Applications of Pellikaan Decoding to Small Binary Linear Codes

Julien du Crest
supervised by Gilles Zemor

Institut Mathematique de Bordeaux

June 10, 2020

Overview

Pellikaan Decoding

The L^2 Construction

Lowrank Decoding

Experimental results

- Reed-Muller Codes
- Projective Geometry Codes
- Concatenated Codes

Pellikaan Decoding

Definitions

Schur Product

Given $u = (u_1, ..., u_n), v = (v_1, ..., v_n)$,

$$uv = (u_1 v_1, ... u_n v_n)$$

Product Code

Given two linear codes C, D,

$$CD = \{cd, \quad c \in C, d \in D\}$$

Pellikaan Decoding

Definitions

Given three linear codes

- $C : [n, k, \_]$ (*encoding code*)
- $L : [n, p+1, \_]$ (*locator code*)
- $\Pi = CL$ (*product code*)

C is used to encode the codewords, L and Π to decode.

$$y = c + e \quad (|e| = p)$$

Pellikaan Decoding

1. Find $l \in L$ such that $ly \in \Pi$
2. Find c^* such that $c^* l = yl$
3. Return c^*

Pellikaan Decoding

Necessary Conditions

1. $\dim L > p$

   $\exists l \in L \ s.t. \ le = 0$

2. $\dim L + \dim \Pi \leqslant n$

   $ly = \pi, l \in L, \pi \in \Pi$ has less variables than equations

3. dmin $\Pi > p$

   $yl = \pi \implies el = (0, ..., 0)$

4. dmin $L +$ dmin $C > n$

   $\exists! c^* \ s.t. \ c^* l = yl$

Pellikaan Decoding

Necessary Conditions

1. $\dim L > p$

   $\exists l \in L \text{ s.t. } le = 0$

2. $\dim L + \dim \Pi \leqslant n$

   $ly = \pi, l \in L, \pi \in \Pi$ has less variables than equations

3. $\text{dmin } \Pi > p$

   $yl = \pi \implies el = (0, ..., 0)$

4. $\text{dmin } L + \text{dmin } C > n$

   $\exists! c^* \text{ s.t. } c^* l = yl$

Relaxation

Conditions 3 and 4 are removed

The L^2 Construction

1. Generate L
2. Compute L^2
3. Let $C = {L^2}^{\perp}$

$$
\begin{aligned}
< c, ll' > = < cl, l' > &\implies CL \subset L^{\perp} \\
&\implies \dim \Pi + \dim L \leqslant n
\end{aligned}
$$

Verified Conditions

Just fix $p < \dim L$ and conditions 1 and 2 are verified

My Work

Lowrank Decoding

Motivations

Pb 1 : The Binary Curse

$\mathbf{E}(|l|) \approx \frac{n}{2}$ implies $\{c^* \ s.t. \ c^* l = yl\}$ is big
Solution : Take the union of several l instead

$$
\begin{aligned}
S &= \{l \in L \ s.t. \ ly \in \Pi\} \\
&= \underset{le=0}{S^*} \oplus \underset{le\neq 0}{S^\dagger}
\end{aligned}
$$

Pb 2 : Exponantial growth of Parasites

The sum of a non-parasite and a parasite is a parasite
Solution : **None**

Lowrank Decoding

A Different Approach

Low Rank of $S_{|e}$

$\dim S_{|e} = \dim S^{\dagger}$

So if $\dim S \gg \dim S^{\dagger}$, the difference is noticeable...

But we can't test all p-subsets to find it !

Lowrank Decoding

A Different Approach

Low Rank of $S_{|e}$

$\dim S_{|e} = \dim S^{\dagger}$
So if $\dim S \gg \dim S^{\dagger}$, the difference is noticeable...
But we can't test all p-subsets to find it !

Idea : The columns of $S_{|e}$ appear more often that they should

Lowrank Decoding Algorithm

1. Count the appearances of each column
2. 'Remove' the most appearing ones
3. Decode on the remaining positions

Experimental Results

Code	n	k	p	succ.	dmin fail.	other fail.	p^*
Random Codes	200	80	14	.80	.001	0.19	17
Random Codes*	200	79	14	.999	.001	0.	17
Bin. Reed-Muller	256	93	31	.999	.001	0.	23
Qary Reed-Muller	256	85	30	.98	.02	0	26
Proj. Geom.	585	184	60	1.	.00?	0.	$60^{\approx}$

Table: Comparaison de differents codes

Additional Results

Caracterisation of S

$$\dim S^* = \dim L - |e| + \dim \Pi_{\subset e}$$
$$\dim S^\dagger \leqslant \dim \Pi_{\subset e}$$

where $\Pi_{\subset e} = \{\pi \in \Pi \text{ } s.t. \text{ } supp(\pi) \subset supp()\}$

The Kernel Mystery Revealed

$$\cancel{\dim \ker IC \approx \dim C - |I|}$$
$$\dim \ker IC \approx \dim C - |I| + \dim L$$

Conclusion

Pros	Cons
Correct more errors	Probabilistic failures
Algebraic Method	Any usage (Crypto, Codes)?

Bibliography

Le décodage de codes linéaires par paires localisatrices d'erreur
Elie Bouscatie, Célian Banquet - 2020

http://www.codetables.de/
Marcus Grassl

On decoding linear codes by error correcting pairs
Ruud Pellikaan - 1988