On a Decoding Algorithm for Codes on Maximal Curves

RUUD PELLIKAAN

Abstract—A decoding algorithm is given for algebraic geometric codes on maximal curves that decodes in polynomial time $\lfloor (d^*-1)/2 \rfloor$ errors, where d^* is the designed minimum distance of the code.

INTRODUCTION

SKOROBOGATOV and Vlădut [14], following ideas of Justesen *et al.* [8], have given a decoding algorithm for algebraic geometric codes. The latter were introduced by Goppa [4]–[6]. This algorithm decodes up to $\lfloor (d^*-g-1)/2 \rfloor$ errors with complexity $O(n^3)$, where d^* is the designed minimum distance, g the genus of the curve used, and n the word length of the code. We shall give an algorithm which decodes up to $\lfloor (d^*-1)/2 \rfloor$ errors with complexity $O(n^4)$, by applying the above algorithm a number of times in parallel.

The decoding algorithm works in case the class number h (the number of divisors of degree zero modulo principal divisors) is sufficiently greater than a_{g-1} (the number of effective divisors of degree $g-1$). We show how h and a_{g-1} can be computed by means of the zeta function of the curve. In particular, we do this for maximal curves, that is to say, for curves for which the Hasse–Weil upper bound is in fact an equality: $N_1 = q+1+2g\sqrt{q}$.

We prove the existence of the decoding algorithm on maximal curves by showing the existence of certain divisors; however, we have so far been unable to give an efficient procedure of finding these divisors. We follow the notation of van der Geer and van Lint [3] and also refer to it for unproven statements concerning curves. We refer to van Lint [9] for coding theory.

I. DECODING ALGEBRAIC GEOMETRIC CODES

In this section we give a brief overview of the paper by Skorobogatov and Vlădut [14]. Let X be a nonsingular absolutely irreducible projective curve defined over the finite field $\mathbb{F}_q$; we say for brevity, X is a curve. Let $P_1, \cdots, P_n$ be points on X that are rational over $\mathbb{F}_q$. Let D be the divisor $D = P_1 + \cdots + P_n$. Let G be a divisor of degree m, with support disjoint from the support of D.

Manuscript received August 26, 1988; revised April 1989. This paper was presented at the Algebraic and Combinatorial Coding Theory Workshop, Varna, Bulgaria, September 18–24, 1988.

The author is with the Department of Mathematics and Computing Science, Technical University of Eindhoven, Den Dolech 2, P.O. Box 513, 5600 MB Eindhoven, The Netherlands.

IEEE Log Number 8931187.

Consider the map

$$\alpha^*: \Omega(G-D) \to \mathbb{F}_q^n$$
$$\omega \mapsto \left(\operatorname{res}_{P_1}(\omega), \cdots, \operatorname{res}_{P_n}(\omega)\right)$$

The code $C^*(D,G)$ is by definition the image of α^*; its dimension is denoted by k^*. If $m > 2g-2$, then α^* is injective and $k^* = \dim \Omega(G-D) \geq n-m+g-1$. Moreover, equality holds if $m < n$.

The minimum distance is at least $m+2-2g$, and this last mentioned number is called the designed minimum distance of $C^*(D,G)$. This we denote by d^*. The dual code $C(D,G)$ is, by the residue theorem, obtained as the image of the map

$$\alpha: L(G) \to \mathbb{F}_q^n$$
$$f \mapsto \left(f(P_1), \cdots, f(P_n)\right).$$

If $f_1, \cdots, f_k$ is a basis of $L(G)$, then $(f_i(P_j))$, $1 \leq i \leq k$, $1 \leq j \leq n$, is a parity check matrix of $C^*(D,G)$.

A rational differential form ω exists with simple poles at P_i and $\operatorname{res}_{P_i}(\omega) = 1$ for all $i = 1, \cdots, n$. Hence $C(D,G) = C^*(D, D+(\omega)-G)$ (see van der Geer [3, lemma 3.5]). We therefore restrict our attention to the codes $C^*(D,G)$ and henceforth denote them by C.

For every word $w \in \mathbb{F}_q^n$ we define the syndrome of w with respect to $f \in L(G)$ by

$$s(w,f) = \sum_{i=1}^{n} w_i f(P_i).$$

Notice that $s(w,f) = 0$ for all $f \in L(G)$ if and only if $w \in C$. Let $C^V := \{\gamma | \gamma: C \to \mathbb{F}_q \text{ is an } \mathbb{F}_q \text{ linear map}\}$. Define the syndrome map s of the code C in $\mathbb{F}_q^n$ by

$$s: \mathbb{F}_q^n \to L(G)^V$$
$$w \mapsto (f \mapsto s(w,f)).$$

A word w in $\mathbb{F}_q^n$ is a codeword if and only if $s(w) = 0$.

Let F be a divisor with support disjoint from the support of D. We define a map E_w, which we call the *error locator map* of w, by

$$E_w: L(F) \to L(G-F)^V$$
$$f \mapsto (h \mapsto s(w, fh)).$$

If $w = c + e$ with $c \in C$ and $g \in L(G)$, then $s(w,g) = s(e,g)$. Furthermore, $fh \in L(G)$ if $f \in L(F)$ and $h \in L(G-F)$. Hence $E_w = E_e$.

Let $w \in \mathbb{F}_q^n$. Define the support of w as $\mathrm{supp}(w) = \{P_i | w_i \neq 0,\ i = 1, \cdots, n\}$. If $Q_1, \cdots, Q_t$ are the places where w has an error, that is to say $w = c + e$, with $c \in C$ and $t = wt(e) = d(w, C)$ and $\mathrm{supp}(e) = \{Q_1, \cdots, Q_t\}$ then $L(F - \sum_{i=1}^{t} Q_i)$ is a linear subspace of $\ker E_w$.

Proposition 1: If $t < \dim L(F)$, then $L(F - \sum_{i=1}^{t} Q_i) \neq 0$.

The proof is trivial since one imposes t linear conditions on the vector space $L(F)$, which has dimension greater than t.

Proposition 2: If $\deg(G - F) > t + 2g - 2$, then

$$\ker E_w = L\left(F - \sum_{i=1}^{t} Q_i\right).$$

Proof: See [14]. For the proof of this proposition one uses the fact that the map $\phi(F, Q)$ defined by

$$\phi(F, Q)\colon L(G - F) \to \mathbb{F}_q^t$$
$$h \mapsto (h(Q_1), \cdots, h(Q_t))$$

having kernel $L(G - F - \sum_{i=1}^{t} Q_i)$, is surjective under the assumption $\deg(G - F) > t + 2g - 2$ by Riemann-Roch. Let $Q = (Q_1, \cdots, Q_t)$ and $Q_j = P_{ij}$, for $j = 1, \cdots, t$. Define the map $\pi_Q\colon \mathbb{F}_q^n \to \mathbb{F}_q^t$ by $\pi_Q(w) = (w_{i_1}, \cdots, w_{i_t})$. Define the map $i_Q\colon \mathbb{F}_q^t \to \mathbb{F}_q^n$ by $i_Q(v)_i = v_j$ if $i = i_j$ for some $j = 1, \cdots, t$ and $i_Q(v)_i = 0$ otherwise. Define the map s_Q by

$$s_Q\colon \mathbb{F}_q^t \to L(G)^V$$
$$v \mapsto \left(g \mapsto \sum_{i=1}^{t} v_i g(Q_i)\right).$$

Proposition 3: Let f be a nonzero element of $\ker E_w$. Assume $\deg(G - F) > e + g - 2$ and $g \leq e$. If w is a word and c a codword of $C = C^*(D, G)$ such that $w = c + e$ and $t = wt(e) = d(w, C) \leq e$ and $\mathrm{supp}(e) = \{Q_1, \cdots, Q_t\}$ is contained in the zero set of f, then the equation

$$s_Q(x) = s(w)$$

has the unique solution $\pi_Q(e)$.

Proof: See [14].

Algorithm A(F): Compute the matrix of E_w and its kernel. If $\ker E_w = 0$, then w has more than e errors. If $\ker E_w \neq, 0$ then choose a nonzero element f of $\ker E_w$.

Let $\{Q_1, \cdots, Q_t\} = \{P_i | f(P_i) = 0,\ i = 1, \cdots, n\}$ and $Q = (Q_1, \cdots, Q_t)$. If $s_Q(x) = s(w)$ has no or more than one solution, then w has more than e errors. If $s_Q(x) = s(w)$ has the unique solution x_0 and if $wt(x_0) > e$, then w has more than e errors. If $wt(x_0) \leq e$, then w is decoded by $w - i_Q(x_0)$.

Theorem 1: If $C^*(D, G)$ is an algebraic geometric code of word length n and designed minimum distance d^* on a curve of genus g and if, moreover, $e \leq (d^* - 1 - g)/2$, then for every divisor F of degree $e + g$ with support disjoint with the support of D the algorithm $A(F)$ decodes $C^*(D, G)$ up to e errors with complexity $O(n^3)$.

Proof: See [14] and also [12].

Remark 1: The two conditions $\dim(F) > e$ and $\deg(G - F) > e + 2g - 2$ together imply that $e \leq (d^* - 1 - g)/2$ in case $\Omega(F) = 0$ and $e \leq (d^* - 1)/3$ in case $\Omega(F) \neq 0$ by Clifford's theorem. There are two ways to improve the decoding error capacity of the algorithm:

1) by finding a divisor F such that $\dim \Omega(F)$ is nonzero and equal to g at best;
2) by applying the algorithm s times in parallel with different divisors $F_1, \cdots, F_s$ such that, for at least one i the algorithm $A(F_i)$ decodes the received word w in case w has at most $(d^* - 1)/2$ errors.

The first way is pursued by Skorobogatov and Vlădut [14] for codes on curves which are complete intersections, in which case the divisor G is a multiple hyperplane section. In the particular instance of plane curves, G is a line section. In such a case, G may be small. The second possibility is examined in the rest of this paper and in [14], where a modified decoding algorithm decodes up to $\lfloor (d^* - 1)/2 \rfloor$ errors for some codes, in particular for codes on elliptic curves.

Remark 2: The idea of an error locating map is generalized to arbitrary linear codes by Pellikaan [12].

II. The Algorithm s Times Executed

Let $\mathbb{D}_k := \{D | D \text{ effective divisor on } X \text{ of degree } k\}$ and $\mathbb{D}_k^s$ be the s-fold Cartesian product of $\mathbb{D}_k$. Let $\mathbb{D}_k = \emptyset$ for $k < 0$. Let $\mathrm{Pic}(X)$ be the Abelian group of all divisors on X modulo principal divisors, called the *Picard group* of X. If D is a divisor, then its class in $\mathrm{Pic}(X)$ is denoted by $[D]$. $\mathrm{Pic}^0(X)$ is the subgroup of $\mathrm{Pic}(X)$ of divisors of degree zero modulo principal divisors, also called the Jacobian of X and denoted by $J(X)$. The number of elements is called the class number of X and denoted by h, that is to say $h = \#J(X)$. For references see Mumford [11] and Serre [13].

Let s be an integer $s \geq 2$. Define the map ψ_k^s by

$$\psi_k^s\colon \mathbb{D}_k^s \to J(X)^{s-1}$$
$$D = (D_1, \cdots, D_s) \mapsto ([D_1 - D_2], \cdots, [D_{s-1} - D_s]).$$

Proposition 4: Let $D_0 \in \mathbb{D}_k$ and $\psi_k\colon \mathbb{D}_k \to J(X)$ be the map defined by $\psi_k(D) := [D - D_0]$. Suppose $k \geq g$. Then ψ_k is surjective.

Proof: This is a well-known consequence of the theorem by Riemann-Roch.

Corollary 1: Let s, k, and l be integers such that $s \geq 2$, $k \geq g$ and $l \leq g - 1$. Suppose ψ_l^s is not surjective. Then there is an s-tuple F in $\mathbb{D}_k^s$ such that $\psi_k^s(F)$ is not in the image of ψ_l^s.

Proposition 5: Let $e = \lfloor (d^* - 1)/2 \rfloor$. Let s and m be integers such that $s \geq 2$ and $m \geq 4g - 2$. Suppose ψ_{g-1}^s or ψ_{g-2}^s is not surjective in case m is odd or even, respectively. Then there exists an s-tuple $F = (F_1, \cdots, F_s)$ in $\mathbb{D}_{g+e}^s$ such that, for every e-tuple $Q = (Q_1, \cdots, Q_e)$ with $Q_1, \cdots, Q_e \in \{P_1, \cdots, P_n\}$, at least one i, $1 \leq i \leq s$, exists such that the map $\phi(F_i, Q)$ is surjective.

Proof: The map ψ^s_{g-j} is not surjective, for $j=1$ or 2 and hence there is an s-tuple $\boldsymbol{F}=(F_1,\cdots,F_s)$ in $\mathbb{D}^s_{g+e}$ such that $\psi^s_{g+e}(\boldsymbol{F})$ is not in the image of ψ^s_{g-j}, by Corollary 1. Let $\boldsymbol{Q}=(Q_1,\cdots,Q_e)$ with $Q_1,\cdots,Q_e\in\{P_1,\cdots,P_n\}$. If m is odd, then $e=(m-2g+1)/2\geq g$, since $d^*=m-2g+2$ and $m\geq 4g-1$. Hence $\deg(G-F_i)=e+g-1>2g-2$. Thus $\dim L(G-F_i)=e$ by the theorem of Riemann-Roch. If m is even, then $e=(m-2g)/2\geq g-1$, since $d^*=m-2g+2$ and $m\geq 4g-2$. Hence $\deg(G-F_i)=e+g>2g-2$. Thus $\dim L(G-F_i)=e+1$, by the theorem of Riemann-Roch. Thus the map $\phi(F_i,\boldsymbol{Q})$ is surjective if and only if $\dim\ker\phi(F_i,\boldsymbol{Q})=0$ or 1 in case m is odd or even, respectively. Now $\ker\phi(F_i,\boldsymbol{Q})=L(G-F_i-\sum_{j=1}^e Q_j)$ is zero- or one-dimensional if and only if $\Omega(G-F_i-\sum_{j=1}^e Q_j)=(0)$. Suppose for all i, $1\leq i\leq s$, the map $\phi(F_i,\boldsymbol{Q})$ is not surjective; then for all i a nonzero rational differential form ω_i exists such that $(\omega_i)\geq G-F_i-\sum_{j=1}^e Q_j$. All divisors of nonzero rational differential forms are equivalent modulo principal divisors and their class is denoted by K. Let $E_i=(w_i)-G+F_i+\sum_{j=1}^e Q_j$. Then E_i is an effective divisor of degree $g-1$ or $g-2$, in case m is odd or even, respectively. Thus $[E_i-F_i]=K-[G-\sum_{i=1}^e Q_j]$ does not depend on i. Thus $[E_{i_1}-E_{i_2}]=[F_{i_1}-F_{i_2}]$ for all i_1,i_2; $1\leq i_1,\ i_2\leq s$. Hence $\psi^s_{g-j}(\boldsymbol{E})=\psi^s_{g+e}(\boldsymbol{F})$ for $j=1$ in case m is odd and $j=2$ in case m is even. This is a contradiction. Thus the map $\phi(F_i,\boldsymbol{Q})$ is surjective for at least one i, $1\leq i\leq s$. This proves the proposition.

Remark 3: Proposition 5 holds *a fortiori* for every t-tuple $\boldsymbol{Q}=(Q_1,\cdots,Q_t)$ with $Q_1,\cdots,Q_t\in\{P_1,\cdots,P_n\}$ as long as $t\leq e=\lfloor(d^*-1)/2\rfloor$. Consequently, for every word w with errors at the places $Q_1,\cdots,Q_t$, there is at least one F_i such that $\ker E_w=L(F_i-\sum_{j=1}^t Q_j)$, as long as $t\leq e$.

Algorithm: Let $A(F_1,\cdots,F_s)$ be the algorithm $A(F_1),\cdots,A(F_s)$ run in parallel.

Theorem 2: Let $C^*(D,G)$ be an algebraic geometric code of word length n and designed minimum distance d^* on a curve of genus g. Let $4g-2\leq m=\deg G$. Let $e=\lfloor(d^*-1)/2\rfloor$. If ψ^s_{g-1} is not surjective in case m is odd and ψ^s_{g-2} is not surjective in case m is even, then an s-tuple $(F_1,\cdots,F_s)$ exists with all F_i of degree $e+g$ with support disjoint from the support of D such that the algorithm $A(F_1,\cdots,F_s)$ decodes $C^*(D,G)$ up to e errors with complexity $O(n^3s)$.

Proof: The proof of this theorem is similar to the proof of Theorem 1. Choose any s-tuple $\boldsymbol{F}=(F_1,\cdots,F_s)$ in $\mathbb{D}^s_{g+e}$ such that $\psi^s_{g+e}(\boldsymbol{F})$ is not in the image of ψ^s_{g-1} or ψ^s_{g-2} in case m is odd or even, respectively. Note that it is always possible to find a representative F_i which has support disjoint from the support of D (but then we can no longer insist on F_i being effective) by the theorem of independence of rational functions, see Chevalley [1].

At least one of the subroutines $A(F_i)$, for $i=1,\cdots,s$ decodes w, as long as w has not more than e errors (by Proposition 5), and they do so uniquely, that is if $A(F_{i_1})$ and $A(F_{i_2})$ decode, then they give the same codeword. Note that we can apply Proposition 3, since by assumption $e\geq g$ and $\deg(G-F)>e+g-2$, (see the proof of Proposition 5). This proves the theorem.

III. The Z-Function of a Curve

In this section we investigate whether the map ψ^s_{g-1}, and thus *a fortiori* ψ^s_{g-2}, is not surjective by means of the Z-function of the curve (see [3, sec. 4]). Let $a_k=\#\mathbb{D}_k$ and $Z(X,t)=\sum_{k=0}^\infty a_k t^k$. Then $Z(X,t)$ is called the *Z-function* of the curve X and $\zeta(X,s)=Z(X,q^{-s})$ the *zeta-function* of X. We state some of the main properties.

Property 1: $Z(X,t)=p(t)/(1-t)(1-qt)$, where $p(t)$ is a polynomial of degree $2g$ with integral coefficients.

Property 2: $Z(X,q^{-1}t^{-1})=q^{1-g}t^{2-2g}Z(X,t)$. The functional equation.

Property 3: $p(t)=\prod_{i=1}^g(1-\alpha_i t)(1-\bar{\alpha}_i t)$ where $|\alpha_i|=|\bar{\alpha}_i|=\sqrt{q}$.

Property 4: Let $N_r:=\#X(\mathbb{F}_{q^r})$. Then $N_r=q^r+1-(\sum_{i=1}^g\alpha_i^r+\bar{\alpha}_i^r)$.

Property 5: $|N_1-(q+1)|\leq 2g\sqrt{q}$, the Hasse-Weil bound.

Property 6: Let $h=\#J(X)$. Then $h=p(1)=\prod_{i=1}^g(1-\alpha_i)(1-\bar{\alpha}_i)$.

Property 7: Let $p(t)=\sum_{j=0}^{2g}p_j t^j$. Then $q^{g-j}p_j=p_{2g-j}$. This is a direct consequence of the functional equation.

Proposition 6:

$$a_k=\sum_{i+j=k}\frac{q^{i+1}-1}{q-1}p_j.$$

In particular

$$a_{g-1}=\frac{1}{q-1}\left(\sum_{i=g+1}^{2g}p_j-\sum_{j=0}^{g-1}p_j\right).$$

Proof:

$$Z(X,t)=\frac{\sum_{j=0}^{2g}p_j t^j}{(1-t)(1-qt)}=\left(\sum_{i=0}^{\infty}\frac{q^{i+1}-1}{q-1}t^i\right)\left(\sum_{j=0}^{2g}p_j t^j\right)$$
$$=\sum_{k=0}^{\infty}\left(\sum_{i+j=k}\frac{q^{i+1}-1}{q-1}p_j\right)t^k=\sum_{k=0}^{\infty}a_k t^k.$$

Hence

$$a_k=\sum_{i+j=k}\frac{q^{i+1}-1}{q-1}p_j.$$

In particular,

$$a_{g-1}=\frac{1}{q-1}\left(\sum_{j=0}^{g-1}q^{g-j}p_j-p_j\right)=\frac{1}{q-1}\left(\sum_{j=0}^{g-1}p_{2g-j}-p_j\right),$$

by Property 6. Hence

$$a_{g-1}=\frac{1}{q-1}\left(\sum_{j=g+1}^{2g}p_j-\sum_{j=0}^{g-1}p_j\right).$$

Remark 4: $h=p(1)=\sum_{j=0}^{2g}p_j$.

Corollary 2: If X is a curve such that $p_i \geq 0$ for all $i = 0, \cdots, 2g$, then

$$a_{g-1} \leq \frac{h}{q-1}.$$

Definition: A curve X is called maximal if q is a square and $\alpha_i = \bar{\alpha}_i = -\sqrt{q}$ for all i, that is, if N_1 achieves the Hasse-Weil upper bound.

Remark 5: If X is a maximal curve, then

$$h = \left(1+\sqrt{q}\right)^{2g} \qquad p_j = \binom{2g}{j} q^{j/2}$$

$$a_{g-1} = \frac{1}{q-1}\left(\sum_{j=g+1}^{2g}\binom{2g}{j}q^{j/2} - \sum_{j=0}^{g-1}\binom{2g}{j}q^{j/2}\right).$$

Example 1: For an elliptic curve over $\mathbb{F}_q$ with more than one rational point, one has that $a_{g-1} = a_0 = 1$ and $h > 1$ since $X(\mathbb{F}_q) = J(X)$ and $\#X(\mathbb{F}_q) > 1$ by assumption. Thus ψ_0^2 is not surjective and it suffices to take F_1, $F_2 \in \mathbb{D}_{1+e}$ such that $[F_1] \neq [F_2]$ to obtain a decoding algorithm, by Theorem 2, which decodes up to $\lfloor (d-1)/2 \rfloor$ errors. In case $m = \deg(G)$ is even, ψ_{g-2}^1 is not surjective, since $\mathbb{D}_{-1}^1$ is empty and thus $s = 1$ suffices. Driencourt and Michon found a decoding algorithm for elliptic codes which decodes up to about $d/4$ errors [2]. As pointed out in Remark 1, the modified decoding algorithm of Skorobogatov and Vlădut [14] decodes $\lfloor (d-1)/2 \rfloor$ errors for elliptic codes.

Example 2: Let $q = 4^2$ and X the plane curve over $\mathbb{F}_q$ defined by $x^5 + y^5 + z^5 = 0$. This is a Hermite curve of genus 6 and maximal, see [7]. The codes on this curve are investigated by Van Lint and Springer [10] and by Tiersma [15]. We have that $h = 5^{12}$ and $a_{g-1} = a_5 = 15\ 896\ 673$. Hence $a_{g-1}^7 = a_5^7 = 2.6^* 10^{50} \pm 10^{49}$ and $h^6 = 2.1^* 10^{50} \pm 10^{49}$. However, $a_{g-1}^8 < h^7$. Hence ψ_{g-1}^8 is not surjective. It still is a problem to find a concrete 8-tuple $\boldsymbol{F} = (F_1, \cdots, F_8)$ in $\mathbb{D}_{6+e}^8$ such that $\psi_{6+e}^8(\boldsymbol{F})$ is not in the image of ψ_{g-1}^8.

Example 3: This example we owe to Hansen; it shows that one does not always have $a_{g-1} \leq h/(q-1)$. Let X be the Klein quartic defined over $\mathbb{F}_4$. Then

$$Z(X,t) = \frac{1 - 9t^3 + 64t^6}{(1-t)(1-4t)}.$$

Hence $h = 56$ and $a_{g-1} = a_2 = 21$, which is greater than $h/(q-1)$.

The following proposition is due to van Wee.

Proposition 8: If $a_{g-1} \leq h/(q-1)$ and $q \geq 3$ and $s > 2g \log_{q-1}(1+\sqrt{q})$, then ψ_{g-1}^s is not surjective.

Proof: $h = \prod_{i=1}^{g}(1-\alpha_i)(1-\bar{\alpha}_i) \leq (1+\sqrt{q})^{2g}$, since $|\alpha_i| = |\bar{\alpha}_i| = \sqrt{q}$, by Property 3. If $s > 2g \log_{q-1}(1+\sqrt{q})$, then $(q-1)^s > (1+\sqrt{q})^{2g} \geq h$. Thus $a_{g-1}^s \leq (h/(q-1))^s < h^{s-1}$. Therefore, ψ_{g-1}^s is not surjective.

Remark 6: Let s be the smallest integer such that $s > 2g \log_{q-1}(1+\sqrt{q})$. Then $s = O(g)$ if $g \to \infty$. Moreover, if $q > 4$, then $1 + \sqrt{q} < q - 1$, hence $\log_{q-1}(1+\sqrt{q}) < 1$. Therefore, $s = 2g > 2g \log_{q-1}(1+\sqrt{q})$.

Corollary 3: If X is a maximal curve over $\mathbb{F}_q$ and $q > 4$, then ψ_{g-1}^{2g} and ψ_{g-2}^{2g} are not surjective.

The corollary shows that for maximal curves with $q > 4$, we do not need more than 2 g divisors F_i for the decoding algorithm in Theorem 2 to work.

Remark 7: Over $\bar{\mathbb{F}}_q$, $\mathbb{D}_{g-1}$ is the $(g-1)$-fold symmetric product of X and therefore a projective variety of dimension $g-1$. Thus $\mathbb{D}_{g-1}^{g+1}$ is a projective variety of dimension $g^2 - 1$. The Jacobian $J(X)$ is a projective variety of dimension g over $\bar{\mathbb{F}}_q$ and hence $J(X)^g$ has dimension g^2. Therefore, ψ_{g-1}^{g+1} is a proper map from a variety of dimension $g^2 - 1$ to a variety of dimension g^2 and hence it cannot be surjective over $\bar{\mathbb{F}}_q$. (see Mumford [11] or Serre [13]).

Questions:

1) Is it always true that for some s the map ψ_{g-1}^s is not surjective and, if so, what is an *a priori* bound for such an s. In particular, is it ture that $s = O(g)$ for $g \to \infty$?
2) Is it always true that ψ_{g-1}^{g+1} is not surjective?

Remark 8: Vlădut [16] informed me that ψ_{g-1}^s is not surjective for $s \geq 2g$ if either $q \geq 37$, or $q \geq 17$ and $g \geq g_0(q)$. Furthermore for some curves over $\mathbb{F}_2$, $\mathbb{F}_3$, or $\mathbb{F}_4$, the map ψ_{g-1}^s is surjective for any s.

IV. Conclusion and Questions

We conclude with the following theorem.

Theorem 3: Let X be a maximal curve over $\mathbb{F}_q$, with $q \geq 3$ and C an algebraic geometric code $C = C^*(D, G)$ with $m = \deg G$. If $4g - 2 \leq m$, then there is a decoding algorithm with complexity of order $O(n^4)$ which runs $O(n)$ subroutines in parallel each of complexity $O(n^3)$ and which decodes $\lfloor (d^* - 1)/2 \rfloor$ errors, where n is the word length, g the genus of the curve X, and d^* the designed minimum distance.

Proof: The proof follows by Theorem 2, Corollary 2, Remark 6, and Corollary 3, and since $O(g) = O(n)$ for g and $n \to \infty$ by the Hasse-Weil bound (Property 5).

Apart from the question for which s and the maps ψ_{g-1}^s and ψ_{g-2}^s are not surjective (questions 1 and 2, above), there is also the important question of finding an explicit element in $J(X)^{s-1}$ which is not in the image. Some property on the group $J(X)^{s-1}$ might give an element outside the image.

Acknowledgment

I wish to thank G. van der Geer, J. P. Hansen, H. J. Tiersma, and G. J. M. van Wee for their valuable discussions and their advice concerning algebraic geometry and coding theory.

REFERENCES

[1] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, vol. VI of *Math. Surveys*. New York: Amer. Math. Soc., 1951.

[2] Y. Driencourt and J. F. Michon, "Some properties of elliptic codes over a field of characteristic 2," in *Algebraic Algorithms and Error-Correcting Codes*, Notes in Computer Science 229 (1985), 185–193.

[3] G. van der Geer and J. H. van Lint, *Introduction to Coding theory and Algebraic Geometry*, DMV seminar, Band 12. Basel: Birkhäuser Verlag, 1988.

[4] V. D. Goppa, "Codes associated with divisors," *Problemy Peredachi Inform.*, vol. 13, pp. 33–39, 1977.

[5] ____, "Codes on algebraic curves," *Sov. Math. Dokl.*, vol. 24, pp. 170–172, 1981.

[6] ____, "Algebraic-geometric codes," *Math. USSR Izvestija*, vol. 21, pp. 75–91, 1983.

[7] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*. Oxford, England: Oxford Univ. Press, 1979.

[8] J. Justesen, K. J. Larsen, H. E. Jensen, A. Havemose, and T. Høholdt, "Construction and decoding of algebraic geometric codes, *IEEE Trans. Inform. Theory*, vol. IT-35, pp. 811–821, July 1989.

[9] J. H. van Lint, *Introduction to Coding Theory*. New York: Springer-Verlag, 1982.

[10] J. H. van Lint and T. A. Springer, "Generalized Reed solomon codes from algebraic geometry," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 305–309, 1987.

[11] D. Mumford, *Abelian Varieties*. Oxford, England: Oxford Univ. Press, 1974.

[12] R. Pellikaan, "On decoding linear codes by error locating pairs," preprint, Eindhoven, The Netherlands, 1988.

[13] J. P. Serre, *Groupes Algébriques et Corps de Classes*. Paris, France: Hermann et cie., 1959.

[14] A. N. Skorobogatov and S. G. Vlădut, "On the decoding of algebraic-geometric codes," preprint, Inst. Problems of Information Transmission, 1988.

[15] H. J. Tiersma, "Remarks on codes from Hermitian curves," *IEEE Trans. Inform. Theory*, vol. IT-33, no. 4, pp. 605–609, 1987.

[16] S. G. Vlădut, letter, Oct. 22, 1988.