SCHUR PRODUCTS OF CODES AND ADDITIVE COMBINATORICS

NİHAN TANISALI

1. From Additive Combinatorics to Codes

My thesis aims to investigate multiplicative analogs in coding theory "namely analogs of so-called inverse theorems such as Vosper or Freiman Theorem". We start with some prerequisites from Additive combinatorics.

Definition 1.1 (Sumsets)**.** Let G be an abelian group. Let $A, B \subseteq G$ be non-empty, finite additive sets (subsets of G). The sumset $A + B$ is defined as

$$A + B := \{a + b \mid a \in A \text{ and } b \in B\}.$$

- A trivial upper bound for $|A + B|$ is $|A| \times |B|$ is $|A + B| \leq \frac{|A|(|A|+1)}{2}$
- For $A_1 \subset \mathbb{Z}$ with $|A_1| = 4$, the bound $6 + 4 = 10$ is attained where

$$A_1 := \{1, 3, 7, 15\}$$
$$A_1 + A_1 = \{2, 4, 6, 8, 10, 14, 16, 18, 22, 30\}.$$

Kneser theorem gives a lower bound for the size of sumsets, and Vosper theorem gives a classification of the structure of the sets which attain this bound.

Theorem 1.2 (Kneser)**.** *Let G be an abelian group. Let $A, B \subseteq G$ be non-empty, finite subsets. Then*

$$|A + B| \geq |A| + |B| - |\operatorname{St}(A + B)|.$$

where

$$\operatorname{St}(A + B) := \{g \in G : g + c \in A + B \text{ for all } c \in A + B\}.$$

Theorem 1.3 (Vosper)**.** *Let G be an abelian group of prime order p. Let $A, B \subset G$ be subsets, with $|A|, |B| \geq 2$ and $|A + B| \leq p - 2$. If*

$$|A + B| = |A| + |B| - 1$$

then A and B are arithmetic progressions with the same gap.

Now, we briefly give the notions that are required to explain the multiplicative analogs of Kneser and Vosper theorems in a coding theoretic context.

Definition 1.4 (Schur Product)**.**

- The Schur product of $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{F}_q^n$ is defined as

$$\alpha * \beta := (\alpha_1\beta_1, \ldots, \alpha_n\beta_n).$$

Date: July 13, 2025.

- Given two linear codes $A, B \subset \mathbb{F}_q^n$, the Schur product $A * B$ (or AB) denotes

$$\langle \alpha * \beta \mid \alpha \in A \text{ and } \beta \in B \rangle.$$

- For a linear code C, the Schur product $C * C$ (or C^2) is called the square of C.
- For $\alpha \in \mathbb{F}_q^n$, $\alpha * \mathcal{C}$ is a code, if α has full support $\dim(\alpha * \mathcal{C}) = \dim(\mathcal{C})$.

In cryptographic applications, one is interested in the dimension of $C * C$. Cascudo, Cramer and Zemor [2] proved that with high probability, for a random code C,

$$\dim(C * C) = \min\left(n, \frac{\dim C(\dim C - 1)}{2} + (\dim C)^2\right).$$

The main objective of my thesis is to classify codes with small $\dim(C^2)$.

Similar to the role of Cauchy Davenport in Vosper theorem, the following is crucial to prove the multiplicative analog of Vosper.

Theorem 1.5 (D. Mirandola, G. Zemor,[6])**.** *(Analog of Kneser) Let $S, T \subset K^n$ be non-zero K-vector spaces. Then*

$$\dim ST \geq \dim S + \dim T - \dim(\mathrm{St}(ST)).$$

where

$$\mathrm{St}(CD) := \{x \in \mathbb{F}_q^n \mid xCD \subset CD\}.$$

Theorem 1.6. *[D. Mirandola, G. Zemor,[6]]/(Analog of Vosper) Let $C, D \subset \mathbb{F}^n$ be MDS codes[1], with $\dim C, \dim D \geq 2$ and $\dim CD \leq n - 2$.*

$$\dim CD = \dim C + \dim D - 1$$

then C and D are Reed-Solomon codes with a common evaluation-point sequence.

Let the ambient space be $\mathbb{F}_q^8$ for $q \geq 7$. The following example illustrates why one considers to put MDS condition in the hypothesis of Theorem 1.6.

- Let the ambient space be ${\mathbb{F}_q}^8$ for $q \geq 4$

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

  Let $\mathcal{C}, \mathcal{A}$ to be the codes generated by G, H respectively. $\dim(\mathcal{C} * \mathcal{A}) = 3 \neq \dim(\mathcal{C}) + \dim(\mathcal{A}) - 1 = 4$.

Question 1.7. Is is possible to relax the MDS hypothesis?

[1] $\dim C + d_{\min} C = n + 1$

Question 1.8. Is it possible to extend this result to codes satisfying

$$\dim C * C = 2 \dim C - 1 + \gamma$$

for small values of γ? Algebraic geometry codes from curves of genus γ satisfy this property. Some subcodes of Reed–Solomon codes too. Is it possible to provide a complete classification of such codes?

1.1. **Current state.** I am working on $\gamma = 1$ case of Question 1.8. The expected codes are elliptic codes (evaluation of Riemann-Roch spaces over elliptic curves). I am working with Alain Couvreur and Gilles Zémor for this problem. We tried to follow the same path as [6]. Our fir

Lemma 1.9. *Let $\mathcal{C} \subseteq \mathbb{F}^n$ be a full support code with $\dim \mathcal{C} \geq 2$ and $d_{\min}(\mathcal{C}) > 1$. Assume there exists a 2 dimensional MDS code $\mathcal{A} \subseteq \mathbb{F}^n$ generated by $\langle 1, \alpha \rangle$ for some $\alpha \in F^n$ distinct entries such that*

$$\dim \mathcal{AC} = \dim \mathcal{A} + \dim C.$$

Then $\mathcal{C}$ is generated by $g_1\langle 1, \alpha, \ldots, \alpha^{l_1-1}\rangle \oplus g_2\langle 1, \alpha, \ldots, \alpha^{l_2-1}\rangle(\alpha)$ where $l_1 + l_2 = \dim(\mathcal{C})$.

The analog of lemma 1.9 for $\gamma = 0$ case is the main tool to prove theorem 1.6. However, for $\gamma = 1$, the case $\dim \mathcal{A} = 2$ is not sufficient. We are now trying to classify codes $\mathcal{C}$ with

$$\dim \mathcal{BC} = \dim \mathcal{B} + \dim C$$

for some MDS code $\mathcal{B}$. This problem turned out to be harder than I was hoping.

2. Second Project

Another research direction is based on a paper Sur les équations définissant une courbe algébrique by Saint Donat. The main statement is the following.

Proposition 2.1. Let $I \subset k[X_0, \ldots, X_{n-1}]$ be the homogeneous ideal associated to $\varphi(C)$. Then, I is generated by elements of degree 2 and 3. Moreover, if $\deg D \geq 2g + 2$ then I is generated by elements of degree 2.

With Alain Couvreur, we are translating this note in English while using a more basic language of curves. The aim is to use this proof in Freiman-like theorems on codes?.

3. TGRS

This part of my studies was a joint work with Ilaria Zappatore, Rakhi Pratihar and Alain Couvreur that I did in my first year of PhD. This third part is related to the first part of the work in the sense that it illustrates why it is useful to have classifications of small square codes in terms of cryptographic applications. More precisely, we develop a distinguisher using the smallness of dimension of the Schur square of a code with respect to the dimension of the code, and transform it into an attack.

Recently, in [1], TRS codes are proposed as an alternative to Goppa codes for the McEliece-based cryptosystem and example parameters are given that provides reduction

in key sizes than the original McEliece cryptosystem for the same security level. The authors also singled out a subfamily of twisted Reed-Solomon codes which they 'provably' claim to be resistant against several known structural attacks on the McEliece cryptosystem based on RS-like codes: Sidenlikov–Shestakov [8], Wieschebrink [9], Schur square-distinguishing [3]. For Wieschebrink's attack on the dual code and Wieschebrink's squaring attack [10] we could say only that the attack does not seem to apply.

There is an efficient key-recovery attack on the TRS variant proposed in [1] based on *subfield subcode* presented by Lavauzelle and Reiner [5], but that is for TRS codes with very constrained set of parameters.

The 1-twisted polynomials, and 1-twisted Reed Solomon Codes are of the form:

$$P := \mathcal{P}^{n,k}_{\mathbf{t},\mathbf{h},\eta} = \left\langle \left\{ 1, x, x^2, \ldots, \widehat{x^h}, \ldots, x^{k-1}, x^h + \eta x^{k-1+t} \right\} \right\rangle, \tag{1}$$

$$\mathcal{C} := \mathcal{C}^{n,k}_{\alpha,\mathbf{t},\mathbf{h},\eta} = \mathrm{ev}_\alpha(\mathcal{P}^{n,k}_{\mathbf{t},\mathbf{h},\eta}) \subset \mathbb{F}_q^n \tag{2}$$

where $\alpha \in \mathbb{F}_q^n$ have distinct entries and

$$\mathrm{ev}_\alpha(V) := \{f(\alpha) : \alpha \in V\}$$

defined for any set $V \subseteq \mathbb{F}_q^n$. We define the monomial space by

$$E := \left\langle \left\{ 1, x, x^2, \ldots, \widehat{x^h}, \ldots, x^{k-1} \right\} \right\rangle. \tag{3}$$

In this work we aimed the following:

- We realized that the claim that the distinguisher based attack [3] is not feasible for the subfamily is not completely correct. And we show that TRS codes can be distinguished from random by squaring some shortening of the code.
- We aim to give an efficient key-recovery attack for the McEliece scheme instantiated with TRS. The first step is to recover $\mathrm{ev}_\alpha(E)$.

We first oberved that

$$\dim(f * P + g * P + h * P) \quad \leq 2k + 2 \text{ if } f, g, h \in E$$

Our attack repeatedly made use of the fact that two polynomials $f, g \in \mathbb{F}_q[x]_{\leq n}$ with fixed degree a and b are coprime with probability $1 - \frac{1}{q}$. This fact leads to the fact that the quantity

$$\frac{|\{f, g, h \in E\}|}{|\{f, g, h \in P : \dim(fP + gP + hP) \leq 2k + 2\}|}$$

is "close" to 1. Using this, we give an algorithm to recover a basis for E.

4. Formation, Presentations, and other

4.1. **Formation.**

- Scientific Formation (Required: 40-60):

  I already have 40+ credits:

  Three Encode schools (the phd network I am in is called Encode).

I followed a course on quantum computing offered by Thomas Debris-Alazard in my first year.

- Language (Required: 0-20): I took 20+ language courses in French as well
- Non-scientific Formation (Required: 40-60):

  I took only 7 credits of ethics. I need to have 33 more credits in my last year

4.2. **Presentations.** This year, I gave the following talks:

- Box Progressions and Abelian Power Free Words, Journees Arithmetiques slides
- On the structure of the Schur squares of Twisted Generalized Reed-Solomon codes and application to cryptanalysis, Journées Codage et Cryptographie , PQ Crypto, and ENCODE summer school slides
- A Schur-Square Analysis of Twisted Generalized Reed-Solomon Codes, Inria Paris

4.3. **Visa Issues.** I am a part of a European doctoral network called Encode. Every student has a cosupervisor. My cosupervisor is in University College Dublin.

Since I am not European, and Ireland is not Schengen I have to get a visa. However, applying for an Irish visa as a French resident is hard. For example, if you want to stay in Ireland for 3 months, you have to have a valid residence permit in France for 5 months: 2 months for Ireland to produce the visa, 3 months of stay, and the residence permit must be valid when you come back to France. This, I think I never had.

In France, I have some problems about the permit. For example, after I apply for a residence permit with all the documents required, the prefecture wants me to add other documents after 2 months. These new documents are not in the original list, and they repeat this two times. The point is, since they ask additional files, they do not give me the residence permit card for one year, rather they give me travel documents for short-term. It would be more easy for everyone to clearly list all required documents at once.

I also think, for students in doctoral networks, it would be much more easy to get the visa when they were in their home country. It was really hard for me to find translators in Paris, to ask the bank sign a document (they reject to sign or ask me to take an appointment after a week or so) and etc. I think, it is hard by itself as I do not speak French well. But also, some people are not really friendly with foreigners from some countries. To sum up, in my country, I was able to do these things efficiently in a well-organized manner. However, in France, I do not know what to do to get what I want.

References

[1] Beelen, P., Bossert, M., Puchinger, S., Rosenkilde, J., *Structural properties of twisted Reed-Solomon codes with applications to cryptography*, In 2018 IEEE International Symposium on Information Theory (ISIT) (pp. 946–950), IEEE.

[2] Cascudo, I., Cramer, R., Mirandola, D., Zémor, G. (2015). Squares of random linear codes. IEEE Transactions on Information Theory, 61(3), 1159-1173.

[3] Couvreur, A., Gaborit, P., Gauthier-Umaña, V., Otmani, A., Tillich, J. P. *Distinguisher-based attacks on public-key cryptosystems using Reed–Solomon codes*, Designs, Codes and Cryptography, **73**, 641–666, (2014).

[4] Couvreur A., Márquez-Corbella I., Pellikaan R., "Cryptanalysis of McEliece Cryptosystem Based on Algebraic Geometry Codes and Their Subcodes," in IEEE Transactions on Information Theory, vol. 63, no. 8, pp. 5404-5418, Aug. 2017, doi: 10.1109/TIT.2017.2712636. keywords: Geometry;Decoding;Public key cryptography;Proposals;Algebraic geometry codes;McEliece public key cryptosystem;error-correcting pair,

[5] Lavauzelle, J., Renner, J., *Cryptanalysis of a system based on twisted Reed–Solomon codes*, Designs, Codes and Cryptography, **88(7)**, (2020), 1285–1300.

[6] Mirandola, D., Zémor, G. (2015). Critical pairs for the product singleton bound. IEEE Transactions on Information Theory, 61(9), 4928-4937.

[7] Randriambololona, H. (2015). On products and powers of linear codes under componentwise multiplication. Algorithmic arithmetic, geometry, and coding theory, 637, 3-78.

[8] V.M. Sidelnikov and S.O. Shestakov, *On the insecurity of cryptosystems based on generalized Reed-Solomon codes*, Discrete Math. Appl., **1(4)** , pp. 439–444, 1992.

[9] C. Wieschebrink, *An Attack on a Modified Niederreiter Encryption Scheme*, in PKC, vol. 3958. Springer, 2006, pp. 14–26.

[10] C. Wieschebrink, *Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes*, In Post-Quantum Cryptography 2010, volume 6061 of LNCS, pages 61–72. Springer, 2010.

[11] B. Saint-Donat, Sur les équations définissant une courbe algébrique, 1972

Centre de recherche INRIA Saclay, Laboratoire LIX, CNRS UMR 7161, France
Email address: nihan.tanisali@inria.fr