BILINEAR COMPLEXITY OF 3-TENSORS LINKED TO CODING THEORY

Giuseppe Cotardo
joint work with E. Byrne

UCD School of Mathematics and Statistics

GT Équipe GRACE

November 18th, 2021

OVERVIEW

- INTRODUCTION
  - WHAT IS COMPLEXITY?
  - 3-TENSORS
  - APPLICATIONS OF TENSOR DECOMPOSITION
- TENSOR RANK OF 3-TENSORS
  - TENSOR RANK OF 3-LAYER TENSORS
  - TENSOR RANK OF $(nm - s)$-LAYER TENSORS
- TENSOR RANK OF $\mathbb{F}_{q^m}$-LINEAR CODES

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.

- It is allowed to freely use the *intermediate results* once they are computed.
- A *computation* is said to be **finished** if the quantities that the computation is supposed to compute are among the *intermediate results*.

WHAT IS COMPLEXITY ?

- 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.

- **Lower bounds** can be often obtain by establishing relations between the complexity of the problem and the invariants of the appropriate structure (algebraic, topological, geometric or combinatorial).

- 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.

AN EXAMPLE: 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:

$$\begin{aligned} c_1 &= a_1 b_1 + a_2 b_3, \qquad & c_2 &= a_1 b_2 + a_2 b_4, \\ c_3 &= a_3 b_1 + a_4 b_3, \qquad & c_4 &= a_3 b_2 + a_4 b_4. \end{aligned}$$

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

AN EXAMPLE: MULTIPLICATION OF 2×2 MATRICES

We can compute $C = AB$ 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

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

It requires 7 **multiplications** and 18 **additions**.

AN EXAMPLE: MULTIPLICATION OF 2×2 MATRICES

Algorithm	# multiplications	# additions
standard	8	4
Strassen's	7	18

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).

LINEAR MAPS

Let A, B be vector spaces over the same field $\mathbb{K}$ and denote by A^* the **dual vector space** of A, i.e. $A^* := \{f : A \longrightarrow \mathbb{K} \mid f \text{ linear}\}$. For $\alpha \in A^*$ and $b \in B$, one can define a *rank one* linear map

$$\alpha \otimes b : A \longrightarrow B : a \longmapsto \alpha(a)b.$$

Definition

The **rank** $\tau(f)$ of a linear map $f : A \longrightarrow B$ is the smallest integer R such that there exist $\alpha_1, \ldots, \alpha_R \in A^*$ and $b_1, \ldots, b_R \in B$ such that

$$f = \sum_{i=1}^{R} \alpha_i \otimes b_i.$$

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.

Definition

A 3-**tensor** is an element of $\mathbb{K}^k \otimes \mathbb{K}^n \otimes \mathbb{K}^m$.

If $\{a_1, \ldots, a_k\}, \{b_1, \ldots, b_n\}, \{c_1, \ldots, c_m\}$ are bases of $\mathbb{K}^k, \mathbb{K}^n, \mathbb{K}^m$, respectively, then a basis for $\mathbb{K}^k \otimes \mathbb{K}^n \otimes \mathbb{K}^m$ is

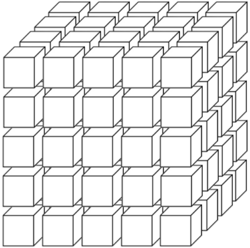
$$\{a_i \otimes b_j \otimes c_\ell : 1 \leq i \leq k, 1 \leq j \leq n, 1 \leq \ell \leq m\}.$$

In particular we have $\dim(\mathbb{K}^k \otimes \mathbb{K}^n \otimes \mathbb{K}^m) = \dim(\mathbb{K}^k)\dim(\mathbb{K}^n)\dim(\mathbb{K}^m) = knm$.

COORDINATE TENSORS

A tensor $X := \sum_r a_r \otimes b_r \otimes c_r$ can be represented as an array. That is as the map

$$X : \{1, \ldots, k\} \times \{1, \ldots, n\} \times \{1, \ldots, m\} \longrightarrow \mathbb{K}$$



given by $X = (X_{ij\ell} : 1 \leq i \leq k, 1 \leq j \leq n, 1 \leq \ell \leq m)$.

Therefore, X is related to the the 3-dimensional array

$$X_{ij\ell} = \sum_r a_{\ell r} b_{ir} c_{jr}.$$

$$a_r := (a_{\ell r} : 1 \leq \ell \leq k), b_r := (b_{ir} : 1 \leq i \leq n), c_r := (a_{jr} : 1 \leq j \leq m).$$

Remark

This representation of X is called **coordinate tensor** and allows to identify the space $\mathbb{K}^k \otimes \mathbb{K}^n \otimes \mathbb{K}^m$ with $\mathbb{K}^{k \times n \times m}$.

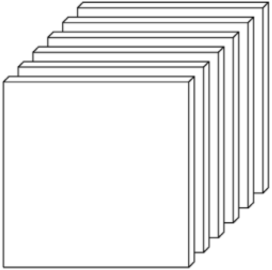
MATRIX REPRESENTATION

Consider the map $\mu : \mathbb{K}^k \times \mathbb{K}^{k\times n\times m} \longrightarrow \mathbb{K}^{k\times n\times m} : (v, X) \longmapsto \sum_r (v \cdot a_r) \otimes b_r \otimes c_r$, and notice that this map yields a 3-tensor of the form $\sum_r \lambda_r \otimes b_r \otimes c_r$, where $\lambda_r \in \mathbb{K}$, which can be identify as the 2-tensor $\sum_r \lambda_r b_r \otimes c_r$, since $\mathbb{K} \otimes \mathbb{K}^n$ and $\mathbb{K}^n$ are isomorphic.

As a consequence, we can identify the tensor X with the array of $n \times m$ matrices $X = (X_1 \mid \dots \mid X_k)$, where

$$X_s := \mu(e_s, X) = \sum_r (a_r)_s b_r \otimes c_r$$

and e_s is the s-th element of the canonical basis for $\mathbb{K}^k$, for all $1 \leq s \leq k$.



3 - TENSORS

Let $X = (X_1 \,|\, \dots \,|\, X_k) \in \mathbb{K}^{k \times n \times m}$ be a 3-tensor.

Definition

The **first slice space** $\mathrm{ss}_1(X)$ of X is defined as the span $\langle X_1, \dots, X_k \rangle$ over $\mathbb{K}$. We say that $\mathrm{ss}_1(X)$ is **nondegenerate** if $\dim(\mathrm{ss}_1(X)) = k$.

Definition

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 $X = a \otimes b \otimes c$.

Definition

The **tensor rank** $\mathrm{trk}(X)$ of X is defined as the smallest integer R such that X can be expressed as sum of R simple tensors.

PERFECT BASE

Let $X = (X_1 \,|\, \dots \,|\, X_k) \in \mathbb{K}^{k \times n \times m}$ be a 3-tensor.

Definition

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

$$\mathrm{ss}_1(X) \leq \langle A_1, \dots, A_R \rangle \, .$$

Lemma

The following are equivalent.

- $\mathrm{trk}(X) \leq R$.
- There exists an R-base for X.

AN EXAMPLE

Let $X \in \mathbb{F}_5^{2\times 2\times 2}$ be the 3-tensor defined as

$$X := \left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 1 & 3 & 1 \end{array}\right).$$

One can check that $\operatorname{trk}(X) = 3$ and a 3-base for X is given by

$$\mathcal{A} := \left\{ \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 4 \\ 2 & 4 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix} \right\}.$$

In particular, we have

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} + \begin{pmatrix} 2 & 4 \\ 2 & 4 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 \\ 3 & 1 \end{pmatrix} = 2\begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} + \begin{pmatrix} 2 & 4 \\ 2 & 4 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}$$

EQUIVALENT 3-TENSORS

Let $X = (X_1 \,|\, \ldots \,|\, X_k)$ and $Y = (Y_1 \,|\, \ldots \,|\, Y_k)$ be 3-tensors in $\mathbb{K}^{k \times n \times m}$.

Definition

We say that X, Y are **equivalent** if there exist $P \in \mathrm{GL}_n(\mathbb{K})$ and $Q \in \mathrm{GL}_m(\mathbb{K})$ such that $\mathrm{ss}_1(X) = P\,\mathrm{ss}_1(Y)\,Q := \{P\,N\,Q : N \in \mathrm{ss}_1(Y)\}$.

EQUIVALENT 3-TENSORS

Let $X = (X_1 \mid \ldots \mid X_k)$ and $Y = (Y_1 \mid \ldots \mid Y_k)$ be 3-tensors in $\mathbb{K}^{k\times n\times m}$.

Definition

We say that X, Y are **equivalent** if there exist $P \in \mathrm{GL}_n(\mathbb{K})$ and $Q \in \mathrm{GL}_m(\mathbb{K})$ such that $\mathrm{ss}_1(X) = P\,\mathrm{ss}_1(Y)\,Q := \{P\,N\,Q : N \in \mathrm{ss}_1(Y)\}$.

Remark

For any pair of matrices $P \in \mathrm{GL}_n(\mathbb{K})$ and $Q \in \mathrm{GL}_m(\mathbb{K})$, if $\mathcal{A}$ is a perfect base for X then $\{P\,A\,Q : A \in \mathcal{A}\}$ is a perfect base for the 3-tensor $P\,X\,Q$.

APPLICATIONS OF TENSOR DECOMPOSITION

- Cumulants
  (Statistics)
- Fluorescence spectroscopy
  (Chemistry)
- Interpretation of MRI
  (Medicine)
- Blind source separation
  (e.g. Cocktail Party Problem)
  (Digital Signal Processing)
- Storage and Encoding
  (Coding Theory)

$$K(t) = \sum_{i=0}^{\infty} \kappa_n \frac{t^n}{n!} = \mu t + \sigma^2 \frac{t^2}{2} + \cdots$$

APPLICATIONS OF TENSOR DECOMPOSITION

- Cumulants
  (Statistics)
- Fluorescence spectroscopy
  (Chemistry)
- Interpretation of MRI
  (Medicine)
- Blind source separation
  (e.g. Cocktail Party Problem)
  (Digital Signal Processing)
- Storage and Encoding
  (Coding Theory)

APPLICATIONS OF TENSOR DECOMPOSITION

- Cumulants
  (Statistics)
- Fluorescence spectroscopy
  (Chemistry)
- Interpretation of MRI
  (Medicine)
- Blind source separation
  (e.g. Cocktail Party Problem)
  (Digital Signal Processing)
- Storage and Encoding
  (Coding Theory)

APPLICATIONS OF TENSOR DECOMPOSITION

- Cumulants
  (Statistics)
- Fluorescence spectroscopy
  (Chemistry)
- Interpretation of MRI
  (Medicine)
- Blind source separation
  (e.g. Cocktail Party Problem)
  (Digital Signal Processing)
- Storage and Encoding
  (Coding Theory)

APPLICATIONS OF TENSOR DECOMPOSITION

- Cumulants
  (Statistics)
- Fluorescence spectroscopy
  (Chemistry)
- Interpretation of MRI
  (Medicine)
- Blind source separation
  (e.g. Cocktail Party Problem)
  (Digital Signal Processing)
- Storage and Encoding
  (Coding Theory)

APPLICATIONS OF TENSOR DECOMPOSITION

- Cumulants
  (Statistics)
- Fluorescence spectroscopy
  (Chemistry)
- Interpretation of MRI
  (Medicine)
- Blind source separation
  (e.g. Cocktail Party Problem)
  (Digital Signal Processing)
- Storage and Encoding
  (Coding Theory)

Low tensor rank 3-tensors perform well in terms of storage and encoding complexity!

ISSUES IN TENSOR DECOMPOSITION

- **Existence**: determine the rank of a tensor X.

ISSUES IN TENSOR DECOMPOSITION

- **Existence**: determine the rank of a tensor X.

Tensor rank is np-complete, *J. Håstad*
International Colloquium on Automata, Languages, and Programming, Springer, 1989.

ISSUES IN TENSOR DECOMPOSITION

- **Existence**: determine the rank of a tensor X.

  Tensor rank is np-complete, *J. Håstad*
  International Colloquium on Automata, Languages, and Programming, Springer, 1989.

- **Performing the decomposition**: find algorithms that exactly decompose a tensor X in terms of simple tensors.

ISSUES IN TENSOR DECOMPOSITION

- **Existence**: determine the rank of a tensor X.

  Tensor rank is np-complete, *J. Håstad*
  International Colloquium on Automata, Languages, and Programming, Springer, 1989.

- **Performing the decomposition**: find algorithms that exactly decompose a tensor X in terms of simple tensors.

- **Uniqueness**: it is an important issue with problems coming from spectroscopy and signal processing. If the rank is sufficiently small, uniqueness is assured with probability one.

ISSUES IN TENSOR DECOMPOSITION

- **Existence**: determine the rank of a tensor X.

  Tensor rank is np-complete, *J. Håstad*
  International Colloquium on Automata, Languages, and Programming, Springer, 1989.

- **Performing the decomposition**: find algorithms that exactly decompose a tensor X in terms of simple tensors.

- **Uniqueness**: it is an important issue with problems coming from spectroscopy and signal processing. If the rank is sufficiently small, uniqueness is assured with probability one.

- **Noise**: in order to talk about noise in data, we must have a distance function. In some applications, these functions come from science, in other case they are chosen by convenience. For example, in signal processing, assuming that the noise has a certain behaviour (iid or Gaussian) can determine a distance function.

TENSOR RANK OF 3-LAYER TENSORS

PRELIMINARIES AND NOTATION

In the following we let $2 \leq n \leq m$,

- $I_m \in \mathbb{K}^{m\times m}$ be the $m \times m$ identity matrix,
- $Y_n \in \mathbb{K}^{n\times m}$ be the matrix $Y_n := \left(\begin{array}{c|c} I_n & 0 \end{array} \right)$,
- $E_{i,j} \in \mathbb{K}^{n\times m}$ be the matrix with 1 is position (i,j) and 0 elsewhere,
- $M \in \mathbb{K}^{m\times m}$ be the matrix

$$M := \left(\begin{array}{c|c} 0 & I_{m-1} \\ \hline a_1 & a_2 \ldots a_m \end{array} \right).$$

PRELIMINARIES AND NOTATION

In the following we let $2 \leq n \leq m$,

- $I_m \in \mathbb{K}^{m\times m}$ be the $m \times m$ identity matrix,
- $Y_n \in \mathbb{K}^{n\times m}$ be the matrix $Y_n := \left(\begin{array}{c|c} I_n & 0 \end{array} \right)$,
- $E_{i,j} \in \mathbb{K}^{n\times m}$ be the matrix with 1 is position (i,j) and 0 elsewhere,
- $M \in \mathbb{K}^{m\times m}$ be the matrix

$$M := \left(\begin{array}{c|c} 0 & I_{m-1} \\ \hline a_1 & a_2 \dots a_m \end{array} \right).$$

Theorem (Jaja - 1979)

Let $|\mathbb{K}| \geq m$. We have that the tensor rank of $(I\,|\,M) \leq \mathbb{K}^{2\times m\times m}$ is m if M is diagonalizable and $m+1$ otherwise.

Let $X := (\, I \mid M \mid M^{-1}\,) \in \mathbb{K}^{k\times n\times m}$ be a 3-tensor.

Theorem (Byrne, C.)

Let $|\mathbb{K}| \geq m+1$ and let $f = (x-\alpha_1)\,\cdots\,(x-\alpha_{m-\deg(g)})\,g \in \mathbb{K}[x]$ be the characteristic polynomial of M, where $\deg(g) \leq 1$ or $\deg(g) \geq 2$ and g is not decomposable into linear factors. There exist $P \in \mathrm{GL}_m(\mathbb{K})$ and $A, B \in \mathbb{K}^{m\times m}$ of rank 1 such that the following hold.

(1) If $0 \leq \deg(g) \leq 1$ then an m-base of X is $\{P^{-1}E_{i,i}P : i \in [m]\}$.

(2) If $\deg(g) = 2$ then an $(m+1)$-base of X is $\{P^{-1}E_{i,i}P : i \in [m]\} \cup \{A\}$.

(3) If $\deg(g) \geq 3$ then an $(m+2)$-base of X is $\{P^{-1}E_{i,i}P : i \in [m]\} \cup \{A, B\}$.

AN EXAMPLE

Let $f := (x-1)g$, where $g := x^3+3x+3$ is irreducible over $\mathbb{F}_5$, and $h := (x-2)(x-3)(x-4)$ be polynomials in $\mathbb{F}_5[x]$. Let

$$M := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 3 & 0 & 2 & 1 \end{pmatrix}, \qquad M_g := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 2 & 0 \end{pmatrix}, \qquad M_h := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 4 & 4 & 4 \end{pmatrix}$$

be the companion matrices of f, g and h respectively. Let $\overline{Q} \in \mathrm{GL}_3(\mathbb{F}_5)$ and $Q, P \in \mathrm{GL}_4(\mathbb{F}_5)$ be such that $\overline{Q}M_h\overline{Q}^{-1} = \mathrm{diag}(4,3,2)$, $Q := \mathrm{diag}(1, \overline{Q})$ and $PMP^{-1} = \mathrm{diag}(1, M_g)$, i.e.

$$Q := \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & \overline{Q} \end{array}\right) = \left(\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 1 \\ 0 & 3 & 4 & 1 \\ 0 & 2 & 3 & 1 \end{array}\right), \qquad P := \begin{pmatrix} 3 & 3 & 0 & 1 \\ 4 & 1 & 0 & 0 \\ 0 & 4 & 1 & 0 \\ 0 & 0 & 4 & 1 \end{pmatrix}.$$

AN EXAMPLE

Define

$$D_1 := \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & M_g - M_h \end{array}\right), \qquad D_2 := \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & M_g^{-1} - M_h^{-1} \end{array}\right).$$

We have that an 6-base for $(\, I_4 \mid M \mid M^{-1}\,)$ is given by

$$\mathcal{A} := \{P^{-1}\, Q^{-1}\, E_{i,i}\, Q\, P : i \in \{1, \dots, 4\}\} \cup \{P^{-1}\, D_1\, P,\ P^{-1}\, D_2\, P\}$$

that is

$$\mathcal{A} = \left\{ \begin{pmatrix} 4 & 4 & 0 & 3 \\ 4 & 4 & 0 & 3 \\ 4 & 4 & 0 & 3 \\ 4 & 4 & 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 1 & 4 \\ 3 & 2 & 3 & 2 \\ 1 & 4 & 1 & 4 \\ 3 & 2 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 4 & 3 \\ 4 & 3 & 1 & 2 \\ 3 & 1 & 2 & 4 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 4 & 2 & 1 & 3 \\ 2 & 1 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 0 & 4 & 2 \\ 4 & 0 & 4 & 2 \\ 4 & 0 & 4 & 2 \\ 1 & 0 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 2 & 1 & 2 \\ 0 & 1 & 3 & 1 \\ 0 & 1 & 3 & 1 \\ 0 & 1 & 3 & 1 \end{pmatrix} \right\}.$$

Let $n \in \{2,3\}$ and $X := \left(Y_n M^{-1} \mid Y_n \mid Y_n M \mid \cdots \mid Y_n M^{m-2} \right) \in \mathbb{K}^{k \times n \times m}$.

Corollary (Byrne, C.)

Let $|\mathbb{K}| \geq m+1$, $n \in \{2,3\}$, and let $f = (x-\alpha) \cdots (x - \alpha_{m-\deg(g)})\, g \in \mathbb{K}[x]$ be the characteristic polynomial of M, where $\deg(g) \leq 1$ or $\deg(g) \geq 2$ and g is not decomposable into linear factors. There exist $P \in \mathrm{GL}_m(\mathbb{K})$ and $A, B \in \mathbb{K}^{m \times m}$ such that the following hold.

(1) If $0 \leq \deg(g) \leq 1$ then $\{Y_n P^{-1} E_{i,i} P : 1 \leq i \leq m\}$ is a m-base of X.

(2) If $\deg(g) = 2$ then $\{Y_n P^{-1} E_{i,i} P : 1 \leq i \leq m\} \cup \{Y_n A\}$ is an $(m+1)$-base of X.

(3) If $\deg(g) \geq 3$ then $\{Y_n P^{-1} E_{i,i} P : 1 \leq i \leq m\} \cup \{Y_n A, Y_n B\}$ is an $(m+2)$-base of X.

TENSOR RANK OF $(nm-2)$-LAYER TENSORS

Theorem (Atkinson, Lloyd - 1983)

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

Inspired by this result, we show that, for any $s \in \{1, \ldots, m-1\}$, the tensor rank of the *dual* of some families of s-layer tensors in $\mathbb{K}^{s\times n\times m}$ is $mn-s$ and we give and explicit construction for an $(mn - s)$-base for such tensors.

PRELIMINARIES AND NOTATION

Definition

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

Definition (Atkinson, Lloyd - 1983)

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

Definition

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

Definition (Atkinson, Lloyd - 1983)

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

Let $\gamma \in \mathbb{K} \setminus \{0\}$. We denote by J and $\mathcal{E}(\gamma)$ the matrices of $\mathbb{K}^{m\times m}$ defined as

$$J := \left(\begin{array}{c|c} 0 & 1 \\ \hline I_{m-1} & 0 \end{array}\right), \qquad \mathcal{E}(\gamma) := \left(\begin{array}{ccccc} \gamma^m & \gamma^{m-1} & \cdots & \gamma & 1 \\ -\gamma^{m+1} & -\gamma^m & \cdots & -\gamma^2 & -\gamma \\ \hline \multicolumn{5}{c}{\text{\Large 0}} \end{array}\right).$$

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 invertible. Then

$$\langle I_m, M, \dots, M^{s-1} \rangle^{\perp} \leq \mathbb{K}^{m \times m}$$

is perfect and an $(m^2 - s)$-base is

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

PROOF FOR $\left\langle I_m, M, M^2 \right\rangle^{\perp}$

Let $|\mathbb{K}| \geq 4$ and $\mathcal{S} := \{1, \alpha, \beta\}$ be a set of distinct elements of $\mathbb{K} \setminus \{0\}$. Define the set $\mathcal{A} := \{A_i : 1 \leq i \leq 13\}$, where

$$A_1 := \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad A_2 := \begin{pmatrix} \alpha^3 & \alpha^2 & \alpha & 1 \\ -\alpha^4 & -\alpha^3 & -\alpha^2 & -\alpha \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad A_3 := \begin{pmatrix} \beta^3 & \beta^2 & \beta & 1 \\ -\beta^4 & -\beta^3 & -\beta^2 & -\beta \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad A_4 := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

and the remaining matrices of $\mathcal{A}$ are

$$\begin{aligned} A_5 &:= J A_1 \left(M^{-1}\right)^t, & A_6 &:= J A_2 \left(M^{-1}\right)^t, & A_7 &:= J A_3 \left(M^{-1}\right)^t, \\ A_8 &:= J A_4 \left(M^{-1}\right)^t, & A_9 &:= J^2 A_1 \left(M^{-2}\right)^t, & A_{10} &:= J^2 A_2 \left(M^{-2}\right)^t, \\ A_{11} &:= J^2 A_3 \left(M^{-2}\right)^t, & A_{12} &:= J^2 A_4 \left(M^{-2}\right)^t, & A_{13} &:= J^3 A_4 \left(M^{-3}\right)^t. \end{aligned}$$

We want to show that $\mathcal{A}$ is a 13-base for $\left\langle I, M, M^2 \right\rangle^{\perp}$.

PROOF FOR $\langle I_m, M, M^2 \rangle^{\perp}$

Split $\mathcal{A}$ in the following disjoint subsets.

$$\mathcal{A}_0 := \{A_1, A_2, A_3, A_4\}, \quad \mathcal{A}_1 := \{A_5, A_6, A_7, A_8\}, \quad \mathcal{A}_2 := \{A_9, A_{10}, A_{11}, A_{12}\}, \quad \mathcal{A}_3 := \{A_{13}\}.$$

Define the matrices B_i's whose rows are the vector representation of the non-zero rows of the matrices in $\mathcal{A}_i$, for $0 \leq i \leq 3$. We have

$$B_0 := \left(\; B_0^{(1)} \; \middle| \; B_0^{(2)} \; \right) = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ \alpha^3 & \alpha^2 & \alpha & 1 & -\alpha^4 & -\alpha^3 & -\alpha^2 & \alpha \\ \beta^3 & \beta^2 & \beta & 1 & -\beta^4 & \beta^3 & \beta^2 & \beta \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array} \right),$$

$$B_1 := \left(\; B_0^{(1)} \left(M^{-1}\right)^t \; \middle| \; B_0^{(2)} \left(M^{-1}\right)^t \; \right)$$

$$B_2 := \left(\; B_0^{(1)} \left(M^{-2}\right)^t \; \middle| \; B_0^{(2)} \left(M^{-2}\right)^t \; \right)$$

$$B_3 := \left(\; \overline{B_0}^{(1)} \left(M^{-3}\right)^t \; \right) = \left(\; c_4 \quad b_4 \quad a_4 \quad 0 \; \right)$$

PROOF FOR $\langle I_m, M, M^2 \rangle^{\perp}$

Let B the matrix whose rows are the vector representation of the matrices in $\mathcal{A}$. Therefore, we can observe that

$$B = \begin{pmatrix} B_0^{(1)} & B_0^{(2)} & & 0 \\ & B_0^{(1)}\left(M^{-1}\right)^t & B_0^{(2)}\left(M^{-1}\right)^t & \\ & & B_0^{(1)}\left(M^{-2}\right)^t & B_0^{(2)}\left(M^{-2}\right)^t \\ 0 & & & \overline{B_0}^{(1)}\left(M^{-3}\right)^t \end{pmatrix}$$

and

$$\mathrm{rk}(B) = \mathrm{rk}\left(B_0^{(1)}\right) + \mathrm{rk}\left(B_0^{(1)}\left(M^{-1}\right)^t\right) + \mathrm{rk}\left(B_0^{(1)}\left(M^{-2}\right)^t\right) + \mathrm{rk}\left(\overline{B_0}^{(1)}\left(M^{-3}\right)^t\right) = 13.$$

Corollary (Byrne, C.)

Let $s \in \{1, \dots m-1\}$, $|\mathbb{K}| \geq s+1$ and $\mathcal{S} := \{1, \gamma_1, \dots, \gamma_{s-1}\}$ be a set of distinct elements of $\mathbb{K} \setminus \{0\}$. Then $\langle Y_n, Y_n M, \dots, Y_n M^{s-1} \rangle^{\perp} \leq \mathbb{K}^{n \times m}$ is perfect and an $(nm-s)$-base is

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

Corollary (Byrne, C.)

Let $s \in \{1, \dots m-1\}$, $|\mathbb{K}| \geq s+1$ and $\mathcal{S} := \{1, \gamma_1, \dots, \gamma_{s-1}\}$ be a set of distinct elements of $\mathbb{K} \setminus \{0\}$. Then $\langle Y_n, Y_n M, \dots, Y_n M^{s-1} \rangle^{\perp} \leq \mathbb{K}^{n \times m}$ is perfect and an $(nm-s)$-base is

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

Proposition (Byrne, C.)

Let $M \in \mathbb{K}^{2 \times 2}$. Then $\langle I_2, M \rangle^{\perp}$ is perfect if $M_{2,1} = 0$ and $M_{2,2} \neq 0$ or $M_{2,1} \neq 0$ and the polynomial $M_{2,1} x^2 + M_{2,2} x - 1 \in \mathbb{K}[x]$ has two distinct roots in $\mathbb{K} \setminus \{0\}$.

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

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.

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 with equality are called **MTR** (**Minimal Tensor Rank**).

Let $\Gamma := \{\gamma_1, \ldots, \gamma_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and $v \in \mathbb{F}_{q^m}^n$. We define by $\Gamma(v) \in \mathbb{F}_q^{n\times m}$ the vector defined by

$$v_i = \sum_{j=1}^{m} \Gamma(v)_{i,j}\, \gamma_j.$$

The map $v \mapsto \Gamma(v)$ is an $\mathbb{F}_q$-isomorphism. Moreover, for a subspace V of $\mathbb{F}_{q^m}^n$, we define $\Gamma(V) := \{\Gamma(v) : v \in V\}$.

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 $\mathbb{F}_{q^m}/\mathbb{F}_q$.

Proposition

A vector code C is MTR if and only if $\mathrm{trk}(C) = \dim_{\mathbb{F}_q}(C) + d(C) - 1$.

Proposition

A vector code C is MTR if and only if $\mathrm{trk}(C) = \dim_{\mathbb{F}_q}(C) + d(C) - 1$.

Proposition (Byrne, C.)

Let s be a positive integer such that $1 \leq s \leq n$. Let $\beta_1, \dots, \beta_n \in \mathbb{F}_{q^m}$ such that $\langle \beta_1, \dots, \beta_n \rangle_{\mathbb{F}_q}$ has dimension s. Suppose that $\langle \beta_1, \dots, \beta_n \rangle_{\mathbb{F}_q} = \langle \beta_1, \dots, \beta_s \rangle_{\mathbb{F}_q}$, then we have

$$\mathrm{trk}\left(\langle (\beta_1, \beta_2, \dots, \beta_n) \rangle_{\mathbb{F}_q}\right) = \mathrm{trk}\left(\langle (\beta_1, \beta_2, \dots, \beta_s) \rangle_{\mathbb{F}_q}\right).$$

Theorem (Byrne, C.)

Let $q \geq m+n-k-1$, α be a primitive element of $\mathbb{F}_{q^m}$, $\lambda_1, \dots, \lambda_k \in \mathbb{F}_{q^m}$ and let $V \leq \mathbb{F}_{q^m}^n$ be the k-dimensional space given by the row-space of

$$G := \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 & \lambda_1\,\alpha & \cdots & \lambda_1\,\alpha^{n-k} \\ 0 & \lambda_2 & \cdots & 0 & \lambda_2\,\alpha^q & \cdots & \lambda_2\,\alpha^{q(n-k)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \lambda_k & \lambda_k\,\alpha^{q^k} & \cdots & \lambda_k\,\alpha^{q^k(n-k)} \end{pmatrix} \in \mathbb{F}_{q^m}^{k\times n},$$

We have that $\mathrm{trk}(V) \leq k(m+n-k)$.

DELSARTE-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** $\mathcal{G}_k$ is defined as

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

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

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** $\mathcal{G}_k$ is defined as

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

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

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

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

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

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

DELSARTE-GABIDULIN CODES

Proposition (Byrne, Neri, Ravagnani, Sheekey - 2019)
Let $q \geq m+n-2$ and α be primitive element of $\mathbb{F}_{q^m}$. For any integer $j \in \{0,\ldots,m-1\}$, we have

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

and, in particular, $\mathcal{G}_1(1,\alpha^{q^j},\ldots,\alpha^{nq^j})$ is MTR.

DELSARTE-GABIDULIN CODES

Proposition (Byrne, Neri, Ravagnani, Sheekey - 2019)
Let $q \geq m+n-2$ and α be primitive element of $\mathbb{F}_{q^m}$. For any integer $j \in \{0,\dots,m-1\}$, we have

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

and, in particular, $\mathcal{G}_1(1,\alpha^{q^j},\dots,\alpha^{nq^j})$ is MTR.

Proposition (Byrne, C.)
Let $q \geq m+n-2$ and $n \in \{2,3\}$. Let α be primitive element of $\mathbb{F}_{q^m}$ and $j \in \{0,\dots,m-1\}$. There exist $P \in \mathrm{GL}_m(\mathbb{F}_q)$ and $A, B \in \mathbb{F}_q^{n\times m}$ of rank 1 such that an $(m+n-1)$-base for $\mathcal{G}_1(1,\alpha^{q^j},\dots,\alpha^{nq^j})$ is

(1) $\{Y_n P^{-1} E_{i,i} P : 1 \leq i \leq m\} \cup \{A\}$ if $n=2$;

(2) $\{Y_n P^{-1} E_{i,i} P : 1 \leq i \leq m\} \cup \{A, B\}$ if $n=3$;

Proposition (Byrne, C.)

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

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

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

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

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

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 $k \in \{2, \dots, n-2\}$. Study the tensor rank of k-dimensional Delsarte-Gabidulin codes.
- Find new classes of MTR codes.

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 $k \in \{2, \ldots, n-2\}$. 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.