Finite Fields and Their Applications 18 (2012) 746–759

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Parameters of AG codes from vector bundles

Tohru Nakashima *,[1]

Department of Mathematical and Physical Sciences, Faculty of Science, Japan Women's University, Mejirodai, Bunkyoku, Tokyo 112-8681, Japan

ARTICLE INFO

Article history:
Received 15 May 2011
Revised 14 April 2012
Accepted 17 April 2012
Available online 27 April 2012
Communicated by H. Stichtenoth

MSC:
94B27
14H60
14J60

Keywords:
Algebraic–geometric codes
Vector bundles

ABSTRACT

We investigate the parameters of the algebraic–geometric codes constructed from vector bundles on a projective variety defined over a finite field. In the case of curves we give a method of constructing weakly stable bundles using restriction of vector bundles on algebraic surfaces and illustrate the result by some examples.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements and let X be a projective curve defined over $\mathbb{F}_q$, which is smooth and geometrically irreducible. Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be a set of distinct $\mathbb{F}_q$-rational points of X. For a divisor D on X, let $L(D)$ denote the associated vector space of rational functions. The usual algebraic–geometric (AG) code is defined to be the image of the evaluation map

$$\varphi_D : L(D) \to \mathbb{F}_q^n,$$

$$f \mapsto \big(f(P_1), f(P_2), \ldots, f(P_n)\big).$$

* Fax: +81 3 5981 3636.
E-mail address: nakashima@fc.jwu.ac.jp.

[1] The author was supported in part by Grant-in-Aid for Scientific Research (C) (21540049).

1071-5797/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ffa.2012.04.004

Viewing this as the evaluation map of the sections of the corresponding line bundle $\mathcal{O}_X(D)$, the definition of AG codes has been generalized for varieties of higher dimension [9].

Recently, it has been shown that the interleaved AG code may be interpreted geometrically as the image of the evaluation map for a vector bundle $\mathcal{O}_X(D)^{\oplus r}$ [1]. Motivated by this observation, V. Savin has given the notion of AG codes defined by arbitrary vector bundles [12]. In [11], we further generalized this construction and gave the definition of AG codes defined by vector bundles on varieties of arbitrary dimension.

Let X be a projective variety defined over $\mathbb{F}_q$, which we assume to be smooth and geometrically irreducible. Let E be a vector bundle of rank r on X defined over $\mathbb{F}_q$. Given a set $\mathcal{P} = \{P_1, P_2, \dots, P_n\}$ of $\mathbb{F}_q$-rational points of X, we fix an isomorphism of the fiber $E_{P_i} \cong \mathbb{F}_q^r \cong \mathbb{F}_Q$ for each i, where we set $Q = q^r$ and we assume that an isomorphism $\mathbb{F}_q^r \cong \mathbb{F}_Q$ is chosen. Then we define the code $C(X, \mathcal{P}, E)$ to be the image of the evaluation map

$$\varphi_E : H^0(X, E) \to \bigoplus_{i=1}^{n} E_{P_i} \cong \mathbb{F}_Q^n,$$

$$s \mapsto \big(s(P_1), s(P_2), \dots, s(P_n)\big).$$

Thus $C(X, \mathcal{P}, E)$ may be considered to be the most general class of AG codes defined so far. We notice that this code is not $\mathbb{F}_Q$-linear in general. However, as observed in [1,12], the decoding process is more efficient if we work over $\mathbb{F}_Q$.

The problem of determining the parameters of these codes is difficult in general. In [12], Savin introduced the notion of weakly stable bundles and gave a lower bound for the minimum distance of the codes defined by these bundles. He also proved an existence result of weakly stable bundles. In [11] we generalized the notion of weakly stable bundles of type α for a rational number α and gave a method of construction using finite coverings. A vector bundle E of rank $r \geqslant 2$ on a curve X is said to be a weakly stable bundle of type α if, for any sub-line bundle $L \subset E$, we have

$$\deg L \leqslant \frac{\deg E}{r} + \alpha.$$

In view of the results obtained in [11], the case $\alpha \leqslant 0$ is interesting for applications to coding theory, since we obtain better lower bounds for the minimum distance of $C(X, \mathcal{P}, E)$. On the other hand, a theorem of Mukai–Sakai states that α must satisfy the inequality $\alpha \geqslant -\frac{r-1}{r} g(X)$, where $g(X)$ denotes the genus of X. Since the right-hand side of this inequality becomes arbitrarily negative as $g(X)$ becomes large, we may ask whether the following weak converse to the theorem holds: Given an integer $r \geqslant 2$ and a rational number $\alpha \leqslant 0$, does there exist a constant g_0 such that, for any curve X of genus $g(X) \geqslant g_0$, there exists a vector bundle of rank r on X which is weakly stable of type α? In this paper we give a positive answer to the problem in the case of plane curves. To do this, we introduce the method exploiting the restriction of stable bundles on surfaces, which is based on the effective restriction theorem of A. Langer [7].

We are grateful to the referees for their valuable comments on the first draft of the present article.

2. Weakly stable vector bundles on curves

Let $\mathbb{F}_q$ be a finite field with q elements and let X be a projective variety of dimension $N \geqslant 1$ defined over $\mathbb{F}_q$, which is smooth and geometrically irreducible. Let $X(\mathbb{F}_q)$ denote the set of $\mathbb{F}_q$-rational points of X. Let $\mathcal{P} = \{P_1, P_2, \dots, P_n\}$ be a set of distinct $\mathbb{F}_q$-rational points of X. Let E be a vector bundle of rank r on X defined over $\mathbb{F}_q$. For a point $P \in \mathcal{P}$, let $\kappa(P)$ denote the residue field at P and let $E_P = E \otimes \kappa(P)$. We set $Q = q^r$ and we choose an isomorphism $\mathbb{F}_q^r \cong \mathbb{F}_Q$. For each i, we fix an isomorphism $E_{P_i} \cong \mathbb{F}_q^r \cong \mathbb{F}_Q$ as $\mathbb{F}_q$-vector spaces. Let

$$\varphi : H^0(X,E) \to \bigoplus_{i=1}^{n} E_{P_i} \cong \mathbb{F}_Q^n,$$
$$s \mapsto \big(s(P_1), s(P_2), \ldots, s(P_n)\big)$$

be the evaluation map. We define the code $C(X,\mathcal{P},E)$ to be the image of φ as an $\mathbb{F}_q$-vector space. In case $\mathcal{P} = X(\mathbb{F}_q)$, we write $C(X,\mathcal{P},E) = C(X,E)$. It should be noted that although $C(X,\mathcal{P},E)$ is an $\mathbb{F}_q$-subspace of $\bigoplus_{i=1}^n E_{P_i}$, it is not an $\mathbb{F}_Q$-subspace in general.

The length of $C(X,\mathcal{P},E)$ is equal to $n = \#\mathcal{P}$ and, following [12], we define the dimension of $C(X,\mathcal{P},E)$ to be the real number k given by

$$k = \log_{q^r} \#C(X,\mathcal{P},E).$$

Since $C(X,\mathcal{P},E)$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_Q^n$, the minimum distance d of $C(X,\mathcal{P},E)$ is given by

$$d = \min_{c \neq 0 \in C(X,\mathcal{P},E)} w(c).$$

Here $w(c)$ denotes the Hamming weight of c in $\mathbb{F}_Q^n$.

Assume that X is a curve. To determine the parameters of $C(X,\mathcal{P},E)$, we recall the notion of weak stability and its generalization as introduced in [12,11].

Let X be a smooth and irreducible projective curve defined over an algebraically closed field. Let E be a vector bundle of rank r on X. The degree of E is defined to be the degree of its determinant line bundle, that is, $\deg E := \deg(\det E)$. The slope of E is defined by

$$\mu(E) = \frac{\deg E}{r}.$$

E is said to be weakly stable if, for any sub-line bundle $L \subset E$, we have

$$\mu(L) \leqslant \mu(E).$$

We notice that the usual definition of semistability (respectively stability) is that, for any subbundle $F \subset E$ with $0 < \operatorname{rk} F < r$, we have

$$\mu(F) \leqslant \mu(E) \quad (\text{resp. } <).$$

Thus every semistable bundle is clearly weakly stable and the converse holds if $r = 2$. However, weakly stable bundles are not necessarily semistable if $r > 2$.

A generalization of the weak stability has been introduced in [11]. For a rational number $\alpha \leqslant 0$, E is said to be weakly stable of type α if, for any sub-line bundle $L \subset E$, we have

$$\mu(L) \leqslant \mu(E) + \alpha.$$

In case $\alpha < 0$, this notion is stronger than the weak stability of Savin.

Let X be a smooth and geometrically irreducible projective curve defined over $\mathbb{F}_q$ and E a vector bundle on X defined over $\mathbb{F}_q$. Let $\overline{X} = X \times \overline{\mathbb{F}}_q$ and $\overline{E}$ the base change of E to $\overline{X}$, where $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$. We say that E is weakly stable or weakly stable of type α if so is $\overline{E}$.

Generalizing the algorithm for interleaved AG codes given in [1], Savin proposed a decoding algorithm for weakly stable bundles [12]. The significance of the notion of weak stability of type α comes from the following result, which is proved in [11].

Proposition 2.1. *If E is a vector bundle which is weakly stable of type $\alpha \leqslant 0$ and $n > \mu(E) + \alpha$, then we have*

$$k = \frac{h^0(X, E)}{r},$$
$$d \geqslant n - \mu(E) - \alpha.$$

Using the code $C(X, E)$, Savin's algorithm can correct all ϵ errors with

$$\epsilon < \left\lfloor t^* - \frac{\alpha + g(X)}{2} \right\rfloor$$

where t^* is the designed correction capacity defined by

$$t^* = \left\lfloor \frac{n - \mu(E)}{2} \right\rfloor.$$

It follows from the proposition above that, for applications to coding theory, it is desirable to find vector bundles E which are weakly stable of type α with α as negative as possible. However, we notice that an explicit lower bound for α exists, in view of its relation to Segre invariants. We recall that the first Segre invariant $s_1(E)$ of E is the integer defined as follows:

$$s_1(E) = \deg E - r \max_{L \subset E} \deg L$$

where L varies over all sub-line bundles of E. By a theorem of Mukai–Sakai [8], we have the following upper bound for $s_1(E)$:

$$s_1(E) \leqslant (r - 1)g(X).$$

As a consequence, we obtain the following lower bound for α.

Proposition 2.2. *Let E be a vector bundle of rank $r \geqslant 2$, which is weakly stable of type $\alpha \leqslant 0$. Then*

$$\alpha \geqslant -\frac{(r - 1)g(X)}{r}.$$

Proof. Let $L \subset E$ be a sub-line bundle of maximal degree. Then

$$\deg L = \frac{\deg E - s_1(E)}{r} = \mu(E) - \frac{s_1(E)}{r} \leqslant \mu(E) + \alpha.$$

Hence the theorem of Mukai–Sakai yields

$$\alpha \geqslant -\frac{s_1(E)}{r} \geqslant -\frac{(r - 1)g(X)}{r}. \qquad \square$$

In the rest of this paper we give a method of constructing vector bundles which are weakly stable of type α for a given rational number $\alpha \leqslant 0$. For this purpose, we will need some results on stable vector bundles on algebraic surfaces.

3. Review of vector bundles on surfaces

In this section we give a brief review of the basic properties of vector bundles on algebraic surfaces which we need in the rest of this paper. We refer the reader to [3], [4, Appendix A] for general properties of Chow groups and Chern classes. Vector bundles on algebraic surfaces are treated in detail in [2,5].

Let S be a smooth projective surface defined over a field k. Since S is smooth, the sheaf of differentials Ω_S^1 on S is a vector bundle of rank two on S and the canonical bundle K_S is given by its determinant: $K_S = \det \Omega_S^1$. The tangent bundle T_S of S is by definition the dual bundle of Ω_S^1: $T_S = \Omega_S^\vee$.

For each integer $i \geqslant 0$, we denote by $A^i(S)$ the i-th Chow group which consists of cycles of codimension i on S modulo rational equivalence. $A^1(S)$ can be identified with the Picard group $\mathrm{Pic}(S)$ which consists of line bundles on X modulo isomorphism. A divisor on S is an element of the free abelian group generated by reduced irreducible closed subschemes of codimension one. We can associate a line bundle $\mathcal{O}_S(D)$ to a divisor D such that D is the zero-scheme of a section $s \in H^0(S, \mathcal{O}_S(D))$. The intersection theory on S gives a paring $\mathrm{Pic}(S) \times \mathrm{Pic}(S) \to \mathbb{Z}$. Thus we can define the intersection number $L \cdot M$ for $L, M \in \mathrm{Pic}(S)$ and $D \cdot D'$ for divisors D, D'.

For any vector bundle E on S and each integer $0 \leqslant i \leqslant 2$, the i-th Chern class $c_i(E) \in A^i(S)$ can be defined. The first Chern class of E is defined by $c_1(E) = c_1(\det E) \in \mathrm{Pic}(S)$. $c_i(E)$ for $i > 1$ is defined by the so-called splitting principle. Assume that E is the direct sum of line bundles: $E \cong L_1 \oplus \cdots \oplus L_r$. Then we have

$$1 + c_1(E) + c_2(E) = \bigl(1 + c_1(L_1)\bigr) \cdots \bigl(1 + c_1(L_r)\bigr).$$

For general vector bundle E, we can reduce to the above case using a filtration of E by subbundles E_i such that E_i/E_{i-1} are line bundles. Since we have $A^2(S) \cong \mathbb{Z}$, the second Chern class $c_2(E)$ can be identified with an integer.

Let

$$0 \to F \to E \to G \to 0$$

be an exact sequence of vector bundles on S. Then we have the following Whitney product formula:

$$c(E) = c(F) \cdot c(G)$$

where $c(E) = 1 + c_1(E) + c_2(E)$ denotes the total Chern class. This allows us to compute the Chern classes of the vector bundles obtained by an extension of two bundles. We may define the Chern classes of arbitrary coherent sheaf E by means of the locally free resolution: Let

$$0 \to E^n \to \cdots \to E^0 \to E \to 0$$

be an exact sequence of sheaves where E^i are vector bundles. Then the total Chern class of E is given by

$$c(E) = \prod_{i=0}^{n} c\bigl(E^i\bigr)^{(-1)^i}.$$

In addition to vector bundles on S, we have to consider torsion-free sheaves in the next section. If E is a torsion-free sheaf, then its double dual $E^{\vee\vee}$ is a vector bundle and there is a natural injection $E \hookrightarrow E^{\vee\vee}$ whose cokernel is a torsion sheaf supported on a finite set of points. Thus torsion-free sheaves may be considered as vector bundles with singularities. Let $Z \subset S$ be a 0-dimensional closed subscheme and let $\mathcal{I}_Z$ denote its ideal sheaf. The length $l(Z)$ of Z is defined to be the length of the torsion sheaf $\mathcal{O}_Z$. We have

$$c_1(E)=c_1\big(E^{\vee\vee}\big),\qquad c_2(E)=c_2\big(E^{\vee\vee}\big)+l\big(E^{\vee\vee}/E\big).$$

Thus, from the exact sequence

$$0\to\mathcal{I}_Z\to\mathcal{O}_S\to\mathcal{O}_Z\to 0,$$

we obtain

$$c_1(\mathcal{I}_Z)=0,\qquad c_2(\mathcal{I}_Z)=l(Z).$$

For a torsion-free sheaf E of rank r and a line bundle L on S, we have

$$\begin{aligned}&c_1(E\otimes L)=c_1(E)+rL,\\&c_2(E\otimes L)=c_2(E)+(r-1)c_1(E)\cdot L+\binom{r}{2}L^2.\end{aligned}$$

For a line bundle and a coherent sheaf E, we simply write the tensor product $E\otimes L$ as $E(L)$. Similarly, we write $E\otimes\mathcal{O}_S(D)$ as $E(D)$. The Chern classes of the twisted ideal sheaf $\mathcal{I}_Z(L)$ can be computed by the formula above as follows.

$$c_1\big(\mathcal{I}_Z(L)\big)=L,\qquad c_2\big(\mathcal{I}_Z(L)\big)=l(Z).$$

An important method of constructing the vector bundles on a surface is the elementary transformation. Let $D\subset S$ be a reduced and irreducible divisor with the inclusion $\iota: D\hookrightarrow S$. The restriction $E_{|D}$ of a vector bundle E on S to D is a bundle on D of degree $c_1(E)\cdot D$. For a vector bundle T of rank s on D, let $E_{|D}\to T$ be a surjection and let R denote its kernel. The kernel G of the composite map $E\to E_{|D}\to T$ is called the elementary transformation of E along T [5, p. 152]. G fits in the following exact sequences:

$$\begin{gathered}0\to G\to E\to\iota_*T\to 0,\\0\to E(-D)\to G\to\iota_*R\to 0.\end{gathered}$$

G has the following properties [5, Proposition 5.2.2].

Lemma 3.1. *G is a vector bundle on S of rank r with the Chern classes*

$$\begin{aligned}&c_1(G)=c_1(E)-sD,\\&c_2(G)=c_2(E)+\deg T+\frac{s(s-1)}{2}D^2-sc_1(E)\cdot D.\end{aligned}$$

In the case of rank two, there is another method of constructing vector bundles on a surface, called the Serre correspondence [5, Theorem 5.1.1]. This is well known in the case of algebraically closed fields. Since we need it on surfaces over finite fields, we state the result explicitly as follows.

Lemma 3.2. *Let S be a projective surface defined over $\mathbb{F}_q$ which is smooth and geometrically irreducible. Let Z be a 0-dimensional closed subscheme of S of length c defined over $\mathbb{F}_q$. Let L be a line bundle on S defined over $\mathbb{F}_q$ such that $|L + K_S| = \emptyset$. Then there exists an extension*

$$0 \to \mathcal{O}_S \to E \to \mathcal{I}_Z(L) \to 0$$

which defines a rank two bundle E defined over $\mathbb{F}_q$ with $c_1(E) = L$, $c_2(E) = c$.

Let S be a smooth, irreducible projective surface defined over an algebraically closed field k. Let E be a torsion-free sheaf of rank $r \geqslant 2$ on S. For an ample line bundle H on S, the H-slope of E is defined by

$$\mu_H(E) = \frac{c_1(E) \cdot H}{r}.$$

We recall that E of rank r is said to be H-semistable (respectively H-stable) if, for any coherent subsheaf $F \subset E$ with $0 < \operatorname{rk} F < r$, we have

$$\mu_H(F) \leqslant \mu_H(E) \quad (\text{resp. } <).$$

Assume that S is smooth and geometrically irreducible surface defined over $\mathbb{F}_q$ and that both H and E are defined over $\mathbb{F}_q$. Then E is said to be H-stable if the base change $\overline{E}$ is an $\overline{H}$-stable bundle over $\overline{S}$.

It is well known that every torsion-free sheaf E possesses a canonical filtration

$$0 = E_0 \subset E_1 \subset \cdots \subset E_{m-1} \subset E_m = E$$

such that the quotient sheaves $G_i := E_i/E_{i+1}$ are H-semistable torsion-free sheaves which satisfy

$$\mu_H(G_1) > \mu_H(G_2) > \cdots > \mu_H(G_{m-1}) > \mu_H(G_m).$$

Such filtration is said to be the Harder–Narasimhan filtration of E with respect to H [6], [5, p. 28]. $\mu_{\max}(E) = \mu_H(G_1)$ (resp. $\mu_{\min}(E) = \mu_H(G_m)$) are called the maximal (resp. minimal) slope of the filtration.

The discriminant $\Delta(E)$ of a torsion-free sheaf E of rank r and the Chern classes $c_i(E)$ is the integer defined as follows [5, p. 79].

$$\Delta(E) = 2rc_2(E) - (r-1)c_1(E)^2.$$

If E is a vector bundle, we have $\Delta(E) = c_2(\mathcal{E}nd\, E)$ where $\mathcal{E}nd\, E := E \otimes E^\vee$ denotes the endomorphism bundle of E. The invariant $\Delta(E)$ is significant in studying the stability properties of the sheaf E. For example, in case the characteristic of k is zero, every H-semistable torsion-free sheaf E satisfies the well-known Bogomolov inequality [5, Theorem 7.3.1]:

$$\Delta(E) \geqslant 0.$$

Although the Bogomolov inequality does not hold any more if the characteristic of k is $p > 0$, certain lower bound for $\Delta(E)$ exists. To state this, we choose a nef divisor A on S such that $T_S(A)$ is globally generated. Given integer r, let β_r be the number defined by

$$\beta_r = \left(\frac{r(r-1)}{p-1} A \cdot H\right)^2.$$

By [7, Theorem 5.1], we have the following result.

Lemma 3.3. *Assume that S is a smooth and irreducible projective surface defined over an algebraically closed field of characteristic $p > 0$. For any torsion-free sheaf E of rank r on S, we have*

$$\Delta(E) + r^2\big(\mu_{\max}(E) - \mu_H(E)\big)\big(\mu_H(E) - \mu_{\min}(E)\big) + \beta_r \geqslant 0.$$

4. Weakly stable bundles via restriction from surfaces

Let S be a smooth and irreducible projective surface defined over an algebraically closed field of characteristic $p > 0$. We explain a method of constructing weakly stable bundles of type α via restriction of stable bundles on S. Let $X \subset S$ be a smooth irreducible curve and let E be a stable vector bundle on S. We are interested in the weak stability of $E_{|X}$. We prove a restriction theorem for stable bundles on surfaces in positive characteristic, which is a modification of a result of A. Langer [7, Theorem 5.2]. We choose a nef divisor A on S such that $T_S(A)$ is globally generated and define the number β_r as in the previous section. Assume that X is linearly equivalent to lH for a very ample divisor H on S and a positive integer l. The following result states that any H-stable bundle on S restricts to a weakly stable bundle on X if l is sufficiently large.

Proposition 4.1. *Let S be a smooth and irreducible projective surface defined over an algebraically closed field of characteristic $p > 0$ and H a very ample divisor on S. Let E be an H-stable vector bundle of rank $r \geqslant 2$ on S. Let $\alpha \leqslant 0$ be a rational number and let l be an integer with*

$$l \geqslant \frac{r-1}{rH^2}\left(H^2\Delta(E) - 2rH^2\alpha + \frac{1}{(r-1)^2} + 2r(r-1)\beta_r\right).$$

Then, for any smooth irreducible curve $X \in |lH|$, the restriction $E_{|X}$ of E to X is a vector bundle which is weakly stable of type α.

Proof. Assume that there exists a smooth and irreducible curve $X \in |lH|$ such that $E_{|X}$ is not weakly stable of type α and let $\iota : X \hookrightarrow S$ be the inclusion. Then, there exists a maximal sub-line bundle $L \subset E_{|X}$ satisfying $\deg L > \mu(E_{|X}) + \alpha$. Then the quotient $T = E_{|X}/L$ is torsion-free, hence locally free and has $\operatorname{rk} T = r - 1$ and $\deg T = c_1(E) \cdot X - \deg L$. Hence

$$r \deg T - (r-1)c_1(E) \cdot X < -r\alpha.$$

Let G denote the elementary transformation of E along T. By Lemma 3.1, we compute

$$\begin{aligned}\Delta(G) &= \Delta(E) - (r-1)X^2 + 2\big(r\deg T - (r-1)c_1(E)\cdot X\big)\\ &< \Delta(E) - (r-1)H^2l^2 - 2r\alpha.\end{aligned}$$

Claim: We have the following inequalities.

$$\begin{aligned}\mu_{\max}(G) - \mu_H(G) &\leqslant \frac{r-1}{r}H^2l - \frac{1}{r(r-1)},\\ \mu_H(G) - \mu_{\min}(G) &\leqslant \frac{1}{r}H^2l - \frac{1}{r(r-1)}.\end{aligned}$$

To prove the claim, let

$$0 = G_0 \subset G_1 \subset \cdots \subset G_{m-1} \subset G_m = G$$

be the Harder–Narasimhan filtration of G. If G is H-semistable, we have $\mu_{\max}(G) = \mu_H(G)$. In this case the claim is clear since $\frac{r-1}{r}H^2 l - \frac{1}{r(r-1)} \geqslant 0$ for $r \geqslant 2$. Assume that G is not H-semistable and let $s = \operatorname{rk} G_1$. Since G_1 is a subsheaf of E which is H-stable, we have

$$\mu_{\max}(G) = \mu_H(G_1) = \frac{c_1(G_1)\cdot H}{s} < \mu_H(E) = \frac{c_1(E)\cdot H}{r}$$

which yields $rc_1(G_1)\cdot H \leqslant sc_1(E)\cdot H - 1$. Hence

$$\mu_{\max}(G) \leqslant \mu_H(E) - \frac{1}{rs} \leqslant \mu_H(E) - \frac{1}{r(r-1)}.$$

Thus the first inequality follows. To prove the second inequality, we consider the quotient sheaf $E(-X) \to Q$ induced from the projection $G \to G/G_{m-1}$ and use the stability of $E(-X)$. This proves the claim.

Applying Lemma 3.3 to G, we obtain

$$\begin{aligned}
-2r(r-1)\beta_r &\leqslant H^2\Delta(G) + r^2\bigl(\mu_{\max}(G) - \mu_H(G)\bigr)\bigl(\mu_H(G) - \mu_{\min}(G)\bigr) \\
&< H^2\Delta(E) - (r-1)\bigl(H^2\bigr)^2 l^2 - 2rH^2\alpha \\
&\quad + r^2\left(\frac{r-1}{r}H^2 l - \frac{1}{r(r-1)}\right)\left(\frac{1}{r}H^2 l - \frac{1}{r(r-1)}\right) \\
&= H^2\Delta(E) - 2rH^2\alpha - \frac{r}{r-1}H^2 l + \frac{1}{(r-1)^2}.
\end{aligned}$$

Thus

$$l < \frac{r-1}{rH^2}\left(H^2\Delta(E) - 2rH^2\alpha + \frac{1}{(r-1)^2} + 2r(r-1)\beta_r\right).$$

However, this contradicts the assumption on l. Hence the proposition has been proved. □

Lemma 4.2. *Let S, H and E be as above. Let $X \in |lH|$ be a smooth curve which is geometrically irreducible. Assume that E is H-stable and that $E_{|X}$ is weakly stable of type α. Assume that*

$$X\cdot H \geqslant \mu_H(E) \quad \textit{and} \quad n > \mu(E_{|X}) + \alpha.$$

Then the dimension k of the code $C(X, E_{|X})$ satisfies

$$k \geqslant \frac{h^0(S,E)}{r}.$$

If we assume further $H^1(S, E(-X)) = 0$, then the equality holds.

Proof. We consider the following exact sequence on S.

$$0 \to E(-X) \to E \to E_{|X} \to 0.$$

It follows from the assumptions that $H^0(S, E(-X)) = 0$ since $\mu_H(E(-X)) \leqslant 0$ and $E(-X)$ is H-stable. Thus the induced cohomology sequence shows that we have the inclusion $H^0(S, E) \subset H^0(X, E_{|X})$. Hence, by Proposition 2.1, the dimension k of $C(X, E_{|X})$ satisfies

$$k = \frac{h^0(X, E_{|X})}{r} \geqslant \frac{h^0(S, E)}{r}$$

and the equality holds, if further we have $H^1(S, E(-X)) = 0$. □

Remark 4.3. For fixed r, we have $H^0(\widetilde{E}(-l)) = 0$ for any stable bundles $\widetilde{E}$ of rank r and $c_1(\widetilde{E}) = 1$ on $\mathbb{P}^2$ for sufficiently large l. Hence the code $C(X, E)$ has dimension $k = \frac{r-1}{r}$ for $l \gg 0$.

5. AG codes on projective plane curves

We apply the results in the previous section to $S = \mathbb{P}^2$ and the tautological line bundle $H = \mathcal{O}_{\mathbb{P}^2}(1)$. To do this, we first prove the existence of stable bundles on $\mathbb{P}^2$. Since $\mathrm{Pic}(\mathbb{P}^2)$ is generated by $\mathcal{O}_{\mathbb{P}^2}(1)$, one may identify the line bundle $\mathcal{O}_{\mathbb{P}^2}(m)$ on $\mathbb{P}^2$ with the integer m. For a coherent sheaf E on $\mathbb{P}^2$, we write $E \otimes \mathcal{O}_{\mathbb{P}^2}(m)$ as $E(m)$.

Lemma 5.1. *For any $c > 0$, there exists a 0-dimensional closed subscheme $Z \subset \mathbb{P}^2$ of length c defined over $\mathbb{F}_q$, which consists of c distinct points.*

Proof. This is obvious since, choosing any line $\mathbb{P}^1 \subset \mathbb{P}^2$ defined over $\mathbb{F}_q$, we can always find c distinct points $P_i \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ $(1 \leqslant i \leqslant c)$ such that the cycle $Z := P_1 + P_2 + \cdots + P_c$ is invariant under the Frobenius map, hence is defined over $\mathbb{F}_q$. □

Lemma 5.2. *Let $\mathbb{P}^2$ be the projective plane defined over an algebraically closed field. Let Q be an H-stable torsion-free sheaf of rank $r - 1 \geqslant 1$ on $\mathbb{P}^2$ with $c_1(Q) = 1$ and $c_2(Q) = c$. Let E be a sheaf which sits in the non-split extension*

$$0 \to \mathcal{O}_{\mathbb{P}^2} \to E \to Q \to 0.$$

Then E is an H-stable torsion-free sheaf of rank r with $c_1(E) = 1$ and $c_2(E) = c$.

Proof. This in fact follows from the proof of [10, Lemma 1.4]. We give a proof for the sake of completeness. If E were not stable, then we would obtain a semistable subsheaf $F \subset E$ with $\mu(F) \geqslant \mu(E)$. Let $f : F \hookrightarrow E \to Q$ denote the composite map. We see that f cannot be trivial, for otherwise we would have a non-trivial map $F \to \mathcal{O}_{\mathbb{P}^2}$, which is impossible since F is semistable and $\mu(F) > 0$. Thus the image $\overline{F}$ of f is a non-trivial subsheaf of Q, which satisfies $\mu(\overline{F}) \geqslant \mu(F)$. In case $\mathrm{rk}\,\overline{F} < \mathrm{rk}\,Q$, then the stability of Q yields $\mu(\overline{F}) < \mu(Q)$ which is a contradiction. Hence we must have $\mathrm{rk}\,\overline{F} = \mathrm{rk}\,Q = r - 1$. Then we see that $\mathrm{rk}\,\overline{F} = \mathrm{rk}\,F$ and f is generically surjective. Since E is torsion-free, f has trivial kernel and hence $F \cong \overline{F}$. Let T denote the cokernel of f, which is a torsion sheaf. If T has support of codimension one, then we obtain $c_1(T) \cdot H > 0$, which yields $c_1(F) \cdot H = (c_1(E) - c_1(T)) \cdot H \leqslant 0$. However this contradicts the assumption $\mu(F) \geqslant \mu(E) > 0$. Hence we conclude that T has support of codimension two.

The exact sequence

$$0 \to F \to Q \to T \to 0$$

induces the exact sequence

$$\cdots \to \mathrm{Ext}^1(T, \mathcal{O}_{\mathbb{P}^2}) \to \mathrm{Ext}^1(Q, \mathcal{O}_{\mathbb{P}^2}) \to \mathrm{Ext}^1(F, \mathcal{O}_{\mathbb{P}^2}) \to \cdots.$$

Let $e \in \operatorname{Ext}^1(Q, \mathcal{O}_{\mathbb{P}^2})$ denote the class corresponding to the sequence defining E. Since $F \cong \overline{F}$, e maps to zero in $\operatorname{Ext}^1(F, \mathcal{O}_{\mathbb{P}^2})$. This implies that $e = 0$ since T has support of codimension two and hence $\operatorname{Ext}^1(T, \mathcal{O}_{\mathbb{P}^2}) = 0$. It follows that the original short exact sequence splits, which contradicts the assumption. Therefore we conclude that E is H-stable with the claimed invariants. □

We have the following result concerning the existence of stable bundles E on $\mathbb{P}^2$ with $c_1(E) = 1$ defined over $\mathbb{F}_q$.

Proposition 5.3. *For all $r \geqslant 2$ and all $c \geqslant r$, there exists a stable bundle $E_{r,c}$ on $\mathbb{P}^2$ defined over $\mathbb{F}_q$, of rank r, $c_1(E_{r,c}) = 1$ and $c_2(E_{r,c}) = c$. Further we have $h^0(E_{r,c}) \geqslant r - 1$ and $\dim \operatorname{Ext}^1(E_{r,c}, \mathcal{O}_{\mathbb{P}^2}) = c - r + 1$.*

Proof. We prove the proposition by induction on r. By Lemma 5.1, for any $c \geqslant 1$, we may choose a 0-dimensional subscheme Z of length c defined over $\mathbb{F}_q$ such that the support consists of c distinct points. We have $|\mathcal{O}_{\mathbb{P}^2}(1) + K_{\mathbb{P}^2}| = |\mathcal{O}_{\mathbb{P}^2}(-2)| = \emptyset$, hence by Lemma 3.2, there exists a rank two bundle $E_{2,c}$ which fits in a non-split extension

$$0 \to \mathcal{O}_{\mathbb{P}^2} \to E_{2,c} \to \mathcal{I}_Z(1) \to 0$$

and we have $h^0(E_{2,c}) \geqslant 1$, $c_1(E_{2,c}) = 1$ and $c_2(E_{2,c}) = c$. Further $E_{2,c}$ is H-stable by Lemma 5.2 since $\mathcal{I}_Z(1)$ is a rank one torsion-free sheaf, which is stable by definition. Taking $\operatorname{Hom}(\,, \mathcal{O}_{\mathbb{P}^2})$ of the sequence above, we obtain the exact sequence

$$\cdots \to \operatorname{Hom}(E_{2,c}, \mathcal{O}_{\mathbb{P}^2}) \to \operatorname{Hom}(\mathcal{O}_{\mathbb{P}^2}, \mathcal{O}_{\mathbb{P}^2}) \to \operatorname{Ext}^1\bigl(\mathcal{I}_Z(1), \mathcal{O}_{\mathbb{P}^2}\bigr) \to \operatorname{Ext}^1(E_{2,c}, \mathcal{O}_{\mathbb{P}^2}) \to \cdots.$$

We have $\operatorname{Ext}^1(\mathcal{O}_{\mathbb{P}^2}, \mathcal{O}_{\mathbb{P}^2}) = 0$ and $\operatorname{Hom}(E_{2,c}, \mathcal{O}_{\mathbb{P}^2}) = 0$ since $E_{2,c}$ is stable. Hence the sequence above yields $\dim \operatorname{Ext}^1(E_{2,c}, \mathcal{O}_{\mathbb{P}^2}) = \dim \operatorname{Ext}^1(\mathcal{I}_Z(1), \mathcal{O}_{\mathbb{P}^2}) - 1$. On the other hand, we have $\operatorname{Ext}^1(\mathcal{I}_Z(1), \mathcal{O}_{\mathbb{P}^2}) \cong H^1(\mathcal{I}_Z(-2))^\vee$ by Serre duality. Since we have the exact sequence

$$0 \to \mathcal{I}_Z(-2) \to \mathcal{O}_{\mathbb{P}^2}(-2) \to \mathcal{O}_Z(-2) \to 0,$$

the induced cohomology sequence gives $H^1(\mathcal{I}_Z(-2)) \cong H^0(\mathcal{O}_Z(-2)) \cong \mathbb{F}_q^{\oplus c}$. Hence $\dim \operatorname{Ext}^1(E_{2,c}, \mathcal{O}_{\mathbb{P}^2}) = c - 1$ and the claim is true for $r = 2$.

Assume that the claim holds up to $r - 1$. Then, for any $c \geqslant r - 1$, there exists an H-stable bundle $E_{r-1,c}$ satisfying $h^0(E_{r-1,c}) = r - 2$ and $\dim \operatorname{Ext}^1(E_{r-1,c}, \mathcal{O}_{\mathbb{P}^2}) = c - r + 2$. In particular, for any $c \geqslant r$, we have $\dim \operatorname{Ext}^1(E_{r-1,c}, \mathcal{O}_{\mathbb{P}^2}) > 0$. Hence there exists a non-split extension

$$0 \to \mathcal{O}_{\mathbb{P}^2} \to E_{r,c} \to E_{r-1,c} \to 0.$$

The bundle $E_{r,c}$ is H-stable by Lemma 5.2 again and $\operatorname{rk} E_{r,c} = r$, $c_1(E_{r,c}) = 1$ and $c_2(E_{r,c}) = c$. Considering the induced cohomology sequence, we obtain $h^0(E_{r,c}) = h^0(E_{r-1,c}) + 1 \geqslant r - 1$ and $\dim \operatorname{Ext}^1(E_{r,c}, \mathcal{O}_{\mathbb{P}^2}) = \dim \operatorname{Ext}^1(E_{r-1,c}, \mathcal{O}_{\mathbb{P}^2}) - 1 = c - r + 1$. Hence the claim is true for r. This completes the proof. □

Theorem 5.4. *Let X be a plane curve of degree l defined over $\mathbb{F}_q$, which is smooth and geometrically irreducible and let $n = \#X(\mathbb{F}_q)$. Let $r \geqslant 2$ be an integer and $\alpha \leqslant 0$ a rational number. Assume that*

$$n > \frac{l}{r} + \alpha \quad \textit{and} \quad l \geqslant \frac{r-1}{r}\left(2r^2 - (r-1) - 2r\alpha + \frac{1}{(r-1)^2}\right).$$

Then there exists a vector bundle E of rank r on X which defines the code $C(X, E)$ with the parameters

$$k \geqslant \frac{r-1}{r},$$
$$d \geqslant n - \frac{l}{r} - \alpha.$$

Using the code $C(X,E)$, the algorithm of Savin decodes all ϵ errors with

$$\epsilon < \left\lfloor t^* - \frac{2\alpha + (l-1)(l-2)}{4} \right\rfloor.$$

Proof. We let $\widetilde{E} := E_{r,r}$ in Proposition 5.3. Then $\operatorname{rk}\widetilde{E} = r$, $c_1(\widetilde{E}) = 1$ and $c_2(\widetilde{E}) = r$. We know that $T_{\mathbb{P}^2}$ is generated by global sections since it fits in the Euler sequence

$$0 \to \mathcal{O}_{\mathbb{P}^2} \to \mathcal{O}_{\mathbb{P}^2}(1)^{\oplus 3} \to T_{\mathbb{P}^2} \to 0.$$

Hence we have $\beta_r = 0$ by choosing $A = 0$ in the definition of β_r. Applying Proposition 4.1 to $\widetilde{E}$ and $H = \mathcal{O}_{\mathbb{P}^2}(1)$, we conclude that $E := \widetilde{E}_{|X}$ is weakly stable of type α if

$$l \geqslant \frac{r-1}{r}\left(\Delta(\widetilde{E}) - 2r\alpha + \frac{1}{(r-1)^2}\right) = \frac{r-1}{r}\left(2r^2 - (r-1) - 2r\alpha + \frac{1}{(r-1)^2}\right).$$

Since we have

$$X \cdot H = l \geqslant \mu_H(\widetilde{E}) = \frac{1}{r} \quad \text{and} \quad n > \mu(E) = \frac{l}{r} + \alpha,$$

the code $C(X,E)$ defined by E has the desired properties by Proposition 2.1 and Lemma 4.2. □

Example 5.5. Let X denote the Hermitian curve defined by the equation $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$. It is known that $n = \#X(\mathbb{F}_{q^2}) = q^3 + 1$. Assume that q, r and $\alpha \leqslant 0$ satisfy

$$q + 1 \geqslant \frac{r-1}{r}\left(2r^2 - (r-1) - 2r\alpha + \frac{1}{(r-1)^2}\right).$$

Then Theorem 4.3 yields the code $C(X,E)$ with the parameters

$$k \geqslant \frac{r-1}{r},$$
$$d \geqslant q^3 + 1 - \frac{q+1}{r} - \alpha.$$

We can decode by $C(X,E)$ all ϵ errors with

$$\epsilon < \left\lfloor t^* - \frac{2\alpha + q(q-1)}{4} \right\rfloor.$$

We may also construct the codes which always have dimension $k > 1$ exploiting bundles of different type.

Theorem 5.6. *Let X, n be as in Theorem* 5.4. *Let $r \geqslant 2$ be an integer and $\alpha \leqslant 0$ a rational number. For a positive integer m, let*

$$r_m = \frac{m(m+3)}{2}.$$

Assume that

$$n > \frac{lm}{r_m} + \alpha \quad \textit{and} \quad l \geqslant \frac{r_m - 1}{r_m}\left((r_m+1)m^2 - 2r_m\alpha + \frac{1}{(r_m-1)^2}\right).$$

Then there exists a bundle E_m on X which defines the code $C(X, E_m)$ with the parameters

$$k \geqslant \frac{r_m+1}{r_m},$$
$$d \geqslant n - \frac{ml}{r_m} - \alpha.$$

Proof. For any positive integer m, the line bundle $\mathcal{O}_{\mathbb{P}^2}(m)$ is globally generated. Hence the evaluation map

$$\varphi_m : H^0\big(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(m)\big) \otimes \mathcal{O}_{\mathbb{P}^2} \to \mathcal{O}_{\mathbb{P}^2}(m)$$

is surjective. We denote by $\widetilde{E}_m$ the dual of the kernel of φ_m. Then $\widetilde{E}_m$ is a vector bundle defined over $\mathbb{F}_q$ which fits in the exact sequence

$$0 \to \mathcal{O}_{\mathbb{P}^2}(-m) \to H^0\big(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(m)\big)^\vee \otimes \mathcal{O}_{\mathbb{P}^2} \to \widetilde{E}_m \to 0.$$

From this sequence we obtain

$$\operatorname{rk}\widetilde{E}_m = h^0\big(\mathcal{O}_{\mathbb{P}^2}(m)\big) - 1 = (m+2)(m+1)/2 - 1 = r_m$$

and $c_1(\widetilde{E}_m) = m$ and $c_2(\widetilde{E}_m) = m^2$. The sequence above induces an isomorphism $H^0(\widetilde{E}_m) \cong H^0(\mathcal{O}_{\mathbb{P}^2}(m))^\vee$ since $H^i(\mathcal{O}_{\mathbb{P}^2}(-m)) = 0$ for $i \leqslant 1$ and all $m > 0$. Hence we obtain $h^0(\widetilde{E}_m) = r_m + 1$. Furthermore it has been proved that $\widetilde{E}_m$ is an $\mathcal{O}_{\mathbb{P}^2}(1)$-stable bundle on $\mathbb{P}^2$ [13, Proposition 2.1]. By Proposition 4.1, $E_m := \widetilde{E}_{m|X}$ is weakly stable of type α if

$$l \geqslant \frac{r_m-1}{r_m}\left(\Delta(\widetilde{E}_m) - 2r_m\alpha + \frac{1}{(r_m-1)^2}\right) = \frac{r_m-1}{r_m}\left((r_m+1)m^2 - 2r_m\alpha + \frac{1}{(r_m-1)^2}\right).$$

Then the bundle E_m has the required properties as before. □

References

[1] A. Brown, L. Minder, M.A. Shokrollahi, Improved Decoding of Interleaved AG Codes, Lecture Notes in Comput. Sci., vol. 3796, Springer, 2005, pp. 37–46.

[2] R. Friedman, Algebraic Surfaces and Holomorphic Vector Bundles, Springer-Verlag, 1998.

[3] W. Fulton, Intersection Theory, Springer-Verlag, 1984.

[4] R. Hartshorne, Algebraic Geometry, Springer-Verlag, 1977.

[5] D. Huybrechts, M. Lehn, The Geometry of Moduli Spaces of Sheaves, second ed., Cambridge University Press, 2010.

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

[7] A. Langer, Semistable sheaves in positive characteristic, Ann. of Math. 159 (2004) 251–276.

[8] S. Mukai, F. Sakai, Maximal subbundles of vector bundles on a curve, Manuscripta Math. 52 (1985) 25–256.

[9] Y.I. Manin, S.G. Vladut, Linear codes and modular curves, J. Soviet Math. 30 (1985) 2611–2643.

[10] T. Nakashima, Reflection of sheaves on a Calabi–Yau variety, Asian J. Math. 6 (2002) 567–577.

[11] T. Nakashima, AG codes from vector bundles, Des. Codes Cryptogr. 57 (2010) 107–115.

[12] V. Savin, Algebraic–geometric codes from vector bundles and their decoding, arXiv:0803.1096 [math].

[13] V. Trivedi, Semistability of syzygy bundles on projective spaces in positive characteristic, arXiv:0804.0547 [math].