On the gonality of curves, abundant codes and decoding

Ruud Pellikaan *

Appeared in: in *Coding Theory Algebraic Geometry*, Luminy 1991, (H. Stichtenoth and M.A. Tsfasman eds.), Lect. Notes Math. **1518**, Springer, Berlin, 1992, 132-144.

1 Introduction

Let $\mathcal{X}$ be a curve defined over the finite field $\mathbf{F}_q$ with q elements. The genus of $\mathcal{X}$ is denoted by $g(\mathcal{X})$, or more often by g. Let $P_1, \ldots, P_n$ be n distinct rational points on the curve $\mathcal{X}$. Let D be the divisor $P_1 + \ldots + P_n$. Let G be a divisor on $\mathcal{X}$ of degree m. The code $C_L(D, G)$ is defined as the image of $L(G)$ in $\mathbf{F}_q^n$, under the evaluation map $f \longmapsto (f(P_1), \ldots, f(P_n))$. Goppa [5] showed that the functional code $C_L(D, G)$ has dimension at least $m + 1 - g$ and minimum distance at least $n - m$ in case $m < n$. If moreover $m > 2g - 2$, then the dimension is equal to $m + 1 - g$. We call $n - m$ the Goppa designed minimum distance of $C_L(D, G)$, and denote it by d_G. Tsfasman, Vlăduţ, Zink and Ihara showed that modular curves have many rational points with respect to the genus, if q is a square, that is to say $N \sim (\sqrt{q} - 1)g$, see [21, 4.1.52]. In case $q \geq 49$ the Tsfasman-Vlăduţ-Zink bound R_{TVZ} gives an improvement of the Gilbert-Varshamov bound R_{GV}, see [21, 3.4.4]. In the corners, where the graphs of R_{TVZ} and R_{GV} meet, Vlăduţ made a slight improvement, moreover he showed that there are codes, comming from curves, with parameters lying on the maximum of the above mentioned bounds, see [21, 3.4.11]. Later Pellikaan, Shen and van Wee [14] proved that every linear code can be represented with a curve, but if one imposes the condition $m < n$, then long binary algebraic-geometric codes have information rate at most $\frac{1}{2}$. So the question of finding good codes can be restated in the question: Which divisors give good codes ?
There are two ways to improve the bounds Goppa gave. In the first place by taking divisors such that the dimension is bigger than $m + 1 - g$. These are so called special divisors. If the field of constants is algebraically closed and $g - k(g - m + k - 1) \geq 0$, then there exists a divisor of degree m and dimension at least k , by Brill-Noether theory. But this is no longer true over a finite field. The second possibility, which we will pursue in this paper, is to try to improve the bound on the minimum distance.
In section 2 we show that the minimum distance is at least $\mathrm{t}(\mathcal{X}) - a$ for an abundant

*Department of Mathematics and Computing Science of the Eindhoven University of Technology, P.O. Box 513, MB 5600 Eindhoven, The Netherlands, email ruudp@win.tue.nl

divisor of abundance a, that is for a divisor which is equivalent to $D + A$, where A is an effective divisor of degree a. The number $\mathrm{t}(\mathcal{X})$ is the minimal degree of a map from the curve to the projective line, also called the gonality of the curve. This was proved by Goppa [5, section 10] in the case $a = 0$, he called such codes canonical. It is easily seen that $\mathrm{t}(\mathcal{X}) \geq N/(q+1)$, where N is the number of rational points of the curve $\mathcal{X}$. In section 3 we show that abundant codes give asymptotically good codes for small relative minimum distance, better than the TVZ-bound, but still worse than the GV-bound. We discuss upper bounds of the gonality in section 4, using upper bounds for the parameters of codes. We will give an application to the error correcting capacity of some codes in section 5. We use the book of Tsfasman and Vlăduţ [21] as a reference, but our notation is different. We denote the functional code $(\mathcal{X}, D, G)_L$ by $C_L(D, G)$, and the residue code $(\mathcal{X}, D, G)_\Omega$ by $C_\Omega(D, G)$.

2 Abundant codes

In this section we show that divisors equivalent with $D + A$, so called abundant divisors, give an improvement on the bound of Goppa on the minimum distance. As a preparation we define the gonality of a curve and proof some simple properties. At the end we give some examples with the Hermitian curve and weighted Reed-Muller codes.

Definition 2.1 The *gonality* of a curve $\mathcal{X}$ over a field $\mathbf{F}$ is the smallest degree of a non-constant map, defined over the field $\mathbf{F}$, from $\mathcal{X}$ to the projective line. We denote the gonality of $\mathcal{X}$ by $\mathrm{t}(\mathcal{X})$, or shortly by t.

Lemma 2.2 *If E is a divisor of degree smaller than $t(\mathcal{X})$, then $l(E) \leq 1$.*

Proof If $l(E) > 1$, then there exists a non-constant rational function f such that $(f) \geq -E$, so $(f)_\infty \leq E$. One can consider f as a non-constant map, defined over the field of constants, from $\mathcal{X}$ to the projective line. The degree of this map is equal to $\deg((f)_\infty)$, which is at most $\deg(E)$, and smaller than $\mathrm{t}(\mathcal{X})$, by assumption. This gives a contradiction with the definition of the gonality of $\mathcal{X}$. □

Corollary 2.3 $t \leq g + 1$.

Proof Over a finite field there exists a divisor of degree $g + 1$, see [11, Theorem 3.2], and such a divisor has dimension at least 2, by the Riemann-Roch Theorem. Now the claim follows from Lemma 2.2. □

Corollary 2.4 *If $\mathcal{X}$ has a rational point and $deg(E) \geq t - 1$, then $l(E) \leq deg(E) + 2 - t$.*

Proof Let P be a rational point of $\mathcal{X}$. Let $b = \deg(E) - t + 1$. Then $b \geq 0$, since $\deg(E) \geq t - 1$. Let $F = E - bP$. If $l(E) > \deg(E) + 2 - t$, then $l(F) \geq l(E) - b > 1$. But $\deg(F) = t - 1$, which contradicts Lemma 2.2. □

Remark 2.5 The gonality is one if and only if $\mathcal{X}$ is isomorphic with the projective line. The gonality of a curve is two if and only if the curve is elliptic or hyperelliptic.
For a plane curve of degree m with a rational point P one can project the curve with

center P to a line outside this point. In this way we get a map from the curve to the projective line of degree at most $m-1$, so the gonality is at most $m-1$. In fact the gonality is equal to $m-1$, which follows from Namba [12] in characteristic zero, and Homma [6] in general. Coppens [2] considered the gonality of plane curves with nodes.
If the field of constants is algebraically closed, then $\mathrm{t}(\mathcal{X}) \leq \lfloor (g+3)/2 \rfloor$, by Brill-Noether theory, and equality holds for a general curve. The above inequality is not true over a finite field, as the following example shows. Consider a smooth plane curve of degree four over a finite field without rational points. Such curves exist. Take for example the curve with equation $X^4+Y^4+Z^4=0$ over $\mathbf{F}_5$. The fourth power of an element in $\mathbf{F}_5$ is either zero or one, so $x^4+y^4+z^4$ is equal to 0,1,2 or 3 whenever 3,2,1 or 0, respectively, out of the three elements $x, y, z \in \mathbf{F}_5$ are zero. Thus this curve has no $\mathbf{F}_5$-rational points. Another example is the curve with equation $X^4+Y^4+Z^4+Y^2Z^2+X^2Z^2+X^2Y^2+X^2YZ+XY^2Z+XYZ^2$ over $\mathbf{F}_2$. If there exists an effective special divisor of degree m and dimension k on a curve of genus g, then there exists an effective special divisor of degree $2g-2-m$ and dimension $k-m-1+g$, by the Riemann-Roch Theorem. A smooth plane curve of degree 4 has genus 3. If such a curve has no rational points, then its gonality is 4. Otherwise there exists an effective divisor of degree 3 and dimension 2, so this divisor is special and by the above remark there is an effective special divisor of degree one, thus there is a rational point, which is a contradiction. Therefore the gonality of such curves is 4, which is greater than $\lfloor (g+3)/2 \rfloor$.
This example shows that the gonality can change if one extends the field of constants.
The above example also shows that the upperbound $g+1$ in Corollary 2.3 can be obtained for curves of genus greater than 1. If a curve has gonality $g+1 > 2$, then it has no rational points, it even has no effective divisors of degree $g-2$. Otherwise, let A be an effective divisor of degree $g-2$, then there exists a canonical divisor K with support disjoint from A. So $l(K-A) \geq l(K) - \deg(A) = 2$, and $\deg(K-A) = g$. Thus $t \leq g$, by Lemma 2.2. Thus a curve of gonality $g+1 > 2$ has no effective divisors of degree $g-2$, and therefore it has no rational points over an extension of degree $g-2$. So $g < 2\log_q(2g)+1$, by the Hasse-Weil bound, thus $g \leq 10$ and $q \leq 31$.
In section 4 we will consider upper bounds for the gonality of curves over a finite field using coding theory.

Remark 2.6 Over a finite field one has the following lower bound, which is proved and used by Rosenbloon and Tsfasman [15, Lemma 1.1]. A similar reasoning can be found in a paper of Lewittes [9], where it is proved that $N \leq qa+1$, if a is non-gap of a rational point. A third place where this reasoning can be found is in a paper of Lachaud and Martin-Deschamps [8], where it is applied to all finite extensions of $\mathbf{F}_q$ to get a relation between the zeta function and the gonality of the curve.

Proposition 2.7 *Let $\mathcal{X}$ be a curve defined over $\mathbf{F}_q$. Let N be the number of rational points of $\mathcal{X}$. Then $t(\mathcal{X}) \geq N/(q+1)$.*

Proof Let f be a non-constant map, defined over $\mathbf{F}_q$, of degree $t = \mathrm{t}(\mathcal{X})$. Then the rational points on $\mathcal{X}$ are mapped to the $q+1$ rational points on the projective line. The map has degree t, so there are at most t rational points on $\mathcal{X}$ above a rational point on the projective line. So the number of rational points N on $\mathcal{X}$ is at most $t(q+1)$. $\square$

Definition 2.8 A divisor with support disjoint from the support of D and which is linear equivalent with $D+A$ for some effective divisor A is called *abundant*, and $\deg(A)$ is called the *abundance* of G. If G is an abundant divisor, then the code $C_L(D,G)$ is called *abundant*.

Remark 2.9 The name abundant refers to the fact that the degree of such divisors is at least n, whereas in Goppa's bound one assumes $m < n$. In [14, Proposition 11] it is proved that binary AG codes (i.e. binary codes of the form $C_L(D,G)$ such that $m < n$) of length longer than 13 have information rate smaller than $1/2$.
Note that $C_L(D,G) = C_\Omega(D, K-A)$, for some canonical divisor K [18, Corollary 2.6]. So abundant codes of abundance zero are also of the form $C_\Omega(D,K)$, where K is a canonical divisor. These codes were called *canonical* by Goppa [5, section 10].
For every effective divisor A there exists a divisor G with support disjoint from the support of D, which is equivalent with $D+A$, by the independance of valuations [1]. But it is not true that for every divisor G of degree at least n there exists an effective divisor A such that G is equivalent to $D+A$.

Lemma 2.10 *Let G be equivalent with $D+A$, for some effective divisor A. If there exists a non-zero code word in $C_L(D,G)$ of weight d, then $l(P_{i_1}+\ldots+P_{i_d}+A) > 1$ for some $i_1 < \ldots < i_d$.*

Proof Let $\mathbf{c}$ be a non-zero codeword of weight d. After a permutation of $P_1, \ldots P_n$, we may assume that the first d coordinates of $\mathbf{c}$ are non-zero. So there exists an $f \in L(G)$ such that $f(P_i) = c_i$. Thus $(f) \geq -G$ and $f(P_i) = 0$ for all $i > d$. Therefore $(f) \geq -G + P_{d+1} + \ldots + P_n$, since G has disjoint support with D. Let $E = (f) + G - (P_{d+1} + \ldots + P_n)$. Then E is effective and

$$E \sim G - (P_{d+1} + \ldots + P_n) \sim D + A - (P_{d+1} + \ldots + P_n) \sim P_1 + \ldots + P_d + A$$

If $P_i \in \mathrm{supp}(E)$ for some $i \leq d$, then $c_i = f(P_i) = 0$ for $i \leq d$, which is a contradiction. Thus E and $P_1 + \ldots + P_d + A$ are equivalent but not equal. Thus $l(P_1 + \ldots + P_d + A) > 1$. □

Theorem 2.11 *Let $\mathcal{X}$ be a curve over $\mathbf{F}_q$ with N rational points and of gonality t. If G is an abundant divisor of abundance a and $a < t$, then $C_L(D,G)$ is an $[n,k,d]$ code such that $d \geq t - a$ and $k \geq n + a - g$. If moreover $n + a > 2g - 2$, then $k = n + a - g$.*

Proof The special case $a = 0$ is treated by Goppa [5, section 10]. The statement about the minimum distance follows directly from Lemma 2.10 and 2.2. The code $C_L(D,G)$ is the image under the evaluation map of the vector space $L(G)$ and $l(G) \geq n + a + 1 - g$, by the Riemann-Roch Theorem, and equality holds in case $n + a > 2g - 2$. The kernel of this map is equal to $L(G - D)$, which is isomorphic to $L(A)$, since G is equivalent with $D + A$. The dimension of $L(A)$ is 1, by lemma 2.2, since $a < t$. Thus the dimension of the code is at least $n + a - g$, and equality holds in case $n + a > 2g - 2$. □

Remark 2.12 If G is equivalent with $D - A$, for some effective divisor A, then the minimum distance of $C_L(D,G)$ is at least t, since $C_L(D,G)$ is contained in $C_L(D, G+A)$ and the last one is abundant of abundance zero.

Definition 2.13 We call t the *abundant* designed minimum distance, and denote it by d_A.

Example 2.14 A specific case of an abundant code is studied in [14, Proposition 15]. There it is shown that the binary [7,4,3] Hamming code is canonical, see also [11, 5.7.1]. The curve used is a smooth plane curve of degree 4, hence of genus 3, which goes through all the 7 rational points of the projective plane. If we take for D the sum of these 7 points, and for G a divisor equivalent with D, and disjoint support with D, we get a $[7, 4, \geq 3]$ code, by Theorem 2.11, which must be the [7,4,3] Hamming code.

Example 2.15 The Hermitian plane curve with equation $X^{r+1} + Y^{r+1} + Z^{r+1} = 0$ over $\mathbf{F}_q$, where $q = r^2$, has $r^3 + 1$ rational points and genus $r(r-1)/2$. So the gonality is at least $(r^3+1)/(r^2+1)$, by Proposition 2.7, and at most r, since the curve is a plane curve of degree $r+1$, see Remark 2.5. Thus the gonality is equal to r. Fix any of the rational points and call it P_∞, and let D be the sum of the remaining r^3 rational points. Let $n = r^3$ and $G_m = mP_\infty$. The code C_m, where $C_m = C_L(D, G_m)$ is extensively studied. If $m < n$, then the Goppa designed minimum distance d_G is equal to $n - m$. If $m < n$ and m is a multiple of r or $m \leq n - q$, then the true minimum distance of C_m is equal to d_G, see Stichtenoth [19, Theorem 4]. Yang and Kumar [24] and Xing [23] proved that C_m has minimum distance at most $n - m + t$, in case $m < n$ and $m = rs + t$ and $0 \leq t \leq r - 1$. Furthermore the divisor $r^3 P_\infty$ is equivalent with D, see [20] or [19]. Thus if $m \geq n$, then G_m is an abundant divisor of abundance $m - n$. Therefore C_{n+a} is an $[r^3, r^3 + a - r(r-1)/2, \geq r - a]$ code for all $0 \leq a < r$, by Theorem 2.11. Every line over $\mathbf{F}_q$ either intersects the curve in exactly $r+1$ different rational points or is tangent to a rational point with multiplicity $r+1$, i.e. the rational points of a Hermitian curve form a $2 - (r^3 + 1, r + 1, 1)$ design. If l is the tangent line to the curve at P_∞ and m is another line through P_∞ containing the points $P_1, \ldots P_r, P_\infty$, then the rational function m/l has divisor $P_1 + \ldots + P_r - rP_\infty$, so $l(P_1 + \ldots + P_r) > 1$. Thus the minimum distance of C_n is exactly r, by Lemma 2.10. Similarly there exists a rational function with divisor $P_1 + \ldots + P_{r-1} + P_\infty - rP_r$, thus the minimum distance of C_{n+1} is exactly $r - 1$. We also get as a result that the codes C_m have at least minimum distance r, for all $n - r \leq m < n$, by Remark 2.13. Yang and Kumar [24] and Xing [23] proved that in fact equality holds.

Definition 2.16 Let $\mathbf{w} = (w_1, \ldots, w_l)$ be an l-tuple of positive integers such that $w_1 \leq \ldots \leq w_l$. Let

$$V(\mathbf{w}, m, l, q) = \{f \in \mathbf{F}_q[X_1, \ldots, X_l] | \deg_{\mathbf{w}}(f) \leq m\},$$

where $\deg_{\mathbf{w}} X_1^{e_1} \ldots X_l^{e_l} = \sum_i w_i e_i$, and $deg_{\mathbf{w}}(f)$ is the largest weighted degree of a monomial in f with a non-zero coefficient. Let $P_1, \ldots, P_n$ be the q^l rational points of the affine space over $\mathbf{F}_q$ of dimension l. Define $WARM(\mathbf{w}, m, l, q)$, the *weighted affine Reed-Muller* code of weight $\mathbf{w}$, order m and lenth q^l over q, as follows

$$WARM(\mathbf{w}, m, l, q) = \{(f(P_1), \ldots, f(P_n)) | f \in V(\mathbf{w}, m, l, q)\}.$$

Remark 2.17 The definition of the weighted affine Reed-Muller code is due to Sørensen [17], who proved that the minimum distance is equal to $(q-c)q^{l-b-1}$, where $b = \max\{i | m \geq (q-1)(w_1 + \ldots + w_i)\}$, and $c = \max\{s | m \geq (q-1)(w_1 + \ldots w_b) + sw_{b+1}\}$. This code

appears on the curve $\tilde{\mathcal{X}}(l,q)$ in [14]. This curve has q^l+1 rational points over $\mathbf{F}_q$, one of them is called $\tilde{P}_\infty$ and $P_1,\ldots,P_n$ are the remaining rational points. Let $D=P_1+\ldots+P_n$. Then $WARM(\mathbf{w},m,l,q)=C_L(D,m\tilde{P}_\infty)$, see [17, Example 4.1].

Proposition 2.18 *Let $w_i=q^{l-i}(q+1)^{i-1}$, for $1\leq i\leq l$, and $\mathbf{w}=(w_1,\ldots,w_l)$. If $m\geq q^l$, then $WARM(\mathbf{w},m,l,q)$ is an abundant code.*

Proof One has

$$\prod_{\alpha}(z_1-\alpha)=D-n\tilde{P}_\infty,$$

where α runs over all the elements of $\mathbf{F}_q$. Hence G is equivalent with $D+(m-n)\tilde{P}_\infty$. Thus G is abundant, since $m=\nu(q+1)^{l-1}\geq q^l=n$, and therefore $WARM(\mathbf{w},m,l,q)$ is abundant, by Remark 2.18. □

Remark 2.19 The curve $\tilde{\mathcal{X}}(l,q)$ has q^l+1 rational points over $\mathbf{F}_q$. Thus the gonality t of $\mathcal{X}(l,q)$ is at least $(q^l+1)/(q+1)$. The value q^{l-1} is a non-gap of the point $\tilde{P}_\infty$, so $t\leq q^{l-1}$. If $0\leq b\leq q-1$ and $m=q^l+bq^{l-2}$, then the abundant designed distance of $C_L(D,m\tilde{P}_\infty)$ is $d_A=t-bq^{l-2}$, so $(q^l+1)/(q+1)-bq^{l-2}\leq d_A\leq q^{l-1}-bq^{l-2}$, by our results. Sørensen [17] proved that the true minimim distance is $(q-b)q^{l-2}$, see Remark 2.18. So we are left with the following question: Is the gonality of the curve $\tilde{\mathcal{X}}(l,q)$ equal to q^{l-1} ?

3 Abundant codes are asymptotically good

In this section we consider the parameters of asymptotically good abundant codes. As usual we denote the information rate k/n by R, and the relative minimum distance d/n by δ.

Definition 3.1 Let $A(q)$ be the limes superior of all quotients N/g, taken over all curves $\mathcal{X}$ over $\mathbf{F}_q$ with N rational points and genus g. Let $\gamma_q=1/A(q)$.

Definition 3.2 Define the function R_A as follows.

$$R_A(\delta)=\begin{cases}1+\frac{1}{q+1}-\gamma_q-\delta & \text{for } 0\leq\delta\leq\frac{1}{q+1}\\ 1-(q+1)\gamma_q\delta & \text{for } \frac{1}{q+1}\leq\delta\leq\frac{\sqrt{q}-1}{q+1}\end{cases}$$

We call the graph of R_A the abundant- or A-bound.

Proposition 3.3 *If q is a square of a prime power, then for every $0\leq\delta\leq(\sqrt{q}-1)/(q+1)$ there exists a sequence of abundant codes of increasing length such that the relative minimum distance is at least δ and the information rate is at least $R_A(\delta)$.*

Proof By Theorem 2.11 and Proposition 2.7, there exist abundant codes such that $k\geq n+a+N/(q+1)-g$ and $d\geq N(q+1)-a$, for all n and a such that $n\leq N$ and $0\leq a<N/(q+1)$, if there exists a curve with N rational points. It follows from the work of Tsfasman, Vlăduţ, Zink and Ihara, see [21], that $\gamma_q=1/(\sqrt{q}-1)$. If we take $n=N$

and $0 \leq a < N/(q+1)$, then we get the result for δ in the first interval; and if $a = 0$ and $0 < n < N$, then for δ in the second interval. $\Box$

Remark 3.4 In Figures 1, 2, 3, and 4, respectively, we give the graphs of these functions in case $q = 4, 9, 16$ and 25, respectively, on scale. The A-bound is always below the GV-bound, and for $0 \leq \delta < q - \sqrt{q} + 2$, the A-bound is above the TVZ-bound.
It is not difficult to show that the codes obtained by Katsman and Tsfasman [21, 3.4.23], using subfield subcodes of algebraic-geometric codes, are always better than the A-bound.
Concatenation of abundant codes over $\mathbf{F}_4$ with a [3,2,2] binary code, gives binary codes above the line $R + \delta = 2/15$, also this bound is below the KT-bound
Codes on the TVZ- and KT-bound, and also abundant codes have a polynomial construction. It is not known whether codes on the GV-bound have a polynomial construction.

4 Applications of bounds on codes to bounds on the gonality

Remark 4.1 We used that the gonality of a curve is always at least $N/(q+1)$, but maybe there exists a sequence of curves with many rational points and high gonality. Let $\mathcal{X}_{2^m}$ be the modular curve over $\mathbf{F}_p$, p a prime, as defined in [21, 4.1.50]. Then this curve has at least $2^{m-3}(p-1)$ rational points over $\mathbf{F}_q$, where $q = p^2$, and genus $2^{m-3} + 1 - \delta_m$, where δ_m is equal to $3.2^{m/2-2}$ in case m is even, and $2^{(m-1)/2}$ in case m is odd, see [21, 4.1.59]. So the gonality of the curve is at least $2^{m-3}(\sqrt{q}-1)/(q+1)$, by Proposition 2.7. The divisor $2^{m-4}\infty$ has dimension 2 and degree 2^{m-4}, see [21, 4.1.60]. So the gonality of the curve is at most 2^{m-4}, which is asymptotically of the size $g/2$, see Remark 2.5.

Question Is there a sequence of curves over $\mathbf{F}_q$ with an increasing number of rational points such that $\mathcal{X}(\mathbf{F}_q) \sim (\sqrt{q}-1)g$ and $t \sim g/2$?

A positive answer would give a considerable improvement of the asymptotic parameters of abundant codes. So we are looking for curves with high gonality. We already remarked in 2.5 that $\mathrm{t}(\mathcal{X}) \leq \lfloor (g+3)/2 \rfloor$, for a curve $\mathcal{X}$ over an algebraically closed field. In the sequel we investigate upper bounds on the gonality over finite fields, by applying bounds on codes.

Proposition 4.2 *If there exists a curve over $\mathbf{F}_q$ of genus g and gonality t with N rational points, then*

$$g \geq log_q(\sum_{i=0}^{e} \tbinom{N}{i}(q-1)^i),$$

where $e = \lfloor (t-1)/2 \rfloor$.

Proof This result is due to Goppa [5, section 10]. There exists an $[N, k, d]$ code such that $k \geq N - g$ and $d \geq t$. The Hamming bound gives

$$q^k \leq A(N,d) \leq q^N / V_q(N,e),$$

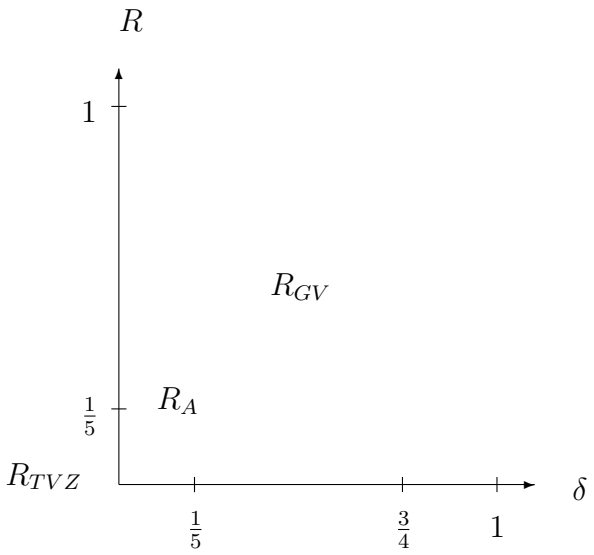

Figure 1: Bounds for $q = 4$, on scale

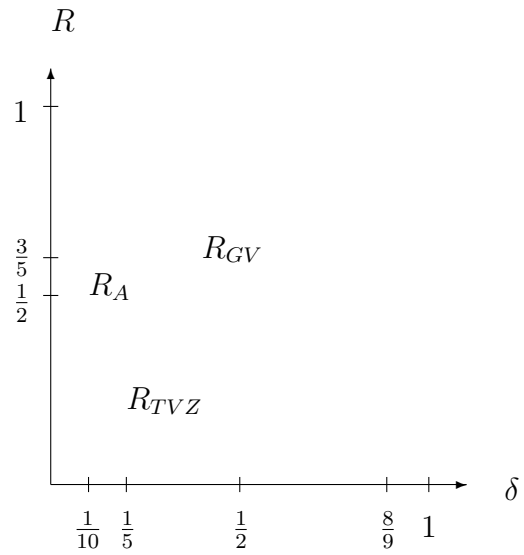

Figure 2: Bounds for $q = 9$, on scale

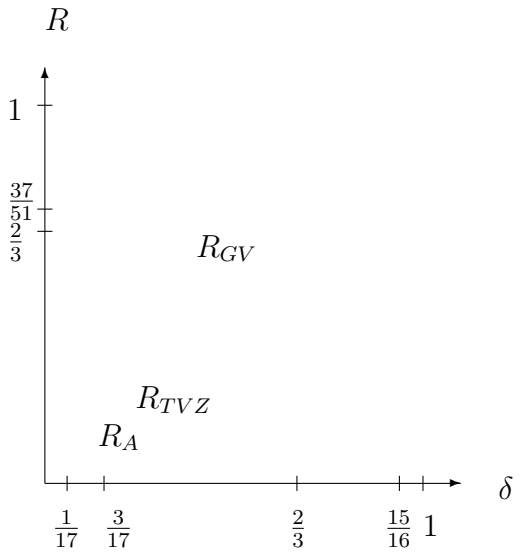

Figure 3: Bounds for $q = 16$, on scale

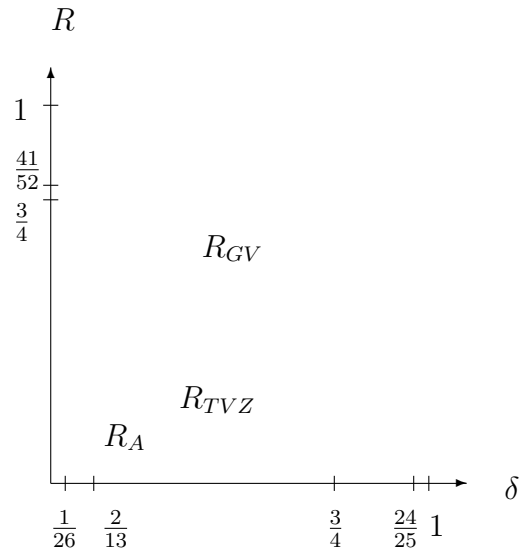

Figure 4: Bounds for $q = 25$, on scale

Figure 5: Bounds , not onscale

Figure 6: Bounds , not on scale

see [21, 1.1.41]. Hence $V_q(N,e) \leq q^{N-k} \leq q^g$. Taking the q-logarithm gives the desired result. □

Proposition 4.3 *Let $\theta = (q-1)/q$. Let n and N be positive integers such that $n \leq N$. If there exists a curve over $\mathbf{F}_q$ of genus g, gonality t and N rational points, then*

$$n + log_q(1 - \theta N/t) \leq g \quad if \quad t > \theta n$$

$$t - \theta log_q(t) < \theta g + 1 \quad if \quad t \leq \theta N$$

Proof The proof is similar to the application of the Hamming bound on abundant codes, but now with the Plotkin bound on abundant codes, see [10, 5.2.4 and 5.2.5]. □

Remark 4.4 We give another application of the Plotkin bound, now on the existence of special divisors. Brill-Noether says that if $g - k(g - m + k - 1 \geq 0$, then on a curve of genus g there exists a divisor of degree m and dimension at least k. Take the particular case $m = g - 1$ and $k^2 \geq g$, then there exists a divisor of degree g-1 and dimension at least $\sqrt{g}$. If we apply this to Goppa's construction on this curve, then we get a code of length equal to the number of rational points on the curve, the dimension is at least $\sqrt{g}$, and the minimum distance is at least $n - g + 1$. If we use a sequence of modular curves, then we get a sequence of codes with information rate $R \geq \sqrt{\gamma_q}$, and relative minimum distance $\delta \geq 1 - \gamma_q$, see [21]. In particular for $q = 9$ we get $\gamma_9 = 1/2, R \geq \sqrt{2}/2$, and $\delta \geq 1/2$. But the Plokin bound gives the upper bound $R \leq 1 - \delta q/(q-1)$ for such a sequence, so in the above case, we get $R \leq 7/16$, which is a contradiction. This is one example, but for many m and q one gets a lower bound for R conflicting with an upper bound, like the Plotkin bound.

Remark 4.5 We are interested in asymptotically good abundant codes, and the asymptotic Plotkin bound implies that curves of gonality t and N rational points such that $t > N(q-1)/q$ do not give asymptotically good codes. We therefore give the following definition.

Definition 4.6 Let λ_q be the limes superior of the set of quotients t/g, taken over all curves over $\mathbf{F}_q$ of genus g, gonality t and at least $tq/(q-1)$ rational points.

Proposition 4.7

$$\lambda_q \leq (q-1)/q$$

$$(\sqrt{q}-1)/(q+1) \leq \lambda_q \quad if\ q\ is\ a\ square$$

Proof The first inequality follows immediately from Proposition 4.3, since $\theta \log_q(t)/g \leq \theta \log_q(g+1)/g$, by Corollary 2.3, and the last expression tends to zero if g tends to infinity. The second inequality follows from Proposition 2.7 and the existence of curves with $N \sim (\sqrt{q}-1)g$ rational points whenever q is a square, see [21]. □

Remark 4.8 The asymptotic Hamming bound gives $H_q(\delta/2) \leq \gamma$, if δ and γ are the asymptotic relative distance and relative genus of a sequence of curves. But one verifies in a straightforward way that $H_q(\gamma_q/2) \leq \gamma_q$, if q is a square, so this gives not an improvement of the bound $\lambda_q \leq 1$.

5 An application to decoding

The dual of the functional code $C_L(D,G)$ is the residue code $C_\Omega(D,G)$, which is the image of the residue map from $\Omega(G-D)$ to $\mathbf{F}_q^n$, see [21], and is an [n,k,d] code such that $k \geq n-m+g-1$ and $d \geq m-2g+2$, if $m > 2g-2$. If morover $m < n$, then $k = n-m+g-1$. We call $m-2g+2$ the Goppa designed minimum distance of $C_\Omega(D,G)$, and denote it by d_G. It is known that every functional code $C_L(D,G)$ is also a residue code, i.e. of the form $C_\Omega(D,G')$, where $G' = K+D-G$, for some canonical divisor K, see [18, Corollary 2.6]. Now we discuss the decoding of $C_\Omega(D,G)$. Let F be a divisor such that F has disjoint support with D and furthermore

1. $\dim(L(F)) > e$
2. $d(C_\Omega(D,G-F)) > e$
3. $d(C_L(D,G)) + d(C_\Omega(D,G)) > n$

Then one can decode e errors with F, see [7], [16] and [21, 3.3]. There always exists such a divisor F if $e = \lfloor (d_G-1-g)/2 \rfloor$. By applying the above idea several times one can decode $\lfloor (d_G-1)/2 \rfloor$ errors, see [13] and[22], but an efficient algorithm to find these divisors is known only in case of (hyper)elliptic curves, see [16] and [3]. Ehrhard [4] showed that one can decode $\lfloor (d_G-1-g+t)/2 \rfloor$ errors with $t+1$ divisors, given explicitly.
Now we want to apply section 2 to decoding. If the minimum distance of $C_\Omega(D,G-F)$ is more than one expects, i.e. $\deg(G-F)-2g+2$, then maybe one can decode more than $e = \lfloor (d_G-1-g)/2 \rfloor$ errors with a single F; and indeed this is the case. Before we do that we need a slight change of the conditions 2 and 3. Remark that condition 2 is equivalent with

4. $C_\Omega(Q,G-F) = 0$ for all Q such that $0 \leq Q \leq D$ and $\deg(Q) \leq e$

Furthermore $C_\Omega(Q,G-F) = 0$ if and only if $\Omega(G-F) = \Omega(G-F-Q)$. Consider the following condition

5. $\Omega(G-F-Q) = 0$ for all Q such that $0 \leq Q \leq D$ and $\deg(Q) \leq e$

Duursma [3] showed that conditions 1 and 5 imply that one can decode e errors with F.

Lemma 5.1 *Let $\mathcal{X}$ be a curve of gonality t. Let $P_1,\ldots,P_n,P_\infty$ be $n+1$ distinct rational points on $\mathcal{X}$. Let $D = P_1+\ldots+P_n$. Let F_0 be a divisor of dimension at least $e+2$. Let A be an effective divisor of degree $t-e-1$ and disjoint support with D andP_∞. Let K be a canonical divisor with disjoint support with D and such that P_∞ is not in the negative part of K. Let $G = F_0+K-A$ and $F = F_0-P_\infty$. Then one can decode e errors of $C_\Omega(D,G)$ with F.*

Proof The dimension of $L(F)$ is at least $e+1$, since the dimension of $L(F_0)$ is at least $e+1$ by assumption. Furthermore $G-F_0 = K-A$, so $C_\Omega(D,G-F_0)$ is an abundant code of abundance $t-e-1$, by Remark 2.10, and therefore its minimum distance is at least $e+1$. So $\Omega(G-F_0) = \Omega(G-F_0-Q)$ for all Q such that $0 \leq Q \leq D$ and $\deg(Q) \leq e$, by Remark 5.1. Now $\Omega(G-F_0) = \Omega(K-A)$, which is equal to $\Omega(K)$, since A is effective and

of degree smaller than the gonality t. Thus $\Omega(G - F_0)$ is one dimensional and generated by a differential ω with support K. So $\Omega(G - F_0 - Q) = \Omega(K - A - Q)$, is generated by ω, and the valuation of ω and $K - A$ at P_∞ are the same, since P_∞ is not in the negative part of K and not in the support of $A + Q$. Hence $\Omega(G - F - Q) = 0$, for all Q such that $0 \leq Q \leq D$ and $\deg(Q) \leq e$. Thus conditions 1 and 5 are satisfied, and one can decode e errors with F. $\Box$

Proposition 5.2 *Let $\mathcal{X}$ be a curve of gonality t. Let $P_1, \ldots, P_n, P_\infty$ be $n + 1$ distinct rational points on $\mathcal{X}$. Let $D = P_1 + \ldots + P_n$. Let G be a divisor of degree m. Let $e = \lfloor (d_G - 2 - g + t)/2 \rfloor$. If there is an effective divisor of degree $e - t - 1$ and disjoint support with D and P_∞, then there exists a divisor F such that one can decode e errors of the code $C_\Omega(D, G)$ with F.*

Proof Let A be an effective divisor of degree $t - e - 1$ and disjoint support with D and P_∞. Such a divisor exsits by assumption. Let K be a canonical divisor such that the support of K is disjoint from D, and P_∞ is not in the negative part of K. Such a divisor exists, by the independence of valuations. Let $F_0 = G - K + A$, and let $F = F_0 - P_\infty$. Then F_0 has degree $m - 2g + 1 + t - e$, which is at least $g + e + 1$, by the choice of e. Hence the dimension of $L(F_0)$ is at least $e + 2$, by the Riemann-Roch Theorem. Thus one can decode e errors of $C_\Omega(D, G)$ with F, by Lemma 5.2. $\Box$

Remark 5.3 If the number of rational points is at least $n + 2$, then the existence of the divisor A is assured. One can take $A = (t - e - 1)Q_\infty$, where Q_∞ is a rational point different from P_∞ and not contained in D. Now $0 \leq t - e - 1$, since $m \leq 3g - 2 + t$. Hence A is effective.

Example 5.4 The code $C_\Omega(D, mP_\infty)$ on the Hermitian curve over $\mathbf{F}_q$, where $q = r^2$, has Goppa designed minimum distance $m - r^2 + r + 2$. It follows from work of Tiersma [20], in case q is even, and Stichtenoth [19] for arbitrary q, that $C_\Omega(D, mP_\infty)$ is the dual of C_m which is equal to $C_{r^3+r^2-r-2-m}$. Suppose $m \leq r(3r - 1)/2 - 2$. Let $e = \lfloor (m - r(3r - 5)/2)/2 \rfloor$. Suppose $r - e - 1 > 2$. It follows from the zeta function of the Hermitian curve that there exist places of any degree not equal to 2. Let A be a place of degree $r - e - 1$. Let $K = (r^2 - r - 2)P_\infty$. Then K is a canonical divisor. If we take $F = (m - r^2 + r + 1)P_\infty + A$, then we can decode e errors of the code $C_\Omega(D, mP_\infty)$ with F, by Proposition 5.3.

Example 5.5 If not only the minimum distance of $C_\Omega(D, G - F)$ is greater than one expects, but also the dimension of $L(F)$ is greater than $\deg(F) + 1 - g$, then sometimes one can decode even more errors. Let F_0 be the divisor $i(r + 1)P_\infty$, for $0 < i < r - 1$, on the Hermitian curve of degree $r + 1$. Then $L(F_0)$ has dimension $\binom{i+2}{2}$. Let $e = (i^2 + 3i - 2)/2$. Suppose $r - e - 1 > 2$. Let A be a place of degree $r - e - 1$. Let $K = (r^2 - r - 2)P_\infty$. Then K is a canonical divisor. Let $G = F_0 + K - A$ and $F = F_0 - P_\infty$. Then the code $C_\Omega(D, G)$ has Goppa designed minimum distance $i(i + 2r + 5)/2 - r$ and one can decode $e = (i^2 + 3i - 2)/2$ errors of this code with $(ir + i - 1)P_\infty$, by Lemma 5.2. In particular, if $i = 1$, then the designed minimum distance is 3 and one can decode 1 error with rP_∞.

Remark 5.6 The function $\alpha_q^{pol\ dec,lin}(\delta)$ of asymptotic good linear codes with a polynomial construction and polynomial contructable decoding algorithm, is bounded below by the Skorobogatov-Vlăduţ-bound $R_{SV}(\delta) = 1 - 2\gamma_q - \delta$, see [21, Theorem 3.4.34]. We have the following improvement.

Proposition 5.7

$$\alpha_q^{pol\ dec,lin}(\delta) \geq 1 - 2\gamma_q + (q+1)^{-1} - \delta$$

Proof This follows immediately from Proposition 5.2 and Remark 5.3, whenever $\delta \leq 2\lambda_q$. For arbitrary δ it is proved by Ehrhard [4], see also Remark 5.1.
□

References

[1] C. Chevalley, Introduction to the theory of algebraic functions in one variable, Math. Surveys VI, Providence, AMS 1951.

[2] M. Coppens, The gonality of general smooth curves with a prescribed plane nodal model, Math. Ann. **289** (1991), 89-95.

[3] I. Duursma, Algebraic decoding using special divisors, preprint april 1991.

[4] D. Ehrhard, Über das Dekodieren algebraisch-geometrischer Codes, Thesis, Düsseldorf University, 1991.

[5] V.D. Goppa, Algebraico-geometric codes, Izv. Akad. Nauk SSSR **46** (1982), = Math. USSR Izvestija **21** (1983), 75-91.

[6] M. Homma, Funny plane curves in char $p > 0$, Comm. in Algebra, **15** (1987), 1469-1501.

[7] J. Justesen, K.J. Larsen, H.E. Jensen, A. Havemose and T. Høholdt, Construction and decoding of a class of algebraic geometric codes, IEEE Trans. Inform. Theory IT-**35** (1989), 811-821.

[8] G. Lachaud and M. Martin-Deschamps, Nombre de points des jacobiens sur un corps fini, Acta Arithmetica **16** (1990), 329-340.

[9] J. Lewittes, Places of degree one in function fields over finite fields, J. Pure Appl. Algebra, **69** (1990), 177-183.

[10] J.H. van Lint, Introduction to coding theory, Grad. Texts Math.**86**, Springer-Verlag, Berlin, 1982.

[11] C.J. Moreno, Algebraic curves over finite fields, Cambridge Texts in Math. **97**, Cambridge University Press, Cambridge, 1991.

[12] M. Namba, Families of meromorphic functions on compact Riemann surfaces, Lect. Notes Math. **767**, Springer-Verlag, Berlin, 1979.

[13] R. Pellikaan, On a decoding algorithm for codes on maximal curves, IEEE Trans. Inform. Theory IT-**35** (1989), 1228-1232.

[14] R. Pellikaan, B.Z. Shen and G.J.M. van Wee, Which linear codes are algebraic geometric ?, IEEE Trans. INform. Theory IT-**37** (1991), 583-602.

[15] M. Yu. Rosenbloom and M.A. Tsfasman, Multiplicative lattices in global fields, Invent. Math. **101** (1990), 687-696.

[16] A.N. Skorobogatov and S.G. Vlăduţ, On the decoding of algebraic-geometric codes, IEEE Trans. Inform. Theory IT-**36** (1990), 1051-1060.

[17] A.B. Sørensen, Weighted Reed-Muller codes, preprint june 1991.

[18] H. Stichtenoth, Selbst-dual Goppa codes, J. Pure Appl. Algebra **55** (1988), 199-211.

[19] H. Stichtenoth, A note on Hermitian codes over GF(q^2), IEEE Trans. Inform. Theory IT-**34** (1988), 1345-1348.

[20] H.J. Tiersma, Codes comming from Hermitian curves, IEEE Trans. Inform. Theory IT-**33** (1987), 605-609.

[21] M.A. Tsfasman, S.G. Vlăduţ, Algebraic-geometric codes, Mathematics and its Applications **58**, Kluwer Academic Publishers, Dordrecht, 1991.

[22] S.G. Vlăduţ, On the decoding of algebraic-geometric codes over GF(q) for $q \geq 16$, IEEE Trans. Inform. Theory **36** (1990), 1461-1463.

[23] Xing C.-P., A note on the minimum distance of Hermitian codes, preprint, Un. Science and Techn. of China, Hefei, Anhui, june 1991.

[24] K. Yang and P.V. Kumar, On the true minimum distance of Hermitian codes, preprint, june 1991.