International Journal of Pure and Applied Mathematics

Volume 15 No. 1 2004, 51-56

EVALUATION CODES ON RULED VARIETIES

E. Ballico

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

Abstract: Let C be a smooth projective curve over $GF(q)$ and E a vector bundle on C defined over $GF(q)$. Here we compute the parameters of the evaluation codes obtained from line bundles on the rule variety $X := \mathbf{P}(E)$.

AMS Subject Classification: 14G50, 14H60
Key Words: ruled varieties, evaluation codes, linear codes, vector bundles on curves, p-semistability, finite field nullstellensatz

1. Evaluation Codes Using Vector Bundles

Let C be a smooth projective curve over $GF(q)$ and E a vector bundle on C defined over $GF(q)$. Here we compute the parameters of the evaluation codes obtained from line bundles on the rule variety $X := \mathbf{P}(E)$. Such codes were studied for certain very special ruled surfaces in [4]. For background on vector bundles on curves and the notion of semistability, see [6]. Here is our main result; here $\mu(E) := \deg(E)/\mathrm{rank}(E)$; for the definition of the line bundle $L_{a,R}$, see Section 2.

Theorem 1. *Let C be a smooth and geometrically connected curve of genus g defined over $GF(q)$ and E a rank r p-semistable vector bundle on C defined over $GF(q)$. Set $X := \mathbf{P}(E)$ and $\bar{n} := \mathrm{card}(C(q))$. Fix integers a and b and $R \in \mathrm{Pic}^b(C)$. Set $m := \bar{n}\binom{a+r-1}{r-1}$. Assume $0 \leq a \leq q$. There is $S \subseteq X(q)$ with $\mathrm{card}(S(q)) = m$ and with the following properties. Let*

Received: May 5, 2004

$\phi_{L_{a,R,S}} : H^0(X, L_{a,R}) \to GF(q)^m$ be the evaluation map at the points of S. If $a\mu(E) + b < \bar{n}$, then $\phi_{L_{a,R,S}}$ is injective and hence it defines an $h^0(C, S^a(E) \otimes R) \times m$ linear code $C(E, L_{a,R}, S)$. The code $C(E, L_{a,R}, S)$ has minimum distance $\geq \bar{n} - a\mu(E) + b$.

In the remaining part of this section we will recall how to associate a linear code using a vector bundle and a variety, both defined over the same finite field.

Let p be a prime integer and q a power of p. $GF(q)$ will denote the finite field with q elements and $\mathbb{K}$ its algebraic closure. For any scheme X defined over $\mathbb{K}$ let $X(\mathbb{K})$ be the set of its Spec($\mathbb{K}$)-points in the usual sense (or, equivalently, in the sense of the theory of schemes). If X is a reduced scheme defined over $GF(q)$, then $X(q)$ will denote the set of its $GF(q)$-points in the usual sense of coding theory: every element of $X(q)$ corresponds to an equivalence class of morphisms $\mathrm{Spec}(GF(q)) \to X$ with the additional condition that the corresponding local ring of X has $GF(q)$ (not just a finite extension of $GF(q)$) as its residue field; thus if X has an embedding into $\mathbf{P}^x$ defined over $GF(q)$, so that we may see $X(\mathbb{K})$ as a subset of $\mathbf{P}^x(\mathbb{K})$, then $X(q) = X(\mathbb{K}) \cap PG(x, q)$. Here we will explain how to obtain linear codes using rank r vector bundles instead of just line bundles (case $r = 1$). First, we consider the case of curves. Let X be a reduced projective curve defined over $GF(q)$. Let E be a rank r vector bundle on X defined over $GF(q)$ and H an ample and effective Cartier divisor on X. Since H is ample, there is an integer $m_0(E)$ such that for all integers $m \geq m_0(E)$ the vector bundle $E(mH)$ is spanned by its global sections. We will fix any integer $m \geq m_0(E)$ and we will use $H^0(X, E(mH))$ and $X(q)$ to define a linear code. Since $\dim(X) \leq 1$, and $E(mH)$ is spanned by its global sections, it is easy to check the existence of $r-1$ global sections of $E(mH)$ which are linearly independent at each point of $X(\mathbb{K})$ (see e.g. [1], Theorem 2). Since cohomology groups commute with field extensions ([2], Proposition III.9.3), we may even find these linearly independent sections defined over $GF(q)$. Thus we have an exact sequence

$$0 \to \mathcal{O}_X^{\oplus(r-1)} \to E(mH) \to \det(E(mH)) \to 0 \tag{1}$$

defined over $GF(q)$. Since H is ample, $X \backslash H_{red}$ is affine. Hence by Theorem B of Serre ([2], Theorem III.5.2) the restriction of (1) to $X \backslash H_{red}$ splits. Thus we obtain

$$E(mH)|X \backslash H_{red} \cong (\mathcal{O}_{X \backslash H_{red}}^{\oplus(r-1)} \oplus \det(E(mH)))|X \backslash H_{red}.$$

For all Cartier hypersurfaces R_i, $1 \leq i \leq s+x$, $s \geq 0, x \geq 0, s+x > 0$, such that $R_i \neq R_j$ for all $i \neq j$ and any Cartier divisor $D = \sum_{i=1}^{s} a_i R_i - \sum_{i=s+1}^{s+m} a_i R_i$, $a_i > 0$ for all i, set $\mathrm{Supp}(D) = \cup_{i=1}^{s+m} R_i$. Call H_{red} the support of H. Since

H is ample, there is a (non-necessarly effective) Cartier divisor D such that $\det(E) \cong \mathcal{O}_X(D)$ and $\mathrm{Supp}(D) \subseteq H_{red}$. Since $\det(E(mH)) \cong \det(E)(rmH)$, the line bundle $\det(E(mH))$ is represented by a Cartier divisor, $D + rmH$, whose support is contained in H_{red}. Thus $\det(E(mH))|X\backslash H_{red}$ is trivial. Hence $E(mH)|X\backslash H_{red} \cong \mathcal{O}^{\oplus r}_{X\backslash H_{red}}$. From now on, we fix this trivialization. With this convention the evaluation of any $f \in H^0(X, E(mH))$ at any $P \in (X\backslash H_{red})(q)$ gives an element of $GF(q)^{\oplus r}$ (seen as the set of all matrices with one column and r rows). Set $n := \mathrm{card}(X\backslash H_{red})(q))$. In this way we obtain a $GF(q)$-linear map $\phi : H^0(X, E(mH)) \to GF(q)^{\oplus rn}$. The map ϕ defines a code if and only if it is injective. We can find H (and hence do the construction) simultaneously for all rank r vector bundles for any (but fixed) finite family of vector bundles.

Now we consider the general case. Let X be a reduced and projective scheme defined over $GF(q)$ and without any isolated point. Let H be an effective ample divisor defined over $GF(q)$. First, we fix a rank r vector bundle E on X defined over $GF(q)$. We make the same construction. The only difference is that now instead of the exact sequence (1) we have an exact sequence

$$0 \to \mathcal{O}_X^{\oplus(r-1)} \to E(mH) \to \mathcal{I}_Z \otimes \det(E(mH)) \to 0\,, \tag{2}$$

with Z closed subscheme of X defined over $GF(q)$ and everywhere of codimension at least two. We may find H as above with the additional property $Z_{red} \subseteq H_{red}$. Hence restricting (2) to $X\backslash H_{red}$ gives $E(mH)|X\backslash H_{red} \cong \mathcal{O}^{\oplus r}_{X\backslash H_{red}}$. Fixing any such isomorphism we may work as in the one-dimensional case. We only point out that we may find such an ample H not passing through any point in $X(q)$. With this additional choice we have $n = \mathrm{card}(X(q))$ and in particular n does not depend from E. We can find H (and hence do the construction) simultaneously for all rank r vector bundles for any (but fixed) finite family of vector bundles.

2. Proof of Theorem 1

Let C be a smooth, connected and projective curve of genus g and E a rank r vector bundle on C. Let $\mu(E) := \deg(E)\mathrm{rank}(E)$ denote the slope of E. By Riemann-Roch we have $h^0(C, E) - h^1(C, E) = \deg(E) + r(1 - g)$. Hence $h^0(C, E) > 0$ if $\mu(E) > g-1$. If $h^1(C, E) = 0$, then $h^0(C, E) = \deg(E)+r(1-g)$. E is called stable (resp. semistable) if for every proper non-zero subsheaf F of E we have $\mu(F) < \mu(E)$ (resp. $\mu(F) \leq \mu(E)$). Every line bundle id stable. There is a unique integer s such that $1 \leq s \leq s$ and a unique increasing filtration $\{E_i\}_{0\leq i\leq s}$ of E by subbundles of E such that $E_0 = \{0\}$, $E_s = E$ and

$\mu(E_{i+1})/\mu(E_i) < \mu(E_i)/\mu(E_{i-1})$ for every integer i such that $1 \le i \le s-1$. This filtration is called the Harder-Narasimhan filtration of E. Each vector bundle E_i/E_{i-1}, $1 \le i \le s$, is semistable. Set $\mu_+(E) := \mu(E_1/E_0)$ and $\mu_-(E) := \mu(E_s/E_{s-1}$. We have $\mu_-(E) \le \mu(E) \le \mu_+(E)$. E is semitable if and only if $s = 1$ if and only if $\mu_+(E) = \mu(E)$ if and only if $\mu(E) = \mu_-(E)$ if and only if $\mu_-(E) = \mu_+(E)$. Obviously, $h^0(C,E) \ge h^0(C,\mu(E_1)$ and hence $h^0(C,E) > 0$ if $\mu_+(E) > g-1$. Standard properties of the semistability and Serre duality imply $h^1(C,E) = 0$ if either $\mu_-(E) > 2g-2$ or if E is stable with slope $2g-2$, but it is not the canonical bundle.

Proposition 1. *Fix n distinct points $P_1,\dots,P_n \in C(q)$. Let E be a rank r vector bundle on C such that $h^0(C,E) > 0$. Let $\phi_E : H^0(C,E) \to GF(q)^{rn}$ be the evaluation map associated to a trivialization in Section 1. Assume $n > \mu_+(E)$. Then ϕ_E is injective and hence it defines an $h^0(C,E) \times rn$ code $C(E)$. $C(E)$ has minimum distance $\ge n - \mu_+(E)$. If E is stable and $r \ge 2$, then $C(E)$ has minimum distance $> n - \mu_+(E)$.*

Proof. For any integer $c > 0$ and any points $Q_1,\dots,Q_c \in C$ we have $\mu(E(-Q_1-\cdots-Q_c) = \mu(E)-c$ and $\mu_+(E(-Q_1-\cdots-Q_c) = \mu_+(E)-c$. Thus $H^0(E(-Q_1-\cdots-Q_c)) = 0$ if either $c > \mu_+(E)$ or $c = \mu_+(E)$, E is semistable and $E \ncong \mathcal{O}_C(Q_1+\vdots+Q_c)^{\oplus r}$. If $r \ge 2$ and $E \cong \mathcal{O}_C(Q_1+\vdots+Q_c)^{\oplus r}$, then E is semistable, but not stable. □

Now we consider evaluation codes obtained using line bundles on a variety X ruled over a curve C.

Let C be a smooth and geometrically connected curve of genus g defined over $GF(q)$ and E a rank $r \ge 2$ vector bundle on C defined over $GF(q)$. Set $X := \mathbf{P}(E)$, $\bar{n} := \mathrm{card}(C(q))$ and $n := \bar{n}(q^r-1)/(q-1)$. Thus $n = \mathrm{card}(X(q))$. The ruled variety X is equipped with a projection $f : X \to C$ whose fibers are $\mathbf{P}^{r-1}$'s and with a line bundle H such that its restriction to every fiber of f has degree one and $f_*(H) \cong E$. The latter condition defines uniquely H. We have $\mathrm{Pic}(X) \cong \mathbf{Z}H \oplus f^*(\mathrm{Pic}(C))$, i.e. for every line bundle L on X there is a unique integer a and a unique line bundle R on C such that $L \cong H^{\otimes a} \otimes f^*(R)$. Set $L_{a,R} := H^{\otimes a} \otimes f^*(R)$ ([2], Lemma II.7.9). The restriction of $L_{a,R}$ to any fiber of f has degree a. Thus $h^0(X,L_{a,R}) = 0$ if $a < 0$. Hence the line bundles $L_{a,R}$ with $a < 0$ are not interesting to define evaluation codes on X. If $a \ge 0$ we have $f_*(L_{a,R}) \cong S^a(E) \otimes R$ ([2], Proposition II.7.11) and hence $H^0(X,L_{a,R}) = h^0(C,S^a(E) \otimes R)$. This formula explains our interest in the symmetric powers of E.

Remark 1. Let C be a smooth and connected projective curve defined over $\mathbb{K}$ and $F_C : C \to C$ the absolute Frobenius (see [5]). A vector bundle E on C is said to be p-semistable if it is semistable and for all integers $t > 0$ the vector bundle $(F_C)^{t*}(E)$ is semistable (see [5]). Let E be a p-semistable vector bundle on C. By [5], lines 8–10 of p. 365, for every integer $a > 0$ the vector bundle $S^a(E)$ is p-semistable and in particular it is semistable.

Theorem 2. *Let C be a smooth and geometrically connected curve of genus g defined over $GF(q)$ and E a rank r p-semistable vector bundle on C defined over $GF(q)$. Set $X := \mathbf{P}(E)$, $\bar{n} := \operatorname{card}(X(q))$ and $n = \bar{n}(q^r - 1)/(q-1)$. Fix integers a and b and $R \in \operatorname{Pic}^b(C)$. Assume $0 \le a \le q$. Let $\phi_{L_{a,R,X(q)}} : H^0(X, L_{a,R}) \to GF(q)^n$ be the evaluation map at the points of $X(q)$. If $a\mu(E) + b < \bar{n}$, then $\phi_{L_{a,R,X(q)}}$ is injective and hence it defines an $h^0(C, S^a(E) \otimes R) \times n$ linear code $C(E, L_{a,R})$. The code $C(E, L_{a,R})$ has minimum distance $\ge \bar{n} - a\mu(E) + b$.*

Proof. Write $\{Q_1, \dots, Q_{\bar{n}}\} = C(q)$. The restriction, $\alpha(Q_i)$, of any section α of $L_{a,R}$ to any fiber $f^{-1}(Q_i)$ of the ruling of X is a homogeneous degree a polynomial. Since $a \le q$ every homogeneous degree a forms on $\mathbf{P}^{r-1}$ vanishing on $PG(r-1,q)$ is identically zero. Thus $\alpha(Q_i) = 0$ if α vanishes at all points of $f^{-1}(Q_i)(q)$. We have $\mu(S^a(E)) = a\mu(E)$ and hence $\mu(S^a(E) \otimes R) = a\mu(E) + b$. Since E is p-semistable, $S^a(E)$ is semistable (Remark 1) and hence $S^a(E) \otimes R(-Q_1 - \cdots - Q_{\bar{n}})$ is semistable. Since $\mu(S^a(E) \otimes R(-Q_1 - \cdots - Q_{\bar{n}})) = a\mu(E) + b - \bar{n}$, we have $h^0(C, S^a(E) \otimes R(-Q_1 - \cdots - Q_{\bar{n}})) = 0$. Hence no nonzero section of $L_{a,R}$ may vanishes identically on $\bar{n}$ fibers of the ruling of X. Since $a \le q$, we obtain the injectivity of $\phi_{L_{a,R}}$. Taking a subset of $C(q)$ instead of $C(q)$ the same computation gives the lower bound for the minimum distance of $C(E, L_{a,R})$. □

To prove Theorem 1 we use the following construction.

Example 1. Fix an integer a such that $0 < a \le q$. Since

$$h^0(\mathbf{P}^{r-1}, \mathcal{O}_{\mathbf{P}^{r-1}}(a)) = \binom{r+a-1}{r-1}$$

and $h^0(\mathbf{P}^{r-1}, \mathcal{I}_{PG(r-1,q)}(a)) = 0$, there is $S \subseteq PG(r-1,q)$ such that $\operatorname{card}(S) = \binom{a+r-1}{r-1}$ such that 0 is the only homogeneous degree a forms on $\mathbf{P}^{r-1}$ vanishing on S. An explicit inductive construction of one such set S is easy and we present it in the case $r-1 = 2$, because it may be useful to give more explicitly the code. Fix any line $D_1 \in PG(2,q)$ and any $a+1$ points $A_{1,1}, \dots, A_{1,a+1} \in D_1(q)$. Then take a line $D_2 \subset PG(2,q)$ such that $A_{1,j} \notin D_2$. Take a points $A_{2,1}, \dots, A_{2,a} \in$

$D_2(q)$. If $a = 1$, then we stop. If $a \geq 2$ we define inductively $a+1$ lines $D_i \subset PG(2,q)$, $1 \leq i \leq q$, and choose $a+2-i$ points $A_{i,1}, \dots, A_{a+2-i} \in D_i(q)$ such that $A_{u,v} \notin D_w$ if $u < w$. Set $S := \cup_{i,j} A_{i,j}$. We need to apply this construction not on a single $PG(r-1,q)$ but on all $\bar{n}$ fibers of the ruling $f : X \to C$ over the points of $C(q)$. We may do that because we have chosen a trivialization of E near $C(q)$ to define the evaluation code. With this explicit construction the proof of Theorem 2 gives verbatim the proof of Theorem 1.

Acknowledgements

The author was partially supported by MIUR and GNSAGA of INdAM (Italy).

References

[1] M.F. Atiyah, Vector bundles over an elliptic curve, *Proc. London Math. Soc.*, **7**, No. 3 (1957), 414-452; Reprinted in: *Michael Atiyah Collected Works*, Volume **I**, Oxford Science Publications, Oxford (1988), 105-143.

[2] R. Hartshorne, *Algebraic Geometry*, Springer, Berlin-Heidelberg-New York (1977).

[3] J.H. van Lint, G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry*, DMV Seminar Band **12**, Birkhäuser, Basel-Boston-Berlin (1988).

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

[5] A. Moriwaki, A note on Bogomolov-Gieseker's inequality in positive characteristic, *Duke Math. J.*, **64**, No. 2 (1991), 361-377.

[6] C.S. Seshadri, *Fibrés Vectoriels sur les Courbes Algébriques*, Astérisque, **96**, Soc. Math. France (1982).