Il principio di indeterminazione dal punto di vista della teoria dei codici

Martino Borello

Université Paris 8 - LAGA

Seminario congiunto UMI
Gruppo Crittografia e Codici
02/03/2022

Outline

Preliminaries

K finite field of cardinality q.

Basic definitions

- A q-ary **linear code** $\mathcal{C}$ of **length** n is a subspace of K^n.
- For $c = (c_1, \dots, c_n) \in \mathcal{C}$ (**codeword**), the (Hamming) **support** of c is

$$\mathrm{supp}(c) = \{i \in \{1, \dots, n\} \mid c_i \neq 0\}$$

  and $\mathrm{wt}(c) = \#\mathrm{supp}(c)$ (**weight**).

Parameters

Parameters: $[n, k, d]_q$.

- $d = \mathrm{d}(\mathcal{C}) = \min_{c \in \mathcal{C}, c \neq 0} \mathrm{wt}(c)$ (**minimum distance**).
- $R = k/n$ (**information rate**).

Preliminaries

$G \neq \{1_G\}$ **finite group**.

Definition

A G-**code** (or a **group code**) over K is a right ideal in the **group algebra**

$$KG = \left\{ a = \sum_{g \in G} a_g g \;\middle|\; a_g \in K \right\}.$$

Definition

- $G = C_m$ (cyclic group of order m) $\Rightarrow$ **cyclic code**.
- $G = D_{2m}$ (dihedral group of order $2m$) $\Rightarrow$ **dihedral code**.
- $G = C_m \rtimes C_r$ (metacylic group of order rm) $\Rightarrow$ **metacyclic code**.

Preliminaries

Remark

If $\#G = n$, fix an ordering $G = \{g_1, \dots, g_n\}$, then

$$\begin{array}{rccc} \varphi : & KG & \xrightarrow{\sim} & K^n \\ & \displaystyle\sum_{i=1}^{n} a_i g_i & \mapsto & (a_1, \dots, a_n). \end{array}$$

The isomorphism is not canonical!
Different orderings yield permutation equivalent codes.

Via φ:

$$\begin{array}{rcl} G\text{-codes} & \rightsquigarrow & \text{Linear codes.} \\ \text{Hamming metric in } KG & \leftsquigarrow & \text{Hamming metric in } K^n. \\ \text{Inner product in } KG & \leftsquigarrow & \text{Inner product in } K^n. \\ \text{Action of } G & \rightsquigarrow & \text{Permutation automorphism (regular) subgroup.} \end{array}$$

Preliminaries

Examples

- The self-dual $[24, 12, 8]$ **Golay code** is a S_4-code (Bernhardt, Landrock and Manz - 1990) and a D_{24}-code (McLoughlin and Hurley - 2008).
- The self-dual $[48, 24, 12]$ **extended quadratic residue code** is a D_{48}-code.
- The self-dual $[72, 36, 16]$ code (if it exists!) is not a group code, since $\#\mathrm{PAut}(\mathcal{C}) \leqslant 5$ (B., Willems and many others).
- The $[12, 6, 6]_3$ **Golay code** $\mathcal{G}$ is not a group code, even if $\#\mathrm{PAut}(\mathcal{G}) = 660$.
- The **Reed-Muller codes** $\mathcal{RM}_p(r, m) = J^{m(p-1)-r}$ (p prime), with J Jacobson radical (intersection of maximal ideals) of KG, where G is elementary abelian of rank m (Berman - 1967 and Charpin - 1988).

Asymptotic performance of G-codes

Definition

A family of codes $\mathcal{F}$ is called **asymptotically good** if it exists an infinite set $\{\mathcal{C}_n\}_{n\in\mathcal{I}} \subseteq \mathcal{F}$ of $[n, k_n, d_n]_q$ codes such that

$$R = \liminf_{n\to\infty} k_n/n > 0 \quad (\textbf{asymptotic rate}),$$

$$\delta = \liminf_{n\to\infty} d_n/n > 0 \quad (\textbf{asymptotic relative minimum distance}).$$

Open problem (Assmus, Mattson, Turyn - 1966)

Is the family of cyclic codes asymptotically good?

Asymptotic performance of G-codes

Theorem (Lin, Weldon - 1967)

Long (particular) BCH codes are bad.

Theorem (Berman - 1967)

Cyclic codes are bad if only finitely many primes are involved in the lengths of the codes.

Theorem (Babai, Shpilka, Stefankovic - 2005)

- There are no good cyclic LDPC (low density parity check) codes.
- There are no good cyclic locally testable codes.

Open problem (Assmus, Mattson, Turyn - 1966)

Is the family of cyclic codes asymptotically good? Maybe not!

Asymptotic performance of G-codes

Theorem (Bazzi, Mitter - 2006, Solé et al. - 2016)

Binary dihedral codes are asymptotically good.

Theorem (B., Willems - 2020)

$C_p \rtimes C_q$-codes over K are asymptotically good.

Theorem (B., Moree, Solé - 2020)

Assuming Artin's conjecture for primitive roots in arithmetic progression (true under GRH), metacyclic codes are aymptotically good.

Open problem (Assmus, Mattson, Turyn - 1966)

Is the family of cyclic codes asymptotically good? Maybe yes!

The classical uncertainty principle

G **finite abelian group** and $f : G \to \mathbb{C}$.

Definition

The **dual group** of G is

$$\hat{G} = \{\text{homomorphisms } \chi : G \to \mathbb{S}^1\} \cong G$$

where $\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$.

Definition

The **Fourier transform** of f is $\hat{f} : \hat{G} \to \mathbb{C}$ defined by

$$\hat{f}(\chi) = \frac{1}{\#G} \sum_{g \in G} f(g)\overline{\chi(g)}$$

The classical uncertainty principle

$\mathrm{supp}(f) = \{g \in G \mid f(g) \neq 0\}$.

Theorem (Donoho, Stark - 1989)

Every $f : G \to \mathbb{C}$, $f \neq 0$, satisfies

$$\#\mathrm{supp}(f) \cdot \#\mathrm{supp}(\hat{f}) \geqslant \#G.$$

(Uncertainty Principle)

Stronger version for $G = C_p$, observed first by Meshulam.

Theorem (Goldstein, Guralnick, Isaac / Tao - 2005)

Every $f : C_p \to \mathbb{C}$, $f \neq 0$, satisfies

$$\#\mathrm{supp}(f) + \#\mathrm{supp}(\hat{f}) \geqslant p + 1.$$

(Uncertainty Principle for simple cyclic group)

The classical uncertainty principle

- $f : G \to \mathbb{C} \longleftrightarrow \sum_{g\in G} f(g)g \in \mathbb{C}G$
- $\mathbb{C}C_p = \mathbb{C}[x]/(x^p - 1)$ and $f = a_0 + a_1x + \ldots + a_{p-1}x^{p-1}$.
- $\hat{C}_p \cong \mu_p(\mathbb{C}) = \{\zeta \in \mathbb{C} \mid \zeta^p = 1\}$ by $\chi \mapsto \chi(1)$ and

$$\hat{f}(\zeta) = \frac{1}{p}(a_0 + a_1\zeta^{-1} + \ldots + a_{p-1}\zeta^{-(p-1)})$$

- Let $\mathcal{I}_f = (f)$ in $\mathbb{C}[x]/(x^p - 1)$, with $f | x^p - 1$. Then

$$\dim \mathcal{I}_f = p - \deg(f) = p - \#zeros(f) = \#\mathrm{supp}(\hat{f}).$$

Theorem (Uncertainty Principle reformulated)

Every $f \in \mathbb{C}[x]/(x^p - 1)$, $f \neq 0$, satisfies

$$\mathrm{wt}(f) + \dim \mathcal{I}_f \geqslant p + 1.$$

The classical uncertainty principle

Corollary (Evra, Kowalski, Lubotzky - 2017)

Cyclic codes over $\mathbb{C}$ are asymptotically good.

Proof

Let ζ_p is a primitive p-th root of unity and

$$f = \prod_{i=1}^{\frac{p-1}{2}} (x - \zeta_p^i).$$

Then $\dim \mathcal{I}_f = p - \deg(f) = \frac{p+1}{2}$ and for $h \in \mathcal{I}_f,\ h \neq 0$,

$$\mathrm{wt}(h) \geqslant p + 1 - \dim \mathcal{I}_h \geqslant p + 1 - \dim \mathcal{I}_f = \frac{p+1}{2}.$$

So $\mathcal{I}_f$ is a $[p, \frac{p+1}{2}, \frac{p+1}{2}]_{\mathbb{C}}$ cyclic code.

Uncertainty principle and cyclic codes

What about finite fields?

Definition

$$\mu(K,n)=\min\{\mathrm{d}(\mathcal{I}_f)+\dim\mathcal{I}_f \mid f\in K[x]/(x^n-1)\}.$$

- $\mu(\mathbb{C},p)=p+1$ for all prime p.
- $\mu(K,n)\leqslant n+1$ (**Singleton bound**).
- $\mu(K,p)=p+1$ if q is primitive modulo p, i.e. $\mathrm{ord}_p(q)=p-1$.

Definition (Evra, Kowalski, Lubotzky - 2017)

K satisfies the **(strong) Uncertainty Principle** if for all prime p

$$\mu(K,p)=p+1.$$

Uncertainty principle and cyclic codes

Theorem (B., Solé - 2020)

Assume MDS conjecture. If q is not primitive modulo p and $p > q+2$, then

$$\mu(K,p) < p+1.$$

Proof

- q is not primitive modulo $p \Rightarrow$ it exists $f | x^p - 1$ such that

$$1 < \deg(f) < p-1, \text{ i.e. } 1 < \dim \mathcal{I}_f < p-1.$$

- By contradiction, $\mathrm{d}(\mathcal{I}_f) + \dim \mathcal{I}_f \geqslant \mu(K,p) \geqslant p+1$ $\Rightarrow \mathcal{I}_f$ is MDS of length p, non-trivial.
- MDS conjecture $\Rightarrow p \leqslant q+2$.

Something similar is true without MDS conjecture (e.g. nontrivial MDS codes have length at most $2q-2$). So, **the (strong) UP is not true for any K.**

Uncertainty Principle and cyclic codes

Definition (Weak Uncertainty Principle)

Let $0 < \varepsilon < \lambda \leqslant 1$. K satisfies the (ε, λ)-**Uncertainty Principle** if there exists an infinite set of primes $\mathcal{P}$ such that for all $p \in \mathcal{P}$,

- $\mu(K, p) > \lambda p$
- $\mathrm{ord}_p(q) < \varepsilon p$.

Theorem (Evra, Kowalski, Lubotzky - 2017)

If K satisfies the (ε, λ)-Uncertainty Principle, then cyclic codes over K are asymptotically good.

Idea:

- $\mu(K, p) > \lambda p \Rightarrow$ we can find ideals with large distance.
- $\mathrm{ord}_p(q) < \varepsilon p \Rightarrow$ we can find ideals with large dimension.

Uncertainty principle and cyclic codes

Proposition (B., Solé - 2020)

If K satisfies the (ε, λ)-Uncertainty Principle, then $\lambda < \frac{q-1}{q}$.

Proof

- There exists a sequence of cyclic codes of length $p \in \mathcal{P}$, asymptotic rate R and asymptotic relative distance δ.
- $p\delta + pR \geqslant \mu(K, p) > \lambda p$.
- $\lambda < \min\{\delta + \alpha_q(\delta)\}$, where $\alpha_q(\delta)$ is the largest possible rate of a code of relative distance δ.
- Asymptotic Plotkin bound $\Rightarrow \min\{\delta + \alpha_q(\delta)\} = \frac{q-1}{q}$.

Does it exist any K satisfying the Weak Uncertainty Principle for some ε, λ?

Uncertainty principle and cyclic codes

Generalization of Donoho-Stark :

Proposition (B., Solé - 2020)

For $f \neq 0$,

$$\mathrm{wt}(f) \cdot \mathrm{wt}(\hat{f}) \geqslant n.$$

(Naive Uncertainty Principle)

Proof: BCH bound.

Corollary

Let $\mathcal{I}_f = (f)$, with $f \neq 0$. Then

$$\mathrm{d}(\mathcal{I}_f) \cdot \dim \mathcal{I}_f \geqslant n.$$

Uncertainty principle and cyclic codes

Theorem (B., Solé - 2020)

For every real number $0 < \alpha < 1/2$, there are sequences of cyclic codes of asymptotic rate R with minimum distance $\Omega(n^\alpha)$.

Proof

- $n = q^p - 1$, with p prime.
- $x^n - 1 = \prod_{a \neq 0}(x - a) \prod_{i=1}^{s} f_i$, with f_i irreducible of degree p.
- $g_I = \prod_{i \in I} f_i$, with $\#I = \lfloor s(1-R) \rfloor$.
- $\mathcal{I}_{g_I} = (g_I)$ has asymptotic rate R.
- Calculate $\Lambda_n \geqslant \#\{\text{codes containing a codewords of weight at most } n^\alpha\}$ (using naive UP).
- Prove that asymptotically $\Lambda_n \cdot \#B_0(n^\alpha) \leqslant \#\{\text{possible } g_I\}$.

Remark

The square-root bound is a similar result for QR codes (only for $R \leqslant 1/2$).

Uncertainty principle and G-codes

What about general G-codes?

Definition

Let $\emptyset \neq S \subseteq G$. A sequence $g_1, \ldots, g_t$ in G has **right S-rank** t if

$$Sg_i = \{sg_i \mid s \in S\} \nsubseteq \bigcup_{j<i} Sg_j \qquad \forall i \in \{2, \ldots, t\}.$$

For any $f \in KG$,

- $T_f : KG \to KG$ the map $v \mapsto fv$.
- $\mathcal{I}_f = \mathrm{Im}(T_f)$.

Lemma

Let $0 \neq f \in KG$ and $S = \mathrm{supp}(f)$. If $\exists$ a sequence in G with right S-rank $t \Rightarrow$

$$\dim \mathcal{I}_f = \mathrm{rank}_K(T_f) \geqslant t.$$

Uncertainty principle and G-codes

Generalization of Meshulam - 1992.

Theorem (B., Willems, Zini - 2022)

For any $0 \neq f \in KG$,

$$|\mathrm{supp}(f)| \cdot \mathrm{rank}_K(T_f) \geqslant |G|.$$

Corollary

For any nonzero G-code $\mathcal{C}$,

$$d(\mathcal{C}) \cdot \dim \mathcal{C} \geqslant |G|. \tag{1}$$

In particular,

$$2\sqrt{|G|} \leqslant d(\mathcal{C}) + \dim \mathcal{C} \leqslant |G| + 1.$$

Uncertainty principle and G-codes

Examples

- Let $\mathcal{C}$ be the self-dual $[24, 12, 8]$ Golay code, which is an S_4-code:

$$d(\mathcal{C}) \cdot \dim \mathcal{C} = 8 \cdot 12 = 96 > |G|.$$

- Let $\mathcal{C} = \mathcal{RM}(r, m)$, which is a G-code, for G an elementary abelian 2-group of rank m:

$$d(\mathcal{C}) \cdot \dim \mathcal{C} = 2^{m-r} \cdot \sum_{i=0}^{r} \binom{m}{i} \geqslant 2^{m-r} \cdot \sum_{i=0}^{r} \binom{r}{i} = 2^m = |G|.$$

Theorem (B., Willems, Zini - 2022)

A G-code $\mathcal{C}$ satisfies $d(\mathcal{C}) \cdot \dim \mathcal{C} = |G| \Leftrightarrow \exists H \leqslant G$ and $c \in KH$ s.t. $|H| = d(\mathcal{C})$, cKH has dimension 1 and $\mathcal{C} = cKG$.

Conclusion and outlook

Conclusion

- We presented arguments **for and against** the existence of asymptotically good families of cyclic codes.
- We presented different versions of the **uncertainty principle** and the relation with the problem above.
- **"Almost good" cyclic codes** of any asymptotic rate.

- Algebraic structure of the zeros of a cyclic code $\Rightarrow$ BCH bound.
- Algebraic structure of the zeros of a G-code, with G abelian and KG semisimple $\Rightarrow$ Shift bound (Feng, Hollmann, Xiang - 2019)

Outlook

- How to define **"zeros"** of $\mathcal{C}$ in relation to the submodules of $\mathcal{C}$, and hence to $\dim \mathcal{C}$ for general G-codes?
- Can we get **bounds better than** (1) for some families of G-codes?
- Other asymptotically good or "almost good" families of G-codes as before?

References

- M. Borello, P. Solé. *The uncertainty principle over finite fields*, Discrete Math. 345(1), 112670, **2022**.
- M. Borello, W. Willems, G. Zini. *On ideals in group algebras: an uncertainty principle and the Schur product*, `arXiv: 2202.12621`, **2022**.
- D.L. Donoho, P.B. Stark. *Uncertainty principles, and signal recovery*. SIAM J. Appl. Math. 49, 906–931, **1989**.
- S. Evra, E. Kowalski, A. Lubotzky. *Good cyclic codes and the uncertainty principle*. L'Enseignement Mathématique, 63, 305–332 **2017**.
- T. Tao. *An uncertainty principle for cyclic groups of prime order*. Mathematical Research Letters 12, 121–127 **2005**.

References

- M. Borello, P. Solé. *The uncertainty principle over finite fields*, Discrete Math. 345(1), 112670, **2022**.
- M. Borello, W. Willems, G. Zini. *On ideals in group algebras: an uncertainty principle and the Schur product*, `arXiv: 2202.12621`, **2022**.
- D.L. Donoho, P.B. Stark. *Uncertainty principles, and signal recovery*. SIAM J. Appl. Math. 49, 906–931, **1989**.
- S. Evra, E. Kowalski, A. Lubotzky. *Good cyclic codes and the uncertainty principle*. L'Enseignement Mathématique, 63, 305–332 **2017**.
- T. Tao. *An uncertainty principle for cyclic groups of prime order*. Mathematical Research Letters 12, 121–127 **2005**.

Thank you very much for the attention!