International Journal of Pure and Applied Mathematics
Volume 4 No. 1 2003, 31-42

RANK TWO BUNDLES ON ALGEBRAIC CURVES AND DECODING OF GOPPA CODES

Trygve Johnsen
Department of Mathematics
University of Bergen
Johs. Bruns GT. 12, N-5008 Bergen, NORWAY
e-mail: johnsen@mi.uib.no

Abstract: We study a connection between two topics: Decoding of Goppa codes arising from an algebraic curve, and rank two extensions of certain line bundles on the curve. The material about each isolated topic is well known. Our contribution is just to expose a connection between them.

AMS Subject Classification: 14J28, 14H45
Key Words: rank two bundles, decoding of Goppa codes

1. Introduction

Let C be a curve over a finite field F_q. Some years ago V. Goppa showed how to produce codes from such a curve (For a survey, see for example Gieseker [7]). In this note we will show how socalled syndrome decoding of (the duals of the original) Goppa codes in an intimate way is connected to the study of rank two bundles, that are extensions of the structure sheaf $\mathcal{O}_C$ and a certain fixed line bundle on C determined by the code in question. In fact, each syndrome corresponds to an extension. Moreover syndromes due to correctable error vec-

Received: November 7, 2002

tors always correpond to unstable rank two bundles, that is: semistable bundles never correspond to syndromes of correctable errors (here we call an error vector, or simply error, correctable if its Hamming weight is at most $\frac{d-1}{2}$, where d is the designed minimum distance of the code). For correctable errors the process of error location is translated into finding a certain quotient line bundle of minimal degree (or dually: a line subbundle of maximal degree) of the rank two bundle defined by the syndrome, and then pick the relevant section of this line bundle. If an error is not correctable, there is not necessarily a unique such quotient line bundle of minimal degree. We gain our insight through a certain projective embedding $C \subset \mathbf{P}$, with the property that the columns of the parity check matrix of the Goppa code in question are interpreted as points of the embedded copy of C. We study j-secant $(j-1)$-planes to C, for $j = 1, 2, ...$. Using the proper definitions of these geometrical objects, we thus obtain a stratification of $\mathbf{P}$, which viewed from one angle is a stratification of syndromes, according to how many errors that have to be made to obtain the syndrome. Viewed from another angle it is a stratification of rank two extensions according to the so-called s-invariant. The geometric picture associated to rank two extensions was given very explicitly in Lange and Narasimhan [11], and the basic idea was given already in Atiyah [1]. We just remark that the aspects interesting to us carry over to the case of positive characteristic. Then we compare with the picture obtained from the space of syndrome vectors. So far we have not been able to utilize these geometrical observations to make any constructive decoding algorithms. To do so one would have to introduce some kind of "extention arithmetic" to perform decoding. Some explicit considerations along these lines are made in [4]. For constructive decoding algorithms for Goppa codes in general, see the celebrated Feng and Rao [6], or for example Duursma [5], Justesen et al [10], Pellikaan [12], Skorobogatov and Vladut [14], or the special issue IEEE Trans. of Info. Theory, Vol. 41, No.6, Nov. 1995.

In Section 2 we recall some basic facts concerning algebraic-geometric (Goppa) codes. We also define and make an elementary study of the secant varieties that in a natural way turn up in connection with these codes. In Section 3 we introduce vector bundle language, and in Theorem 3.4 we present the connection between correctable errors and unstable bundle extensions of rank two.

Remark 1.1. In Goppa [8] one describes an algorithm for decoding of Goppa codes from rational curves. There one assumes first of all that at most t errors are made, where $t = [(d-1)/2]$. Then one assumes that exactly t errors are made, and sets up a system of equations to solve the problem of error-location given that this extra assumption holds. If the equations yield no solution, one assumes that $t-1$ errors are made, sets up a new system of equations, and so on. In the end one arrives at a point, where one finds a solution since the basic assumption is that at most t errors are made. The coefficient matrices, set up to find the elementary symmetric functions in the parameter values of the error locations are Toeplitz, and in particular symmetric. This process is in many ways reminiscent of describing complete quadrics through various blowing-ups of the space of usual quadrics, which is again a space of symmetric square matrices. Hence, in order to generalize to arbitrary curves, one could describe some kind of analogy to complete quadrics for curves of positive genus. Such a generalization, in terms of an object obtained through various blowing-ups of the secant strata of C inside $\mathbf{P}$, has been given in Bertram [3], using vector bundle language. It is possible that understanding this or similar objects can give new insight into decoding of Goppa codes.

2. Definitions and Basic Facts About Goppa codes

A q-ary code of length n is a subset of the vector space F_q^n, where F_q is a finite field with q elements. A linear code is a linear subspace of F_q^n. Let $\overline{F}_q$ be an algebraic closure of F_q. Let C be a curve of genus g defined over these fields. Let D and G be divisors on C defined over F_q, such that their supports are disjoint. Moreover the support of D consists of n distinct points $P_1, ..., P_n$ of degree one, where $n = \deg(D)$. For a divisor M defined over F_q, denote by $L(M)$ the set of the zero element and those elements f of the function field $F_q(C)$, such that $(f) + M \geq 0$. Denote by $l(M)$ the dimension of $L(M)$ as a vector space over F_q. This dimension is the same as the one obtained if we work over $\overline{F}_q$.

Following for example van Lint et al [15] we denote by $C(D, G)$ the code, which is the image of $L(G)$ in F_q^n under the map:

$$\phi : f \rightarrow \ (f(P_1), ..., f(P_n)).$$

In Pellikaan et al [13], such a code is called a WAG, which is short for weakly algebraic- geometric code. Moreover one shows there that all linear codes are WAG. By the theorem of Riemann-Roch (which remains valid over finite fields) we have:

$$\dim(C(D, G)) = l(G) - \dim(ker f) = l(G) - l(G - D)$$

$$= \deg(G) + 1 - g + l(K - G) - l(G - D).$$

As usual K denotes a canonical divisor. Set $m = \deg(G)$. A WAG is called a SAG (strongly algebraic-geometric code) if the following composite condition is fullfilled: $2g-2 < m < n$. For a SAG we observe: $l(K-G) = l(G-D) = 0$, and hence: $\dim C(D,G) = m+1-g$. By a generator matrix for a code one means a $(k \times n)$-matrix, where the rows constitute a base for the code as a linear space over F_q. A generator matrix for $C(D,G)$ is:

$$M = \begin{bmatrix} f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ \cdots & & & \\ \cdots & & & \\ f_k(P_1) & f_k(P_2) & \cdots & f_k(P_n) \end{bmatrix},$$

where $k = m+1-g$, and $f_1, ..., f_k$ is a basis for $L(G)$, both over F_q and over $\overline{F}_q$. By a parity check matrix for a code one means a $((n-k) \times n)$ - coefficient matrix of a set of equations cutting out the code as a subspace of F_q^n and of $\overline{F}_q^n$. One denotes by $C^*(D,G)$ the linear code having the matrix M above as parity check matrix. Hence $C^*(D,G)$ is the orthogonal complement of $C(D,G)$ and vice versa. One also says that the codes are dual to each other. For a WAG defined as $C(D,G)$ consider the exact sequence of sheaves on C:

$$0 \to \mathcal{O}(G-D) \to \mathcal{O}(G) \to \mathcal{O}(G)/\mathcal{O}(G-D) \to 0.$$

The long exact cohomology sequence gives:

$$0 \to L(G-D) \to L(G) \to F_q^n$$

$$\to H^1(C, \mathcal{O}(G-D)) \to H^1(C, \mathcal{O}(G)) \to 0.$$

Moreover by Serre duality : $H^1(C, \mathcal{O}(G-D))$ is dual to $L(K+D-G)$, and $H^1(C, \mathcal{O}(G))$ is dual to $L(K-G)$. For a SAG the long exact sequence reduces to:

$$0 \to L(G) \to F_q^n \to L(K+D-G)^* \to 0. \tag{1}$$

Here K can (by Riemann-Roch) be chosen, such that $G^* = K+D-G$ has support disjoint from D. We can identify the elements of $L(K+D-G)$ with differential forms being zero of order the same as order(G) at the points of the support of G, and having at most simple poles at the points of the support of D, and no poles elsewhere. Hence we see that evaluating elements of $L(K+D-G)$ can be interpreted as evaluating residues of the differential forms described (after multiplying each value $f(P_i)$ by a non-zero value $\mathrm{Res}_{P_i}(\eta)$, where $K = (\eta)$). Moreover we have for f in $L(G)$ and ω a differential form as described:

$$0 = \Sigma_i \mathrm{Res}_{P_i}(f\omega) = \Sigma_i f(P_i) \mathrm{Res}_{P_i}(\omega). \tag{2}$$

From equations (1) and (2) we easily conclude that $C(D,G^*)$ is code equivalent to $C^*(D,G)$. In the original work by Goppa the code obtained from the divisors D and G was $C^*(D,G)$, and it was obtained by means of residues of differential forms. By a Goppa code we will here simply mean a SAG. One easily verifies that $C(D,G^*)$ is a SAG if and only if $C(D,G)$ is so. For a SAG we see that if $\{h_1, \cdots, h_{k^*}\}$ is a basis for $L(G^*)$, then a parity check matrix for $C(D,G)$ is (essentially, after a trivial equivalence operation):

$$M = \begin{bmatrix} h_1(P_1) & h_1(P_2) & \cdots & h_1(P_n) \\ \cdots & & & \\ \cdots & & & \\ h_{k^*}(P_1) & h_{k^*}(P_2) & \cdots & h_{k^*}(P_n) \end{bmatrix},$$

where $k^* = n-k = n-m+g-1$.

Remark 2.1. We see that the columns of M^* represent the points of the support of D if C is embedded into $\mathbf{P} = \mathbf{P}^{n-m+g-2} = \mathbf{P}(H^0(C, K+D-G)^*)$ by means of sections of $L(G^*)$.

For $\mathbf{w_1}$ and $\mathbf{w_2}$ in F_q^n, let the Hamming distance $d(\mathbf{w_1}, \mathbf{w_2})$ denote the number of coordinate positions, in which $\mathbf{w_1}$ and $\mathbf{w_2}$ differ; it is clearly a metric on F_q^n. Let the minimum distance of a code be the minimum Hamming distance for any pair of codewords. For a linear code this is easily seen to be the minimum number of non-zero coordinates (minimum weight) for any non-zero codeword. Denote by d_1 the minimum distance of the code $C(D,G)$. If a code word has weight d_1, then there is a divisor D_1 with $D_1 \leq D$, and $\deg(D_1) = n - d_1$, such that $L(G-D_1) \neq 0$, Hence $m-(n-d_1) \geq 0$, that is: $d_1 \geq n-m$. We denote by d the integer $n-m$, which is positive since $C(D,G)$ is a SAG. We call d the designed minimum distance. We also see that C is embedded into $\mathbf{P}(H^0(C, K+H)^*)$, where $d = \deg(H)$ (and $H = D-G$). Denote by t the integer $[(d-1)/2]$. We also call t the designed error correcting capacity. Recall the basic fact:

Remark 2.2. Let N be the parity check matrix of a code. The minimum distance of the code is equal to s if all choices of $s-1$ columns of N are independent, and some choice of s columns of N are dependent.

Let $\mathbf{x}$ be an element (codeword) of $C(D,G) \subset F_q^n$, and assume that $\mathbf{x}$ is transmitted, and $\mathbf{y} = \mathbf{x} + \mathbf{e}$ is received. The difference $\mathbf{e}$ is called the error vector. Denote by $S(\mathbf{y})$ the matrix product $M^*\mathbf{y}$. Clearly $S(\mathbf{y})$ is a vector in $F_q^{k^*}$, and $S(\mathbf{y}) = S(\mathbf{e}) = \mathbf{0}$, if and only if $\mathbf{y}$ is itself a codeword. $S(\mathbf{y})$ is called the syndrome vector of $\mathbf{y}$. We can also interpret $S(\mathbf{y})$ as a point of

$\mathbf{P} = \mathbf{P}^{k^*-1} = \mathbf{P}^{d+g-2}$. For each integer a, let the (Hamming) a-ball centered at $\mathbf{x}$ be the set of those $\mathbf{y}$, such that $d(\mathbf{x}, \mathbf{y}) \leq a$. The following is immediate from the triangle equality:

Remark 2.3. The restriction of the map S: $F_q^n \rightarrow F_q^{k^*}$ to any t-ball is injective.

Secant Varieties

Now we view C as any curve defined over the algebraic closure $\overline{F}_q$, and let C be embedded in some projective space over this field. Let A be an effective divisor on C, possibly with repeated points. Let C_j be the j'th symmetric product of C, for j=1,2,... .

Definition 2.4. (a) We denote by $\operatorname{Span}(A)$ the intersection of all hyperplanes $\mathcal{H}$, such that we have: $\Sigma_i I(Q_i, C \cap \mathcal{H}) Q_i \geq A$ (Here $I(Q, V_1 \cap V_2)$ denotes the usual Bezout intersection number of two varieties of complementary dimension at a point Q).

(b) We say that C is k-spanned if $\dim(\operatorname{Span}(A)) = j - 1$, for all A with $\deg(A) = j$, and $j \leq k + 1$.

(c) We set $\operatorname{Sec}_j(C) = \cup \operatorname{Span}(A)$, where the union is taken over all A in C_j.

(d) For a point P in projective space we set $h(P) = h$ if P is contained in $\operatorname{Sec}_h(C) - \operatorname{Sec}_{h-1}(C)$.

Proposition 2.5. *Let C be the curve treated in Section 2, defined over F_q and embedded into $\mathbf{P}^{d+g-2}$ by the linear system $K + D - G$ as described. Then we have:*

(a) C is $(d-2)$-spanned. In particular C is smoothly embedded if $d \geq 3$.

(b) If $h(P) = h \leq [(d-1)/2] = t$, then there is a unique effective divisor A with degree at most h, such that P is contained in $\operatorname{Span}(A)$.

Proof. (a) An easy application of Riemann-Roch. Let A be a divisor of degree $j \leq d - 1$. Set $H = D - G$. Then

$$l(K+H-A) = 2g-2+d-j+1-g+l(A-H) = d+g-1-j = l(K+H)-j,$$

so A imposes j independent conditions on the linear system.

(b) Assume P is contained in $\text{Span}\,(A_1) \cap \text{Span}\,(A_2)$. If the supports of the divisors A_1 and A_2 are disjoint, then we have: $\text{Span}\,(A_1 + A_2) =$ the linear span of $\text{Span}\,(A_1) \cup \text{Span}\,(A_2)$, so

$$\dim(\text{Span}\,(A_1 + A_2)) = 1 + \dim(\text{Span}\,(A_1)) + \dim(\text{Span}\,(A_2))$$

$$- \dim((\text{Span}\,(A_1) \cap \text{Span}\,(A_2)) \leq 1 + 2(h-1) - 1 = 2h - 2.$$

Hence C is not $(2h-1)$-spanned, and thus not $(d-2)$-spanned, since $h \leq [(d-1)/2]$. We leave it to the reader to modify the argument if the supports of the two divisors are not disjoint. □

By abuse of notation (see Remark 2.1 above) we denote by P_i column nr. i of the parity matrix M^*. Assume that a codeword $\mathbf{x}$ is transmitted, $\mathbf{y}$ is received, and that the error vector $\mathbf{e}$ has weight h with coordinates $e_1, \cdots, e_h$ in positions $i_1, \cdots, i_h$ respectively. We have: The syndrome $S(\mathbf{y}) = S(\mathbf{e}) = e_1 P_1 + \cdots + e_h P_h$. Interpreting $S(\mathbf{y})$ as a point of $\mathbf{P}$, we then see that $S(\mathbf{y})$ is contained in $\text{Sec}_h(C)$, and that $h(S(\mathbf{y})) \leq h$. Moreover it is clear that if $h \leq t$, then $h(S(\mathbf{y})) = h$, and that the "error divisor" $P_1 + \cdots + P_h$ is the unique divisor A of degree at most h over $\overline{F}_q$, such that $S(\mathbf{y})$ is contained in $\text{Span}\,(A)$. So, error location amounts to finding such a divisor A, given the point $S(\mathbf{y})$. A priori we know that this divisor consists of distinct points, all of degree 1 defined over F_q, and that even the errors $e_1, \cdots, e_h$ are in F_q.

3. Vector Bundles of Rank Two on C

We continue using the notation from Section 2. The following exposition is to a great extent taken from Lange and Narasimhan [11] and Bertram [3]. Let $\text{Ext}_{\mathcal{O}_C}(H, \mathcal{O}_C)$ be the set of isomorphism classes of exact sequences

$$(e) : 0 \to \mathcal{O}_C \to E \to H \to 0.$$

The map $\mathcal{O}_C \to E$ is denoted by f and the map $E \to H$ by g. The zero element (e_0) corresponds to the case of a split exact sequence. Here $\mathcal{O}_C$ as usual denotes the structure sheaf on C, and H is the fixed line bundle or invertible sheaf $D - G$, see Section 2 (by abuse of notation we do not distinguish between the divisor $H = D - G$, or the invertible sheaf or line bundle, of which the divisor corresponds to a global section). The middle term E is a locally free sheaf, or vector bundle, of rank 2. Standard cohomology theory and Serre duality give:

$$\text{Ext}_{\mathcal{O}_C}(H, \mathcal{O}_C) = \text{Ext}_{\mathcal{O}_C}(\mathcal{O}_C, -H) = H^1(C, -H) = H^0(C, K + H)^*.$$

Hence $\mathbf{P}(\operatorname{Ext}_{\mathcal{O}_C}(H,\mathcal{O}_C)) = \mathbf{P}(H^0(C,K+H)^*) = \mathbf{P}$. This means that (up to isomorphism and a multiplicative factor) the points of our well-known projective space $\mathbf{P}$ described in Section 2 are identified with extensions as described.

Definition 3.1. Let E be a rank two vector bundle on C.

(a) Denote by $s(E)$ the integer

$$\deg(E) - 2\max(\deg(L)) = 2\min(\deg(M)) - \deg(E),$$

where the maximum is taken over all line subbundles L of E and the minimum is taken over the quotient line bundles M of E.

(b) E is called stable if $s(E) > 0$; semistable if $s(E) \geq 0$; unstable if $s(E) < 0$.

(c) For an extension (e) as above we set $s((e)) = s(E)$, where E is the middle term. An extension is called stable (semistable, unstable) if the middle term E is so.

The definitions of stable and semistable coincide if $\deg(E)$ is odd. For the zero element (e_o) we observe: $s(E) = -d$, and for all non-split extension (e) we have $d \geq s((e)) \geq 2-d$. Moreover, if M is a quotient line bundle of E of minimal degree $(s+d)/2 \geq 1$, with quotient map h, then the composition of h and f is non-zero:

$$\mathcal{O}_C \to \; E \to \; M.$$

Hence M is isomorphic to $\mathcal{O}_C(A)$, for an effective divisor A of degree $(s+d)/2$. This implies again that (identifying (e) with its corresponding point of $\mathbf{P}$) the point (e) is contained in the kernel of the map:

$$\operatorname{Ext}^1_{\mathcal{O}_C}(H,\mathcal{O}_C) \to \; \operatorname{Ext}^1_{\mathcal{O}_C}(H,\mathcal{O}_C(A)),$$

that is, in the kernel of:

$$H^0(C,K+H)^* \to \; H^0(C,K+H-A)^*.$$

This observation has many consequences. First we see that the set of points in $\mathbf{P}$ with s-value $2-d$ are precisely those that represent bundles with a quotient bundle of type $\mathcal{O}_C(Q)$, for some point Q on C. If we assume that $d \geq 3$, then C is smoothly embedded by Proposition 2.5. Then we can identify C with its embedded image in $\mathbf{P}$, and the point Q on C then corresponds to a bundle extension with a quotient bundle isomorphic to $\mathcal{O}_C(Q)$. Moreover it is clear that the observation above is equivalent to: (e) is contained in $\operatorname{Span}(A)$.

Remark 3.2. Arguing in a dual way, we get that if (e) is contained in Span (A), then the line bundle corresponding to $H - A$ is a subbundle of E.

Summing up, we now formulate the following result, which is practically identical to Proposition 1.1. of Lange and Narasimhan [11] (recall the functions h and s from $\mathbf{P}$ to $\mathbf{Z}$, introduced in Definition 2.4 (d) and Definition 3.1 (a), respectively).

Proposition 3.3. *Let P be a point of $\mathbf{P}$. Then $s(P) = 2h(P) - d$. In particular P is a unstable point (semistable, stable) if and only if $h(P) < d/2$ ($h(P) \geq d/2$, $h(P) > d/2$).*

We are now able to formulate the main result of the paper:

Theorem 3.4. *Let $P = S(\mathbf{y})$ be the syndrome of a received message using the code $C(D, G)$. Then P is the syndrome of some error vector with weight at most the designed error correcting capasity $t = [(d-1)/2]$ only if P is an unstable point. Moreover in that case the process of error location is reduced to finding the error divisor A among global sections of the unique quotient line bundle of degree h of the vector bundle $E(P)$ of rank two, appearing as the middle term in the extension corresponding to P.*

Proof. This follows directly from Proposition 3.3 and the argument above. □

Remark 3.5. The "only if" in the theorem can be replaced by "if and only if" if we define the syndrome map over $\overline{F}_q$.

Remark 3.6. The definitions of stable, semistable, unstable can be viewed as special cases of more general definitions of these concepts in the setting of Geometric Invariant Theory (GIT), which again is an essential tool in building moduli spaces parametrizing various objects. The spaces arise as quotients of various group actions. In order to get quotients with good properties one usually has to disregard certain "bad objects", which are the unstable ones. In our case the relevant construction is that of $\mathcal{SU}_2(C)$, the moduli space of isomorphism classes of vector bundles of rank two on C (See Gieseker [9], p. 51-52). This has dimension $4g - 3 = g + (3g - 3)$, where the sum decomposition corresponds to $g = \dim(\mathrm{Jac}\,(C))$ degrees of freedom to choose a line bundle H, and $3g - 3 = \dim(\mathcal{SU}_2(C, H))$ degrees of freedom to choose the rank two bundle with determinant H (where $\mathcal{SU}_2(C, H)$ = modulo space of rank two bundles with determinant H). Moreover, for $\mathcal{SU}_2(C, H)$ there are essentially only 2 cases; $\deg(H)$ odd and $\deg(H)$ even, since tensoring a rank two bundle with a line bundle gives rise to an isomorphism between two such spaces with determinants H with degrees of equal parity. One can show that the natural map:

$$\mathbf{P} - \operatorname{Sec}_t(C) \rightarrow \mathcal{SU}_2(C,H)$$

is birational if $d = \deg(H) = 2g-1$, and that it maps birationally on to the θ-divisor if $d = \deg(H) = 2g-2$, where the θ-divisor parametrizes the rank two-bundles with a global section.

One observes that the situation in coding theory in a certain way is complementary to that of applying GIT to build $\mathcal{SU}_2(C,H)$, since the good(syndrome) points in coding theory are the bad ones for GIT, and vice versa. On the other hand the issue for those who work with moduli spaces is often precisely what to do with the unstable points, so the focal point of the theories are still in a certain sense overlapping. One is for example interested in blowing up various s-negative strata of $\mathbf{P}$ to obtain compactifications of $\mathbf{P} - \operatorname{Sec}_t(C)$ and $\mathcal{SU}_2(C,H)$ with desired properties. See Bertram [2] and [3]. One could hope that insight in such compactifications could be instrumental in understanding algorithms for decoding of Goppa codes. One can also ask: Is it possible that the minimum distance of $C(D,G)$ exceeds d, or weaker: Given a reasonable small integer k_0, like 2, 3 or 17; is there a positive limit s_0, such that if $s(P) \leq s_0 = 2h_0 - d$, then there are at most k_0 divisors A (even over $\overline{F}_q$) of degree h_0, such that P is contained in $\operatorname{Span}(A)$? For practical purposes this would in some situations be almost as good as unique decoding. In vector bundle language one is then interested maximal sublinebundles of P corresponding to divisors of type $H - A$. The question of such maximal subbundles is the main issue in Lange and Narasimhan [11].

Example 3.7. Assume $g = 0$. Then C is mapped into $\mathbf{P} = \mathbf{P}^{d-2}$ as a curve of degree $d-2$, that is as a rational normal curve. It is well-known that on $C = \mathbf{P}^1$ all rank two bundles of degree d split as $\mathcal{O}(a) \oplus \mathcal{O}(b)$, with $a+b = d$. If d is odd, we then see the largest possible s-value is $-1 = d - 2[(d+1)/2]$. Hence all rank two-bundles are unstable, corresponding to the fact that $\mathbf{P} = \operatorname{Sec}_t(C)$ over F_q.

Acknowledgements

I am grateful to Emma Previato for informing me about the manuscript [4], and to the authors of [4] for correcting a mistake in an old version of my paper.

References

[1] M. Atiyah, Complex fibre bundles and ruled surfaces, *Proc. London Math. Soc.*, **5** (1955), 407-434.

[2] A. Bertram, Moduli of rank-2 vector bundles, theta divisors, and the geometry of curves in projective space, *Journal of Diff. Geometry* , **35** (1992), 429-469.

[3] A. Bertram, Complete extensions and their map to moduli space, *London Math. Soc. Lect. Notes Series*, **179** (1992), 81-91.

[4] T. Bouganis, D. Coles, *A Geometric View of Decoding AG Codes*, Manuscript (2002), 10 pages.

[5] I. Duursma, Algebraic decoding using special divisors, *IEEE Trans. of Info. Theory*, **39**, No. 2 (1993), 694-698.

[6] G.L. Feng, T.R.N. Rao, Decoding algebraic-geometric codes up to the designed minimum distance, *IEEE Trans. of Info. Theory*, **39**, No. 1 (1993), 37-45.

[7] V.D. Goppa, Algebraic-geometric codes, *Math. USSR Izvestiya*, **21** (1983), 75-90.

[8] V.D. Goppa, *Geometry and Codes*, Mathematics and Its Applications, Soviet Series, **21**, Kluwer Ac. Publ., (1989).

[9] D. Gieseker, Geometric invariant theory and applications to moduli problems, *Springer Lect. Notes in Math.*, **996** (1983), 45-63.

[10] J. Justesen, K.J. Larsen, H. Elbrönd Jensen, T. Höholdt, Fast decoding of codes from algebraic plane curves, *IEEE Trans. of Info. Theory*, **38**, No. 1 (1992), 111-119.

[11] H. Lange, M.S. Narasimhan, Maximal subbundles of rank 2 vector bundles on curve, *Math. Ann.*, **266** (1983), 55-72.

[12] R. Pellikaan, On a decoding algorithm for codes on maximal curves, *IEEE Trans. of Info. Theory*, **35**, No. 6 (1989), 1228-1232.

[13] R. Pellikaan, B.Z. Shen, G.J.M. van Wee, Which linear codes are algebraic geometric?, *IEEE Trans. of Info. Theory*, **37**, No. 3 (1991), 583-682.

[14] A.N. Skorobogatov, S.G. Vladut, On the decoding of algebraic-geometric codes, *IEEE Trans. of Info. Theory* **36**, No. 5 (1990), 1051-1060.

[15] J. van Lint, G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry*, DMW Seminar **12**, Birkhauser (1995).