The syzygy distinguisher

Hugues Randriambololona

ANSSI, Laboratoire de cryptographie

Abstract. We present a new distinguisher for alternant and Goppa codes, whose complexity is subexponential in the error-correcting capability, hence better than that of generic decoding algorithms. Moreover it does not suffer from the strong regime limitations of the previous distinguishers or structure recovery algorithms: in particular, it applies to the codes used in the `Classic McEliece` candidate for postquantum cryptography standardization. The invariants that allow us to distinguish are graded Betti numbers of the homogeneous coordinate ring of a shortening of the dual code.
Since its introduction in 1978, this is the first time an analysis of the McEliece cryptosystem breaks the exponential barrier.

1 Introduction

In the McEliece cryptosystem [20], a private message is encoded as a codeword in a public binary Goppa code [13], with some noise added. Knowing the secret algebraic data that served to construct the public code, the legitimate recipient has an efficient decoding algorithm and can recover the message. However, to an attacker, the public code looks like a random code, and removing the noise is untractable.

Slightly more formally, a security proof for the system relies on two assumptions:

1. Goppa codes are computationally indistinguishable from generic linear codes (say, when described by generator matrices in reduced row echelon form).
2. Decoding a generic linear code is difficult.

Cryptanalytic attempts can be classified depending on whether they target assumption 1 or 2.

First, those aiming at assumption 1 themselves come in two flavours:

- *Distinguishers* address the decisional version of the problem: given a generator matrix, decide whether it is that of a Goppa code or a generic code.
- *Key recovery attacks* address the computational version: recover the Goppa structure of the code, or at least an equivalent one [12], if it exists.

Although certain arguments, such as the fact that the class of Goppa codes is very large, make assumption 1 plausible, it remains quite ad hoc from a theoretical point of view. Its sole virtue is that it passed the test of time. There seems to be something special with Goppa codes happening there: indeed, variants of the McEliece system were proposed, with Goppa codes replaced with other types of codes allowing more manageable parameters; however, most of these propositions were eventually broken, as the hidden structure of the codes could be recovered. Also, although the McEliece cryptosystem marked the birth of code-based cryptography, the idea of having an object (such as a Goppa code) constructed from data defined over an extension field and then masked by considering it over a small subfield, was then found in other branches of cryptography: for instance it is at the basis of the HFE cryptosystem [23] in multivariate cryptography. Such systems can often be attacked by algebraic methods (including, but not limited to, the use of Gröbner basis algorithms). This suggests that if a weakness in assumption 1 were to be uncovered one day, then algebraic methods should be a tool of choice. However, up to now, the best distinguishers and key recovery algorithms such as those in [11][7][6][1] only apply to alternant or Goppa codes with very degraded parameters. Against McEliece with cryptographically relevant parameters, either they have exponential complexity with large constants, which makes them useless, or worse: they simply cease to work.

Assumption 2, on the other hand, stands on a firm theoretical ground: the decoding problem for generic linear codes is known to be NP-hard [2]. As such, it is believed to resist the advent of quantum computers, which made the McEliece system a good candidate for postquantum cryptography. However, starting with Prange's information set decoding algorithm [24], generic decoding methods saw continuous incremental improvements over time. Joint with technological progress in computational power, this eventually led to practical *message recovery attacks* against the McEliece system with its initially proposed parameter set. However, it appears that this weakness was only the result of a too optimistic choice of parameters. With the need for new standards for postquantum cryptography, an updated version named `Classic McEliece` was proposed, still relying on binary Goppa codes, but with more conservative parameter sets adapted to resist the best generic decoding attacks with some margin of safety. In the design rationale of this new system [4] one can find an impressive list of several dozens of papers on generic decoding algorithms, ranging over the last five decades. It is then observed that all these algorithms have complexity exponential in the error-correcting capability of the code. Better, the constant in this exponential is still the same as in Prange's original result: all improvements remain confined in terms of lesser order! This gives a quite convincing feeling that we could possibly have reached the intrinsic complexity of cryptanalysis of this system.

This belief is false, and there is nothing special with Goppa codes. In this work, we present a new distinguisher for alternant and Goppa codes, i.e. a basic structural analysis of the McEliece cryptosystem, whose complexity is subexponential in the error-correcting capability, hence better than that of generic decoding algorithms. Moreover it does not suffer from the strong regime limitations of the previous distinguishers or key recovery methods: in particular, it applies to the codes used in `Classic McEliece`.

Principles and organization

A natural strategy to build a distinguisher is to design code invariants — quantities that intrinsically depend only on the code, not on the choice of a generator matrix — that behave differently for the classes of codes we want to distinguish. The invariants we use here are graded Betti numbers of the homogeneous coordinate ring of a shortening of the dual code. Generators of the dual of an alternant or Goppa code, after extension of scalars, satisfy quadratic relations of a special form: they can be expressed as 2×2 minors of a matrix. As such, we can find relations between these quadratic relations, called *syzygies*. Then these syzygies also satisfy relations, and iterating this process we get higher syzygies up to some order that we can estimate. However, for generic codes, we do not expect this to happen in the same magnitude. This directly gives a distinguisher, at least in theory. In practice, computing these spaces of syzygies only involves basic linear algebra: they can be constructed iteratively, as the kernel of some generalized Macaulay matrices. This can be done efficiently, except for the fact that the dimension of the spaces involved grows exponentially. Our last ingredient is then shortening, which allows us to work with syzygies of a lesser order, and keep these dimensions more under control.

Let us quickly illustrate our result with two basic examples.

First, our distinguisher can be seen as a generalization of the so-called *square code* distinguisher, first presented in [11], reinterpreted in [19], and fully analyzed in [21]. Let C be a $[n, k]$-code, and S_2 the space of quadratic forms in k indeterminates. Let

$$\mathrm{ev}_2 : S_2 \longrightarrow \mathbb{F}^n \tag{1}$$

be the evaluation map at the columns of a given generator matrix of C. Then the image of ev_2 is the square code $\mathsf{C}^{\langle 2 \rangle}$, and its kernel is the space of quadratic relations $I_2(\mathsf{C})$. The dimensions of these spaces are related, and can be expressed as a Betti number:

$$\beta_{1,2}(\mathsf{C}) = \dim(I_2(\mathsf{C})) = \binom{k+1}{2} - \dim(\mathsf{C}^{\langle 2 \rangle}). \tag{2}$$

Now [11] gives a lower bound on this $\beta_{1,2}(\mathsf{C})$ when C is an alternant or (binary) Goppa code. On the other hand, [3] shows $\beta_{1,2}(\mathsf{C}) = \left(\binom{k+1}{2} - n\right)^+$ with high probability when C is random. If this quantity is smaller than the said lower bound, we can distinguish.

Likewise we claim that Theorem 2.8 of [9] provides a $\beta_{2,3}$-based distinguisher for GRS codes among $[7, 4]$-codes, where we restrict to codes whose square is the whole space — otherwise we can use the square distinguisher. For such a code we always have $\dim(I_2(\mathsf{C})) = \binom{4+1}{2} - 7 = 3$. Let Q_1, Q_2, Q_3 be a basis of $I_2(\mathsf{C})$. By definition, Q_1, Q_2, Q_3 do not satisfy linear relations with coefficients in $\mathbb{F}$, however they can satisfy relations whose coefficients are forms of degree 1. Such relations are also called degree 3 syzygies. They live in the kernel of the degree 3 Macaulay matrix

$$\mathbf{M}_3 : I_2(\mathsf{C}) \otimes S_1 \longrightarrow S_3 \tag{3}$$

where S_1 (resp. S_3) is the space of homogeneous linear (resp. cubic) forms in $k = 4$ variables. Now Theorem 2.8 of [9] shows that for a non-GRS code the map $\mathbf{M}_3$ is injective. On the other hand, if C is GRS with standard basis $\mathbf{y}, \mathbf{yx}, \mathbf{yx}^2, \mathbf{yx}^3$ then we can take

$$Q_1 = X_1X_3 - X_2^2, \quad Q_2 = X_1X_4 - X_2X_3, \quad Q_3 = X_2X_4 - X_3^2 \tag{4}$$

and these satisfy the syzygies

$$X_1Q_3 - X_2Q_2 + X_3Q_1 \;=\; X_2Q_3 - X_3Q_2 + X_4Q_1 \;=\; 0. \tag{5}$$

Thus we can distinguish by computing $\beta_{2,3}(\mathsf{C}) = \dim\ker(\mathbf{M}_3)$, which will yield 2 for GRS and 0 for non-GRS $[7, 4]$-codes.

We generalize these examples to higher Betti numbers, following the exact same pattern:

- On one hand, we give lower bounds on the Betti numbers of algebraic codes (dual alternant, dual Goppa, and their shortened subcodes). This is done in section 3, using the Eagon-Northcott complex, a tool precisely crafted to detect long conjugate GRS subcodes.
- On the other hand, we estimate the Betti numbers of random codes in terms of raw code parameters (length, dimension, distance). This is done in section 4, partially relying on heuristics for which we do not have full proofs, but still providing experimental evidence, and sometimes also partial theoretical arguments.

Prior to that, section 2 explains how these invariants can be effectively computed. Last, section 5 combines everything and chooses parameters in order to optimize asymptotic complexity.

Related (and unrelated) works

As already noted, our distinguisher can be seen as a generalization of the square distinguisher of [11]. Using an approach similar to ours, the work [6] also extends this square distinguisher by exploiting special properties of the space of quadratic relations, but in a different direction. Last, the key recovery attack in [1] combines shortening of the dual code with ideas from the square distinguisher, and a careful algebraic modeling in order to apply tools from Gröbner basis theory. All these results have limited range of applicability, but they introduced numerous techniques that influenced the present work.

From a geometric point of view, the Betti numbers and the syzygies we consider are those of a set of points in projective space (namely, defined by the columns of a parity check matrix of the code). As such, they have been already extensively studied. Of notable importance to us are the works [14][18][16][10], in relation with the so-called *minimal resolution conjecture* — regardless of it being false in general: we just request it being "true enough". Initially, syzygies of sets of points were considered as a mere tool in the study of syzygies of curves. They were then studied for themselves, but the focus was mostly on points in generic position, over an algebraically closed field. Keeping applications to coding theory and cryptography in mind, we will have more interest in finite field effects.

Syzygies sometimes appear as a tool in cryptanalytic works, or in the study of Gröbner basis algorithms; however in general only the first module of syzygies is considered, not those of higher order. Likewise, a few works in coding theory (such as [26] or [15]) use homological properties of finite sets of points; but the applications differ from ours.

Last, note that our approach is apparently unrelated to the series of works initiated with [17]: while these authors also define Betti numbers for codes, these are constructed from the Stanley-Reisner ring of the code matroid, not the homogeneous coordinate ring. This leads to different theories, although seeking links between the two could be an interesting project.

Acknowledgements

The author learned a lot from the code-based cryptography seminar organized by Jean-Pierre Tillich at Inria Paris. More important perhaps, without his friendly pressure, probably this work would have stayed eternally in limbo. He should be thanked for all that. The very favourable environment towards research at ANSSI in general, and at LCR in particular, was also highly helpful. Henri Gilbert's advices led to improvements in several aspects of the presentation. Anonymous members of LCR unsuccessfully suggested the title "The Dyztynguysher" for this work.

The author is part of the ANR-21-CE39-0009 BARRACUDA and ANR-21-CE39-0008 KLEPTOMANIAC research projects. Some of the computations were done on the `lame` servers in Télécom Paris.

Notation and conventions

We use row vector convention. We try to consistently use lowercase bold font for codewords and vectors: $\mathbf{c}$, $\mathbf{x}$, $\mathbf{y}$; uppercase bold for matrices: $\mathbf{G}$, $\mathbf{H}$, $\mathbf{M}$; sans-serif for codes: C, GRS, Alt, Gop.

The book [9] will be our main source on syzygies. For codes, especially the link between powers of codes and the geometric view on coding theory, we will follow [25].

Given a field $\mathbb{F}$, we see $\mathbb{F}^n$ as the standard product algebra of dimension n. Thus $\mathbb{F}^n$ is not a mere vector space, it comes canonically equipped with componentwise multiplication: for $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$ in $\mathbb{F}^n$,

$$\mathbf{x}\mathbf{y} = (x_1 y_1, \dots, x_n y_n). \tag{6}$$

(Some authors call this the Schur product of $\mathbf{x}$ and $\mathbf{y}$; how the name of this great mathematician ended associated with this trivial operation is quite convoluted.)

In any algebra, we can define a trace bilinear form. In the case of $\mathbb{F}^n$, this trace bilinear form is the standard scalar product:

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + \dots + x_n y_n. \tag{7}$$

A k-dimensional subspace $\mathsf{C} \subseteq \mathbb{F}^n$ is called a $[n,k]$-code (and a $[n,k]_q$-code in case $\mathbb{F} = \mathbb{F}_q$). The orthogonal space $\mathsf{C}^\perp$ is called the *dual code* of C.

Componentwise multiplication extends to codes, taking the linear span: for $\mathsf{C}, \mathsf{C}' \subseteq \mathbb{F}^n$,

$$\mathsf{C}\mathsf{C}' = \langle \mathbf{c}\mathbf{c}' : \ \mathbf{c} \in \mathsf{C},\, \mathbf{c}' \in \mathsf{C}' \rangle_{\mathbb{F}}. \tag{8}$$

Powers $\mathsf{C}^{\langle r \rangle}$ of a code are defined inductively: $\mathsf{C}^{\langle 0 \rangle} = \mathbb{F} \cdot \mathbf{1}$ is the 1-dimensional repetition code, and $\mathsf{C}^{\langle r+1 \rangle} = \mathsf{C}^{\langle r \rangle}\mathsf{C}$.

If C is a $[n,k]$-code, a generator matrix for C is a $k \times n$ matrix $\mathbf{G}$ whose rows $\mathbf{c}_1, \dots, \mathbf{c}_k$ form a basis of C. A parity check matrix $\mathbf{H}$ for C is a generator matrix for $\mathsf{C}^\perp$.

Thanks to the algebra structure, polynomials in one or several variables can be evaluated in $\mathbb{F}^n$. In particular, let

$$S = \mathbb{F}[X_1, \dots, X_k] \tag{9}$$

be the algebra of polynomials in k variables over $\mathbb{F}$, graded by total degree. Evaluation at the rows $\mathbf{c}_1, \dots, \mathbf{c}_k$ of $\mathbf{G}$ then gives linear map

$$\mathrm{ev}_{\mathbf{G}} : S \longrightarrow \mathbb{F}^n. \tag{10}$$

Observe that if $\mathbf{p}_1, \dots, \mathbf{p}_n$ are the columns of $\mathbf{G}$, then for $f(X_1, \dots, X_k) \in S$ we have

$$\begin{aligned} \mathrm{ev}_{\mathbf{G}}(f) &= f(\mathbf{c}_1, \dots, \mathbf{c}_k) \\ &= (f(\mathbf{p}_1), \dots, f(\mathbf{p}_n)) \end{aligned} \tag{11}$$

where in the first line we have one evaluation of f at a k-tuple of vectors, while in the second line we have a vector of evaluations of f at k-tuples of scalars.

A code is projective if it has dual minimum distance $\mathrm{d}_{\min}(\mathsf{C}^\perp) \geq 3$, or equivalently if no two of the $\mathbf{p}_i$ are proportional. Any code can be "projectivized" by discarding (puncturing) coordinates, keeping only one $\mathbf{p}_i$ in each nonzero proportionality class.

Restricting to homogeneous polynomials of degree r, we have a *surjective* map $S_r \longrightarrow \mathsf{C}^{\langle r \rangle}$, whose kernel we denote $I_r(\mathsf{C})$. We then define the homogeneous coordinate ring of C:

$$\mathsf{C}^{\langle \cdot \rangle} = \bigoplus_{r \geq 0} \mathsf{C}^{\langle r \rangle} \tag{12}$$

and its homogeneous ideal:

$$I(\mathsf{C}) = \bigoplus_{r \geq 0} I_r(\mathsf{C}). \tag{13}$$

It turns out these are also the homogeneous coordinate ring and the homogeneous ideal of the finite set of points

$$\{\mathbf{p}_1, \dots, \mathbf{p}_n\} \subseteq \mathbf{P}^{k-1}. \tag{14}$$

The short exact sequence

$$0 \longrightarrow I(\mathsf{C}) \longrightarrow S \longrightarrow \mathsf{C}^{\langle\cdot\rangle} \longrightarrow 0 \tag{15}$$

makes $\mathsf{C}^{\langle\cdot\rangle}$ a homogeneous quotient ring of S. In this work we will use coordinates, but identifying S with the symmetric algebra of C would allow to make all this coordinatefree.

Given $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$, all entries of $\mathbf{x}$ distinct, all entries of $\mathbf{y}$ nonzero, the *generalized Reed-Solomon code* of order k with support vector $\mathbf{x}$ and multiplier $\mathbf{y}$ is

$$\mathsf{GRS}_k(\mathbf{x}, \mathbf{y}) = \langle \mathbf{y}, \mathbf{y}\mathbf{x}, \dots, \mathbf{y}\mathbf{x}^{k-1} \rangle_{\mathbb{F}} = \{\mathbf{y}f(\mathbf{x}) :\ f(X) \in \mathbb{F}[X]_{<k}\} \subseteq \mathbb{F}^n. \tag{16}$$

It is a $[n, k]$-code if $k \leq n$.

Now let $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ be an extension of finite fields. Given $\mathbf{x}, \mathbf{y} \in (\mathbb{F}_{q^m})^n$ satisfying the same conditions as above, the *alternant code* of order t and extension degree m over $\mathbb{F}_q$, with support $\mathbf{x}$ and multiplier $\mathbf{y}$, is

$$\begin{aligned} \mathsf{Alt}_t(\mathbf{x}, \mathbf{y}) &= \mathsf{GRS}_t(\mathbf{x}, \mathbf{y})^{\perp} \cap (\mathbb{F}_q)^n \\ &= \{\mathbf{c} \in (\mathbb{F}_q)^n :\ c_1 y_1 x_1^j + \dots + c_n y_n x_n^j = 0 \quad (0 \leq j < t)\}, \end{aligned} \tag{17}$$

with parameters $[n, (\geq) n - mt]_q$.

Last, given a polynomial $g(X) \in \mathbb{F}_{q^m}[X]$ that does not vanish on any entry of $\mathbf{x}$, the q-ary *Goppa code* with support $\mathbf{x}$ and Goppa polynomial g is

$$\mathsf{Gop}(\mathbf{x}, g) = \mathsf{Alt}_{\deg(g)}(\mathbf{x}, g(\mathbf{x})^{-1}). \tag{18}$$

We will work mostly in the class

$$\mathsf{Alt}^{\perp}_{q,m,n,t} \tag{19}$$

of *dual* q-ary alternant codes of extension degree m, length n, and order t. If q is unspecified we take $q = 2$. If n is unspecified we take $n = q^m$. We say a code $\mathsf{C} \in \mathsf{Alt}^{\perp}_{q,m,n,t}$ is *proper* if it has dimension

$$k = mt. \tag{20}$$

In this case, after extension of scalars, we have

$$\mathsf{C}_{\mathbb{F}_{q^m}} = \mathsf{GRS}_t(\mathbf{x}, \mathbf{y}) \oplus \mathsf{GRS}_t(\mathbf{x}^q, \mathbf{y}^q) \oplus \dots \oplus \mathsf{GRS}_t(\mathbf{x}^{q^{m-1}}, \mathbf{y}^{q^{m-1}}). \tag{21}$$

Likewise we define the corresponding class

$$\mathsf{Gop}^{\perp}_{q,m,n,t} \tag{22}$$

of dual Goppa codes, and $\mathsf{C} \in \mathsf{Gop}^{\perp}_{q,m,n,t}$ is said proper if it is when seen in $\mathsf{Alt}^{\perp}_{q,m,n,t}$. Also we define subclasses $\mathsf{Gop}^{\mathrm{irr},\perp}_{q,m,n,t} \subseteq \mathsf{Gop}^{\mathrm{sqfr},\perp}_{q,m,n,t} \subseteq \mathsf{Gop}^{\perp}_{q,m,n,t}$, in which the Goppa polynomial is irreducible or squarefree, respectively.

2 Minimal resolutions and graded Betti numbers

Generalities

We freely borrow results and terminology from [9], and then elaborate on the parts of the theory that we will need.

Let $S = \mathbb{F}[X_1, \ldots, X_k]$ be the k-dimensional polynomial ring over $\mathbb{F}$, graded by total degree. If M_0 is a finitely generated graded S-module, and F_0 is the free module on a minimal system of homogeneous generators of M_0, then the (first) syzygy module of M_0 is $M_1 = \ker(\ F_0 \longrightarrow M_0\ )$. Iterating this construction, we obtain a minimal resolution

$$\cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \tag{23}$$

of M_0, where the graded free modules F_i, together with the iterated syzygy modules M_i, are constructed inductively:

- F_i is the free module on a minimal system of homogeneous generators of M_i
- $M_{i+1} = \ker(\ F_i \longrightarrow M_i\ )$.

Thus the F_i are of the form

$$F_i = \bigoplus_{j \geq 0} S(-j)^{\beta_{i,j}} \tag{24}$$

where $S(-j)$ is the free S-module of rank 1 generated in degree j, so $S(-j)_d = S_{d-j}$; and $\beta_{i,j}$, the (i,j)-th graded Betti number of M_0, is the number of elements of degree j in a minimal system of generators of M_i.

From now on let C be a $[n,k]$-code, and $M_0 = \mathsf{C}^{\langle\cdot\rangle}$ its homogeneous coordinate ring. Then M_0 is a dimension 1 Cohen-Macaulay quotient of S, and by the Auslander-Buchsbaum formula its minimal resolution has length $k-1$. So we have an exact sequence

$$0 \longrightarrow F_{k-1} \longrightarrow \cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 = S \longrightarrow \mathsf{C}^{\langle\cdot\rangle} \longrightarrow 0 \tag{25}$$

with $M_0 = \mathsf{C}^{\langle\cdot\rangle}$, $F_0 = S$, $M_1 = I(\mathsf{C})$, hence $\beta_{0,0}(\mathsf{C}) = 1$, $\beta_{0,j}(\mathsf{C}) = 0$ for $j \neq 0$, and $\beta_{1,j}(\mathsf{C})$ is the number of homogeneous polynomials of degree j in a minimal system of generators of $I(\mathsf{C})$.

It is customary to display the graded Betti numbers in the form of a Betti diagram, as follows:

	0	1	...	i	...	$k-1$
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
r	$\beta_{0,r}$	$\beta_{1,r+1}$	...	$\beta_{i,r+i}$	...	$\beta_{k-1,r+k-1}$
$r+1$	$\beta_{0,r+1}$	$\beta_{1,r+2}$	...	$\beta_{i,r+i+1}$	...	$\beta_{k-1,r+k}$
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$

with null entries marked as "$-$" for readability. In our situation, as $F_0 = S$, the 0-th column of the Betti diagram is always $(1, -, -, \ldots)^\top$.

By the minimality property of the resolution, if for some i and D we have $\beta_{i,j} = 0$ for all $j \leq D$, then also $\beta_{i+1,j} = 0$ for all $j \leq D+1$. Applied recursively, this means all the upper-right quadrant of the Betti diagram defined by $\beta_{i,D}$ vanishes. In particular, as the evaluation map $S_1 \longrightarrow C$ is an isomorphism, we see that $I(\mathsf{C})$ is generated in degrees ≥ 2, which implies:

Lemma 1. *For any $i \geq 1$, the i-th syzygy module M_i of C is generated in degrees $\geq i+1$. Thus we have $F_{i,j} = M_{i,j} = 0$ for $j \leq i$, and*

$$F_{i,i+1} = M_{i,i+1} = \mathbb{F}^{\beta_{i,i+1}}. \tag{26}$$

Hence the 0-th row of the Betti diagram is $(1, -, -, \dots)$.

Figures 1-3 offer a few such diagrams for contemplation.

	0	1	2	3
0	1	–	–	–
1	–	3	–	–
2	–	1	6	3

Fig. 1. the $[7,4]_2$ Hamming code

	0	1	2	3	4	5
0	1	–	–	–	–	–
1	–	10	16	–	–	–
2	–	1	5	26	20	5

Fig. 2. the $[11,6]_3$ Golay code

	0	1	2	3	4	5	6	7	8	9	10	11
0	1	–	–	–	–	–	–	–	–	–	–	–
1	–	55	320	891	1408	1210	320	55	–	–	–	–
2	–	1	11	55	220	650	1672	1870	1221	485	110	11

Fig. 3. the $[23,12]_2$ Golay code ($d = 7$, $d^\perp = 8$)

Effective computation

There are several algorithms to compute minimal resolutions and graded Betti numbers in general. Many of them rely first on a Gröbner basis computation. However in this work we will only be interested in computing the first (nontrivial) row of the Betti diagram, or equivalently, the so-called *linear strand* of the resolution. This easier computation can be described in elementary terms. First, for any $r \geq 3$, consider the natural multiplication map

$$\varphi_r : M_{r-2,r-1} \otimes S_1 \longrightarrow M_{r-2,r}. \tag{27}$$

Lemma 2. *We have:*

$$\ker(\varphi_r) = M_{r-1,r} \simeq \mathbb{F}^{\beta_{r-1,r}} \tag{28}$$

$$\operatorname{coker}(\varphi_r) \simeq \mathbb{F}^{\beta_{r-2,r}}. \tag{29}$$

Proof. We prove (29) first. Let $\mathcal{G}$ be a minimal system of homogeneous generators of M_{r-2}, and for each j let $B_{r-2,j} \subseteq M_{r-2,j}$ be the linear subspace generated by the degree j elements of $\mathcal{G}$. Then, as M_{r-2} is generated in degrees $\geq r-1$, we have $B_{r-2,r-1} = M_{r-2,r-1}$, and $B_{r-2,r}$ is a supplementary subspace to $S_1 \cdot B_{r-2,r-1} = \mathrm{im}(\varphi_r)$ in $M_{r-2,r}$. This proves (29).

Now let F_{r-2} be the free graded module on $\mathcal{G}$. Then $M_{r-1,r}$ is the kernel of the natural map $F_{r-2,r} \longrightarrow M_{r-2,r}$. However, under the decompositions $F_{r-2,r} = (B_{r-2,r-1} \otimes S_1) \oplus B_{r-2,r}$ and $M_{r-2,r} = \mathrm{im}(\varphi_r) \oplus B_{r-2,r}$, this natural map decomposes as $\varphi_r \oplus \mathrm{id}_{B_{r-2,r}}$. This proves (28).

This readily gives a coarse upper bound on the $\beta_{r-1,r}$:

Lemma 3. *We have $\beta_{1,2} \leq \frac{k(k-1)}{2}$, and $\beta_{r-1,r} \leq (k-1)\beta_{r-2,r-1}$ for $r \geq 3$. Hence $\beta_{r-1,r}(\mathsf{C}) \leq \frac{k}{2}(k-1)^{r-1}$ for any $r \geq 2$.*

Proof. We have $\dim(\mathsf{C}^{\langle 2\rangle}) \geq \dim(C) = k$ hence $\beta_{1,2} = \binom{k+1}{2} - \dim(\mathsf{C}^{\langle 2\rangle}) \leq \frac{k(k-1)}{2}$. Now let $r \geq 3$. As M_{r-2} is a submodule of the free module F_{r-3}, multiplication by X_1 is injective on M_{r-2}. Hence $M_{r-2,r-1} \simeq X_1 M_{r-2,r-1} \subseteq \mathrm{im}(\varphi_r)$ from which it follows $\beta_{r-1,r} = k\beta_{r-2,r-1} - \dim \mathrm{im}(\varphi_r) \leq (k-1)\beta_{r-2,r-1}$.

Proposition 1. *The $M_{r-1,r}$ can be computed iteratively as follows. For $r = 3$:*

$$M_{2,3} = \ker(\ I_2(\mathsf{C}) \otimes S_1 \longrightarrow S_3\ ) \tag{30}$$

where $I_2(\mathsf{C}) \otimes S_1 \longrightarrow S_3$ is the natural multiplication map. Then for $r \geq 4$:

$$M_{r-1,r} = \ker(\ M_{r-2,r-1} \otimes S_1 \longrightarrow M_{r-3,r-2} \otimes S_2\ ) \tag{31}$$

where the map $\psi_r : M_{r-2,r-1} \otimes S_1 \longrightarrow M_{r-3,r-2} \otimes S_2$ is obtained first by tensoring the inclusion $M_{r-2,r-1} \subseteq M_{r-3,r-2} \otimes S_1$ by S_1, and then composing with the multiplication map $S_1 \otimes S_1 \longrightarrow S_2$.

Proof. First, (30) is just the case $r = 3$ of (28), composed with the inclusion $I_3(\mathsf{C}) \subseteq S_3$. Likewise to prove (31) we must show $\ker(\varphi_r) = \ker(\psi_r)$ for $r \geq 4$. For this we just observe that the diagram

$$\begin{array}{ccccc} & & M_{r-2,r} & & \\ & \overset{\varphi_r}{\nearrow} & & \searrow & \\ M_{r-2,r-1} \otimes S_1 & & & & F_{r-3,r} \\ & \underset{\psi_r}{\searrow} & & \nearrow & \\ & & M_{r-3,r-2} \otimes S_2 = F_{r-3,r-2} \otimes S_2 & & \end{array} \tag{32}$$

commutes, with the two arrows on the right injective.

Thus we have two descriptions of $M_{r-1,r}$. The description $M_{r-1,r} = \ker(\varphi_r)$ is closer to the abstract definition, and will be used later to estimate the value of the Betti numbers. The description $M_{r-1,r} = \ker(\psi_r)$ is more amenable to effective computation.

Corollary 1. *The $M_{r-1,r}(\mathsf{C})$ only depend on $I_2(\mathsf{C})$.*

To make things even more explicit we introduce the following matrices. Assume C is given by a generator matrix $\mathbf{G} \in \mathbb{F}^{k \times n}$, with rows $\mathbf{c}_1, \ldots, \mathbf{c}_k$. Choose monomial bases $\mathcal{M}_1 = (X_a)_{1 \leq a \leq k}$, $\mathcal{M}_2 = (X_a X_b)_{1 \leq a \leq b \leq k}$, and $\mathcal{M}_3 = (X_a X_b X_c)_{1 \leq a \leq b \leq c \leq k}$ of S_1, S_2, S_3, ordered with respect to some monomial order.

Definition 1. *The squared matrix of* $\mathbf{G}$ *is the matrix*

$$\mathbf{G}_2 \in \mathbb{F}^{\binom{k+1}{2} \times n} \tag{33}$$

with rows indexed by $\mathcal{M}_2$*: the row corresponding to* $X_a X_b$ *is* $\mathbf{c}_a \mathbf{c}_b$*.*

Then $I_2(\mathsf{C})$ is the left kernel of $\mathbf{G}_2$, and we choose a basis $\mathcal{B}_2$ of this space. Thus $\mathcal{B}_2$ consists of $\beta_{1,2}$ vectors, each of which has its entries indexed by $\mathcal{M}_2$.

Definition 2. *The degree* 3 *Macaulay matrix of* $\mathcal{B}_2$ *is the matrix*

$$\mathbf{M}_3 \in \mathbb{F}^{k\beta_{1,2} \times \binom{k+2}{3}} \tag{34}$$

with rows indexed by $\mathcal{M}_1 \times \mathcal{B}_2$ *and columns indexed by* $\mathcal{M}_3$*: the row corresponding to* $(X_a, \mathbf{q}) \in \mathcal{M}_1 \times \mathcal{B}_2$*, where* $\mathbf{q} = (q_M)_{M \in \mathcal{M}_2}$*, has entry* q_M *at position corresponding to* $X_a M \in \mathcal{M}_3$*, and* 0 *elsewhere.*

Then by (30), $M_{2,3}$ is the left kernel of $\mathbf{M}_3$, and we choose a basis $\mathcal{B}_3$ of this space. Thus $\mathcal{B}_3$ consists of $\beta_{2,3}$ vectors, each of which has its entries indexed by $\mathcal{M}_1 \times \mathcal{B}_2$.

Now let $r \geq 4$, and assume inductively for all $3 \leq i \leq r-1$ we have constructed a basis $\mathcal{B}_i$ of $M_{i-1,i}$, consisting of $\beta_{i-1,i}$ vectors, each of which has its entries indexed by $\mathcal{M}_1 \times \mathcal{B}_{i-1}$.

Definition 3. *The degree* r *blockwise Macaulay matrix of* $\mathcal{B}_{r-1}, \mathcal{B}_{r-2}$ *is the matrix*

$$\mathbf{M}_r \in \mathbb{F}^{k\beta_{r-2,r-1} \times \binom{k+1}{2}\beta_{r-3,r-2}} \tag{35}$$

with rows indexed by $\mathcal{M}_1 \times \mathcal{B}_{r-1}$ *and columns indexed by* $\mathcal{M}_2 \times \mathcal{B}_{r-2}$*: the row corresponding to* $(X_a, \mathbf{s}) \in \mathcal{M}_1 \times \mathcal{B}_{r-1}$*, where* $\mathbf{s} = (s_{X_b,\mathbf{t}})_{X_b \in \mathcal{M}_1, \mathbf{t} \in \mathcal{B}_{r-2}}$*, has entry* $s_{X_b,\mathbf{t}}$ *at position corresponding to* $(X_a X_b, \mathbf{t}) \in \mathcal{M}_2 \times \mathcal{B}_{r-2}$*, and* 0 *elsewhere.*

Then by (31), $M_{r-1,r}$ is the left kernel of $\mathbf{M}_r$, and we proceed.

All this is summarized in Algorithm 1.

Observe that our computation only relies on mere linear algebra, and does not make use of any Gröbner basis theory. However, the two topics are clearly related. In particular, the many linear algebra optimizations used in Gröbner basis algorithms could certainly apply in our context.

Further properties

We will have a particular interest in the length of the linear strand, or equivalently, in the following quantity:

Algorithm 1 Compute bases $\mathcal{B}_r$ of $M_{r-1,r}(\mathsf{C})$ up to some degree D

Input: – a generator matrix $\mathbf{G}$ of the $[n,k]$-code C
– a target degree $D \leq k$

```
construct the matrix G_2 according to Definition 1
compute a left kernel basis B_2 of G_2
construct the matrix M_3(B_2) according to Definition 2
compute a left kernel basis B_3 of M_3
for r = 4 ... D do
    construct the matrix M_r(B_{r-1}, B_{r-2}) according to Definition 3
    compute a left kernel basis B_r of M_r
end for
```

Definition 4. *For a linear code* C*, we set*

$$r_{\max}(\mathsf{C}) = \max\{r : \beta_{r-1,r}(\mathsf{C}) > 0\}. \tag{36}$$

As the minimal resolution of a $[n,k]$-code C has length $k-1$, we always have $r_{\max}(\mathsf{C}) \leq k$.

Sometimes we only control the syzygies of certain subideals of $I(\mathsf{C})$, and from these we want to deduce information on the syzygies of the whole ideal. Intuitively, we expect syzygies between elements of the subideals could be seen as syzygies between elements of the ideal. Of course this fails in general, but it remains true if we restrict to the linear strand:

Proposition 2. *Let* M *be a finite* S*-module generated in degrees* $\geq d_0$*, and suppose its degree* d_0 *part* M_{d_0} *decomposes as a direct sum*

$$M_{d_0} = A_{d_0} \oplus B_{d_0}. \tag{37}$$

Let $A = \langle A_{d_0} \rangle_S$ *and* $B = \langle B_{d_0} \rangle_S$ *be the sub-*S*-modules of* M *generated by* A_{d_0} *and* B_{d_0}*. Let* $\widehat{M}$ *be the (first) syzygy module of* M*, and* $\widehat{A}$ *and* $\widehat{B}$ *those of* A *and* B*. Then we have a natural inclusion*

$$\widehat{A}_{d_0+1} \oplus \widehat{B}_{d_0+1} \;\subseteq\; \widehat{M}_{d_0+1} \tag{38}$$

the cokernel of which identifies with $A_{d_0+1} \cap B_{d_0+1}$*, hence a (non-canonical) isomorphism*

$$\widehat{M}_{d_0+1} \;\simeq\; \widehat{A}_{d_0+1} \oplus \widehat{B}_{d_0+1} \oplus (A_{d_0+1} \cap B_{d_0+1}). \tag{39}$$

Proof. We have surjective maps

$$(A_{d_0} \oplus B_{d_0}) \otimes S_1 \;\twoheadrightarrow\; A_{d_0+1} \oplus B_{d_0+1} \;\twoheadrightarrow\; A_{d_0+1} + B_{d_0+1} \tag{40}$$

with $\widehat{A}_{d_0+1} \oplus \widehat{B}_{d_0+1}$ the kernel of the leftmost map, $A_{d_0+1} \cap B_{d_0+1}$ the kernel of the rightmost map, and $\widehat{M}_{d_0+1}$ the kernel of the composite map. We conclude with the associated kernel-cokernel exact sequence.

Corollary 2. *Suppose $I_2(\mathsf{C})$ contains a certain direct sum of l subspaces:*

$$I_2(\mathsf{C}) \supseteq V^{(1)} \oplus \cdots \oplus V^{(l)}. \tag{41}$$

Then the the minimal resolution of $\mathsf{C}^{\langle\cdot\rangle}$ canonically admits the direct sum of the linear strands of the minimal resolutions of $S/\langle V^{(1)}\rangle$, ..., $S/\langle V^{(l)}\rangle$ as a subcomplex. In particular for all $r \geq 2$ we have

$$\beta_{r-1,r}(\mathsf{C}) \;\geq\; \beta_{r-1,r}(S/\langle V^{(1)}\rangle) + \cdots + \beta_{r-1,r}(S/\langle V^{(l)}\rangle). \tag{42}$$

Proof. Apply Proposition 2 repeatedly.

Recall that $\pi\mathsf{C}$ is a punctured code of C if it is obtained from C by discarding some given set of coordinates (equivalently, discarding some subset of the associated set of points in projective space).

Corollary 3. *Let $\pi\mathsf{C}$ be a punctured code of C. Assume* $\dim(\pi\mathsf{C}) = \dim(\mathsf{C})$. *Then for all $r \geq 2$ we have*

$$\beta_{r-1,r}(\pi\mathsf{C}) \geq \beta_{r-1,r}(\mathsf{C}) \tag{43}$$

hence

$$r_{\max}(\pi\mathsf{C}) \geq r_{\max}(\mathsf{C}). \tag{44}$$

Proof. Let $S = \mathbb{F}[X_1, \ldots, X_k]$ where $k = \dim(\pi\mathsf{C}) = \dim(\mathsf{C})$. Then the surjective map $S \longrightarrow (\pi\mathsf{C})^{\langle\cdot\rangle}$ factors through $\mathsf{C}^{\langle\cdot\rangle}$, so that $I_2(\pi\mathsf{C}) \supseteq I_2(\mathsf{C})$.

Last, the following easy result is also useful:

Lemma 4. *Minimal resolutions are preserved under extension of scalars. In particular if a code C is defined over $\mathbb{F}$, and if $\mathbb{F} \subseteq \mathbb{K}$ is a field extension, then $\beta_{i,j}(\mathsf{C}) = \beta_{i,j}(\mathsf{C}_{\mathbb{K}})$ for all i, j.*

3 Lower bounds from the Eagon-Northcott complex

Generalities

Let R be a ring, and for integers $f \geq g$, temporarily switching to column vector convention, let $\mathbf{\Phi} \in R^{g\times f}$ define a linear map

$$\mathbf{\Phi} : F = R^f \longrightarrow G = R^g. \tag{45}$$

The Eagon-Northcott complex [8] of $\mathbf{\Phi}$ is the following complex of R-modules, defined in terms of the exterior and (dual of) symmetric powers of F and G:

$$0 \to (\mathrm{Sym}^{f-g} G)^\vee \otimes \bigwedge^{f} F \to \cdots \to G^\vee \otimes \bigwedge^{g+1} F \to \bigwedge^{g} F \xrightarrow{\bigwedge^g \mathbf{\Phi}} \bigwedge^{g} G \simeq R. \tag{46}$$

Under mild hypotheses, this complex is exact [9, Th. A.2.60 & Th. 6.4], so it defines a resolution of the quotient $R/\operatorname{im}(\bigwedge^g \mathbf{\Phi})$ defined by the ideal generated by the maximal minors of $\mathbf{\Phi}$.

In this work we will only need the case $g = 2$. In this case the complex has length $f-1$, and for $2 \le r \le f$ its $(r-1)$-th module is free of rank

$$\mathrm{rk}\left((\mathrm{Sym}^{r-2} G)^\vee \otimes \bigwedge^r F \right) \;=\; (r-1)\binom{f}{r}. \tag{47}$$

All this can be made explicit, in coordinates. Let

$$\mathbf{\Phi} = \begin{pmatrix} x_1 \; x_2 \; \dots \; x_f \\ x'_1 \; x'_2 \; \dots \; x'_f \end{pmatrix} \tag{48}$$

for $x_i, x'_i \in R$. Then:

- $\mathrm{im}(\bigwedge^2 \mathbf{\Phi})$ is generated by the $\binom{f}{2}$ minors

$$q_{i,j} = x_i x'_j - x_j x'_i \tag{49}$$

  for $1 \le i < j \le f$,
- these q_{ij} are annihilated by the $2\binom{f}{3}$ relations

$$\begin{aligned} r_{ijk} &= x_i q_{jk} - x_j q_{ik} + x_k q_{ij} \\ r'_{ijk} &= x'_i q_{jk} - x'_j q_{ik} + x'_k q_{ij} \end{aligned} \tag{50}$$

  for $1 \le i < j < k \le f$,
- these r_{ijk} and r'_{ijk} are annihilated by the $3\binom{f}{4}$ relations

$$\begin{aligned} s_{ijkl} &= x_i r_{jkl} - x_j r_{ikl} + x_k r_{ijl} - x_l r_{ijk} \\ s'_{ijkl} &= x_i r'_{jkl} - x_j r'_{ikl} + x_k r'_{ijl} - x_l r'_{ijk} + \\ &\qquad + x'_i r_{jkl} - x'_j r_{ikl} + x'_k r_{ijl} - x'_l r_{ijk} \\ s''_{ijkl} &= x'_i r'_{jkl} - x'_j r'_{ikl} + x_k r'_{ijl} - x_l r'_{ijk} \end{aligned} \tag{51}$$

  for $1 \le i < j < k < l \le f$,

and so on. These are just the cases $r = 2, 3, 4$ of the more general:

Proposition 3. *In the multivariate polynomial ring*

$$R[Z^{(j)}_{r;i_1,\dots,i_r}] \tag{52}$$

where, for each $2 \le r \le f$, indices range over the $(r-1)\binom{f}{r}$ values $1 \le j \le r-1$ and $1 \le i_1 < \dots < i_r \le f$, construct polynomials $s^{(j)}_{r;i_1,\dots,i_r}$ as follows. First for $r = 2$ we define the constant polynomials

$$s^{(1)}_{2;i_1,i_2} = x_{i_1} x'_{i_2} - x'_{i_1} x_{i_2} \tag{53}$$

given by the minors of $\mathbf{\Phi}$; and for $r \ge 3$ we define linear polynomials

$$s^{(j)}_{r;i_1,\dots,i_r} = \sum_{u=1}^{r} (-1)^{u-1} (x_{i_u} Z^{(j)}_{r-1;i_1,\dots,\widehat{i_u},\dots,i_r} + x'_{i_u} Z^{(j-1)}_{r-1;i_1,\dots,\widehat{i_u},\dots,i_r}) \tag{54}$$

where we replace $Z^{(j)}_{r;i_1,\dots,i_r}$ with zero if $j \le 0$ or $j \ge r$. Then, for all $r \ge 3$, we have

$$\mathbf{s}_r(\mathbf{s}_{r-1}) = \mathbf{0}. \tag{55}$$

Proof. Either express (46) in the standard bases of $F = R^f$ and $G = R^2$. Or more directly, consider the $\mathbf{Z}_r$ and $\mathbf{s}_r$ as $(r-1)$-tuples of (exterior) r-vectors, observe that (53) means $\mathbf{s}^{(1)}_2 = \mathbf{x} \wedge \mathbf{x}'$, that (54) means $\mathbf{s}^{(j)}_r = \mathbf{x} \wedge \mathbf{Z}^{(j)}_{r-1} + \mathbf{x}' \wedge \mathbf{Z}^{(j-1)}_{r-1}$, so the alternating property gives $\mathbf{s}^{(1)}_3(\mathbf{s}_2) = \mathbf{x}\wedge\mathbf{x}\wedge\mathbf{x}' = \mathbf{0}$, $\mathbf{s}^{(2)}_3(\mathbf{s}_2) = \mathbf{x}'\wedge\mathbf{x}\wedge\mathbf{x}' = \mathbf{0}$, and for $r \ge 4$:

$$\begin{aligned}\mathbf{s}^{(j)}_r(\mathbf{s}_{r-1}) = \mathbf{x} \wedge \mathbf{x} \wedge \mathbf{Z}^{(j)}_{r-2} + \mathbf{x} \wedge \mathbf{x}' \wedge \mathbf{Z}^{(j-1)}_{r-2} + \\ + \mathbf{x}' \wedge \mathbf{x} \wedge \mathbf{Z}^{(j-1)}_{r-2} + \mathbf{x}' \wedge \mathbf{x}' \wedge \mathbf{Z}^{(j-2)}_{r-2} = \mathbf{0}.\end{aligned} \tag{56}$$

Shortening (or projection from a point)

We have interest in how this Eagon-Northcott complex interacts with reduction to a subcode, and in particular with shortening. By induction it suffices to consider the case of a codimension 1 subcode, or a 1-shortening respectively.

So let C be a $[n, k]$-code over $\mathbb{F}$, and $\mathsf{C}_{\mathcal{H}}$ a codimension 1 subcode. We will assume C projective, but then $\mathsf{C}_{\mathcal{H}}$ need not be so. Choose a basis $\mathbf{c}_1, \dots, \mathbf{c}_{k-1}$ of $\mathsf{C}_{\mathcal{H}}$, and complete it to a basis $\mathbf{c}_1, \dots, \mathbf{c}_k$ of C. Let $\mathbf{G}_{\mathcal{H}}$ and $\mathbf{G}$ be the corresponding generating matrices of $\mathsf{C}_{\mathcal{H}}$ and C. Let also $S = \mathbb{F}[X_1, \dots, X_k]$ be the polynomial ring in k indeterminates, and $S_{\mathcal{H}} = \mathbb{F}[X_1, \dots, X_{k-1}]$ its subring in the first $k-1$ indeterminates. We have a commutative diagram

$$\begin{array}{ccc} S_{\mathcal{H}} & \longrightarrow & \mathsf{C}^{\langle\cdot\rangle}_{\mathcal{H}} \\ \big\downarrow & & \big\downarrow \\ S & \longrightarrow & \mathsf{C}^{\langle\cdot\rangle} \end{array} \tag{57}$$

where horizontal maps denote evaluation, and vertical maps inclusion. Also set

$$\mathcal{H} = S_{\mathcal{H},1} = \langle X_1, \dots, X_{k-1}\rangle_{\mathbb{F}} \subseteq S_1 \tag{58}$$

and let $\mathbf{p}_{\mathcal{H}} = (0 : \cdots : 0 : 1)^\top \in \mathbf{P}^{k-1}$ be the associated point. Last, let $\{\mathbf{p}_1, \dots, \mathbf{p}_n\} \subseteq \mathbf{P}^{k-1}$ be the set of points defined by the columns of $\mathbf{G}$. Then we have two possibilities:

- Either $\mathbf{c}_1, \dots, \mathbf{c}_{k-1}$ all vanish at some common position i, or equivalently, $\mathbf{p}_{\mathcal{H}} = \mathbf{p}_i$. Puncturing this position, we can identify $\mathsf{C}_{\mathcal{H}}$ with the 1-shortened subcode of C at i. Then the set of points in $\mathbf{P}^{k-2}$ defined by the columns of $\mathbf{G}_{\mathcal{H}}$ is the image of $\{\mathbf{p}_1, \dots, \widehat{\mathbf{p}}_i, \dots, \mathbf{p}_n\}$ under the projection from $\mathbf{p}_i$.
- Otherwise, if there is no such i, then $\mathsf{C}_{\mathcal{H}}$ is a "general" codimension 1 subcode, and the set of points in $\mathbf{P}^{k-2}$ defined by the columns of $\mathbf{G}_{\mathcal{H}}$ is the image of $\{\mathbf{p}_1, \dots, \mathbf{p}_n\}$ under the projection from $\mathbf{p}_{\mathcal{H}}$.

(As already observed, $\mathsf{C}_{\mathcal{H}}$ need not be projective, so these image points need not be distinct.)

Let $f \geq g \geq d \geq 2$ be integers, and let $\mathbf{\Phi} \in S_1^{g\times f}$ be a matrix whose entries are homogeneous linear forms, i.e. elements of S_1. Recall from [9, §6B] that such a matrix is said to be 1-generic if for any nonzero $\mathbf{a} \in \overline{\mathbb{F}}^g$ and $\mathbf{b} \in \overline{\mathbb{F}}^f$, $\mathbf{a\Phi b}^\top$ is nonzero. Let $V_{\mathbf{\Phi}} \subseteq S_1^g$ be the column span of $\mathbf{\Phi}$, so $\dim(V_{\mathbf{\Phi}}) \leq f$, and set

$$V_{\mathbf{\Phi},\mathcal{H}} = V_{\mathbf{\Phi}} \cap \mathcal{H}^g. \tag{59}$$

Set $f_{\mathcal{H}} = \dim(V_{\mathbf{\Phi},\mathcal{H}}) \geq \dim(V_{\mathbf{\Phi}}) - g$, and then let $\mathbf{\Phi}_{\mathcal{H}} \in \mathcal{H}^{g\times f_{\mathcal{H}}}$ be a matrix whose columns form a basis of $V_{\mathbf{\Phi},\mathcal{H}}$.

Proposition 4. *Under these hypotheses:*

1. *If $I_d(\mathsf{C})$ contains the $d \times d$ minors of $\mathbf{\Phi}$, then $I_d(\mathsf{C}_{\mathcal{H}})$ contains the $d \times d$ minors of $\mathbf{\Phi}_{\mathcal{H}}$.*
2. *If $\mathbf{\Phi}$ is 1-generic, then $\mathbf{\Phi}_{\mathcal{H}}$ is 1-generic, and $f_{\mathcal{H}} \geq f - g$.*
3. *If $I_d(\mathsf{C})$ contains the $d \times d$ minors of $\mathbf{\Phi}$, if $\mathbf{\Phi}$ is 1-generic, and if $\mathsf{C}_{\mathcal{H}}$ is a 1-shortened subcode of C, then $f_{\mathcal{H}} \geq f - d + 1$.*

Proof. By (57) we have $I_d(\mathsf{C}_{\mathcal{H}}) = I_d(\mathsf{C}) \cap S_{\mathcal{H}}$. Columns of $\mathbf{\Phi}_{\mathcal{H}}$ belong to the column span of $\mathbf{\Phi}$, so $d\times d$ minors of $\mathbf{\Phi}_{\mathcal{H}}$ are linear combinations of $d\times d$ minors of $\mathbf{\Phi}$. On the other hand, $\mathbf{\Phi}_{\mathcal{H}}$ has coefficients in $\mathcal{H}$, so its $d \times d$ minors belong to $S_{\mathcal{H}}$. This proves 1.

Assume $\mathbf{\Phi}$ is 1-generic. As columns of $\mathbf{\Phi}_{\mathcal{H}}$ are linearly independent and belong to the column space of $\mathbf{\Phi}$, we can write $\mathbf{\Phi}_{\mathcal{H}} = \mathbf{\Phi M}$ where $\mathbf{M} \in \mathbb{F}^{f\times f_{\mathcal{H}}}$ has $\mathrm{rk}(\mathbf{M}) = f_{\mathcal{H}}$. Then for $\mathbf{a} \in \overline{\mathbb{F}}^g$ and $\mathbf{b} \in \overline{\mathbb{F}}^{f_{\mathcal{H}}}$ nonzero we have $\mathbf{a\Phi}_{\mathcal{H}}\mathbf{b}^\top = \mathbf{a\Phi Mb}^\top \neq 0$ because $\mathbf{Mb}^\top$ is nonzero. This proves that $\mathbf{\Phi}_{\mathcal{H}}$ is 1-generic. Then it is easily seen that a 1-generic matrix has linearly independent columns, so $\dim(V_{\mathbf{\Phi}}) = f$, hence $f_{\mathcal{H}} \geq f - g$. This finishes the proof of 2.

Now we prove 3. Assume $\mathsf{C}_{\mathcal{H}}$ is the 1-shortened subcode of C at position i, hence $\mathbf{p}_i = \mathbf{p}_{\mathcal{H}} = (0 : \cdots : 0 : 1)^\top$. As $\mathbf{\Phi}$ is 1-generic, we have $\dim(V_{\mathbf{\Phi}}) = f$. Let $\mathrm{ev}_{\mathbf{p}_{\mathcal{H}}} : S \longrightarrow \mathbb{F}$ denote evaluation at $\mathbf{p}_{\mathcal{H}}$. Applied coordinatewise, we also have evaluation maps $\mathrm{ev}_{\mathbf{p}_{\mathcal{H}}} : S^g \longrightarrow \mathbb{F}^g$ and $\mathrm{ev}_{\mathbf{p}_{\mathcal{H}}} : S^{g\times f} \longrightarrow \mathbb{F}^{g\times f}$. Also we can restrict $\mathrm{ev}_{\mathbf{p}_{\mathcal{H}}}$ to subspaces, so for instance $\mathcal{H} = \ker(\mathrm{ev}_{\mathbf{p}_{\mathcal{H}}} : S_1 \longrightarrow \mathbb{F})$. It then follows

$$V_{\mathbf{\Phi},\mathcal{H}} = V_{\mathbf{\Phi}} \cap \mathcal{H}^g = \ker(\,\mathrm{ev}_{\mathbf{p}_{\mathcal{H}}} : V_{\mathbf{\Phi}} \longrightarrow \mathbb{F}^g\,), \tag{60}$$

while the image $\mathrm{ev}_{\mathbf{p}_{\mathcal{H}}}(V_{\mathbf{\Phi}}) \subseteq \mathbb{F}^g$ is the column span of $\mathrm{ev}_{\mathbf{p}_{\mathcal{H}}}(\mathbf{\Phi}) \in \mathbb{F}^{g\times f}$. As the $d \times d$ minors of $\mathbf{\Phi}$ belong to $I_d(\mathsf{C})$, they vanish at each column of $\mathbf{G}$, in particular they vanish at $\mathbf{p}_{\mathcal{H}} = \mathbf{p}_i$. But this means precisely that the $d \times d$ minors of $\mathrm{ev}_{\mathbf{p}_{\mathcal{H}}}(\mathbf{\Phi})$ all vanish, or equivalently,

$$\dim(\mathrm{ev}_{\mathbf{p}_{\mathcal{H}}}(V_{\mathbf{\Phi}})) \leq d - 1. \tag{61}$$

Joint with (60) this gives $f_{\mathcal{H}} = \dim(V_{\mathbf{\Phi},\mathcal{H}}) \geq \dim(V_{\mathbf{\Phi}}) - (d-1) = f - d + 1$.

Application to alternant and Goppa codes

Consider a code $\mathsf{C} \in \mathsf{Alt}^{\perp}_{q,m,n,t}$, assumed to be proper. By (21), after extension of scalars, $\mathsf{C}_{\mathbb{F}_{q^m}}$ admits as a basis the $k = mt$ vectors $(\mathbf{y}\mathbf{x}^a)^{q^u}$ for $0 \leq a \leq t-1$ and $0 \leq u \leq m-1$. Rename the $k = mt$ variables in our polynomial ring S accordingly, so that our evaluation map now is

$$S = \mathbb{F}_{q^m}[X_a^{(u)}] \longrightarrow \mathsf{C}^{\langle \cdot \rangle}_{\mathbb{F}_{q^m}} \tag{62}$$

where $X_a^{(u)}$ evaluates as $(\mathbf{y}\mathbf{x}^a)^{q^u}$.

If $\mathbf{M}$ is a matrix (or more generally an expression) in the $X_a^{(u)}$, we denote by $\mathbf{M}^{(v)}$ the same matrix (or expression) with each $X_a^{(u)}$ replaced by $X_a^{(u+v)}$, where $u+v$ is considered mod m. We also write $\mathbf{M}' = \mathbf{M}^{(1)}$, $\mathbf{M}'' = \mathbf{M}^{(2)}$, etc.

Set

$$e = \lfloor \log_q(t-1) \rfloor, \tag{63}$$

and for any $0 \leq u \leq e$ define a $2 \times (t - q^u)$ matrix

$$\mathbf{B}_u = \begin{pmatrix} X_0^{(0)} & X_1^{(0)} & \dots & X_{t-1-q^u}^{(0)} \\ X_{q^u}^{(0)} & X_{q^u+1}^{(0)} & \dots & X_{t-1}^{(0)} \end{pmatrix}. \tag{64}$$

We then define the block matrix

$$\mathbf{\Phi} = \left(\mathbf{B}_0^{(e)} \middle| \mathbf{B}_1^{(e-1)} \middle| \cdots \middle| \mathbf{B}_e^{(0)} \right) \tag{65}$$

of total size $2 \times f$ where $f = (e+1)t - \frac{q^{e+1}-1}{q-1}$. Observe that this matrix only depends on q and t, debatably on m, but certainly not on n nor on the specific choice of C.

Lemma 5. *The 2×2 minors of $\mathbf{\Phi}$ belong to $I_2(\mathsf{C}_{\mathbb{F}_{q^m}})$.*

Proof. The 2×2 minor defined by the columns $\begin{bmatrix} X_a^{(e-u)} \\ X_{q^u+a}^{(e-u)} \end{bmatrix}$ of $\mathbf{B}_u^{(e-u)}$ and $\begin{bmatrix} X_b^{(e-v)} \\ X_{q^v+b}^{(e-v)} \end{bmatrix}$ of $\mathbf{B}_v^{(e-v)}$ is

$$X_a^{(e-u)} X_{q^v+b}^{(e-v)} - X_{q^u+a}^{(e-u)} X_b^{(e-v)} \tag{66}$$

which evaluates under (62) to

$$(\mathbf{y}\mathbf{x}^a)^{q^{e-u}} (\mathbf{y}\mathbf{x}^{q^v+b})^{q^{e-v}} - (\mathbf{y}\mathbf{x}^{q^u+a})^{q^{e-u}} (\mathbf{y}\mathbf{x}^b)^{q^{e-v}} = \mathbf{0}. \tag{67}$$

Lemma 6. *The matrix $\mathbf{\Phi}$ is 1-generic.*

Proof. Let $\mathbf{a} \in \overline{\mathbb{F}}_q^2$ and $\mathbf{b} \in \overline{\mathbb{F}}_q^f$ be nonzero. Let a_i be the rightmost nonzero entry of $\mathbf{a}$ and b_j the rightmost nonzero entry of $\mathbf{b}$. Then the $X_c^{(u)}$ variable that multiplies $a_i b_j$ in $\mathbf{a}\mathbf{\Phi}\mathbf{b}^\top$ does not appear elsewhere in $\mathbf{a}\mathbf{\Phi}\mathbf{b}^\top$, so $\mathbf{a}\mathbf{\Phi}\mathbf{b}^\top \neq 0$.

Theorem 1. *Let $\mathsf{C} \in \mathsf{Alt}^{\perp}_{q,m,n,t}$ be proper, $e = \lfloor \log_q(t-1) \rfloor$, $f = (e+1)t - \frac{q^{e+1}-1}{q-1}$. For any $s \geq 0$, let C_s be a s-shortened subcode of C. Then for all $r \geq 2$ we have $\beta_{r-1,r}(\mathsf{C}_s) \geq (r-1)\binom{f-s}{r}$, hence*

$$r_{\max}(\mathsf{C}_s) \geq f - s. \tag{68}$$

Proof. By Lemma 4 we can extend scalars to $\mathbb{F}_{q^m}$. By Lemma 5, $I_2(\mathsf{C})$ then contains the 2×2 minors of the $2 \times f$ matrix $\mathbf{\Phi}$, and this matrix $\mathbf{\Phi}$ is 1-generic by Lemma 6. By Proposition 4 applied s times (with $g = d = 2$), $I_2(\mathsf{C}_s)$ then contains the 2×2 minors of a $2 \times f_s$ matrix $\mathbf{\Phi}_s$, where $f_s \geq f - s$, and this matrix $\mathbf{\Phi}_s$ is 1-generic also. Then by [9, §6B], the 2×2 minors of $\mathbf{\Phi}_s$ are linearly independent, and its Eagon-Northcott complex is exact with only nonzero Betti numbers $\beta_{0,0} = 1$ and $\beta_{r-1,r} = (r-1)\binom{f_s}{r}$ for $2 \leq r \leq f_s$. We then conclude with Corollary 2 (with $l = 1$ and $V^{(1)} = \mathrm{im}(\bigwedge^2 \mathbf{\Phi}_s)$).

Remark 1. It is possible to improve the lower bound on $\beta_{r-1,r}(\mathsf{C}_s)$, using not only $\mathbf{\Phi} = \mathbf{\Phi}^{(0)}$, but also its conjugates $\mathbf{\Phi}^{(1)}, \ldots, \mathbf{\Phi}^{(m-1)}$. See the corresponding discussion in the Supplementary material.

Examples show the bound (68) on $r_{\max}$ is tight in general for alternant codes. However one can improve it in the Goppa case. Let us focus on $q = 2$ for simplicity. Let $\varphi : a \mapsto a^2$ be the Frobenius map, acting on any $\mathbb{F}_2$-algebra. For any polynomial $g \in \mathbb{F}_{2^m}[X]$, set $L_g = g(X)^{-1}\mathbb{F}_{2^m}[X]_{<\deg(g)} \subseteq \mathbb{F}_{2^m}(X)$.

Lemma 7. *Let $g(X) \in \mathbb{F}_{2^m}[X]$ be squarefree (i.e. separable). Then*

$$L_g \;+\; \varphi(L_g) \;=\; L_{g^2}, \tag{69}$$

the sum being direct

Proof. Set $t = \deg(g)$. Then L_g and $\varphi(L_g)$ both are t-dimensional subspaces of the $2t$-dimensional space L_{g^2}. To conclude we only have to prove $L_g \cap \varphi(L_g) = 0$. However we have $F(X) \in L_g \cap \varphi(L_g)$ if and only if $F(X) = \frac{A(X)}{g(X)} = \frac{B(X)^2}{g(X)^2}$ for some A, B of degree $< t$. But then this implies $g(X) | B(X)^2$ with g squarefree of degree t, which is impossible unless $B = 0$.

From this we readily deduce:

Lemma 8. *Let $\mathbf{x} \in (\mathbb{F}_{2^m})^n$ be a support, and $g(X) \in \mathbb{F}_{2^m}[X]$ squarefree of degree $t \leq n/2$, not vanishing on any entry of $\mathbf{x}$. Then*

$$\mathsf{GRS}_t(\mathbf{x}, g(\mathbf{x})^{-1}) + \mathsf{GRS}_t(\mathbf{x}^2, g(\mathbf{x})^{-2}) = \mathsf{GRS}_{2t}(\mathbf{x}, g(\mathbf{x})^{-2}), \tag{70}$$

the sum being direct.

Proposition 5. *Let $\mathsf{C} = \mathsf{Gop}(\mathbf{x}, g)^{\perp} \in \mathsf{Gop}^{\mathrm{sqfr},\perp}_{2,m,n,t}$ be proper, with g squarefree. Set $\mathbf{y} = g(\mathbf{x})^{-1}$. Then*

$$\mathsf{C}_{\mathbb{F}_{q^m}} = \bigoplus_{i=0}^{m/2-1} \mathsf{GRS}_{2t}(\mathbf{x}^{4^i}, \mathbf{y}^{4^i}), \quad \textit{or} \tag{71}$$

$$\mathsf{C}_{\mathbb{F}_{q^m}} = \left(\bigoplus_{i=0}^{(m-1)/2-1} \mathsf{GRS}_{2t}(\mathbf{x}^{4^i}, \mathbf{y}^{4^i}) \right) \oplus \mathsf{GRS}_t(\mathbf{x}^{2^{m-1}}, \mathbf{y}^{2^{m-1}}) \tag{72}$$

depending on whether m is even or odd.

Corollary 4. *Let $\mathsf{C} = \mathsf{Gop}(\mathbf{x}, g)^{\perp} \in \mathsf{Gop}^{\mathrm{sqfr},\perp}_{2,m,n,t}$ be proper, with g squarefree. Set $\widehat{e} = \lfloor \log_4(2t-1) \rfloor$ and $\widehat{f} = (2\widehat{e}+2)t - \frac{4^{\widehat{e}+1}-1}{3}$. For any $s \geq 0$, let C_s be a s-shortened subcode of C. Then for all $r \geq 2$ we have $\beta_{r-1,r}(\mathsf{C}_s) \geq (r-1)\binom{\widehat{f}-s}{r}$, hence*

$$r_{\max}(\mathsf{C}_s) \geq \widehat{f} - s. \tag{73}$$

Proof. Same as Theorem 1, with $\mathbf{\Phi}$ adapted to fit Proposition 5.

4 Regularity 2 and the small defect heuristic

Regularity 2 and consequences

If C is a $[n,k]$-code, we let

$$B_j = \sum_{i \geq 0} (-1)^i \beta_{i,j} \tag{74}$$

be the alternating sum of its Betti numbers degree j, and $B(z) = \sum_{j \geq 0} B_j z^j$ their generating polynomial (it is indeed a finite sum).

Let also $H_{\mathsf{C}}(z) = \sum_{r \geq 0} z^r \dim \mathsf{C}^{\langle r \rangle}$ be the Hilbert series of C.

Proposition 6. *We have*

$$B(z) = (1-z)^k H_{\mathsf{C}}(z). \tag{75}$$

Proof. Generating series reformulation of [9, Cor. 1.10].

Definition 5 ([25, Def. 1.5 & Th. 2.35]). *The Castelnuovo-Mumford regularity of a projective $[n,k]$-code C is the smallest integer r such that $\mathsf{C}^{\langle r \rangle} = \mathbb{F}^n$.*

Definition 6 (cf. [9, §4A], after [22, Lect. 14]). *The Castelnuovo-Mumford regularity of $\mathsf{C}^{\langle \cdot \rangle}$ is $\max\{r : \exists i,\ \beta_{i,i+r}(\mathsf{C}) > 0\}$.*

Proposition 7 ([9, Th. 4.2]). *These two definitions coincide.*

The square code distinguisher, and the filtration attack from [1] that extends it, work for codes C with $\mathsf{C}^{\langle 2 \rangle} \subsetneq \mathbb{F}^n$, i.e. of regularity > 2. This means that codes of regularity 2 are hard to deal with under this approach. On the opposite, for us, codes of regularity 2 are nice because Definition 6 means their Betti diagram is simple: it has only two nontrivial rows. Observe that most codes of interest have regularity 2 (with the notable exception of self-dual codes).

Definition 7. *If $f : U \longrightarrow V$ is a linear map between finite dimensional $\mathbb{F}$-vector spaces, we define its index*

$$\begin{aligned}\operatorname{ind}(f) &= \dim(U) - \dim(V) \\ &= \dim\ker(f) - \dim\operatorname{coker}(f)\end{aligned} \tag{76}$$

and its defect

$$\begin{aligned}\operatorname{def}(f) &= \min(\dim(U), \dim(V)) - \operatorname{rk}(f) \\ &= \min(\dim\ker(f), \dim\operatorname{coker}(f)).\end{aligned} \tag{77}$$

For any real x we set $x^+ = \max(x, 0)$ and $x^- = (-x)^+$, so $x = x^+ - x^-$. Then we always have

$$\dim\ker(f) \geq \operatorname{ind}(f)^+ \tag{78}$$

$$\dim\operatorname{coker}(f) \geq \operatorname{ind}(f)^- \tag{79}$$

and then

$$\operatorname{def}(f) = \dim\ker(f) - \operatorname{ind}(f)^+ = \dim\operatorname{coker}(f) - \operatorname{ind}(f)^- \tag{80}$$

measures the distance to equality in these two inequalities.

For $r \geq 3$, recall the linear map $\varphi_r : M_{r-2,r-1} \otimes S_1 \longrightarrow M_{r-2,r}$ from (27). It will also be handy to let $\varphi_2 = \mathrm{ev}_{\mathbf{G},2} : S_2 \longrightarrow \mathsf{C}^{\langle 2\rangle}$ be the evaluation map.

Theorem 2. *For all $r \geq 2$ we have*

$$\dim\ker(\varphi_r) = \beta_{r-1,r} \tag{81}$$

$$\dim\operatorname{coker}(\varphi_r) = \beta_{r-2,r} \tag{82}$$

and moreover, if $\mathsf{C}^{\langle 2\rangle} = \mathbb{F}^n$, then

$$\operatorname{ind}(\varphi_r) = \left(\frac{k(k+1)}{r} - n\right)\binom{k-1}{r-2}. \tag{83}$$

Proof. For $r = 2$ this is proved directly. Now assume $r \geq 3$. Then the first two equalities are reformulations of Lemma 2. Now assume moreover $\mathsf{C}^{\langle 2\rangle} = \mathbb{F}^n$. Then $H_{\mathsf{C}}(z) = 1 + kz + n\frac{z^2}{1-z}$, so $B(z) = (1+kz)(1-z)^k + nz^2(1-z)^{k-1}$ by Proposition 6, thus $B_r = (-1)^{r-1}(r-1)\binom{k+1}{r} + (-1)^r n\binom{k-1}{r-2} = (-1)^{r-1}\left(\frac{k(k+1)}{r} - n\right)\binom{k-1}{r-2}$. On the other hand, $\mathsf{C}^{\langle 2\rangle} = \mathbb{F}^n$ also means C has regularity 2 in the sense of Definition 6, so (74) reduces to $B_r = (-1)^{r-1}\beta_{r-1,r} + (-1)^{r-2}\beta_{r-2,r} = (-1)^{r-1}\operatorname{ind}(\varphi_r)$ and we conclude.

Corollary 5. *If $\mathsf{C}^{\langle 2\rangle} = \mathbb{F}^n$, then the bottom right entry of its Betti diagram is*

$$\beta_{k-1,k+1} = n - k. \tag{84}$$

Proof. The minimal resolution of C has length $k-1$, so $\beta_{i,j}=0$ for $i>k-1$, hence $\beta_{k-1,k+1}=-\operatorname{ind}(\varphi_{k+1})=n-k$.

Regularity 2 helps in computing the full Betti diagram. We already gave examples in Figures 1-3. In order to provide a few more, let us first recall that a $[n,k]$ code C is MDS if it has dual minimum distance $\mathrm{d_{min}}(\mathsf{C}^{\perp})=k+1$.

Lemma 9 ([14, Th. 1], reformulated). *Let C be a $[n,k]$-code with $n\leq 2k-1$. Assume C is MDS. Then for all $r\leq 2k+1-n$ we have $\beta_{r-2,r}(\mathsf{C})=0$.*

Proposition 8. *Let C be a $[k+1,k]$ MDS code, for instance a parity code or a $[k+1,k]$ GRS code. Then the nonzero Betti numbers of C are $\beta_{0,0}=\beta_{k-1,k+1}=1$, and*

$$\beta_{r-1,r}=\frac{(r-1)(k-r)}{k}\binom{k+1}{r} \tag{85}$$

for $2\leq r\leq k-1$. In particular they satisfy the symmetry $\beta_{i,j}=\beta_{k-1-i,k+1-j}$.

Proof. The parameters imply that C has regularity 2. By Lemma 9 we have $\beta_{r-2,r}=0$ for $r\leq k$. Then $\beta_{r-1,r}=\operatorname{ind}(\varphi_r)=\left(\frac{k(k+1)}{r}-(k+1)\right)\binom{k-1}{r-2}$ and we conclude with a straightforward calculation.

Proposition 9. *Let C be a $[2k-1,k]$ GRS code. Then the nonzero Betti numbers of C are:*

- $\beta_{0,0}=1$
- $\beta_{r-1,r}=(r-1)\binom{k-1}{r}$ *for* $2\leq r\leq k-1$
- $\beta_{r-2,r}=(r-2)\binom{k-1}{r-2}$ *for* $3\leq r\leq k+1$ *(so $\beta_{r-2,r}=\beta_{k+2-r,k+4-r}$).*

In particular the ideal $I(\mathsf{C})$ is generated by $\beta_{1,2}=\frac{(k-1)(k-2)}{2}$ quadratic forms and $\beta_{1,3}=k-1$ cubic forms.

Proof. Using the basis $\mathbf{y},\mathbf{yx},\dots,\mathbf{yx}^{k-1}$ of C, we see $I_2(\mathsf{C})$ contains the 2×2 minors of $\mathbf{\Phi}=\begin{pmatrix}X_0\ X_1\ \dots\ X_{k-2}\\ X_1\ X_2\ \dots\ X_{k-1}\end{pmatrix}$, i.e. $I_2(\mathsf{C})\supseteq\operatorname{im}(\bigwedge^2\mathbf{\Phi})$ of dimension $\binom{k-1}{2}$.

Now set $n=2k-1$.

Because $n\geq 2k-1$, we have $\dim\mathsf{C}^{\langle 2\rangle}=2k-1$, hence $\dim I_2(\mathsf{C})=\binom{k-1}{2}$, so $I_2(\mathsf{C})=\operatorname{im}(\bigwedge^2\mathbf{\Phi})$. Corollary 1 and the Eagon-Northcott complex of $\mathbf{\Phi}$ then give $\beta_{r-1,r}=(r-1)\binom{k-1}{r}$.

Because $n\leq 2k-1$, we have $\mathsf{C}^{\langle 2\rangle}=\mathbb{F}^n$. Then $\beta_{r-2,r}=\beta_{r-1,r}-\operatorname{ind}(\varphi_r)=(r-1)\binom{k-1}{r}-\left(\frac{k(k+1)}{r}-(2k-1)\right)\binom{k-1}{r-2}$, and a straightforward calculation allows to conclude.

Figures 4 and 5 illustrate Propositions 8 and 9.

Exercise 1. Compute the Betti diagram of $[n,k]$ GRS codes for $k+1<n<2k-1$.

	0	1	2	3	4	5	6	7
0	1	–	–	–	–	–	–	–
1	–	27	105	189	189	105	27	–
2	–	–	–	–	–	–	–	1

Fig. 4. a $[9,8]$ parity or GRS code

	0	1	2	3	4	5	6	7
0	1	–	–	–	–	–	–	–
1	–	21	70	105	84	35	6	–
2	–	7	42	105	140	105	42	7

Fig. 5. a $[15,8]$ GRS code

The small defect heuristic

A direct application of Definition 7 and Theorem 2 gives:

Proposition 10. *If* C *is a* $[n,k]$*-code with* $\mathsf{C}^{\langle 2\rangle}=\mathbb{F}^n$*, then for all* $r\geq 2$ *we have*

$$\beta_{r-1,r}(\mathsf{C})=\left(\frac{k(k+1)}{r}-n\right)^{+}\binom{k-1}{r-2}+\operatorname{def}(\varphi_r) \tag{86}$$

$$\beta_{r-2,r}(\mathsf{C})=\left(\frac{k(k+1)}{r}-n\right)^{-}\binom{k-1}{r-2}+\operatorname{def}(\varphi_r). \tag{87}$$

It is tempting to see this result as an estimate for the Betti numbers of random codes, with a leading term given by $\operatorname{ind}(\varphi_r)^{\pm}$ (compare with the bound in Lemma 3), and a secondary term given by $\operatorname{def}(\varphi_r)$. Indeed, it is well known that under a reasonable probability model, a random linear map tends to have a small defect. Unfortunately, if C is a random code (say, uniform among codes of given $[n,k]$), it is not easy to control the distribution of the maps φ_r.

Still, in the special case $r=2$, [3] manages to give lower bounds, exponentially close to 1, on the probability that $\operatorname{def}(\varphi_2)=0$. One might wonder how this generalizes. Let us review some arguments that support such a generalization, but also impose some limitations on its validity.

Reformulated in our setting, the *minimal resolution conjecture* of [18] postulates that, over an infinite field, a Zariski-generic code has $\operatorname{def}(\varphi_r)=0$ for all $r\geq 2$, or equivalently, that $\beta_{r-1,r}(\mathsf{C})=0$ for $r\geq\frac{k(k+1)}{n}$ and $\beta_{r-2,r}(\mathsf{C})=0$ for $r\leq\frac{k(k+1)}{n}$. However, two points require our attention:

1. This conjecture is known to be false in general [10].
2. We work over a finite field, not an infinite one.

Concerning point 1, we will argue that the conjecture is still "true enough" for us. First, a nonzero defect might not be a problem in our Betti number estimates, as long as it remains small. Moreover, as noted in the introduction of [10], the conjecture has been proved for a large range of values of n and k. In fact, although [10] provides an infinity of counterexamples, these remain limited to specific parameters, namely of the form $n=k+O(\sqrt{k})$. And indeed, perhaps the most valuable result for us is [16], which proves that the conjecture is true when n is large enough with respect to k.

Concerning point 2, it is true that codes behave quite differently over a finite field and over an infinite field. For instance, generic codes over an infinite field are MDS for any parameter set, while over a finite field they clearly are not. This makes it desirable to investigate links between Betti numbers and distance properties of a code.

	0	1	2	3	4	5	6	7	8	9	10	11
0	1	–	–	–	–	–	–	–	–	–	–	–
1	–	55	319	880	1353	990	–	–	–	–	–	–
2	–	–	–	–	–	330	1617	1870	1221	485	110	11

Fig. 6. an idealized $[23, 12]$-code according to the minimal resolution conjecture

	0	1	2	3	4	5	6	7	8	9	10	11
0	1	–	–	–	–	–	–	–	–	–	–	–
1	–	55	319	881	1371	1122	315	63	6	–	–	–
2	–	–	1	18	132	645	1680	1876	1221	485	110	11

	0	1	2	3	4	5	6	7	8	9	10	11
0	1	–	–	–	–	–	–	–	–	–	–	–
1	–	55	319	884	1392	1181	300	49	4	–	–	–
2	–	–	4	39	191	630	1666	1874	1221	485	110	11

Fig. 7. some actual $[23, 12]_2$-codes with $d = 4$, $d^\perp = 4$ (compare also with Figure 3)

For any code C, let us denote by $A_i(\mathsf{C})$ the number of codewords of Hamming weight i in C.

Experimental fact 1. *Let C be a $[n, k]_q$-code of regularity 2, with minimum distance $d = \mathrm{d}_{\min}(\mathsf{C})$ and dual minimum distance $d^\perp = \mathrm{d}_{\min}(\mathsf{C}^\perp)$.*

1. *For all $r \geq d^\perp$ we have $\beta_{r-2,r}(\mathsf{C}) > 0$. Moreover, quite often (but not always) we have $\beta_{d^\perp-2,d^\perp}(\mathsf{C}) = A_{d^\perp}(\mathsf{C}^\perp)$.*
2. *Dually, for all $r \leq k + 1 - d$ we have $\beta_{r-1,r}(\mathsf{C}) > 0$. Moreover, quite often (but not always) we have $\beta_{k-d,k+1-d}(\mathsf{C}) = A_d(\mathsf{C})$.*

It follows that $\mathrm{def}(\varphi_r) > 0$ for $d^\perp \leq r \leq \frac{k(k+1)}{n}$ and for $\frac{k(k+1)}{n} \leq\ r \leq k+1-d$, when applicable (i.e. when these intervals are nonempty).

Conversely, for a random C among codes of given parameters $[n, k, d, d^\perp]_q$, the probability that $\mathrm{def}(\varphi_r) = 0$ tends quickly to 1 as $r \ll \min\left(d^\perp, \frac{k(k+1)}{n}\right)$ and as $r \gg \max\left(\frac{k(k+1)}{n}, k+1-d\right)$. In particular $r_{\max}(\mathsf{C}) = \max\left(\left\lfloor\frac{k(k+1)}{n}\right\rfloor, k+1-d\right)$, or is very close to this value, with high probability.

As an illustration, Figure 13 in the Supplementary material presents statistics on $\mathrm{def}(\varphi_r)$ for random $[56, 16]_2$-codes.

Consequently, we postulate:

Heuristic 1. *Fix a field cardinality q, assume n is not too close to k in order to stay away from the counterexamples to the minimal resolution conjecture, and $n < \binom{k+1}{2}$ in order to ensure regularity 2. Then for random $[n, k]_q$-codes, with high probability:*

1. *if* $d^{\perp} > \frac{k(k+1)}{n}$ *we expect* $\beta_{r-1,r} = \left(\frac{k(k+1)}{r} - n\right)\binom{k-1}{r-2}$ *for* $r < \frac{k(k+1)}{n}$
2. *if* $d > k+1-\frac{k(k+1)}{n}$ *we expect* $\beta_{r-1,r} = 0$ *for* $r > \frac{k(k+1)}{n}$.

Remark 2. Consider this Heuristic in the asymptotic regime. Setting $R = k/n$, we can take $d = \mathrm{d}_{GV}(q,n,k) \approx H_q^{-1}(1-R)n$ and $d^{\perp} = \mathrm{d}_{GV}(q,n,n-k) \approx H_q^{-1}(R)n$ the corresponding Gilbert-Varshamov distance. Then the condition in 1. translates as $H_q^{-1}(R) > R^2$, and the condition in 2. translates as $H_q^{-1}(1-R) > R(1-R)$, both of which are satisfied when R is small enough. In particular for $q = 2$, we find that 1. is satisfied for $R < 0.141$ and 2. is satisfied for $R < 0.277$.

5 The distinguisher, with and without shortening

General principles

Distinguishers for alternant or Goppa codes tend to work better when t is small and n is large. When benchmarking, it is thus common to:

- first fix q, m, and then for $n = q^m$, find the largest distinguishable t
- once such a t is found, fix q, m, t, and find the smallest distinguishable n.

Also, distinguishers typically work by computing certain code invariants. We might have theoretical bounds on the values of these invariants, that are essential for an asymptotic analysis. However these bounds need not be tight. Hence for a given set of finite parameters, we can also adopt a more empirical approach: sample a certain number of codes, compute their invariants, and observe when the distinguisher "just works".

So for given q, m, t and a type of codes (alternant or Goppa), we set $n = q^m$ and we compute the Betti numbers of a certain number of dual codes. Most of the time, it turns out that these numbers are the same for all samples. We will denote by $\beta^*_{r-1,r}$ these common values. By Corollary 3, these $\beta^*_{r-1,r}$ still provide lower bounds on $\beta_{r-1,r}$ for smaller n.

On the other hand, for random codes of dimension $k = mt$, if Heuristic 1 applies, (86) gives that $\beta_{r-1,r}$ should be equal, or very close, to $\left(\frac{k(k+1)}{r} - n\right)^{+}\binom{k-1}{r-2}$. Thus we expect to distinguish when this value is smaller than $\beta^*_{r-1,r}$, or equivalently when

$$n \geq \left\lceil \frac{k(k+1)}{r} - \frac{\beta^*_{r-1,r} - 1}{\binom{k-1}{r-2}} \right\rceil \tag{88}$$

(provided $\beta^*_{r-1,r} > 0$).

When $r = 2$, this gives the distinguishability threshold of the square code distinguisher of [11]. Using syzygies of higher degree r allows to make the term $\frac{k(k+1)}{r}$ smaller and reach a broader range of parameters.

As for shortening, we do not expect it to improve the distinguishability threshold. This technique is used only, but crucially, to reduce the overall complexity when parameters grow larger.

Now let us see how our syzygy distinguisher fares, first on the examples proposed in [6], and then on the `Classic McEliece` system.

Goppa codes with $q = 4$, $m = 4$, $t = 4$, irreducible Goppa polynomial

For these parameters, the square code distinguisher works down to $n_{\text{square}} = \mathbf{97}$, while the distinguisher of [6] works down to $n_{\text{CMT}} = \mathbf{80}$.

We experimentally find that dual Goppa codes C with these parameters, with $n = q^m = 256$, consistently have $r_{\max} = 4$, which is better than the lower bound in Theorem 1 ($e = 0$, $r_{\max} \geq t - 1 = 3$). Moreover, their Betti numbers are:

$$\beta^*_{1,2} = 40, \qquad \beta^*_{2,3} = 80, \qquad \beta^*_{3,4} = 12. \tag{89}$$

We then observe that the $\beta_{2,3}$-distinguisher works down to $n_{\beta_{2,3}} = \mathbf{86}$, and the $\beta_{3,4}$-distinguisher works down to $n_{\beta_{3,4}} = \mathbf{68}$, both of which coincide with (88). More precisely, computing the Betti numbers of dual Goppa and random codes around these values of n consistently yields:

n	$\cdots$	88	87	**86**	85	84	$\cdots$	70	69	**68**	67	66	$\cdots$
$\beta_{2,3}^{\mathsf{Gop}^{\text{irr},\perp}}$		80	80	**80**	85	100		310	325	340	355	370	
$\beta_{2,3}^{\text{random}}$		40	55	**70**	85	100		310	325	340	355	370	
$\beta_{3,4}^{\mathsf{Gop}^{\text{irr},\perp}}$		12	12	12	12	12		12	12	**12**	105	210	
$\beta_{3,4}^{\text{random}}$		0	0	0	0	0		0	0	**0**	105	210	

We see that they stick to their "predicted" values: $\beta_{r-1,r} = \max(\beta^*_{r-1,r}, \text{ind}(\varphi_r)^+)$ for dual Goppa, and $\beta_{r-1,r} = \text{ind}(\varphi_r)^+$ for random codes.

Goppa codes with $q = 2$, $m = 6$, $t = 3$, irreducible Goppa polynomial

For these parameters, the square code distinguisher works down to $n_{\text{square}} = \mathbf{62}$, while the distinguisher of [6] works down to $n_{\text{CMT}} = \mathbf{59}$.

We experimentally find that dual Goppa codes C with these parameters, with $n = q^m = 64$, consistently have $r_{\max} = 8$, which is better than the lower bound in Corollary 4 ($\widehat{e} = 1$, $r_{\max} \geq 7$). Moreover, their top Betti numbers are:

$$\beta^*_{5,6} = 1020, \qquad \beta^*_{6,7} = 288, \qquad \beta^*_{7,8} = 42. \tag{90}$$

From (88) we expect to distinguish at $\beta_{5,6}$ for $n \geq 57$, at $\beta_{6,7}$ for $n \geq 49$, and at $\beta_{7,8}$ for $n \geq 43$.

And indeed at $n_{\beta_{5,6}} = \mathbf{57}$ we consistently find $\beta_{5,6} \geq 1020$ for dual Goppa codes, while $\beta_{5,6} < 500$ for random codes with quite high probability.

For smaller n we have to pass to $\beta_{6,7}$. The $\beta_{6,7}$-distinguisher works well for $n = 56$, but the quality gradually falls (distinguishing errors occur more frequently) as n becomes smaller. It is difficult to point a precise threshold where the distinguisher ceases to work. Arguably we still have a positive advantage at

$n_{\beta_{6,7}} = \mathbf{50}$, but not anymore at $n = 49$. We could then try with $\beta_{7,8}$, but this fails too.

What happens? It turns out the conditions in Heuristic 1 are not satisfied anymore to ensure $\mathrm{def}(\varphi_r) = 0$, or even $\mathrm{def}(\varphi_r)$ small, for these values of r and n. From Experimental fact 1, in order to have $\beta_{r-1,r} = 0$, we need $r > k+1-d$, where $d = \mathrm{d}_{\min}(\mathsf{C})$. For $r = 7$ and $k = mt = 18$ this gives $d \geq 13$. For smaller d we expect a loose link between $\beta_{r-1,r}$ and the weight distribution of C. The distinguisher still works as long as random codes satisfy $\beta_{r-1,r} < \beta^*_{r-1,r}$ w.h.p., and experimentally, for $r = 7$, we find this inequality is satisfied for random codes of minimum distance $d \geq 10$, while $d = 9$ is a borderline case, and $d \leq 8$ fails invariably. Now, as n decreases from 56 to 50, the proportion of random codes with $d \geq 10$ also decreases, and they become minority for $n = 49$.

The `Classic McEliece 348864` system

We consider a dual code $\mathsf{C} \in \mathsf{Gop}^{\mathrm{irr},\perp}_{2,12,3488,64}$ proper of dimension $k = mt = 768$. Theorem 1 gives $e = 5$, $r_{\max}(\mathsf{C}) \geq 321$, which Corollary 4 improves to $\widehat{e} = 3$, $r_{\max}(\mathsf{C}) \geq 427$.

For $n = 3488$ and $k = 768$ we have $\left\lfloor \frac{k(k+1)}{n} \right\rfloor = 169$. Moreover, $d = \mathrm{d}_{GV}(2, n, k) = 810$, so $k + 1 - d < 0$. By Heuristic 1 we expect to distinguish at $\beta_{r-1,r}$ with $r = 170$, with a large margin of safety. For this, Algorithm 1 computes the left kernel of the matrices $\mathbf{M}_i$ for $i \leq r$, where $\mathbf{M}_i$ has size $k\beta_{i-2,i-1} \times \binom{k+1}{2}\beta_{i-3,i-2}$. Using $\mathrm{ind}(\varphi_i) = \left(\frac{k(k+1)}{i} - n\right)\binom{k-1}{i-2}$ as a lower bound for these $\beta_{i-1,i}$, we find that the maximal dimension of these matrices is at least 2^{596}. Using $\omega \approx 2.372$ for the exponent of linear algebra gives a complexity at least 2^{1414}.

However we have plenty of space in the interval $170 \leq r \leq 427$ to apply shortening. Set $s = 377$, $n_s = n - s = 3111$, $k_s = k - s = 391$. If C_s is a s-shortened $\mathsf{Gop}^{\mathrm{irr},\perp}_{2,12,3488,64}$, Corollary 4 ensures $r_{\max}(\mathsf{C}_s) \geq 427 - s = 50$. On the other hand, we have $\left\lfloor \frac{k_s(k_s+1)}{n_s} \right\rfloor = 49$, and $d_s = \mathrm{d}_{GV}(2, n_s, k_s) = 921$, so $k_s + 1 - d_s \ll 0$. Thus we expect to distinguish at β_{r_s-1,r_s} with $r_s = 50$. Now, for $i \leq r_s$, the matrix $\mathbf{M}_i$ has size $k_s\beta_{i-2,i-1} \times \binom{k_s+1}{2}\beta_{i-3,i-2}$. As $d_s^\perp = \mathrm{d}_{GV}(2, n_s, n_s - k_s) = 55 > r_s$, these $\beta_{i-1,i}$ can be estimated as $\mathrm{ind}(\varphi_i) = \left(\frac{k_s(k_s+1)}{i} - n_s\right)\binom{k_s-1}{i-2}$. We then find that the maximal dimension of these matrices is around 2^{223}, and the complexity around 2^{529}.

Asymptotics

Fix a base field cardinality q, for instance $q = 2$, and a (dual) rate R. In [4] it is suggested to work with a primal code of rate between 0.7 and 0.8, so passing to the dual gives $0.2 \leq R \leq 0.3$. For $n \to \infty$ we set:

- $m = \lceil \log_q(n) \rceil = \log_q(n) + O(1)$
- $k \approx Rn$ such that:
- $t = \frac{k}{m}$ is an integer.

Theorem 3. *Let $\mathcal{T} = \mathsf{Alt}^\perp$, $\mathsf{Gop}^\perp$, $\mathsf{Gop}^{\mathrm{sqfr},\perp}$, or $\mathsf{Gop}^{\mathrm{irr},\perp}$ be a type of codes. Assume we have a lower bound of the form*

$$r_{\max}(\mathsf{C}_s) \geq k - s^* - s \tag{91}$$

with $s^* = s^*(\mathcal{T}_{q,m,n,t}) = o(n)$, valid for all $\mathsf{C} \in \mathcal{T}_{q,m,n,t}$ and all s-shortened subcodes C_s of C. Let then $r = o(n)$ be an integer such that $\frac{(s^*+r)(s^*+r+1)}{n-k+s^*+r} < r$. Now let C be a $[n,k]_q$-code. Then computing

$$\beta_{r-1,r}(\mathsf{C}_{k-s^*-r}), \tag{92}$$

where C_{k-s^*-r} is a $(k-s^*-r)$-shortening of C, allows to distinguish with high probability whether C is a random code ($\beta_{r-1,r} = 0$) or an element of $\mathcal{T}_{q,m,n,t}$ ($\beta_{r-1,r} > 0$), by doing at most r kernel computations of linear maps between vector spaces whose maximal dimension can be estimated as $(s^*+r)^3\binom{s^*+r}{r-3}$.

In fact it is possible to take $s^* \approx R\frac{\log_q \log_q(n)}{\log_q(n)}n$ and $r \approx \frac{R^2}{1-R}\left(\frac{\log_q \log_q(n)}{\log_q(n)}\right)^2 n$, which gives for the total complexity of the process an estimated upper bound of

$$\kappa = q^{\left(\omega\frac{R^2}{1-R}+o(1)\right)\frac{(\log_q \log_q(n))^3}{(\log_q(n))^2}n}. \tag{93}$$

Observe [5, §3.4] that the security parameter in the `Classic McEliece` system, based on the complexity of generic decoding algorithms, is linear in $t \propto n/\log(n)$. Then in (93) we have $\frac{\log(\kappa)}{n/\log(n)} \propto \frac{(\log\log(n))^3}{\log(n)} \to 0$, which means that our complexity is subexponential in the security parameter.

Proof. The shortened code C_{k-s^*-r} has dimension s^*+r and length $n-k+s^*+r$. As s^* and r are $o(n)$ we have $s^*+r \ll n-k+s^*+r$, and d_{GV} is close to the length. Moreover $\frac{(s^*+r)(s^*+r+1)}{n-k+s^*+r} < r$ by hypothesis. Thus Heuristic 1 applies, and we expect $\beta_{r-1,r}(\mathsf{C}_{k-s^*-r}) = 0$ with high probabilty when C is random. On the other hand, (91) gives $\beta_{r-1,r}(\mathsf{C}_{k-s^*-r}) > 0$ for $\mathsf{C} \in \mathcal{T}_{q,m,n,t}$. Using Algorithm 1 we obtain $\beta_{r-1,r}(\mathsf{C}_{k-s^*-r})$ after computing the left kernel of the matrices $\mathbf{M}_i$ for $i \leq r$, where $\mathbf{M}_i$ has size $(s^*+r)\beta_{i-2,i-1}(\mathsf{C}_{k-s^*-r}) \times \binom{s^*+r+1}{2}\beta_{i-3,i-2}(\mathsf{C}_{k-s^*-r})$. As the rate $\frac{s^*+r}{n-k+s^*+r}$ goes to zero, by Heuristic 1 again we can estimate the largest dimension of this matrix as $\binom{s^*+r+1}{2}\mathrm{ind}(\varphi_{i-2,\mathsf{C}_{k-s^*-r}}) \leq (s^*+r)^3\binom{s^*+r}{r-3}$, for random codes — and we can assume this holds also for codes in $\mathcal{T}$, otherwise computing this dimension readily provides a distinguisher with lower complexity.

Now for a concrete choice of s^* and r, set

- $e = \lfloor \log_q(t-1) \rfloor = \log_q(n) - \log_q \log_q(n) + O(1)$
- $f = (e+1)t - \frac{q^{e+1}-1}{q-1} = et + O(t)$

so

$$f = \left(1 - \frac{\log_q \log_q(n)}{\log_q(n)} + O\left(\frac{1}{\log_q(n)}\right)\right)k. \tag{94}$$

By Theorem 1, for all s and all $\mathsf{C} \in \mathcal{T}_{q,m,n,t}$ we have $r_{\max}(\mathsf{C}_s) \geq f - s$, so we can take $s^* = k - f \approx R\frac{\log_q \log_q(n)}{\log_q(n)}n$ as claimed. (In the binary Goppa case we could use Corollary 4 instead of Theorem 1, but this leads to the same estimate on f, hence on s^*.) Then for $\varepsilon > 0$, setting $r = \left\lceil (1+\varepsilon)\frac{R^2}{1-R}\left(\frac{\log_q \log_q(n)}{\log_q(n)}\right)^2 n \right\rceil \ll s^*$, we have $\frac{(s^*+r)(s^*+r+1)}{n-k+s^*+r} \approx \frac{(s^*)^2}{n-k} \approx \frac{R^2}{1-R}\left(\frac{\log_q \log_q(n)}{\log_q(n)}\right)^2 n \ll r$, and then we can let $\varepsilon \to 0$.

Last, for the complexity estimate (93), using $r \ll s^*$ again and Stirling's formula, we get $\log_q\left((s^*+r)^3\binom{s^*+r}{r-3}\right) \approx r\log_q\left(\frac{s^*}{r}\right)$, and we conclude.

We observe it is possible to slightly relax the condition $m = \lceil \log_q(n) \rceil$: complexity remains subexponential as long as $\frac{m}{\log_q(n)} \to 1$ fast enough.

6 Conclusion and open problems

We presented the first structural analysis of the McEliece cryptosystem whose asymptotic complexity is better than that of generic decoding algorithms, more precisely, subexponential in the error-correcting capability of the code. However this is only an asymptotic result. For concrete, finite parameters, such as those proposed in the `Classic McEliece` specification, a naive implementation of our distinguisher still falls beyond the security parameter by a non-negligible factor.

Problem 1. To what extent can the implementation of the distinguisher be improved? For instance, if we choose a monomial order in Algorithm 1, and have a reduced basis for one syzygy space, then the generalized Macaulay matrix constructed from it will be:

- somewhat sparse
- already partially reduced.

This could be exploited to make the computation of (a reduced basis of) the next syzygy space faster. More generally, optimizations used in related domains, for instance in Gröbner basis algorithms, could probably be imported.

(Interestingly, the author was led to introduce the shortening technique in this distinguisher by serendipity, after witnessing a strange phenomenon while partially implementing the optimization alluded in Problem 1.)

Problem 2. Can our distinguisher, and in particular the Betti number computation, benefit from a quantum speedup?

Problem 3. Our lower bounds on the Betti numbers, and in particular the $r_{\max}$, of dual alternant or Goppa codes, are not tight in general. Can they be improved? Better, can one give a complete, explicit description of the minimal resolution of these codes? (See the Supplementary material for elements in this direction.) How would this impact the complexity of the distinguisher?

We initiated the study of syzygies of codes (or equivalently, of finite sets of points in projective space) from a genuinely coding theoretical perspective.

Problem 4. Pursue this study in a systematic way. This should cover basic operations on codes that have a standard geometric interpretation, such as puncturing (discarding one subset from a set of points), shortening (projection from one or several of the points), duality of codes ("Gale duality"), tensor product of codes (Segre embedding), and powers of codes (Veronese embedding), but also other operations such as the $(u|u+v)$, subfield subcode, or trace code constructions; and crucially, make links with various metric properties of the code such as its weight distribution, generalized weight hierarchy, etc.

Problem 5. Can syzygies serve in decoding algorithms?

Problem 6. Can our syzygy distinguisher be turned into a key recovery attack, or more properly, can some of the ideas beneath be used to build a key recovery attack? For instance, one would like to combine syzygies with:

- filtration arguments
- extraction of short relations, e.g. via `MinRank` techniques.

(Observe that some of the explicit syzygies described in Proposition 3 are short.)

It is very common that new mathematical tools (Euclidean lattices, elliptic curves, pairings, isogenies...) are introduced in the cryptographic realm first for cryptanalytic purposes, i.e. to break systems. Once digested by the community, they are then used in a more constructive way, to build new cryptosystems.

Problem 7. Can one devise syzygy-based cryptography?

References

1. Bardet, M., Mora, R., Tillich, J.P.: Polynomial Time Key-Recovery Attack on High Rate Random Alternant Codes. IEEE Trans. Inform. Theory **70**(6), 4492–4511 (2024)
2. Berlekamp, E.R., McEliece, R.J., van Tilborg, H.C.A.: On the inherent intractability of certain coding problems. IEEE Trans. Inform. Theory **IT-24**(3), 384–386 (1978)
3. Cascudo, I., Cramer, R., Mirandola, D., Zémor, G.: Squares of random linear codes. IEEE Trans. Inform. Theory **61**(3), 1159–1173 (2015)
4. Classic McEliece: conservative code-based cryptography: design rationale (23 October 2022), available at http://classic.mceliece.org/mceliece-rationale-20221023.pdf
5. Classic McEliece: conservative code-based cryptography: guide for security reviewers (23 October 2022), available at http://classic.mceliece.org/mceliece-security-20221023.pdf
6. Couvreur, A., Mora, R., Tillich, J.P.: A new approach based on quadratic forms to attack the McEliece cryptosystem. In: Guo, J., Steinfeld, R. (eds.) ASIACRYPT 2023, Part IV. LNCS, vol. 14441, pp. 3–38. Springer, Heidelberg, Germany, Guangzhou, China (Dec 4–8, 2023). https://doi.org/10.1007/978-981-99-8730-6˙1

7. Couvreur, A., Otmani, A., Tillich, J.P.: Polynomial time attack on wild McEliece over quadratic extensions. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 17–39. Springer, Heidelberg, Germany, Copenhagen, Denmark (May 11–15, 2014). https://doi.org/10.1007/978-3-642-55220-5˙2
8. Eagon, J.A., Northcott, D.G.: Ideals defined by matrices and a certain complex associated with them. Proc. Roy. Soc. London Ser. A **269**, 188–204 (1962)
9. Eisenbud, D.: The geometry of syzygies, Graduate Texts in Mathematics, vol. 229. Springer-Verlag, New York (2005)
10. Eisenbud, D., Popescu, S.: Gale duality and free resolutions of ideals of points. Invent. Math. **136**(2), 419–449 (1999)
11. Faugère, J.C., Gauthier-Umaña, V., Otmani, A., Perret, L., Tillich, J.P.: A distinguisher for high-rate McEliece cryptosystems. IEEE Trans. Inform. Theory **59**(10), 6830–6844 (2013)
12. Gibson, J.K.: Equivalent Goppa codes and trapdoors to McEliece's public key cryptosystem (rump session). In: Davies, D.W. (ed.) EUROCRYPT'91. LNCS, vol. 547, pp. 517–521. Springer, Heidelberg, Germany, Brighton, UK (Apr 8–11, 1991). https://doi.org/10.1007/3-540-46416-6˙46
13. Goppa, V.D.: A new class of linear correcting codes. Problemy Peredači Informacii **6**(3), 24–30 (1970)
14. Green, M., Lazarsfeld, R.: Some results on the syzygies of finite sets and algebraic curves. Compositio Math. **67**(3), 301–314 (1988)
15. Hansen, J.P.: Linkage and codes on complete intersections. Appl. Algebra Engrg. Comm. Comput. **14**(3), 175–185 (2003)
16. Hirschowitz, A., Simpson, C.: La résolution minimale de l'idéal d'un arrangement général d'un grand nombre de points dans $\mathbf{P}^n$. Invent. Math. **126**(3), 467–503 (1996)
17. Johnsen, T., Verdure, H.: Stanley-Reisner resolution of constant weight linear codes. DCC **72**(2), 471–481 (2014)
18. Lorenzini, A.: The minimal resolution conjecture. J. Algebra **156**(1), 5–35 (1993)
19. Marquez-Corbella, I., Pellikaan, R.: Error-correcting pairs for a public-key cryptosystem (2012), Code-based Cryptography Workshop 2012, 9–11 May 2012, Lyngby, Denmark
20. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory (1978), DSN Progress Report 42-44
21. Mora, R., Tillich, J.P.: On the dimension and structure of the square of the dual of a Goppa code. DCC **91**(4), 1351–1372 (2023)
22. Mumford, D.: Lectures on curves on an algebraic surface, Annals of Mathematics Studies, vol. 59. Princeton University Press, Princeton, NJ (1966), with a section by G. M. Bergman
23. Patarin, J.: Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In: Maurer, U.M. (ed.) EUROCRYPT'96. LNCS, vol. 1070, pp. 33–48. Springer, Heidelberg, Germany, Saragossa, Spain (May 12–16, 1996). https://doi.org/10.1007/3-540-68339-9˙4
24. Prange, E.: The use of information sets in decoding cyclic codes. IRE Trans. **IT-8**, S 5–S 9 (1962)
25. Randriambololona, H.: On products and powers of linear codes under componentwise multiplication. In: Algorithmic arithmetic, geometry, and coding theory, Contemp. Math., vol. 637, pp. 3–78. Amer. Math. Soc., Providence, RI (2015)
26. Rentería, C., Tapia-Recillas, H.: Linear codes associated to the ideal of points in $\mathbf{P}^d$ and its canonical module. Comm. Algebra **24**(3), 1083–1090 (1996)

Supplementary material

More on syzygies of shortened dual alternant and Goppa codes

It is possible to improve the lower bound on $\beta_{r-1,r}(\mathsf{C}_s)$ in Theorem 1, using not only $\mathbf{\Phi} = \mathbf{\Phi}^{(0)}$, but also its conjugates $\mathbf{\Phi}^{(1)}, \dots, \mathbf{\Phi}^{(m-1)}$.

Let us first consider the simpler case $s = 0$.

The Eagon-Northcott complex of each such conjugate gives a subcomplex of the minimal resolution of C, however one should take care of the fact that in general these subcomplexes are not in direct sum. Proposition 3 gives a basis $s^{(j)}_{r;i_1,\dots,i_r}(\mathbf{\Phi}^{(u)})$ for each syzygy space $M_{r-1,r}(\mathbf{\Phi}^{(u)})$. The indices $i_1, \dots, i_r$ correspond to columns of $\mathbf{\Phi}^{(u)} = \left(\mathbf{B}_0^{(u+e)} \middle| \mathbf{B}_1^{(u+e-1)} \middle| \cdots \middle| \mathbf{B}_e^{(u)}\right)$. It is then easily seen:

Proposition 11. *The $s^{(j)}_{r;i_1,\dots,i_r}(\mathbf{\Phi}^{(u)})$ with column i_1 not in $\mathbf{B}_0^{(e+u)}$ also belong to $M_{r-1,r}(\mathbf{\Phi}^{(u-1)})$. Conversely, for $e < m/2$, those with i_1 in $\mathbf{B}_0^{(e+u)}$ are linearly independent, hence form a basis of the subspace $V_r = M_{r-1,r}(\mathbf{\Phi}^{(0)}) + \cdots + M_{r-1,r}(\mathbf{\Phi}^{(r)})$ of $M_{r-1,r}(\mathsf{C})$.*

This gives the improved lower bound:

Corollary 6. *Set $e = \lfloor \log_q(t-1) \rfloor$ and $f = (e+1)t - \frac{q^{e+1}-1}{q-1}$. Then for any $r \geq 2$ we have*

$$\beta_{r-1,r}(\mathsf{C}) \ \geq \ \dim(V_r) = m(r-1)\left(\binom{f}{r} - \binom{f-(t-1)}{r}\right). \tag{95}$$

For $r = 2$ this specializes to

$$\beta_{1,2}(\mathsf{C}) \ \geq \ \dim(V_2) = \frac{m(t-1)}{2}\left((2e+1)t - 2\frac{q^{e+1}-1}{q-1}\right), \tag{96}$$

a result already proved in [11] by (essentially) the same method. It is observed moreover than in many cases the lower bound (96) is an equality, so we actually have

$$I_2(\mathsf{C}) = V_2. \tag{97}$$

Likewise for $r > f - (t-1)$ this gives

$$\beta_{r-1,r}(\mathsf{C}) \ \geq \ \dim(V_f) = m(r-1)\binom{f}{r} \tag{98}$$

and we will see examples where this is an equality.

However for arbitrary r, the improved lower bound (95) still isn't tight, because the inclusion $V_r \subseteq M_{r-1,r}(\mathsf{C})$ is strict in general. For instance, one can show that $M_{2,3}(\mathsf{C})$ contains syzygies of the form

$$\begin{aligned} X_a(X^{(u)}_{b+1}X^{(u+v)}_{c+1} - X^{(u)}_{b+q^v+1}X^{(u+v)}_{c}) - X_{a+q^u}(X^{(u)}_{b}X^{(u+v)}_{c+1} - X^{(u)}_{b+q^v}X^{(u+v)}_{c}) + \\ + X^{(u+v)}_{c}(X_aX^{(u)}_{b+q^v+1} - X_{a+q^u}X^{(u)}_{b+q^v}) - X^{(u+v)}_{c+1}(X_aX^{(u)}_{b+1} - X_{a+q^u}X^{(u)}_{b}) = 0 \end{aligned} \tag{99}$$

that do not belong to V_3 in general.

In principle, under (97) it should be possible to use the explicit description of V_2 together with Proposition 2 to compute (the linear strand of) the minimal resolution of C. However the combinatorics appears quite complicated.

Now for general s, (68) and (73) can be extended to:

Experimental fact 2. *Let C be a dual alternant code. Then for all s we have*

$$r_{\max}(\mathsf{C}_s) \geq r_{\max}(\mathsf{C}) - s. \tag{100}$$

It would be tempting to conjecture that (100) holds for all codes, but it turns out that one can find counterexamples. However, these counterexamples are quite rare. So maybe an interesting problem instead should be to give criteria for (100) to hold.

Observe that shortening is dual to puncturing. As the behaviour of minimal resolutions of codes under puncturing is quite well understood (Corollary 3), maybe the study of shortening should go hand-in-hand with that of code duality. Experiments suggest a loose link between $\beta_{r-2,r}(\mathsf{C}^{\perp})$ and $\beta_{k-r,k+1-r}(C)$, at least for some regimes of parameters.

Back to dual alternant or Goppa codes, we actually observe a strong regular pattern (for Goppa codes the author only tested the irreducible case, but the result is likely to generalize):

Experimental fact 3. *Let $\mathcal{T} = \mathsf{Alt}^{\perp}$ or $\mathsf{Gop}^{\mathrm{irr},\perp}$ be a type of codes, namely, either dual alternant codes, or dual Goppa codes with irreducible Goppa polynomial. Let q be a field cardinality, and $t \geq 3$ an integer.*

1. *For all m large enough,*
$$r_{\max}(\mathsf{C}) = r^*_{\mathcal{T},q,t} \tag{101}$$
is the same for generic proper $\mathsf{C} \in \mathcal{T}_{q,m,q^m,t}$, i.e. it generically does not depend on m nor on the choice of C, but only on $\mathcal{T}, q, t$.

Now $\mathcal{T}, q, t$ being fixed, we set $r^* = r^*_{\mathcal{T},q,t}$. Also, given m, t, we set $k = mt$.

2. *For all m, for all $n \leq q^m$, for generic proper $\mathsf{C} \in \mathcal{T}_{q,m,n,t}$, and for all $s \leq r^* - 2$, if $r^* - s > \max\left(\frac{(k-s)(k-s+1)}{n-s}, k - s + 1 - \mathrm{d}_{\min}(\mathsf{C}_s)\right)$, then*
$$r_{\max}(\mathsf{C}_s) = r^* - s. \tag{102}$$

3. *For $0 \leq i \leq r^* - 2$ there are functions $b_i(r)$ (actually depending on $\mathcal{T}, q, t$, so $b_i(r) = b_{i,\mathcal{T},q,t}(r)$) such that, for all m, for all $n \leq q^m$, for generic proper $\mathsf{C} \in \mathcal{T}_{q,m,n,t}$, for all $s \leq r^* - 2$, and for all r in the interval $2 \leq r \leq r^* - s$, if $r > \max\left(\frac{(k-s)(k-s+1)}{n-s}, k - s + 1 - \mathrm{d}_{\min}(\mathsf{C}_s)\right)$, then*
$$\beta_{r-1,r}(\mathsf{C}_s) = m\, b_{r^*-s-r}(r). \tag{103}$$

4. We have $b_0(r) = r - 1$ *independently of* $\mathcal{T}, q, t$, *so* (103) *reduces to*

$$\beta_{r^*-s-1,r^*-s}(\mathsf{C}_s) = m\,(r^* - s - 1). \qquad (104)$$

More generally for $i \geq 1$ *we have* $b_i(r) = (r-1)\binom{r+i}{i}$ *for a certain number of (but now, not for all) values of* $\mathcal{T}, q, t$, *so then* (103) *reduces to*

$$\beta_{r-1,r}(\mathsf{C}_s) = m\,(r-1)\binom{r^* - s}{r}. \qquad (105)$$

We observe that (68) gives a lower bound on r^*. For alternant codes, experimentally, this lower bound is an equality. However for Goppa codes this lower bound seems to be always a strict inequality. And even for binary Goppa codes, the improved lower bound (73) still is a strict inequality.

s	$\beta_{1,2}$	$\beta_{2,3}$	$\beta_{3,4}$	$\beta_{4,5}$	$\beta_{5,6}$	$\beta_{6,7}$	$\beta_{7,8}$
0	251	1400	3230	2480	**1400**	**480**	**70**
1	202	880	1170	**840**	**350**	**60**	–
2	154	440	**450**	**240**	**50**	–	–
3	107	**200**	**150**	**40**	–	–	–
4	66	**80**	**30**	–	–	–	–
5	31	**20**	–	–	–	–	–
6	**10**	–	–	–	–	–	–
7	–	–	–	–	–	–	–

Fig. 8. s-shortened $\mathsf{Alt}^{\perp}_{2,10,5}$ $(r^* = 8)$

s	$\beta_{1,2}$	$\beta_{2,3}$	$\beta_{3,4}$	$\beta_{4,5}$	$\beta_{5,6}$	$\beta_{6,7}$	$\beta_{7,8}$
0	222	1943	1725	**1120**	**700**	**240**	**35**
1	193	1344	**525**	**420**	**175**	**30**	–
2	165	801	**225**	**120**	**25**	–	–
3	138	312	**75**	**20**	–	–	–
4	112	**40**	**15**	–	–	–	–
5	87	**10**	–	–	–	–	–
6	63	–	–	–	–	–	–
7	40	–	–	–	–	–	–
8	18	–	–	–	–	–	–

Fig. 9. s-shortened $\mathsf{Alt}^{\perp}_{3,5,6}$ $(r^* = 8)$

s	$\beta_{1,2}$	$\beta_{2,3}$	$\beta_{3,4}$	$\beta_{4,5}$	$\beta_{5,6}$	$\beta_{6,7}$	$\beta_{7,8}$	$\beta_{8,9}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
8	280	3224	7464	4272	**3360**	**1728**	**504**	**64**
9	249	2510	1800	**1792**	**1120**	**384**	**56**	–
10	219	1856	**840**	**672**	**280**	**48**	–	–
11	190	1260	**360**	**192**	**40**	–	–	–
12	162	720	**120**	**32**	–	–	–	–
13	135	234	**24**	–	–	–	–	–
14	109	**16**	–	–	–	–	–	–

Fig. 10. s-shortened $\mathsf{Gop}^{\perp}_{2,8,5}$ $(r^* = 17)$

s	$\beta_{1,2}$	$\beta_{2,3}$	$\beta_{3,4}$	$\beta_{4,5}$	$\beta_{5,6}$	$\beta_{6,7}$
0	180	1293	3090	3144	960	**36**
1	151	810	1350	732	**30**	–
2	123	450	450	**24**	–	–
3	96	210	24	–	–	–
4	70	30	–	–	–	–
5	45	–	–	–	–	–
6	21	–	–	–	–	–
7	–	–	–	–	–	–

Fig. 11. s-shortened $\mathsf{Gop}^{\perp}_{3,6,5}$ $(r^* = 7)$

s	$\beta_{1,2}$	$\beta_{2,3}$	$\beta_{3,4}$	$\beta_{4,5}$	$\beta_{5,6}$	$\beta_{6,7}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
32	719	8474	**450**	**240**	**50**	–
33	662	6216	**150**	**40**	–	–
34	606	4070	**30**	–	–	–
35	551	2034	–	–	–	–

Fig. 12. s-shortened $\mathsf{Gop}^{\perp}_{2,10,9}$ $(r^* = 38)$

These Figures illustrate the last Experimental fact. Boldface values match (105). This strongly suggests that the minimal resolution of the codes contains m conjugate Eagon-Northcott complexes of length r^*, whose top degree components are in direct sum.

Experimental data on defects for random codes

Figure 13 presents statistics on $\mathrm{def}(\varphi_r)$ ($2 \leq r \leq 8$) for random $[56, 16]_2$-codes. For each pair $(d, d^\perp)$, a few thousands of codes with these parameters were sampled uniformly (using rejection sampling). The average value of $\mathrm{def}(\varphi_r)$ among these samples is displayed, and also its 99% distribution interval (which means at most 0.5% fall below and at most 0.5% above).

Here we have $\frac{k(k+1)}{n} \approx 4.86$. Then, in accordance with Experimental fact 1, we can check $\mathrm{def}(\varphi_r) > 0$ for $d^\perp \leq r \leq 4$ and for $5 \leq r \leq 17 - d$ (when applicable), while $\mathrm{def}(\varphi_r) = 0$ with high probability as we move away from these intervals.

$d^\perp = 3$

r	$d=11$ mean	$d=11$ 99%	$d=12$ mean	$d=12$ 99%	$d=13$ mean	$d=13$ 99%	$d=14$ mean	$d=14$ 99%
2	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$
3	1.269	$[1,3]$	1.245	$[1,3]$	1.201	$[1,3]$	1.164	$[1,3]$
4	23.821	$[15,55]$	23.171	$[15,52]$	21.975	$[15,48]$	20.902	$[14,47]$
5	6.927	$[5,21]$	1.948	$[1,8]$	0.345	$[0,5]$	0.067	$[0,1]$
6	1.341	$[1,7]$	0.086	$[0,1]$	0.006	$[0,1]$	0.000	$[0,0]$
7	0.042	$[0,1]$	0.001	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$
8	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$

$d^\perp = 4$

r	$d=11$ mean	$d=11$ 99%	$d=12$ mean	$d=12$ 99%	$d=13$ mean	$d=13$ 99%	$d=14$ mean	$d=14$ 99%
2	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$
3	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$
4	6.178	$[1,14]$	5.963	$[1,14]$	5.525	$[1,12]$	4.885	$[1,11]$
5	6.514	$[5,20]$	1.882	$[1,8]$	0.357	$[0,5]$	0.053	$[0,1]$
6	1.263	$[1,7]$	0.090	$[0,1]$	0.010	$[0,1]$	0.000	$[0,0]$
7	0.035	$[0,1]$	0.000	$[0,0]$	0.001	$[0,0]$	0.000	$[0,0]$
8	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$

$d^\perp = 5$

r	$d=11$ mean	$d=11$ 99%	$d=12$ mean	$d=12$ 99%	$d=13$ mean	$d=13$ 99%	$d=14$ mean	$d=14$ 99%
2	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$
3	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$
4	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$
5	5.847	$[5,15]$	1.485	$[1,6]$	0.197	$[0,2]$	0.033	$[0,1]$
6	1.153	$[1,6]$	0.055	$[0,1]$	0.002	$[0,0]$	0.000	$[0,0]$
7	0.020	$[0,1]$	0.001	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$
8	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$	0.000	$[0,0]$

Fig. 13. some experimental data on $\mathrm{def}(\varphi_r)$ for random $[56, 16]_2$-codes