4. Locator algorithm.

As suggested by Justesen e.a. [J] the Peterson algorithm for decoding RS codes may be generalized to be applied to Goppa codes. Skorobogatov and Vladut [S] then formulate the algorithm in terms of divisors. Pellikaan [P] presents a version of the algorithm that allows more errors to be corrected (in some cases of weight up to [(d-1)/2]).

To describe the algorithm we will treat $(\mathbf{F_q})^n$ as a $\mathbf{F_q}$-algebra, that is we allow multiplication of vectors (componentwise). We may then define three kind of linear maps: α (encoding), μ (multiplication) and π (projection). Indices to distinguish different maps of the same kind are allways redundant and will therefore be ommitted.

Let D,G be a pair of divisors on a curve $X/\mathbf{F_q}$ as in def.1.9.: D is the sum of different rational points and $Supp(D)\cap Supp(G)=\emptyset$. From the definitions 1.2 (linear spaces L(G) and $\Omega(G)$) and 1.9 (Goppa codes $C^*(D,G)$ and C(D,G)) one verifies immediately that the following linear maps are well defined.

4.1.Definition. For any pair D,G on $X/\mathbf{F_q}$ as above an encoding map, denoted α, is one of the following

$$L(G) \to C(D,G) \qquad , f \to (f(P))_{P\in D}$$
$$\Omega(G) \to C^*(D,G+D) \qquad , \eta \to (res_P(\eta))_{P\in D}$$

Let F be a divisor on $X/\mathbf{F_q}$, $Supp(D)\cap Supp(F)=\emptyset$. Then a multiplication map, denoted μ, is one of the following

$$L(F) \times L(G) \to L(F+G) \qquad , (f,g) \to fg$$
$$L(F) \times \Omega(G) \to \Omega(G-F) \qquad , (f,\eta) \to f\eta$$
$$C(D,F) \times C(D,G) \to C(D,F+G) \qquad , (\underline{x},\underline{y}) \to \underline{xy}$$
$$C(D,F) \times C^*(D,G+D) \to C^*(D,G-F+D) \qquad , (\underline{x},\underline{y}) \to \underline{xy}$$

Let Q be a divisor on $X/\mathbf{F_q}$, $0 \le Q \le D$. Then a projection map, denoted π, is one of the following

$$C(D,G) \to C(Q,G) \qquad , (x_P)_{P\in D} \to (x_P)_{P\in Q}$$
$$C^*(D,G+D) \to C^*(Q,G+Q) \qquad , (x_P)_{P\in D} \to (x_P)_{P\in Q}$$

Considering the embedding of $\mathbf{F_q}$-algebras $(\mathbf{F_q})^n \to M_n(\mathbf{F_q})$, $\underline{x} \to \mathrm{diag}(\underline{x})$ we may define an m-linear form as follows

4.2.Definition. On $(\mathbf{F_q})^n \times \ldots \times (\mathbf{F_q})^n$ (m copies) we have a multilinear form

$$<.> : \quad (\mathbf{F_q})^n \times \ldots \times (\mathbf{F_q})^n \to \mathbf{F_q}$$
$$(\underline{x}_1,\ldots,\underline{x}_m) \to \mathrm{Tr}(\mathrm{diag}(\underline{x}_1)\ldots\mathrm{diag}(\underline{x}_m)) \qquad (=\sum_i \underline{x}_1^{(i)}\ldots\underline{x}_m^{(i)})$$

The following definition, related to the notion of syndrome in coding theory, plays a central role in theorem 4.6.

4.3.Definition. Let S, or S^*, be the composition of <.> and $(\mathrm{id},\alpha,\alpha)$ as shown in the following diagrams respectively

$$\begin{array}{ccc} & \overset{S}{\to} & \\ (\mathbf{F_q})^{\deg(D)} \times L(F) \times \Omega(G-D+F) & & \mathbf{F_q} \\ \downarrow (\mathrm{id},\alpha,\alpha) & & \| \\ & \overset{<.>}{\to} & \\ (\mathbf{F_q})^{\deg(D)} \times C(D,F) \times C^*(D,G+F) & & \mathbf{F_q} \end{array}$$

$$\begin{array}{ccc} & \overset{S^*}{\to} & \\ (\mathbf{F_q})^{\deg(D)} \times L(F) \times L(G-F) & & \mathbf{F_q} \\ \downarrow (\mathrm{id},\alpha,\alpha) & & \| \\ & \overset{<.>}{\to} & \\ (\mathbf{F_q})^{\deg(D)} \times C(D,F) \times C(D,G-F) & & \mathbf{F_q} \end{array}$$

4.4.Convention. Let T be a multilinear form $T : A_1 \times A_2 \times \ldots \times A_m \to \mathbf{F_q}$ and $a \in A \subset A_1$. We denote the restriction $T|_{A \times A2 \times \ldots \times Am}$ by $T|_A : A \times A_2 \times \ldots \times A_m \to \mathbf{F_q}$. We may interpret $T|_{\{a\}}$ as a multilinear form and if so we will denote it by $T_a : A_2 \times A_3 \ldots \times A_m \to \mathbf{F_q}$.

4.5.Lemma. With the convention and S, S^* as in definition 4.3 we have

$$S|_{C(D,G)} \equiv 0 \qquad\qquad S^*|_{C^*(D,G)} \equiv 0$$

Proof. We may factorize <.> in the definition of S, or S*, using the multiplication map μ from def.4.1

$$\begin{array}{ccc} & \overset{<.>}{} & \\ C(D,G) \times C(D,F) \times C^*(D,G+F) & \to & \mathbf{F_q} \\ \downarrow (\mu,id) & & \| \\ & \overset{<.>}{} & \\ C(D,G+F) \times C^*(D,G+F) & \to & \mathbf{F_q} \\ \\ & \overset{<.>}{} & \\ C^*(D,G) \times C(D,F) \times C(D,G-F) & \to & \mathbf{F_q} \\ \downarrow (\mu,id) & & \| \\ & \overset{<.>}{} & \\ C^*(D,G-F) \times C(D,G-F) & \to & \mathbf{F_q} \end{array}$$

Then use duality of C and C* (remark 1.10) $\Diamond$.

Let $w \in (\mathbf{F_q})^{\deg(D)}$. We apply convention 4.4 with T=S to obtain a bilinear form S_w and for $f \in L(F)$ a linear form $S_{w,f}$. Now suppose

$\exists (c,e) \in C(D,G) \times (\mathbf{F_q})^{\deg(D)}$

(i) $w = c+e$

(ii) $e_P \neq 0 \Leftrightarrow P \in Q$

then clearly

$f \in L(F\text{-}Q) \Rightarrow S_{w,f} \equiv S_{e,f} \equiv 0$

For the converse we have

4.6.Theorem. For $w \in (\mathbf{F_q})^{deg(D)}$

$S_{w,f} \equiv 0 \Rightarrow f \in L(F-Q)$ $\qquad$ $S^*_{w,f} \equiv 0 \Rightarrow f \in L(F-Q)$

iff

$\exists (c,e) \in C(D,G) \times (\mathbf{F_q})^{deg(D)}$ $\qquad$ $\exists (c,e) \in C^*(D,G) \times (\mathbf{F_q})^{deg(D)}$

(i) $w = c+e$ $\qquad$ (i) $w = c+e$

(ii) $e_P \neq 0 \Leftrightarrow P \in Q$ $\qquad$ (ii) $e_P \neq 0 \Leftrightarrow P \in Q$

(iii) $eC(D,F) \cap C(D,G+F) = 0$ $\qquad$ (iii) $eC(D,F) \cap C^*(D,G-F) = 0$

Proof. (We prove the left case) Let $f \in L(F)$ and $(c,e) \in C(D,G) \times (\mathbf{F_q})^{deg(D)}$ with (i-ii). Consider $\underline{x} = (e_P f(P))_{P \in D} \in eC(D,F)$. Then we have the two equivalences (for the first note the factorization of S in def.4.3)

$\underline{x} \in C(D,G+F) \Leftrightarrow S_{w,f} \equiv 0$

$\underline{x} \neq 0$ and (ii) $\Leftrightarrow f \notin L(F-Q)$

Since $f \in L(F)$ (or $\underline{x} \in eC(D,F)$) is arbitrary the result follows $\Diamond$.

4.7.Remark. If (c,e) is the decoding we look for, then F should be such that e satisfies (iii). The theorem then gives a criterion, based on the recieved word w only, to find the error positions.
Note that (iii) is more likely to be satisfied by small errors e, i.e. errors with many zeros. Also (iii) becomes more likely by choosing F of small degree, however for the algorithm to be succesful the linear space L(F-Q) should be nontrivial.

In the corollaries we give some sufficient conditions to find a $f \in L(F-Q)$. Observe that on the assumption that the error positions are in the support of Q the map <.> in definition 4.3 factorizes as follows

$$
\begin{array}{ccc}
 & \overset{<.>}{} & \\
(\mathbf{F_q})^{\deg(D)} \times C(D,F) \times C^*(D,G+F) & \rightarrow & \mathbf{F_q} \\
\downarrow (\pi,\pi,\pi) & & \| \\
 & \overset{<.>}{} & \\
(\mathbf{F_q})^{\deg(Q)} \times C(Q,F) \times C^*(Q,G+F-D+Q) & \rightarrow & \mathbf{F_q} \\
 & \overset{<.>}{} & \\
(\mathbf{F_q})^{\deg(D)} \times C(D,F) \times C(D,G-F) & \rightarrow & \mathbf{F_q} \\
\downarrow (\pi,\pi,\pi) & & \| \\
 & \overset{<.>}{} & \\
(\mathbf{F_q})^{\deg(Q)} \times C(Q,F) \times C(Q,G-F) & \rightarrow & \mathbf{F_q}
\end{array}
$$

and condition (iii) of the theorem becomes

$$(\pi e)C(Q,F) \cap C(Q,G+F-D+Q) = 0 \quad \text{or}$$
$$(\pi e)C(Q,F) \cap C^*(Q,G-F)=0$$

The last condition implies that all errors at Q may be corrected iff C(Q,F) and C*(Q,G–F) contain no elements with equal weight distribution.

4.8.Corollary. ([P]) Let conditions (ii,iii) be as in theorem 4.6. Then (ii,iv)⇒(ii,iii)

(iv) $C(Q,G+F-D+Q) = 0$ (iv) $C^*(Q,G-F)=0$

Proof. Immediate from the observation above ◊.

4.9.Corollary. ([S]) Let d, or d*, be the design minimum distance of C(D,G), or C*(D,G), respectively. Then (ii,v)⇒(ii,iii),

(v) $\deg(F+Q) < d$ (v) $\deg(F+Q) < d^*$

Proof. Let d_F denote the design minimum distance of C(D,G+F). The dual of corollary 1.12 yields d_F=d-deg(F). Then

$$\underline{x} \in eC(D,F) \quad \Rightarrow \quad wt(\underline{x}) \leq wt(e) = deg(Q)$$
$$0 \neq \underline{x} \in C(D,G+F) \quad \Rightarrow \quad d_F \leq wt(\underline{x})$$

Hence, by (v), $\underline{x} \in eC(D,F) \cap C(D,G+F) \Rightarrow \underline{x}=0$ ◊.

4.10.Remark. Note that the argument of cor.4.9 can be used to obtain a weaker condition (v) if the minimum distance of C(D,G+F) (or C*(D,G–F)) is known explicitly.

One can prove (ii,v)⇒(ii,iv)⇒(ii,iii) by a direct calculation of the dimensions of the linear spaces in (iv), e.g.

$\dim_{\mathbf{F_q}} C^*(Q,G-F) = l(K-G+F+Q)-l(K-G+F)$ (as in the note to par.1)

$d^*=deg(G-K)$ (cor.1.12)

so (v) yields $\dim_{\mathbf{F_q}} C^*(Q,G-F)=0$.

What we look for is a more careful argument to show that linear spaces of the given form have a trivial intersection (iii). In practice one might just hope that ,although (iv) is not satisfied, the algorithm works because the particular error satisfies (iii). It then becomes a probabilistic algorithm.

5. MacWilliams theorem

We prove the relation between the weight distributions of two dual linear codes, known as MacWilliams theorem ([MS]). To this end we compare dimensions of suitable subspaces of the codes. We then note that for Goppa codes this comparison of dimensions comes down to applying Riemann-Roch.

5.1.Theorem (MacWilliams). Let C be a linear code of type [n,k] over $\mathbf{F_q}$ with weight enumerator $A(z,w) = \sum_{i=0\ldots n} A_i z^i w^{n-i}$ and let $B(z,w) = \sum_{i=0\ldots n} B_i z^i w^{n-i}$ denote the weight enumerator of the dual code C^*. Then

$$B(z,z+w) = q^{-k}A(w,w+qz) \tag{5.1}$$

Proof. Define, for $S \subset \{1,2,\ldots,n\}$

$$C_S = \{\underline{x}\in C: \forall i\in S\ x_i=0\} \qquad C_S^* = \{\underline{y}\in C^*: \forall i\notin S\ y_i=0\} \tag{5.2}$$

$$K_i = \sum_{\#S=i} \#C_S \qquad M_i = \sum_{\#S=i} \#C_S^* \tag{5.3}$$

$$K(z,w) = \sum_{i=0\ldots n} K_i z^i w^{n-i} \qquad M(z,w) = \sum_{i=0\ldots n} M_i z^i w^{n-i}$$

Equalities (5.4-6), to be proved in *(i)-(iii)*, then clearly yield (5.1)

$$K(z,w) = A(w,w+z) \tag{5.4}$$

$$M(z,w) = B(z,z+w) \tag{5.5}$$

$$M(z,w) = q^{-k}K(qz,w) \tag{5.6}$$

Equation (5.4) expresses the relation between the cardinalities of the sets C_S and the weight enumeration of the code C. For the dual code C^* we find (5.5). Duality of the codes gives us (5.6).

(i) We verify (5.4). Note that K_i, as defined in (5.3), counts codewords of C. Words of weight j, i.e. containing exactly n–j zeros, have multiplicity $\binom{n-j}{i}$. Hence they give a contribution of $A_j\binom{n-j}{i}$. The contribution of A_j to K_i in (5.4) is the coefficient of $z^i w^{n-i}$ in $A_j w^j (w+z)^{n-j}$, that is, $A_j\binom{n-j}{i}$.

(ii) Let S' be the complement of S in {1,2,…,n} and let M' be given by

$$M'(z,w) = B(w,w+z)$$

On the analogy of (5.3-4) we have, with $M'(z,w) = \sum_{i=0\ldots n} M'_i z^i w^{n-i}$

$$M'_i = \sum_{\#S=i} \#C_{S'} = \sum_{\#S'=n-i} \#C_{S'} = M_{n-i}$$

Thus $M(z,w) = M'(w,z) = B(z,z+w)$

(iii) Let k_S and m_S be the dimension, as a vectorspace over F_q, of C_S and C_S^*. Note $k_\emptyset = k$, $m_\emptyset = 0$. For (5.6) it suffices to prove, for $j \notin S$

$$(k_S - k_{S\cup\{j\}}) + (m_{S\cup\{j\}} - m_S) = 1 \qquad (5.7)$$

since we then have

$$(m_S - k_S) = \#S + (m_\emptyset - k_\emptyset) = \#S - k \qquad (5.8)$$

and
$$M_i = \sum_{\#S=i} \#C_S^* = \sum_{\#S=i} q^{m_S} = \sum_{\#S=i} q^{(\#S-k+k_S)} =$$
$$= q^{(i-k)} \sum_{\#S=i} q^{k_S} = q^{(i-k)} \sum_{\#S=i} \#C_S = q^{(i-k)} K_i$$

or
$$M(z,w) = \sum_{i=0\ldots n} M_i z^i w^{n-i} = q^{-k} \sum_{i=0\ldots n} K_i q^i z^i w^{n-i} = q^{-k} K(qz,w)$$

To prove (5.7) we consider the dot product $\langle \underline{x},\underline{y} \rangle$, for $\underline{x} \in C_S$ and $\underline{y} \in C_{S\cup\{j\}}{}^*$

$$0 = \langle \underline{x},\underline{y} \rangle = \sum_{i\in S} x_i y_i + x_j y_j + \sum_{i\notin S\cup\{j\}} x_i y_i$$

(5.2) then implies $x_j y_j = 0$ and we have

$$C_S \neq C_{S\cup\{j\}} \quad \Leftrightarrow \quad \exists \underline{x} \in C_S \text{ with } x_j \neq 0$$
$$\Leftrightarrow \quad \forall \underline{y} \in C_{S\cup\{j\}}{}^* \text{ with } y_j = 0 \quad \Leftrightarrow \quad C_S^* = C_{S\cup\{j\}}{}^*$$

Since $k_S - k_{S\cup\{j\}}$, $m_{S\cup\{j\}} - m_S \in \{0,1\}$, (5.7) follows ◊.

Remark. As shown under *(iii)*, the dimensions k_S and m_S of C_S and C_S^* satisfy a relation (with in fact, constant = –k, by considering S=Ø)

$$m_S - k_S = \#S + \text{constant} \tag{5.8}$$

We show that for Goppa codes (5.8) is a consequence of Riemann-Roch (th.1.3). In fact (5.7) represents Noether's reduction lemma, that may be used in the proof of Riemann–Roch (See [F]).

Let $X/\mathbf{F}_q$ be a curve, $P_1,\ldots,P_n$ points of $X(\mathbf{F}_q)$ and G an effective divisor on $X/\mathbf{F}_q$. With $D=P_1+\ldots+P_n$ def.1.9 gives is us the dual Goppa codes C=C(D,G) and $C^*=C^*(D,G)$ as the images of α and α^*

$$\alpha: L(G)\to(\mathbf{F}_q)^n \qquad , f\to(f(P_1),\ldots,f(P_n))$$
$$\alpha^*: \Omega(G-D)\to(\mathbf{F}_q)^n \qquad , \eta\to(res_{P1}(\eta),\ldots,res_{Pn}(\eta))$$

Applying definition (5.2) to these codes gives

$$C_S = \alpha[L(G-\sum_{i\in S} P_i)]$$
$$C_S^* = \alpha^*[\Omega(G-D+\sum_{i\notin S} P_i)]$$

and
$$k_S = \dim C_S = \dim L(G-\sum_{i\in S} P_i) - \dim \ker \alpha$$
$$m_S = \dim C_S^* = \dim \Omega(G-\sum_{i\in S} P_i) - \dim \ker \alpha^*$$

Since $\dim_{\mathbf{F}_q}\Omega(E) = l(K-E)$, for E a divisor on X (cor.1.4), Riemann-Roch (th.1.3) yields (5.8)

$$m_S - k_S = \deg(K-G+\sum_{i\in S} P_i)+1-g-\dim \ker \alpha^*+\dim \ker \alpha$$
$$= \#S + \text{constant} \qquad \Diamond.$$