Harder-Narasimhan theory for linear codes (with an appendix on Riemann-Roch theory)

Hugues Randriambololona

HAL Id: hal-03022588

https://telecom-paris.hal.science/hal-03022588

Submitted on 21 Oct 2021

Harder-Narasimhan theory for linear codes
(with an appendix on Riemann-Roch theory)

Hugues Randriambololona

École nationale supérieure des télécommunications ("Telecom ParisTech")
Laboratoire traitement et communication de l'information (LTCI)
46 rue Barrault, 75634 Paris cedex 13, France

Abstract

In this text we develop some aspects of Harder-Narasimhan theory, slopes, semistability and canonical filtration, in the setting of combinatorial lattices. Of noticeable importance is the Harder-Narasimhan structure associated to a Galois connection between two lattices. It applies, in particular, to matroids.

We then specialize this to linear codes. This could be done from at least three different approaches: using the sphere-packing analogy, or the geometric view, or the Galois connection construction just introduced. A remarkable fact is that these all lead to the same notion of semistability and canonical filtration. Relations to previous propositions toward a classification of codes, and to Wei's generalized Hamming weight hierarchy, are also discussed.

Last, we study the two important questions of the preservation of semistability (or more generally the behaviour of slopes) under duality, and under tensor product. The former essentially follows from Wei's duality theorem for higher weights—and its matroid version—which we revisit in an appendix, developing analogues of the Riemann-Roch, Serre duality, Clifford, and gap and gonality sequence theorems. Likewise the latter is closely related to the bound on higher weights of a tensor product, conjectured by Wei and Yang, and proved by Schaathun in the geometric language, which we reformulate directly in terms of codes. From this material we then derive semistability of tensor product.

Contents

Introduction

A powerful guiding principle in arithmetic geometry is the analogy between number fields and function fields. This analogy already manifests itself when one considers "linear algebra" over these fields: it then translates into common properties shared by euclidean or hermitian lattices over rings of integers of number fields, and vector bundles over curves. The main motivation of the present work is to emphasize how some of these similarities extend to linear codes.

This will certainly be no surprise for anyone familiar with the subject. Indeed, many connections are known between codes and lattices on one side, and between codes and curves on the other. However, there might be a deeper explanation for this phenomenon.

Shortly said, a linear code is just a subspace of a finite dimensional L^1 space over a trivially valued field. Following the philosophy of Arakelov theory, putting a metric on a linear object can be seen as a replacement for an integral structure. From this point of view, one could then argue that coding theory is nothing but linear algebra over a certain combinatorial base object of dimension one, hence of arithmetic nature.

The corpus of results that we would like to borrow from number theory and algebraic geometry into coding theory consists of two parts: first of all, Harder-Narasimhan theory, and to a lesser extent, Riemann-Roch theory.

Harder and Narasimhan [19] first introduced slopes and the canonical filtration as a tool in the computation of the number of points (and more generally the étale cohomology) of certain moduli spaces over finite fields. The analogue for euclidean and hermitian lattices was then developed by Stuhler [25] and Grayson [18]. The theory subsequently saw multiple extensions, and propositions toward a more unified understanding were made, especially in a categorical framework [1][8].

Our aim is more modest. We will completely ignore functoriality issues, and focus on the more elementary combinatorial aspects. For this we first develop the theory in the context of combinatorial lattices[1]: what makes Harder-Narasimhan theory work is the existence of certain features, such as the so-called second isomorphism theorem, and also rank and degree functions satisfying Grayson's parallelogram constraint. It turns out these are well captured by a classical notion in combinatorial lattice theory, that of (semi)modularity. This allows us to present Harder-Narasimhan theory under minimalist hypotheses.[2] As an illustration, we then explain how a Galois connection between two lattices canonically produces a Harder-Narasimhan structure on them.

Specializing to codes, the most natural approach is perhaps to take inspiration from the analogy with euclidean lattices, where the degree function is $-\log$ of the covolume of a sublattice. We claim that the right analogue of the covolume is the support size of a subcode. This allows us to define slopes, the canonical filtration of a code, and a notion of semistability, using the degree function

$$\deg(C') = n - w(C')$$

for a subcode C' of a $[n,k]$-code C. However other approaches are possible, for instance, via algebraic geometry using the equivalence with configurations of points in a projective space, or via our combinatorial lattice construction using a certain natural Galois connection. A very satisfactory result is that all these approaches lead to the same theory.

Our definition of the degree function from the support size implies a close link with Wei's generalized weight hierarchy $d_i(C)$ from [29]: the canonical polygon of C is the upper convex envelope of the set of points

$$\{(i, n - d_i(C)) : 0 \le i \le k\}.$$

If this polygon has N sides, the code admits a canonically defined N-step filtration

$$0 = C_0 \subsetneq C_1 \subsetneq \cdots \subsetneq C_N = C.$$

However, for codes used in practical applications, this will essentially always be trivial ($N = 1$): these codes are stable, and our construction becomes void. Thus it is to be expected that true coding specialists will find the present work pointless. Probably, meaningful uses of the theory would appear only when considering questions involving the class of *all* codes, good and bad.

---

[1] In this work we will encounter two distinct notions of "lattices" which, quite unfortunately, English terminology does not distinguish. The first one, *réseau* in French, means a discrete subgroup in a continuous space; for us it will always be endowed with a euclidean or hermitian structure. The second, *treillis* in French, is a poset with meet and join; again we will often add an adjective, such as "combinatorial", in order to help make the distinction.

(Actually, French terminology cannot claim superiority there, since in turn, *réseau* is used for two distinct notions, one that translates in English as lattice, the other as network; and *treillis* also is used for two distinct notions, one that translates as lattice, the other as trellis!)

[2] Added in the revised version: this approach is so natural that, almost simultaneously with this work, it was also introduced in [11]—but then the focus shifts to other directions.

In most Harder-Narasimhan categories, semistability is preserved under duality. We show it is true for codes, and more generally, we explain how the slopes and canonical filtration of C and $C^\perp$ are related.

Less clear is the preservation of semistability under tensor product. It is known to be true for vector bundles over curves in characteristic zero, but false in positive characteristic, where counter-examples have been constructed [17]. For euclidean and hermitian lattices the question has been popularized by Bost and is still open, despite recent progress [6][16] that allow to settle low dimensional cases, or lattices admitting a large group of automorphisms. We show it holds for codes, where it is closely related to Schaathun's lower bound on higher weights of a tensor product. Schaathun's proof [23] is written in the geometric language, in terms of projective systems of points. We reformulate (and somehow simplify) the proof, directly in terms of codes, and then derive semistability of tensor product, with the hope that it could provide inspiration for new advances in the euclidean lattice situation.

The Riemann-Roch and Serre duality theorems certainly form the core of the theory of algebraic curves, on which almost all other results are based. In particular the Riemann-Roch theorem is closely related to the functional equation of the zeta function of a curve [46][48, §5.1]. Analogues for euclidean and hermitian lattices over integers of number fields have been developed at various levels of sophistication, based on the functional equation of the theta function [50], or using the language of Arakelov theory [49][41][47], or a combination of both [45][40][42][34][35] (references in chronological order).

Linear codes also admit zeta functions with a functional equation [37], and we can see the MacWilliams relation for the weight enumerator as an analogue of the functional equation of the theta function. This suggests that some sort of Riemann-Roch theory should exist also for codes. And indeed, in an appendix that can be read independently, we propose a definition of H^0 and H^1 spaces for codes that satisfy analogues of Serre duality and Riemann-Roch (see Theorems 48 and 49), and seem to fit well in this framework. Maybe these notions are not entirely new: previous occurrences can be hinted, for instance, in [38]. However our version is more precise and makes the analogy very explicit.

This Riemann-Roch theory can serve as a nice way to present the behaviour of slopes and canonical filtration under duality. It can also be used to reprove Wei's duality theorem for higher weights [29].

Closely related to linear codes is the notion of matroid. Whenever possible, we tried to explain how our theory extends in this framework. Matroids also admit slopes and a canonical filtration, hence a notion of semistability. They satisfy a form of Riemann-Roch theory, from which duality results for their slopes and canonical filtration can be derived, extending those for codes. We do not try to extend the notion of tensor product to matroids, although this certainly is an interesting question.

Satisfactorily, matroid theory recently gained interest among algebraic and arithmetic geometers (we refer to [43] for an introduction to this topic), especially thanks to its interplay with non-archimedean and tropical geometry.

Relevant in this context is the Riemann-Roch theorem for graphs of [33], and its many further generalizations. To any graph there is an associated matroid, however, it is unclear whether our Riemann-Roch theorem for matroids and this Riemann-Roch theorem for graphs could be related. Last, a very elaborate cohomology theory for matroids was recently introduced in [32]. Again, to which extent our work could possibly relate to it remains unclear.

We will borrow some notations commonly used in combinatorial theory. We let $[n] = \{1, \ldots, n\}$ be the standard set with n elements. Given a set S, we identify S^n with $S^{[n]}$. We also let 2^S stand for the set of all subsets of S, and $\binom{S}{n}$ for the set of its subsets of cardinality n.

Most of the content of this text was known to the author since at least half a dozen years. Impetus for writing it down and making it publicly available was provided by ANR-14-CE25-0015 project GARDIO and ANR-15-CE39-0013 project MANTA.

1. Harder-Narasimhan theory for combinatorial lattices

Basic definitions.

We recall that a combinatorial lattice $(L, \subseteq, \wedge, \vee)$ is a poset in which any two elements admit a meet and a join. Here the symbol $\subseteq$ stands for an abstract partial order relation, although in many examples it will be set inclusion, hence our notation. We will use the book [3] as our main reference on this topic.

A lattice L is said to be *of finite length* if there is a finite upper bound on the length of chains in L. Unless otherwise specified, this will always be the case in this work. Then L admits a minimal element, say 0_L, and also a maximal element, say 1_L. We define the rank $\mathrm{rk}(x)$ of an element $x \in L$ as the maximal length of a chain from 0_L to x. Note that our terminology here departs slightly from [3] and the standard literature, where our notion of rank is more commonly called height.

Given $x, y \in L$ with $y \subseteq x$, we will let x/y stand for the sublattice of L made of all z with $y \subseteq z \subseteq x$. Sometimes, by abuse of notation, it will also be tempting to let x stand for $x/0_L$; we might use this licence occasionally, although we will refrain from doing so too often (observe it makes the notations $y \subseteq x$ and $y \in x$ interchangeable). Likewise, we might occasionally write L/y for $1_L/y$.

In this work we will only consider *modular* lattices [3, §I.7]. There are various equivalent characterizations of this important notion. We will use the one from [3, §II.8, Th. 16]. First we recall that a function $f : L \longrightarrow \mathbb{R}$ is said *lower semimodular* if for any $x, y \in L$ we have

$$f(x) + f(y) \leq f(x \vee y) + f(x \wedge y). \tag{1}$$

Dually f is upper semimodular if $-f$ is lower semimodular. And f is *modular* if it is both lower and upper semimodular, that is, if for any $x, y \in L$ we have

$$f(x) + f(y) = f(x \vee y) + f(x \wedge y). \tag{2}$$

5

Then, a lattice L of finite length is *modular* if and only if it satisfies the following two conditions:

- the rank function $\mathrm{rk} : L \longrightarrow \mathbb{Z}$ is modular, and moreover

- (Jordan-Dedekind) all maximal chains between two $y \subseteq x$ in L have the same length, necessarily equal to $\mathrm{rk}(x) - \mathrm{rk}(y)$.

It is known that for any x, y in a modular lattice, we have a natural identification $(x \vee y)/y \simeq x/(x \wedge y)$ [3, §I.7, Th. 13].

Definition 1. A Harder-Narasimhan lattice is a modular lattice L of finite length equipped with a lower semimodular function $\deg : L \longrightarrow \mathbb{R}$.

Lemma 2. *Suppose $(L, \deg)$ is a Harder-Narasimhan lattice, and let L' be another modular lattice of finite length together with a morphism $L' \longrightarrow L$ (meaning that it respects meet and join). Then pulling back the degree function to L' makes it into a Harder-Narasimhan lattice.*

In particular, for any elements $y \subseteq x$ in L, the sublattice x/y is a Harder-Narasimhan lattice.

Proof. Clear. $\qquad\square$

To any $x \in L$ we associate a point p_x in the real plane, with coordinates $p_x = (\mathrm{rk}(x), \deg(x))$. Graphically, the modularity and semimodularity relations

$$
\begin{aligned}
\mathrm{rk}(x) + \mathrm{rk}(y) &= \mathrm{rk}(x \vee y) + \mathrm{rk}(x \wedge y) \\
\deg(x) + \deg(y) &\leq \deg(x \vee y) + \deg(x \wedge y)
\end{aligned}
\tag{3}
$$

translate into Grayson's parallelogram constraint [18, Fig. 1.14]: any three points among $p_x, p_y, p_{x \wedge y}, p_{x \vee y}$ determine a parallelogram, and then the fourth point lies vertically below (if it is p_x or p_y) or above (if it is $p_{x \wedge y}$ or $p_{x \vee y}$) the fourth vertex of this parallelogram.[3]
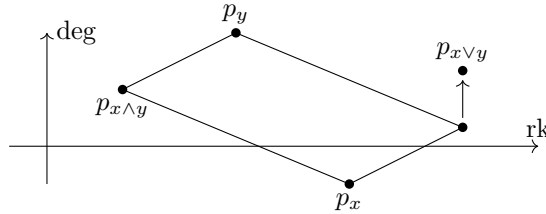
If L is nontrivial we define its slope as $\mu(L) = (\deg(1_L) - \deg(0_L)) / \mathrm{rk}(L)$ where by abuse of notation we set $\mathrm{rk}(L) = \mathrm{rk}(1_L)$. Accordingly, given $y \subsetneq x$ in

---

[3]Actually, in Grayson's original paper the constraint goes in the opposite direction. This is because his sign convention for the degree function makes it upper semimodular instead of lower semimodular.

L, the slope from y to x is

$$\mu(x/y) = \frac{\deg(x) - \deg(y)}{\mathrm{rk}(x) - \mathrm{rk}(y)} \tag{4}$$

that is, the slope of the line segment joining p_y to p_x. We also define the slope of $x \neq 0_L$ to be $\mu(x/0_L)$ and the co-slope of $x \neq 1_L$ to be $\mu(1_L/x)$.

Lemma 3. *Let $(L, \deg)$ be a Harder-Narasimhan lattice. Then the degree function* $\deg$ *is bounded from above.*

Proof. We proceed by induction on the length $n = \mathrm{rk}(L)$ of L. The result is obvious if $n = 0$ or 1, so we assume L has length $n \geq 2$ and make the following *Induction hypothesis*: on every Harder-Narasimhan lattice of length at most $n - 1$, the degree function is bounded from above.

By contradiction suppose $\deg$ is not bounded on L, and choose r maximal such that the set
$$E_r = \{\deg(x) : x \in L, \mathrm{rk}(x) = r\}$$
is unbounded (observe $r \leq n - 1$ since $E_n = \{\deg(1_L)\}$ is finite).

Now fix an $a \in L$ of rank $\mathrm{rk}(a) = 1$, and let $x \in L$ vary with $\mathrm{rk}(x) = r$ and $\deg(x)$ arbitrarily large. The sublattice L/a has length $n - 1$, so by our *Induction hypothesis* we will have $x \notin L/a$ as soon as $\deg(x)$ is large enough. This means $a \nsubseteq x$, and forces $a \wedge x = 0_L$ and

$$\mathrm{rk}(a \vee x) = r + 1.$$

But then, by semimodularity,

$$\deg(a \vee x) \geq \deg(x) + \deg(a) - \deg(0_L)$$

can be arbitrarily large when $\deg(x)$ is. This means precisely that E_{r+1} is unbounded, contradicting the maximality of r. $\qquad\square$

This boundedness allows us to define a concave, piecewise linear function

$$P_L : [0, \mathrm{rk}(L)] \longrightarrow \mathbb{R} \tag{5}$$

as the infimum of all linear functions whose graph lies above the set $\{p_x : x \in L\}$. The graph of P_L is then called the *canonical polygon* of L.

Let N be the number of sides of this polygon, and label its vertices $(i_\alpha, P_L(i_\alpha))$, for $0 \leq \alpha \leq N$, according to increasing rk-coordinate

$$0 = i_0 < i_1 < \cdots < i_N = \mathrm{rk}(L). \tag{6}$$

Note that by construction these i_α are integers.

Definition 4. The successive slopes of L are the slopes of its canonical polygon.

Actually, depending on the authors, there are two conflicting labeling schemes for these successive slopes. One first variant would be to define the i-th slope of L as $P_L(i) - P_L(i-1)$, for $1 \leq i \leq \mathrm{rk}(L)$. This gives a non-increasing sequence, with repetition allowed. The other variant, which is the one we will adopt, is to extract only the set of distinct values from this sequence. So, for $1 \leq \alpha \leq N$, we define the α-th slope of L as

$$\mu_\alpha(L) = P_L(i_\alpha) - P_L(i_\alpha - 1) = \frac{P_L(i_\alpha) - P_L(i_{\alpha-1})}{i_\alpha - i_{\alpha-1}}. \tag{7}$$

This gives a strictly decreasing sequence. We also set $\mu_{\max} = \mu_1$ and $\mu_{\min} = \mu_N$. By construction we then have

$$\mu_{\max}(L) \geq \mu(L) = \frac{1}{\mathrm{rk}(L)} \sum_{1 \leq \alpha \leq N} (i_\alpha - i_{\alpha-1})\mu_\alpha(L) \geq \mu_{\min}(L). \tag{8}$$

Many examples of Harder-Narasimhan lattices satisfy a Northcott-type property, which reads that for any real B, there are only finitely many $x \in L$ with $\deg(x) \geq B$. Thus, under this hypothesis, for any i, the supremum $\sup_{\mathrm{rk}(x)=i} \deg(x)$ is attained. In particular, for any α, there is an $x_\alpha \in L$ with $\mathrm{rk}(x_\alpha) = i_\alpha$ and $\deg(x_\alpha) = P_L(i_\alpha)$; that means p_{x_α} is the corresponding vertex of the canonical polygon. It turns out this last assertion holds *unconditionally*, as will be seen in Theorem 6 below.

Lemma 5. *Let $x, y \in L$ satisfy $\mathrm{rk}(y) = i_\beta \leq \mathrm{rk}(x) = i_\alpha$ but $y \nsubseteq x$. Suppose $\deg(x) \geq P_L(i_\alpha) - \varepsilon$ for some $\varepsilon > 0$. Then we have $\deg(y) \leq P_L(i_\beta) - (\mu_\beta(L) - \mu_{\alpha+1}(L)) + \varepsilon$.*

Proof. This is a consequence of the parallelogram constraint (3). Indeed, since $y \nsubseteq x$, we have $\mathrm{rk}(x \wedge y) < i_\beta$, so we can write $\mathrm{rk}(x \wedge y) = i_\beta - k$ with $k \geq 1$, and then $\mathrm{rk}(x \vee y) = i_\alpha + k$. By concavity of P_L and by definition of the slopes we deduce $\deg(x \wedge y) \leq P_L(i_\beta) - k\mu_\beta(L)$ and $\deg(x \vee y) \leq P_L(i_\alpha) + k\mu_{\alpha+1}(L)$. From semimodularity of the degree we then conclude $\deg(y) \leq \deg(x \wedge y) + \deg(x \vee y) - \deg(x) \leq P_L(i_\beta) - k(\mu_\beta(L) - \mu_{\alpha+1}(L)) + \varepsilon$. $\square$

Theorem 6 (compare [18, Th. 1.18]). *Let L be a Harder-Narasimhan lattice.*

(i) *For any α, there is an $x_\alpha \in L$ with $\mathrm{rk}(x_\alpha) = i_\alpha$ and $\deg(x_\alpha) = P_L(i_\alpha)$. Moreover this x_α is unique, and in fact any $y \neq x_\alpha$ with $\mathrm{rk}(y) = i_\alpha$ is subject to the gap condition*

$$\deg(y) \leq P_L(i_\alpha) - (\mu_\alpha(L) - \mu_{\alpha+1}(L)).$$

(ii) *These x_α form a chain, i.e. for $\beta \leq \alpha$ we have $x_\beta \subseteq x_\alpha$.*

Proof. The first assertion follows from Lemma 5 with $\beta = \alpha$ and $\varepsilon \to 0$. Likewise for the second assertion, if we set $x = x_\alpha$ and $y = x_\beta$ and take ε small enough, then from $x_\beta \nsubseteq x_\alpha$ we would get a contradiction in Lemma 5. $\square$

Definition 7. This chain

$$0_L = x_0 \subsetneq x_1 \subsetneq \cdots \subsetneq x_N = 1_L,$$

with $p_{x_\alpha} = (i_\alpha, P_L(i_\alpha))$, is called the *canonical filtration* of 1_L (or of L).

Definition 8. We say L is *semistable* if its canonical filtration is trivial, which means L has only one slope ($N = 1$), or equivalently, if any $x \neq 0_L, 1_L$ has slope $\mu(x/0_L) \leq \mu(L)$, or equivalently, co-slope $\mu(1_L/x) \geq \mu(L)$.

Moreover we say L is *stable* if any $x \neq 0_L, 1_L$ has slope $\mu(x/0_L) < \mu(L)$, or equivalently, co-slope $\mu(1_L/x) > \mu(L)$.

Proposition 9. *Let L be a Harder-Narasimhan lattice.*

(i) *Let $x \in L$, $x \neq 0_L, 1_L$, with $\mu_{\min}(x/0_L) \geq \mu_{\max}(1_L/x)$. Then the canonical polygon of L can be obtained by pasting together those of $x/0_L$ and $1_L/x$.*

(ii) *Let $x \in L$, $x \neq 0_L, 1_L$. Then x is part of the canonical filtration of L if and only if $\mu_{\min}(x/0_L) > \mu_{\max}(1_L/x)$.*

(iii) *A chain $0_L = x_0 \subsetneq x_1 \subsetneq \cdots \subsetneq x_N = 1_L$ is the canonical filtration of L if and only if all x_i/x_{i-1} are semistable with $\mu(x_{i+1}/x_i) > \mu(x_i/x_{i-1})$.*

Proof. Consequence of Theorem 6, as in [18, Cor. 1.29-1.31]. $\qquad\square$

All these constructions behave well under certain "affine" transformations:

Lemma 10. *Let $(L, \deg)$ be a Harder-Narasimhan lattice, with canonical polygon P_L and slopes $\mu_1 > \cdots > \mu_N$.*

(i) *Let L^{op} be the opposite lattice of L. Then $(L^{op}, \deg)$ is a Harder-Narasimhan lattice. Its canonical polygon is the image of P_L under the plane transformation $(\xi, \eta) \mapsto (\mathrm{rk}(L) - \xi, \eta)$. Its canonical filtration is the opposite of that of L, with slopes $-\mu_N > \cdots > -\mu_1$.*

(ii) *Let $a, b \in \mathbb{R}$ and $c \in \mathbb{R}_{>0}$ be constants. Then $(L, a + b\,\mathrm{rk} + c\,\deg)$ is a Harder-Narasimhan lattice. Its canonical polygon is the image of P_L under the plane transformation $(\xi, \eta) \mapsto (\xi, a + b\xi + c\eta)$. It has the same canonical filtration as $(L, \deg)$, with slopes $b + c\mu_1 > \cdots > b + c\mu_N$.*

As a consequence, as soon as one of these Harder-Narasimhan lattice is semistable (resp. stable), then all of them are.

Proof. Clear. $\qquad\square$

We will say $(L, \deg)$ is normalized if $\deg(0_L) = 0$. We will say it is co-normalized if $\deg(1_L) = 0$. Thanks to the second part of the Lemma, we see that it is always possible to modify the degree function in order to force one, or even both of these conditions, without changing the essential properties of the lattice.

9

Example 11. We recall that a matroid [31][21] is a pair $\mathcal{M} = (E, \mathcal{I})$ where E is a set, and $\mathcal{I} \subseteq 2^E$ a collection of subsets of E (the *independent* sets), such that:

- $\emptyset \in \mathcal{I}$;

- if $I \in \mathcal{I}$ and $I' \subseteq I$, then $I' \in \mathcal{I}$;

- if $I_1, I_2 \in \mathcal{I}$ and $\#I_1 < \#I_2$, then there is some $e \in I_2 \setminus I_1$ such that $I_1 \cup \{e\} \in \mathcal{I}$.

For any subset $J \subseteq E$ (not necessarily independent) we set

$$r(J) = \max\{\#I :\ I \in \mathcal{I},\ I \subseteq J\}. \tag{9}$$

It is easily seen [21, Lemma 1.3.1] that this function r is upper semimodular. As a consequence, if E is finite, the lattice L_E of all subsets of E is modular of finite length, and becomes a Harder-Narasimhan lattice thanks to the degree function

$$\deg(J) = k - r(J) \tag{10}$$

where k could be any arbitrary constant; we will set $k = r(E)$, which makes deg nonnegative and co-normalized.

We observe a quite unfortunate conflict between the well-established terminology of the domain and ours. Indeed, $r(J)$ is traditionally called the rank of J, while for us the rank of J in L_E is $\#J$. Worse, some authors in matroid theory call $\#J$ the degree of J! An explanation for this inversion of terms will come from Remark 21 below.

Example 12. Let E be a vector bundle, *i.e.* a locally free sheaf of finite rank, on a projective curve over a field. Given a subsheaf $F \subseteq E$, we let F^{sat} be the smallest subsheaf of E containing F such that E/F^{sat} is locally free. We say F is saturated if $F = F^{\mathrm{sat}}$. The saturated subsheaves of E form a modular lattice L_E of finite length, whose meet and join are given by $F \wedge F' = F \cap F'$ and $F \vee F' = (F + F')^{\mathrm{sat}}$. Then, the usual degree function for vector bundles is lower semimodular on L_E, so it makes it into a Harder-Narasimhan lattice. Its canonical filtration was first introduced by Harder and Narasimhan [19] as a tool in the computation of the number of points (and more generally the étale cohomology) of certain moduli spaces over finite fields.

Example 13. Let E be a euclidean lattice, *i.e.* a free $\mathbb{Z}$-module of finite rank, equipped with a positive definite scalar product. Given a submodule $F \subseteq E$, we let F^{sat} be the smallest submodule of E containing F such that E/F^{sat} is torsion-free. We say F is saturated if $F = F^{\mathrm{sat}}$. The saturated submodules of E form a modular lattice L_E of finite length, whose meet and join are given by $F \wedge F' = F \cap F'$ and $F \vee F' = (F + F')^{\mathrm{sat}}$. Then, the arithmetic degree function $\deg(F) = -\log \mathrm{covol}(F)$ is lower semimodular on L_E, so it makes it into a Harder-Narasimhan lattice. The analogy with Example 12 was first noticed by Stuhler [25] and used to revisit certain results in reduction theory. It was then

generalized by Grayson [18] in order to study the cohomology of arithmetic groups, by constructing manifolds with boundary on which the group naturally acts, alternative to those of [5].

Remark 14. In both Examples 12 and 13 the rank and degree functions on L_E naturally extend to the lattice L'_E of all (possibly non-saturated) submodules of E, and they still satisfy the parallelogram constraint (3). As a consequence, although L'_E is not of finite length so our Definition 1 does not apply, slopes and the canonical filtration are still well defined for L'_E, and they coincide with those of L_E. In fact the map $F \mapsto F^{\text{sat}}$ from L'_E onto L_E is a morphism of lattices, and it is interesting to note that the degree function becomes modular when restricted to its fibers. Continuing in this spirit it is possible to generalize our theory to lattices that are not of finite length. Moreover, adding suitable topological conditions, it is even possible to allow the degree function to be $\mathbb{R}$-valued instead of $\mathbb{Z}$-valued. We will not elaborate on these ideas since they are not needed in the sequel.

Remark 15. In most Harder-Narasimhan categories (in the sense of [8]), the lattice of subobjects of an object is a Harder-Narasimhan lattice in our sense. However, this fails for [8, Ex. 2], the category of vector spaces with two hermitian norms. Actually, the degree function in this category does not satisfy our semimodularity condition, which [8] omitted in its definitions. This omission leads to certain problems, for instance, the proof of [8, Prop. 4.5] is incorrect (the equality in [8, p. 195, l. 10] holds only if the exact sequence lies in $\mathcal{E}_A$, which is not assumed). A corrected version had been planned [9].

Still, vector spaces with two norms enjoy certain properties very close to ours, and it would be intesting to investigate whether a weaker version of Harder-Narasimhan theory could be developed in order to reflect this.

Modular lattices under a Galois connection.

We recall [3, §V.8] that a *Galois connection* between two lattices L and M is a pair of *order-reversing*[4] maps $(.)^\circ : L \to M$ and $(.)^\circ : M \to L$ such that any x in L or M satisfies

$$x \subseteq x^{\circ\circ}. \tag{11}$$

It then follows that $x^\circ = x^{\circ\circ\circ}$, hence the map $x \mapsto \overline{x} = x^{\circ\circ}$ is a *closure operator* on L and on M, *i.e.* it satisfies $x \subseteq \overline{x}$ and $\overline{x} = \overline{\overline{x}}$. We say x is *closed* if $x = \overline{x}$, which happens precisely when x is of the form $x = a^\circ$ for some a (*e.g.* $a = x^\circ$).

It is also easily shown that for any $l \in L$ and $m \in M$ we have

$$l \subseteq m^\circ \quad \Longleftrightarrow \quad m \subseteq l^\circ, \tag{12}$$

and in fact one could show conversely that this property entirely characterizes Galois connections, *i.e.* that (12) implies the conditions in the definition.

---

[4] So this is sometimes called an "antitone" Galois connection. There is the alternative notion of a "monotone" Galois connection, in which the maps are order-preserving, leading to an essentially equivalent theory.

Proposition 16. *Let L, M be given with such a Galois connection, and take $x, y \in L$ or $x, y \in M$. Then we have*

$$x^\circ \vee y^\circ \subseteq (x \wedge y)^\circ \tag{13}$$

and

$$x^\circ \wedge y^\circ = (x \vee y)^\circ. \tag{14}$$

Proof. Since $(.)^\circ$ is order-reversing we get $x^\circ \subseteq (x \wedge y)^\circ$ and $y^\circ \subseteq (x \wedge y)^\circ$, hence (13). Likewise we get $x^\circ \supseteq (x \vee y)^\circ$ and $y^\circ \supseteq (x \vee y)^\circ$, hence

$$x^\circ \wedge y^\circ \supseteq (x \vee y)^\circ \tag{15}$$

which is half of (14).

On the other hand by (11) and (13) we have

$$x \vee y \ \subseteq \ x^{\circ\circ} \vee y^{\circ\circ} \ \subseteq \ (x^\circ \wedge y^\circ)^\circ. \tag{16}$$

Applying (12) we deduce $x^\circ \wedge y^\circ \subseteq (x \vee y)^\circ$ and conclude. $\qquad\square$

As a consequence we get that the subset L^{cl} of closed elements in L is a lattice with meet $x \wedge y$ and join $\overline{x \vee y}$, so the natural map $\overline{(.)} : L \to L^{\mathrm{cl}}$ becomes a morphism of lattices (although we will make no use of it, it is amusing to note the analogy with the map $(.)^{\mathrm{sat}} : L'_E \to L_E$ of Remark 14). Moreover, $(.)^\circ$ then becomes an anti-isomorphism between the lattices L^{cl} and M^{cl}.

Theorem 17. *Let L, M be two modular lattices of finite length. Let rk_L be the natural rank function of L, and rk_M that of M. Suppose given a Galois connection $(.)^\circ$ between L and M. Then the degree functions*

$$\deg_L(l) = \mathrm{rk}_M(l^\circ)$$

and $\deg_M(m) = \mathrm{rk}_L(m^\circ)$, for $l \in L$ and $m \in M$, make L and M into Harder-Narasimhan lattices.

Proof. The roles of L and M being symmetric, it suffices to show that $\deg_L$ is lower semimodular. And indeed, for $x, y \in L$ we find

$$\begin{aligned}
\deg_L(x) + \deg_L(y) &= \mathrm{rk}_M(x^\circ) + \mathrm{rk}_M(y^\circ) \\
&= \mathrm{rk}_M(x^\circ \vee y^\circ) + \mathrm{rk}_M(x^\circ \wedge y^\circ) \\
&\leq \mathrm{rk}_M((x \wedge y)^\circ) + \mathrm{rk}_M((x \vee y)^\circ) \\
&= \deg_L(x \wedge y) + \deg_L(x \vee y)
\end{aligned} \tag{17}$$

where we used that rk_M is modular and the intermediate inequality comes from Proposition 16. $\qquad\square$

Because of the identity $x^{\circ\circ\circ} = x^\circ$, we observe that all $l \in L$ satisfy

$$\deg_L(\bar{l}) = \deg_L(l) \tag{18}$$

12

and likewise $\deg_M(\overline{m}) = \deg_M(m)$ for all $m \in M$.

It is easily seen (say from (12)) that we have $0_L^\circ = 1_M$ and $0_M^\circ = 1_L$, hence 1_L and 1_M are closed. From this we also find $1_M^\circ = \overline{0}_L$ and $1_L^\circ = \overline{0}_M$, which motivates the following:

Definition 18. We say that L is separated (with respect to the given Galois connection) if $1_M^\circ = 0_L$, or equivalently, if $0_L = \overline{0}_L$ is closed. And we say the Galois connection is separated if both L and M are.

Any Galois connection between L and M induces (by restriction) a separated Galois connection between $L/\overline{0}_L$ and $M/\overline{0}_M$. So by Theorem 17 it defines a degree function on $L/\overline{0}_L$ (resp. on $M/\overline{0}_M$), which is just a translate of the restriction of the degree function of L (resp. of M). Moreover, an element x in $L/\overline{0}_L$ (resp. in $M/\overline{0}_M$) is closed if and only if it is closed in L (resp. in M).

Lemma 19. *We have $\mu_{\max}(L) \le 0$ and $\deg_M(1_M) \ge 0$. Moreover, the following assertions are equivalent:*

- $\mu_{\max}(L) = 0$

- $\deg_M(1_M) > 0$

- *L is not separated.*

If any of these assertions holds, the first nonzero element of the canonical filtration of L is $\overline{0}_L$, with slope 0, and rank $\mathrm{rk}_L(\overline{0}_L) = \deg_M(1_M)$. And then the subsequent elements of the canonical filtration of L, and its subsequent slopes, are those of $L/\overline{0}_L$ (relative to the induced separated Galois connection).

Proof. Let $0_L = x_0 \subsetneqq x_1 \subsetneqq \cdots \subsetneqq x_N = 1_L$ be the canonical filtration of L. Then $x_1^\circ \subseteq x_0^\circ$, so $\deg_L(x_1) = \mathrm{rk}_L(x_1^\circ) \le \mathrm{rk}_L(x_0^\circ) = \deg_L(x_0)$, hence $\mu_1 \le 0$.

Moreover if $\mu_1 = 0$, which means $\deg_L(x_1) = \deg_L(x_0)$, then necessarily $x_1^\circ = x_0^\circ = 1_M$, hence $1_M^\circ \supseteq x_1$, and $\deg_M(1_M) = \mathrm{rk}_L(1_M^\circ) \ge \mathrm{rk}_L(x_1) > 0$. In turn if $\deg_M(1_M) = \mathrm{rk}_L(1_M^\circ) > 0$, then $\overline{0}_L = 1_M^\circ \supsetneqq 0_L$, so L is not separated. Last, if L is not separated, then $\mu_1 \ge \mu(\overline{0}_L/0_L) = 0$, so $\mu_1 = 0$.

This shows the equivalence of the three conditions.

Now if any of them holds, say the first one, then x_1 is the largest element of L with $x_1^\circ = 1_M$, which means $x_1 = 1_M^\circ = \overline{0}_L$. And then the relation between the canonical filtration of L and that of $L/\overline{0}_L$ follows from the first point in Proposition 9. $\qquad\square$

Proposition 20. *Under the hypotheses of Theorem 17, the canonical polygons of L and M are image of each other under the reflection across the diagonal in the first quadrant.*

In particular, if the Galois connection is separated, these canonical polygons are defined, respectively, by functions

$$P_{L,M} : [0, \mathrm{rk}(L)] \to [0, \mathrm{rk}(M)]$$

and
$$P_{M,L} : [0, \mathrm{rk}(M)] \to [0, \mathrm{rk}(L)],$$
that are inverse of each other.

More precisely, suppose that the Galois connection is separated, and let L have canonical filtration
$$0_L = x_0 \subsetneqq x_1 \subsetneqq \cdots \subsetneqq x_N = 1_L$$
with slopes
$$\mu_1 > \cdots > \mu_N.$$
Then the x_α are closed, the μ_α are negative, and M has canonical filtration
$$0_M = x_N^\circ \subsetneqq x_{N-1}^\circ \subsetneqq \cdots \subsetneqq x_0^\circ = 1_M$$
with slopes
$$\mu_N^{-1} > \cdots > \mu_1^{-1}.$$
In particular, L is semistable if and only if M is.

Proof (abridged). Direct consequence of the symmetry between $(L, \deg_L)$ and $(M, \deg_M)$ in Theorem 17. $\qquad\square$

Proof (detailed). Thanks to Lemma 19, the first assertion reduces to the second. So we suppose the Galois connection is separated (and in particular $0_L = x_0$ is closed). By Lemma 19 again, we deduce $\mu_1 < 0$, hence all $\mu_\alpha < 0$.

For any real $\nu > 0$ consider the function $\Phi_{L,\nu}$ on L defined by
$$\Phi_{L,\nu}(l) = \nu\,\mathrm{rk}_L(l) + \deg_L(l), \tag{19}$$
which we might also view as the linear form $(\xi, \eta) \mapsto \nu\xi + \eta$ on the real plane, evaluated at the point $p_l = (\mathrm{rk}_L(l), \deg_L(l))$.

Observe the following *Fact*: if l is not closed, then $\mathrm{rk}_L(\bar{l}) > \mathrm{rk}_L(l)$, while $\deg_L(\bar{l}) = \deg_L(l)$ by (18), hence $\Phi_{L,\nu}(\bar{l}) > \Phi_{L,\nu}(l)$.

That μ_α is the α-th slope of the canonical polygon of L means that there is a certain constant c_α such that all $l \in L$ satisfy
$$\Phi_{L,-\mu_\alpha}(l) \le c_\alpha \tag{20}$$
and that equality is effectively attained for at least two l, the smallest of which being $x_{\alpha-1}$, and the largest x_α.

Since $\Phi_{L,-\mu_\alpha}(x_\alpha) = c_\alpha$ but $\Phi_{L,-\mu_\alpha}(\bar{x}_\alpha) > c_\alpha$ is forbidden, then from the *Fact* just above we deduce that $x_\alpha = \bar{x}_\alpha$ is closed.

Last take $m \in M$, and write (20) in the form
$$(-\mu_\alpha)\,\mathrm{rk}_L(l) + \mathrm{rk}_M(l^\circ) \le c_\alpha. \tag{21}$$
Setting $l = m^\circ$ we then find
$$\mathrm{rk}_L(m^\circ) + (-\mu_\alpha^{-1})\,\mathrm{rk}_M(m^{\circ\circ}) \le (-\mu_\alpha^{-1})c_\alpha, \tag{22}$$

and since $\mathrm{rk}_M(m) \leq \mathrm{rk}_M(m^{\circ\circ})$ we deduce

$$\Phi_{M,-\mu_\alpha^{-1}}(m) \leq c'_\alpha \qquad (23)$$

with $c'_\alpha = (-\mu_\alpha^{-1})c_\alpha$. Moreover a necessary and sufficient condition for equality in (23) is that $l = m^\circ$ reaches equality in (20) and $m = m^{\circ\circ}$ is closed. Thus we see that equality is attained for at least two m, the smallest of which being x_α°, and the largest $x_{\alpha-1}^\circ$. This means precisely that μ_α^{-1} is a slope of M, and x_α° and $x_{\alpha-1}^\circ$ the corresponding successive elements of its canonical filtration. $\qquad \square$

Remark 21. In the proof of Theorem 17, we observe that (17) still works if rk_M is only assumed lower semimodular, instead of modular. We deduce:

Let $(.)^\circ$ be a Galois connection between a modular lattice L of finite length and a lower semimodular lattice M. Then the degree function

$$\deg_L(l) = \mathrm{rk}_M(l^\circ) \qquad (24)$$

makes L into a Harder-Narasimhan lattice.

Now let E be a finite matroid, and let $L_{E,\mathrm{fl}}$ be its lattice of flats [21, §1.7]. It is known that $L_{E,\mathrm{fl}}$ is upper semimodular, so the opposite lattice $L_{E,\mathrm{fl}}^{\mathrm{opp}}$ is lower semimodular. Let then L_E be the (modular) lattice of all subsets of E. We define a Galois connection between L_E and $L_{E,\mathrm{fl}}^{\mathrm{opp}}$ as follows: in one direction, we map any $X \in L_E$ to its closure (or span) in $L_{E,\mathrm{fl}}^{\mathrm{opp}}$; in the other direction, we just use the forgetful map, *i.e.* the natural inclusion $L_{E,\mathrm{fl}}^{\mathrm{opp}} \hookrightarrow L_E$. Observe these maps are order reversing, by definition of the opposite lattice.

It is then easily seen that, under this Galois connection, the degree function on L_E given by (24) coincides with (10) in Example 11.

2. Linear codes

From now on we will use the following notations:

- $n \geq 1$ is an integer;

- $[n] = \{1, \ldots, n\}$ is the standard set with n elements

- $\mathbb{F}$ is a field;

- $|.|$ is the trivial absolute value on $\mathbb{F}$, so $|0| = 0$ and $|x| = 1$ for $x \in \mathbb{F}^\times$;

- $\|.\|$ is the corresponding L^1 norm on the standard $\mathbb{F}$-vector space $\mathbb{F}^n$, also called the Hamming norm.

  It follows that for $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}^n$ we have

$$\|\mathbf{x}\| = |x_1| + \cdots + |x_n| = \# \mathrm{Supp}(\mathbf{x}) \qquad (25)$$

where $\mathrm{Supp}(\mathbf{x}) = \{i \in [n] : x_i \neq 0\}$ is the support of $\mathbf{x}$.

Now we recall that a (linear) code of length n and dimension k over $\mathbb{F}$, sometimes called a $[n, k]$-code, is a k-dimensional vector subspace

$$C \subseteq \mathbb{F}^n \tag{26}$$

equipped with the induced norm. Beside its length and dimension, another important parameter of a code is its minimal distance

$$\mathrm{d}_{\min}(C) = \lambda_1(C) = \min_{\mathbf{c} \in C \setminus \{\mathbf{0}\}} \|\mathbf{c}\|. \tag{27}$$

A $[n, k]$-code with minimum distance d is also called a $[n, k, d]$-code.

The definition of a code we just gave was oriented in a way to stress some similarity with certain branches of arithmetic geometry (*e.g.* Arakelov, Berkovich, or tropical geometry), where metrics are introduced in order to reflect a certain integral structure in the objects considered. However, this analogy is certainly not perfect. For instance, arithmeticians tend to favor metrics that satisfy the ultrametric inequality. We observe that in our case, although the trivial absolute value $|.|$ is ultrametric, the Hamming norm $\|.\|$, as a L^1 norm, is *not*.

First approach: the sphere-packing analogy.

Many deep connections exist between the theory of codes and that of euclidean lattices. Classical references on this topic are [10][14]. Perhaps the similarity between these objects becomes the most striking when both are viewed as defining regular packings: of Hamming spheres in $\mathbb{F}^n$ for codes, and of euclidean spheres in $\mathbb{R}^n$ for lattices. In both cases, a central problem is then that of the determination of the densest such packings. However, many other notions and problems, either purely mathematical or more algorithmic, can be formulated in a very similar way in both contexts, and are equally interesting. Let us just mention Minkowski's successive minima, which generalize the notion of the minimum distance of a lattice, and whose analogues, the successive minima of our $[n, k]$-code C, can be defined as

$$\lambda_i(C) = \min\{t > 0 : \dim_{\mathbb{F}}\langle C \cap \mathbf{B}_{\|.\|}(\mathbf{0}, t)\rangle \geq i\} \tag{28}$$

for $1 \leq i \leq k$. On the other hand, as discussed in [4][6][7], slopes of euclidean lattices are known to be closely related to successive minima, while enjoying better functorial properties. Our aim here will be to find the analogue of this theory for codes. That is, we want to define a suitable degree function that makes the lattice L_C of linear subspaces of C into a Harder-Narasimhan lattice, in a way as close as possible to Example 13.

In Example 13, the degree of $F \subseteq E$ is an elementary function of its covolume $\mathrm{covol}(F)$. When F has rank 1, this covolume is just the norm of a generating vector. Now for a subcode $C' \subseteq C$ of dimension 1, all generating vectors have the same norm, which is also the cardinality of their common support. This suggests more generally that the analogue of the covolume for an arbitrary subcode $C' \subseteq C$ should be the cardinality of its support

$$\mathrm{Supp}(C') = \bigcup_{\mathbf{c} \in C'} \mathrm{Supp}(c) = \{i \in [n] : \exists \mathbf{c} = (c_1, \ldots, c_n) \in C', \, c_i \neq 0\}. \tag{29}$$

And then the degree should be an elementary function of this support size.

Definition 22. Let $C \subseteq \mathbb{F}^n$ be a $[n,k]$-code. We define the degree of a linear subcode $C' \subseteq C$ by the formula

$$\deg(C') = n - w(C') \tag{30}$$

where $w(C') = \# \operatorname{Supp}(C')$ is its support size.

In fact, since degree functions differing only by an additive constant define the same slopes (Lemma 10), we could equally well have used $-w(C')$ in Definition 22 instead of $n - w(C')$. Still, for reasons that will appear later, we will keep this choice, even if a peculiar consequence is that the zero subcode then has degree $\deg(0) = n$.

Proposition 23. *This degree function* $\deg : L_C \longrightarrow \{0, \ldots, n\}$ *is lower semimodular, so it makes* L_C *into a Harder-Narasimhan lattice.*

Proof. Observe that for linear subcodes $C', C'' \subseteq C$ we have

$$\begin{aligned} \operatorname{Supp}(C' + C'') &= \operatorname{Supp}(C') \cup \operatorname{Supp}(C'') \\ \operatorname{Supp}(C' \cap C'') &\subseteq \operatorname{Supp}(C') \cap \operatorname{Supp}(C''). \end{aligned} \tag{31}$$

It follows that $C' \mapsto w(C')$ is upper semimodular, and we conclude. $\square$

We define the *effective rate* of a nonzero subcode $C' \subseteq C$ as

$$\mathrm{R}(C') = \frac{\dim_{\mathbb{F}}(C')}{w(C')}. \tag{32}$$

Observe that if C itself has full support, *i.e.* if $\operatorname{Supp}(C) = [n]$, then $\mathrm{R}(C) = k/n$ is its rate in the usual sense. In fact coordinates outside $\operatorname{Supp}(C)$ play no role, so we can always reduce to this case.

Proposition 24. *The slope of a nonzero* $C' \subseteq C$ *is*

$$\mu(C'/0) = -\mathrm{R}(C')^{-1}. \tag{33}$$

Consequently, C is semistable (resp. stable) iff for all $0 \subsetneq C' \subsetneq C$ we have

$$\mathrm{R}(C') \leq \mathrm{R}(C) \quad (resp. \ \mathrm{R}(C') < \mathrm{R}(C)). \tag{34}$$

Proof. Direct from the definitions. $\square$

Sometimes it is useful to reformulate (34) as follows: C is semistable iff all C' satisfy

$$w(C') \geq \frac{\dim(C')}{R(C)}, \tag{35}$$

and similarly with $>$ for stability. In particular, the minimum distance of a stable code satisfies the (admittedly unimpressive) lower bound

$$\mathrm{d}_{\min}(C) > \frac{1}{R(C)}. \tag{36}$$

Remark 25. In Example 13, take $F \subseteq E$ and set $l = \mathrm{rk}(F)$. Then we have $\mathrm{covol}(F) = \|v_1 \wedge \cdots \wedge v_l\|$ where $v_1, \ldots, v_l$ are generators of F and $\|.\|$ is the l-th alternate power of the norm of E. Back to codes, we have a natural identification $\bigwedge^l \mathbb{F}^n = \mathbb{F}^{\binom{n}{l}}$, and we can define the l-th alternate power of the Hamming norm of $\mathbb{F}^n$ as the Hamming norm of $\mathbb{F}^{\binom{n}{l}}$. So given $C' \subseteq C \subseteq \mathbb{F}^n$ of dimension $\dim(C') = l$, we get a line $\bigwedge^l C' \subseteq \mathbb{F}^{\binom{n}{l}}$, and the norm of a generator of this line would be another convincing analogue of the notion of covolume. In fact, this norm is easily seen to be the number of *information sets* of C', so it is at most $\binom{w(C')}{l}$. However, inequality could be strict. This raises two natural questions: can one use this construction to define another semimodular degree function, hence another Harder-Narasimhan structure on L_C? if so, how does it compare with the one deduced from Definition 22?

Second approach: the geometric view.

Roughly speaking, the geometric view on coding theory, developed by the Russian school, aims at seeing any code as an evaluation code. A standard reference on the topic is [27].

Let $C \subseteq \mathbb{F}^n$ be a $[n, k]$-code. We can view C as an abstract k-dimensional vector space equipped with n linear forms $\pi_1, \ldots, \pi_n$, where $\pi_i : C \to \mathbb{F}$ is the i-th coordinate projection. It is easily seen that $\pi_1, \ldots, \pi_n$ span the dual vector space $C^\vee$. Now, to make things simpler, we shall assume that C has dual distance at least 3, which means that these π_i are nonzero and pairwise nonproportional. As a consequence they define n distinct points $\overline{\pi}_1, \ldots, \overline{\pi}_n$ in the projective space $\mathbb{P}(C) = \mathrm{Proj}\, S^. C \simeq \mathbb{P}^{k-1}$ that parameterizes hyperplanes in C (or equivalently, lines in $C^\vee$). One can then show that the set of points

$$\Pi = \{\overline{\pi}_1, \ldots, \overline{\pi}_n\} \subseteq \mathbb{P}(C) \tag{37}$$

uniquely determines C up to linear code equivalence, *i.e.* up to the natural action of $\mathfrak{S}_n \ltimes (\mathbb{F}^\times)^n$, the group of linear isometries of $\mathbb{F}^n$. This might be thought as a reformulation of the celebrated MacWilliams extension theorem, a proof of which along these lines can be found in [2, Prop. 3.1].

In case C only has dual distance 2 (*i.e.* C has full support, so the π_i still are nonzero, but some of them can be proportional), then things work the same provided we consider Π as a multiset, counting the now possibly nondistinct $\overline{\pi}_i$ according to their multiplicity.

Finite configurations of points in a projective space can be classified thanks to geometric invariant theory (GIT), which provides in particular its own notion of (semi)stability. Recall (see *e.g.* [20, Prop. 3.4], [13, Ch. II, Th. 1], or [12, Th. 11.2] with all $k_i = 1$):

The configuration of points $\Pi \subseteq \mathbb{P}(C)$ is semistable (resp. stable) if and only if for all linear subspaces $\emptyset \neq V \subsetneq \mathbb{P}(C)$ we have

$$\frac{\#(\Pi \cap V)}{\dim(V) + 1} \leq \frac{n}{k} \qquad (\text{resp. } <). \tag{38}$$

This could be extended in order to fit into our framework:

Proposition 26. *Let $L_{\mathbb{P}(C)}$ be the lattice of all linear subspaces $V \subseteq \mathbb{P}(C)$, including $V = \emptyset$ considered as the unique linear subspace of dimension -1. Then:*

1. *This lattice $L_{\mathbb{P}(C)}$ is modular, with rank function $\mathrm{rk}(V) = \dim(V) + 1$.*

2. *The degree function $\deg_\Pi(V) = \#(\Pi \cap V)$ is lower semimodular, hence makes $L_{\mathbb{P}(C)}$ into a Harder-Narasimhan lattice.*

3. *Then $(L_{\mathbb{P}(C)}, \deg_\Pi)$ is semistable (resp. stable) in our sense, if and only if $\Pi \subseteq \mathbb{P}(C)$ is semistable (resp. stable) in the sense of GIT (38).*

Proof. Routine verification. $\square$

We observe that, in turn, this construction also provides a Harder-Narasimhan structure on the lattice L_C of linear subcodes of C. Indeed, since we defined $\mathbb{P}(C)$ as the projective space of hyperplanes in C, there is a natural identification

$$L_{\mathbb{P}(C)} = (L_C)^{\mathrm{opp}}. \tag{39}$$

We then have only to apply Lemma 10.

Third approach: the cosupport Galois connection.

Let $C \subseteq \mathbb{F}^n$ be a $[n,k]$-code. We construct a Galois connection between the lattice L_C of subcodes of C and the lattice $L_{[n]}$ of subsets of $[n]$, as follows.

Definition 27. Given a subcode $C' \subseteq C$ we set

$$(C')^\circ = \mathrm{Cosupp}(C') = [n] \setminus \mathrm{Supp}(C') \tag{40}$$

the cosupport of C', *i.e.* the set of coordinates on which C' is identically 0.

Given a subset $J \subseteq [n]$ we set

$$J^\circ = C_{[n] \setminus J} = C \cap \mathbb{F}^{[n] \setminus J} \tag{41}$$

the subcode made of all the codewords of support disjoint from J, *i.e.* the largest subcode vanishing identically over J.

It is easily seen that $(.)^\circ : L_C \to L_{[n]}$ and $(.)^\circ : L_{[n]} \to L_C$ indeed define a Galois connection, which we will call the *cosupport Galois connection*.

From this we get a Harder-Narasimhan structure on L_C (and also on $L_{[n]}$) thanks to Theorem 17, on which Proposition 20 applies. Separation is treated by the following:

Lemma 28. *The lattice L_C is always separated under the cosupport Galois connection. On the other hand, the lattice $L_{[n]}$, hence also the cosupport Galois connection itself, is separated if and only if C has full support.*

Proof. The zero subcode satisfies $0^\circ = [n]$ hence $\overline{0} = [n]^\circ = 0$. On the other hand we have $\emptyset^\circ = C$ hence $\overline{\emptyset} = [n] \setminus \mathrm{Supp}(C)$. $\square$

19

As follows from (41), the Harder-Narasimhan structure just constructed on $L_{[n]}$ is given by the degree function

$$\deg(J) = \dim(C_{[n]\setminus J}).\tag{42}$$

Actually this can be related to another classical construction. We can view the inclusion $C \subseteq \mathbb{F}^n$ as a length 1 filtration on the vector space $\mathbb{F}^n$, from which we get (see *e.g.* [8, Ex. 1], or [15][26] for the original works) a degree function $\deg(V) = \dim(C \cap V)$ for V in the lattice $L_{\mathbb{F}^n}$ of all vector subspaces of $\mathbb{F}^n$. Now mapping $J \subseteq [n]$ to $\mathbb{F}^J \subseteq \mathbb{F}^n$ embeds $L_{[n]}$ as a sublattice of $L_{\mathbb{F}^n}$, so this degree function pulls back by Lemma 2. Last the involution $J \mapsto [n] \setminus J$ identifies $L_{[n]}$ and $(L_{[n]})^{\mathrm{opp}}$; applying Lemma 10 we retrieve (42).

We mention yet another interpretation, in terms of matroids: if $[n]$ is viewed as the index set of the columns of a given generating matrix G of C, then (42) coincides with the degree function (10) of the corresponding matroid. Indeed, the row-span of the submatrix G_J of columns of G indexed by J is $\pi_J(C)$, where $\pi_J : \mathbb{F}^n \to \mathbb{F}^J$ is the natural projection, so $r(J) = \mathrm{rk}(G_J) = \dim \pi_J(C)$, and

$$k - r(J) = \dim \ker(\pi_J|_C) = \dim(C_{[n]\setminus J})\tag{43}$$

as claimed.

Discussion.

We have just introduced three Harder-Narasimhan structures on the lattice L_C of linear subcodes of C:

- one given by Definition 22

- one deduced from Proposition 26, through the natural identification $L_C = (L_{\mathbb{P}(C)})^{\mathrm{opp}}$ and Lemma 10

- one deduced from the cosupport Galois connection of Definition 27, through Theorem 17.

Proposition 29. *These three Harder-Narasimhan structures on L_C coincide.*

Proof. Keep all the notations introduced before. It is well known (see *e.g.* the proof of [28, Th. 2.1]) that if $V \subseteq \mathbb{P}(C)$ is a l-codimensional linear subspace, corresponding to a l-dimensional subcode $C' \subseteq C$, then $w(C') = n - \#(\Pi \cap V)$, or
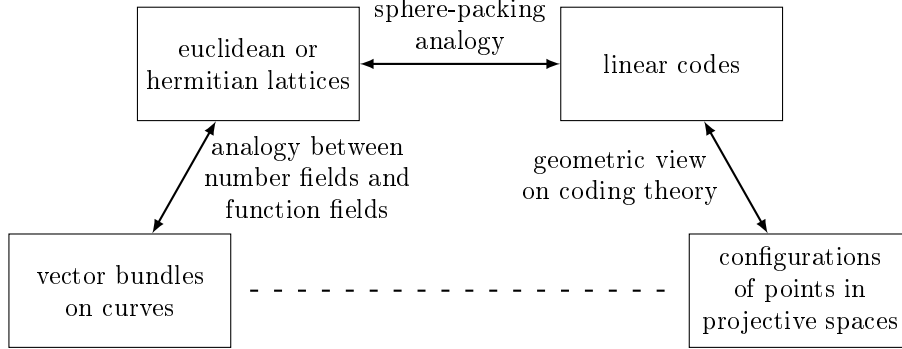
$$\#(\Pi \cap V) = n - w(C').\tag{44}$$

This gives equality of the first and second Harder-Narasimhan structures.

On the other hand we have $(C')^\circ = [n] \setminus \mathrm{Supp}(C')$ hence

$$\mathrm{rk}_{L_{[n]}}((C')^\circ) = \#((C')^\circ) = n - w(C'),\tag{45}$$

which gives equality of the first and the third. $\qquad\square$

Relationships between the various mathematical objects encountered in this work can be summarized by the following diagram:

The two extremal objects in this diagram belong to the realm of classical algebraic geometry, and can be classified using GIT. It is quite remarkable that the associated Harder-Narasimhan structures, and in particular the notions of slopes, canonical filtration, and semistability, are compatible with this chain of analogies.

Remark 30 (thanks to a suggestion of Bost). In the discussion following (42) we saw how the degree function on the Galois dual lattice $L_{[n]}$ could be deduced from the formalism of (multi-)filtered vector spaces of Faltings-Wüstholz and Totaro, applied to the length 1 filtration $C \subseteq \mathbb{F}^n$. It turns out this theory can also be applied directly to the lattice L_C: consider the collection of length 1 filtrations $H_i \subseteq C$, for $1 \leq i \leq n$, where $H_i = \ker \pi_i|_C$ is the i-th coordinate hyperplane. This makes C into a multi-filtered vector space, with associated degree function

$$\deg'(V) = \sum_{1 \leq i \leq n} \dim(V \cap H_i)$$

for $V \subseteq C$. However we have $\dim(V \cap H_i) = \dim(V)$ if $V \subseteq H_i$, i.e. if $i \notin \mathrm{Supp}(V)$, and $\dim(V \cap H_i) = \dim(V) - 1$ else. It follows

$$\deg'(V) = n \dim(V) - w(V) = \deg(V) + n \dim(V) - n,$$

so the two degree functions deg and deg$'$ are equivalent up to some affine transformation. In particular, by Lemma 10, they define the same canonical filtration on C.

Moreover, to any multi-filtered vector space (at least in characteristic zero), Faltings-Wüstholz associate a certain vector bundle on a curve, whose stalks are determined by the filtrations, in such a way that this construction preserves semistability [15, proof of Th. 4.1]. Specializing to the case where the filtrations are of length 1 and defined by hyperplanes, or equivalently, by a configuration of points in the dual projective space, this fits as the dashed line in our diagram.

A still largely open problem is that of the classification of codes (say up to linear isometries), or at least the description of a certain "structure theory" from which one could easily identify "good" codes [24][2]. Since the geometric view on linear codes makes them equivalent with projective configurations of points, GIT

appears as a natural tool toward this goal. Arguably one could see the present work as a first step in this direction. Actually, "zero-th step" would probably be a more accurate description: indeed, as could be hinted from (35), codes used for real world error correction will invariably tend to be stable. So their canonical filtration, and all our associated constructions, become trivial. Finer geometric invariants have to be considered. (Still there are a few other exotic applications of codes beside error correction, and one could wonder whether the canonical filtration has a role to play there.)

Our Harder-Narasimhan theory appears to be decorelated from the notions of criticality and spectrum introduced by Assmus in [2]. Recall that a code is decomposable (resp. indecomposable) if it can (resp. cannot) be written as the direct sum of two nontrivial subcodes with disjoint supports. An indecomposable code is critical if "puncturing" any coordinate, *i.e.* projecting onto the remaining $n-1$ positions, produces a decomposable code. The spectrum of an indecomposable k-dimensional code C is then the set of all (isometry classes of) critical k-dimensional codes C' that can be obtained by projecting C onto some subset of the coordinates. A sample of the diversity of possible situations is illustrated by the following examples:

- The binary $[3, 2, 2]$-code is stable and critical.

- The q-ary k-dimensional simplex code, of length $\frac{q^k-1}{q-1}$, whose associated projective configuration is the set of all points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$, is stable but not critical as soon as $k \geq 3$. In fact, its spectrum is the set of *all* (classes of) k-dimensional critical codes.

- The binary $[9, 7]$-code C with generating matrix

$$
\begin{pmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
$$

  is critical (it is an instance of *The Construction* of [2, p. 621] with the 3-partition $X = [9] = \{1, 2\} \cup \{3, 4\} \cup \{5, 6, 7, 8, 9\}$, $X' = \emptyset$) but not semistable (its subcode $C_{\{5,6,7,8,9\}}$ has rate $4/5 > 7/9$).

Given an (increasing) filtration $\mathrm{Fil}^{\cdot}$ on an object X in an abelian category, it is customary to define an associated graded object by considering the subsequent quotients $\mathrm{gr}^t X = \mathrm{Fil}^t X / \mathrm{Fil}^{t-1} X$. Unfortunately, the category of linear codes [2] is not abelian: in general it lacks a good notion of quotient code. Still, a nice quotient can be defined for subcodes defined by a support condition: given subsets $S \subseteq S' \subseteq [n]$ we define formally $C_{S'}/C_S = \pi_{S' \setminus S}(C_{S'})$. This is

compatible with our convention for (combinatorial) lattices, since subcodes of $\pi_{S'\backslash S}(C_{S'})$ identify with intermediary subcodes between C_S and $C_{S'}$.

Now let C be a $[n,k]$-code with full support, with canonical filtration

$$0 = C_0 \subsetneq C_1 \subsetneq \cdots \subsetneq C_N = C$$

and associated slopes $\mu_1 > \cdots > \mu_N$. By Proposition 20 the C_α are closed, *i.e.* they satisfy $C_\alpha = C_{\mathrm{Supp}(C_\alpha)}$, so the above applies and we can define

$$\mathrm{gr}^\alpha(C) = \pi_{T_\alpha}(C_\alpha) \tag{46}$$

where $T_\alpha = \mathrm{Supp}(C_\alpha)\backslash\mathrm{Supp}(C_{\alpha-1})$. If C_α has parameters $[n_\alpha, k_\alpha]$, then $\mathrm{gr}^\alpha(C)$ has parameters $[n_\alpha - n_{\alpha-1}, k_\alpha - k_{\alpha-1}]$ and is semistable of slope $\mu_\alpha = -\frac{n_\alpha - n_{\alpha-1}}{k_\alpha - k_{\alpha-1}}$. This gives a way to extract "possibly good", *i.e.* semistable codes, from "assuredly bad" ones.

The same works for matroids: if $\mathcal{M} = (E, \mathcal{I})$ has canonical filtration

$$\emptyset = J_0 \subsetneq J_1 \subsetneq \cdots \subsetneq J_N = E$$

with associated slopes $\mu_1 > \cdots > \mu_N$, we set

$$\mathrm{gr}^\alpha(\mathcal{M}) = (T_\alpha, \mathcal{I} \cap 2^{T_\alpha}) \tag{47}$$

where $T_\alpha = J_\alpha \setminus J_{\alpha-1}$. This is a semistable matroid, of slope μ_α.

Last, there is an obvious link between our constructions and Wei's theory of generalized Hamming weights [29]. Recall that the i-th weight of a (full support) $[n,k]$-code C is

$$d_i(C) = \min\{w(C') : \ C' \subseteq C, \dim(C') = i\} \tag{48}$$

so $0 = d_0(C) < d_1(C) = \mathrm{d_{min}}(C) < \cdots < d_k(C) = n$. The $C' \subseteq C$ for which the min is attained in (48) will be called minimum weight subcodes (of dimension i). One should keep in mind that, for a given i, there need not be a unique such subcode. More generally, two arbitrary minimum weight subcodes (of different dimension) need not be included one in the other. A code is said to satisfy the *chain condition* [30], or to be *chained*, if it admits a complete filtration by minimum weight subcodes.

From (30) and (48) we see that the canonical polygon of C is entirely determined by its weight hierarchy, or more precisely:

Lemma 31. *The canonical polygon of C is the upper convex envelope of the set of points*

$$\{(i, n - d_i(C)) : \ 0 \le i \le k\}.$$

In particular, the vertices of the canonical polygon form a subset of this set of points, and the subcodes in the canonical filtration of C are minimum weight subcodes. Thus, even if C is not chained, our theory (especially Theorem 6) allows to extract a subsequence of dimensions, and corresponding minimum

weight subcodes, that form a (partial) filtration, in a canonical way. For instance, if C is totally unstable, *i.e.* if it admits k different slopes, then it is chained. However, this example is rather extreme: as already noted, on the contrary, good codes tend to be stable. And it is possible for a code to be both stable and chained: such is the simplex code introduced a few paragraphs above, or also its affine counterpart, the Reed-Muller code of order 1.

As in the setting of vector bundles on curves, or in that of euclidean or hermitian lattices over number fields, an important question is that of the behaviour of the canonical polygon (and in particular, the preservation of semistability) under basic operations such as extension of scalars, duality, and tensor product.

The first one is almost immediate:

Proposition 32. *The canonical polygon of C, its canonical filtration, and its slopes, are preserved by extension of scalars.*

Proof. Invariance of the weight hierarchy of C under extension of scalars. $\square$

3. Slopes and duality

Recall that if $C \subseteq \mathbb{F}^n$ is a $[n,k]$-code, then its *dual code* $C^\perp \subseteq \mathbb{F}^n$ is the $[n, n-k]$-code defined as the orthogonal of C relative to the standard bilinear scalar product on $\mathbb{F}^n$.

Remark 33. At first, the word "dual" might seem misused here, however it has been well established historically. Moreover, $C^\perp$ enjoys certain properties that make this terminology better suited than one could have first thought, especially in our context. For instance, say in the binary case, we observe that if $\Gamma_C \subseteq \mathbb{R}^n$ is the euclidean lattice obtained from C by the so-called Construction A (of [10, §5.2], but suitably normalized, as in [14, §1.3]), then Γ_C and $\Gamma_{C^\perp}$ are dual lattices in the usual sense.

In this section we will give the relation between the canonical polygon of a code C and that of its dual code $C^\perp$. Thanks to Lemma 31, this could be deduced from Wei's duality theorem [29], which gives the relation between the weight hierarchy of C and that of $C^\perp$. However, it turns out it is slightly easier to work first from the other side of our cosupport Galois connection (40)(41), in terms of matroids. Actually, our proof does not require the matroid to come from a code, so what we will first state is a duality result for slopes of general matroids. This will then be translated back to codes thanks to Proposition 20.

A remarkable fact is that, although the proof uses only arguments from elementary linear algebra, these can be reinterpreted as part of some sort of Riemann-Roch theory, as developed in the Appendix at the end of this work.

We say that a finite matroid $\mathcal{M} = (E, \mathcal{I})$ is a $[n,k]$-matroid if it has cardinality $\#E = n$ and rank $r(E) = k$. Recall [21, §2.1] that the *dual matroid* $\mathcal{M}^*$ of $\mathcal{M}$ is then the $[n, n-k]$-matroid with the same underlying set E but whose bases (maximal independent sets) are the complements of those of $\mathcal{M}$.

For instance, the matroid $\mathcal{M}$ associated with a $[n, k]$-code C is a $[n, k]$-matroid, and its dual matroid $\mathcal{M}^*$ is then the matroid associated with the dual code $C^{\perp}$.

Theorem 34. *Let $\mathcal{M} = (E, \mathcal{I})$ be a $[n, k]$-matroid. Suppose that, relative to $\mathcal{M}$ and the associated degree function* (10), *the lattice L_E has canonical polygon*

$$P_{\mathcal{M}} : [0, n] \longrightarrow \mathbb{R}, \tag{49}$$

with slopes

$$\mu_1 > \cdots > \mu_N$$

(in the real interval $[-1, 0]$). Then, relative to the dual matroid $\mathcal{M}^*$, the lattice L_E has canonical polygon

$$\begin{array}{rrc} P_{\mathcal{M}^*} : & [0, n] & \longrightarrow & \mathbb{R} \\ & x & \mapsto & P_{\mathcal{M}}(n - x) + n - x - k, \end{array} \tag{50}$$

with slopes

$$-1 - \mu_N > \cdots > -1 - \mu_1.$$

Moreover, if the vertices of (49) *correspond to the canonical filtration*

$$\emptyset = J_0 \subsetneqq J_1 \subsetneqq \cdots \subsetneqq J_N = E, \tag{51}$$

then those of (50) *correspond to the dual filtration*

$$\emptyset = (E \setminus J_N) \subsetneqq \cdots \subsetneqq (E \setminus J_1) \subsetneqq (E \setminus J_0) = E. \tag{52}$$

Proof. By definition the canonical polygon of $\mathcal{M}$ is the upper convex envelope of the set of points

$$(\#J, \deg(J))$$

for $J \in L_E$, where by (10) we have $\deg(J) = k - r(J)$. Hence it is also the the upper convex envelope of the set of points

$$(j, f_{\mathcal{M}}(j))$$

where for $0 \leq j \leq n$ we set

$$f_{\mathcal{M}}(j) = \max\{\deg(J) : \ J \subseteq E, \#J = j\}.$$

Likewise the canonical polygon of $\mathcal{M}^*$ is the upper convex envelope of the set of points

$$(j, f_{\mathcal{M}^*}(j))$$

where $f_{\mathcal{M}^*}(j) = \max\{\deg^*(J) : \ J \subseteq E, \#J = j\}$, $\deg^*(J) = n - k - r^*(J)$.
Now a basic duality result for matroids [21, Prop. 2.1.9] reads

$$r^*(J) = \#J - k + r(E \setminus J),$$

25

which we can also write as

$$\deg^*(J) = \deg(E \setminus J) + n - \#J - k.$$

Letting J vary in this last equality, with $\#J = j$ fixed, we then find that the maximum is attained in the left-hand and right-hand side for the same J, with value

$$f_{\mathcal{M}^*}(j) = f_{\mathcal{M}}(n - j) + n - j - k$$

(which is actually Proposition 51 in the Appendix). The conclusion follows. $\square$

Corollary 35. *The matroid $\mathcal{M}$ is semistable if and only if its dual $\mathcal{M}^*$ is.*

Corollary 36. *Suppose that C has both minimum distance and dual distance at least 2, i.e. that both C and $C^\perp$ have full support. Let then C have canonical filtration*

$$0 = C_0 \subsetneqq C_1 \subsetneqq \cdots \subsetneqq C_N = C$$

with slopes

$$\mu_1 > \cdots > \mu_N$$

(in $\mathbb{R}_{<-1}$). Then $C^\perp$ has canonical filtration

$$0 = (C^\perp)_{[n] \setminus \mathrm{Supp}(C_N)} \subsetneqq \cdots \subsetneqq (C^\perp)_{[n] \setminus \mathrm{Supp}(C_1)} \subsetneqq (C^\perp)_{[n] \setminus \mathrm{Supp}(C_0)} = C^\perp$$

with slopes

$$-1 + (\mu_N + 1)^{-1} > \cdots > -1 + (\mu_1 + 1)^{-1}.$$

Proof. Let $\mathcal{M}$ be the matroid associated with C, so $\mathcal{M}^*$ is the matroid associated with $C^\perp$. From the canonical filtration and slopes of C, we can deduce those of $\mathcal{M}$ thanks to Proposition 20. We then deduce those of $\mathcal{M}^*$ thanks to Theorem 34, and finally we deduce those of $C^\perp$ back thanks to Proposition 20 again. $\square$

From this last result, the case where C or $C^\perp$ does not have full support is also easily treated, *e.g.* thanks to the "standard decomposition" [2, eq. (2)], and our Lemma 19 (or also Proposition 24). For instance, we see that $C^\perp$ does not have full support if and only if $\mu_{\max}(C) = -1$, in which case the first step of the canonical filtration of C is the subcode $V \subseteq C$ generated by the codewords of weight 1.

Corollary 37. *A linear code C is semistable if and only if its dual $C^\perp$ is.*

4. Semistability and tensor product

Given a $[n_A, k_A]$-code $A \subseteq \mathbb{F}^{n_A}$ and a $[n_B, k_B]$-code $B \subseteq \mathbb{F}^{n_B}$, we can form their tensor product

$$A \otimes B \quad \subseteq \quad \mathbb{F}^{n_A} \otimes \mathbb{F}^{n_B} \simeq \mathbb{F}^{n_A n_B}$$

which is thus a $[n_A n_B, k_A k_B]$-code, of rate $\mathrm{R}(A \otimes B) = \mathrm{R}(A)\,\mathrm{R}(B)$.

From the geometric point of view, if A corresponds to a collection of n_A points $\Pi_A \subseteq \mathbb{P}^{k_A - 1}$, and B to a collection of n_B points $\Pi_B \subseteq \mathbb{P}^{k_B - 1}$, then $A \otimes B$ corresponds to the image of $\Pi_A \times \Pi_B$ under the Segre embedding $\mathbb{P}^{k_A - 1} \times \mathbb{P}^{k_B - 1} \to \mathbb{P}^{k_A k_B - 1}$.

It is easily shown that if A has minimum distance $d_1(A) = d_A$ and B has minimum distance $d_1(B) = d_B$, then $A \otimes B$ has minimum distance $d_1(A \otimes B) = d_A d_B$. An interesting problem is the derivation of similar estimates for the higher weights $d_r(A \otimes B)$. In [23], Schaathun proved an important lower bound on these quantities.

For $0 \le r \le k_A k_B$, set

$$d_r^*(A \otimes B) = \min \left\{ \sum_{i=1}^{s} (d_i(A) - d_{i-1}(A)) d_{t_i}(B) : \right.$$

$$\left. 1 \le t_s \le \cdots \le t_1 \le k_B, \;\; s \le k_A, \;\; \sum_{i=1}^{s} t_i = r \right\}$$

$$= \min \left\{ \sum_{i=1}^{k_A} (d_i(A) - d_{i-1}(A)) d_{t_i}(B) : \right.$$

$$\left. 0 \le t_{k_A} \le \cdots \le t_1 \le k_B, \;\; \sum_{i=1}^{k_A} t_i \ge r \right\}$$

(observe that the minimum in the second line is the same as in the first: this is because the $d_i(A)$ and $d_i(B)$ form monotonously increasing sequences).

Theorem 38 ([23]). *With the notations above, for any subcode $C \subseteq A \otimes B$ of dimension $\dim(C) = r$, we have $w(C) \ge d_r^*(A \otimes B)$. Or equivalently,*

$$d_r(A \otimes B) \ge d_r^*(A \otimes B).$$

Previously, in [30], Wei and Yang had proved inequality in the other direction when both A and B are chained (hence Schaathun's bound implies equality in this case).

Thanks to Lemma 31, a lower bound on the weight hierarchy is the same as an upper bound on the canonical polygon. It is then no surprise that Schaathun's bound will be the key ingredient to our:

Theorem 39. *Suppose the linear codes A and B are semistable. Then their tensor product $A \otimes B$ is semistable.*

The analogue of Theorem 39 is known to be true for vector bundles over curves in characteristic zero, but false in positive characteristic, where counterexamples have been constructed [17]. For euclidean lattices (or more generally hermitian lattices, or adelic vector bundles over number fields) the question has been popularized by Bost and is still open, despite recent progress [6][16]

that allow to settle low dimensional cases, or lattices admitting a large group of automorphisms.

Schaathun's proof of Theorem 38 was written in terms of systems of points in a projective space, using the geometric view on coding theory. We propose here a reformulation directly in terms of codes.

Because of the close links between lattices of codes, it is not unreasonable to hope that this reformulation could provide inspiration for new approaches on the semistability conjecture for tensor products of lattices. Moreover the proof we will give here will appear to be shorter and marginally simpler than Schaathun's original one, although closer inspection would reveal the ideas remain fundamentally the same.

First we introduce some notation. For any $j \in [n_B]$, let $\pi_j : \mathbb{F}^{n_B} \to \mathbb{F}$ be the j-th standard projection. Tensoring with $\mathbb{F}^{n_A}$ then gives us

$$\widehat{\pi}_j : \mathbb{F}^{n_A} \otimes \mathbb{F}^{n_B} \longrightarrow \mathbb{F}^{n_A}.$$

It is customary to identify $\mathbb{F}^{n_A} \otimes \mathbb{F}^{n_B}$ with the space $\mathbb{F}^{n_A \times n_B}$ of matrices with n_A rows and n_B columns. The projection $\widehat{\pi}_j$ is then just the linear map that associates to each such matrix its j-th column. Under this identification, $A \otimes B$ becomes the space of matrices all of whose columns are in A and all of whose rows are in B. Thus, for any subcode $C \subseteq A \otimes B$, we see that $\widehat{\pi}_j(C)$ is a subcode of A. Moreover, the support size of C can be computed as

$$w(C) = \sum_{j=1}^{n_B} w(\widehat{\pi}_j(C)). \tag{53}$$

In order to prove Theorem 38, it suffices, given any $C \subseteq A \otimes B$, to construct a sequence $0 \leq t_{k_A} \leq \cdots \leq t_1 \leq k_B$ such that $w(C) \geq \sum_{i=1}^{k_A}(d_i(A) - d_{i-1}(A))d_{t_i}(B)$ and $\sum_{i=1}^{k_A} t_i \geq \dim(C)$. Thus Theorem 38 follows from the following more precise result:

Lemma 40. *Given a subcode $C \subseteq A \otimes B$, set, for $1 \leq i \leq k_A$,*

$$J_i = \{j \in [n_B] : \dim(\widehat{\pi}_j(C)) \geq i\}$$

and

$$t_i = \dim(B_{J_i}).$$

Then we have

$$w(C) \geq \sum_{i=1}^{k_A}(d_i(A) - d_{i-1}(A))d_{t_i}(B) \tag{54}$$

and

$$\sum_{i=1}^{k_A} t_i \geq \dim(C). \tag{55}$$

28

Proof (of Lemma 40, hence also of Theorem 38). For $1 \leq i \leq k_A$ we have, by the very definition of higher weights,

$$w(\widehat{\pi}_j(C)) \geq d_i(A) \qquad \text{for } j \in J_i \tag{56}$$

and

$$\#J_i \geq w(B_{J_i}) \geq d_{t_i}(B). \tag{57}$$

This works also for $i = 0$ and $i = k_A + 1$ if we set $J_0 = [n_B]$, $t_0 = k_B$, and $J_{k_A+1} = \emptyset$, $t_{k_A+1} = 0$.

The decreasing filtration $[n_B] = J_0 \supseteq J_1 \supseteq \cdots \supseteq J_{k_A} \supseteq J_{k_A+1} = \emptyset$ then allows to rewrite (53) as

$$
\begin{aligned}
w(C) &= \sum_{i=0}^{k_A} \sum_{j \in J_i \setminus J_{i+1}} w(\widehat{\pi}_j(C)) \\
&\geq \sum_{i=0}^{k_A} d_i(A)(\#J_i - \#J_{i+1}) && \text{by (56)} \\
&= \sum_{i=1}^{k_A} (d_i(A) - d_{i-1}(A))\#J_i && \text{summation by parts} \\
&\geq \sum_{i=1}^{k_A} (d_i(A) - d_{i-1}(A))d_{t_i}(B) && \text{by (57)},
\end{aligned}
$$

which proves (54).

Now for any i, choose a relative information set S_i for B_{J_i} modulo $B_{J_{i+1}}$, *i.e.* a subset

$$S_i \subseteq J_i \setminus J_{i+1}$$

such that the projection π_{S_i} induces a bijection

$$B_{J_i}/B_{J_{i+1}} \xrightarrow{\sim} \mathbb{F}^{S_i}$$

(this is possible since, by definition, $B_{J_i} = B \cap \mathbb{F}^{J_i} \subseteq \mathbb{F}^{J_i}$ so, passing to the quotient, $\pi_{J_i \setminus J_{i+1}}$ induces an injection $B_{J_i}/B_{J_{i+1}} \hookrightarrow \mathbb{F}^{J_i \setminus J_{i+1}}$). Then necessarily, $\#S_i = \dim(B_{J_i}/B_{J_{i+1}}) = t_i - t_{i+1}$.

Considering the filtration $B = B_{J_0} \supseteq B_{J_1} \supseteq \cdots \supseteq B_{J_{k_A}} \supseteq B_{J_{k_A+1}} = 0$, we see that the disjoint union $S = S_0 \sqcup S_1 \sqcup \cdots \sqcup S_{k_A}$ is an information set for B, *i.e.* we have an isomorphism

$$\pi_S : B \xrightarrow{\sim} \mathbb{F}^S.$$

Tensoring with A then gives $\widehat{\pi_S} : A \otimes B \xrightarrow{\sim} A^S$, which restricts to C as

$$C \simeq \widehat{\pi_S}(C) \ \subseteq \ \bigoplus_{j \in S} \widehat{\pi}_j(C)$$

(or said more concretely: a codeword in B is determined by its coordinates over S, hence a codeword in $A \otimes B$, thus *a fortiori* a codeword in C, is determined by its columns over S).

Now writing $\bigoplus_{j \in S} \widehat{\pi}_j(C) = \bigoplus_{i=0}^{k_A} \bigoplus_{j \in S_i} \widehat{\pi}_j(C)$, and using the fact that $\dim(\widehat{\pi}_j(C)) = i$ for $j \in S_i \subseteq J_i \setminus J_{i+1}$, we conclude

$$\dim(C) \leq \sum_{i=0}^{k_A} \sum_{j \in S_i} \dim(\widehat{\pi}_j(C)) = \sum_{i=0}^{k_A} i \# S_i = \sum_{i=0}^{k_A} i(t_i - t_{i+1}) = \sum_{i=1}^{k_A} t_i.$$

$\square$

We can now proceed to our proof of the semistability theorem for tensor products of codes. This can be derived either as a consequence of Theorem 38, or slightly more directly, by reworking part of the proof of Lemma 40. We propose the latter:

Proof of Theorem 39. Let $C \subseteq A \otimes B$ be any subcode, and let then the J_i and the t_i be given by Lemma 40. Thanks to (35), semistability of A implies

$$\begin{aligned} w(\widehat{\pi}_j(C)) &\geq \dim(\widehat{\pi}_j(C))/\operatorname{R}(A) \\ &\geq i/\operatorname{R}(A) \qquad \text{for } j \in J_i, \end{aligned} \tag{58}$$

and semistability of B implies

$$\# J_i \geq w(B_{J_i}) \geq t_i/\operatorname{R}(B). \tag{59}$$

The computation in the first half of the proof of Lemma 40 then becomes:

$$\begin{aligned} w(C) &= \sum_{i=0}^{k_A} \sum_{j \in J_i \setminus J_{i+1}} w(\widehat{\pi}_j(C)) \\ &\geq \frac{1}{\operatorname{R}(A)} \sum_{i=0}^{k_A} i(\# J_i - \# J_{i+1}) \qquad\qquad \text{by (58)} \\ &= \frac{1}{\operatorname{R}(A)} \sum_{i=1}^{k_A} \# J_i \qquad\qquad\qquad\qquad \text{summation by parts} \\ &\geq \frac{1}{\operatorname{R}(A)\operatorname{R}(B)} \sum_{i=1}^{k_A} t_i \geq \frac{\dim(C)}{\operatorname{R}(A \otimes B)} \qquad \text{by (59) and (55).} \end{aligned}$$

Using (35) again, this means precisely that $A \otimes B$ is semistable. $\square$

Remark 41. We have shown that semistability is preserved under many natural operations on codes, such as extension of scalars, duality, and tensor product. Here is an operation that does not preserve it: although *componentwise product*

of codes is closely related to tensor product [22, §1.10], it is easily checked (*e.g.* using Proposition 24) that the binary $[5, 2]$-code C, with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

is semistable, and even stable, while its square $C^{\langle 2 \rangle}$, with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

is unstable.

Remark 42. In Remark 30 we saw that codes could be seen as multi-filtered spaces in the sense of Faltings-Wüstholz and Totaro, in a way that preserves the canonical filtration. Moreover these authors also proved that, in characteristic zero, a tensor product of semistable multi-filtered spaces is semistable (in [15, Th. 4.1] this is done by reducing to the case of vector bundles on curves, and in [26] this is done in a somehow more elementary way, although still relying on the GIT machinery).

However one should be careful: *the tensor product of codes does not coincide with the tensor product of multi-filtered spaces!*

A first point is that [15][26] consider two spaces with the same number n of filtrations, and produce a tensor product also with n filtrations. From this perspective, the theory is more similar to that of componentwise products of the preceding remark, than to that of tensor products, where A has n_A filtrations, B has n_B, and $A \otimes B$ has $n_A n_B$.

This first objection is easily bypassed. Indeed, let A be equipped with the n_A filtrations $A \supseteq H_i$, and B with the n_B filtrations $B \supseteq K_j$. Then we can repeat n_B times each H_i, and repeat n_A times each K_j. Doing so, A and B get the same number $n_A n_B$ of filtrations, and their tensor product as multi-filtered spaces is then equipped with the $n_A n_B$ filtrations

$$A \otimes B \; \supseteq \; (H_i \otimes B) + (A \otimes K_j) \; \supseteq \; H_i \otimes K_j$$

of length 2.

However, the multi-filtered space associated with the tensor product code only corresponds to the *truncated* filtrations

$$A \otimes B \; \supseteq \; (H_i \otimes B) + (A \otimes K_j)$$

of length 1. In matrix form, codewords in $(H_i \otimes B) + (A \otimes K_j)$ are those vanishing at position (i, j), as expected, while codewords in $H_i \otimes K_j$ are those whose whole i-th row and j-th column are identically zero.

Thus our result and the one in [15][26] are of a quite different nature. It is unclear whether one could be deduced from the other. Still it would be interesting to try to adapt the method of proof of our Theorem 39, which holds in arbitrary characteristic, to tensor products of multi-filtered spaces.

References (main)

[1] Y. André. Slope filtrations. Confluentes Math. 1 (2009) 1–85.

[2] E. Assmus. The category of linear codes. IEEE Trans. Inform. Theory 44 (1998) 612–629.

[3] G. Birkhoff. Lattice theory (3rd ed). Colloquium Publ., vol. 25, Amer. Math. Soc., Providence, 1979.

[4] T. Borek. Successive minima and slopes of hermitian vector bundles over number fields. J. Number Theory 113 (2005) 380–388.

[5] A. Borel & J.-P. Serre. Corners and arithmetic groups. Comment. Math. Helv. 48 (1973) 436–491.

[6] J.-B. Bost & H. Chen. Concerning the semistability of tensor products in Arakelov geometry. J. Math. Pures Appl. 99 (2013) 436–488.

[7] J.-B. Bost & K. Künnemann. Hermitian vector bundles and extension groups on arithmetic schemes. I. Geometry of numbers. Adv. Math. 223 (2010) 987–1106.

[8] H. Chen. Harder-Narasimhan categories. J. Pure Appl. Alg. 214 (2010) 187–200.

[9] H. Chen. Personal communication (2016).

[10] J. Conway & N. Sloane. Sphere packings, lattices and groups (3rd ed). Grundlehren der Math. Wissenschaften, vol. 290, Springer-Verlag, New York, 1999.

[11] C. Cornut. On Harder-Narasimhan filtrations and their compatibility with tensor products. To appear in Confluentes Math.

[12] I. Dolgachev. Lectures on invariant theory. London Mathematical Society Lecture Note Series, vol. 296, Cambridge University Press, Cambridge, 2003.

[13] I. Dolgachev & D. Ortland. Point sets in projective spaces and theta functions. Astérisque 165 (1988).

[14] W. Ebeling. Lattices and codes (3rd ed). Advanced Lectures in Math., Springer Spektrum, Wiesbaden, 2013.

[15] G. Faltings & G. Wüstholz. Diophantine approximations on projective spaces. Invent. Math. 116 (1994) 109–138.

[16] É. Gaudron & G. Rémond. Minima, pentes et algèbre tensorielle. Israel J. Math. 195 (2013) 565–591.

[17] D. Gieseker. Stable vector bundles and the Frobenius morphism. Ann. Sci. École Norm. Sup. (4) 6 (1973) 95–101.

[18] D. Grayson. Reduction theory using semistability. Comment. Math. Helvetici 59 (1984) 600–634.

[19] G. Harder & M. Narasimhan. On the cohomology groups of moduli spaces of vector bundles on curves. Math. Ann. 212 (1975) 215–248.

[20] D. Mumford & J. Fogarty & F. Kirwan. Geometric invariant theory. Third edition. Ergebnisse der Mathematik und ihrer Grenzgebiete (2), vol. 34, Springer-Verlag, Berlin, 1994.

[21] J. Oxley. Matroid theory. Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1992.

[22] H. Randriambololona. On products and powers of linear codes under componentwise multiplication. In: Algorithmic arithmetic, geometry, and coding theory. Contemp. Math., vol. 637, Amer. Math. Soc., Providence, RI, 2015, pp. 3–78.

[23] H. Schaathun. The weight hierarchy of product codes. IEEE Trans. Inform. Theory 46 (2000) 2648–2651.

[24] D. Slepian. Some further theory of group codes. Bell Syst. Tech. J. 39 (1960) 1219–1252.

[25] U. Stuhler. Eine Bemerkung zur Reduktionstheorie quadratischer Formen. Arch. Math. 27 (1976) 604–610.

[26] B. Totaro. Tensor products of semistables are semistable. In: Geometry and analysis on complex manifolds. World Sci. Publ., River Edge, NJ, 1994, pp. 242–250.

[27] M. Tsfasman & S. Vladut. Algebraic-geometric codes. Mathematics and its Appl. (Soviet Series), vol. 58, Kluwer Acad. Publ. Group, Dordrecht, 1991.

[28] M. Tsfasman & S. Vladut. Geometric approach to higher weights. IEEE Trans. Inform. Theory 41 (1995) 1564–1588.

[29] V. Wei. Generalized Hamming weights for linear codes. IEEE Trans. Inform. Theory 37 (1991) 1412–1418.

[30] V. Wei & K. Yang. On the generalized Hamming weights of product codes. IEEE Trans. Inform. Theory 39 (1993) 1709–1713.

[31] H. Whitney. On the abstract properties of linear independence. Amer. J. Math. 57 (1935) 509–533.

Appendix: A Riemann-Roch theory for linear codes and matroids

Subspace pair cohomology.
We introduce cohomology groups associated to triples (V, A_1, A_2) where:

- V is a vector space,

- $A_1, A_2 \subseteq V$ are two linear subspaces.

Definition 43. Given such a triple (V, A_1, A_2) we set

$$H^0(V; A_1, A_2) = A_1 \cap A_2 \tag{60}$$

and

$$H^1(V; A_1, A_2) = V/(A_1 + A_2), \tag{61}$$

of dimension, respectively:

$$h^0(V; A_1, A_2) = \dim(H^0(V; A_1, A_2)), \quad h^1(V; A_1, A_2) = \dim(H^1(V; A_1, A_2)).$$

It turns out these H^0 and H^1 can be identified with the cohomology groups of any of the following two quasi-isomorphic complexes of length 2:

$$0 \longrightarrow A_1 \oplus A_2 \longrightarrow V \longrightarrow 0, \tag{62}$$

or

$$0 \longrightarrow V \longrightarrow V/A_1 \oplus V/A_2 \longrightarrow 0. \tag{63}$$

Remark 44. To be more precise, the exact definition of these complexes, together with a quasi-isomorphism between them, and the identification of (60) and (61) with their cohomology groups, all depend on some choice of signs. A possible choice is the following:

$$
\begin{array}{ccccccccc}
0 \to & A_1 \cap A_2 & \xrightarrow{++} & A_1 \oplus A_2 & \xrightarrow{+-} & V & \longrightarrow & V/(A_1+A_2) & \to 0 \\
 & \| & & \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle p_2} & & \| & \\
0 \to & A_1 \cap A_2 & \longrightarrow & V & \xrightarrow{-+} & V/A_1 \oplus V/A_2 & \xrightarrow{++} & V/(A_1+A_2) & \to 0
\end{array}
$$

where the maps are defined as follows: on the top line, the left $++$ map sends $x \in A_1 \cap A_2$ to $(x, x) \in A_1 \oplus A_2$, the middle $+-$ map sends $(a_1, a_2) \in A_1 \oplus A_2$ to $a_1 - a_2 \in V$, and the right map is natural projection; on the bottom line, the left map is natural inclusion, the middle $-+$ maps sends $v \in V$ to (the class of) $(-v, v) \in V/A_1 \oplus V/A_2$, and the right $++$ map sends (the class of) $(v_1, v_2) \in V/A_1 \oplus V/A_2$ to (the class of) $v_1 + v_2 \in V/(A_1 + A_2)$; then the vertical i_1 sends $(a_1, a_2) \in A_1 \oplus A_2$ to $a_1 \in V$, and the vertical p_2 sends $v \in V$ to (the class of) $(0, v) \in V/A_1 \oplus V/A_2.$[5]

---

[5]It is easily checked this makes everything commute, for instance, the middle square maps $(a_1, a_2) \in A_1 \oplus A_2$ to (the class of) $(0, a_1) \in V/A_1 \oplus V/A_2$.

Lemma 45. *Let (V, A_1, A_2) be a triple as above. Then, if V is finite dimensional, we have*

$$h^0(V; A_1, A_2) - h^1(V; A_1, A_2) = \dim(A_1) + \dim(A_2) - \dim(V).$$

Proof. Direct from Definition 43, or alternatively, Euler characteristic of the complex (62) (or of (63)). $\square$

Lemma 46. *Let (V, A_1, A_2) be a triple as above. Then for any linear subspace $A_2' \subseteq A_2$ we have a long exact sequence*

$$0 \longrightarrow H^0(V; A_1, A_2') \longrightarrow H^0(V; A_1, A_2) \longrightarrow A_2/A_2' \longrightarrow \ldots$$
$$\ldots \longrightarrow H^1(V; A_1, A_2') \longrightarrow H^1(V; A_1, A_2) \longrightarrow 0.$$

Proof. Direct from Definition 43, or alternatively, snake lemma for

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & A_1 \oplus A_2' & \longrightarrow & A_1 \oplus A_2 & \longrightarrow & A_2/A_2' & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & V & \longrightarrow & V & \longrightarrow & 0 & \longrightarrow & 0
\end{array}
$$

$\square$

Recall that $V^\vee$ denotes the dual vector space of V, *i.e.* the space of linear forms on V. Given a linear subspace $A \subseteq V$, we let $A^\perp \subseteq V^\vee$ be the space of linear forms vanishing on A. We have natural identifications $A^\perp = (V/A)^\vee$ and $V^\vee/A^\perp = A^\vee$.

Lemma 47. *Given a triple (V, A_1, A_2) as above, we have a natural identification*

$$H^1(V; A_1, A_2) = H^0(V^\vee; A_1^\perp, A_2^\perp)^\vee.$$

Proof. Direct from Definition 43, or alternatively, from the fact that dualizing exact sequence (62) for $(V; A_1, A_2)$ gives exact sequence (63) for $(V^\vee; A_1^\perp, A_2^\perp)$ (actually, with sign reversed compared to Remark 44, but this does not change its cohomology). $\square$

Serre duality and Riemann-Roch for codes.
Let $C \subseteq \mathbb{F}^n$ be a $[n, k]$-code. We will apply the formalism just introduced to the following triple:

- $V = \mathbb{F}^n$ somehow seen as an "adèle space"[6]

- $A_1 = C$ the subspace of principal adèles

---

[6]Although we will not really need it, we observe that our adèle space is in fact an adèle *ring*, and even more precisely a $\mathbb{F}$-algebra, thanks to componentwise multiplication. The standard scalar product, for which $C^\perp$ is the orthogonal of C, is then nothing but the canonically associated trace bilinear form [22, §2.37].

- $A_2 = \mathbb{F}^J$ the subspace of adèles with poles in a subset $J \subseteq [n]$ (where we actually identify $\mathbb{F}^J$ with $\mathbb{F}^J \times \{0\}^{[n]\setminus J}$).

This will allow us to mimic Weil's adelic proof of the Riemann-Roch theorem, as modern coding theorists often learn, for instance, in [48].

Slightly changing notations, we thus get the following cohomology groups:

$$\begin{aligned} H^0(C, J) &= H^0(\mathbb{F}^n; C, \mathbb{F}^J) \\ &= C \cap \mathbb{F}^J \\ &= C_J, \end{aligned} \tag{64}$$

the largest (a.k.a. "shortened") subcode of C with support in J, and

$$\begin{aligned} H^1(C, J) &= H^1(\mathbb{F}^n; C, \mathbb{F}^J) \\ &= \mathbb{F}^n/(C + \mathbb{F}^J) \\ &= \mathbb{F}^{[n]\setminus J}/\pi_{[n]\setminus J}(C), \end{aligned} \tag{65}$$

where $\pi_{[n]\setminus J} : \mathbb{F}^n \to \mathbb{F}^{[n]\setminus J}$ is the natural projection. The author does not know whether this H^1 has ever been considered in the literature. Its elements can be seen as syndromes, so maybe it could be of use, for instance, in some decoding algorithms.

Lemma 46 provides, for any disjoint $J, J' \subseteq [n]$, a long exact sequence

$$0 \to H^0(C, J) \to H^0(C, J \sqcup J') \xrightarrow{\pi_{J'}} \mathbb{F}^{J'} \to H^1(C, J) \to H^1(C, J \sqcup J') \to 0 \tag{66}$$

where we used the $\sqcup$ symbol as a reminder of the fact that the union is disjoint. Of course this readily extends to possibly non-disjoint J, J' using the equality $J \cup J' = J \sqcup (J' \setminus J)$.

As before we also set $h^0(C, J) = \dim H^0(C, J)$ and $h^1(C, J) = \dim H^1(C, J)$.

Theorem 48. *Let $C \subseteq \mathbb{F}^n$ be a $[n, k]$-code. Then for any subset $J \subseteq [n]$ we have a canonical identification*

$$H^1(C, J) = H^0(C^\perp, [n] \setminus J)^\vee.$$

Proof. This is Lemma 47. □

Theorem 49. *Let $C \subseteq \mathbb{F}^n$ be a $[n, k]$-code. Then for any subset $J \subseteq [n]$ we have the equality*

$$h^0(C, J) - h^0(C^\perp, [n] \setminus J) = \#J + k - n.$$

Proof. Combine Lemma 45 with Theorem 48. □

Since $h^0(C, J)$ vanishes for $\#J < d = \mathrm{d}_{\min}(C)$, it is convenient to introduce the normalized cardinality $|J|_{\mathrm{norm}} = \#J - d$. Theorem 49 then becomes:

$$h^0(C, J) - h^0(C^\perp, [n] \setminus J) = |J|_{\mathrm{norm}} + 1 - g \tag{67}$$

where $g = n - k - d + 1$ is the Singleton defect of C.

We find it pleasant to think of Theorem 48 as a Serre duality theorem for codes, and of Theorem 49, or (67), as a Riemann-Roch theorem. Seemingly, when C is an AG code defined by evaluation of functions on an algebraic curve, these results partially reflect Serre duality and Riemann-Roch on the underlying curve. However we would like to stress that they hold for *any* arbitrary linear code.

Of course a more direct proof could be given using only elementary linear algebra, for instance by combining lemmas from [39]. However our main purpose here is not really in the content of these theorems, nor in giving the most efficient proof, but rather on the analogy with the geometric situation. Thus our "adelic" proof was presented in order to make this analogy even stronger.

Observe that our statements do not involve only the code C but also its dual $C^\perp$, and hence become more symmetric when applied to *self-dual* codes. Although it is not entirely clear what status self-dual codes enjoy under our chain of analogies (*e.g.* "2-torsion points" in some "Jacobian"?), they certainly have a great arithmetic significance. For instance, Construction A of [10, §5.2] (suitably normalized) transforms binary self-dual codes into unimodular integral euclidean lattices. We refer to [14] for more on this topic. In a more anecdotal way, we observe that self-dual codes also satisfy the following *Clifford*-like estimate:

$$h^0(C, J) \le \frac{1}{2} \# J. \tag{68}$$

It is interesting to note that, even if not explicitely stated so, the analogy of Theorems 48 and 49 with Serre duality and Riemann-Roch was already implicit in previous works of other authors. We point out especially [38]: as observed below, the h^0 and h^1 introduced there, p. 123, coincide with ours. A consequence of this observation (and, in the first place, of the results in [38]) is that this Riemann-Roch theorem for codes implies the functional equation for the Duursma zeta function essentially in the same way that the usual Riemann-Roch theorem implies the functional equation for the zeta function of curves over finite fields.

Generalization to matroids.

It turns out our Theorem 49 admits a generalization, and also a more direct proof, in the context of matroids.

We keep notations as in section 3 of the main text: a finite matroid $\mathcal{M} = (E, \mathcal{I})$ is a $[n, k]$-matroid if it has cardinality $\#E = n$ and rank $r(E) = k$; its dual matroid $\mathcal{M}^*$ then is a $[n, n - k]$-matroid.

Now, following [38], for any $J \subseteq E$, we set

$$h^0(\mathcal{M}, J) = r(E) - r(E \setminus J). \tag{69}$$

Our Riemann-Roch theorem for matroids then reads:

Proposition 50. *Let $\mathcal{M} = (E, \mathcal{I})$ be a $[n, k]$-matroid. Then for any $J \subseteq E$ we have*

$$h^0(\mathcal{M}, J) - h^0(\mathcal{M}^*, E \setminus J) = \# J + k - n.$$

Proof. Replacing with (69), $r(E) = k$, and $r^*(E) = n - k$, we are reduced to show $r^*(J) - r(E \setminus J) = \#J - k$, which is nothing but [21, Prop. 2.1.9].　　□

Observe that if $\mathcal{M}$ is the matroid with underlying set $[n]$, defined by the columns of the generating matrix of a $[n, k]$-code C, then for any $J \subseteq [n]$ we have
$$h^0(\mathcal{M}, J) = h^0(C, J).$$
Also the dual matroid $\mathcal{M}^*$ corresponds in the same way to the dual code $C^\perp$. Thus in this situation, Proposition 50 reduces to Theorem 49.

In [38] one also finds the quantity
$$h^1(\mathcal{M}, J) = \#(E \setminus J) - r(E \setminus J). \tag{70}$$

From Proposition 50 (or from [21, Prop. 2.1.9]) we immediately see that it satisfies
$$h^1(\mathcal{M}, J) = h^0(\mathcal{M}^*, E \setminus J),$$
a weak form of Serre duality (equality of "dimensions", but no actual duality map as in Theorem 48).

In case $\mathcal{M}$ comes from a linear code C, we also have $h^1(\mathcal{M}, J) = h^1(C, J)$ (direct consequence of (65)). So the two definitions of h^1 coincide, as did the h^0.

Wei's duality for higher weights.

We define the weight hierarchy and the dimension/length profile (DLP) of a matroid as the two "dual" sequences
$$d_i(\mathcal{M}) = \min\{\#J : \ J \subseteq E, h^0(\mathcal{M}, J) = i\} \qquad (i = 0 \dots k)$$
and
$$k_j(\mathcal{M}) = \max\{h^0(\mathcal{M}, J) : \ J \subseteq E, \#J = j\} \qquad (j = 0 \dots n).$$

When $\mathcal{M}$ comes from a code C, these are easily seen to coincide with those introduced in [29] and [39].

Pursuing our geometric analogy, the weight hierarchy clearly corresponds to the gonality sequence of a curve X
$$\gamma_i(X) = \min\{\deg(D) : \ D \in \mathrm{Div}(X), h^0(X, D) = i\} \qquad (i > 0),$$
an observation already made in [44][51][38]. Then in [38] there is also a derivation of Wei's duality theorem using the rank polynomial of the code. Here we will proceed in a way closer to that of [39]. Observe that all our computations will be in the matroid setting, so what we will get in the end is a matroid version of Wei's duality. Actually, such a result is not new: it first appeared in [36].

As in [39], we first prove duality for the DLP. Interestingly, this result is also at the heart of our Theorem 34 on duality for slopes and canonical filtration.

Proposition 51. *Let $\mathcal{M} = (E, \mathcal{I})$ be a $[n, k]$-matroid. Then for any $j \in [n]$ we have*
$$k_{n-j}(\mathcal{M}^*) = k_j(\mathcal{M}) + n - j - k.$$
Moreover, if $k_j(\mathcal{M}) = h^0(\mathcal{M}, J)$ for some $J \subseteq E$ with $\#J = j$, then $k_{n-j}(\mathcal{M}^*) = h^0(\mathcal{M}^*, E \setminus J)$.

Proof. For $J \subseteq E$ with $\#J = j$ we write Proposition 50 as
$$h^0(\mathcal{M}^*, E \setminus J) = h^0(\mathcal{M}, J) + n - j - k. \tag{71}$$
Letting J vary with $\#J = j$ fixed, we then find that the minimum is attained in the left-hand and right-hand side for the same J, with value $k_{n-j}(\mathcal{M}^*) = k_j(\mathcal{M}) + n - j - k$ as claimed. $\square$

From the very definition, for any $J \subseteq E$ and $e \in E \setminus J$, we have $r(J \cup \{e\}) = r(J)$ or $r(J) + 1$. This translates as
$$h^0(\mathcal{M}, J \cup \{e\}) = h^0(\mathcal{M}, J) \text{ or } h^0(\mathcal{M}, J) + 1 \tag{72}$$
(in case $\mathcal{M}$ comes from a code C, this also follows from (66) with $J' = \{e\}$).

Plugging this into the definition of the DLP, it follows easily:

Lemma 52. *For any integer $j \in [n]$ we have $k_j(\mathcal{M}) = k_{j-1}(\mathcal{M})$ or $k_{j-1}(\mathcal{M}) + 1$.*

Definition 53. Let $\mathcal{M}$ be a $[n, k]$-matroid, and $j \in [n]$ an integer.

- We say that j is a *gap* for $\mathcal{M}$ if $k_j(\mathcal{M}) = k_{j-1}(\mathcal{M})$.

- Else, we say j is a *non-gap* if $k_j(\mathcal{M}) = k_{j-1}(\mathcal{M}) + 1$.

Since $k_0(\mathcal{M}) = 0$ and $k_n(\mathcal{M}) = k$, we deduce that $\mathcal{M}$ admits precisely $n - k$ gaps and k non-gaps.

Lemma 54. *An integer $j \in [n]$ is a non-gap for $\mathcal{M}$ if and only if $n + 1 - j$ is a gap for $\mathcal{M}^*$ (and conversely).*

Proof. Replacing in Proposition 51, we see $k_j(\mathcal{M}) = k_{j-1}(\mathcal{M}) + 1$ if and only if $k_{n-j}(\mathcal{M}^*) = k_{n+1-j}(\mathcal{M}^*)$. $\square$

Lemma 55. *The non-gaps of $\mathcal{M}$ coincide with its (nonzero) higher weigths $d_1(\mathcal{M}), \ldots, d_k(\mathcal{M})$.*

Proof. That j is a non-gap means $l = k_j(\mathcal{M}) > k_{j-1}(\mathcal{M}) = l - 1$, or equivalently, there is a $J \subseteq E$ with $h^0(\mathcal{M}, J) = l$ and $\#J = j$, but $h^0(\mathcal{M}, J') < l$ for all J' of cardinality $\#J' < j$. In turn, this means precisely $d_l(\mathcal{M}) = j$. $\square$

We can now finish our proof of Wei's duality for higher weights of matroids:

Proposition 56 ([36, Th. 1]). *Let $\mathcal{M}$ be a $[n, k]$-matroid. Then the two sets of integers*
$$\{d_i(\mathcal{M}) : i \in [k]\} \qquad and \qquad \{n + 1 - d_i(\mathcal{M}^*) : i \in [n - k]\}$$
are disjoint, hence they form a partition of $[n]$.

Proof. Combine Lemma 54 and Lemma 55. $\square$

Supplementary references (appendix)

[32] K. Adiprasito, J. Huh & E. Katz. Hodge theory for combinatorial geometries. Preprint (2015) `arxiv:1511.02888`

[33] M. Baker & S. Norine. Riemann-Roch and Abel-Jacobi theory on a finite graph. Adv. Math. 215 (2007) 766–788.

[34] A. Borisov. Convolution structures and arithmetic cohomology. Compositio Math. 136 (2003) 237–254.

[35] J.-B. Bost. Theta invariants of euclidean lattices and infinite-dimensional hermitian vector bundles over arithmetic curves. Preprint (2015) `arxiv: 1512.08946`

[36] T. Britz & T. Johnsen & D. Mayhew & K. Shiromoto. Wei-type duality theorems for matroids. Des. Codes Cryptogr. 62 (2012) 331–341.

[37] I. Duursma. Weight distributions of geometric Goppa codes. Trans. Amer. Math. Soc. 351 (1999) 3609–3639.

[38] I. Duursma. Combinatorics of the two-variable zeta function. In: Finite fields and applications. Lecture Notes in Comput. Sci., vol. 2948, Springer, Berlin, 2004, pp. 109–136.

[39] G. Forney. Dimension/length profiles and trellis complexity of linear block codes. IEEE Trans. Inform. Theory 40 (1994) 1741–1752.

[40] G. van der Geer & R. Schoof. Effectivity of Arakelov divisors and the theta divisor of a number field. Selecta Math. N.S. 6 (2000) 377–398.

[41] H. Gillet & C. Soulé. On the number of lattice points in convex symmetric bodies and their duals. Israel J. Math. 74 (1991) 347–357.

[42] R. Groenewegen. An arithmetic analogue of Clifford's theorem. J. Théor. Nombres Bordeaux 13 (2001) 143–156.

[43] E. Katz. Matroid theory for algebraic geometers. In: M. Baker & S. Payne (eds). Nonarchimedean and tropical geometry. Simons Symposia, Springer, 2016, pp. 435–517.

[44] C. Munuera. On the generalized Hamming weights of geometric Goppa codes. IEEE Trans. Inform. Theory 40 (1994) 2092–2099.

[45] D. Roessler. The Riemann-Roch theorem for arithmetic curves. ETH Diplomarbeit, 1993.

[46] F.K. Schmidt. Analytische Zahlentheorie in Körpern der Charakteristik p. Math. Z. 33 (1931) 1–32.

[47] C. Soulé. Hermitian vector bundles on arithmetic varieties. In: Algebraic geometry—Santa Cruz 1995. Proc. Sympos. Pure Math. vol. 62(1), Amer. Math. Soc., Providence, RI, 1997, pp. 383–419.

[48] H. Stichtenoth. Algebraic function fields and codes (2nd ed). Graduate Texts in Math., vol. 254, Springer-Verlag, Berlin, 2009.

[49] L. Szpiro. Degrés, intersections, hauteurs. In: Séminaire sur les pinceaux arithmétiques. La conjecture de Mordell. Astérisque 127 (1985) 445–450.

[50] J. Tate. Fourier analysis in number fields, and Hecke's zeta-functions. Ph.D. Thesis, Princeton University 1950. Reprinted in: J. Cassels & A. Fröhlich (eds). Algebraic number theory. Academic Press, London, 1986.

[51] K. Yang & P.V. Kumar & H. Stichtenoth. On the weight hierarchy of geometric Goppa codes. IEEE Trans. Inform. Theory 40 (1994) 913–920.