Evaluation Subspace Codes and Convolutional Codes

Joachim Rosenthal
University of Zürich

MTNS 2022 in Bayreuth
September 13, 2022

University of Zurich

Outline

Subspace Codes

Definition

Denote by $\mathcal{P}(n)$ the set of all linear subspaces inside the vector space $\mathbb{F}_q^n$.

Subspace Codes

Definition

Denote by $\mathcal{P}(n)$ the set of all linear subspaces inside the vector space $\mathbb{F}_q^n$.

Definition

On $\mathcal{P}(n)$ define a metric through:

$$d_S(V, W) := \dim(V + W) - \dim(V \cap W).$$

Subspace Codes

Definition

Denote by $\mathcal{P}(n)$ the set of all linear subspaces inside the vector space $\mathbb{F}_q^n$.

Definition

On $\mathcal{P}(n)$ define a metric through:

$$d_S(V, W) := \dim(V + W) - \dim(V \cap W).$$

Remark

Check that the map: $d_S : \mathcal{P}(n) \times \mathcal{P}(n) \to \mathbb{N}_+$ defines a metric on $\mathcal{P}(n)$.

Subspace Codes for Linear Network Codes

Definition

A subset $\mathcal{C}$ of $\mathcal{P}(n)$ will be called a subspace code.

Subspace Codes for Linear Network Codes

Definition

A subset $\mathcal{C}$ of $\mathcal{P}(n)$ will be called a subspace code.

Definition

In the usual way one defines the distance of the subspace code $\mathcal{C} \subset \mathcal{P}(n)$ through:

$$\mathrm{dist}(\mathcal{C}) := \min \{ d_S(V, W) \mid V, W \in \mathcal{C},\ V \neq W \}$$

and the size of $\mathcal{C}$ as $M := |\mathcal{C}|$.

Subspace Codes for Linear Network Codes

Definition

A subset $\mathcal{C}$ of $\mathcal{P}(n)$ will be called a subspace code.

Definition

In the usual way one defines the distance of the subspace code $\mathcal{C} \subset \mathcal{P}(n)$ through:

$$\mathrm{dist}(\mathcal{C}) := \min \{ d_S(V, W) \mid V, W \in \mathcal{C},\ V \neq W \}$$

and the size of $\mathcal{C}$ as $M := |\mathcal{C}|$.

Remark

As always one has as a goal to construct for any natural numbers n, M and any finite field $\mathbb{F}_q$ codes having maximal distance d and efficient decoding algorithms.

Induced Metric on the the Grassmannian $\mathrm{G}(k, \mathbb{F}_q^n)$

Definition

In the sequel we will assume that a subspace code is a subset of the Grassmannian $\mathrm{G}(k, \mathbb{F}_q^n)$. We call such codes also constant-dimension codes.

Induced Metric on the the Grassmannian $\mathrm{G}(k, \mathbb{F}_q^n)$

Definition

In the sequel we will assume that a subspace code is a subset of the Grassmannian $\mathrm{G}(k, \mathbb{F}_q^n)$. We call such codes also constant-dimension codes.

Definition

The metric on $\mathcal{P}(n)$ induces a metric on the Grassmannian $\mathrm{G}(k, \mathbb{F}_q^n)$:

$$d_S(V, W) := \dim(V + W) - \dim(V \cap W)$$

Induced Metric on the the Grassmannian $\mathrm{G}(k, \mathbb{F}_q^n)$

Definition

In the sequel we will assume that a subspace code is a subset of the Grassmannian $\mathrm{G}(k, \mathbb{F}_q^n)$. We call such codes also constant-dimension codes.

Definition

The metric on $\mathcal{P}(n)$ induces a metric on the Grassmannian $\mathrm{G}(k, \mathbb{F}_q^n)$:

$$d_S(V, W) := \dim(V + W) - \dim(V \cap W)$$

Remark

The main constant-dimension subspace coding problem is: For every size M construct codes $\mathcal{C} \subset \mathrm{G}(k, \mathbb{F}_q^n)$ having maximal possible distance.

Fundamental Research Questions

- For every finite field and positive integers d, k, n find the maximum number of subspaces in the Grassmannian $\mathrm{G}(k, \mathbb{F}_q^n)$ such that this code has distance d.

Fundamental Research Questions

- For every finite field and positive integers d, k, n find the maximum number of subspaces in the Grassmannian $\mathrm{G}(k, \mathbb{F}_q^n)$ such that this code has distance d.
- Find constructions of codes together with efficient decoding algorithms.

Evaluation Codes in the Theory of Block Codes

Let X be a curve (or a variety) defined over the finite field $\mathbb{F}_q$. Let G be a divisor and let $(P_1, \ldots, P_n)$ be n distinct points on X and define the divisor $P := P_1 + \cdots + P_n$. We assume that the supports of G and P are disjoint.

Evaluation Codes in the Theory of Block Codes

Let X be a curve (or a variety) defined over the finite field $\mathbb{F}_q$. Let G be a divisor and let $(P_1, \ldots, P_n)$ be n distinct points on X and define the divisor $P := P_1 + \cdots + P_n$. We assume that the supports of G and P are disjoint.

Definition

Consider the Riemann-Roch space $L(G)$. The evaluation code, or function code, is defined as the image under the map

$$\begin{array}{rcc} \varphi : L(G) & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

Evaluation Codes in the Theory of Block Codes

Let X be a curve (or a variety) defined over the finite field $\mathbb{F}_q$. Let G be a divisor and let $(P_1, \ldots, P_n)$ be n distinct points on X and define the divisor $P := P_1 + \cdots + P_n$. We assume that the supports of G and P are disjoint.

Definition

Consider the Riemann-Roch space $L(G)$. The evaluation code, or function code, is defined as the image under the map

$$\begin{array}{rcc} \varphi : L(G) & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

Remark

The importance of evaluation codes was recognized by Valery Goppa in 1972 and algebraic geometric Goppa codes belong to the most important classes of codes.

Aim for a construction

Like in Goppa's construction of algebraic geometric codes

$$\begin{array}{rcl} \varphi : L(G) & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

wee seek:

University of Zurich

Aim for a construction

Like in Goppa's construction of algebraic geometric codes

$$\begin{array}{rcl} \varphi : L(G) & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

wee seek:

- A variety X.

University of Zurich

Aim for a construction

Like in Goppa's construction of algebraic geometric codes

$$\begin{array}{rcc} \varphi : L(G) & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

wee seek:

- A variety X.
- A morphism
$$\varphi : X \longrightarrow \mathrm{G}(k, \mathbb{F}_q^n),$$
such that the image is a subspace code having excellent distance.

Hermann Martin map

It was an important contribution of [MH78] that every linear system defines in a natural way a curve of genus zero in a Grassmann variety. One often calls the resulting curve the Hermann-Martin curve induced by the linear system.

University of Zurich

Hermann Martin map

It was an important contribution of [MH78] that every linear system defines in a natural way a curve of genus zero in a Grassmann variety. One often calls the resulting curve the Hermann-Martin curve induced by the linear system.

Definition

Let $G(s)$ be a $k \times m$ transfer function and consider the map

$$h: \ \mathbb{K} \longrightarrow \mathrm{G}(k, \mathbb{K}^{k+m}), \ s \mapsto \mathrm{rowspace}_{\mathbb{K}}[I_k \ \ G(s)]. \tag{1}$$

Then h is called the Hermann-Martin map *associated to the transfer function $G(s)$.*

Evaluation of Hermann Martin Curves

In the sequel assume that the base field is the finite field $\mathbb{F}$. If $G(s)$ is a transfer function having the left coprime factorization $G(s) = D^{-1}(s)N(s)$ then we know from systems theory that $\mathrm{rowspace}_{\mathbb{K}}[D(\alpha)\ N(\alpha)]$ has full row rank for all elements α in any extension field of $\mathbb{F}$.

University of Zurich

Evaluation of Hermann Martin Curves

In the sequel assume that the base field is the finite field $\mathbb{F}$. If $G(s)$ is a transfer function having the left coprime factorization $G(s) = D^{-1}(s)N(s)$ then we know from systems theory that $\mathrm{rowspace}_{\mathbb{K}}[D(\alpha)\ N(\alpha)]$ has full row rank for all elements α in any extension field of $\mathbb{F}$.

Based on this observation one can define a subspace code through:

$$\{\mathrm{rowspace}_{\mathbb{K}}[D(\alpha)\ N(\alpha)] \mid \alpha \in \mathbb{K}\}\,, \tag{2}$$

where $\mathbb{K} = \mathbb{F}_{q^m}$ is a finite extension field of $\mathbb{F}$.

University of Zurich

Evaluation of Hermann Martin Curves

In the sequel assume that the base field is the finite field $\mathbb{F}$. If $G(s)$ is a transfer function having the left coprime factorization $G(s) = D^{-1}(s)N(s)$ then we know from systems theory that $\mathrm{rowspace}_{\mathbb{K}}[D(\alpha)\ N(\alpha)]$ has full row rank for all elements α in any extension field of $\mathbb{F}$.
Based on this observation one can define a subspace code through:

$$\{\mathrm{rowspace}_{\mathbb{K}}[D(\alpha)\ N(\alpha)] \mid \alpha \in \mathbb{K}\}, \tag{2}$$

where $\mathbb{K} = \mathbb{F}_{q^m}$ is a finite extension field of $\mathbb{F}$.
Of course note that the resulting subspace code is a subspace code in the Grassmannian $\mathrm{G}(k, \mathbb{K}^n)$ defined over the extension field. It is also not clear how good the codes can be if one does such an evaluation.

Spread inside $\mathrm{G}(k, \mathbb{F}_q^n)$

Definition

$S \subset \mathrm{G}(k, \mathbb{F}_q^n)$ is a spread of $\mathbb{F}_q^n$ if:

- *$V \cap W = \{0\}$ for all $V, W \in S$, and*
- *for any $v \in \mathbb{F}_q^n$, $v \neq 0$, exists unique $V \in S$ such that $v \in V$.*

University of Zurich

Spread inside $\mathrm{G}(k, \mathbb{F}_q^n)$

Definition

$S \subset \mathrm{G}(k, \mathbb{F}_q^n)$ is a spread of $\mathbb{F}_q^n$ if:

- *$V \cap W = \{0\}$ for all $V, W \in S$, and*
- *for any $v \in \mathbb{F}_q^n$, $v \neq 0$, exists unique $V \in S$ such that $v \in V$.*

Question

Spreads exist for every choice of k and n?

Spread inside $\mathrm{G}(k, \mathbb{F}_q^n)$

Definition

$S \subset \mathrm{G}(k, \mathbb{F}_q^n)$ is a spread of $\mathbb{F}_q^n$ if:

- *$V \cap W = \{0\}$ for all $V, W \in S$, and*
- *for any $v \in \mathbb{F}_q^n$, $v \neq 0$, exists unique $V \in S$ such that $v \in V$.*

Question

Spreads exist for every choice of k and n?

Theorem

There exists a spread $S \subset \mathrm{G}(k, \mathbb{F}_q^n)$ if and only if $k \mid n$.

University of Zurich

Spread Codes

Setting:

- $n, k, r \in \mathbb{N}_+$ such that $n = kr$;
- $p \in \mathbb{F}_q[x]$ irreducible of degree k and $P \in Mat_{k\times k}(\mathbb{F}_q)$ its companion matrix;
- $\mathbb{F}_q[P] \subset GL_k(\mathbb{F}_q)$, $\mathbb{F}_q[P] \cong \mathbb{F}_{q^k}$.

Spread Codes

Setting:

- $n, k, r \in \mathbb{N}_+$ such that $n = kr$;
- $p \in \mathbb{F}_q[x]$ irreducible of degree k and $P \in Mat_{k\times k}(\mathbb{F}_q)$ its companion matrix;
- $\mathbb{F}_q[P] \subset GL_k(\mathbb{F}_q)$, $\mathbb{F}_q[P] \cong \mathbb{F}_{q^k}$.

Theorem

The collection of subspaces

$$\mathcal{S} := \bigcup_{i=1}^{r} \{\mathrm{rowsp}\,[0_k \;\; \cdots \;\; 0_k \;\; I_k \;\; A_{i+1} \;\; \cdots \;\; A_r] \mid A_{i+1}, \ldots, A_r \in \mathbb{F}_q[P]\}$$

is a subset of $\mathrm{G}(k, \mathbb{F}_q^n)$ *and a spread of* $\mathbb{F}_q^n$.

Definition and Properties

Definition

The set $\mathcal{S}$ constructed as in the previous slide will be called a Spread Codes of $\mathrm{G}(k, \mathbb{F}_q^n)$.

Definition and Properties

Definition

The set $\mathcal{S}$ constructed as in the previous slide will be called a Spread Codes of $\mathrm{G}(k, \mathbb{F}_q^n)$.

Properties:

- MDS-like for the distance $d = 2k$.
- every nonzero vector of $\mathbb{F}_q^n$ belong to one and only one code-word.

University of Zurich

Constructing spreads from permutation rational maps

As before let $p \in \mathbb{F}_q[x]$ be irreducible of degree k and $P \in Mat_{k\times k}(\mathbb{F}_q)$ its companion matrix. Let

$$\psi : \mathbb{F}_{q^k} \longrightarrow \mathbb{F}_q[P]$$

be the induced isomorphism.

Constructing spreads from permutation rational maps

As before let $p \in \mathbb{F}_q[x]$ be irreducible of degree k and $P \in Mat_{k\times k}(\mathbb{F}_q)$ its companion matrix. Let

$$\psi : \mathbb{F}_{q^k} \longrightarrow \mathbb{F}_q[P]$$

be the induced isomorphism.

Definition

A permutation rational map over the field $\mathbb{F}_{q^k}$ is a bijectiove map

$$\begin{array}{cccc} \rho : \mathbb{P}^1_{\mathbb{F}_{q^k}} & \longrightarrow & : \mathbb{P}^1_{\mathbb{F}_{q^k}} \\ (s,t) & \longmapsto & (\rho_1(s,t)), \rho_2(s,t)) \end{array},$$

where ρ_1, ρ_2 are both homogeneous polynomials of the same degree.

Constructing spreads from permutation rational maps

Remark

permutation rational maps naturally generalize permutation polynomials and Ferraguti and Micheli recently provided some classification.

Constructing spreads from permutation rational maps

Remark

permutation rational maps naturally generalize permutation polynomials and Ferraguti and Micheli recently provided some classification.

Theorem

Let ρ be a permutation rational map. Then the morphism

$$\begin{array}{rcc} \rho : \mathbb{P}^1_{\mathbb{F}_{q^k}} & \longrightarrow & \mathrm{G}(k, \mathbb{F}_q^{2k}), \\ (s,t) & \longmapsto & \mathrm{rowsp}(\psi(\rho_1(s,t)), \psi(\rho_2(s,t))) \end{array},$$

defines a spread code.

Constructing spreads from permutation morphisms

Definition

A permutation morphism over the field $\mathbb{F}_{q^k}$ is a bijectiove map

$$\begin{array}{rcl} \rho : \mathbb{P}^m_{\mathbb{F}_{q^k}} & \longrightarrow & : \mathbb{P}^m_{\mathbb{F}_{q^k}} \\ (s_1, \ldots, s_{m+1}) & \longmapsto & (\rho_1(s_1, \ldots, s_{m+1}), \ldots, \rho_{m+1}(s_1, \ldots, s_{m+1})) \end{array}$$

where $\rho_1, \ldots, \rho_{m+1}$ are homogeneous polynomials of the same degree.

University of Zurich

Constructing spreads from permutation morphisms

Definition

A permutation morphism over the field $\mathbb{F}_{q^k}$ is a bijectiove map

$$\begin{array}{rcl} \rho : \mathbb{P}^m_{\mathbb{F}_{q^k}} & \longrightarrow & : \mathbb{P}^m_{\mathbb{F}_{q^k}} \\ (s_1, \ldots, s_{m+1}) & \longmapsto & (\rho_1(s_1, \ldots, s_{m+1}), \ldots, \rho_{m+1}(s_1, \ldots, s_{m+1})) \end{array}$$

where $\rho_1, \ldots, \rho_{m+1}$ are homogeneous polynomials of the same degree.

Theorem

Let ρ be a permutation morphism. Then the morphism

$$\begin{array}{rcl} \rho : \mathbb{P}^m_{\mathbb{F}_{q^k}} & \longrightarrow & \mathrm{G}(k, \mathbb{F}_q^{(m+1)k}), \\ (s_1, \ldots, s_{m+1}) & \longmapsto & \end{array}$$

$$\mathrm{rowsp}(\psi(\rho_1(s_1, \ldots, s_{m+1})), \ldots, \psi(\rho_{m+1}(s_1, \ldots, s_{m+1})))$$

defines a spread code.

Conclusion

1. Subspace codes are a class of codes heavily studied in the area of network coding.

University of Zurich

Conclusion

1. Subspace codes are a class of codes heavily studied in the area of network coding.
2. Kötter and Kschischang [KK08] showed a relation to rank metric codes which provides a way to construct good subspace codes through a 'lifting technique'. Beyond this there are few algebraic construction techniques for subspace codes.

University of Zurich

Conclusion

1. Subspace codes are a class of codes heavily studied in the area of network coding.
2. Kötter and Kschischang [KK08] showed a relation to rank metric codes which provides a way to construct good subspace codes through a 'lifting technique'. Beyond this there are few algebraic construction techniques for subspace codes.
3. It would be desirable to have classes of good network codes which appear as images inside the Grassmannian variety.

University of Zurich

Conclusion

1. Subspace codes are a class of codes heavily studied in the area of network coding.
2. Kötter and Kschischang [KK08] showed a relation to rank metric codes which provides a way to construct good subspace codes through a 'lifting technique'. Beyond this there are few algebraic construction techniques for subspace codes.
3. It would be desirable to have classes of good network codes which appear as images inside the Grassmannian variety.
4. Using permutation rational maps and and permutation morphisms we showed how to construct spread codes.

Thank you for your attention.

V. D. Goppa.
Algebraic-geometric codes.
Izv. Akad. Nauk SSSR Ser. Mat., 46(4):762–781, 896, 1982.

A.-L. Horlemann-Trautmann and J. Rosenthal.
Constructions of constant dimension codes.
In M. Greferath, M. Pavcevic, N. Silberstein, and M.A. Vazquez-Castro, editors, *Network Coding and Subspace Design*, Signals and Communication Technology, pages 25–42. Springer Verlag, 2018.

R. Kötter and F.R. Kschischang.
Coding for errors and erasures in random network coding.
IEEE Transactions on Information Theory, 54(8):3579–3591, August 2008.

F. Manganiello, E. Gorla, and J. Rosenthal.

Spread codes and spread decoding in network coding.

In *Proceedings of the 2008 IEEE International Symposium on Information Theory*, pages 851–855, Toronto, Canada, 2008.

C. F. Martin and R. Hermann.

Applications of algebraic geometry to system theory: The McMillan degree and Kronecker indices as topological and holomorphic invariants.

SIAM J. Control Optim., 16:743–755, 1978.

A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal.

Cyclic orbit codes.

arXiv:1112.1238, [cs.IT], 2011.

A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal.
Cyclic orbit codes.
IEEE Trans. Inform. Theory, 59(11):7386–7404, November 2013.

A.-L. Trautmann, F. Manganiello, and J. Rosenthal.
Orbit codes - a new concept in the area of network coding.
In *Information Theory Workshop (ITW), 2010 IEEE*, pages 1 –4, Dublin, Ireland, August 2010.

A.-L. Trautmann and J. Rosenthal.
New improvements on the echelon-ferrers construction.
In *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems – MTNS*, pages 405–408, Budapest, Hungary, 2010.