Polynomial Approach to Construct Cyclic Subspace Codes

Kamil Otal

Middle East Technical University, Ankara

(Joint work with Ferruh Özbudak)

Network Coding and Designs
April 4-8, 2016
Dubrovnik

Outline

Subspace codes

Consider the following notations and definitions.

- q: a prime power,
- $\mathbb{F}_q$: the finite field of size q,
- N, k: positive integers such that $1 < k < N$,
- $\mathcal{P}_q(N)$: the set of all subspaces of $\mathbb{F}_q^N$,
- $\mathcal{G}_q(N, k)$: the set of k-dimensional subspaces in $\mathcal{P}_q(N)$,
- **Subspace distance**:

$$d(U, V) := \dim U + \dim V - 2\dim(U \cap V)$$

for all $U, V \in \mathcal{P}_q(N)$.

Subspace codes

- **Subspace code**: A nonempty subset $\mathcal{C}$ of $\mathcal{P}_q(N)$ with the subspace distance.
- **Constant dimension code**: A subspace code $\mathcal{C}$ if $\mathcal{C} \subseteq \mathcal{G}_q(N, k)$.
- **Distance of a code**:

$$d(\mathcal{C}) := \min\{d(U, V) : U, V \in \mathcal{C} \text{ and } U \neq V\}.$$

Cyclic subspace codes

- Consider $\mathbb{F}_{q^N}$ instead of $\mathbb{F}_q^N$ equivalently (and richly).
- $\mathbb{F}^*_{q^N}$: the set of nonzero elements of $\mathbb{F}_{q^N}$.
- **Cyclic shift** of a codeword U by $\alpha \in \mathbb{F}^*_{q^N}$:

$$\alpha U := \{\alpha u : u \in U\}.$$

- **Frobenius shift** of a codeword U:

$$U^q := \{u^q : u \in U\}.$$

- It is easy to show that the cyclic shift and the Frobenius shift are also subspaces of the same dimension.

Cyclic subspace codes

- **Orbit** of a codeword U:

$$Orb(U) := \{\alpha U : \alpha \in \mathbb{F}_{q^N}^*\}.$$

- It is easy to show that orbits form an equivalence relation in $\mathcal{G}_q(N,k)$ and so in $\mathcal{P}_q(N)$.
- **Cyclic (subspace) code**: A subspace code $\mathcal{C}$ if $Orb(U) \subseteq \mathcal{C}$ for all $U \in \mathcal{C}$.

Cyclic subspace codes

The following proposition is well known.

Proposition

Let $U \in \mathcal{G}_q(N,k)$. $\mathbb{F}_{q^d}$ is the largest field such that U is also $\mathbb{F}_{q^d}$-linear (i.e. linear over $\mathbb{F}_{q^d}$) if and only if

$$|Orb(U)| = \frac{q^N - 1}{q^d - 1}.$$

Cyclic subspace codes

Let d denote the largest integer where U is also $\mathbb{F}_{q^d}$-linear.

- **Full length orbit**: An orbit if $d = 1$.
- **Degenerate orbit**: An orbit which is not full length.
- Remark that d divides both N and k. More explicitly,

$$U \in \mathcal{G}_q(N,k) \quad \Leftrightarrow \quad U \in \mathcal{G}_{q^d}(N/d, k/d) \ .$$

Therefore, it is enough to study on full length orbits.

Literature

- Subspace codes, particularly constant dimension codes, have been intensely studied in the last decade due to their application in random network coding[1].
- Cyclic subspace codes are useful in this manner due to their efficient encoding and decoding algorithms. Some recent studies about cyclic codes and their efficiency are:
  - –> A. Kohnert and S. Kurz; *Construction of large constant dimension codes with a prescribed minimum distance*, Lecture Notes Computer Science, vol. 5395, pp. 31–42, 2008.
  - –> T. Etzion and A. Vardy; *Error correcting codes in projective space*, IEEE Trans. on Inf. Theory, vol. 57, pp. 1165–1173, 2011.

[1] R. Kötter and F. R. Kschischang; *Coding for errors and erasures in random network coding*, IEEE Trans. on Inf. Theory, vol. 54, pp. 3579–3591, 2008.

Literature

- A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal; *Cyclic orbit codes*, IEEE Trans. on Inf. Theory, vol. 59, pp. 7386–7404, 2013.
- M. Braun, T. Etzion, P. Ostergard, A. Vardy and A. Wasserman; *Existence of q-analogues of Steiner systems*, arXiv:1304.1462, 2013.
- H. Gluesing-Luerssen, K. Morrison and C. Troha; *Cyclic orbit codes and stabilizer subfields*, Adv. in Math. of Communications, vol. 25, pp. 177–197, 2015.
- E. Ben-Sasson, T. Etzion, A. Gabizon and N. Raviv; *Subspace polynomials and cyclic subspace codes*, IEEE Trans. on Inf. Theory (to appear).

Subspace Polynomials

- **Linearized polynomial (q-polynomial)**:

$$F(x) = \alpha_s x^{q^s} + \alpha_{s-1} x^{q^{s-1}} + \ldots + \alpha_0 x \in \mathbb{F}_{q^N}[x]$$

  for some nonnegative integer s.
- The roots of F form a subspace of an extension of $\mathbb{F}_{q^N}$.
- The multiplicity of each root of F is the same, and equal to q^r for some nonnegative integer $r \leq s$. Explicitly, r is the smallest integer satisfying α_r is nonzero.

Subspace Polynomials

- **Subspace polynomial**: A monic linearized polynomial such that
  - splits completely over $\mathbb{F}_{q^N}$ (i.e. all roots are in $\mathbb{F}_{q^N}$),
  - has no multiple roots (i.e. $\alpha_0 \neq 0$).
- More explicitly, it is the polynomial

$$\prod_{u \in U} (x - u)$$

where U is a subspace of $\mathbb{F}_{q^N}$.

Related work

Theorem[a]

[a] E. Ben-Sasson, T. Etzion, A. Gabizon and N. Raviv; *Subspace polynomials and cyclic subspace codes*, IEEE Trans. on Inf. Theory (to appear).

Let

- n be a prime,
- γ be a primitive element of $\mathbb{F}_{q^n}$,
- $\mathbb{F}_{q^N}$ be the splitting field of the polynomial

$$x^{q^k} + \gamma^q x^q + \gamma x,$$

- $U \in \mathcal{G}_q(N, k)$ is this polynomial's kernel.

Related work

Theorem (cont'd.)

Then

$$\mathcal{C} := \bigcup_{i=0}^{n-1} \{\alpha U^{q^i} : \alpha \in \mathbb{F}_{q^N}^*\}$$

is a cyclic code of size $n\frac{q^N-1}{q-1}$ and minimum distance $2k-2$.

Our goal

Our goal is to generalize their result in two directions:

- Larger codes? That is, insert more orbits?
- More diverse N values? Via other types of subspace polynomials?

A generalization: More codewords

Result 1

Let n and r be positive integers such that $r \leq q^n - 1$ and let

- $\gamma_1, \ldots, \gamma_r$ be distinct elements of $\mathbb{F}_{q^n}^*$,
- $T_i(x) := x^{q^k} + \gamma_i^q x^q + \gamma_i x$ for all $i \in \{1, \ldots, r\}$,
- N_i be the degree of the splitting field of T_i for all $i \in \{1, \ldots, r\}$,
- $U_i \subseteq \mathbb{F}_{q^{N_i}}$ be the kernel of T_i for all $i \in \{1, \ldots, r\}$,
- N be a multiple of $\mathrm{lcm}(N_1, \ldots, N_r)$.

A generalization: More codewords

Result 1 (cont'd.)

Then the code $\mathcal{C} \subseteq \mathcal{G}_q(N,k)$ given by

$$\mathcal{C} = \bigcup_{i=1}^{r} \{\alpha U_i : \alpha \in \mathbb{F}_{q^N}^*\}$$

is a cyclic code of size $r\frac{q^N-1}{q-1}$ and the minimum distance $2k-2$. Moreover,

$$(\exists m)\ \gamma_i = \gamma_j^{q^m} \Rightarrow U_i = U_j^{q^m} (\text{ and so } N_i = N_j).$$

A generalization: More codewords

Main Idea of the Proof

It is enough to show that

$$\dim(\alpha U_i \cap \beta U_j) \leq 1$$

when $i \neq j$ or $\frac{\alpha}{\beta} \notin \mathbb{F}_q$. To show it, solve the system

$$\begin{aligned} T_i(x) &= 0, \\ T_j\left(\tfrac{\alpha}{\beta}x\right) &= 0. \end{aligned}$$

A generalization: More codewords

Corollary 1

In Result 1, taking

$$\gamma_1 = \gamma, \gamma_2 = \gamma^q, \ldots, \gamma_n = \gamma^{q^{n-1}} \in \mathbb{F}_{q^n}$$

for some positive integer n and irreducible element $\gamma \in \mathbb{F}_{q^n}$, we obtain a code $\mathcal{C}$ with

$$\#(\mathcal{C}) = \frac{q^N - 1}{q - 1} \text{ and } d(\mathcal{C}) = 2k - 2.$$

$\mathcal{C}$ is the same with the one in the theorem of Ben-Sasson et al for given n and γ.

A generalization: More codewords

Remark

In their theorem, it is assumed that n is prime and γ is primitive. However, in Corollary 1 they are not needed, only γ's irreducibleness is assumed. Therefore, Corollary 1 is also an improvement of their theorem.

Example

Let $q = 2$, $n = 4$ and $k = 3$. We can take $\gamma \in \mathbb{F}_{q^n}^*$ such that the minimal polynomial of γ over $\mathbb{F}_q$ is $x^4 + x^3 + x^2 + x + 1$. Here, $n = 4$ is not a prime and γ is not primitive but we can apply Corollary 1 (or their theorem) and thus obtain a cyclic code $\mathcal{C} \subseteq \mathcal{G}_q(12, 3)$ of size $4(2^{12} - 1)$ and the minimum distance 4.

A generalization: More codewords

Remark

In Result 1, we can choose r as strictly larger than n.

Example

Let $q = 3$, $n = 2$ and $k = 4$. Also let $\omega \in \mathbb{F}_{q^n}^*$ with the minimal polynomial $x^2 + 2x + 2$ over $\mathbb{F}_q$. Then we construct the cyclic codes $\mathcal{C}_0, \mathcal{C}_1 \subset \mathcal{G}_3(52, 4)$ of distance 6 as follows.

	$\mathcal{C}_0$ (using Theorem)	$\mathcal{C}_1$ (using Result 1)
Tools:	ω (and so ω^q)	$\omega, \omega^q, \omega^2, \omega^{2q}, 1$
Size:	$2\frac{3^{52}-1}{2}$	$5\frac{3^{52}-1}{2}$

Size has increased % 150! Also $\mathcal{C}_1$ contains $\mathcal{C}_0$.

Further improvement: More diverse parameters

Question

Consider the set

$$\{x^{q^k} + \theta x^q + \gamma x : \theta, \gamma \in \mathbb{F}_{q^n}^*\}$$

for some positive integer n. How should we choose polynomials from this set so that the collection of orbits of their kernels forms a cyclic code of distance $2k - 2$?

Further improvement: More diverse parameters

Result 2

Consider a set of r polynomials

$$T_i(x) := x^{q^k} + \theta_i x^q + \gamma_i x \in \mathbb{F}_{q^n}[x], 1 \leq i \leq r$$

satisfying $\theta_i \neq 0$ and $\gamma_i \neq 0$ for all $1 \leq i \leq r$, and

$$\frac{\gamma_i}{\gamma_j} \neq \left(\frac{\gamma_i}{\gamma_j}\left(\frac{\theta_i}{\theta_j}\right)^{-1}\right)^M \text{ when } i \neq j,$$

where $M := \frac{q^k-1}{q-1} \mod q^n - 1$.

Further improvement: More diverse parameters

Result 2 (cont'd.)

Also let

- N_i be the degree of the splitting field of T_i for all $i \in \{1, ..., r\}$,
- $U_i \subseteq \mathbb{F}_{q^{N_i}}$ be the kernel of T_i for all $i \in \{1, ..., r\}$,
- N be a multiple of $\text{lcm}(N_1, ..., N_r)$.

Then the code $\mathcal{C} \subseteq \mathcal{G}_q(N, k)$ given by

$$\mathcal{C} = \bigcup_{i=1}^{r} \{\alpha U_i : \alpha \in \mathbb{F}_{q^N}^*\}$$

is a cyclic code of size $r\frac{q^N-1}{q-1}$ and the distance $2k - 2$.

Further improvement: More diverse parameters

Remark

Result 1 is a special case of Result 2 with $\theta_i = \gamma_i^q$. Notice that the assumption

$$\frac{\gamma_i}{\gamma_j} \neq \left(\frac{\gamma_i}{\gamma_j} \left(\frac{\theta_i}{\theta_j} \right)^{-1} \right)^M \text{ when } i \neq j$$

has been automatically satisfied due to the fact that $\gcd(q^k, q^n - 1) = 1$.

Further improvement: More diverse parameters

Result 2 give us an opportunity to construct codes of diverse lengths as we can observe in the following example.

Example

Let $q = 3, n = 2, k = 4$ and $\mathbb{F}_{3^2} = \mathbb{F}_3(\omega)$ where ω is a root of the primitive polynomial $x^2 + 2x + 2 \in \mathbb{F}_3[x]$. If we use Result 1 then we must choose only the polynomials from the list below.

Polynomial	Degree of the splitting field
$x^{q^k} + x^q + x$	26
$x^{q^k} + \omega^q x^q + \omega x$	52
$x^{q^k} + \omega^{2q} x^q + \omega^2 x$	52
$x^{q^k} + \omega^{3q} x^q + \omega^3 x$	80

Further improvement: More diverse parameters

Example (cont'd.)

Polynomial	Degree of the splitting field
$x^{q^k} + 2x^q + 2x$	48
$x^{q^k} + \omega^{5q}x^q + \omega^5 x$	52
$x^{q^k} + \omega^{6q}x^q + \omega^6 x$	48
$x^{q^k} + \omega^{7q}x^q + \omega^7 x$	52

If we want $N = 26$ (or an odd multiple of 26) then we have only one orbit (obtained by $x^{q^k} + x^q + x$), i.e. construct a code of size $\frac{3^N-1}{2}$, distance 6 and N an odd multiple of 26. If we want more orbits using Result 1, then N must change and it can not be an odd multiple of 26 any more.

Further improvement: More diverse parameters

Example (cont'd.)

However, using Result 2 we have $M = 0$ and so the only restriction is $\gamma_i \neq \gamma_j$ when $i \neq j$. So we can choose the polynomials below.

Polynomial	Degree of the splitting field
$x^{q^k} + \omega^2 x^q + x$	26
$x^{q^k} + \omega x^q + \omega^2 x$	26
$x^{q^k} + \omega x^q + \omega^6 x$	26

In that way, the length N is kept as an odd multiple of 26 and we can construct a code including three orbits, i.e. construct a code of size $3\frac{3^N-1}{2}$, distance 6 and length an odd multiple of 26.

About the distance 2k-2s

An generalization of Result 2 for the distance $2k-2s$ (where $1 \le s \le k-1$) using also degenerate orbits considering the set of polynomials

$$T_i(x) := x^{q^k} + \gamma_{s,i}x^{q^s} + \ldots + \gamma_{1,i}x^q + \gamma_{0,i}x \in \mathbb{F}_{q^n}[x], 1 \le i \le r$$

is immediate.

Adjoint codes

- Let $T(x) \in \mathbb{F}_{q^N}[x]$ be a subspace polynomial having the rootspace U. We can determine another subspace $\overline{U} \subseteq \mathbb{F}_{q^N}$ associated with $T(x)$.
- $u \in \overline{U}$ if and only if

$$T(x) = \left(x^q - \frac{1}{u^{q-1}}x\right) \circ Q(x)$$

for some q-polynomial $Q(x)$ over $\mathbb{F}_{q^N}$.

Adjoint codes

- This space can be also characterized by

$$u \in \overline{U} \Leftrightarrow u^q \text{ is a root of } \overline{T}(x) := (\alpha_0 x)^{q^k} + \ldots + (\alpha_{k-1} x)^q + x$$

where

$$T(x) = x^{q^k} + \alpha_{k-1} x^{q^{k-1}} + \ldots + \alpha_0 x.$$

- Here, $\dim_{\mathbb{F}_q}(U) = \dim_{\mathbb{F}_q}(\overline{U})$. $\overline{U}$ is called the *adjoint space* of T (or, of U).

(See Theorems 14, 15 and 16 in the paper of Ore (1933)[2] for the proofs of these facts.)

[2] O. Ore, *"On a special class of polynomials"*, Trans. Amer. Math. Soc., vol. 35 (1933), pp. 559–584.

Adjoint codes

Result 2'

Consider a set of r polynomials

$$\overline{T_i}(x) := x + \gamma_i^q x^{q^{k-1}} + \theta_i x^{q^k} \in \mathbb{F}_{q^n}[x], 1 \leq i \leq r$$

satisfying $\theta_i \neq 0$ and $\gamma_i \neq 0$ for all $1 \leq i \leq r$, and

$$\frac{\gamma_i}{\gamma_j} \neq \left(\frac{\gamma_i}{\gamma_j}\left(\frac{\theta_i}{\theta_j}\right)^{-1}\right)^M \text{ when } i \neq j,$$

where $M := \frac{q^k-1}{q-1} \mod q^n - 1$.

Adjoint codes

Result 2' (cont'd.)

Also let

- N_i be the degree of the splitting field of $\overline{T_i}$ for all $i \in \{1, ..., r\}$,
- $\overline{U_i} \subseteq \mathbb{F}_{q^{N_i}}$ be the kernel of $\overline{T_i}$ for all $i \in \{1, ..., r\}$,
- N be a multiple of $\mathrm{lcm}(N_1, ..., N_r)$.

Then the code $\mathcal{C} \subseteq \mathcal{G}_q(N, k)$ given by

$$\mathcal{C} = \bigcup_{i=1}^{r} \{\alpha \overline{U_i} : \alpha \in \mathbb{F}_{q^N}^*\}$$

is a cyclic code of size $r\frac{q^N-1}{q-1}$ and the distance $2k-2$.

Finally...

Thank you!

☺