International Journal of Pure and Applied Mathematics

Volume 18 No. 4 2005, 495-499

A REMARK ON ERROR-CORRECTING CODES FROM RULED SURFACES

E. Ballico[1 §], Claudio Fontanari[2]

[1,2]Department of Mathematics
University of Trento
380 50 Povo (Trento) - Via Sommarive, 14, ITALY
[1]e-mail: ballico@science.unitn.it
[2]e-mail: fontanar@science.unitn.it

Abstract: This short note offers a contribution to the theory of error-correcting codes from higher dimensional projective varieties along the lines of [5]. By applying standard vector bundles techniques, we complete the classification of codes from ruled surfaces over elliptic curves left open in [8]. In particular, we disprove the naive conjecture that higher degree vector bundles should provide better codes.

AMS Subject Classification: 94B50
Key Words: error-correcting codes, vector bundles, ruled surfaces

1. Introduction

The interest in error-correcting codes arising from algebraic geometry has been constantly increasing since the early eighties, when Goppa (see [4]) generalized Reed-Solomon codes to codes on algebraic curves and Tsfasman, Vlăduţ, and Zink (see [9]) constructed Goppa codes overcoming the Varshamov-Gilbert bound. In order to obtain good codes from algebraic curves, the standard strategy is looking for curves with a lot of rational points; since it is easier to find rational points on a higher dimensional variety, it seems rather promising to construct error-correcting codes starting from a projective surface instead of a curve. A serious attempt in this direction is contained in the paper [5], which establishes some basic results and collects several nice examples. In particu-

Received: January 5, 2005

§Correspondence author

lar, Proposition 4.2 in [5] provides the set-up for constructing codes from ruled surfaces. As it is well-known (see for instance [7], V, Proposition 2.8), a ruled surface is the projectivization of a normalized rank two vector bundle of degree d on a smooth curve of genus g. For $g = 0$, the resulting error-correcting codes are explicitly classified in [8], Theorem 5.2.1; [8] contains also a complete discussion of the case $g = 1$, $d = 0$, but the case $g = 1$, $d = 1$ is left open. However, Conclusion 5.5 in [8] points out that since in degree 0 the code is comparable to the corresponding product code, in degree 1 the code is expected to be as good as or even better than the product code. The aim of the present note is indeed a full clarification of this delicate matter. First of all, we perform a computation of the number of independent sections of certain vector bundles over an elliptic curve (see Lemma 1). Next, by applying this tool we obtain the lacking classification in the degree 1 case (see Theorem 1). Finally, a closer inspection to the parameters disproves the above conjecture: it turns out that no better codes arise in degree 1 (see Proposition 1).

We work over a finite field $\mathbb{F}_q$ of characteristic p.

2. The Results

We are going to make a free use of standard definitions and notations from algebraic geometry (see [7]).

Lemma 1. *Let C be a smooth elliptic curve and let $P \in C$ be a point. If E is an ample vector bundle on C of degree d and rank r, then we have*

$$h^0(C, \mathrm{Symm}^a(E) \otimes \mathcal{O}_C(bP)) = \binom{r+a-1}{r-1}(a\mathfrak{d}r + b)$$

for every $a \geq 0$, $b \geq 0$.

Proof. Since E is ample and $b \geq 0$, from [2], Theorem 3.3, it follows that $\mathrm{Symm}^a(E) \otimes \mathcal{O}_C(bP)$ is ample, in particular $h^0(C, (\mathrm{Symm}^a(E) \otimes \mathcal{O}_C(bP))^\vee) = 0$. Hence by applying Serre duality and Riemann-Roch we deduce

$$h^0(C, \mathrm{Symm}^a(E) \otimes \mathcal{O}_C(bP)) = \deg(\mathrm{Symm}^a(E) \otimes \mathcal{O}_C(bP)).$$

Recall now that the slope of a vector bundle F is by definition $\mu(F) := \frac{\deg(F)}{\mathrm{rank}\,(F)}$, so we have

$$\deg(\mathrm{Symm}^a(E) \otimes \mathcal{O}_C(bP)) = \binom{r+a-1}{r-1}\mu(\mathrm{Symm}^a(E) \otimes \mathcal{O}_C(bP)).$$

On the other hand, by additivity

$$\mu(\mathrm{Symm}^a(E) \otimes \mathcal{O}_C(bP)) = \mu(\mathrm{Symm}^a(E)) + \deg(\mathcal{O}_C(bP)) = a\frac{d}{r} + b.$$

By putting everyting together, we obtain the result. □

We recall that a $[n, k, d]$ code is a k-dimensional linear subspace V of $\mathbb{F}_q^n$ such that

$$d = \min |\{v_i \neq 0 : (v_1, \dots, v_n) \in V \setminus \{0\}\}|.$$

By definition, the *information rate* of the code is $R := \frac{k}{n}$ and its *error correcting capability* is $\delta := \frac{d}{n}$.

Theorem 1. *Let C be a smooth elliptic curve over $\mathbb{F}_q$ with $\gamma > 0$ rational points. Let a, b integers with $0 < a + b < \gamma$, $0 \leq a < q + 1$. Then from any indecomposable rank two vector bundle of degree 1 over C we can construct $[n, k, d]$ codes with parameters:*

$$\begin{aligned} n &= (q+1)\gamma\,, \\ k &= (a+1)\left(\frac{a}{2} + b\right)\,, \\ d &\geq (q+1-a)(\gamma - a - b). \end{aligned}$$

Proof. Let E be an indecomposable rank two vector bundle over C of degree 1 (notice that E has always a global section; moreover, by [1], Corollary to Theorem 7, E is uniquely determined up to tensor product with a line bundle of degree 0). By [6] or [3], we know that E is ample. Hence from [5], Proposition 4.2, it follows that for $l := a + b < \gamma$ there are $[n, k, d]$ codes with parameters:

$$\begin{aligned} n &= (q+1)\gamma\,, \\ k &= h^0(C, \mathrm{Symm}^a(E) \otimes \mathcal{O}_C(bP))\,, \\ d &\geq n - (\gamma - l)a - (q+1)l\,. \end{aligned}$$

By Lemma 1, we have $k = (a+1)\left(\frac{a}{2} + b\right)$, and by substituting $n = (q+1)\gamma$ and $l = a + b$ we obtain $d \geq (q + 1 - a)(\gamma - a - b)$. Finally, notice that the numerical assumptions imply that the bound on d is positive. □

We call *Lomont codes* the codes constructed in [8], Theorem 5.4.3, starting from an indecomposable rank two vector bundle of degree 0 over an elliptic curve.

Proposition 1. *Let C be a smooth elliptic curve over $\mathbb{F}_q$ with $\gamma > 0$ rational points. Then for every code from Theorem 1 there is a Lomont* *code defined over C having the same error correcting capability and higher information rate.*

Proof. Let a, b the integers corresponding to a fixed $[n, k, d]$ code from Theorem 1 and set $a_0 := a$, $b_0 := a + b$. By assumption, we have $0 < b_0 < \gamma$, $0 \leq a_0 < q + 1$. Hence by [8], Theorem 5.4.3, there is a Lomont code with parameters:

$$\begin{aligned} n_0 &= (q+1)\gamma = n\,, \\ k_0 &= (a+1)(a+b) \geq k\,, \\ d_0 &\geq (q+1-a)(\gamma - b_0) = d\,. \end{aligned}$$

Therefore $\delta_0 = \delta$ and $R_0 \geq R$, so the proof is over. □

References

[1] M.F. Atiyah, Vector bundles over an elliptic curve, *Proc. London Math. Soc.*, **7**, No. 3 (1957), 414-452.

[2] C.M. Barton, Tensor products of ample vector bundles in characteristic p, *Amer. J. Math.*, **93** (1971), 429-438.

[3] D. Gieseker, p-ample bundles and their Chern classes, *Nagoya Math. J.*, **43** (1971), 91-116.

[4] V.D. Goppa, Codes on algebraic curves, *Dokl. Akad. Nauk SSSR*, **259** (1981), 1289-1290, In Russian.

[5] S.H. Hansen, Error-correcting codes from higher-dimensional varieties, *Finite Fields Appl.*, **7** (2001), 531-552.

[6] R. Hartshorne, Ample vector bundles on curves, *Nagoya Math. J.*, **43** (1971), 73-89.

[7] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, **52**, Springer-Verlag, New York-Heidelberg (1977).

[8] C. Lomont, Error correcting codes on algebraic surfaces, math. NT/0309123 (2003).

[9] M.A. Tsfasman, S.G. Vlăduţ, T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.*, **109** (1982), 21-28.