THE TENSOR RANK IN CODING THEORY

Giuseppe Cotardo
joint work with E. Byrne

Joint Mathematics Meetings 2023

January 4, 2023

VIRGINIA TECH

AA
RG

WHAT IS COMPLEXITY?

Definition

The **complexity** of a *problem* is the cost of the optimal procedure among all the ones that solve the *problem* and fit into a given model of computation.

- The cost of a *computation* that solves a problem is an **upper bound** on the complexity of that problem with respect to the given model.
- We are interested in the so-called **nonscalar model** where additions, subtractions and scalar multiplications are free of charge. The (**nonscalar**) **cost** of an algorithm is therefore the number of multiplications and divisions needed to compute the result.

MULTIPLICATION OF 2×2 MATRICES

Let A, B be 2×2 following matrices

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \qquad B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}.$$

The standard algorithm returns the matrix $C = AB$ by computing the following intermediate results:

$$c_1 = a_1 b_1 + a_2 b_3, \qquad c_2 = a_1 b_2 + a_2 b_4,$$
$$c_3 = a_3 b_1 + a_4 b_3, \qquad c_4 = a_3 b_2 + a_4 b_4.$$

It requires 8 **multiplications** and 4 **additions**. Therefore, an **upper bound** for the complexity (in the nonscalar model) is 8.

MULTIPLICATION OF 2×2 MATRICES

Let A, B be 2×2 following matrices

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \qquad B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}.$$

We can compute $C = AB$ in 7 **multiplications** and 18 **additions** using Strassen's algorithm, which gives

$$c_1 = S_1 + S_4 - S_5 + S_7, \qquad c_2 = S_2 + S_4, \qquad c_3 = S_3 + S_5, \qquad c_4 = S_1 + S_3 - S_2 + S_6$$

where the S_i's are the intermediate steps

$$\begin{aligned} &S_1 = (a_1 + a_4)(b_1 + b_4), && S_2 = (a_3 + a_4)b_1, && S_3 = a_1(b_3 - b_4), \\ &S_4 = a_4(b_3 - b_1), && S_5 = (a_1 + a_2)b_4, && S_6 = (a_3 - a_1)(b_1 + b_2), \\ &S_7 = (a_2 - a_4)(b_3 + b_4). \end{aligned}$$

MULTIPLICATION OF 2×2 MATRICES

Let A, B be 2×2 following matrices

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \qquad B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}.$$

Remark

The complexity of multiplying 2×2 matrices (in the nonscalar model) is 7. The upper-bound is given by Strassen (1969), the lower bound was proved by Winograd (1971).

BILINEAR MAPS

Let A, B, C be vector spaces over the same field $\mathbb{K}$. For $\alpha \in A^*$, $\beta \in B^*$ and $c \in C$, one can define a *rank one* bilinear map

$$\alpha \otimes \beta \otimes c : A \times B \longrightarrow C : (a, b) \longmapsto \alpha(a)\beta(b)c.$$

Definition

The **rank** $\tau(T)$ of a bilinear map $T : A \times B \longrightarrow C$ is the smallest integer R such that there exist $\alpha_1, \ldots, \alpha_R \in A^*$, $\beta_1, \ldots, \beta_R \in B^*$ and $c_1, \ldots, c_R \in C$ such that

$$T = \sum_{i=1}^{R} \alpha_i \otimes \beta_i \otimes c_i.$$

BILINEAR MAPS AND COMPLEXITY

- If a bilinear map T has rank R then T can be *executed* by performing R multiplications (and $\mathcal{O}(R)$ additions).

- The rank of a bilinear map gives a measure of its complexity.

BILINEAR MAPS AND COMPLEXITY

- If a bilinear map T has rank R then T can be *executed* by performing R multiplications (and $\mathcal{O}(R)$ additions).
- The rank of a bilinear map gives a measure of its complexity.

Example

Matrix multiplication of $n \times n$ matrices is a bilinear map:

$$M_{n,n,n} : \mathbb{K}^{n\times n} \times \mathbb{K}^{n\times n} \longrightarrow \mathbb{K}^{n\times n}.$$

We observed that $R(M_{2,2,2}) = 7$ and it is known that $19 \leq R(M_{3,3,3}) \leq 23$.

3-TENSORS

We assume n, m, k to be integers with $n \leq m$.

Definition

A 3-**tensor** $X := \sum_r a_r \otimes b_r \otimes c_r$ is an element of $\mathbb{K}^k \otimes \mathbb{K}^n \otimes \mathbb{K}^m$.

3-TENSORS

We assume n, m, k to be integers with $n \leq m$.

Definition

A 3-**tensor** $X := \sum_r a_r \otimes b_r \otimes c_r$ is an element of $\mathbb{K}^k \otimes \mathbb{K}^n \otimes \mathbb{K}^m$.

X can be seen as the representation of a bilinear map

$$\mathbb{K}^n \times \mathbb{K}^m \longrightarrow \mathbb{K}^k.$$

3-TENSORS

We assume n, m, k to be integers with $n \leq m$.

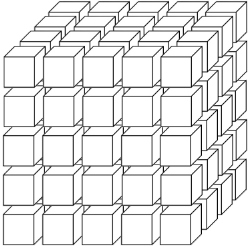
Definition

A 3-**tensor** $X := \sum_r a_r \otimes b_r \otimes c_r$ is an element of $\mathbb{K}^k \otimes \mathbb{K}^n \otimes \mathbb{K}^m$.

X is is related to the the 3-dimensional array

$$X_{ij\ell} = \sum_r (a_r)_\ell \cdot (b_r)_i \cdot (c_r)_j$$

which implies $\mathbb{K}^k \otimes \mathbb{K}^n \otimes \mathbb{K}^m \simeq \mathbb{K}^{k \times n \times m}$.



3-TENSORS

We assume n, m, k to be integers with $n \leq m$.

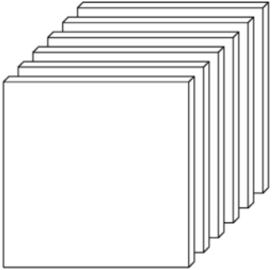
Definition

A 3-**tensor** $X := \sum_r a_r \otimes b_r \otimes c_r$ is an element of $\mathbb{K}^k \otimes \mathbb{K}^n \otimes \mathbb{K}^m$.

We can also identify the tensor X with the array of $n \times m$ matrices

$$X = (\, X_1 \mid \ldots \mid X_k \,).$$

In the remainder, we assume X to be non-degenerate, i.e. such that $X_1, \ldots, X_k$ linearly independent.



3-TENSORS

Definition

Let X be a 3-tensor. X is said to be **simple** (or **rank one**) if there exist $a \in \mathbb{K}^k$, $b \in \mathbb{K}^n$ and $c \in \mathbb{K}^m$ such that $X = a \otimes b \otimes c$. The **tensor rank** $\operatorname{trk}(X)$ of X is defined as the smallest R such that X can be expressed as sum of R l.i. simple tensors.

Definition

Let $\mathcal{A} := \{A_1, \ldots, A_R\} \subseteq \mathbb{K}^{n \times m}$ be a set of R l.i. rank-1 matrices. We say that $\mathcal{A}$ is a **perfect base** (or R-**base**) for the tensor X if $\langle X_1, \ldots, X_k \rangle \leq \langle A_1, \ldots, A_R \rangle$.

3-TENSORS

Definition

Let X be a 3-tensor. X is said to be **simple** (or **rank one**) if there exist $a \in \mathbb{K}^k$, $b \in \mathbb{K}^n$ and $c \in \mathbb{K}^m$ such that $X = a \otimes b \otimes c$. The **tensor rank** $\operatorname{trk}(X)$ of X is defined as the smallest R such that X can be expressed as sum of R l.i. simple tensors.

Definition

Let $\mathcal{A} := \{A_1, \ldots, A_R\} \subseteq \mathbb{K}^{n \times m}$ be a set of R l.i. rank-1 matrices. We say that $\mathcal{A}$ is a **perfect base** (or R-**base**) for the tensor X if $\langle X_1, \ldots, X_k \rangle \leq \langle A_1, \ldots, A_R \rangle$.

Lemma

There exists an R-base for X if and only if $\operatorname{trk}(X) \leq R$.

TENSOR RANK OF MATRIX SPACES

Theorem (Atkinson, Lloyd - 1983)

Let $\mathrm{char}(\mathbb{K}) \neq 2$ and let $X \in \mathbb{K}^{(mn-2)\times n\times m}$ be a tensor. We have $\mathrm{trk}(X) = mn-2$ unless X is such that $X_{j,1,1} + X_{j,2,2} = 0$ and $X_{j,1,2} = 0$ for all $1 \leq j \leq mn-2$.

TENSOR RANK OF MATRIX SPACES

Theorem (Atkinson, Lloyd - 1983)

Let $\mathrm{char}(\mathbb{K}) \neq 2$ and let $X \in \mathbb{K}^{(mn-2)\times n\times m}$ be a tensor. We have $\mathrm{trk}(X) = mn - 2$ unless X is such that $X_{j,1,1} + X_{j,2,2} = 0$ and $X_{j,1,2} = 0$ for all $1 \leq j \leq mn - 2$.

Definition

The **dual** of $V \leq \mathbb{K}^{n\times m}$ is $V^{\perp} := \{N \in \mathbb{K}^{n\times m} : \mathrm{Tr}(MN^t) = 0 \ \ \forall\, M \in V, M \neq 0\}$.

Definition (Atkinson, Lloyd - 1983)

A space of $n \times m$ matrices is said to be **perfect** if it is generated by rank-1 matrices.

TENSOR RANK OF MATRIX SPACES

Theorem (Byrne, C.)

Let $s \in \{1, \dots, m-1\}$, $|\mathbb{K}| \geq s+1$, $\mathcal{S} := \{1, \gamma_1, \dots, \gamma_{s-1}\}$ be a set of distinct elements of $\mathbb{K} \setminus \{0\}$ and $M \in \mathbb{K}^{m\times m}$ be a companion matrix of an irreducible polynomial of degree m. We have that $\langle I, M, \dots, M^{s-1}\rangle^{\perp} \leq \mathbb{K}^{m\times m}$ is perfect and an (m^2-s)-base is

$$\mathcal{A}(\mathcal{S}) := \{J^i\, E_{1,j}\, \left(M^{-i}\right)^t : s+1 \leq j \leq m, 0 \leq i \leq m-1\} \cup \{\, J^i\, \mathcal{E}(\gamma)\, \left(M^{-i}\right)^t : 0 \leq i \leq m-2, \gamma \in \mathcal{S}\},$$

where $E_{1,j}$ is the matrix with 1 in position $(1,j)$ and zeros elsewhere,

$$J := \left(\begin{array}{c|c} 0 & 1 \\ \hline I_{m-1} & 0 \end{array}\right) \quad \text{and} \quad \mathcal{E}(\gamma) := \left(\begin{array}{ccccc} \gamma^m & \gamma^{m-1} & \dots & \gamma & 1 \\ -\gamma^{m+1} & -\gamma^m & \dots & -\gamma^2 & -\gamma \\ \hline & & \mathbf{0} & & \end{array}\right).$$

RANK-METRIC CODES

Definition

A (**matrix rank-metric**) **code** is a subspace $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$. The **minimum** (**rank**) **distance** of a non-zero code $\mathcal{C}$ is $d(\mathcal{C}) := \min(\{\mathrm{rk}(M) : M \in \mathcal{C}, M \neq 0\})$ and for $\mathcal{C} := \{0\}$, we define $d(\mathcal{C})$ to be $n+1$.

RANK-METRIC CODES

Definition

A (**matrix rank-metric**) **code** is a subspace $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$. The **minimum** (**rank**) **distance** of a non-zero code $\mathcal{C}$ is $d(\mathcal{C}) := \min(\{\mathrm{rk}(M) : M \in \mathcal{C}, M \neq 0\})$ and for $\mathcal{C} := \{0\}$, we define $d(\mathcal{C})$ to be $n+1$.

It is well-know that the dual $\mathcal{C}^{\perp}$ of $\mathcal{C}$ is a code.

RANK-METRIC CODES

Definition

A (**matrix rank-metric**) **code** is a subspace $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$. The **minimum** (**rank**) **distance** of a non-zero code $\mathcal{C}$ is $d(\mathcal{C}) := \min(\{\mathrm{rk}(M) : M \in \mathcal{C}, M \neq 0\})$ and for $\mathcal{C} := \{0\}$, we define $d(\mathcal{C})$ to be $n+1$.

It is well-know that the dual $\mathcal{C}^\perp$ of $\mathcal{C}$ is a code.

Proposition (Kruskal - 1977)

We have that $\mathrm{trk}(\mathcal{C}) \geq \dim_{\mathbb{F}_q}(\mathcal{C}) + d(\mathcal{C}) - 1$.

Codes meeting this bound are called **MTR** (**Minimal Tensor Rank**).

$\mathbb{F}_{q^m}$-LINEAR RANK-METRIC CODES

Let $\Gamma := \{\gamma_1, \ldots, \gamma_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and $v \in \mathbb{F}_{q^m}^n$ and we define the map

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \xmapsto{\quad\quad\Gamma\quad\quad} \begin{pmatrix} v_{11} & \cdots & v_{1m} \\ \vdots & & \vdots \\ v_{n1} & \cdots & v_{nm} \end{pmatrix}.$$

This map is an $\mathbb{F}_q$-isomorphism.

Definition

A **vector (rank-metric) code** is a subspace $C \leq \mathbb{F}_{q^m}^n$. The **minimum distance** $d(C)$ of C is the minimum distance of $\Gamma(C)$ for any choice of a basis Γ of $\mathbb{F}_{q^m}/\mathbb{F}_q$.

GABIDULIN CODES

Definition

Let $k \in \{1, \dots, n\}$ and $\beta_1, \dots, \beta_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$. The $\mathbb{F}_{q^m}$**-linear Delsarte-Gabidulin code** $\mathcal{G}_k(\beta_1, \dots, \beta_n)$ is defined as

$$\mathcal{G}_k(\beta_1, \dots, \beta_n) := \{(f(\beta_1), \dots, f(\beta_n)) : f \in \mathcal{G}_k\},$$

where $\mathcal{G}_k := \left\{ f_0 x + f_1 x^q + \dots + f_{k-1} x^{q^{k-1}} : f_0, \dots, f_{k-1} \in \mathbb{F}_{q^m} \right\}$.

GABIDULIN CODES

Definition

Let $k \in \{1, \dots, n\}$ and $\beta_1, \dots, \beta_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$. The $\mathbb{F}_{q^m}$**-linear Delsarte-Gabidulin code** $\mathcal{G}_k(\beta_1, \dots, \beta_n)$ is defined as

$$\mathcal{G}_k(\beta_1, \dots, \beta_n) := \{(f(\beta_1), \dots, f(\beta_n)) : f \in \mathcal{G}_k\},$$

where $\mathcal{G}_k := \left\{ f_0 x + f_1 x^q + \cdots + f_{k-1} x^{q^{k-1}} : f_0, \dots, f_{k-1} \in \mathbb{F}_{q^m} \right\}$.

It was shown that $\mathcal{G}_k(\beta_1, \dots, \beta_n)$ has dimension k and minimum distance $n - k + 1$.

Proposition (Sheekey - 2016)

Let $\beta_1, \dots, \beta_n$ be elements of $\mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$. The dual of the code $\mathcal{G}_k(\beta_1, \dots, \beta_n)$ is equivalent to $\mathcal{G}_{n-k}(\beta_1, \dots, \beta_n)$.

AN EXAMPLE

Let $k = 1$ and α be a primitive element of $\mathbb{F}_{5^3}$. We have

$$\begin{aligned} C := \mathcal{G}_1(\alpha^4, \alpha^7) &= \left\{(f(\alpha^4), f(\alpha^7)) : f \in \{f_0 x : f_0 \in \mathbb{F}_5\}\right\} \\ &= \{f_0(\alpha^4, \alpha^7) : f_0 \in \mathbb{F}_5\} = \left\langle(\alpha^4, \alpha^7)\right\rangle_{\mathbb{F}_5}. \end{aligned}$$

Let $\Gamma := \{1, \alpha, \alpha^2\}$ be a $\mathbb{F}_5$-basis of $\mathbb{F}_{5^3}$, $N := \Gamma((\alpha^4, \alpha^7))$ and M the companion matrix of the minimal polynomial of α, i.e.

$$N := \begin{pmatrix} 0 & 2 & 2 \\ 3 & 2 & 3 \end{pmatrix}, \qquad M := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 2 & 0 \end{pmatrix}.$$

One can check that

$$\Gamma(C) = \left\langle N, N\, M, N\, M^2 \right\rangle_{\mathbb{F}_5} = \left\langle \begin{pmatrix} 0 & 2 & 2 \\ 3 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 4 & 2 \\ 1 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 3 & 4 \\ 4 & 0 & 4 \end{pmatrix} \right\rangle_{\mathbb{F}_5}.$$

GABIDULIN CODES

Proposition (Byrne, Neri, Ravagnani, Sheekey - 2019)

Let $q \geq m+n-2$, α be a primitive element of $\mathbb{F}_{q^m}$ and $\lambda \in \mathbb{F}_{q^m}$. For any $j \in \{0, \dots, m-1\}$, we have

$$\mathrm{trk}\left(\mathcal{G}_1\left(\lambda, \lambda\alpha^{q^j}, \dots, \lambda\alpha^{nq^j}\right)\right) = m+n-1$$

and, in particular, the code is MTR.

- If $n = m$ then 1-dimensional Gabidulin codes corresponds to the multiplication in $\mathbb{F}_{q^m}$. This is well studied problem in complexity theory.
- The tensor rank is invariant under equivalence but does not dualize.

DELSARTE-GABIDULIN CODES

Proposition (Byrne, C.)

Let $q \geq m$ and α be primitive element of $\mathbb{F}_{q^m}$. For any $j \in \{0, \dots, m-1\}$, we have

$$\mathrm{trk}(\mathcal{G}_1(1, \alpha^{q^j}, \dots, \alpha^{nq^j})^\perp) = nm - m + 1$$

and, in particular, $\mathcal{G}_1(1, \alpha^{q^j}, \dots, \alpha^{nq^j})^\perp$ is MTR. Moreover, an $(nm - m + 1)$-base for $\mathcal{G}_1(1, \alpha^{q^j}, \dots, \alpha^{nq^j})^\perp$ is

$$\begin{aligned} \mathcal{A}(\mathcal{S}) := &\{ Y_n J^i E_{1,m} (M^{-i})^t : 0 \leq i \leq n-1 \} \\ &\cup \{ Y_n J^i \mathcal{E}(\gamma) (M^{-i})^t : 0 \leq i \leq n-2, \gamma \in \mathcal{S} \}. \end{aligned}$$

where $\mathcal{S} := \{1, \gamma_1, \dots, \gamma_{m-2}\}$ is a set of distinct element of $\mathbb{F}_q \setminus \{0\}$.

FURTHER QUESTIONS

- Let $j \in \{0, \ldots, m-1\}$ and $n \notin \{2, 3\}$. Construct an $(n+m-1)$-base for the 1-dimensional Delsarte-Gabidulin code $\mathcal{G}_1(1, \alpha^{q^j}, \ldots, \alpha^{nq^j})$.
- Let $k \in \{2, \ldots, n-2\}$ and $4 < n \leq m$. Study the tensor rank of k-dimensional Delsarte-Gabidulin codes.
- Find new classes of MTR codes.

FURTHER QUESTIONS

- Let $j \in \{0, \dots, m-1\}$ and $n \notin \{2, 3\}$. Construct an $(n+m-1)$-base for the 1-dimensional Delsarte-Gabidulin code $\mathcal{G}_1(1, \alpha^{q^j}, \dots, \alpha^{nq^j})$.
- Let $k \in \{2, \dots, n-2\}$ and $4 < n \leq m$. Study the tensor rank of k-dimensional Delsarte-Gabidulin codes.
- Find new classes of MTR codes.

Bilinear Complexity of 3-Tensors Linked to Coding Theory
E. Byrne, G. Cotardo, arXiv: 2103.08544.