On Maximal Families of Polynomials with Pairwise Linear Common Factors

Maximilien Gadouleau, **Luca Mariot**, Federico Mazzone

l.mariot@utwente.nl

BFA 2024 – Dubrovnik, September 12, 2024

Problem Statement

Notation:

- Let $n \in \mathbb{N}$ and q be a power of a prime
- $S_n := \{f \in \mathbb{F}_q[x] : \deg(f) = n, f \text{ monic}, f(0) \neq 0\}$

Problem

Given $d \in \{0, \ldots, n\}$, define $\mathcal{M}_n^d$ as:

$$\mathcal{M}_n^d := \{R \subseteq S_n : \forall f \neq g \in R, \deg(\gcd(f, g)) \leq d\}$$

What is the size of the largest subset $R \in \mathcal{M}_n^d$?

Outline

Network Coding and Subspace codes

- Routing packets on networks is not always efficient [K12]

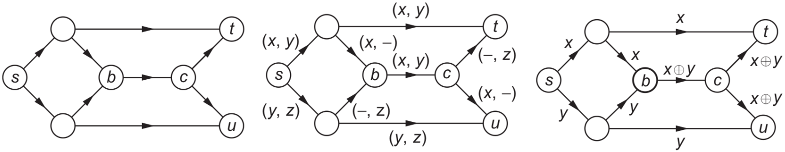


Image credits: F. R. Kschischang, *An Introduction to Network Coding*

- **Network Coding**: combine packets together as linear combinations
- **Noncoherent setting**: does not consider the underlying topology of the network (subspace codes)

Linear Codes

Notation:

- $\mathbb{F}_q = \{0,1\}$: finite field of order q
- $\mathbb{F}_q^n = \{0,1\}^n$: n-dimensional vector space over $\mathbb{F}_q$

Definition

A (n,k,d) binary linear code C: A (n,d) code C that is also a k-dimensional subspace of $\mathbb{F}_q^n$

$$g_1, \cdots, g_k \in \mathbb{F}_q^n \text{ basis of } C \Leftrightarrow G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix} k \times n \text{ generator matrix of } C$$

Subspace Codes

- **Idea:** codewords are not vectors, but *vector subspaces*
- **Distance** between two subspaces:

$$d(A,B) = dim(A) + dim(B) - 2dim(A \cap B) \quad .$$

Definition ([KK08])

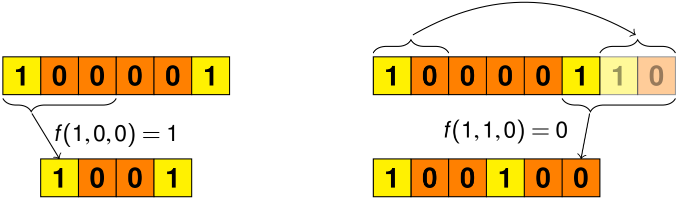
A subspace code $\mathcal{C}$ of parameters $[n, \ell(\mathcal{C}), \log_q |\mathcal{C}|, D(\mathcal{C})]$ is a family of subsets of $\mathbb{F}_q^n$ where $\ell(\mathcal{C}) = \max_{V \in \mathcal{C}}\{dim(V)\}$ and $D(\mathcal{C})$ is the minimum distance of $\mathcal{C}$, defined as:

$$D(\mathcal{C}) = \min_{U,V \in \mathcal{C}} \{d(U,V)\}$$

Cellular Automata

- Vectorial functions $F : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ with *uniform* (shift-invariant) coordinates [MPLJ19]

Example: $q = 2$, $n = 6$, $d = 3$, $f(s_i, s_{i+1}, s_{i+2}) = s_i \oplus s_{i+1} \oplus s_{i+2}$



No Boundary CA – NBCA

Periodic Boundary CA – PBCA

Linear CA

- Local rule: *linear combination* of the neighborhood cells

$$f(x_1,\cdots,x_d) = a_1x_1 + \cdots + a_dx_d \ , \ a_i \in \mathbb{F}_q$$

- Associated polynomial:

$$f \mapsto p_f(X) = a_1 + a_2X + \cdots + a_dX^{d-1} \in \mathbb{F}_q[X]$$

- $(n-d+1)\times n$ transition matrix:

$$M_F = \begin{pmatrix} a_1 & \cdots & a_d & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_1 & \cdots & a_d & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_1 & \cdots & a_d \end{pmatrix}, \quad x \mapsto M_F x^\top$$

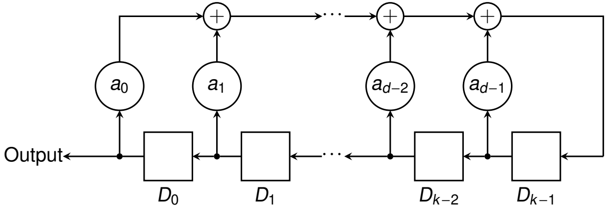
- **Remark:** a linear rule is bipermutive iff $a_1, a_d \neq 0$

Linear Recurring Sequences (LRS)

- Sequence $\{x_i\}_{i\in\mathbb{N}}$ satisfying the following relation [LN97]:

$$a_0 x_i + a_1 x_{i+1} + \ldots + a_{d-1} x_{i+d-1} = x_{i+d}$$

- Computed by a *Linear Feedback Shift Register* (LFSR):



- Feedback polynomial:

$$f(X) = a_0 + a_1 X + \cdots a_{d-1} X^{d-1} + X^d$$

Linear map associated to a LRS

- Take the *projection* of all sequences satisfying the LRS defined by $f(X)$ onto their first $2d$ coordinates [GMP23]
- Consider the d-dim subspace $S_f \subseteq \mathbb{F}_q^{2d}$ which is the kernel of the linear map $F : \mathbb{F}_q^{2d} \to \mathbb{F}_q^{d}$:

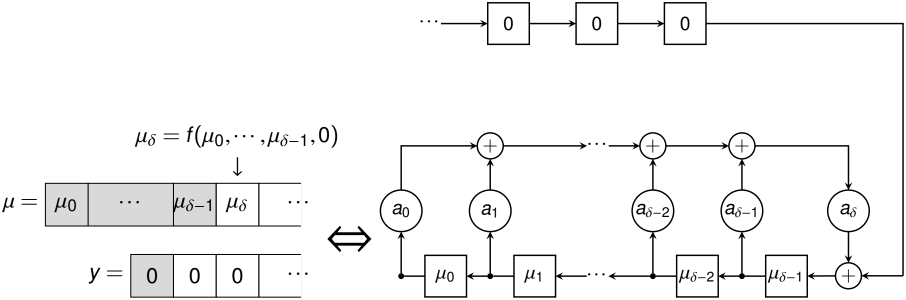
$$F(x_0, \cdots, x_{2d-1})_i = a_0 x_i + a_1 x_{i+1} + \ldots + a_{d-1} x_{i+d-1} + x_{i+d} \ ,$$

associated matrix:

$$M_F = \begin{pmatrix} a_0 & \cdots & a_{d-1} & 1 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_0 & \cdots & a_{d-1} & 1 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & a_0 & \cdots & a_{d-1} & 1 \end{pmatrix}$$

- ... but this is *exactly* the global rule of a linear CA!

Kernel as CA preimage computation



Kernel $\Leftrightarrow$ 0-preimage of CA [ML18]

Partial Spreads from Coprime Polynomials

Partial spread: A family $\mathcal{S}$ of subspaces of $\mathbb{F}_q^n$ with pairwise trivial intersection [C21]

Lemma ([GMP23])

Given $f, g \in \mathbb{F}_q[X]$ over $\mathbb{F}_q$ of degree $d \geq 1$, defined as:

$$f(X) = a_0 + a_1 X + \cdots + a_{d-1} X^{d-1} + X^d \ , \tag{1}$$

$$g(X) = b_0 + b_1 X + \cdots + b_{d-1} X^{d-1} + X^d \ , \tag{2}$$

Then, the kernels of $F, G : \mathbb{F}_q^{2d} \to \mathbb{F}_q^d$ have trivial intersection if and only if $\gcd(f, g) = 1$

Consequence: a family of t pairwise coprime polynomials gives CA kernels that form a partial spread

Subspaces Codes from kernels of linear CA

Theorem ([MM23])

Let $\mathcal{F}$ be a set of linear CA of length $2k$ and diameter d, $k = d-1$. Then, the minimum distance of the subspace code $\mathcal{C}_{\mathcal{F}}$ is:

$$D(\mathcal{C}_{\mathcal{F}}) = 2k - 2 \cdot \max_{\substack{F,G \in \mathcal{F} \\ F \neq G}} \left\{ \deg(\gcd(P_f, P_g)) \right\} \ , \tag{3}$$

where P_f, P_g are the polynomials associated to F and G.

- **Coprime case**: maximum distance (partial spread codes [GR14], bent functions [GMP23])
- **trade-off**: the higher the degree of the GCD, the lower the distance, the more subspaces we can squeeze into the code

Maximal Families with Pairwise Linear GCD

Problem

Given $d \in \{0,\ldots,n\}$, define $\mathcal{M}_n^d$ as:

$$\mathcal{M}_n^d := \{R \subseteq S_n : \forall f \neq g \in R, \deg(\gcd(f,g)) \leq d\}$$

What is the size of the largest subset $R \in \mathcal{M}_n^d$?

Contributions (this abstract):

- Lower bound for the general case
- Optimal construction for $d = 1$ and $q = 2$

Notation:

- $\mathcal{I}_k$: set of all irreducible polynomials of degree k, $I_k = |\mathcal{I}_k|$

Lower Bound

Given n and d, construct R as follows:

Construction-Lower-Bound(n, d)

1. Add all irreducible polynomials of degree n, i.e. $\mathcal{I}_n$.
2. For $i \in \{1, \ldots, d\}$, for all $h \in \mathcal{I}_{n-i}$, pick $g \in \mathcal{I}_i$ and add gh.
3. For $i \in \{d+1, \ldots, \lfloor (n-1)/2 \rfloor\}$, for all $g \in \mathcal{I}_i$, pick $h \in \mathcal{I}_{n-i}$ not previously used and add gh.
4. If n is even, add g^2 for all $g \in \mathcal{I}_{n/2}$
5. For $i \in \{1, \ldots, d\}$, for all $g \in \mathcal{I}_i$, pick $h \in \mathcal{I}_{n-\lfloor n/i \rfloor i}$ and add $g^{\lfloor n/i \rfloor} h$.

Size of R:

$$|R| = \sum_{i=1}^{\lfloor n/2 \rfloor} I_i + \sum_{i=n-d}^{n-1} I_i + I_n$$

Optimal Construction for $d = 1$, $q = 2$

If $d = 1$ and $q = 2$, the only possible GCDs are 1 and $X + 1$.

Construction-Maximal(n)

1. Add all irreducible polynomials of degree n, i.e. $\mathcal{I}_n$
2. For all $g \in \mathcal{I}_{n-1}$, add $(x + 1)g$
3. For $i \in \{2, \ldots, \lfloor (n-1)/2 \rfloor\}$, for all $g \in \mathcal{I}_i$, pick $h \in \mathcal{I}_{n-i}$ not previously used and add gh
4. If n is even, add g^2 for all $g \in \mathcal{I}_{n/2}$
5. Add $(x + 1)^n$.

Theorem

For $q = 2$, any maximal element of $\mathcal{M}_n^1$ has cardinality:

$$N_n = \sum_{i=1}^{\lfloor n/2 \rfloor} I_i + I_{n-1} + I_n$$

Conclusions and Future Works

Summing up:

- Furthered the study of subspace codes defined by linear CA
- Characterized the maximal families of binary polynomials with pairwise linear GCD

Future work:

- Generalization to larger GCD degrees: just found an optimal construction for $d < n/4$!
- Characterize families with uniform degree of pairwise GCD (equidistant codes)
- Investigate decoding efficiency of CA-based subspace codes [ML18a]

References

[C21] Carlet, C.: Boolean functions for cryptography and coding theory. Cambridge University Press (2021)

[GMP23] M. Gadouleau, L. Mariot, S. Picek. Bent functions in the partial spread class generated by linear recurring sequences. Des. Codes and Cryptogr. 91(1): 63-82 (2023)

[GR14] E. Gorla, A. Ravagnani: Partial spreads in random network coding. Finite Fields Their Appl. 26: 104–115 (2014)

[KK08] R. Koetter, F.R. Kschischang: Coding for errors and erasures in random network coding. IEEE Trans. Inf. Theory 54(8): 3579–3591 (2008)

[K12] F.R. Kschischang: An introduction to network coding. In: Network Coding. Elsevier, pp. 1–37 (2012)

[LN97] R. Lidl, H. Niederreiter: Finite fields. Cambridge University Press (1997)

[MM23] L. Mariot, F. Mazzone: On the Minimum Distance of Subspace Codes Generated by Linear Cellular Automata. In: Proceedings of AUTOMATA 2023, LNCS vol. 14152, pp. 105-119, Springer (2023)

[MPLJ9] L. Mariot, S. Picek, A. Leporati, and D. Jakobovic. Cellular automata based S-boxes. Cryptography and Communications 11(1): 41-62 (2019)

[ML18] L. Mariot, A. Leporati: A cryptographic and coding-theoretic perspective on the global rules of cellular automata. Nat. Comput. 17(3): 487-498 (2018)

[ML18a] L. Mariot, A. Leporati: Inversion of mutually orthogonal cellular automata. In: Proceedings of ACRI 2018, LNCS vol. 11115, pp. 364–376, Springer (2018)