Sidon sets, sum-free sets and linear codes

Ingo Czerwinski Alexander Pott

Otto von Guericke University Magdeburg, Germany

ALCOCRYPT 2023: Algebraic and Combinatorial Methods for Coding and Cryptography

February 21, 2023

Contact: ingo@czerwinski.eu and alexander.pott@ovgu.de

Overview

1. Sidon sets
2. Sum-free sets
3. Linear codes

Sidon sets

Example

$M_4 = \{ (0,0,0,0), (1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,1,1) \}$ *is a subset of* $\mathbb{F}_2^4$.

Observation:

Sidon sets

Example

$M_4 = \{ (0,0,0,0), (1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,1,1) \}$ *is a subset of* $\mathbb{F}_2^4$.

Observation: *All sums of distinct elements are distinct.*

Sidon sets

Example

$M_4 = \{ (0,0,0,0), (1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,1,1) \}$ *is a subset of* $\mathbb{F}_2^4$.

Observation: *All sums of distinct elements are distinct.*

Definition

Let M be a subset of $\mathbb{F}_2^t$. M is called Sidon if $m_1 + m_2 \neq m_3 + m_4$ for all pairwise distinct $m_1, m_2, m_3, m_4 \in M$.

- Sidon introduced B_2-sequences of positive integers [Sid32], [Sid35] in his work on Fourier analysis.
- Later, Babai and Sós [BS85] generalised the definition of B_2-sequences to arbitrary groups and called them Sidon sets.
- In this work, we focus only on Sidon sets in $\mathbb{F}_2^t$.

Why are they interesting?

Definition

Let M be a subset of $\mathbb{F}_2^t$. M is called Sidon if $m_1 + m_2 \neq m_3 + m_4$ for all pairwise distinct $m_1, m_2, m_3, m_4 \in M$.

Why are they interesting?

Definition

Let M be a subset of $\mathbb{F}_2^t$. M is called Sidon if $m_1 + m_2 \neq m_3 + m_4$ for all pairwise distinct $m_1, m_2, m_3, m_4 \in M$.

Fundamental Problem

What is $s_{max}(\mathbb{F}_2^t)$, the maximal size of a Sidon set in $\mathbb{F}_2^t$?

Why are they interesting?

Definition

Let M be a subset of $\mathbb{F}_2^t$. M is called Sidon if $m_1 + m_2 \neq m_3 + m_4$ for all pairwise distinct $m_1, m_2, m_3, m_4 \in M$.

Fundamental Problem

What is $s_{max}(\mathbb{F}_2^t)$, the maximal size of a Sidon set in $\mathbb{F}_2^t$?

Important Relations

- Linear codes
- APN functions (not in the focus of this talk)
  - The graph of an APN function is Sidon.
  - Changing APN functions in one point:
    see Carlet [Car22]; Budaghyan, Carlet, Helleseth, Li, Sun [Bud+18].
  - APN exponents:
    see Carlet, Pizcek [CP21]; Carlet, Mesnager [CM22].

Maximal size of a Sidon set

Fundamental Problem

What is $s_{max}(\mathbb{F}_2^t)$, the maximal size of a Sidon set M in $\mathbb{F}_2^t$?

Maximal size of a Sidon set

Fundamental Problem

What is $s_{max}(\mathbb{F}_2^t)$, the maximal size of a Sidon set M in $\mathbb{F}_2^t$?

- Trivial bound (see Babai and Sós [BS85]):
  All sums of pairwise distinct elements of M have to be distinct, hence

$$\binom{|M|}{2} = \frac{|M|(|M|-1)}{2} \leq |\mathbb{F}_2^t \setminus \{0\}|.$$

- This is equivalent to:

$$s_{max}(\mathbb{F}_2^t) \leq \begin{cases} 2^{\frac{t+1}{2}} & \text{for } t \text{ odd}, \\ \left\lfloor \sqrt{2^{t+1}} + 0.5 \right\rfloor & \text{for } t \text{ even}. \end{cases} \tag{1}$$

- As far as we know: no progress in the last decades.
- We will improve this later.

Maximal Sidon sets

Question

Is it possible to extend every Sidon set to a Sidon set of maximal size by adding elements?

Maximal Sidon sets

Question

Is it possible to extend every Sidon set to a Sidon set of maximal size by adding elements? **No**, *already not in dimension 6 (see next slide).*

Maximal Sidon sets

Question

Is it possible to extend every Sidon set to a Sidon set of maximal size by adding elements? **No**, *already not in dimension 6 (see next slide).*

Definition

A Sidon set $M \subseteq \mathbb{F}_2^t$ *is called maximal if* $M = S$ *for every Sidon set* S *with* $M \subseteq S \subseteq \mathbb{F}_2^t$.

Example

$M_4 = \{ (0,0,0,0), (1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,1,1) \}$ *is maximal Sidon.*

Observation: $\{m_1 + m_2 + m_3 : m_1, m_2, m_3 \in M_4\} = \mathbb{F}_2^4$.

Maximal Sidon sets in small dimensions

Theorem (Czerwinski, Pott 2022)

Let M be a maximal Sidon set of $\mathbb{F}_2^t$. Then it has the following size:

t	1	2	3	4	5	6	7	8
$\lvert M\rvert$	2	3	4	6	7	8 or 9	12	15, 16 or 18

Remark

- $t \leq 6$ *obtained via a classification.*
- $t = 7$ *and* 8 *obtained by computer calculations.*
- *Two maximal Sidon sets of different sizes for* $t = 6$*:*
  $M_{6a} = \{0, \ \text{standard basis}, \ (1,1,1,1,1,1)\}$,
  $M_{6b} = \{0, \ \text{standard basis}, \ (1,1,1,1,0,0), (1,1,0,0,1,1)\}$.

Sum-free sets

Definition

Let M be a subset of $\mathbb{F}_2^t$. M is called sum-free if $m_1 + m_2 \neq m_3$ for all $m_1, m_2, m_3 \in M$.

Example

$M_4 = \{ (0,0,0,0), (1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,1,1) \}$ *is not sum-free.*

Observation: $M_4^* = M_4 \setminus \{0\}$ *is sum-free.*

Remark

It is equivalent discussing the maximal size of a Sidon set and discussing the maximal size of a sum-free Sidon set (off-by-one).

Linear codes

- A (binary) *linear code* $\mathcal{C}$ of *length* n and *dimension* k is a k dimensional vector subspace $\mathcal{C} \subseteq \mathbb{F}_2^n$.
- Such a code $\mathcal{C}$ is called a $[n, k]$-*code* and $c \in \mathcal{C}$ is called *code word* of $\mathcal{C}$.
- If the *minimum distance* of $\mathcal{C}$ is d, that is the minimum number of non-zero entries of all non-zero code words of $\mathcal{C}$, then $\mathcal{C}$ is called a $[n, k, d]$-*code*.

One-to-one correspondence I

Correspondence between additive structures and linear codes from Cohen and Zémor [CZ99]:

$$\begin{array}{ccc} M & \longmapsto & \mathcal{C}_M \\ M_{\mathcal{C}} & \longmapsto & \mathcal{C} \end{array}$$

Idea: Use $M \subseteq \mathbb{F}_2^t \setminus \{0\}$ as columns for the parity check matrix of $\mathcal{C}_M$.

One-to-one correspondence I

Correspondence between additive structures and linear codes from Cohen and Zémor [CZ99]:

$$\begin{array}{ccc} M & \longmapsto & \mathcal{C}_M \\ M_{\mathcal{C}} & \longleftarrow & \mathcal{C} \end{array}$$

Idea: Use $M \subseteq \mathbb{F}_2^t \setminus \{0\}$ as columns for the parity check matrix of $\mathcal{C}_M$.

Example

$M_4^* = \{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,1,1)\}$
leads to

$$\mathcal{C}_{M_4^*} = \left\{ (c_1, c_2, c_3, c_4, c_5) \in \mathbb{F}_2^5 : \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{pmatrix} = 0 \right\}.$$

One-to-one correspondence II

Correspondence between additive structures and linear codes from Cohen and Zémor [CZ99]:

$$\begin{array}{ccc} M & \longmapsto & \mathcal{C}_M \\ M_{\mathcal{C}} & \longmapsto & \mathcal{C} \end{array}$$

- One-to-one correspondence between additive properties of a set and properties on the associated code like minimum distance or covering radius to and vice versa.
- For example, let M be a non-empty subset of $\mathbb{F}_2^t \setminus \{0\}$ and let $\mathcal{C}_M$ be its associated $[|M|, k, d]$-code then:
  - M is sum-free if and only if $d \geq 4$; and
  - M is sum-free Sidon if and only if $d \geq 5$.

Non-existence of linear codes and Sidon sets

From the one-to-one correspondence follows:

Proposition (Cohen, Zémor [CZ99])

Let be $n, t \in \mathbb{N}$. Then the following statements are equivalent:

1. *There is no $[n, n-t, 5]$ code.*
2. *There is no Sidon set $M \subseteq \mathbb{F}_2^t$ of size $n+1$.*
3. $s_{max}(\mathbb{F}_2^t) \leq n$.

Sharpening of the Johnson bound

Theorem (Brouwer, Tolhuizen [BT93])

There is no $[n, n-t, 5]$ *code for* $n = 2^{(t+1)/2} - 2$, *hence*

$$s_{max}(\mathbb{F}_2^t) \leq 2^{(t+1)/2} - 2$$

for t *odd with* $t \geq 7$.

Sharpening of the Johnson bound

Theorem (Brouwer, Tolhuizen [BT93])

There is no $[n, n-t, 5]$ *code for* $n = 2^{(t+1)/2} - 2$, *hence*

$$s_{max}(\mathbb{F}_2^t) \leq 2^{(t+1)/2} - 2$$

for t *odd with* $t \geq 7$.

Remark

- *Improves the trivial bound (1) for odd dimension.*
- *What is about* t *even?*

Main Theorem

Theorem (Czerwinski, Pott 2022)

There is no $[n, n-t, 5]$ *code for* $n = \left\lfloor \sqrt{2^{t+1}} + 0.5 \right\rfloor - \lambda_t$, *hence*

$$s_{max}(\mathbb{F}_2^t) \leq \begin{cases} 2^{(t+1)/2} - 2 & \text{for } t \text{ odd}, \\ \left\lfloor \sqrt{2^{t+1}} + 0.5 \right\rfloor - \lambda_t & \text{for } t \text{ even}, \end{cases} \tag{2}$$

for $t \geq 6$ *and* $\lambda_t = \ldots \in \{0, 1, 2\}$.

Remark

- *Same main arguments as Brouwer and Tolhuizen.*
- *Improves the trivial bound (1) for even dimension.*
- *How to calculate* λ_t*?*

How to calculate λ_t?

Let be $t \geq 6$, $\left\lfloor \sqrt{2^{t+1}} + 0.5 \right\rfloor - 4 = 3a + b$ with $a \in \mathbb{Z}_{\geq 0}$, $b \in \{0, 1, 2\}$ and $\varepsilon = \sqrt{2^{t+1}} + 0.5 - \left\lfloor \sqrt{2^{t+1}} + 0.5 \right\rfloor \in [0, 1)$. Then

$$\lambda_t = \begin{cases} 1 & \text{for } a \text{ odd and } b = 0, \\ 2 & \text{for } a \text{ odd, } b = 1 \text{ and } 0 \leq \varepsilon \leq 1 - \frac{1}{2^{(t-4)/2}}, \\ 1 & \text{for } a \text{ odd, } b = 1 \text{ and } 1 - \frac{1}{2^{(t-4)/2}} < \varepsilon < 1, \\ 2 & \text{for } a \text{ odd and } b = 2, \\ 2 & \text{for } a \text{ even, } b = 0 \text{ and } 0 \leq \varepsilon \leq 0.5, \\ 1 & \text{for } a \text{ even, } b = 0 \text{ and } 0.5 < \varepsilon < 1, \\ 2 & \text{for } a \text{ even, } b = 1 \text{ and } 0 \leq \varepsilon \leq 1 - \frac{1}{2^{(t-5)/2}}, \\ 1 & \text{for } a \text{ even, } b = 1 \text{ and } 1 - \frac{1}{2^{(t-5)/2}} < \varepsilon \leq 1 - \frac{1}{2^{(t+7)/2}}, \\ 0 & \text{for } a \text{ even, } b = 1 \text{ and } 1 - \frac{1}{2^{(t+7)/2}} < \varepsilon < 1, \\ 0 & \text{for } a \text{ even and } b = 2. \end{cases}$$

* Please note the updated short abstract.

Codes table improvements

- The Main Theorem improves for t even and $t \geq 16$ several entries in the codes table of the MinT project from Schürer and Schmid [SS06] (`http://mint.sbg.ac.at/`).
- Some examples are listed in the following Corollary.

Corollary (Czerwinski, Pott 2022)

The best possible minimal distance of a linear code with the following parameters $[n, k]$ *is 4 instead of 4-5:*

$[360, 344]$	$[723, 705]$	$[1446, 1426]$
$[2895, 2873]$	$[5791, 5767]$, $[5792, 5768]$	$[11583, 11557]$

Maximal Sidon size and related bounds

t	9	10	11	12	13	14	15
Trivial bound (1)	32	45	64	91	128	181	256
New bound (2)	30	43	62	90	126	180	254
Codes bound	24	34	58	89	125	179	254
$s_{max}(\mathbb{F}_2^t)$	24	34	≥ 48	≥ 66	≥ 82	≥ 129	≥ 152

- The codes bound arises from the one-to-one correspondence and Grassl's codes table [Gra07] (http://codetables.de).

Sidon sets, sum-free sets and linear codes

Thanks for your attention.

Sidon sets, sum-free sets and linear codes

Thanks for your attention.

Questions?

References I

[BS85] László Babai and Vera T Sós. "Sidon sets in groups and induced subgraphs of Cayley graphs". In: *European Journal of Combinatorics* 6.2 (1985), pp. 101–114.

[BT93] A E Brouwer and L M G M Tolhuizen. "A sharpening of the Johnson bound for binary linear codes and the nonexistence of linear codes with Preparata parameters". In: *Designs, Codes and Cryptography* 3.2 (May 1993), pp. 95–98.

[Bud+18] Lilya Budaghyan et al. "On Upper Bounds for Algebraic Degrees of APN Functions". In: *IEEE Transactions on Information Theory* 64.6 (2018), pp. 4399–4411. DOI: 10.1109/TIT.2017.2757938.

References II

[Car22] Claude Carlet. "On APN Functions Whose Graphs Are Maximal Sidon Sets". In: *LATIN 2022: Theoretical Informatics: 15th Latin American Symposium, Guanajuato, Mexico, November 7–11, 2022, Proceedings*. Guanajuato, Mexico: Springer-Verlag, 2022, 243–254. ISBN: 978-3-031-20623-8. DOI: 10.1007/978-3-031-20624-5_15. URL: https://doi.org/10.1007/978-3-031-20624-5_15.

[CM22] Claude Carlet and Sihem Mesnager. "On those multiplicative subgroups of $\mathbb{F}_{2^n}^*$ which are Sidon sets and/or sum-free sets". In: *Journal of Algebraic Combinatorics* 55.1 (Feb. 2022), pp. 43–59.

[CP21] Claude Carlet and Stjepan Picek. "On the exponents of APN power functions and Sidon sets, sum-free sets, and Dickson polynomials". In: *Advances in Mathematics of Communications* (2021).

References III

[CZ99] Gilles Cohen and Gérard Zémor. "Subset sums and coding theory". en. In: *Structure theory of set addition*. Ed. by Deshouilliers Jean-Marc, Landreau Bernard, and Yudin Alexander A. Astérisque 258. Société mathématique de France, 1999. URL: http://www.numdam.org/item/AST_1999__258__327_0/.

[Gra07] Markus Grassl. *Bounds on the minimum distance of linear codes and quantum codes*. Online available at http://www.codetables.de. Accessed on 2022-11-02. 2007.

[Sid32] Simon Sidon. "Ein Satz über trigonometrische Polynome und seine Anwendung in der Theorie der Fourier-Reihen". In: *Mathematische Annalen* 106.1 (Dec. 1932), pp. 536–539.

[Sid35] Simon Sidon. "Über die Fourier Konstanten der Funktionen der Klasse L_p für $p > 1$". In: *Acta Univ. Szeged Sect. Sci. Math* 7 (1935), pp. 175–176.

References IV

[SS06] Rudolf Schürer and Wolfgang Ch Schmid. "MinT: A database for optimal net parameters". In: *Monte Carlo and Quasi-Monte Carlo Methods 2004*. Springer, 2006, pp. 457–469.

Supplement

Supplement: Maximal Sidon sets in small dimensions II

Let M be a maximal Sidon set of $\mathbb{F}_2^t$ and $e_1, \ldots, e_t$ be the standard basis of $\mathbb{F}_2^t$. Then M is affine equivalent to

t=1: $M_1 = \{0, e_1\} = \mathbb{F}_2^1$ with $|M_1| = 2$.

t=2: $M_2 = \{0, e_1, e_2\} = \mathbb{F}_2^2 \setminus \{0\}$ with $|M_2| = 3$.

t=3: $M_3 = \{0, e_1, e_2, e_3\}$ with $|M_3| = 4$.

t=4: $M_4 = \{0, e_1, e_2, e_3, e_4, e_1 + e_2 + e_3 + e_4\}$ with $|M_4| = 6$.

t=5: $M_{5a} = \{0, e_1, e_2, e_3, e_4, e_5, e_1 + e_2 + e_3 + e_4\}$; or
$M_{5b} = \{0, e_1, e_2, e_3, e_4, e_5, e_1 + e_2 + e_3 + e_4 + e_5\}$;
with $|M_{5a}| = |M_{5b}| = 7$.

t=6: $M_{6a} = M_{5a} \cup \{e_6, e_{i_1} + e_{i_2} + e_5 + e_6\}$; or
$M_{6b} = M_{5b} \cup \{e_6, e_{j_1} + e_{j_2} + e_{j_3} + e_6\}$; or
$M_{6c} = \{0, e_1, e_2, e_3, e_4, e_5, e_6, e_1 + e_2 + e_3 + e_4 + e_5 + e_6\}$;
with distinct $i_1, i_2 \in \{1, 2, 3, 4\}$, pairwise distinct $j_1, j_2, j_3 \in \{1, 2, 3, 4, 5\}$ and $|M_{6a}| = |M_{6b}| = 9 > |M_{6c}| = 8$.

Supplement: 4-sums of Sidon sets

Recall from above: Let $M \subseteq \mathbb{F}_2^t$ be a Sidon set with $|M| \geq 3$ (and therefore $t \geq 2$). Then the following statements are equivalent:

1. M is maximal;
2. $\mathcal{S}_3^*(M) \cup M = \mathbb{F}_2^t$;
3. $\mathcal{S}_3(M) = \mathbb{F}_2^t$.

Theorem (Czerwinski, Pott 2022)

Let M be a Sidon set of $\mathbb{F}_2^t$. If $|M| > s_{max}(\mathbb{F}_2^{t-1})$ then

1. $\mathcal{S}_4(M) = \mathbb{F}_2^t$ *and*
2. $\dim\langle M\rangle = \dim\langle \mathcal{S}_2^*(M)\rangle = t$.

Supplement: One-to-one correspondence III

The following Theorem is another interesting connection between a code property (covering radius) and a Sidon property:

Theorem (Czerwinski, Pott 2022)

Let M be a non-empty subset of $\mathbb{F}_2^t \setminus \{0\}$ and let $\mathcal{C}_M$ be its $[|M|, k, d]$-code with covering radius R.

1. *If M is sum-free Sidon and $|M| \geq s_{max}(\mathbb{F}_2^{t-1})$ then $R = 3$ or $R = 4$.*
2. *M is maximal sum-free Sidon (that means we cannot extend it to a larger sum-free Sidon set) if and only if $R = 3$.*

Supplement: Maximal minimum distance

We define

$$d_{max}(n,k) = \max\{d : \text{there exists an } [n,k,d]\text{-code}\}.$$

as the *maximal minimum distance* of a code with given length n and dimension k.
It is one of the main properties of *optimal* codes and frequently listed as a matrix $(d_{max}(n,k))_{n,k}$.

Proposition (Subdiagonal properties, Czerwinski, Pott 2022)

Let be $n, t \in \mathbb{N}$.

1. $d_{max}(n, n-t) = 3$ *if and only if* $2^{t-1} < n < 2^t$.
2. $d_{max}(n, n-t) = 4$ *if and only if* $s_{max}(\mathbb{F}_2^t) \leq n \leq 2^{t-1}$.
3. $d_{max}(n, n-t) = 5$ *if and only if* $s_{max}(\mathbb{F}_2^{t-1}) < n < s_{max}(\mathbb{F}_2^t)$.
4. $d_{max}(n, n-t) \geq 6$ *if and only if* $n \leq s_{max}(\mathbb{F}_2^{t-1})$.