The structure of Sidon set systems

Max Wötzel

University of Amsterdam

European Conference on Combinatorics, Graph Theory and Applications 2023

August 28th 2023
Sidon sets

**Sidon sets**

- Classical objects of study in additive number theory
- **Idea:** sets with little additive structure
Sidon sets

**Definition (\(B_h\)-set)**

For a positive integer \(h\), a (finite) subset \(A \subset G\) of an abelian group \(G\) is called \(B_h\)-set if for any \(a_1, \ldots, a_{2h} \in A\) it holds that

\[
a_1 + \cdots + a_h = a_{h+1} + \cdots + a_{2h} \iff \{a_1, \ldots, a_h\} = \{a_{h+1}, \ldots, a_{2h}\}\]
as multisets.

A \(B_2\)-set is also called *Sidon set*. 

**Classical objects of study in additive number theory**

**Idea:** sets with little additive structure
Sidon systems

This talk: interested in a generalization to set systems (families).

Operation: the sumset \( A + B = \{a + b : a \in A, b \in B\} \) of two sets \( A \) and \( B \).
**This talk:** interested in a generalization to set systems (families).

**Operation:** the sumset $A + B = \{a + b : a \in A, b \in B\}$ of two sets $A$ and $B$.

**Definition ($B_h$-system)**

For a positive integer $h$, a family $\mathcal{F} \subset 2^G$ of subsets of an abelian group $G$ is called a $B_h$-system if for any $A_1, \ldots, A_{2h} \in \mathcal{F}$ it holds that

\[
A_1 + \cdots + A_h = A_{h+1} + \cdots + A_{2h} \iff \{A_1, \ldots, A_h\} = \{A_{h+1}, \ldots, A_{2h}\} \text{ as multisets.}
\]

A $B_2$-system is also called *Sidon system*. 

Sidon systems

This talk: interested in a generalization to set systems (families).

Operation: the sumset $A + B = \{a + b : a \in A, b \in B\}$ of two sets $A$ and $B$.

Definition ($B_h$-system)

For a positive integer $h$, a family $\mathcal{F} \subset 2^G$ of subsets of an abelian group $G$ is called $B_h$-system if for any $A_1, \ldots, A_{2h} \in \mathcal{F}$ it holds that

$$A_1 + \cdots + A_h = A_{h+1} + \cdots + A_{2h} \iff \{A_1, \ldots, A_h\} = \{A_{h+1}, \ldots, A_{2h}\} \text{ as multisets.}$$

A $B_2$-system is also called Sidon system.

Note: Generalization, since a $B_h$-system consisting of singleton sets "is" exactly a $B_h$-set.
Previous results – bounds on Sidon systems

**Today:** Focus on the question: "How large can a Sidon set (system) be?"

**Parametrization:** $F_{k,h}(n)$ the largest size of a $B_h$-system in $\binom{[n]}{k}$, i.e. $k$-element subsets of $[n]$. For $h = 2$ (Sidon systems) we omit the $h$-subscript.
Previous results – bounds on Sidon systems

**Today:** Focus on the question: "How large can a Sidon set (system) be?"

**Parametrization:** $F_{k,h}(n)$ the largest size of a $B_h$-system in $\binom{[n]}{k}$, i.e. $k$-element subsets of $[n]$. For $h = 2$ (Sidon systems) we omit the $h$-subscript.

**Theorem (Erdős, Turán (1941), Bose (1942), Ruzsa (1993), Singer (1938))**

\[ F_1(n) = (1 \pm o(1)) \sqrt{n}. \]
Previous results – bounds on Sidon systems

**Today:** Focus on the question: "How large can a Sidon set (system) be?"

**Parametrization:** \( F_{k,h}(n) \) the largest size of a \( B_h \)-system in \( [n] \), i.e. \( k \)-element subsets of \([n]\). For \( h = 2 \) (Sidon systems) we omit the \( h \)-subscript.

**Theorem (Erdős, Turán (1941), Bose (1942), Ruzsa (1993), Singer (1938))**

\[
F_1(n) = (1 \pm o(1)) \sqrt{n}.
\]

**Theorem (Cilleruelo, Serra, W. (2020))**

Let \( n \geq k \geq 2 \) be integers. Then there exists a constant \( C_k \) such that

\[
C_k n^{k-1} \leq F_k(n) \leq \binom{n-1}{k-1} + n - k.
\]
Previous results – bounds on Sidon systems

**Today:** Focus on the question: "How large can a Sidon set (system) be?"

**Parametrization:** $F_{k,h}(n)$ the largest size of a $B_h$-system in $\binom{[n]}{k}$, i.e. $k$-element subsets of $[n]$. For $h = 2$ (Sidon systems) we omit the $h$-subscript.

**Theorem (Erdős, Turán (1941), Bose (1942), Ruzsa (1993), Singer (1938))**

\[ F_1(n) = (1 \pm o(1)) \sqrt{n}. \]

**Theorem (Cilleruelo, Serra, W. (2020))**

Let $n \geq k \geq 2$ be integers. Then there exists a constant $C_k$ such that

\[ C_k n^{k-1} \leq F_k(n) \leq \binom{n-1}{k-1} + n - k. \]

- Actually showed UB sharp for $k = 2$ and asymptotically correct for $k = 3$. 
Previous results – bounds on Sidon systems

**Today:** Focus on the question: "How large can a Sidon set (system) be?"

**Parametrization:** $F_{k,h}(n)$ the largest size of a $B_h$-system in $\binom{[n]}{k}$, i.e. $k$-element subsets of $[n]$. For $h = 2$ (Sidon systems) we omit the $h$-subscript.

**Theorem (Erdős, Turán (1941), Bose (1942), Ruzsa (1993), Singer (1938))**

$F_1(n) = (1 \pm o(1))\sqrt{n}$.

**Theorem (Cilleruelo, Serra, W. (2020))**

Let $n \geq k \geq 2$ be integers. Then there exists a constant $C_k$ such that

$$C_kn^{k-1} \leq F_k(n) \leq \binom{n-1}{k-1} + n - k.$$

- Actually showed UB sharp for $k = 2$ and asymptotically correct for $k = 3$.
- Also determined up to which size a typical family of $k$-subsets of $[n]$ will be a Sidon system.
Previous results – bounds on Sidon systems

**Today:** Focus on the question: "How large can a Sidon set (system) be?"

**Parametrization:** $F_{k,h}(n)$ the largest size of a $B_h$-system in $\binom{[n]}{k}$, i.e. $k$-element subsets of $[n]$. For $h = 2$ (Sidon systems) we omit the $h$-subscript.

**Theorem (Erdős, Turán (1941), Bose (1942), Ruzsa (1993), Singer (1938))**

\[ F_1(n) = (1 \pm o(1)) \sqrt{n}. \]

**Theorem (Cilleruelo, Serra, W. (2020))**

Let $n \geq k \geq 2$ be integers. Then there exists a constant $C_k$ such that

\[ C_kn^{k-1} \leq F_k(n) \leq \binom{n-1}{k-1} + n - k. \]

- Actually showed UB sharp for $k = 2$ and asymptotically correct for $k = 3$.
- Also determined up to which size a typical family of $k$-subsets of $[n]$ will be a Sidon system.
- **Remark:** $k = 1$ and $k \geq 2$ cases exhibit a gap ($\sqrt{n}$ vs $n^{k-1}$). Disappears if we allow $g \geq 2$ representations!
Main result

We (asymptotically) close the gap.

**Theorem**

Let $n, k, h \geq 2$ be integers. Then $F_{k,h}(n) = (1 \pm o(1))\binom{n}{k-1}$.
Main result

We (asymptotically) close the gap.

**Theorem**

Let $n, k, h \geq 2$ be integers. Then $F_{k,h}(n) = (1 \pm o(1)) \binom{n}{k-1}$.

**Remarks:**

- Also prove a result about largest $B_h$-system in binomial random subset of $\binom{[n]}{k}$.
We (asymptotically) close the gap.

**Theorem**

Let $n, k, h \geq 2$ be integers. Then $F_{k,h}(n) = (1 \pm o(1)) \binom{n}{k-1}$.

**Remarks:**

- Also prove a result about largest $B_h$-system in binomial random subset of $\binom{n}{k}$.
- Both statements are straightforward consequences of a structural result.
Main structural result

**Recall:** $F_k(n) \leq \binom{n-1}{k-1} + n - k$. **Proof idea:**

Partition sets in $[n]_k$ into classes of translates of $k$-sets in $\{0\} \cup [n-1]$ that contain 0.

Observation I: Any positive integer can appear as a difference of translation elements for at most one class.

Observation II: The largest possible difference is $n - k$.

Our main result establishes the other direction.

**Theorem** For any positive integers $k$ and $h$, there exists an integer $\ell(k,h)$ such that the following holds.

Let $A_1, \ldots, A_h, B_1, \ldots, B_h \subset \mathbb{Z}$ be $B_\ell$-sets of cardinality $k$ all having the same minimal element.

Then $A_1 + \cdots + A_h = B_1 + \cdots + B_h \iff \{A_1, \ldots, A_h\} = \{B_1, \ldots, B_h\}$, where the equality on the right-hand side is as multisets.

Implies the first main result since there are only $O(k,h)(n^k - 2)$ non-$B_\ell$-sets of cardinality $k$ in $[n]_k$ that contain e.g. 1, as long as $\ell$ only depends on $k$ and $h$. 
Main structural result

Recall: $F_k(n) \leq \binom{n-1}{k-1} + n - k$. **Proof idea:**

- Partition sets in $\binom{[n]}{k}$ into classes of translates of $k$-sets in $\{0\} \cup [n-1]$ that contain 0.
Main structural result

Recall: $F_k(n) \leq \binom{n-1}{k-1} + n - k$. **Proof idea:**

- Partition sets in $\binom{[n]}{k}$ into classes of translates of $k$-sets in $\{0\} \cup [n - 1]$ that contain 0.
- **Observation I:** Any positive integer can appear as a difference of translation elements for at most one class.
Main structural result

Recall: \( F_k(n) \leq \binom{n-1}{k-1} + n - k \). Proof idea:

- Partition sets in \( \binom{[n]}{k} \) into classes of translates of \( k \)-sets in \( \{0\} \cup [n-1] \) that contain 0.
- Observation I: Any positive integer can appear as a difference of translation elements for at most one class.
- Observation II: The largest possible difference is \( n - k \).
Main structural result

Recall: $F_k(n) \leq \binom{n-1}{k-1} + n - k$. **Proof idea:**

- Partition sets in $\binom{[n]}{k}$ into classes of translates of $k$-sets in $\{0\} \cup [n - 1]$ that contain 0.
- **Observation I:** Any positive integer can appear as a difference of translation elements for at most one class.
- **Observation II:** The largest possible difference is $n - k$.

Our main result establishes the other direction.
Main structural result

Recall: $F_k(n) \leq \binom{n-1}{k-1} + n - k$. Proof idea:

- Partition sets in $\binom{[n]}{k}$ into classes of translates of $k$-sets in $\{0\} \cup [n - 1]$ that contain 0.
- Observation I: Any positive integer can appear as a difference of translation elements for at most one class.
- Observation II: The largest possible difference is $n - k$.

Our main result establishes the other direction.

Theorem

For any positive integers $k$ and $h$, there exists an integer $\ell(k, h) = \ell$ such that the following holds.
Main structural result

Recall: $F_k(n) \leq \binom{n-1}{k-1} + n - k$. Proof idea:

- Partition sets in $\binom{[n]}{k}$ into classes of translates of $k$-sets in $\{0\} \cup [n - 1]$ that contain 0.
- Observation I: Any positive integer can appear as a difference of translation elements for at most one class.
- Observation II: The largest possible difference is $n - k$.

Our main result establishes the other direction.

Theorem

For any positive integers $k$ and $h$, there exists an integer $\ell(k, h) = \ell$ such that the following holds. Let $A_1, \ldots, A_h, B_1 \ldots, B_h \subset \mathbb{Z}$ be $B_{\ell}$-sets of cardinality $k$ all having the same minimal element.
Main structural result

Recall: \( F_k(n) \leq \binom{n-1}{k-1} + n - k \). **Proof idea:**

- Partition sets in \( \binom{[n]}{k} \) into classes of translates of \( k \)-sets in \( \{0\} \cup [n - 1] \) that contain 0.
- **Observation I:** Any positive integer can appear as a difference of translation elements for at most one class.
- **Observation II:** The largest possible difference is \( n - k \).

Our main result establishes the other direction.

**Theorem**

*For any positive integers \( k \) and \( h \), there exists an integer \( \ell(k, h) = \ell \) such that the following holds. Let \( A_1, \ldots, A_h, B_1 \ldots, B_h \subset \mathbb{Z} \) be \( B_\ell \)-sets of cardinality \( k \) all having the same minimal element. Then*

\[ A_1 + \cdots + A_h = B_1 + \cdots + B_h \iff \{A_1, \ldots, A_h\} = \{B_1, \ldots, B_h\}, \]

*where the equality on the right-hand side is as multisets.*

Implies the first main result since there are only \( O_{k,h}(n^{k-2}) \) non-\( B_\ell \)-sets of cardinality \( k \) in \( [n] \) that contain e.g. 1, as long as \( \ell \) only depends on \( k \) and \( h \).
Proof and key lemma

The key tool to prove the structural result will be the following lemma.

**Lemma**

Let $A, B, D \subset G$ be subsets of an abelian group $G$ such that $A$ is a Sidon set. Then for any set $X \subset A$ satisfying $|X| > |B|$, it holds that $X + D \subset A + B \Rightarrow D \subset B$.

**Key insight**

To use this lemma: If $A$ is a $B^2$-set, then $A + X$ is a $B^2$-set for any $X \subset A$.

**Toy example**

$A + B = A + D$ with $k \geq 2$: If $A$ is a $B^4$-set, then $A + A$ is a Sidon set and we have $A + A + B = A + A + D$ and can apply the lemma.

**General case:**

Instead of adding $A$ to both sides of $A + B = C + D$, we add $X_0 = A \cap C$.

Can guarantee $|X_0| \geq 2$ and then repeat this with new intersection $X_1 = (X_0 + A) \cap (X_0 + C)$ until at some point we are larger than $k$. 
Proof and key lemma

The key tool to prove the structural result will be the following lemma.

**Lemma**

Let $A, B, D \subset G$ be subsets of an abelian group $G$ such that $A$ is a Sidon set. Then for any set $X \subset A$ satisfying $|X| > |B|$, it holds that

$$X + D \subset A + B \implies D \subset B.$$
Proof and key lemma

The key tool to prove the structural result will be the following lemma.

**Lemma**

Let $A, B, D \subset G$ be subsets of an abelian group $G$ such that $A$ is a Sidon set. Then for any set $X \subset A$ satisfying $|X| > |B|$, it holds that

$$X + D \subset A + B \implies D \subset B.$$ 

- **Key insight** to use this lemma: If $A$ is a $B_{2\ell}$-set, then $A + X$ is a $B_\ell$-set for any $X \subset A$. 

The key tool to prove the structural result will be the following lemma.

**Lemma**

Let \( A, B, D \subset G \) be subsets of an abelian group \( G \) such that \( A \) is a Sidon set. Then for any set \( X \subset A \) satisfying \( |X| > |B| \), it holds that

\[
X + D \subset A + B \implies D \subset B.
\]

- **Key insight** to use this lemma: If \( A \) is a \( B_{2\ell} \)-set, then \( A + X \) is a \( B_{\ell} \)-set for any \( X \subset A \).
- **Toy example** \( A + B = A + D \) with \( k \geq 2 \): If \( A \) is \( B_4 \)-set, then \( A + A \) is a Sidon set and we have \( A + A + B = A + A + D \) and can apply the lemma.
Proof and key lemma

The key tool to prove the structural result will be the following lemma.

**Lemma**

Let $A, B, D \subset G$ be subsets of an abelian group $G$ such that $A$ is a Sidon set. Then for any set $X \subset A$ satisfying $|X| > |B|$, it holds that

$$X + D \subset A + B \implies D \subset B.$$  

- **Key insight** to use this lemma: If $A$ is a $B_{2\ell}$-set, then $A + X$ is a $B_{\ell}$-set for any $X \subset A$.
- **Toy example** $A + B = A + D$ with $k \geq 2$: If $A$ is $B_4$-set, then $A + A$ is a Sidon set and we have $A + A + B = A + A + D$ and can apply the lemma.
- **General case**: Instead of adding $A$ to both sides of $A + B = C + D$, we add $X_0 = A \cap C$. Can guarantee $|X_0| \geq 2$ and then repeat this with new intersection

$$X_1 = (X_0 + A) \cap (X_0 + C)$$

until at some point we are larger than $k$. 

M. Wötzel (UvA)  
Sidon System Structure  
EuroComb2023
Further outlook and open questions

- Key lemma holds in arbitrary abelian groups, structural theorem also in more general settings than $\mathbb{Z}$ (e.g. $\mathbb{R}$, groups admitting a total order)
Further outlook and open questions

- Key lemma holds in arbitrary abelian groups, structural theorem also in more general settings than \( \mathbb{Z} \) (e.g. \( \mathbb{R} \), groups admitting a total order)

- **Key point:** If we can guarantee \( |(A_i - A_i) \cap (B_j - B_j)| \geq 2 \), then we can boost this to get full structural theorem for any abelian group.

- Main open question: Suppose \( G \) abelian group, \( A, B, C, D \subset G \) with same cardinality and \( A + B = C + D \). Does there always exist \( U \in \{A, B\}, V \in \{C, D\} \) that share a non-zero difference?

- Other questions: Dependence of \( \ell \) on \( k \), sharp threshold in the constants \( c, C \) of the probabilistic statements, ...
Key lemma holds in arbitrary abelian groups, structural theorem also in more general settings than \( \mathbb{Z} \) (e.g. \( \mathbb{R} \), groups admitting a total order).

**Key point:** If we can guarantee \(|(A_i - A_i) \cap (B_j - B_j)| \geq 2\), then we can boost this to get full structural theorem for any abelian group.

**Main open question:** Suppose \( G \) abelian group, \( A, B, C, D \subset G \) with same cardinality and \( A + B = C + D \). Does there always exist \( U \in \{A, B\}, V \in \{C, D\} \) that share a non-zero difference?

Some partial progress on this for specific groups and/or values of \( k \).

Other questions: Dependence of \( \ell \) on \( k \), sharp threshold in the constants \( c, C \) of the probabilistic statements, ...
Further outlook and open questions

- Key lemma holds in arbitrary abelian groups, structural theorem also in more general settings than $\mathbb{Z}$ (e.g. $\mathbb{R}$, groups admitting a total order).

- **Key point:** If we can guarantee $| (A_i - A_i) \cap (B_j - B_j) | \geq 2$, then we can boost this to get full structural theorem for any abelian group.

- **Main open question:** Suppose $G$ abelian group, $A, B, C, D \subset G$ with same cardinality and $A + B = C + D$. Does there always exist $U \in \{ A, B \}, V \in \{ C, D \}$ that share a non-zero difference?

- Some partial progress on this for specific groups and/or values of $k$. 
Further outlook and open questions

- Key lemma holds in arbitrary abelian groups, structural theorem also in more general settings than \( \mathbb{Z} \) (e.g. \( \mathbb{R} \), groups admitting a total order)

- **Key point:** If we can guarantee \(|(A_i - A_i) \cap (B_j - B_j)| \geq 2\), then we can boost this to get full structural theorem for any abelian group.

- **Main open question:** Suppose \( G \) abelian group, \( A, B, C, D \subset G \) with same cardinality and \( A + B = C + D \). Does there always exist \( U \in \{A, B\}, V \in \{C, D\} \) that share a non-zero difference?

- Some partial progress on this for specific groups and/or values of \( k \).

- **Other questions:** Dependence of \( \ell \) on \( k \), sharp threshold in the constants \( c, C \) of the probabilistic statements, ...
Thank you all for your attention!