Some Remarks on Goppa Codes

Iwan Duursma

Universiteit van Amsterdam
February 1989

Abstract. The thesis describes four results in the field of Goppa Codes

We quote a sufficient criterion for a Fermat curve to be maximal (Lachaud [L]). An elementary proof then shows that the criterion is both neccessary and sufficient. This seems to contradict results of B.Segre, quoted by [G]. (par.2)

Using a Fermat curve of degree nine we construct a code of type [513,485,15]. The design minimum distance of the code is one. (par.3)

We describe the decoding algorithm for Goppa codes formulated by [J,SV,P]. Our description allows decoding of a Goppa code in either of its two representations. A neccessary and sufficient condition for the algorithm to work is then easily deduced. The condition is weaker then the original condition used by [SV,P]. (par.4)

MacWilliams identity relates the weight distributions of dual linear codes. We present a proof and show that for Goppa codes the crucial part of it comes down to applying Riemann-Roch . (par.5)

Contents

1. Introduction

$\mathbf{F_q}$ will denote a fixed finite field of q elements and characteristic p (>0). With a curve defined over $\mathbf{F_q}$,denoted X/$\mathbf{F_q}$, we will allways mean a smooth absolutely irreducible projective curve. Some results on the geometry of algebraic curves are given. For such a curve we may then define a Goppa code.
We merely present what we need in the sequel. For a note on the proofs see the end of the paragraph.

1.1 Definition. On a curve X/$\mathbf{F_q}$ we have the following divisors

R	sum of all the rational points over $\mathbf{F_q}$
K	canonical divisor (up to equivalence)
L	line (for a plane curve, up to equivalence)

1.2 Definition. For a divisor E on X/$\mathbf{F_q}$ we define linear spaces

$L(E) = \{ f : f \text{ a rational function, } f\neq 0, \text{ with } (f)+E\geq 0 \} \cup \{0\}$

$\Omega(E) = \{ \eta : \eta \text{ a regular differential form, } \eta\neq 0, \text{ with } (\eta)\geq E \} \cup \{0\}$

One can prove that L(E), as a linear space over $\mathbf{F_q}$, is of finite dimension. Let g be the genus of X/$\mathbf{F_q}$, i.e. $g=\dim_{\mathbf{F_q}} L(K)$. We quote

1.3 Theorem (Riemann-Roch). Let E be a divisor on X/$\mathbf{F_q}$ and let l(E) be the dimension of L(E) over $\mathbf{F_q}$. Then

$$l(E) - l(K-E) = \deg(E) + 1 - g$$

1.4 Corollary. For a divisor E on X/$\mathbf{F_q}$ the dimension of $\Omega(E)$ is given by

$$\dim_{\mathbf{F_q}} \Omega(E) = l(K-E)$$

1.5 Corollary. For the degree of the canonical divisor we obtain

$$\deg(K) = 2g - 2$$

Propositions 1.6-1.8 apply to smooth projective plane curves $X/\mathbf{F_q}$, $X'/\mathbf{F_q}$ of degrees d, d' respectively.

1.6 Proposition (Plücker). For a smooth plane curve $X/\mathbf{F_q}$ the genus is given by

$$g = (d-1)(d-2)/2$$

1.7 Proposition (Adjunction Formula). For a smooth plane curve $X/\mathbf{F_q}$ the canonical divisor satisfies the equivalence relation

$$K \sim (d-3)L$$

1.8 Theorem (Bezout). Let $X/\mathbf{F_q}$ and $X'/\mathbf{F_q}$ be plane curves. Assume that they have no common component. Then the intersection number of X and X' is dd' (points counted with multiplicities).

We may now give the definition of a Goppa code.Thereafter proposition 1.11 will enable us to determine the parameters of a specific code.

1.9 Definition. For any pair D,G of divisors on $X/\mathbf{F_q}$ satisfying $0 \le D \le R$, $\mathrm{Supp}(D) \cap \mathrm{Supp}(G) = \emptyset$ we define a Goppa code $C^*(D,G)$ as the image of the linear map α^*

$$\alpha^* : \Omega(G-D) \to (\mathbf{F_q})^{\deg(D)} \qquad , \eta \to (\mathrm{res}_P(\eta))_{P \in D}$$

1.10 Remark. The same class of codes is obtained by defining a Goppa code C(D,G), D and G as in def.1.9, as the image of the linear map α

$$\alpha : L(G) \to (\mathbf{F_q})^{\deg(D)} \qquad , f \to (f(P))_{P \in D}$$

One can prove that C(D,G) and $C^*(D,G)$ are dual to each other.

1.11 Proposition. For a Goppa code $C^*(D,G)$ with

$$\deg(K) < \deg(G) < \deg(D)$$

length n, dimension k and minimum distance d are given by

$$n = \deg(D)$$
$$k = \deg(D\text{-}G)+g\text{-}1$$
$$d = \min\{\ \deg(D') :\ 0 \le D' \le D \text{ and } \exists Q \ge 0\ G+Q \sim K+D'\ \}$$

1.12 Corollary. For a Goppa code $C^*(D,G)$

$$\deg(G\text{-}K) \le d \le \deg(G\text{-}K)+g$$

We call $d^*=\deg(G\text{-}K)$ the design minimum distance.

Note to par.1. More information about sections 1.1-7 and all of its proofs are contained in Fulton [F], in particular chapter 8 on the Riemann-Roch theorem. The same reference, chapter 5 on projective plane curves, gives a proof of Bezout's theorem 1.8.

Sections 1.9-12, on Goppa codes, are treated in van Lint and van der Geer [LG]. The result on k in prop.1.11 differs slightly because of the assumptions on the degrees of the divisors involved. We have:

$$\begin{aligned} k &= \dim_{F_q}\Omega(G-D) - \dim_{F_q}\Omega(G) \\ &= l(K-G+D) - l(K-G) \\ &= l(K-G+D) \\ &= l(G-D) + \deg(K-G+D) + 1 - g \ =\ \deg(D-G)+g-1 \end{aligned}$$

The left inequality in corr.1.12 is explained by the result on d in the proposition, the right inequality by the result on k and the Singleton bound $k+d \le n+1$

$$n+1-k \ =\ \deg(D) + 1 - \deg(D-G) - g + 1 \ =\ \deg(G-K) + g$$

2. Number of rational points over $\mathbf{F_q}$

Let a curve $X/\mathbf{F_q}$ of genus g, be as defined in the introduction.

2.1 Theorem (Weil). For a curve $X/\mathbf{F_q}$ numbers α_i, with $\alpha_i\alpha_i=q$, $i=1,2,\ldots,g$ exist such that the number of points $N_qs=\#X(\mathbf{F_q}s)$ is given by

$$N_qs = q^s + 1 - \sum_{i=1}^{g} (\alpha_i{}^s+\alpha_i{}^s) \qquad s=1,2,\ldots \qquad (2.1)$$

Proof. The first proof is due to A.Weil, 1948 [W]. Since then more proofs have been given. For information see [H, appendix C]. ◊.

2.2 Remark. The α_i, α_i, $i=1,2,\ldots,g$ are related to the zeros of the zeta function of the curve $X/\mathbf{F_q}$. However the above formulation of the theorem will satisfy our purposes. Relation (2.1) clearly determines the α_i, $i=1,2,\ldots,g$. Combining (2.1) with the fact $\alpha_i\alpha_i=q$ yields

2.3 Corollary. For a curve $X/\mathbf{F_q}$ we have as upperbound for the number of points $N_q=\#X(\mathbf{F_q})$

$$N_q \leq q + 1 + 2g\sqrt{q}$$

2.4 Definition. We call a curve $X/\mathbf{F_q}$ maximal over $\mathbf{F_q}s$ if

$$N_qs = [q^s + 1 + 2g\sqrt{q^s}]$$

Let $X_m/\mathbf{F_q}$ be the Fermat curve of degree m, i.e. defined by $F(x,y,z) = x^m+y^m+z^m = 0$. Theorem 2.6 provides a necessary and sufficient condition for a Fermat curve to be maximal in the case s even. Our assumption that a curve be irreducible implies (m,q)=1. We start with a lemma

2.5 Lemma. Let $X_m/\mathbf{F}_q$ be the Fermat curve of degree m. Assume $m \mid q^2-1$ (say $mk=q^2-1$) and let ζ_m denote a primitive m^{th} root of unity in $\mathbf{F}_{q^2}$. The group $<\zeta_m>^3$ acts on $X_m(\mathbf{F}_{q^2})$ in a natural way. This yields

$$\#X_m(\mathbf{F}_{q^2}) = N_0 m + N_* m^2 \tag{2.2}$$

with N_0 the number of orbits of points with xyz=0

$$N_0 = 3(1+(-1)^{kq})/2 \tag{2.3}$$

and N_* the number of orbits of points with $xyz\neq 0$. For $m \mid q+1$ (say $m\mu=q+1$)

$$N_* = (q-2) + (\mu-1)(\mu-2) \tag{2.4}$$

Proof. The value of N_0, 3 or 0, depends on -1 being an m^{th}-power in $\mathbf{F}_{q^2}$ or not. As for N_* let $\alpha \in \mathbf{F}_{q^2}$ be a generator of $\mathbf{F}_{q^2}^*$ and consider $P \in \mathbf{P}^2(\mathbf{F}_{q^2})$

$$P = (1 : \alpha^{A\mu+r} : \alpha^{B\mu+s})$$

with $A,B \in \mathbf{Z}/m(q-1)\mathbf{Z}$ and $r,s \in \mathbf{Z}/\mu\mathbf{Z}$. To let P represent an orbit we will take $A,B \in \mathbf{Z}/(q-1)\mathbf{Z}$. Then $P \in X_m(\mathbf{F}_{q^2})$ iff

$$1 + \alpha^{A(q+1)+rm} + \alpha^{B(q+1)+sm} = 0$$

Applying the Frobenius automorphism yields a system of two linear equations

$$\begin{pmatrix} \alpha^{rm} & \alpha^{sm} \\ \alpha^{rmq} & \alpha^{smq} \end{pmatrix} \begin{pmatrix} \alpha^{A(q+1)} \\ \alpha^{B(q+1)} \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \end{pmatrix}$$

Let $a=\alpha^{A(q+1)}, b=\alpha^{B(q+1)}$. The coefficient matrix is singular for r=s. For r=s=0 we obtain q−2 solutions by solving $a+b+1=0$, $a,b \in \mathbf{F}_q^*$.

For each pair $r \neq s$ the matrix is regular and we find a unique solution. Since the system of equations is invariant under the Frobenius this solution will be over $\mathbf{F_q}$. Solutions of the desired form, i.e. over $\mathbf{F_q^*}$, correspond to $r,s \neq 0$. We find $(\mu-1)(\mu-2)$ solutions, one for each pair r,s with $r,s,r-s \neq 0$. This proves (2.4) $\Diamond$.

2.6 Theorem. Let $X_m/\mathbf{F_q}$ be the Fermat curve of degree m ((m,q)=1). Then

$$X_m \text{ maximal over } \mathbf{F}_{q^2} \iff m \mid q+1$$

Proof. Using prop.1.6 (Plücker) we see $g=(m-1)(m-2)/2$. With q fixed define

$$N_m = \#X_m(\mathbf{F}_{q^2}) \tag{2.9}$$
$$W_m = q^2 + 1 + (m-1)(m-2)q \tag{2.10}$$

Maximality is then expressed by $N_m = W_m$.

($\Rightarrow$) For $d=(m,q^2-1)$ one verifies $N_d = N_m$. The following inequality and its consequences are then trivial

$$N_d = N_m = W_m \geq W_d \geq N_d \implies W_m = W_d \implies$$
$$\implies m=d \text{ v } m=2,d=1 \implies m=d \text{ v } (m,q)=2$$

The case (m,q)=2 represents a reducible Fermat curve. Hence it suffices to show $m \mid q+1$ in the case m=d. By definition of d

$$m=d \iff m \mid q^2-1 \tag{2.11}$$

and we may apply the lemma. Then (2.2) and (2.10) give us

$$m \mid N_m = W_m = (q+1)^2 + m(m-3)q \implies$$
$$\implies m \mid (q+1)^2 \tag{2.12}$$

Together (2.11,12) yield

$$m \mid 2(q+1) \tag{2.13}$$

Say $mm'=2(q+1)$. We show m' is even, which proves $m \mid q+1$. For q even this follows immediately from (2.11). Now suppose q odd and use (2.3)

$$\begin{aligned} 0 &= 4(W_m - N_m) \\ &= 4(q+1)^2 + 4m(m-3)q - 6(1+(-1)^k)m - 4N_* m^2 \\ &= m^2 m'^2 + 2m(m-3)mm' + 12m + \\ &\quad - 6(1+(-1)^k)m - 4N_* m^2 \end{aligned} \tag{2.14}$$

so

$$m \mid 12 - 6(1+(-1)^k) = \begin{cases} 0 & k \text{ even} \\ 12 & k \text{ odd} \end{cases}$$

We may suppose k is even.
For suppose k is odd. Then $m \mid 12$, say $mm^*=12$. From (2.14)

$$0 = m'^2 + 2(m-3)m' + m^* - 4N_*$$

and

$$m' \text{ odd} \implies m^*=1 \text{ or } 3 \implies m-3=9 \text{ or } 1$$

yielding

$$0 \equiv 1 + 2 + m^* \pmod 4$$

Hence $m^*=1, m=12$ and $mk=q^2-1$ gives $q^2 \equiv 13 \pmod{24}$, a contradiction. Then for k even (2.14) gives us $2m^2 \mid m^2 m'^2$ and m' is even, which proves ($\Rightarrow$)

($\Leftarrow$) Since $m \mid q+1$ we may apply the lemma. Note that $2 \mid (q-1)q \mid kq$. Hence $N_0=3$ and

$$\begin{aligned} N_m &= 3m + (q-2)m^2 + (\mu-1)(\mu-2)m^2 \\ &= 3m + (q-2)m^2 + (q+1-m)(q+1-2m) \\ &= (q+1)^2 + (m^2-3m)q \\ &= W_m \end{aligned}$$

$\Diamond$.

References.

[F] W. Fulton (1969), Algebraic Curves,W.A.Benjamin,New York.

[G] V.D. Goppa (1984), Codes and Information, Russian Math. Surveys 39, pp87-141.

[H] R. Hartshorne (1977), Algebraic Geometry, Springer Verlag, New York.

[J] J. Justesen e.a. (1988), Construction and Decoding of a Class of Algebraic Geometry Codes,Technical University of Denmark, Lyngby.

[L] G. Lachaud (1987), Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, C.R.Acad.Sci.Paris,t.305,SérieI, pp729-732.

[LG] J.H. van Lint and G. van der Geer (1988), Introduction to Coding Theory and Algebraic Geometry, Birkhauser, Basel.

[MS] F.J. MacWilliams and N.J.A. Sloane (1977), The Theory of Error-correcting Codes, North-Holland, Amsterdam.

[P] R. Pellikaan (preprint 1988), Over het volledig decoderen van algebraisch meetkundige codes, Technische Universiteit Eindhoven.

[SV] A.N. Skorobogatov and S.G. Vladut (preprint 1988), On the decoding of Algebraic Geometric Codes, Institute for Problems of Information Transmission, Moscow.

[W] A.Weil (1948), Sur les Courbes Algébriques et les Variétés qui s'en Déduisent, Hermann, Paris.