Cyclic Subspace Codes Via Subspace Polynomials

Kamil Otal and Ferruh Özbudak

Middle East Technical University

Design and Application of Random Network Codes (DARNEC'15)
November 4-6, 2015 / Istanbul, Turkey.

Outline

1. **Introduction**
   - Subspace codes
   - Cyclic subspace codes
   - Subspace Polynomials
2. **Motivation**
   - Literature
   - Related work
   - Our goal
3. **Our contributions**
   - A generalization: More codewords
   - One more generalization: More diverse parameters

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 $\alpha \in \mathbb{F}^*_{q^N}$:

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

- It is easy to show that the cyclic shift is also a subspace of the same dimension.
- **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 theorem is well known.

Theorem

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.

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 $\mathbb{F}_{q^N}$,
  - has no multiple root (equivalently $\alpha_0 \neq 0$).
- More explicitly, it is the polynomial

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

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

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*; arXiv:1404.7739v3, 2015. (Also in ISIT 2015, pp. 586-590.)

Related work

Theorem 1[a]

[a] E. Ben-Sasson, T. Etzion, A. Gabizon and N. Raviv; *Subspace polynomials and cyclic subspace codes*; arXiv:1404.7739v3, 2015. (Also in ISIT 2015, pp. 586-590.)

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 1 (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:

- Can we insert more orbits (i.e. more codewords)?
- Can we use other types of subspace polynomials (and hence cover more diverse values of length N)?

A generalization: More codewords

Theorem 2

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 the least common multiple of $N_1, \ldots, N_r$.

A generalization: More codewords

Theorem 2 (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, if γ_i and γ_j are conjugate as $\gamma_i = \gamma_j^{q^m}$ for some integer m, then $N_i = N_j$ and $U_i = U_j^{q^m}$.

A generalization: More codewords

Corollary 1

Let n be a positive integer and $\gamma_1 = \gamma, \gamma_2 = \gamma^q, \ldots, \gamma_n = \gamma^{q^{n-1}} \in \mathbb{F}_{q^n}$ for some irreducible element γ of $\mathbb{F}_{q^n}$. Then, by using the construction in Theorem 2, we can produce a cyclic code of size

$$n\frac{q^N - 1}{q - 1}$$

and the minimum distance $2k - 2$. Resulting code is the same with the one in Theorem 1.

A generalization: More codewords

Remark 1

In the theorem of Ben-Sasson et al, 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 1

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 Theorem 1) 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 2

In Theorem 2, we can choose r as strictly larger than n.

Example 2

Let $q = 3$, $n = 2$ and $k = 3$. Also let $\gamma \in \mathbb{F}^*_{q^n}$ with the minimal polynomial $x^2 + 2x + 2$ over $\mathbb{F}_q$.

Using Theorem 1	Using Theorem 2
Use: γ (and so γ^q)	Use: $\gamma_1 = \gamma, \gamma_2 = \gamma^q, \gamma_3 = 2$
Size$= 2\frac{3^{52}-1}{2}$	Size$= 3\frac{3^{52}-1}{2}$

- Size has increased % 50.
- The second code is containing the first one.

One more generalization: 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 $2k - 2$?

One more generalization: More diverse parameters

Theorem 3

Consider a set P of polynomials

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

satisfying

- $\theta_i \neq 0$ and $\gamma_i \neq 0$,
- $\frac{\theta_j}{\theta_i} \neq \left(\frac{\gamma_j \theta_i}{\gamma_i \theta_j}\right)^M$ when $i \neq j$

where

$$M = \frac{(q^{\gcd(n,k-1)} - 1)\gcd(k-1, q-1)}{(q-1)\gcd(n, k-1, q-1)}.$$

One more generalization: More diverse parameters

Theorem 3 (cont'd.)

Also let

- N_i be the degree of the splitting field of T_i for all $i \in \{1, \ldots, |P|\}$,
- $U_i \subseteq \mathbb{F}_{q^{N_i}}$ be the kernel of T_i for all $i \in \{1, \ldots, |P|\}$,
- N be the least common multiple of $N_1, \ldots, N_{|P|}$.

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

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

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

One more generalization: More diverse parameters

Remark 3

Theorem 2 is a special case of Theorem 3 with $\theta_i = \gamma_i^q$ and $|P| = r \leq q^n - 1$. Notice that the assumption

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

has been automatically satisfied due to the fact that $q^n - 1$ can not divide q^k.

One more generalization: More diverse parameters

Example 3

Let $q = 2, n = 2$ and $k = 4$. Then $M = 1$. Taking $\gamma_i = 1$ for all i, obtain

$$P = \{x^{2^4} + \theta x^2 + x : \theta \in \mathbb{F}^*_{2^2}\},$$

it is chosen as in Theorem 3. Here, we obtain $N_1 = N_2 = N_3 = 30$ and so

$$N = 30.$$

In that way we construct a cyclic code $\mathcal{C} \subseteq \mathcal{G}_2(30, 4)$ of size $3(2^{30} - 1)$ and minimum distance 6.

One more generalization: More diverse parameters

Example 3 (Cont'd.)

Remark that, if we use Theorem 2 then we must have

$$P = \{x^{2^4} + \theta^2 x^2 + \theta x : \theta \in \mathbb{F}^*_{2^2}\}.$$

Then we obtain $N_1 = N_2 = 14$ and $N_3 = 30$ and so

$$N = 210.$$

In that way we construct a cyclic code $\mathcal{C} \subseteq \mathcal{G}_2(210, 4)$ of size $3(2^{210} - 1)$ and minimum distance 6.

Therefore, Theorem 3 give us an opportunity to construct codes of different lengths.

Finally...

Thank you very much

☺