Numerical semigroup problems motivated by Distributed Matrix Multiplication using AG codes

Adrián Fidalgo-Díaz
(Joint work with Umberto Martínez-Peñas)

University of Valladolid

Motivation: Umberto's talk.

Definition

Let $S \subseteq \mathbb{N}$. We say that S is a numerical semigroup if:

- S is a submonoid of $\mathbb{N}$, i.e, $s_1 + s_2 \in S$ for all $s_1, s_2 \in S$ and $0 \in S$.
- $\mathbb{N} \setminus S$ is finite.

Definition

Let $S \subseteq \mathbb{N}$. We say that S is a numerical semigroup if:

- S is a submonoid of $\mathbb{N}$, i.e, $s_1 + s_2 \in S$ for all $s_1, s_2 \in S$ and $0 \in S$.
- $\mathbb{N} \setminus S$ is finite.

Notation

Let $A \subseteq \mathbb{N}$, we write $A^* := A \setminus \{0\}$.

Definition

Let S be a numerical semigroup we define the following:

- The conductor is the lowest number $c(S)$ such that if $s \geq c(S)$ then $s \in S$.
- $g(S) := |\mathbb{N} \setminus S|$, the number of elements of $\mathbb{N}$ not in S.
- $n(S)$ is the number of elements of S strictly lower than $c(S)$.

Definition

Let $n \in S^*$, we define the Apéry set with respect to $n \in S$ as

$$\mathrm{Ap}(S, n) := \{s \in S : \; s - n \notin S\}$$

Lemma (Kunz coordinates)

Let $n \in S^*$. Then

- $\mathrm{Ap}(S, n) = \{w_0, w_1, \ldots, w_{n-1}\}$, *where w_i is the lowest element of S congruent with $i \mod n$.*
- $c(S) = \max(\mathrm{Ap}(S, n)) - n + 1$.

Preliminaries

AG polynomial codes problem

AG matdot codes problem

Problem

Let $m, n \in \mathbb{N}^*$, *we say that* $D_A, D_B \subseteq S$ *is a solution to the AG polynomial code problem if*

- $|D_A| = m$ *and* $|D_B| = n$.
- *(Non colliding)* $a + b \neq a' + b'$ *for every* $(a, b), (a', b') \in D_A \times D_B$ *such that* $(a, b) \neq (a', b')$.

Problem

Let $m, n \in \mathbb{N}^*$, we say that $D_A, D_B \subseteq S$ is a solution to the AG polynomial code problem if

- $|D_A| = m$ *and* $|D_B| = n$.
- *(Non colliding)* $a + b \neq a' + b'$ *for every* $(a, b), (a', b') \in D_A \times D_B$ *such that* $(a, b) \neq (a', b')$.

We define its recovery threshold as $\max(D_A) + \max(D_B)$ *and we say that the solution is optimal if the recovery threshold is minimum among all the possible solutions.*

Notation

Let $A, B \subseteq \mathbb{N}$, we write $A + B$ to denote the Minkowski sum, i.e.,

$$A + B := \{a + b \in \mathbb{N} : \; a \in A, \quad b \in B\}.$$

Remark

We observe that the non colliding property is equivalent to $|D_A + D_B| = mn$.

Example

Let $S = \langle 2, 5 \rangle = \{0, 2, 4, 5, \rightarrow\}$, $m = 2$ and $n = 3$. Consider the sets:

$$\begin{aligned} D_A &:= \{0, 4\} \\ D_B &:= \{4, 5, 6\}. \end{aligned}$$

We see that $D_A + D_B = \{4, 5, 6, 8, 9, 10\}$. Since $|D_A + D_B| = mn$, this is a solution. It is not an optimal solution but

$$\begin{aligned} D'_A &:= \{4, 5\} \\ D'_B &:= \{0, 2, 4\}. \end{aligned}$$

it is.

Construction (Trivial)

Define the sets

$$\begin{aligned} D_A &:= \{c(S), c(S)+1, \ldots, c(S)+m-1\}, \\ D_B &:= \{c(S), c(S)+m, \ldots, c(S)+(n-1)m\}. \end{aligned}$$

This is a solution to the AG polynomial codes problem since

$$D_A + D_B = \{2c(S), 2c(S)+1, \ldots 2c(S)+nm-1\}$$

and so $|D_A + D_B| = mn$. Its recovery threshold is $2c(S)+nm-1$.

Construction (Apéry)

Let $m' := \min\{s \in S : \ s \geq m\}$. Choose D_A as the subset formed by the first m elements of the Apéry set $\mathrm{Ap}(S, m')$. Define D_B as

$$D_B := \{0, m', \ldots, (n-1)m'\}.$$

This is a solution for AG polynomial code problem by Lemma of Kunz coordinates. Its recovery threshold satisfies the following upper bound

$$\max(D_A) + \max(D_B) \leq c(S) + (m + m(S) - 1)n - 1.$$

If $m \in S$, then $m' = m$ and

$$\max(D_A) + \max(D_B) = c(S) + mn - 1.$$

Lemma

Let $D_A, D_B \subseteq S$ of sizes m and n, respectively. Consider the sets

$$E_A := \{d - d' \in \mathbb{N} : \; d, d' \in D_A, \quad d > d'\},$$
$$E_B := \{d - d' \in \mathbb{N} : \; d, d' \in D_B, \quad d > d'\}.$$

The sets D_A and D_B are a solution to the AG polynomial code problem if and only if $E_A \cap E_B = \emptyset$.

Construction (Difference sets)

Consider the sets

$$D_A := \{c(S), c(S)+1, \dots, c(S)+m-1\},$$
$$D_B := \{m_1, m_2, \dots m_n\},$$

where each m_i is defined recursively as

$$m_i := \begin{cases} 0 & \text{if } i = 1 \\ \min\{s \in S : \; s \geq m_{i-1} + m\} & \text{if } i > 1. \end{cases}$$

Applying the previous lemma we conclude that D_A and D_B form a solution to the AG polynomial code problem, since

$$\max(E_A) = m - 1,$$
$$\min(E_B) \geq m,$$

which implies that $E_A \cap E_B = \emptyset$.

If $m \in S$ then $m_i = m_{i-1} + m$ for each $i = 2, \ldots n$ and

$$\max(D_A) + \max(D_B) = c(S) + mn - 1.$$

Proposition (Lower bound)

Let D_A and D_B be a solution to the AG polynomial code problem. If $mn \geq n(S)$, then

$$\max(D_A) + \max(D_B) \geq g(S) + mn - 1.$$

Proposition (Lower bound)

Let D_A and D_B be a solution to the AG polynomial code problem. If $mn \geq n(S)$, then

$$\max(D_A) + \max(D_B) \geq g(S) + mn - 1.$$

	if $m \notin S$	**if** $m \in S$
Trivial	$2c(S) + mn - 1$	$2c(S) + mn - 1$
Apéry	$c(S) + m'n - 1$	$c(S) + mn - 1$
Difference sets	$c(S) + mn - 1 + \sum_{i=1}^{n-1} \mu_i$	$c(S) + mn - 1$

Table: Recovery threshold of proposed solutions to the AG polynomial code problem.

Topics to explore:

- Obtain new constructions.
- Obtain optimal constructions.
- Improve the lower bound.
- Any of the anterior but restricting to some semigroup family (generated by two elements, symmetric, sparse, Arf, telescopic...).

Problem

Given $m \in \mathbb{N}^*$, we say that $D_A, D_B \subseteq S$ is a solution to the AG matdot code problem if

- $|D_A| = |D_B| = m$.
- *(Maximum colliding) There exists $d \in D_A + D_B$ such that there are exactly m pairs $(a, b) \in D_A \times D_B$ satisfying $d = a + b$.*

Problem

Given $m \in \mathbb{N}^*$, we say that $D_A, D_B \subseteq S$ is a solution to the AG matdot code problem if

- $|D_A| = |D_B| = m$.
- *(Maximum colliding) There exists $d \in D_A + D_B$ such that there are exactly m pairs $(a, b) \in D_A \times D_B$ satisfying $d = a + b$.*

We define the recovery threshold as $\max(D_A) + \max(D_B)$ *and we say that the solution is optimal if the recovery threshold is minimum among all the possible solutions (observe that d is not fixed, only m is fixed).*

Example

Let $S = \langle 2, 3 \rangle$, $m = 4$. Consider the sets:

$$D_A := \{2, 3, 4, 5\}$$
$$D_B := \{3, 4, 5, 6\}$$

This is a solution since

$$d := 8 = 2 + 6 = 3 + 5 = 4 + 4 = 3 + 5$$

It is not an optimal solution but

$$D'_A = D'_B := \{2, 3, 4, 5\}$$

it is.

Construction (Trivial)

Define the sets

$$D_A = D_B := \{c(S), c(S)+1, \ldots, c(S)+m-1\}.$$

These sets form a solution to the AG matdot code problem, where $d = 2c(S)+m-1$. Its recovery threshold is $2(c(S)+m-1)$.

Definition

Let $\delta \in [0, c(S)] \cap S$. Define

$$n(\delta) := |[\delta, c(S) - 1] \cap S|,$$

Proposition (Optimal solution)

Let $m \geq 2c(S)$. Consider an element $\delta \in [0, c(S)] \cap S$ such that $\delta + 2n(\delta)$ is maximum among all the possible δ. Define $d := m - 1 + 2c(S) - 2n(\delta)$. Then

$$\begin{aligned} D_A = D_B := & ([\delta, c(S) - 1] \cap S) \\ & \cup ([c(S), d - c(S)]) \\ & \cup (d - [\delta, c(S) - 1] \cap S), \end{aligned}$$

is an optimal solution to the AG matdot codes problem with recovery threshold $2(m - 1 + 2c(S) - \delta - 2n(\delta))$.

Remark

Observe that the number δ defined before is independent of m (as long as $m \geq 2c(S)$), so we only need to compute it once for the chosen semigroup.

Remark

Observe that the number δ defined before is independent of m (as long as $m \geq 2c(S)$), so we only need to compute it once for the chosen semigroup.

Definition

Define the map Δ given by

$$\begin{aligned}\Delta : S \cap [0, c(S)] &\to \mathbb{N} \\ \delta &\mapsto \delta + 2n(\delta).\end{aligned}$$

Remark

Observe that the number δ defined before is independent of m (as long as $m \geq 2c(S)$), so we only need to compute it once for the chosen semigroup.

Definition

Define the map Δ given by

$$\begin{aligned} \Delta : S \cap [0, c(S)] &\to \mathbb{N} \\ \delta &\mapsto \delta + 2n(\delta). \end{aligned}$$

Proposition

The map Δ reaches its maximum in some $\delta \geq c(S)/2$.

Definition

We say that a numerical semigroup is sparse if it has no consecutive elements lower than the conductor.

Proposition

If S is sparse, then Δ reaches its maximum at $\delta = c(S)$.

Definition

We say that a numerical semigroup is sparse if it has no consecutive elements lower than the conductor.

Proposition

If S is sparse, then Δ reaches its maximum at $\delta = c(S)$.

Proposition

If $S = \langle q, q+1 \rangle$ with $q \geq 2$, then Δ reaches its maximum at $\delta = q\lceil (q-1)/2 \rceil$.

Topics to explore:

- Optimal solutions for $m < 2c(S)$.
- Algorithms to compute where Δ reaches its maximum.
- Any of the anterior but restricting to some semigroup family (generated by two elements, symmetric, Arf, telescopic...).

Thank you for your time!