. Define

$$E_G(h) = \max_{hA \sim G} \# \text{exceptional elements of } A.$$

Theorem (Plagne 2008)

As $h \to \infty$, we have $E_{\mathbf{N}}(h) \sim 2\sqrt{\frac{h}{\log h}}$.

Theorem (Lambert-L.-Plagne 2017)

For any group G, we have $0 \leq E_G(h) \leq h-1$. As far as general groups are concerned, these inequalities are best possible.

Essential subsets

Recall

$$E_G(h) = \max_{hA \sim G} \#\,\text{exceptional elements of } A,$$

and $E_G(h) \leq h - 1$.

Essential subsets

Recall

$$E_G(h) = \max_{hA \sim G} \#\,\text{exceptional elements of } A,$$

and $E_G(h) \leq h - 1$.

A subset $F \subset A$ is called exceptional if $A \setminus F$ is not a basis.

Essential subsets

Recall

$$E_G(h) = \max_{hA \sim G} \#\,\text{exceptional elements of } A,$$

and $E_G(h) \leq h - 1$.

A subset $F \subset A$ is called exceptional if $A \setminus F$ is not a basis. We are tempted to define

$$E_G(h, k) = \max_{hA \sim G} \#\,\text{exceptional subsets of size } k \text{ of } A.$$

Essential subsets

Recall

$$E_G(h) = \max_{hA \sim G} \#\text{exceptional elements of } A,$$

and $E_G(h) \le h - 1$.

A subset $F \subset A$ is called exceptional if $A \setminus F$ is not a basis. We are tempted to define

$$E_G(h, k) = \max_{hA \sim G} \#\text{exceptional subsets of size } k \text{ of } A.$$

However, if a is exceptional, then so is any set F containing a, and hence $E_G(h, k) = \infty$.

Deschamps-Farhi (2007): A subset $F \subset A$ is called essential if it is exceptional and minimal w/r to inclusion (i.e. F' is not exceptional for any $F' \subsetneq F$).

Deschamps-Farhi (2007): A subset $F \subset A$ is called essential if it is exceptional and minimal w/r to inclusion (i.e. F' is not exceptional for any $F' \subsetneq F$).

In other words, F is essential if $A \setminus F$ is not a basis, but $A \setminus F'$ is a basis for any $F' \subsetneq F$.

Deschamps-Farhi (2007): A subset $F \subset A$ is called essential if it is exceptional and minimal w/r to inclusion (i.e. F' is not exceptional for any $F' \subsetneq F$).

In other words, F is essential if $A \setminus F$ is not a basis, but $A \setminus F'$ is a basis for any $F' \subsetneq F$.

$\{a\}$ is essential $\Leftrightarrow$ $\{a\}$ is exceptional, but this is not true when $|F| \geq 2$.

Deschamps-Farhi (2007): A subset $F \subset A$ is called essential if it is exceptional and minimal w/r to inclusion (i.e. F' is not exceptional for any $F' \subsetneq F$).

In other words, F is essential if $A \setminus F$ is not a basis, but $A \setminus F'$ is a basis for any $F' \subsetneq F$.

$\{a\}$ is essential $\Leftrightarrow$ $\{a\}$ is exceptional, but this is not true when $|F| \geq 2$.

Theorem (Deschamps-Farhi 2007)

For any basis A of order h of $\mathbf{N}$, A has only finitely many essential subsets.

Deschamps-Farhi (2007): A subset $F \subset A$ is called essential if it is exceptional and minimal w/r to inclusion (i.e. F' is not exceptional for any $F' \subsetneq F$).

In other words, F is essential if $A \setminus F$ is not a basis, but $A \setminus F'$ is a basis for any $F' \subsetneq F$.

$\{a\}$ is essential $\Leftrightarrow$ $\{a\}$ is exceptional, but this is not true when $|F| \geq 2$.

Theorem (Deschamps-Farhi 2007)

For any basis A of order h of $\mathbf{N}$, A has only finitely many essential subsets.

Deschamps-Farhi (2007): A subset $F \subset A$ is called essential if it is exceptional and minimal w/r to inclusion (i.e. F' is not exceptional for any $F' \subsetneq F$).

In other words, F is essential if $A \setminus F$ is not a basis, but $A \setminus F'$ is a basis for any $F' \subsetneq F$.

$\{a\}$ is essential $\Leftrightarrow$ $\{a\}$ is exceptional, but this is not true when $|F| \geq 2$.

Theorem (Deschamps-Farhi 2007)

For any basis A of order h of $\mathbf{N}$, A has only finitely many essential subsets. However, this number cannot be bounded in terms of h alone.

Define

$$E_G(h,k) = \max_{hA \sim G} \# \text{essential subsets of size } k \text{ of } A.$$

Define

$$E_G(h,k) = \max_{hA \sim G} \#\,\text{essential subsets of size } k \text{ of } A.$$

Theorem (Hegarty 2010)

For fixed h and $k \to \infty$, we have

$$E_{\mathbf{N}}(h,k) \sim (h-1)\frac{\log k}{\log\log k}.$$

For fixed k and $h \to \infty$, we have

$$E_{\mathbf{N}}(h,k) \asymp_k \left(\frac{h^k}{\log h}\right)^{\frac{1}{k+1}}.$$

Deschamps-Farhi's proof works only in **N** (and **Z**). Using a completely different argument, we show that

Deschamps-Farhi's proof works only in $\mathbf{N}$ (and $\mathbf{Z}$). Using a completely different argument, we show that

Theorem (Bienvenu-Girard-L. 2019+)

For any basis A of order h of any group G, A has only finitely many essential subsets.

Deschamps-Farhi's proof works only in **N** (and **Z**). Using a completely different argument, we show that

Theorem (Bienvenu-Girard-L. 2019+)

For any basis A of order h of any group G, A has only finitely many essential subsets.

Deschamps-Farhi's proof works only in **N** (and **Z**). Using a completely different argument, we show that

Theorem (Bienvenu-Girard-L. 2019+)

For any basis A of order h of any group G, A has only finitely many essential subsets.

Theorem (Bienvenu-Girard-L. 2019+)

For any G, h, k,

$$E_G(h,k) \leq (Chk\log(hk))^k$$

for some absolute constant C.

Deschamps-Farhi's proof works only in **N** (and **Z**). Using a completely different argument, we show that

Theorem (Bienvenu-Girard-L. 2019+)

For any basis A of order h of any group G, A has only finitely many essential subsets.

Theorem (Bienvenu-Girard-L. 2019+)

For any G, h, k,

$$E_G(h,k) \leq (Chk \log(hk))^k$$

for some absolute constant C.

Deschamps-Farhi's proof works only in **N** (and **Z**). Using a completely different argument, we show that

Theorem (Bienvenu-Girard-L. 2019+)

For any basis A of order h of any group G, A has only finitely many essential subsets.

Theorem (Bienvenu-Girard-L. 2019+)

For any G, h, k,

$$E_G(h,k) \leq (Chk\log(hk))^k$$

for some absolute constant C.

The truth may be that $E_G(h,k) = O(hk)$. There are examples showing that we cannot do better than this.

Thank you!