UNIVERSAL WISER PUBLISHER

Linear Codes Obtained from Projective and Grassmann Bundles on Curves

E. Ballico

Department of Mathematics, University of Trento, 38123 Povo (TN), Italy
Email: ballico@science.unitn.it

Abstract: We use split vector bundles on an arbitrary smooth curve defined over $\mathbb{F}_q$ to get linear codes (following the general set-up considered by S. H. Hansen and T. Nakashima), generalizing two quoted results by T. Nakashima. If $p \neq 2$ for all integers $d, g \geq 2$, $r > 0$ such that either r is odd or d is even we prove the existence of a smooth curve C of genus g defined over $\mathbb{F}_q$ and a p-semistable vector bundle E on C such that rank(E) = r, deg(E) = d and E is defined over $\mathbb{F}_q$. Most results for particular curves are obtained taking double coverings or triple coverings of elliptic curves.

***Keywords*:** vector bundles on curves, linear code, projective bundle, Grassmann code, p-semistable vector bundle

1. Introduction

Fix a prime p and a p-power q. Any subset $S \subseteq \mathbb{P}^{k-1}(\mathbb{F}_q)$ spanning $\mathbb{P}^{k-1}(\mathbb{F}_q)$ defines an $[n, k]$-code, $n := \#S$, in the following way. For any $P \in S$ pick a representative $A_P \in \mathbb{F}_q^k$. Use these n representatives Ap, $P \in S$, and an ordering of S to get a $k \times n$ matrix with A_P, $P \in S$, as its columns. This matrix is the generator matrix of a linear code and different choices of representatives A_P and orderings of S give equivalent linear codes. Hence the only problem for the construction of these codes is to get nice sets S and nice embedding $S \to \mathbb{P}^{k-1}(\mathbb{F}_q)$. In our set-up S will be the set $X(\mathbb{F}_q)$ of all $\mathbb{F}_q$-points of a nice projective variety X. The embedding $j: S \to \mathbb{P}^{k-1}(\mathbb{F}_q)$ is usually obtained in the following way. There is a very ample line bundle $\mathcal{L}$ on X defined over $\mathbb{F}_q$ such that dim $(H^0(\mathcal{L})) = k$ and the embedding j is the restriction to S of the embedding $j_{\mathcal{L}}: X \to \mathbb{P}^{k-1}$ associated with the complete linear system $|\mathcal{L}|$. We do not claim that in our construction $\mathcal{L}$ will be very ample.

Fix a smooth projective curve C of genus g defined over $\mathbb{F}_q$. Here we follow [5, Remark 4.3] and [10, 11] and use vector bundles E on C to get S and the embedding $S \subset \mathbb{P}^{k-1}(\mathbb{F}_q)$. We only use vector bundles which are direct sums of line bundles. We use the proofs in [10, 11] to prove the following results.

Theorem 1. Let C be a smooth projective curve of genus g defined over $\mathbb{F}_q$. Set $a := \#(C(\mathbb{F}_q))$. Fix integers r, s, e, t, b_1, b_2 such that $r > s > 0$, $0 \leq e < r$, $q \geq b_1 > 0$. Assume

$$a > b_1(t + e) + b_2 \tag{1}$$

$$tb_1 + b_2 \geq g \tag{2}$$

Then there are $P \in C(\mathbb{F}_q), L \in Pic(C)(\mathbb{F}_q)$ *and* $R \in Pic^{b_2}(C)(\mathbb{F}_q)$ with the following properties. Set $E := L(P)^{\oplus e} \oplus L^{\oplus(r-e)}$, and $X := \mathbb{P}(E)$. Then the vector bundle $S^{b_1}(E) \otimes R$ induces a line bundle on X and hence a linear code $\mathcal{C}$ over $\mathbb{F}_q$. The code $\mathcal{C}$ is an $[n, k, d]$-code with $n = a(q^r - 1)/(q-1), k = \binom{r+b_1-1}{r-1}(b_2 + 1 - g + b_1(t + \frac{e}{s}))$ and

$$d \geq (q^{r-1} + (1-b_1)q^{r-2})(a - b_1(t+e) - b_2).$$

The main point of Theorem 1 is in the case $b_1 \geq 2$, because if $b_1 = 1$ we are in the set-up of [4, 8] (projective bundles over C whose fibers are embedded as a linear subspace of $\mathbb{P}^{k-1}$), where more efficient tools are available.

DOI: https://doi.org/10.37256/cm.142020449

For all integers $r > s > 0$ set

$$\begin{bmatrix} r \\ s \end{bmatrix}_q = \frac{(q^r - 1)(q^r - q)\cdots(q^r - q^{s-1})}{(q^s - 1)(q^s - q)\cdots(q^s - q^{s-1})}.$$

We have $\#(G(r,s)(\mathbb{F}_q)) = \begin{bmatrix} r \\ s \end{bmatrix}_q$ ([7, Th. 24.2.1]).

Theorem 2. Let C be a nonsingular projective curve of genus g defined over $\mathbb{F}_q$. Set $a := \#(C(\mathbb{F}_q))$. Fix integers $r > s > 0$, t, b, e such that $0 \le e < r$. Let E be the vector bundle constructed to prove Theorem 1. Let $\pi : Gr_s(E) \to C$ be the Grassmann bundle of rank s quotient bundles of E. Set $Y := Gr_s(E)$. Let f be a fiber of π. Let $\mathcal{O}_Y(1)$ the tautological π-ample line bundle on Y. Set

$$\tilde{N} := (\mathcal{O}_Y(1) - stf)^{(r-s)s} \cdot (\mathcal{O}_Y(1) + bf),\ \tilde{N}_1 := (\mathcal{O}_Y(1) - stf)^{(r-s)s} \cdot f\ .$$

Assume

$$a > \tilde{N} / \tilde{N}_1 \tag{3}$$

$$st + b > g \tag{4}$$

Then there is a line bundle $L_{1,b}$ on Y numerically equivalent to $\mathcal{O}_Y(1) + bf$, defined over $\mathbb{F}_q$ and giving an $[n, k, d]$-linear code on Y such that

$$n = a \cdot \begin{bmatrix} r \\ s \end{bmatrix}_q,\ k = \binom{r-1}{s-1}(rt + e + \frac{r}{s}b),\ d \ge \left(\begin{bmatrix} r \\ s \end{bmatrix}_q - q^{(r-s)s} \right)(a - \tilde{N} / \tilde{N}_1).$$

The case $b_1 = 1$ of Theorem 1 is just the case $s = r - 1$ and $b_2 = b$ of Theorem 2.

If $e > 0$ some parameters of Theorem 1 (resp. Theorem 2) are worst than the ones in [11, Theorem 3.1] (resp. [10, Theorem 3.2]) (roughly speaking, we take t instead of $\mu(E) = t + \frac{e}{r}$). However, Theorems 1 and Theorem 2 have two key features.

Remark 1. To use [10, 11] in the case $g \ge 2$ one needs a p-semistable vector bundle with prescribed rank and degree on a curve of genus g and everything must be defined over $\mathbb{F}_q$. If $e = 0$, then this is easy (Remark 4). In all the other cases, this was unknown (as far as we know). See Theorem 3 for construction on certain curves when $p \ne 2$ and either the degree is even or the rank is odd. See Theorem 4 for the case in which either $d \equiv 0 \pmod 3$ or $r \equiv 1, 2 \pmod 3$. Even more difficult (and more important for the applications) should be the construction of explicit p-semistable vector bundles on explicit curves. It is easy to find line bundles L, R as above on an arbitrary C with $C(\mathbb{F}_q) \ne \emptyset$ and for a huge number of other C, L, R we only need to require an inequality slightly stronger than (2) or (4). Theorems 3 and 4 give explicit curves and explicit vector bundles.

Remark 2. If $g \ge 3$ the assumption $b_1(t + e) + b_2 \ge g$ is better than the assumption $(t + \frac{e}{r})b_1 + b_2 > 2g - 2$ made in [11, Theorem 3.1] and this is not a small issue for the following reason. This assumption (or an assumption $\mu(E)b_1 + b_2 \ge g - 1$ instead of $\mu(E)b_1 + b_2 > 2g - 2$ as in [11, Theorem 3.1]) is essential for the computation of the parameter k of the code $\mathcal{C}$: if $b_1(t + \frac{e}{r}) + b_2 < g - 1$, then $\binom{r + b_1 - 1}{r - 1}\left(b_2 + 1 - g + b_1(t + \frac{e}{s})\right) < 0$. If (1) is not satisfied, then the lower bound for d given in Theorem 1 is negative. Hence if (1) is not satisfied, then we may still have an $[n, k]$-code, but no information on its minimum distance. Combining (1) and (2) (or (3) and (4)) we get a very strong restriction on $a = \#C(\mathbb{F}_q)$, which often conflicts with the Hasse-Weil bound, unless $q \gg tb_1$. Hence going from $2g - 2$ to g seems to be a good improvement.

Let C be a smooth projective curve defined over a field with characteristic p. Let E be a vector bundle on C. Let F : C $\to$ C be the Frobenius map. We recall that E is p-semistable if all pullbacks $F^{m*}(E)$, $m \in \mathbb{N}$, are semistable ([10]).

Theorem 3. Assume $p \neq 2$. Fix integers g, r, d such that $g \geq 2$ and either d is even or r is odd. Then there are a smooth and projective curve C of genus g defined over and *a* p-semistable vector bundle E on C such that rank(E) = r, deg(E) = d and E is defined over $\mathbb{F}_q$.

We may take as C a double covering $h : C \to W$ with h defined over $\mathbb{F}_q$ and W a suitable elliptic curve (see the proof of Theorem 3).

Theorem 4. Assume $p \neq 2$ and $p \neq 3$. Fix integers g, r, d such that $g \geq 5$, $g \neq 6$ and either $d \equiv 0 \pmod 3$ or $r \equiv 1, 2 \pmod 3$. Then there are a smooth projective curve C of genus g defined over $\mathbb{F}_q$ and a p-semistable vector bundle E on C defined over $\mathbb{F}_q$ such that rank(E) = r and deg(E) = d.

In the statement of Theorem 4 we may take as C an explicitly constructed triple covering of an elliptic curve.

2. The proofs

Remark 3. Let C be a smooth projective curve defined over $\mathbb{F}_q$. For any integer d there is a degree d line bundle on C defined over $\mathbb{F}_q$ ([13, Corollary V.1.1.11]).

Remark 4. Fix a smooth curve C of genus g and integers r, d such $d \equiv 0 \pmod r$. We claim the existence of a p-semistable vector bundle on $C(\mathbb{F}_q)$. Fix any $L \in \mathrm{Pic}^{d/r}(C)(\mathbb{F}_q)$ (Remark 3) and take $E := L^{\oplus r}$.For an alternative approach, see [11, Remark 2.1].

To compute cohomology groups of vector bundles on C using Serre duality we will silently (i.e. referring to the proofs in [10, 11]) use the following observation.

Remark 5. Let E_1, E_2 be vector bundles on a scheme Y. For every integer $n > 0$ we have $S^n(E_1 \oplus E_2) = \oplus_{i=0}^n S^i(E_1) \otimes S^{n-i}(E_2)$ ([6, p.66]). Hence $S^n(E^*) \cong S^n(E)^*$ if E is isomorphic to a direct sum of line bundles. Let C be a smooth projective curve of genus g defined over a field with characteristic p. Fix an integer $n > 0$, a p-semistable vector bundle E on Y and $R, M \in \mathrm{Pic}(C)$. Since E is p-semistable, $S^n(E)$ is semistable ([12, Theorem 3.23]). Hence $S^n(E)^*$ and $S^n(E)^* \otimes R^*$ are semistable. Hence $h^0(C, S^n(E)^* \otimes R^*) = 0$ if $\mu(S^n(E)^* \otimes R^*) < 0$, i.e. if $-n \cdot \mu(E) - \deg(R) < 0$. Hence Serre duality gives $h^1(C, S^n(E) \otimes M) = 0$ if $n \cdot \mu(E) + \deg(M) > 2g-2$.

Lemma 1. Assume $C(\mathbb{F}_q) \neq 0$. Fix integers $t > 0$, $b_1 > 0$ and b_2 such that $tb_1 + b_2 \geq g$. Fix any $L \in \mathrm{Pic}(C)(\mathbb{F}_q)$ such that deg(L) = t. Then there is $R \in \mathrm{Pic}^{b_2}(C)(\mathbb{F}_q)$ *such that* $h^1(C, L^{\otimes b_1} \otimes R) = 0$.

Proof. Since $tb_1 + b_2 \geq g$, there is $M \in \mathrm{Pic}^{tb_1+b_2}(C)(\mathbb{F}_q)$ such that $h^1(C, M) = 0$ ([2, 3]). Take $R := M \otimes (L^*)^{\otimes b_1}$.

Notation 1. Let C be a smooth curve defined over $\mathbb{F}_q$ such that $C(\mathbb{F}_q) \neq \emptyset$. Fix integers t, $r > 2$ and e such that $0 < e < r$. Our family of vector bundles with rank r and degree $rt + e$ are of the form $E = L_1 \oplus \cdots \oplus L_r$ with $L_i \in \mathrm{Pic}^{t+1}(C)(\mathbb{F}_q)$ if $1 \leq i \leq e$ and $L_i \in \mathrm{Pic}^t(C)(\mathbb{F}_q)$ if $e < i < r$. To get Theorems 1 and 2 we fix R and L as in Lemma 1 (with $b_1 = s$ and $b_2 = b$ for Theorem 2) and take $L_i = L(P)$ if $1 \leq i \leq e$ and $L_i = L$ if $e + 1 \leq i \leq r$.

Lemma 2. Fix a smooth curve C and r, e, L_i, E as in Notation 1. Set $X := \mathbb{P}(E)$ and let $\mathcal{O}_X(1)$ the associated relatively ample tautological line bundle. Call $u : X \to C$ the ruling. Fix $\beta \in \mathbb{Q}$ and any $M \in \mathrm{Pic}(C)$. Set $y :=$ deg(M). If $t + \beta y \geq 0$, the $\mathcal{O}_X(1) + \beta u^*(M)$ is nef.

Proof. Fix an integral curve $T \subset X$. It is sufficient to prove the inequality $T \cdot (\mathcal{O}_X(1) + \beta u^*(M)) \geq 0$ for every integral curve $T \subset X$. Fix an integral curve $T \subset X$ and $\gamma \in \mathbb{Q}$ such that $\gamma > \beta$. It is sufficient to prove that $T \cdot (\mathcal{O}_X(1) + \gamma y f) \geq 0$, where f is a fiber of $u : X \to C$. We may assume $\Gamma \neq 0$. Write $\Gamma = a/b$ with $a, b \in \mathbb{Z}$, $b > 0$, and $(a, b) = 1$. To prove the latter inequality we first prove the existence of an integer $c > 0$ such that the line bundle $\mathcal{O}_X(cb) \otimes u^*(M^{\otimes ca})$ is spanned. Notice that $S^b(E) \otimes M^{\otimes a}$ is a direct sum of line bundles of degree at least $tb + ay > 0$. Hence for all integers $c \geq 2g + 1$ the vector bundle $S^{cb}(E) \otimes M^{\otimes ca}$ is a direct sum of very ample line bundles. This is true also for $E^{\otimes cb} \otimes M^{\otimes ca}$. We have $u_*(\mathcal{O}_X(cb) \otimes u^*(M^{\otimes ca})) \cong S^{cb}(E) \otimes M^{ca}$. Hence $H^0(X, \mathcal{O}_X(cb) \otimes u^*(M^{\otimes ca})) \cong H^0(C, S^{cb}(E) \otimes M^{cb})$. Hence $\mathcal{O}_X(cb) \otimes u^*(M^{\otimes ca})$ has many sections. The same computation shows that $E^{\otimes cb} \otimes M^{\otimes ca}$ is spanned. By the definition of $\mathcal{O}_X(1)$ there is a surjection $u^*(E) \to \mathcal{O}_X(1)$. Since the tensor product is a right exact functor, we get a surjection $u^*(E^{\otimes cb} \otimes M^{\otimes ca}) \to \mathcal{O}_X(cb) \otimes u^*(M^{\otimes ca})$. Hence $\mathcal{O}_X(cb) \otimes u^*(M^{\otimes ca})$ is spanned for all $c \geq 2g + 1$. Hence $T \cdot (\mathcal{O}_X(1) + \gamma y f) \geq 0$.

Proof of Theorem 1. Fix $L, R \in \mathrm{Pic}(C)(\mathbb{F}_q)$ such that deg(L) = t, deg(R)= b_2 and $h^1(C, L^{\otimes b_1} \otimes R) = 0$ (Lemma 1). Set $E := L(P)^{\oplus e} \oplus L^{\oplus(r-e)}$ and $X := \mathbb{P}(E)$. Let $u : X \to C$ be the associated fibration. Let f be the numerical equivalence class of a fiber of u. As a line bundle $\mathcal{L}$ on X we take the line bundle $\mathcal{O}_X(b_1) \otimes u^*(R)$. Lemma 2 gives that $H := \mathcal{O}_X(1) - tf$ is nef. We have $H^{r-1} \cdot (\mathcal{O}_X(b_1) + b_2 f) = b_1(H^r - (r-1)H^{r-1} \cdot f) + b_2 = b_1(\deg(E) - (r-1)t) + b_2 = b_1(t+e) + b_2$. Hence the proof of [11, Theorem 3.1] gives the lower bound for the minimum distance. We do not claim that the line bundle $\mathcal{O}_X(b_1) \otimes u^*(R)$ on X is very ample. Thus in our set-up S cannot be seen as a subset of $\mathbb{P}^{k-1}(\mathbb{F}_q)$. But still, the code has the prescribed parameters, even if a priori some of its columns may coincide. To get the very ampleness of $\mathcal{O}_X(b_1)\otimes u^*(R)$ we would need to assume too much (e.g. $b_2 + tb_1 \geq 2g + 1$).

Lemma 3. Fix *C, t, r* and $E := L(P)^{\oplus e} \oplus L^{\oplus(r-e)}$ as in Notation 1 and *Y, π*, $\mathcal{O}_Y(1)$, *f* as in Theorem 2 with $Y := \mathbb{P}(E)$. Let H_s be any line bundle on *Y* numerically equivalent to $\mathcal{O}_Y(1) - (st)f$. Then H_s is nef.

Proof. Set $Z := \mathbb{P}(\wedge^s(E))$ and let $\pi : Z \to C$ the associated fibration. Call *f* the numerical class of a fiber of *π* and $\mathcal{O}_Z(1)$ the tautological relatively ample line bundle of *Z*. Let $\phi: Y \to Z$ denote relative Plücker embedding. We have $\mathcal{O}_Y(1) \cong \phi^*(\mathcal{O}_Z(1))$. Notice that $\wedge^s(E)$ is a direct sum of line bundles isomorphic to $L^{\otimes s}(xP)$ for some integer *x* such that $0 \leq x \leq s$. Applying Lemma 2 to the split vector bundle $\wedge^s(E)$ we get that the numerical class of the line bundle $\mathcal{O}_Z(1) - stf$ is nef. The restriction of a nef line bundle *J* of *Z* to any subvariety *T* of *Z* is nef , because to test that *J* is nef we also need to test the curves contained in *T*. Since $H_s = \phi^*(\mathcal{O}_Z(1) - stf)$, we get that H_s is nef.

Proof of Theorem 2. Take *L*, *R* as in the proof of Theorem 1 and set $E := L(P)^{\oplus e} \oplus L^{\oplus(r-e)}$. Set $L_{1,b} := \mathcal{O}_Y(1) \otimes \pi^*(R)$. We have $H^0(Y, L_{1,b}) \cong H^0(C, \wedge^s(E) \otimes \pi^*(M))$. Hence here (as in [10]) to get the value of *k* of the linear code $\mathcal{C}$ associated to $L_{i,b}$ (and not just a lower bound for it) it is equivalent to prove $h^1(C, \wedge^s(E) \otimes R) = 0$. In our set up it is sufficient to have *L*, *R* such that $h^1(C, L^{\otimes s} \otimes R) = 0$. Apply Lemma 1 with $bi := s$. Apply verbatim the proof of [10, Theorem 3.2] taking the line bundle H_s (which is nef by Lemma 3), instead of the nef line bundle *H* numerically equivalent to $\mathcal{O}_Y(1) - s(t + \frac{e}{s})f$.

Lemma 4. Let *W* be an elliptic curve defined over $\mathbb{F}_q$, $q \neq 2$. Fix an integer $d > 0$. Then there are $R \in Pic^d(W)(\mathbb{F}_q)$ and $D \in |R|$ such that *D* is reduced and defined over $\mathbb{F}_q$.

Proof. If $d = 1$, then we may take $R := \mathcal{O}_W(O)$ with *O* the unity of the group *W*. Hence we may assume $d \geq 2$. By the Hasse-Weil bound there is $Q \in W(\mathbb{F}_{q^d})$ not contained in $W(\mathbb{F}_{q^x})$ for any integer $x \geq 1$ dividing *d* and $x \neq d$. Take as *D* the orbit in *W* of *Q* by the action of the Galois group of the extension $\mathbb{F}_{q^d}/\mathbb{F}_q$ and set $R := \mathcal{O}_W(D)$.

Proof of Theorem 3. First assume *d* even. Let *W* be any smooth elliptic curve defined over $\mathbb{F}_q$ and such that $\mathrm{Pic}^0(W)$ has no point of order 2. Any such curve *W* has an affine equation $y^2 = P(x)$ with $P(x)$ a degree 3 polynomial over $\mathbb{F}_q$ with no multiple root over $\mathbb{F}_q$ and with no root in $\overline{\mathbb{F}}_q$ (and the converse holds). Let *F* be any semistable vector bundle on *W* with rank *r* and degree *d*/2; *F* exists by [1]. The vector bundle *F* is *p*-semistable ([11], Corollary 3.1). Hence for any smooth curve *C* and any degree 2 morphism $h : C \to W$ the vector bundle $h^*(F)$ is *p*-semistable ([9, Proposition 5.1]) and $\mathrm{rank}(h^*(F)) = r$, $\deg(h^*(F)) = d$. Thus it is sufficient to find *C* and *f* as above and defined over $\mathbb{F}_q$. Here we use $p \neq 2$. Any such pair (*C*, *h*) as above with *C* of genus *g* is constructed in the following way. Fix $M \in \mathrm{Pic}^{g-1}(W)(\mathbb{F}_q)$. Assume the existence of a reduced divisor $D \in |M^{\otimes 2}|$ and *D* defined over $\mathbb{F}_q$. The pair (*M*, *D*) defines a degree 2 Galois covering $h : C \to W$ with *D* as its branch locus and *C* sitting in the total space $\mathbb{V}(M^*)$ of M^* as an effective divisor with a quadratic equation. By Lemma 4 there is a reduced divisor *D* of degree $2g - 2$ defined over $\mathbb{F}_q$. Hence $\mathcal{O}_W(D) \in \mathrm{Pic}^{2g-2}(W)(\mathbb{F}_q)$. Since $\mathrm{Pic}^0(W)$ has no point of order 2, the map $L \mapsto L^{\otimes 2}$ from $\mathrm{Pic}^{g-1}(W)(\mathbb{F}_q)$ into $\mathrm{Pic}^{2g-2}(W)(\mathbb{F}_q)$ is injective. Since $\#(\mathrm{Pic}^{g-1}(W)(\mathbb{F}_q)) = \#(\mathrm{Pic}^{2g-2}(W)(\mathbb{F}_q))$, this map is surjective. Hence there is $M \in \mathrm{Pic}^{g-1}(W)(\mathbb{F}_q)$ such that $M^{\otimes 2} \cong \mathcal{O}_W(D)$.

Now assume that both *d* and *r* are odd. Hence $d + r$ is even. Take *C* as above such that there is a *p*-semistable vector bundle *G* on *C* defined over $\mathbb{F}_q$ with rank *r* and degree $d + r$. Fix $M \in \mathrm{Pic}^1(C)(\mathbb{F}_q)$ (Remark 3). The vector bundle $E := G \otimes M^*$ is *p*-semistable, defined over $\mathbb{F}_q$, $\mathrm{rank}(E) = r$ and $\deg(E) = d$.

Proof of Theorem 4. First assume $d \equiv 0 \pmod 3$. If *g* is odd, then set $\gamma := (g - 5)/2$. If *g* is even and $g \neq 6$, then set $\gamma := (g - 8)/2$.

(a) Here we assume $\gamma \equiv 0,1 \pmod 3$. Fix an irreducible and monic $f \in \mathbb{F}_q[x]$ such that $\deg(f) = \gamma + 1$. Let *Y* be the normalization of the plane curve with $y^3 = f(x)$ as its equation. By [13, Proposition VI.3.1] *Y* is a smooth curve of genus *γ* defined over $\mathbb{F}_q$. *Y* is equipped with a degree 3 morphism $h: Y \to \mathbb{P}^1$ defined over $\mathbb{F}_q$ and ramified exactly at the point at infinity and at the roots of *f* in $\overline{\mathbb{F}}_q$. All the roots of *f* are conjugate for the Galois group of the extension $\mathbb{F}_{q^{\gamma+1}}/\mathbb{F}_q$. Since $q \geq 5$, there is $S \subseteq \mathbb{F}_q$ and $S' \subseteq \mathbb{F}_{q^6}$ such that $\#S = 4$, $\#S' = 6$, *S′* is invariant by the action of the Galois group of the extension $\mathbb{F}_{q^6}/\mathbb{F}_q$ and *S′* contains no root of *f*. Let $\pi: W \to \mathbb{P}^1$ be the degree 2 covering ramified exactly at *S*. Both *W* and *π* are defined over $\mathbb{F}_q$. Let $\varpi: W' \to \mathbb{P}^1$ be a degree 3 covering ramified ramified only at *S′* and with ramification of minimal order at each point of *S′*. Since $p > 3$, *W′* is an elliptic curve. We may find *W′* and ϖ defined over $\mathbb{F}_q$. First assume *g* odd. Let *X* be the fiber product of *h* and *π*. Since the branch loci of *h* and *π* are disjoint, *X* is a smooth curve equipped with a degree 3 morphism $h_1 : X \to W$ and a degree 2 morphism $\pi_1 : X \to Y$ ramified at 12 point. Hence applying the Riemann-Hurwitz formula to π_1 we get that X has genus $2\gamma - 1 + 6 = g$. Let F be a rank r and degree $d/3$ p-semistable vector bundle on W. We saw in the proof of Theorem 3 that $h_1^*(F)$ is p-semistable. Now assume g even and $g \neq 6$. Let X_1 be the fiber product of h and ϖ.Since the branch loci of h and ϖ are disjoint, X_1 is a smooth curve. The curve X_1 is equipped with a degree 3 morphism $h_2 : X_1 \rightarrow W'$ and a degree 3 morphism $\varpi_1 : X_1 \rightarrow Y$, both defined over $\mathbb{F}_q$. Since ϖ_1 is ramified at exactly 18 points and with ordinary ramification there, X_1 has genus $2\gamma - 1 + 9 = g$. Use h_2 as above to get the p-semistable vector bundle on X_1.

(b) Now assume $\gamma \equiv 2 \pmod 3$. Take monic and irreducible polynomials $f_1, f_2 \in \mathbb{F}_q[x]$ such that $\deg(f_1) = \gamma$, and $\deg(f_2) = 1$. Now take as Y the normalization of the plane curve with $y^3 = f_1(x)f_2^2(x)$ as its equation. Since $\deg(f_1) + 2.\deg(f_1) \equiv 1 \pmod 3$, we may apply [13, Proposition VI.3.1]1, and get that Y has genus γ. We conclude as in step (a).

(c) Now assume $d \equiv 1, 2 \pmod 3$. In this case we assumed $r \equiv 1, 2 \pmod 3$. Hence there is $x \in \{1, 2\}$ such that $d + xr \equiv 0 \pmod 3$. The first part of the proof gives the existence of a smooth curve C of genus g defined over $\mathbb{F}_q$ and a p-semistable vector bundle G on C defined over $\mathbb{F}_q$ and with $\mathrm{rank}(G) = r$ and $\deg(G) = d + xr$. Take any $L \in \mathrm{Pic}^x(\mathbb{F}_q)$ (Remark 3) and set $E := G \otimes L^*$.

References

[1] Aranson, J. K., Elman, E., Jacob, B. On indecomposable vector bundles. *Comm. Algebra*. 1992; 20: 1323-1351.

[2] Ballet, S., Le Brigand, D. On the existence of non-special divisors of degree g and $g - 1$ in algebraic function fields over $\mathbb{F}_q$. *J. Number Theory*. 2006; 116(2): 293-310.

[3] Ballet, S., Ritzenthaler, C., Rolland, R. On the existence of dimension zero divisors in algebraic function fields defined over $\mathbb{F}_q$. *Acta Arith*. 2010; 143(4): 377-392.

[4] Hana, G. M., Johnsen, T. Scroll codes. *Des. Codes Cryptogr*. 2007; 45(3): 365-377.

[5] Hansen, S. H. Error-correcting codes from higher-dimensional varieties. *Finite Fields Appl*. 2001; 7: 530-552.

[6] Hartshorne, R. Ample vector bundles. *Publ. Math. I.H.E.S*. 1966; 29: 63-94.

[7] Hirschfeid, J. W. P., Thas, J. A. *General Galois geometries, Oxford Mathematical Monographs, Oxford Science Publications*. New York: The Clarendon Press, Oxford University Press; 1991.

[8] Johnsen, T., Rasmussen, N. H. Scroll codes over curves of higher genus. *Appl. Algebra Engrg. Comm. Comput*. 2010; 21: 397-415.

[9] Miyaoka, Y. The Chern classes and Kodaira dimension of a minimal variety. *Ad. Stud. Pure Math*. 1984; 10: 449-476.

[10] Nakashima, T. Codes on Grassmann bundles and related varieties. *J. Pure Appl. Algebra*. 2005; 199: 235-244.

[11] Nakashima, T. Error-correcting codes on projective bundles. *Finite Fields Appl*. 2006; 12: 222-231.

[12] Ramanan, S., Ramanathan, A. Some remarks on the instability flag. *Tohoku Math. J*. 1984; 36: 269-291.

[13] Stichtenoth, H. *Algebraic Function Fields and Codes.* Springer, Berlin; 1993.