Rational points on hypersurfaces, Reed-Muller codes and algebraic geometric codes

Anders Bjært Sørensen

Ph.D. Thesis

-

November 1991

Preface

This thesis is about applications of algebraic and projective geometry over finite fields in error-correcting coding theory and computer algebra.

The thesis consists of six sections, a summary in english and a summary in danish. The first section is an introduction to the other five sections. These five sections are written on the basis of five individual papers all appeared as preprints during the period 1.7.89-1.11.91. Furthermore, we have a summary in english at the beginning and a summary in danish at the end of the thesis.

A number of persons have had influence on this thesis and I would like thank them here.

First of all, I would like to express my deep gratitude to my supervisor throughout many years, Ph. D., Lektor Johan P. Hansen, whose professional support and unfailing optimism made this thesis possible.

To the group in coding theory at the Mathematical Institute, The Technical University of Denmark, especially Docent Tom Høholdt and Docent Helge Elbrønd Jensen, I owe warm thanks for many hours of pleasant and fruitful discussion about codes and geometry and for the hospitality I always have met.

Thanks to Carsten Dahl Jensen, Jens Peter Pedersen and Lene Søndergaard for your everlasting (seems to me) patience at our common wintercourse.

A special thank goes to my co-author Jens Peter Pedersen for stimulating discussions and impressive fighting-spirit during our common work.

Let me also say thank you to the faculty at Mathematical Institute, University of Aarhus, at Institute for Problems on Information Processing, Moscow and at Research Institute for Symbolic Computation, Linz for their hospitality. And to the Danish Natural Science Research Council, The Danish Research Academy and "The Cultural Agreement DK-USSR" for financial support.

Thanks to my family and to Andrea.

Aarhus, November 1991

Anders Bjært Sørensen

"Let us suppose these things are like the truth"
XENOPHANES

Contents

Summary 4

1. Introduction 7

1.1 On Reed-Muller codes and algebraic geometric codes 7

1.2 Algorithms deciding rationality and absolutely irreducibility 15

1.3 References 17

2. On the number of rational points on codimension-1 algebraic sets in $\mathbf{P}^n(\mathbf{F}_q)$, 13 pp.

3. Projective Reed-Muller codes, 33 pp.

4. Codes from certain algebraic function fields with many rational points, 10 pp.

5. Weighted Reed-Muller codes, 13 pp.

6. A note on algorithms deciding rationality and absolutely irreducibility based on the number of rational solutions, 13 pp.

Sammenfatning på dansk

Summary

This thesis presents the result of the authors research in the period 1.7.89 till 1.11.91 and form the dissertation delivered to the Faculty of Natural Science at University of Aarhus in order to obtain "licentiatgrad i matematik" equivalent to the Ph.D. degree in Mathematics.

This research is sponsered by a grant from The Danish Natural Science Research Council under the title "Algebraisk geometri over endelige legemer". The Danish Research Academy has supported visits in Moscow and Linz during the period and the "Cultural Agreement DK-USSR" has supported the visit in Moscow.

Our thesis is build on 5 papers written in the period 1.7.89 until 1.11.91. The papers are

[Sø89a] A. B. Sørensen, *A "Full degeneration"-lemma for hypersurfaces in $P(q,n)$*, Preprint Series no. 5, 1989, Matematisk Institut, Aarhus Universitet. Revised version submitted to Discrete Mathematics.

[Sø89b] A. B. Sørensen, *Projective Reed-Muller codes*, Preprint Series no. 11, 1989, Matematisk Institut, Aarhus Universitet. Revised version to appear in IEEE Trans. on Inf. Theory, nov. 91.

[PS90] J. P. Pedersen, A. B. Sørensen,*Codes From Certain Algebraic Function Fields With Many Rational Places*, MAT-REPORT NO. 1990-11, Matematisk Institut, Danmarks Tekniske Højskole, June 1990.

[Sø91a] A. B. Sørensen, *Weighted Reed-Muller Codes*, RISC-Linz Series no. 91-36.0, august 1991, submitted to IEEE Trans. on Inf. Theory.

[Sø91b] A. B. Sørensen, *A Note on Algorithms Deciding Rationality and Absolutely Irreducibility Based on the Number of Rational Solutions*, RISC-Linz Series no. 91-37.0, august 1991.

These papers are the basis of sections 2-6 in the same order. In case of [Sø89a] (section 2) and [Sø89b] (section 3) revised versions are printed. In section 4 the paper [PS90] is reprinted, and in section 5 and 6 papers [Sø91a] and [Sø91b] are reprinted with minor corrections.

In **section 1** we present relevant background theory and put the results obtaind in sections 2-6 in a more general frame. We emphasize on recent results and thereby give an up-to-date presentation of the field. A new example and conjecture not published in the above papers is given.

Apart from section 1 our thesis falls naturally into two parts. The first major part (sections 2-5) is concerned with applications of algebraic and projective geometry over

finite fields in the theory of error-correcting codes. The second part (section 6) is concerned with algorithms in computer algebra and constructive algebraic geometry.

In **section 2,** we give a proof of the socalled "Full degeneration-lemma". Given a codimension-1 algebraic set in $\mathbf{P}^n$ defined over a finite field $\mathbf{F}_q, q$ a prime power, of low degree $d, d \leq q$. It states, that the algebraic set with the maximum number of rational points is d distinct hyperplanes through a common $\mathbf{P}^{n-2}$. Furthermore, we compare the found upper bound with the bound coming from the Weil-conjectures and find that the upper limit on the degree of non-singular plane curves, for which the Weil-bound cannot be achieved coincide with the known result of Serre ([Se83]) using properties on the Weil-conjectures. Our approach is basically combinatorically. An extended version of this section is submitted to Discrete Mathematics for publication.

In **section 3,** the results from section 2 are generalized to any degree. The proof is now based on results from coding theory on Reed-Muller codes. The projective Reed-Muller codes are introduced and their exact code-parameters are found (here the "Full degeneration-lemma" corresponds to the estimate of the minimum distance). It is furthermore shown, that a subclass of the projective Reed-Muller codes are cyclic and their roots are characterized. These generalized results are used to answer the question raised in the book of Tsfasman and Vlăduţ (Algebraic-geometric codes, Mathematics and its Applications **58**, Kluwer Ac. Publ. Dordrecht, The Netherlands, 1991, Problem 1.2.9) in the affirmative.
Section 3 will appear as a full paper in IEEE Trans. on Inf. Theory, Nov. 1991.

In **section 5,** the notion of Reed-Muller codes are generalized and the weighted Reed-Muller codes are introduced. The properties of weighted Reed-Muller codes are studied - codeparameters are estimated, the duals characterized and their connection to algebraic geometric codes discussed. The latter was the motivation to introduce these codes. This paper is submitted to IEEE, Trans. on Inf. Theory for publication.

In **section 4,** (written together with J. P. Pedersen) we investigate the Hansen-Stichtenoth codes in any characteristic (in [HS90] only char 2 was considered). We find the number of rational points, the genus of the corresponding curve and determine the basis of rational functions with prescribed poles at infinity. All results from [HS90] generalize except the maximality property of the corresponding curves with respect to the explicit formulas of Weil.

In **section 6,** the Weil-conjectures for algebraic curves over finite fields are used to built an algorithm that detects rationality of algebraic curves defined over finite fields. Modifications suitable for a practical implementation are discussed. Interesting applications of the number of rational points on hypersurfaces in probabilistic absolute irreducibility tests for multivariable polynomials over $\mathbf{Q}$ are conjectured.

Conclusion. The number of rational points on algebraic curves (varieties) are of interest in many research areas in modern mathematics - both theoretically and in applications. Their importance in the application af algebraic curves over finite fields to coding theory are well-established. Good codes come from curves with many rational points relative to the genus. The results on projective Reed-Muller codes (their minimum distance) have their geometric parallel in the "Full degeneration-lemma". It seems to us, that the number of rational points also contains information of interest in constructively algebraic geometry.

Rational points (and their cardinality) in this way become the link between the two parts of the thesis, and it is the authors believe that more interesting applications of the number of rational points in both areas are to be discovered.

1 Introduction

In this section we present briefly relevant background theory and other related papers in order to give a more complete up-to-date presentation. We try not to repeat the different papers introductions but emphasize on the latest development in the field.

1.1 On Reed-Muller codes and algebraic geometric codes

In 1977, V. D. Goppa [Go77] introduced the application of algebraic curves over finite fields in error-correcting coding theory and after his papers [Go81,Go82, Go84] the ideas have had a big influence on error-correcting coding theory. During the last 10 years a lot of interesting problems have been posed, research papers have been written and many of the problems have been solved. Now, also at least 4 textbooks or lecturenotes on the subject are available [GL88,Go89,TV91,Mo91] and we refer to these for an overview of the field. Here we will just briefly introduce the construction of geometric Goppa codes or algebraic geometric codes.

Let X be a projective, smooth, absolutely irreducible curve of genus g defined over $\mathbf{F}_q$, the finite field with q elements. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be n distinct $\mathbf{F}_q$-rational points and let G be a $\mathbf{F}_q$-rational divisor on X such that $supp(G) \cap \mathcal{P} = \emptyset$. Consider $L(G) = \{f \in \mathbf{F}_q(X) \mid div(f) + G \geq 0\}$, where $\mathbf{F}_q(X)$ is the field of rational functions on X. The map

$$\phi_L : L(G) \rightarrow \mathbf{F}_q^n$$

defined by $\phi_L(f) = (f(P_1), \ldots, f(P_n))$ give rise to a subspace $Im(\phi_L)$ in $\mathbf{F}_q^n$, which we will call the algebraic geometric code $C_L(X, \mathbf{F}_q, \mathcal{P}, G)$ or $C_L(\mathcal{P}, G)$.

The theorem of Riemann-Roch now implies the following

Theorem 1.1 *$C_L(\mathcal{P}, G)$ is a linear $[n, k, d]$-code over $\mathbf{F}_q$, where*

$$k \geq deg(G) + 1 - g - dim(L(G - \sum_{i=1}^{n} P_i)) \text{ and } d \geq n - deg(G). \quad (1)$$

If furthermore $2g - 2 < deg(G) < n$, then $k = deg(g) + 1 - g$.

There exists a dual construction using differential forms, which we will not treat here. For that and other details on the basic construction, see [TV91].

Codes from algebraic varieties of higher dimension. Our first research topic was the problem of generalizing the Goppa construction to higher dimensional varieties. From an abstract algebraic geometric point of view there is no problem - the above construction translates almost word by word to any dimension. From an error-correcting coding theory point of view this translation is not satisfactory, since the codeparameters cannot be determined using the Riemann-Roch theorem with the same nice estimate as above. First of all, the minimum distance is not estimated well. On higher dimensional varieties a

In connection with the hard problem of finding good generalizations one is naturally led to the following considerations. Consider the d-uple embedding of some variety X in $\mathbf{P}^m(\mathbf{F}_q)$, the m-dimensional projective space over $\mathbf{F}_q$ into $\mathbf{P}^M(\mathbf{F}_q), M = \begin{pmatrix} m+d \\ d \end{pmatrix} - 1$ sending

$$X \ni P \overset{\phi}{\mapsto} (s_0(P), \ldots, s_M(P))$$

where s_i runs through all homogeneous forms of degree d in $m+1$ variables.

We can associate a linear code to the d-uple embedding taking as columns in the generatormatrix the projective coordinates of $\phi(P), P \in X$. This code has length $n = |X_{\mathbf{F}_q}|$ (the number of $\mathbf{F}_q$-rational points on X) and dimension $k \leq M+1$. For an estimate on the minimum distance and dimension a more careful analysis is necessary.

Example. In [Cha86], Chakravarti studied the 2-uple embedding of the cubic surface $\chi : \sum_{i=0}^{3} x_i^3 = 0$ in $\mathbf{P}^3(\mathbf{F}_4)$ into $\mathbf{P}^9(\mathbf{F}_4)$. The minimum distance and weightdistribution are computed by complete computersearch, and a [45, 10, 22]-code over $\mathbf{F}_4$ is found. Now actually computersearch is not necessary in order to find the minimum distance in this example, as we will see now.

It is well-known ([Hi87]) that, in $\mathbf{P}^3$ over $\mathbf{F}_q$, elliptic quadrics have $1+q^2$ rational points, hyperbolic quadrics have $(1+q)^2$ rational points, cones have $1+q+q^2$ rational points, two distinct planes have $1+q+2q^2$ rational points, two repeated planes have $1+q+q^2$ rational points and two conjugated planes have $1+q$ rational points.

It is straightforward to calculate that the intersection of the given cubic χ over $\mathbf{F}_4$ with the elliptic quartic $x_0^2 + x_1^2 + x_0x_1 + x_2x_3 = 0$ has 17 rational points in common, with the hyperbolic quartic $x_0x_1 + x_2x_3 = 0$, 21 rational points in common, with the cone $x_0^2 + x_1x_2 = 0$, 15 rational points in common, with the two tritangentplanes $(x_0+x_1)(x_0+x_2) = 0$, 23 rational points in common. In fact, these numbers are the maximal with respect to the type mentioned. This is clear in the elliptic case and the degenerate case (two planes). The cone and the hyperbolic need an argument.

A cone in $\mathbf{P}^3(\mathbf{F}_4)$ consists of 5 lines through a common point and through some plane conic. At most 2 lines can be at the cubic, since 3 lines on the cubic through a common point are in the same plane. If 2 lines are in common, at most $2 \times 5 + 3 \times 2 - 1 = 15$ points are in common. If 1 line is in common, at most 12 points and if no lines are in common, at most $5 \times 3 = 15$ points are in common.

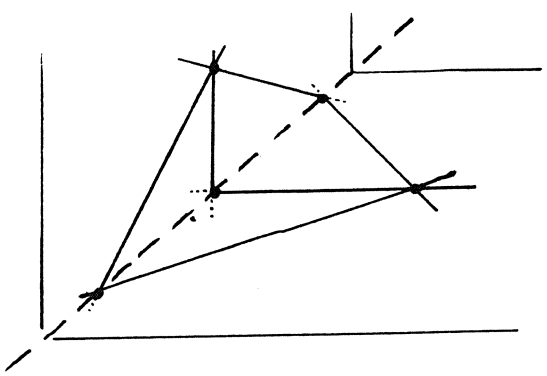
The 25 points on the hyperbolic are on 2×5 skew lines. The incidensstructure of the 27 lines on the cubic are uniquely constructed from arbitrary six skew lines $E_1, \ldots, E_6$. They define uniquely lines $F_{i,j}, i \neq j$ and $G_j, i, j = 1, \ldots, 6$ from the property that $F_{i,j}$ meets E_i and E_j but not $E_k, k \neq i, j$, and G_j meets all E_i, except E_j. Furthermore, $F_{i,j}$ meets $F_{k,l}$ if and only if all i, j, k, l are distinct. $F_{i,j}$ meets G_k if and only if $i = k$ or $j = k$, The lines G_i and $E_i, i = 1, \ldots, 6$ have symmetric properties (see [Har77]).

Assume that 5 skew lines from the hyperbolic were on the cubic. Assume, furthermore, that we can find another line on the cubic, so we alltogether have 6 skew lines. We can without loss of generality assume that they are $E_1, \ldots, E_6$, sincethere exists a permutation of the 27 lines preserving the incidensstructure mapping any six skew lines into given six

skew lines ([Har77]). It is easy from the incidensrelations to see that we cannot find 5 skew lines each of them meeting $E_1, \ldots, E_5$.

If we cannot find the six'th skew line, we can assume without loss of generality that the five skew lines are $E_1, \ldots, E_4, F_{5,6}$. Again it is easy to check that no 5 skew lines meet our given five skew lines. From this we conclude that the cubic cannot contain the 2×5 skew lines from the hyperbolic. If we have four skew lines from hyperbolic on the cubic, we automatically have 2×5 skew lines on the cubic. Therefore, it can at most contain 2×3 skew lines, that is 21 points.

We have now found that the minimumweight codewords correspond to the intersection of the cubic surface and two tritangentplanes like shown in the figure below. There are exactly $3 \times (\frac{1}{2} \times 45 \times 32) = 2160$ such configurations in agreement with [Cha86].



The author has tried to generalize this construction to d-uple embeddings of the Hermitian surface $\sum_{i=0}^{3} x_i^{s+1} = 0$ over $\mathbf{F}_{s^2}$, and conjecture that for $d \leq s$, we get $[(s^2+1)(s^3+1), \frac{(d+3)(d+2)(d+1)}{6}, d(s^3+s^2-s)+s+1]$-codes over $\mathbf{F}_{s^2}$. The minimumweight codewords correspond now to d tangenthyperplanes each intersecting the Hermitian surface in $s+1$ lines such that the d hyperplanes have one line in common and this line intersects the Hermitian surface in $s+1$ points. Unfortunately no proof is found yet and, in general, it seems that the combinatorical complexity of finding the minimum distance increases drastically with the degree d, when we use this strategy of code-construction. Recently, Aubry in [Au91] has studied 1 and 2-uple embeddings of quadrics.

One could go one step further and combine the d-uple embedding of a variety with some linear projection. In this way we get the general embedding of varieties using linear systems. When the linear system is complete we are back to the original Goppa-construction described briefly above.

The simplest example of the d-uple embedding we get by taking $X = \mathbf{P}^m(\mathbf{F}_q)$. The code we get in that situation have similarities with some well-known code constructions in coding theory - the Reed-Muller codes.

Projective Reed-Muller codes. Originally the Reed-Muller codes were constructed as a kind of matrixpuzzle with zeroes and ones (see [DGW70]): Take any binary representation of $0, 1, 2, \ldots, 2^m - 1$ and let them form the columns in a $m \times 2^m$ matrix. Add a row consisting of ones. the now constructed $(m+1) \times 2^m$ matrix M is the generator

matrix of the 1st order binary Reed-Muller code. The second-order binary Reed-Muller code is obtained as the subspace of $\mathbf{F}_2^{2^m}$ generated by vectors on the form $v_1 * v_2$, where v_1, v_2 are rows of M and $*$ are coordinatewise multiplication. In general the ν-th order binary Reed-Muller code is the subspace generated by products $v_1 * v_2 * \cdots * v_\nu$, where the v_i's are rows of M and $*$ are coordinatewise multiplication.

Nowadays other more informative constructions exist in any characteristic, see [DGW70, LM87]. The construction which are of interest here is the polynomial construction discovered by Kasami, Lin and Peterson [KLP68]. In our notation consider

$$V(\nu) = \{F \in \mathbf{F}_q[X_1, \ldots, X_m] \mid deg(F) \leq \nu\}.$$

Consider the $\mathbf{F}_q$-linear map

$$V(\nu) \xrightarrow{\psi} (\mathbf{F}_q)^{q^m}$$

given by $\psi(F) = (F(P_1), \ldots, F(P_{q^m}))$, where P_i runs through all $\mathbf{F}_q$-rational points in the affine m-dimensional space over $\mathbf{F}_q$, $\mathbf{A}^m(\mathbf{F}_q)$. The generalized Reed-Muller code of length q^n and order ν is now the image of $V(\nu)$ under ψ.

It is now clear that the d-uple embedding of $\mathbf{P}^m(\mathbf{F}_q)$ gives a projective analogy of the generalized Reed-Muller code. Define

$$W(\nu) = \{F \in \mathbf{F}_q[X_0, \ldots, X_m] \mid F \text{ homogeneous, } deg(F) = \nu\} \cup \{0\}.$$

and consider the $\mathbf{F}_q$-linear map

$$\phi : W(\nu) \to \mathbf{F}_q^n$$

given by $\phi(F) = (F(P_1), \ldots, F(P_n)), n = (q^{m+1} - 1)/(q - 1)$, where P_i runs through a set of representatives for all points in $\mathbf{P}^m(\mathbf{F}_q)$.

In [Sø89b] (section 3) we find the exact parameters of the projective Reed-Muller codes of any order and over any finite field. We also show that the dual of projective Reed-Muller codes are again projective Reed-Muller codes (almost) and we show that some (but not all) projective Reed-Muller codes are cyclic. For the cyclic codes, we characterize their roots. In this way we answer the question of a generalization of Reed-Muller codes as it is stated in the book of Tsfasman and Vladut [TV91, Problem 1.2.9].

Lachaud is apparently the first to introduce the notation of projective Reed-Muller codes in [La88] and thereby generalize the above multivariable construction to homogeneous polynomials and projective space. Also Manin [VM85] mentions the natural analogy. Lachaud are in [La88] only able to estimate the codeparameters for 1st and 2nd order projective Reed-Muller codes. Independently with the author, Serre solved the problem of the minimum distance for orders less than the size of the field (see [La90]).

The number of rational points and zetafunctions. It is interesting to formulate the estimate of the minimum distance of projective Reed-Muller codes in projective geometry terms. For $\nu \leq q$, the estimate says that the maximal number of $\mathbf{F}_q$-rational points on pure codimension-1 algebraic sets defined over $\mathbf{F}_q$ of degree ν is obtained, when the algebraic set splits into distinct hyperplanes and the intersection of these hyperplanes are

a codimension-2 $\mathbf{F}_q$-linear subspace. If we by $|X_{\mathbf{F}_q}|$ denote the number of $\mathbf{F}_q$-rational points on a pure codimension 1 algebraic set in $\mathbf{P}^n$, we have

$$|X_{\mathbf{F}_q}| \leq \nu q^{n-1} + \frac{q^{n-1}-1}{q-1}. \tag{2}$$

If $\nu > q$, (2) is trivially correct, but it can be strengthened to

$$|X_{\mathbf{F}_q}| = \frac{q^{n+1}-1}{q-1} \text{ or } |X_{\mathbf{F}_q}| \leq \frac{q^{n+1}-1}{q-1} - (q-s)q^{n-r-1}, \tag{3}$$

where $\nu - 1 = r(q-1) + s, 0 \leq s < q-1$.

For $\nu > q$ the geometric picture becomes more complicated. Either we completely cover the whole space (for instance by $q+1$ hyperplanes), or we leave some $(q-s)\mathbf{F}_q-$linear subspaces of dimension $n-r-1$ intersecting in a $\mathbf{F}_q-$linear subspace of dimension $n-r-2$ (for $r < n-1$) uncovered (means outside the algebraic set). The configuration with the maximal number of points have a full-degenerated nature being a set of hyperplanes.

The minimum distance of projective Reed-Muller codes, as we have seen, gives an upper bound on the number of rational points on hypersurfaces of a certain degree. Let us here recapitulate some of the known results coming from zetafunctions corresponding to curves and hypersurfaces.

Let $X \subset \mathbf{P}^n(\mathbf{F}_q)$ be an absolutely irreducible hypersurface (smooth algebraic variety of pure dimension $n-1$) given by some homogeneous polynomial of degree d defined over $\mathbf{F}_q$. Let N_i denote the number of $\mathbf{F}_{q^i}$-rational points on X. The zetafunction $\zeta(X, \mathbf{F}_q)(t)$ is defined by

$$\zeta(t) = \zeta(X, \mathbf{F}_q)(t) = exp(\sum_{i=1}^{\infty} N_i \frac{t^i}{i}). \tag{4}$$

The zetafunction give rise to an upper bound on the number of $\mathbf{F}_q$-rational points on hypersurfaces (a generalized Weil-bound)

$$N_i \leq \sum_{j=0}^{n-1} (q^i)^j + \frac{d-1}{d}((d-1)^n - (-1)^n)(q^i)^{\frac{n-1}{2}}. \tag{5}$$

In [Sø89a] (section 2) we compare this bound with the bound from the projective Reed-Muller code. We then obtain, for q a square, the upper bound

$$d \leq \sqrt{q} + 1 \tag{6}$$

on the degree of the hypersurface for which it is possible to have the maximal number of $\mathbf{F}_q$-rational with respect to the bound (5). We notice that the Hermitian hypersurface shows that this bound is the best possible.

For smooth algebraic curves the Hasse-Weil bound on the number N_i of $\mathbf{F}_q$-rational points reads

$$N_i \leq 1 + q^i + 2g\sqrt{q^i}. \tag{7}$$

Serre in [Se83] noticed the bound

$$g > \frac{q - \sqrt{q}}{2} \tag{8}$$

for which the upper bound (7) is impossible to obtain. We notice that the bound for plane smooth curves coincide with (8)

Weils explicit formulas. We have just seen from (8) that the Hasse-Weil-bound is not always effective. Fortunately, the theory of zetafunctions for smooth curves gives much more than just the bound (7). Following [Se83] a closer look at the zetafunctions reveals the following properties

$$\zeta(t) = \frac{P(t)}{(1-t)(1-qt)} \tag{9}$$

with

$$P(t) = \prod_{i=1}^{2g}(1 - \alpha_i t), \alpha_i \in \mathbf{C}, |\alpha_i| = \sqrt{q}. \tag{10}$$

Let $arg(\alpha_i) = \theta_i$ and define testfunctions

$$f(\theta) = 1 + 2\sum_{n\geq 1} c_n cos(n\theta), c_n \in \mathbf{R}, \tag{11}$$

and powerseries

$$\psi_d(t) = \sum_{n\geq 1} c_{nd} t^{nd}. \tag{12}$$

Now, it is known that

$$\sum_{d\geq 1, d|i} d a_d = N_i, \tag{13}$$

where a_d is the number of effective primedivisors of degree d.

Using (9)-(13), we obtain Weil's explicit formulas

$$\sum_{i=1}^{g} f(\theta_i) + \sum_{d\geq 1} d a_d \psi_d(\frac{1}{\sqrt{q}}) = g + \psi_1(\frac{1}{\sqrt{q}}) + \psi_1(\sqrt{q}). \tag{14}$$

Now clever choises of testfunctions can give new bounds on N_1: If we assume $f(\theta) \geq 0, \forall\theta \in \mathbf{R}$ and $c_n \geq 0, n \geq 1$ and if we only take the first term in the infinite summation in (14), we get the inequality

$$N_1 \leq \frac{1}{\psi_1(\frac{1}{\sqrt{q}})} g + 1 + \frac{\psi_1(\sqrt{q})}{\psi_1(\frac{1}{\sqrt{q}})}, \tag{15}$$

and we have equality if and only if

$$\sum_{i=1}^{g} f(\theta_i) = 0 \text{ and } \sum_{d\geq 2} d a_d \psi_d(t) = 0.$$

For $f(\theta) = 1 + cos(\theta)$, we get the Hasse-Weil-bound

$$N_1 \leq 1 + q + 2g\sqrt{q}$$

with equality if and only if

$$\theta_i = -\pi.$$

Example. The Hermitian curve $\sum_{i=0}^{2} x_i^{\sqrt{q}+1} = 0$ over $\mathbf{F}_q$, q a square, provides an example where the Hasse-Weil-bound is obtained. It has $1+q\sqrt{q}$ $\mathbf{F}_q$-rational points, genus $\frac{1}{2}(q-\sqrt{q})$ and zetafunction

$$\zeta(t) = \frac{(1-2\sqrt{q}t+qt^2)^g}{(1-t)(1-qt)}.$$

.

Let $f(\theta) = (\frac{1}{\sqrt{2}} + cos(\theta))^2 = 1 + 2(\frac{\sqrt{2}}{2}cos(\theta) + \frac{1}{4}cos(2\theta))$. Then we get from (14) the bound

$$N_1 \leq \frac{4q}{2\sqrt{2}\sqrt{q}+1}g + 1 + \frac{2\sqrt{2}\sqrt{q}+q}{2\sqrt{2}\sqrt{q}+1}q \tag{16}$$

with equality if and only if

$$\theta_i \in \{-\frac{3}{4}\pi, \frac{3}{4}\pi\} \text{ and } N_2 = N_1.$$

Example. In [PS90] (section 4) J. P. Pedersen and the author studies the curve

$$y^q - y = x^{q_0}(x^q + x) = 0,$$

where q is a power of a prime and $q_0^2 \mid q$. We show that it has $1 + q^2$ $\mathbf{F}_q$-rational points, genus $g = (q(q-1))/(2q_0)$, and find the basis of $L(mP_\infty)$, where P_∞ is the unique singular point on the curve. We give estimates on the parameters of the corresponding code.

This curve generalizes a curve found by Hansen and Stichtenoth [HS90], where only the case $q = 2^{2n+1}, q_0 = 2^n$ were considered. In this case the curve will meet the bound (16) and have zetafunction

$$\zeta(t) = \frac{(1+\sqrt{2}\sqrt{q}t+qt^2)^g}{(1-t)(1-qt)}.$$

Recently, J. P. Pedersen [Pe91] has found a plane curve, which for $q = 3^{2n+1}, n \in \mathbf{N}$ has the maximal number of points corresponding to another bound derived from (12) taking as testfunction $f(\theta) = \frac{1}{3}(1 + \sqrt{3}cos(\theta) + cos(2\theta))^2$.

The above mentioned examples of curves with the maximal number of points have a more abstract description as Deligne-Lusztig varieties with interesting automorphism-groups. We refer to [Ha91] for a more detailed explanation of this connection.

It would be interesting to find more examples of curves which has the maximal number of points with respect to Weils explict formulas.

Weighted Reed-Muller codes. In the important paper of Pellikaan et al. [PSW91] a space curve $X(l,q)$ is introduced and studied. It is defined by the ideal

$$(x_i^{q+1} - x_i^2 x_0^{q-1} + x_{i+1}x_0^q - x_{i+1}^q x_0, i = 1, \ldots, l-1)$$

and defines an absolutely irreducible, singular curve in $\mathbf{P}^l$ with $1 + q^l$ $\mathbf{F}_q$-rational points. It has only one singular point $P_\infty = (0 : \cdots : 0 : 1)$. The genus of $X(l,q)$ is

$$g = \frac{1}{2}\{\sum_{i=1}^{l-1} q^{l+1-i}(q+1)^{i-1} - (q+1)^{l-1} + 1\} \simeq \frac{l-1}{2}q^l$$

and the Weierstrass gapsequence for the point P_∞ given by the generators of the monoid of non-gaps

$$\{q^{l-i}(q+1)^{i-1}\} \;\; i = 1, \ldots, l.$$

The code $C_L(X(l,q), \mathbf{F}_q, \mathcal{P}, mP_\infty)$ with $\mathcal{P}$ equal to the set of all non-singular rational points, has parameters

$$k \geq m + 1 - g, d \geq q^l - m.$$

Since $g \simeq \frac{l}{2}q^l$, we see that the estimate of the dimension becomes trivial for small m and the estimate of the minimum distance becomes trivial for big m.

The code $C_L(X(l,q), \mathbf{F}_q, \mathcal{P}, mP_\infty)$ has some connection to the Reed-Muller family. This theme is investigated in [Sø91a] (section 5). We generalize the definition of the Reed-Muller codes such that also weighted polynomials are considered. It makes it possible to give a unified description of a class of codes coming from algebraic curves or varieties as complete linear systems with a basis of monomials of coordinatefunctions. We show that the code $C_L(X(l,q), \mathbf{F}_q, \mathcal{P}, mP_\infty)$ turns out to be a weighted affine Reed-Muller code and its exact codeparameters are estimated.

Pellikaan has studied the question how to estimate the parameters of algebraic geometric codes $C_L(X, \mathbf{F}_q, \mathcal{P}, G)$, when $deg(G) > n$, where Theorem 1.1 gives the trivial estimate. In [Pel91] Pellikaan introduces the notion of abundant divisors and abundant codes.

If G is linear equivalent to $\sum_{P_i \in \mathcal{P}} P_i + A$ for some divisor $A \geq 0$, G is said to be abundant of abundance $deg(A)$ and $C_L(X, \mathbf{F}_q, \mathcal{P}, G)$ an abundant code. Pellikaan shows that if $C_L(X, \mathbf{F}_q, \mathcal{P}, G)$ is an abundant $[n,k,d]$-code, then $d \geq t - deg(A)$, where t is the gonality of X (i.e. the smallest degree of a non-constant map from X to $\mathbf{P}^1$ defined over $\mathbf{F}_q$). The gonality of a curve X is bounded by $N/(q+1) \leq t \leq deg(E)$, where $N = |X(\mathbf{F}_q)|$ and E is some effective divisor on X with $dim_{\mathbf{F}_q}(L(E)) > 1$.

Pellikaan shows that the above code $C_L(X(l,q), \mathbf{F}_q, \mathcal{P}, mP_\infty)$ is an abundant code.

1.2 Algorithms deciding rationality and absolutely irreducibility

The last part is concerned with a theme, which has almost nothing to do with coding theory. During the last decade the field of computer algebra has been rapidly growing. The main inspiration, however, to enter this field, came from my knowledge on rational points on curves and hypersurfaces obtained by studying algebraic geometric codes.

A popular definition of computer algebra could be mathematics on computer - even though it is too imprecise. One should add that in computer algebra one is concerned with exact computation and symbolic computation in contrast to numerical computation.

A number of general purpose software products are available. REDUCE, MATHEMATICA, MACSYMA, MAPLE, AXIOM (former SCRATCHPAD) etc. are the most important and well-known. A bigger and steadly increasing number of special purpose software packages are released. They can either be built from ground of or be built on the top of some existing general purpose system. In commutative algebra exists for instance Macauley and CoCoA. Cayley is a package for grouptheory, mainly. Just to mention some of the most well-known special purpose systems.

A keypoint in advanced programming is good algorithms. The interest of the author has been two ideas for algorithms based on the number of rational points on varieties. One is concerned with the rationality of plane curves and the other is concerned with absolutely irreducibility.

Rationality of curves. In different areas of computer aided geometric design the problem of parametrization of curves is natural. Assume in the following that our coefficient-domain is the rational numbers.

It is clear that it is much more efficient to trace a rational curve by its parametrization than by its defining equations. On the other hand, testing whether a given point is on a curve or not is much simpler, when the equations are given than using the parametrization. Other questions related to rational curves have their favorite representation. Efficient algorithms for the transition from the implicit equations to explicit parametrization and back are therefore studied among researches in this field [AB88, SW90, SS91].

The author has been interested in a preprocessing step to the parametrization problem, namely the problem of deciding rationality. It is reasonable to expect that most curves are non-rational - at least it is so in the case of algebraically closed groundfields. Therefore it is important to be able to decide whether a given curve (given by its equations) is rational or not.

Traditionally this is solved by desingularization of all bad singularities [AB88, Ab83], and consequently this gives the genus of the curve and therefore decide rationality or not. It is reasonable to expect that the question of rationality is easier than the determination of genus - one asks for less.

Nevertheless, the author knows of no algorithm that solves the rationality problem without actually calculating the genus. The idea described in [Sø91b] is the following.

Let X be an absolutely irreducible, plane, projective curve, given by $F(X,Y) = 0$, defined over the rational numbers $\mathbf{Q}$. First, choose a prime p such that we have good

reduction, i.e. such that $(F \bmod p) = 0$ defines an absolutely irreducible curve X_p over $\mathbf{F}_p$ of the same genus as X. Next, count the number N_i of degree one places on X_p over $\mathbf{F}_{p^i}$ for suitable many extensions, and deduce rationality or non-rationality.

There are more unclear steps in the above algorithm. First, it is known that all primes but finitely many gives good reduction [De42], but an efficient algorithm that tests primes for "luckyness" remains to be developed. Secondly, the exact counting of places above singular points is a nontriviel task. Probably only a partial algorithm are implementable as discussed in [Sø91b]. These questions we hope to be able to address in the future.

Absolutely irreducibility. Efficient algorithms for factorization and irreducibility tests are standard tools in any computer algebra system, at least in one variable. The multivariable case is much harder and not studied as intensively as the one-varible case. In the multivariate case and in the field of absolute factorization and irreducibility tests a lot of research remains to be done.

However, the question of absolutely irreducibility has been studied by some authors ([No22], [HS81], [Ka85a], [Ka91], [Du91]).

Given a multivariable polynomial over some field. The Noether irreducibility forms are a finite set of polynomials in the indeterminate coefficients of the given multivariable polynomial, with the property that the given multivariable polynomial is absolutely irreducible, if and only if all irreducibility forms vanishes on the coefficients, see [No22] and [Sc76]. Kaltofen studies in [Ka85a] and [Ka91] the Noether irreducibility forms in order to give absolutely irreducibility tests.

In [HS81] the Bertini theorem or General Hyperplane Section Lemma are considered as the basis of a reduction to only bivariate algorithms.

Duval gives in [Du91] a geometric factorization algorithm for bivariate polynomials. It is analogous to the Berlekamp algorithm for polynomials in one variable over a finite field, and provides first a calculation of the number af absolutely irreducible factors (i.e. an abs. irreduciblilitytest) and after that it finds the factors. It is based upon the fact that for absolutely irreducible algebraic curves the space of rational functions on the curve without poles has dimension 1 (the constants).

In [Sø91b] (section 6) we show how knowledge on the number of $\mathbf{F}_p$-rational points can give an outline for an probabilistic absolutely irreducibilitytest of multivariable polynomials defined over $\mathbf{Q}$. The point is that absolutely irreducibility is preserved when we make reduction modulo a prime for allmost all primes, and furthermore we use knowledge on the behaviour of the number of rational points when the size of the field tends to infinity, ([Sc76], [SW54]).

We still need to find a probability-measure to judge on the quality of the algorithm. This question we also hope to be able to address in the future.

1.3 References

[Ab83] S. S. Abhyankar, *Desingularization of Plane Curves*, in Proceedings of Symposion in Pure Mathematics, Vol. **40** (1983), Part 1.

[AB88] S. S. Abhyankar, C. L. Bajaj, *Automatic parametrization of rational curves and surfaces III: Algebraic plane curves*, Computer Aided Geometric Design **5** (1988) 309-321.

[Au91] Y. Aubry, *Reed-Muller Codes associated to Projective Algebraic Varieties*, preprint, C.R.I.M. Luminy, Marseille, (1991).

[BC66] R. C. Bose, I. M. Chakravarti, Hermitian Varieties in a Finite Projective Space PG(N,q^2), Canad. J. Math. **18** (1966) pp. 1161-1182.

[BCL83] B. Buchberger, G. E. Collins, R. Loos (eds.), Computer Algebra - Symbolic and Algebraic Computation, 2nd ed., Springer-Verlag 1983.

[BHVW91] M. Bronstein, M. Hassner, A.Vasquez, C.J. Williamson, *Computer Algebra Algorithms for the Construction of Error Correcting Codes on Algebraic Codes*, preprint, 1991.

[Cha86] I. M. Chakravarti, *The Generalised Goppa Codes and Related Discrete Designs from Hermitian Surfaces in* $PG(3, s^2)$, in Lecture Notes in Computer Science **311**, pp. 116 - 124. (1986).

[Che51] C. Chevalley, Introduction to the theory of algebraic functions in one variable, Math. Surveys VI. AMS 1951.

[Da81] J. H. Davenport, On the integration of algebraic functions, Lecture Notes in Computer Science **102** 1981.

[De42] M. Deuring, *Reduktion algebraischer Funktionskörper nach Primdivisoren des Konstantenkörpers*, Math. Zeit. **47**, pp. 643-654, (1942).

[De73] M. Deuring, Lectures on the theory of algebraic functions of one variable, Lecture Notes in Mathematics **314**, Springer-Verlag, 1973.

[Di15] L. E. Dickson, *The Straight Lines on Modular Cubic Surfaces*, Proc. Nat. Acad. Sci. **1**, 248-253, (1915).

[DGW70] P. Delsarte, J. M. Goethals, F. J. Mac Williams, *On Generalized Reed-Muller Codes and Their Relatives*, Information and Control **16**, 403-442 (1970).

[DST88] J. H. Davenport, Y. Siret, E. Tournier, Computer algebra, Academic Press 1988.

[Du91] D. Duval, *Absolute factorization of polynomials: a geometric approach*, SIAM Jour. on Comput. **20**/1, pp. 1-21, (1991).

[Ei66] M. Eichler, Introduction to the Theory of Algebraic Numbers and Functions, Academic Press, New York, 1966.

[FJ86] M. D. Fried, M. Jarden, Field Arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete 3. Folge Bd 11, Springer-Verlag 1986.

[Fu69] W. Fulton, Algebraic curves, Benjamin 1969.

[GL88] G. van der Geer, J. H. van Lint, Introduction to coding theory and algebraic geometry, DMV Seminar **12**, Birkhäuser Verlag, Basel, 1988.

[Go77] V. D. Goppa, *Codes associated with divisors*, Problems of Information Transmission **13** (1) (1977) pp. 33-39.

[Go81] V. D. Goppa, *Codes on algebraic curves*, Soviet Math. Dokl **24** (1981) pp. 170-172.

[Go83] V. D. Goppa, *Algebraico-geometric codes*, Math. USSR Izvestija **21** (1983) pp. 75-91.

[Go84] V. D. Goppa, *Codes and information*, Russian Math Surveys **39**, (1984) pp. 87-141.

[Go89] V. D. Goppa, Geometry and Codes, Mathematics and its applications, Soviet Series **24**, Kluwer Ac. Publ., Dordrecht, The Netherlands 1989.

[Ha87] J. P. Hansen, *Codes on the Klein Quartic, Ideals and decoding,* IEEE Trans. on Inf. Theory **33** (1987).

[Ha91] J. P. Hansen, *Group Codes on Deligne-Lusztig varieties*, Perprint Series 1991 no. 12, Matematisk Institut, Aarhus Universitet.

[Har77] R. Hartshorne, Algebraic Geometry, GTM **52**, Springer Verlag 1977.

[Hil92] D. Hilbert, *Über die Irreducibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, J. Reine angew. Math. **110**, pp. 104-129 (1892).

[Hir79] J. W. P. Hirschfeld, Projective Geometries over Finite Fields, Clarendon Press, Oxford 1979.

[Hir85] J. W. P. Hirschfeld, Finite Projective Spaces of Three Dimensions, Clarendon Press, Oxford 1985.

[Ho91] C. Hooley, *On the Number of Points on a Complete Intersection over a Finite Field*, Journal of Number Theory **38**, 338-358 (1991).

[HS81] J. Heintz, M. Sieveking, *Absolute Primality of Polynomials is Decidable in Random Polynomial Time in the Number of Variables,* Proc. ICALP '81, Springer Lec. Notes in Comp. Sci. **115**, pp. 16-28, (1981).

[HS90] J. P. Hansen, H. Stichtenoth, *Group codes on certain algebraic curves with many rational points.* Applicable Algebra in Engineering, Communication and Computing 1, 67-77 (1990).

[JLJHH89] J. Justensen, K. J. Larsen, H. E. Jensen, A. Havemose, T. Høholdt, *Construction and decoding of a class of algebraic geometric codes,* IEEE Trans. on Information Theory, IT-**35** (1989), 811-821.

[Ka85a] E. Kaltofen, *Effective Hilbert irreducibility,* Information and Control **66**, pp. 123-137 (1985).

[Ka85b] E. Kaltofen, *Fast parallel absolute irreducibility testing,* J. Symbolic Computation 1 (1985) 37-67.

[Ka91] E. Kaltofen, *Effective Noether Irreducibility Forms and Applications,* preprint 1991. (Proc. 1991 ACM Symp. Theory Comput., ACM Press (may 1991).)

[KLP68] T. Kasami, S. Lin, W. W. Peterson, *New Generalizations of the Reed-Muller Codes Part I: Primitive Codes,* IEEE Trans. on Information Theory, IT-**14**, no. 2, (1968).

[Ko84] N. Koblitz, p-adic Numbers, p-adic Analysis and Zeta-Functions, GTM **58**, Springer-Verlag 1984.

[La86] G. Lachaud, *Les codes géométrique de Goppa*, Sem. Bourbaki no. 641, in Asterisque **133-134**, 189-207 (1986).

[La88] G. Lachaud, *Projective Reed-Muller codes*, in Lecture Notes in Computer Science **311**, Springer Verlag 1988.

[La90] G. Lachaud, *The parameters of Projective Reed-Muler codes,* Discrete Mathematics **81** (1990), pp. 217-221.

[Li82] J. H. van Lint, Introduction to Coding Theory, GTM **86**, Springer-Verlag 1982.

[LM87] P. Landrock, O. Manz, *Classical Codes as Ideals in Group Algebras,* Preprint Series 1986/87 No. 18, Matematisk Institut, Aarhus Universitet.

[LN83] R. Liedl, H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and Its Applications (ed. G.-C. Rota), Vol 20, Addison-Wesley 1983.

[LW54] S. Lang, A. Weil, *Number of points on varieties in finite fields*, Amer. J. Math. **76** (1954), pp. 819-827.

[Mo91] C. J. Moreno, Algebraic curves over finite fields, Cambridge Texts in Math. **97**, Cambridge University Press, Cambridge, 1991.

[MS77] F. J. McWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam 1977.

[MV85] Y. I. Manin, S. G. Vlăduţ, *Linear Codes and Modular Codes,* J. Soviet Mathematics **30**, (1985) pp. 2611-2643.

[No22] E. Noether, *Ein algebraisches Kriterium für absolute Irreducibilität,* Math. Ann. **85**, pp. 26-33 (1922).

[Pe91] J. P. Pedersen, *The functionfield of the Ree group,* preprint June 1991.

[Pel91] R. Pellikaan, *On gonality of curves, abundant codes and decoding,* preprint 1991.

[PS90] J. P. Pedersen, A. B. Sørensen, *Codes From Certain Algebraic Function Fields With Many Rational Points*, MAT-REPORT NO. 1990-11, Matematisk Institut, Danmarks Tekniske Højskole, June 1990.

[PSW91] R. Pellikaan, B. Z. Shen, G. J. M. van Wee, *Which linear codes are algebraic-geometric ?,* IEEE Trans. on Information Theory IT-**37** (1991), pp. 583-602.

[Sc76] W. M. Schmidt, Equations over Finite Fields, An Elementary Approach, Lecture Notes in Mathematics 536, Springer-Verlag, 1976.

[Se79] J.-P. Serre, Local Fields, GTM 67, Springer-Verlag 1979.

[Se83] J.-P. Serre, *Sur le nombre des points rationels d'une courbe algébrique sur un corps fini,* C. R. Acad. Sci. Paris **296** (1983), pp. 397-402.

[SS91] J. Schicho, J. R. Sendra, *On the Choice of Pencils in the Parametrization of Curves,* RISC-Linz Series no. 91-01.0. (1991).

[St88] H. Stichtenoth, *A note on Hermitian Codes over GF(q^2),* IEEE Trans on Inf. Theory **34** 1345-1348 (1988).

[SV90] A. N. Skorobogatov, S. G. Vlăduţ, *On the decoding of algebraic-geometric codes,* IEEE Trans. on Information Theory, IT-**36** (1990), pp. 1051-1060.

[SW90] R. Sendra, F. Winkler, *A Symbolic Algorithmus for the Rational Parametrization of Algebraic Plane Curves,* RISC-report 90-45.0, (1990).

[Sø89a] A. B. Sørensen, *A "Full degeneration"-lemma for hypersurfaces in $P(q,n)$*, Preprint Series no. 5, 1989, Matematisk Institut, Aarhus Universitet.

[Sø89b] A. B. Sørensen, *Projective Reed-Muller codes*, Preprint Series no. 11, 1989, Matematisk Institut, Aarhus Universitet. Revised version to appear in IEEE Trans. on Infor. Theory, Nov. 91.

[Sø91a] A. B. Sørensen, *Weighted Reed-Muller Codes*, RISC-Linz Series no. 91-36.0 august 1991, submitted to IEEE Trans. on Inf. Theory.

[Sø91b] A. B. Sørensen, *A Note on Algorithms Deciding Rationality and Absolutely Irreducibility Based on the Number of Rational Solutions*, RISC-Linz Series no 91-37.0, august 1991.

[TV91] M. A. Tsfasman, S. G. Vlăduţ, Algebraic-geometric codes, Mathematics and its Applications **58**, Kluwer Ac. Publ., Dordrecht, The Netherlands 1991.

[TVZ82] M. A. Tsfasman, S. G. Vlăduţ, T. Zink, *Modular curves and Goppa codes better than Varshamov-Gilbert bound,* Math. Nachr. **109**, 13-28 (1982).

[Wa78] R. J. Walker, Algebraic Curves, Springer-Verlag 1978.

[We48] A. Weil, Variétés abéliennes et courbes algébriques, Hermann, Paris 1948.

[We52] A. Weil, *Sur les "formules explicites" de la théorie des nombres premiers*, Comm. Lund (1952) pp. 252-265 = Oeuvres Sc., II. pp. 48-61.

2 On the number of rational points on codimension-1 algebraic sets in $\mathbf{P}^n(\mathbf{F}_q)$

Revised version of [Sø89a].

On the number of rational points on codimension-1 algebraic sets in $P^n(F_q)$.

by

Anders Bjært Sørensen

Abstract.

An upper bound on the number of $\mathbb{F}_q$-rational points on a pure $(n-1)$-dimensional algebraic set of low degree defined over $\mathbb{F}_q$ in $\mathbb{P}^n(\overline{\mathbb{F}}_q)$ is given. The bound depends on n, q, d, where d is the degree of the algebraic set. A number of corollaries are deduced and applications to coding theory are mentioned.

1. Introduction.

Let us fix the necessary notation from algebraic and finite projective geometry.

Notation .

$\mathbb{F}_q$: finite field with q elements. q a prime power.

$\overline{\mathbb{F}}_q$: the algebraic closure of $\mathbb{F}_q$.

$\mathbb{P}^n(k)$: the n-dimensional projective space over the field k.

An algebraic set $X \subseteq \mathbb{P}^n(\overline{\mathbb{F}}_q)$ is defined over $\mathbb{F}_q$, if the homogeneous polynomials defining X are in $\mathbb{F}_q[x_0,x_1, \ldots ,x_n]$. A point P is a $\mathbb{F}_q$-rational point, if the coordinates of P are in $\mathbb{F}_q$.

An algebraic set $X \subseteq \mathbb{P}^n(\overline{\mathbb{F}}_q)$ has pure dimension s, if all it's irreducible components are of dimension s. An algebraic set $X \subseteq \mathbb{P}^n(\overline{\mathbb{F}}_q)$ of pure dimension $n-1$ is defined by a single polynomial F, i.e. $X=Z(F)=\{ P \in \mathbb{P}^n(\overline{\mathbb{F}}_q) \mid F(P) = 0 \}$, and X has degree d, if the homogeneous polynomium F defining X has degree d.

$Z(F)_{\mathbb{F}_q}$ denotes the set of rational zeroes of F in $\mathbb{P}^n(\mathbb{F}_q)$, i.e. $Z(F)_{\mathbb{F}_q} = \{ P \in \mathbb{P}^n(\mathbb{F}_q) \mid F(P) = 0 \}$.

An r-dimensional flat in $\mathbb{P}^n(\mathbb{F}_q)$ is an r-dimensional linear subspace in $\mathbb{P}^n(\overline{\mathbb{F}}_q)$ defined over $\mathbb{F}_q$.

Subspaces in finite projective geometry.

Denote by $\phi(r,n,q)$ the number of r-dimensional flats of $\mathbb{P}^n(\mathbb{F}_q)$ and by $\chi(s,r,n,q)$, $s \leq r$ the number of r-dimensional flats through a fixed s-dimensional flat in $\mathbb{P}^n(\mathbb{F}_q)$. This notation follows [Hi79], where you also find the following well-known formulas:

$$\phi(r,n,q) = \frac{\prod_{i=n-r+1}^{n+1} (q^i-1)}{\prod_{i=1}^{r+1} (q^i-1)}$$

$$\chi(s,r,n,q) \quad = \quad \frac{\prod\limits_{i\equiv r-s+1}^{n-s} (q^i-1)}{\prod\limits_{i=1}^{n-r} (q^i-1)}$$

and easily deduced relations

$$\chi(s,r,n,q) \quad = \quad \phi(n-r-1,n-s-1,q)$$

$$\phi(r,n,q) \quad = \quad \frac{q^{n-r+1}-1}{q^{r+1}-1}\,\phi(r-1,n,q)$$

$$\phi(r,n,q) \quad = \quad \frac{q^{n+1}-1}{q^{n-r}-1}\,\phi(r,n-1,q)$$

$$\phi(r,n,q) \quad = \quad \frac{q^{n+1}-1}{q^{r+1}-1}\,\phi(r-1,n-1,q)$$

$$\phi(n-r,n,q) \quad = \quad \phi(r-1,n,q).$$

2. On Zetafunctions and Weil-bounds .

We now recapitulate some important results on the number of rational points on hypersurfaces.

Let $X \subseteq \mathbb{P}^n(\overline{\mathbb{F}}_q)$ be a hypersurface (i.e. an $(n-1)$-dimensional, smooth, absolutely irreducible algebraic set) defined over $\mathbb{F}_q$, and let N_i denote the number of $\mathbb{F}_{q^i}$-rational points on X. Assume X has degree d, i.e. $X = Z(F)$, where $F \in \mathbb{F}_q[x_0,x_1, \ldots ,x_n]$ and $deg(F) = d$. Define the zetafunction $\zeta(X,\mathbb{F}_q)(t) = \zeta(t)$ by

$$\zeta(t) = exp\left(\sum_{i=1}^{\infty} N_i \frac{t^i}{i} \right).$$

$$| N_i - (1+q^i) | \leq (d-1)(d-2)(q^{\frac{1}{2}})^i \ .$$

This is a special case of Theorem 2.1 (Corollar 2.2), but also a special case of the following version of the Weil-conjectures [We48]

Theorem 2.4 *If $X \subseteq \mathbb{P}^n(\overline{\mathbb{F}}_q)$ is an smooth, absolutely irreducible curve (i.e. of dimension 1) defined over $\mathbb{F}_q$ and of genus g, then*

$$\zeta(t) = \frac{f(t)}{(1-t)(1-qt)}$$

with $f(t) \in \mathbb{Z}[t]$, $f(t) = \prod_{i=1}^{2g}(1-\alpha_i t)$ *and* $|\alpha_i| = q^{1/2}$ *(Riemann-hypothesis).*

The Weil-bound for curves reads

Corollar 2.5 *X as in Theorem 2.4 . Then*

$$| N_i - (1+q^i) | \leq 2g(q^{1/2})^i \ .$$

Remark. It is known that the bound of Corollar 2.5 for many genus g is not the best possible. Serre shows in [Se83] several improvements. Here we mention

Corollar 2.6 *X as in Theorem 2.4 . Then*

$$| N_i - (1+q^i) | \leq g \lfloor 2(q^{1/2})^i \rfloor ,$$

where $\lfloor x \rfloor$ denotes the integer part of x.

Corollar 2.7 *If $X=Z(F)$ is a hypersurface in $\mathbb{P}^n(\overline{\mathbb{F}}_q)$ of degree d and defined over $\mathbb{F}_q$, with the maximal number of rational points w.r.t. Weil-bound (Corollar 2.2), then*

$$r \leq \left(\frac{q^{2n}-1}{q^2-1} - \frac{q^n-1}{q-1}\right) \Big/ \left(q^{\frac{n-1}{2}} + q^{n-1}\right) .$$

The Weil-conjecture says, cf. [Ko84]

Theorem 2.1 . *With X and $\zeta(t)$ as above*

$$(1) \qquad \zeta(t) = \begin{cases} \dfrac{f(t)}{\prod_{i=0}^{n-1}(1-q^i t)} & n \text{ even} \\ \dfrac{1}{f(t)\prod_{i=0}^{n-1}(1-q^i t)} & n \text{ odd} \end{cases}$$

where $f(t) \in \mathbb{Z}[t]$, $f(t) = \prod_{i=1}^{r}(1-\alpha_i t)$ *with* $r = \frac{d-1}{d}\left((d-1)^n - (-1)^n\right)$

and (Riemann-hypothesis) $|\alpha_i| = q^{\frac{n-1}{2}}$ *(as a complex number).*

Corollar 2.2 . *(Generalized Weil-bound) . With notation as above*

$$| N_i - \sum_{j=0}^{n-1} (q^i)^j | \leq r\, q^{\frac{(n-1)i}{2}}$$

Proof : Taking logaritmic derivitive of (1)

$$N_i = \sum_{j=0}^{n-1} (q^i)^j + (-1)^{n+1} \sum_{j=1}^{r} \alpha_j^i$$

Now $|\alpha_i| = q^{\frac{n-1}{2}}$ and the triangleinequality gives

$$| N_i - \sum_{j=0}^{n-1} (q^i)^j | \leq r\, q^{\frac{(n-1)i}{2}} \quad .$$

□

For $n = 2$ we get

Corollar 2.3 . *If $X = Z(F) \subseteq \mathbb{P}^2(\overline{\mathbb{F}}_q)$ is a plane, smooth, absolutely irreducible algebraic curve of degree d (i.e. $deg(F) = d$) defined over $\mathbb{F}_q$, then*

Proof . Use that

$$N_i = \sum_{j=0}^{n-1} (q^i)^j + (-1)^{n+1} \sum_{j=1}^{r} \alpha_j^i \quad , \quad |\alpha_j| = q^{\frac{n-1}{2}}$$

and for N_1 maximal, we have $\alpha_j = (-1)^{n+1} q^{\frac{n-1}{2}}$. Then $\alpha_j^2 = q^{n-1}$ and the inequality $N_1 \leq N_2$ gives the result. □

Corollar 2.8 *If $X=Z(F)$ is a plane, smooth, absolutely irreducible curve of degree d and genus g, defined over $\mathbb{F}_q$, with the maximal number of rational points w.r.t. Weil-bound (Corollar 2.3), then*

$$g \leq \tfrac{1}{2}(q-\sqrt{q})$$

Proof . Corollar 2.7 for $n=2$.

3. The number of rational points on codimension 1- algebraic set in P^n of low degree.

The main result in this note is

Theorem 3.1 . *Let $X \subseteq \mathbb{P}^n(\overline{\mathbb{F}}_q)$ be a pure $(n-1)$-dimensional algebraic set, defined over $\mathbb{F}_q$, and of degree d. Then*

$$| X |_{\mathbb{F}_q} \leq d q^{n-1} + \frac{q^{n-1}-1}{q-1},$$

where $| X |_{\mathbb{F}_q}$ denotes the number of $\mathbb{F}_q$-rational points on X.

Proof :

The case $n=2$:

Now $X = Z(F) = \{ P \in \mathbb{P}^2(\overline{\mathbb{F}}_q) \mid F(P) = 0,\ F \in \mathbb{F}_q[x_0,x_1,x_2] \}$, where F is homogeneous of degree d.

Suppose that F has no linear factors over $\mathbb{F}_q$, i.e. $Z(F)$ contains no $\mathbb{F}_q$-line components.

Let $M = \{(P,L) \mid P \in X \cap L,\ L\ \mathbb{F}_q\text{-line in } \mathbb{P}^2(\overline{\mathbb{F}}_q)\}$. Obviously $|M| = |X|_{\mathbb{F}_q}(1+q)$, since any point are on $1+q$ different $\mathbb{F}_q$-lines. Now, Bezout's theorem tells that any of the $\phi(1,2,q) = 1+q+q^2$ $\mathbb{F}_q$-lines can meet X in at most d different points. Thus,

$$|X|_{\mathbb{F}_q}(1+q) \leq d(1+q+q^2)$$

i.e.

$$|X|_{\mathbb{F}_q} \leq d\frac{1+q+q^2}{1+q} = dq + \frac{d}{1+q}$$

This proves the theorem for $d \leq 1+q$ $(=\phi(0,1,q))$. For $d > 1+q$, the theorem is trivial, since $dq+1 > 1+q+q^2$ $(=\#\mathbb{F}_q\text{-rational points in } \mathbb{P}^2)$.

Now assume that F has $\mathbb{F}_q$-linear factors. Pick a $\mathbb{F}_q$-rational point P on one of these lines. Let t $(1 \leq t \leq d)$ be the number of different $\mathbb{F}_q$-lines through P, which appear as a

factor in F (counted without multiplicity). These t lines contributes with $tq+1$ to $|X|_{\mathbb{F}_q}$. Any of the $(q+1-t)$ other $\mathbb{F}_q$-lines through P (which is not a factor of F) intersect X in at most $d-t$ other points (Bezout). Therefore, we get an upper estimate

$$|X|_{\mathbb{F}_q} \leq tq + 1 + (q+1-t)(d-t)$$

i.e.

$$|X|_{\mathbb{F}_q} \leq dq + 1 + (d-t)(1-t) \leq dq + 1$$

This proves the theorem for $n=2$.

The general statement follows from an induction argument on n:
Assume

$$|X'|_{\mathbb{F}_q} \leq d\,q^{n'-1} + \frac{q^{n'-1}-1}{q-1}$$

for all pure $(n'-1)$-dimensional algebraic sets, X', in $\mathbb{P}^{n'}(\overline{\mathbb{F}}_q)$ of degree d and defined over $\mathbb{F}_q$, with $n' < n$.
Let $X = \bigcup X_i$, where X_i are the absolutely irreducible components of X ($dim(X_i) = n-1$).
1) If no component X_i is contained in any $\mathbb{F}_q$-hyperplane H, the argument goes like this:
Let

$$M_{X,\mathbb{P}^n} = \{(P,L) \mid P \in X \cap L,\ \ L \text{ a } \mathbb{F}_q\text{-line}\}.$$

Then

$$|M_{X,\mathbb{P}^n}| = |X|_{\mathbb{F}_q}\, \chi(0,\, 1,\, n,\, q).$$

Consider $X' = X \cap H = \bigcup (X_i \cap H)$. X' will be a pure $(n-2)$-dimensional algebraic set of degree d contained in H. By induction we know

$$|X'|_{\mathbb{F}_q} \leq d\,q^{n-2} + \frac{q^{n-2}-1}{q-1}$$

and therefore,

$$|M_{X',\mathbb{P}^n \cap H}| \leq \left(dq^{n-2} + \frac{q^{n-2}-1}{q-1}\right) \chi(0,\, 1,\, n-1,\, q)$$

Summation over all $\mathbb{F}_q$-hyperplanes H in $\mathbb{P}^n(\bar{\mathbb{F}}_q)$ gives

$$|M_{X,\mathbb{P}^n}| \leq \frac{\phi(n-1,\, n,\, q)}{\chi(1,\, n-1,\, n,\, q)}\, |M_{X',\mathbb{P}^n \cap H}|$$

i.e. $$|M_{X,\mathbb{P}^n}| \leq \frac{\phi(n-1,\, n,\, q)}{\chi(1,\, n-1,\, n,\, q)}\, (dq^{n-2} + \frac{q^{n-2}-1}{q-1})\, \chi(0,\, 1,\, n-1,\, q)$$

i.e. $$|M_{X,\mathbb{P}^n}| \leq \frac{q^{n+1}-1}{q^{n-1}-1}\, (dq^{n-2} + \frac{q^{n-2}-1}{q-1})\, \phi(n-3,\, n-2,\, q)$$

i.e. $$|M_{X,\mathbb{P}^n}| \leq \frac{q^{n+1}-1}{q^{n}-1}\, (dq^{n-2} + \frac{q^{n-2}-1}{q-1})\, \phi(n-2,\, n-1,\, q)$$

i.e. $$|M_{X,\mathbb{P}^n}| \leq (dq^{n-1} + \frac{q^{n-1}-1}{q-1})\, \phi(n-2,\, n-1,\, q)$$

when $d \leq q+1$.

Since $|M_{X,\mathbb{P}^n}| = |X|_{\mathbb{F}_q}\, \chi(0,\, 1,\, n,\, q) = |X|_{\mathbb{F}_q}\, \phi(n-2,n-1,q)$ the theorem follows.

For $d \geq q+1$, we have $dq^{n-1} + \frac{q^{n-1}-1}{q-1} \geq \frac{q^{n+1}-1}{q-1}$ $(= \#\ \mathbb{F}_q$-rational points in $\mathbb{P}^n)$ and the theorem is trivial.

2) If there is a hyperplane such that a component of X is contained in H, the hyperplane H is a component itself.

Now suppose $X = X_1 \cup H$, where X_1 consists of absolutely irreducible components, no one contained in any $\mathbb{F}_q$-hyperplane, and H a $\mathbb{F}_q$-hyperplane. (i.e. the situation with exactly one hyperplane as a component). Then X_1 has degree $(d-1)$.

Choose a $\mathbb{F}_q$-rational point P on $H \backslash (H \cap X_1)$. (If this is impossible, $|X|_{\mathbb{F}_q} = |X_1|_{\mathbb{F}_q}$, and we are in the case 1)).

The q^{n-1} $\mathbb{F}_q$-lines through P in $\mathbb{P}^n(\bar{\mathbb{F}}_q) \backslash H$ meets X_1 in at most $(d-1)$ points (Bezout). Thus, from

$$|X|_{\mathbb{F}_q} = |X_1 \backslash (X_1 \cap H)| + |H|$$

we get $$|X|_{\mathbb{F}_q} \leq (d-1)\, q^{n-1} + \frac{q^n-1}{q-1} = dq^{n-1} + \frac{q^{n-1}-1}{q-1}\,.$$

3) Suppose $X = X' \cup H_1 \cup H_2 \cdots \cup H_k$, i.e. X consists of k $\mathbb{F}_q$-hyperplanes $H_1,\ldots,H_k$ and X'
consisting of components containing no $\mathbb{F}_q$- hyperplanes (X' a degree $(d-k)$ component like in 1)).
Then X' contributes with less than $(d-k)q^{n-1} + \frac{q^{n-1}-1}{q-1}$ to $|X|_{\mathbb{F}_q}$, and joining the hyperplane H_1 the argument of 2) tell us that

$$|X' \cup H_1|_{\mathbb{F}_q} \leq (d-k+1)q^{n-1} + \frac{q^{n-1}-1}{q-1}, \tag{2}$$

and joining another hyperplane H_i for $i>1$ will increase the rigth hand side of (2) with q^{n-1} at most, since $|H_1 \cap H_i|_{\mathbb{F}_q} = \frac{q^{n-1}-1}{q-1} = 1 + q + \cdots + q^{n-2}$. Hence ,

$$|X|_{\mathbb{F}_q} \leq (d-k)q^{n-1} + \frac{q^{n-1}-1}{q-1} + kq^{n-1} .$$

The degree increases by 1 for every new hyperplane joined and the theorem follows . □

Remark. d $(n-1)$-dimensional flats defined over $\mathbb{F}_q$ in $\mathbb{P}^n(\bar{\mathbb{F}}_q)$ through a common $(n-2)$-dimensional flat are a $(n-1)$-dimensional algebraic set with

$$d\left(\frac{q^n-1}{q-1}\right) - (d-1)\left(\frac{q^{n-1}-1}{q-1}\right) = dq^{n-1} + \frac{q^{n-1}-1}{q-1}$$

$\mathbb{F}_q$-rational points.
This configuration shows that the bound is exact.

Corollar 3.2 . *If $X=Z(F)$ is a smooth, absolutely irreducible plane curve of degree d with the maximal number of points w.r.t. Weil-bound and q is a square, then*

$$d \leq \sqrt{q} + 1.$$

Proof : A direct comparison of Corollar 2.7 and Theorem 3.1 gives

$$dq + 1 < 1 + q + \tfrac{1}{2}(d-1)(d-2)\lfloor 2\sqrt{q}\rfloor$$

i.e

$$d > \sqrt{q} + 2.$$

Therefore, we only have to exclude the case $d = \sqrt{q} + 2$.
Through any $\mathbb{F}_q$-rational point on X there is at least one $\mathbb{F}_q$-line L such that the intersection multiplicity $I_P(L,X) > 1$, namely choose L as the tangentline in P. Counting pairs (P,L) in two different ways now gives the inequality

$$|X|_{\mathbb{F}_q}(q+1) \leq d(1+q+q^2) - |X|_{\mathbb{F}_q},$$

since any point P on X contributes with at least one (P,L) such that $I_P(L,X) > 1$, and therefore, on the right hand side, we loose at least $|X|_{\mathbb{F}_q}$ many pairs (P,L). We finally get

$$|X|_{\mathbb{F}_q} \leq d\,\frac{1+q+q^2}{q+2}$$

Let $d = \sqrt{q} + 2$ and compare with Weil-bound (Corollar 2.7)

$$(\sqrt{q} + 2)(\frac{1+q+q^2}{q+2}) < 1 + q + \sqrt{q}\,(\sqrt{q} + 1)\sqrt{q}$$

i.e.

$$\sqrt{q} < q\sqrt{q} + 3q$$

Hence, $d = \sqrt{q} + 2$ cannot give maximal curves. □

Example . The Hermitian curve $X_1^{s+1} + X_2^{s+1} + X_3^{s+1} = 0$ over $\mathbb{F}_q$, $q=s^2$ has the maximal number of $\mathbb{F}_q$-rational points w.r.t. Weil-bound, namely (s^3+1). This shows that the bound in Corollar 3.2 cannot be sharpened.

Remark . Corollar 2.9 states that for $g > \frac{q-\sqrt{q}}{2}$, the Weil-bound is not the best possible.

This is for smooth, absolutely irreducible, plane curves precisely the same condition as stated in Corollar 3.2.

Corollar 3.3 . *If $X=Z(F)$ is a hypersurface in $\mathbb{P}^n(\overline{\mathbb{F}}_q)$ of degree d and defined over $\mathbb{F}_q$, q a square, with the maximal number of rational points w.r.t. Weil-bound (Corollar 2.3), then*

$$d \leq \sqrt{q} + 1$$

Proof : This is just a generalization of Corollar 3.2. From Theorem 3.1 we know

$$|X|_{\mathbb{F}_q} \leq d q^{n-1} + \frac{q^{n-1}-1}{q-1}$$

and from Weil-bound

$$|X|_{\mathbb{F}_q} \leq \frac{q^n-1}{q-1} + \frac{d-1}{d}((d-1)^n-(-1)^n)(\sqrt{q})^{n-1} .$$

Simple calculations show that for $d = \sqrt{q} + 1$, we have

$$\frac{q^n-1}{q-1} + \frac{d-1}{d}((d-1)^n-(-1)^n)(\sqrt{q})^{n-1} \leq d q^{n-1} + \frac{q^{n-1}-1}{q-1},$$

but for $d = \sqrt{q} + 2$, we have (for $n > 2$)

$$\frac{q^n-1}{q-1} + \frac{d-1}{d}((d-1)^n-(-1)^n)(\sqrt{q})^{n-1} > d q^{n-1} + \frac{q^{n-1}-1}{q-1}.$$

□

Example . The Hermitian hypersurface $X_0^{s+1} + X_1^{s+1} + \cdots + X_n^{s+1} = 0$ over $\mathbb{F}_q$, $q=s^2$ has $(s^{n+1} + (-1)^n)(s^n - (-1)^n)/(s^2-1)$ $\mathbb{F}_q$-rational points and this is maximal w.r.t. Weil-bound. This shows that Corollar 3.3 cannot be sharpened.

Let $\mathbb{F}_q[X_0,X_1, \ldots ,X_m]_h^\nu \cup\{0\}$ be the vectorspace of homogeneous polynomials in X_0,X_1, $\ldots ,X_m$ with coefficients in $\mathbb{F}_q$ and of degree ν.

In [Sø91] we generalize Theorem 3.1 to arbitrary degree, and prove the following

Theorem 3.4 . *Let* $F(X_0, \ldots, X_n) \in \mathbb{F}_q[X_0, \ldots, X_n]_h^\nu$, $\nu - 1 \leq n(q-1)$, $\nu - 1 = r(q-1) + s$, $0 \leq s < q-1$, *and let* $| Z(F)_{\mathbb{F}_q} |$ *denote the number of zero's of* F *in* $\mathbb{P}^n(\mathbb{F}_q)$. *Then*

$$| Z(F)_{\mathbb{F}_q} | = \frac{q^{n+1}-1}{q-1}.$$

or

$$| Z(F)_{\mathbb{F}_q} | \leq \frac{q^{n+1}-1}{q-1} - (q-s)q^{n-r-1}.$$

Remark. Theorem 3.4 has applications in coding theory, in the way that it provides an estimate for the minimum distance for a class of codes, which are presented in another paper [Sø91]

4. References.

[Hi79] : J.W.P. Hirschfeld, Projective Geometries Over Finite Fields, Clarendon Press, Oxford, 1979.

[Ko84] : N. Koblitz, p-adic Numbers, p-adic Analysis, and Zeta-Functions, GTM 58, Springer, 1984.

[Se83] : J.-P. Serre, "*Sur le nombre des points rationnels d'une courbe algebrique sur un corps fini*" , C. R. Acad. Sc. Paris, Serie I, p. 397-402, (1983)

[Sø91] : A.B.Sørensen : "*Projective Reed Muller-Codes*" , to appear in IEEE Trans. on Inf. Theory, nov. 1991.

[We48] : A. Weil : Varietes abeliennes et courbes algebriques, Herman, Paris, 1948.

3 Projective Reed-Muller codes

Revised version of [Sø89b].

Projective Reed-Muller Codes.

by

Anders Bjært Sørensen

Abstract.

A class of codes in the Reed-Muller family, the projective Reed-Muller codes are studied. The exact parameters of the codes are found and the duals are characterized. It is shown that a subclass of the projective Reed-Muller codes are cyclic and the generatorpolynomial is characterized. Tables over parameters of the codes are given.

1. Introduction.

The generalized Reed-Muller codes (GRM codes) were introduced by Kasami, Lin and Peterson [1] and Weldon [2]. They showed that GRM codes are cyclic and thereby determined the minimum distance. Kasami, Lin and Peterson [3] introduced the polynomial codes as a generalization of GRM codes (and of other codes as well) based on the multivariable approach. Delsarte, Goethals and MacWilliams [4] studied in detail the connection between the multivariable and one-variable approach to GRM codes. All these classical works appeared about 1970.

It seems that Manin and Vladut in a paper on algebraic geometric codes [5] are the first to mention the very natural projective parallel of the multivariabel GRM construction, which leads to the projective Reed-Muller codes (PRM codes). They obtained bounds on the minimum distance of PRM codes over $\mathbb{F}_q$ of order ν for $\nu < q$, q a prime power. Lachaud [6] is the first to introduce the notation of projective Reed-Muller codes and studies PRM codes of order 1 and 2.

This paper defines in **section 2** the PRM codes of all orders and discusses their relation to polynomial codes. In **section 3** the exact parameters of PRM codes are given. The duals are characterized in **section 4** and in parallel to the classical works on GRM codes the cyclic properties are studied in **section 5**. It is shown that a subclass of PRM codes is cyclic. A number of examples are shown in detail and at the end of the paper tables over codeparameters are listed.

2. Definition of Projective Reed-Muller codes.

We introduce some usefull concepts and necessary notation.

Notation .

$\mathbf{F}_q$: finite field with q elements, q a prime power. $\mathbf{F}_q^* = \mathbf{F}_q \setminus \{0\}$.

$\mathbf{F}_q[X_0,X_1,\ldots,X_m]$: the ring of polynomials in $X_0,X_1,\ldots,X_m$ with coefficients in $\mathbf{F}_q$.

$\mathbf{F}_q[X_0,X_1,\ldots,X_m]^\nu \cup \{0\}$: the vectorspace of polynomials in $X_0,X_1,\ldots,X_m$ with coefficients in $\mathbf{F}_q$ and of degree ν.

$\mathbf{F}_q[X_0,X_1,\ldots,X_m]_h \cup \{0\}$: the vectorspace of homogeneous polynomials in $X_0,X_1,\ldots,X_m$ with coefficients in $\mathbf{F}_q$.

$\mathbf{F}_q[X_0,X_1,\ldots,X_m]_h^\nu \cup \{0\}$: the vectorspace of homogeneous polynomials in $X_0,X_1,\ldots,X_m$ with coefficients in $\mathbf{F}_q$ and of degree ν.

$\mathbf{A}^m(\mathbf{F}_q)$: the m-dimensional affine space over $\mathbf{F}_q$ ($= \mathbf{F}_q^m$).

$\mathbf{P}^m(\mathbf{F}_q)$: the m-dimensional projective space over $\mathbf{F}_q$.

We will often use the abbreviations $\mathbf{A}^m$ for $\mathbf{A}^m(\mathbf{F}_q)$, $\mathbf{P}^m$ for $\mathbf{P}^m(\mathbf{F}_q)$ and

$\underline{X} = X_1,\ldots,X_m$ or $\underline{X} = X_0,X_1,\ldots,X_m$.

If $F(\underline{X}) \in \mathbf{F}_q[X_0,X_1,\ldots,X_m]$ and $P \in \mathbf{P}^m(\mathbf{F}_q)$, then $F(P)$ means F evaluated in some representative $(a_0 : a_1 : \ldots : a_m)$ for P. Therefore, $F(P)$ is in general dependent on the choice of representative for P. The standard representation for projective points is on the form $(0 : \ldots : 0 : 1 : a_j : \ldots : a_m)$, that is zeros to the left and the first non-zero entry equal to 1. Unless explict stated otherwise the standard representation will be used.

It is well-known, cf. [4], that the GRM codes $C_\nu(m, q)$ over $\mathbf{F}_q$ of order ν, $1 \leq \nu \leq m(q-1)$ and of length q^m can be defined as

$$C_\nu(m,q) = \{(F(\underline{0}), F(P_1), \ldots, F(P_{q^m-1})) \mid F(X_1,\ldots,X_m) \in \mathbf{F}_q[X_1,\ldots,X_m],\ deg(F) \leq \nu\ \},$$

where $P_i \in \mathbf{A}^m(\mathbf{F}_q)$ runs through $\mathbf{A}^m(\mathbf{F}_q)\setminus\{\underline{0}\}$, for $i = 1,\ldots,q^m-1$.
It is also well-known (cf. [1], [9, p. 72]) that $C_\nu(m,q)$ is an $[q^m, k, d]$ - code with

$$k = \sum_{t=0}^{\nu} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{t-jq+m-1}{t-jq} \tag{1}$$

$$d = (q-s)q^{m-r-1}\ , \tag{2}$$

where $\nu = r(q-1)+s$, $0 \leq s < q-1$, $0 \leq r \leq m-1$.

The main idea is now to emphasize the affine structures of GRM codes and then make their projective parallel.

Definition 2.1 . The projective Reed-Muller code $PC_\nu(m,q)$ over $\mathbf{F}_q$ of order ν, $\nu \in \mathbf{Z}_+$, and of length $n = (q^{m+1}-1)/(q-1)$ is

$$PC_\nu(m,q) =$$

$$\{(F(P_1),\ldots,F(P_n)) \mid F(X_0,\ldots,X_m) \in \mathbf{F}_q[X_0,X_1,\ldots,X_m]_h^\nu\} \cup \{\underline{0}\},$$

where $P_1,\ldots,P_n$ (in standard representation) runs through $\mathbf{P}^m(\mathbf{F}_q)$.

Remark 2.2 . A set of representatives of the points in $\mathbf{P}^n(\mathbf{F}_q)$ different from the standard representatives will, used in definition 2.1, produce a code isometric with $PC_\nu(m,q)$, that means a code with the same codeparameters. This is due to the fact that $F(\widetilde{P}) = \lambda^\nu F(P)$, if $\widetilde{P} = \lambda P$, $\lambda \in \mathbf{F}_q^*$, is another representative of the point P. It corresponds to multiplication of the i'th coordinate of all codewords by some $\mu_i \in \mathbf{F}_q^*$, $i = 1,\ldots,n$.

Definition 2.1 is equivalent to the definition introduced by Lachaud in [6].
Remark 3.4 will explain that the PRM codes are trivial for $\nu \geq m(q-1)+1$, so we will from now on assume that $1 \leq \nu \leq m(q-1)$.

Remark 2.3 . The PRM codes of order ν over $\mathbf{F}_q$, where $1 \leq \nu \leq m(q-1)$, $\nu = 0 \bmod q-1$, extended with the all-one vector coincide with the $(n, m+1, 1, \nu/(q-1), q)$- polynomial codes, as defined in [3] (and they are furthermore the duals of the PRM codes of order $m(q-1)-\nu$, see Theorem 4.4). These codes are in [4] called the nonprimitive generalized Reed-Muller codes. All results in the following are therefore well-known in the case $\nu = 0 \bmod q-1$.

3. The parameters of Projective Reed-Muller codes.

The most difficult parameter to calculate is the the minimum distance. The natural idea is to use the knowledge from the affine situation - the minimum distance of GRM codes. We start with some necessary notation and some lemma's.

Notation.

If $F(\underline{X}) = \sum c_{i_0 i_1 \cdots i_m} X_0^{i_0} X_1^{i_1} \cdots X_m^{i_m}$ is a polynomial in $\mathbf{F}_q[X_0, X_1, \ldots, X_m]$, denote by $\overline{F}(\underline{X})$ the reduced form of $F(\underline{X})$, i.e. the polynomial we get by in any term replacing any factor $X_j^{t_j}$, where $t_j = a(q-1) + b$, $0 < b \leq q-1$, with X_j^b (i.e. reducing modulo $X_j^q - X_j$).

If $M \subseteq \mathbf{F}_q[X_0, \ldots, X_m]$ is any set of polynomials, denote by $\overline{M}$ the corresponding set of reduced polynomials. So $\overline{\mathbf{F}_q[X_0, \ldots, X_m]}$ denotes the set of all reduced polynomials over $\mathbf{F}_q$ in the variables $X_0, \ldots, X_m$.

For F homogeneous (resp. F), we denote by $Z(F)_{\mathbf{F}_q}$ (or just $Z(F)$, when $\mathbf{F}_q$ is clear from the context) the algebraic set of zeros of F in $\mathbf{P}^m(\mathbf{F}_q)$ (resp. $\mathbf{A}^{m+1}(\mathbf{F}_q)$), i.e. $Z(F)_{\mathbf{F}_q} = \{ P \in \mathbf{P}^m(\mathbf{F}_q) \mid F(P) = 0 \}$ (resp. $\{ P \in \mathbf{A}^{m+1}(\mathbf{F}_q) \mid F(P) = 0 \}$). The degree of $X = Z(F)_{\mathbf{F}_q}$ is $\deg(X) = \deg(F)$.

Lemma 3.1 . *If* $F(\underline{X}) \in \mathbf{F}_q[X_0, X_1, \ldots, X_m]$ *and* $G(\underline{X}) \in \mathbf{F}_q[X_0, X_1, \ldots, X_m]_h$ *then*

1) $F(P) = \overline{F}(P)$ *for any* $P \in \mathbf{A}^{m+1}(\mathbf{F}_q)$.
2) $G(P) = \overline{G}(P)$ *for any* $P \in \mathbf{P}^m(\mathbf{F}_q)$.
3) *If* $F(P) = 0$ *for all* $P \in \mathbf{A}^{m+1}(\mathbf{F}_q)$, *then* $\overline{F}(\underline{X}) = 0$.
4) *If* $G(P) = 0$, *for all* $P \in \mathbf{P}^m(\mathbf{F}_q)$, *then* $\overline{G}(\underline{X}) = 0$.

Proof : 1) and 2) is trivial. 4) follows from 3). A proof of 3) can be found in [8, p. 122] or [4]. □

Lemma 3.2 . *Let* $F(\underline{X}) \in \mathbf{F}_q[X_0,X_1,\ldots,X_m]_h^\nu$ *and* $H(\underline{X}) \in \mathbf{F}_q[X_0,X_1,\ldots,X_m]_h^1$. *Assume* $F(P)=0$, *for all* $P \in Z(H)_{\mathbf{F}_q}$. *Then there exists* $\widetilde{F}(\underline{X}) \in \mathbf{F}_q[X_0,X_1,\ldots,X_m]_h^\nu$ *and* $G(\underline{X}) \in \mathbf{F}_q[X_0,X_1,\ldots,X_m]_h^{\nu-1}$ *such that*

$$Z(F)_{\mathbf{F}_q} = Z(\widetilde{F})_{\mathbf{F}_q} \quad \text{and} \quad \widetilde{F} = HG.$$

Proof : Assume that $H(\underline{X}) = X_0$. Let $F(\underline{X}) = X_0F_1(\underline{X}) + F_2(\underline{X})$, where $F_2(\underline{X}) \in \mathbf{F}_q[X_1,\ldots,X_m]_h^\nu$, $F_1(\underline{X}) \in \mathbf{F}_q[X_0,X_1,\ldots,X_m]_h^{\nu-1}$. From Lemma 3.1 (4) we get that $\overline{F}_2(\underline{X}) = 0$, such that $\overline{F}(\underline{X}) = X_0\overline{F}_1(\underline{X})$. Then $\widetilde{F}(\underline{X}) = X_0F_1(\underline{X})$ has the desired properties.

If $H(\underline{X}) \neq X_0$, then consider a $\mathbf{F}_q$-linear injective transformation ϕ that maps $H(\underline{X})$ into X_0. Then write $\phi(\widetilde{F}) = X_0F_3(\underline{X})$, $F_3(\underline{X}) \in \mathbf{F}_q[X_0,X_1,\ldots,X_m]_h^{\nu-1}$ and let $\widetilde{F} = \phi^{-1}(\phi(\widetilde{F})) = H\phi^{-1}(F_3)$. □

Lemma 3.3 . *Let* $P = (0:0:\ldots:1:w_{j+1}:\ldots:w_m) \in \mathbf{P}^m(\mathbf{F}_q)$, $0 \leq j \leq m$.
For any s , $0 < s \leq q-1$, *the polynomial*

$$F_P^s(\underline{X}) = X_j^s \prod_{i=0}^{j-1}(X_j^{q-1}-X_i^{q-1}) \prod_{i=j+1}^{m}(X_j^{q-1}-(X_i-w_iX_j)^{q-1})$$

is indicatorfunction for P *and of degree* $d = s \bmod q-1$.
The $(q^{m+1}-1)/(q-1)$ *polynomials* $\overline{F}_P^s(\underline{X})$ *are a basis for* $\overline{\mathbf{F}_q[X_0,X_1,\ldots,X_m]_h^d}$, *the set of homogeneous polynomials of degree* d *in reduced form, and any* $H \in \overline{\mathbf{F}_q[X_0,X_1,\ldots,X_m]_h^d}$ *is uniquely written as*

$$H(\underline{X}) = \sum_{P \in \mathbf{P}^m(\mathbf{F}_q)} H(P)\,\overline{F}_P^s(\underline{X}). \tag{3}$$

Proof : If $Q = P$, then $\overline{F}_P^s(Q) = 1$, and if $Q \neq P$, then $\overline{F}_P^s(Q) = 0$. Hence $\overline{F}_P^s(\underline{X})$ is indicatorfunction for P and $\overline{F}_P^s(\underline{X})$ is homogeneous of degree $m(q-1)+s = s \bmod (q-1)$.

These functions are linearly independent and any $H \in \overline{\mathbb{F}_q[X_0,X_1,\ldots,X_m]}_h^d$ can be written as in (3). Uniqueness follows from Lemma 3.1 (4). □

Remark 3.4 . Only PRM codes of degree $0 < \nu \leq m(q-1)$ are of any interest, since PRM codes of order $\nu \geq m(q-1)+1$ are trivial:
Let $\underline{c} = (c_1,\ldots,c_n)$ be any word. Choose $F(\underline{X}) \in \mathbb{F}_q[X_0,X_1,\ldots,X_m]_h^\nu$ such that

$$\overline{F}(\underline{X}) = \sum_{P_i \in \mathbb{P}^m(\mathbb{F}_q)} c_i \overline{F}^s_{P_i}(\underline{X}), \quad s = \nu \bmod (q-1)$$

Then $c_i = F(P_i)$, *i.e.* $\underline{c}$ is a codeword and the code is trivial.

Lemma 3.5 . *Let* $F(\underline{X}) \in \mathbb{F}_q[X_0,X_1,\ldots,X_m]$ *and* $Q \in \mathbb{P}^m(\mathbb{F}_q)$. *Assume* $\overline{F}(\underline{X})$ *has degree* $d \leq m(q-1)$ *and* $F(P) = 0$, *for all* $P \in \mathbb{P}^m \setminus \{Q\}$.
Then $F(Q) = 0$.

Proof : Assume $F(Q) \neq 0$. Then $\lambda \overline{F}$ will be an indicatorfunction for Q, $\lambda = F(Q)^{-1}$, and by Lemma 3.3 $\lambda \overline{F} = \overline{F}^s_P(\underline{X})$ for some s, $0 < s \leq q-1$. Now $\deg(\overline{F}^s_P(\underline{X})) > m(q-1)$ and we have a contradiction. □

Now we are able to state and prove the main theorem.

Theorem 3.6. *The projective Reed-Muller code* $C_\nu(m,q)$, $1 \leq \nu \leq m(q-1)$, *is a* $[n,k,d]$-*code with*

$$n = \frac{q^{m+1}-1}{q-1}, \qquad k = \sum_{\substack{t = \nu \bmod q-1 \\ 0 < t \leq \nu}} \left(\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{t-jq+m}{t-jq} \right)$$

$$d = (q-s)q^{m-r-1}, \quad \textit{where } \nu - 1 = r(q-1)+s, \ 0 \leq s < q-1.$$

Proof : The length n is $(q^{m+1}-1)/(q-1)$ by definition.

To find the minimum distance we consider a codeword $\underline{c}=(F(P_1),\ldots,F(P_n))$, $F(\underline{X})\in \mathbb{F}_q[X_0,X_1,\ldots,X_m]_h^\nu$, $\nu-1=r(q-1)+s$, $0\le s<q-1$, $\nu\le m(q-1)+1$. We want to estimate the weight of $\underline{c}$, i.e. the number of zeros of F, when F is evaluated in all points of the m-dimensional projective space.

If $|Z(F)_{\mathbb{F}_q}|$ denotes the number of zeros of F in $\mathbf{P}^m(\mathbf{F}_q)$, the claim is:

$$|Z(F)_{\mathbb{F}_q}| = \frac{q^{m+1}-1}{q-1} \quad \text{or} \quad |Z(F)_{\mathbb{F}_q}| \le \frac{q^{m+1}-1}{q-1} - (q-s)q^{m-r-1} \tag{4}$$

We will prove (4) by induction on m:

If $m=1$, then $\deg(F)=s+1$, $0\le s\le q-1$, and on the projective line $\mathbf{P}^1(\mathbf{F}_q)$, F has at most $s+1$ zeros : If $P_\infty=(0:1)$ is zero of F, then $F(1,X_1)$ has degree (in X_1) less than or equal to s.

Assume that (4) is correct for $m-1$ and consider now the case m:
Consider $X=Z(F)_{\mathbb{F}_q}\subseteq \mathbb{P}^m(\mathbb{F}_q)$, the algebraic set of zeros of F, and let F be of degree ν, where $\nu-1\le m(q-1)$, $\nu-1=r(q-1)+s$, $0\le s<q-1$.

I) if $\nu-1=(m-1)(q-1)+s$, $0\le s<q-1$, we would like to prove

$$|Z(F)_{\mathbb{F}_q}| = \frac{q^{m+1}-1}{q-1} \quad \text{or} \quad |Z(F)_{\mathbb{F}_q}| \le \frac{q^{m+1}-1}{q-1} - (q-s) \tag{5}$$

Assume that (5) is false, i.e. that $0<|\mathbb{P}^m(\mathbb{F}_q)\setminus X|=t<q-s$, and let $\mathbb{P}^m(\mathbb{F}_q)\setminus X=\{P_1,P_2,\ldots,P_t\}$. Let $G_i(\underline{X})$, $i=1,\ldots,t-1$ be linear polynomials defining $t-1$ hyperplanes such that $G_i(P_j)=\delta_{ij}$, $i=1,\ldots,t-1$, $j=1,\ldots,t$.
Then the polynomial

$$H(\underline{X})=F(\underline{X})\prod_{i=1}^{t-1}G_i(\underline{X})$$

has degree $(m-1)(q-1)+(s+t) \leq m(q-1)$ and $Z(H)_{\mathbf{F}_q} = \mathbf{P}^m(\mathbf{F}_q) \setminus \{P_t\}$. This contradicts Lemma 3.5.

II) if $\nu \leq (m-1)(q-1)$:

a) Assume X doesn't contain (as a set of points) any hyperplane in $\mathbf{P}^m(\mathbf{F}_q)$. For any hyperplane π, we can consider $Y = X \cap \pi$ as an algebraic set in $\mathbf{P}^{m-1}(\mathbf{F}_q)$ with $\deg(Y) = \deg(X)$ (first assume $\pi = Z(X_0)$ and then use $\mathbf{F}_q$-linear coordinate transformations to generalize to any hyperplane). We observe that $\deg(Y) = \deg(X) = \nu \leq (m-1)(q-1)$, so by the induction hypothesis we have for all $\mathbf{F}_q$-hyperplanes π that

$$|X \cap \pi| \leq \frac{q^m-1}{q-1} - (q-s)q^{m-r-2}$$

i.e.
$$|\pi \setminus (X \cap \pi)| \geq (q-s)q^{m-r-2} .$$

By counting pairs (P, π), $P \in (\mathbf{P}^m(\mathbf{F}_q) \setminus X) \cap \pi$, π a $\mathbf{F}_q$-hyperplane, in two different ways, we have

$$|\mathbf{P}^m \setminus X| \cdot \frac{q^m-1}{q-1} \geq \frac{q^{m+1}-1}{q-1}(q-s)q^{m-r-2}, \tag{6}$$

since $(q^m-1)/(q-1)$ is the number of $\mathbf{F}_q$-hyperplanes in $\mathbf{P}^m(\mathbf{F}_q)$ through a fixed point and $(q^{m+1}-1)/(q-1)$ is the number of $\mathbf{F}_q$-hyperplanes in $\mathbf{P}^m(\mathbf{F}_q)$.

Equation (6) gives

$$|\mathbf{P}^m \setminus X| \geq (q-s)q^{m-r-1},$$

and we are done.

b) Assume that X contains the set of points of a hyperplane $\pi = Z(H)$, $H(\underline{X}) \in \mathbb{F}_q[X_0,X_1,\ldots,X_m]_h^1$. Then by Lemma 3.2, we can assume that $X = Z(HF_1)$, $F_1(\underline{X}) \in \mathbb{F}_q[X_0,X_1,\ldots,X_m]_h^{\nu-1}$. Let $X' = Z(F_1)$ and observe

$$|X| = |X'\backslash(X'\cap\pi)| + |\pi|. \tag{7}$$

Since $X'\backslash(X'\cap\pi) \subseteq \mathbb{P}^m(\mathbb{F}_q)\backslash\pi \simeq \mathbb{A}^m(\mathbb{F}_q)$, $X'\backslash(X'\cap\pi)$ is an affine algebraic set, i.e. the zero set for some polynomial of degree $\nu-1 = r(q-1)+s$:

If $\pi = Z(X_0)$, then the polynomial defining $X'\backslash(X'\cap\pi)$ is $F_1(1,X_1,\ldots,X_n)$ and $\deg(F_1) = \nu-1$. Using a $\mathbb{F}_q$-linear coordinate transformation taking $H(\underline{X})$ to X_0, the general situation is reduced to this case.

We have seen that $X'\backslash(X'\cap\pi)$ correspond to zeros of some polynomial of degree $\nu-1 = r(q-1)+s$. Using (2), we get

$$|X'\backslash(X'\cap\pi)| \leq q^m - (q-s)q^{m-r-1} \tag{8}$$

Adding $|\pi|$ to (8) yields

$$|X| \leq \frac{q^{m+1}-1}{q-1} - (q-s)q^{m-r-1}.$$

This completes the proof of (4) and gives a lower bound

$$d \geq (q-s)q^{m-r-1}.$$

Equality follows, since the polynomial

$$F(\underline{X}) = X_r \prod_{i=0}^{r-1}(X_i^{q-1}-X_r^{q-1}) \prod_{j=1}^{s}(\lambda_j X_r - X_{r+1}),$$

where $\lambda_i \neq \lambda_j$ for $i \neq j$ and $\lambda_i \in \mathbb{F}_q^*$, has zeros at all points except those on the form $(0:0:\ldots:1:a_{r+1}:\ldots:a_m)$, where $a_{r+1} \neq \lambda_j$, $j=1,\ldots,s$ and $a_t \in \mathbb{F}_q$ for $t=r+2,\ldots,m$.

We see that there is exactly $(q-s)q^{m-r-1}$ such points, so F corresponds to a codeword of minimum weight. This completes the proof of the formula for the minimum distance d.

The dimension k of $PC_\nu(m,q)$ is found by combinatorical reasoning: It follows from Lemma 3.7 below that

$$N(t,m+1,q-1) = \sum_{j=0}^{m+1}(-1)^j\binom{m+1}{j}\binom{t-jq+m}{t-jq}$$

is the number of distinct monomials in $X_0,X_1,\ldots,X_m$ of degree t and such that no reduction is possible (non-reducible), i.e. the exponents are all less than or equal to $q-1$.

Now monomials of degree ν and with exponents greater than $q-1$ can be reduced and this process is many to one (f.ex. $X_0^qX_1$ and $X_0X_1^q$ both reduces to X_0X_1). Divide the set of reducible monomials of degree ν into disjoint classes by calculating the degree of the reduced polynomial. The class corresponding to the degree t , where $t=\nu \bmod q-1$ contributes with $N(t,m+1,q-1)$ distinct monomials of degree t.

All these monomials evaluated gives linearly independent codewords, since a linear dependent combination correspond to a polynomial $F \in \mathbb{F}_q[X_0,X_1,\ldots,X_m]_h^\nu$ such that $F(P)=0, \forall\, P \in \mathbb{P}^m$, and therefore $\overline{F}(X)=0$, by Lemma 3.1. The formula for k now follows by summation. □

Lemma 3.7 . *The number of ways one can place t objects in m cells such that no cell contains more than s objects is*

$$N(t,m,s) = \sum_{j=0}^{m}(-1)^j\binom{m}{j}\binom{t-j(s+1)+m-1}{t-j(s+1)}.$$

Proof :

$$\binom{t+m-1}{t}$$

is the number of ways one can place t objects in m cells without restrictions.

$$\binom{t-j(s+1)+m-1}{t-j(s+1)}$$

is the number of ways one can place t objects in m cells such that j (prespecified) cells contain at least $s+1$ objects (and therefore "fail").
The principle of exclusion and inclusion now gives the result. □

Remark 3.8. The minimum distance for PRM codes in case $\nu \leq q+1$ has been proven independently by J. P. Serre in a letter to M. Tsfasman of July 24, 1989. See also [7].

4. The duals of Projective Reed-Muller codes.

It is well-known, cf.[4], that the dual of a GRM code of order ν (and length q^m) is a GRM code of order $m(q-1)-\nu-1$. Somewhat similar holds for PRM codes.

Let $d(x,m,q)$ denote the number of forms $X_0^{i_0}X_1^{i_1}\cdots X_m^{i_m}$ with $0 \le i_j \le q-1$, $\sum_{j=0}^{m} i_j = x$. First three introductory lemmas:

Lemma 4.1 . *Let* $0 \le s < q-1$.

$$d(x,m,q) = d((m+1)(q-1)-x,m,q) \tag{9}$$

$$\begin{aligned} \sum_{\substack{x<(m+1)(q-1)\\ x=s \bmod (q-1)}} d(x,m,q) = \\ \sum_{\substack{0<x\le(m+1)(q-1)\\ x=s \bmod (q-1)}} d(x,m,q) = \frac{q^{m+1}-1}{q-1}. \end{aligned} \tag{10}$$

Proof : The substitution $X_j^{i_j} \to X_j^{q-1-i_j}$ gives a $1-1$ map between forms of degree x and forms of degree $(m+1)(q-1)-x$ and (9) follows.

Consider the partition of the set of forms $X_0^{i_0}X_1^{i_1}\cdots X_m^{i_m}$ with $0 \le i_j \le q-1$ in $\{1\}, S_1, S_2, \ldots, S_{q-1}$, where S_k is the set of forms $X_0^{i_0}X_1^{i_1}\cdots X_m^{i_m}$ with $0 \le i_j \le q-1$, $\sum_{j=0}^{m} i_j = k \bmod (q-1)$, and $\sum_{j=0}^{m} i_j \ne 0$.

By symmetry $|S_k| = (q^{m+1}-1)/(q-1)$, for $k = 1,\ldots,q-1$, and the formula (10) follows.

□

Lemma 4.2 . *Let* $F(\underline{X}) \in \mathbb{F}_q[X_0,X_1,\ldots,X_m]$ *and* $d = deg(\overline{F}(\underline{X}))$.
If $d<(m+1)(q-1)$, *then*

$$\sum_{P\in\mathbb{A}^{m+1}(\mathbb{F}_q)} F(P) = 0 .$$

Proof : cf. [4, Lemma 1.6]. □

Lemma 4.3 . *Let* $F(\underline{X}) \in \mathbb{F}_q[X_0,X_1,\ldots,X_m]_h$ *and* $d = deg(\overline{F}(\underline{X}))$.
If $d<(m+1)(q-1)$ *and* $d=0$ *mod* $q-1$, *then*

$$\sum_{P\in\mathbb{P}^{m}(\mathbb{F}_q)} F(P) = 0 .$$

Proof : For F homogeneous and $\deg(F)=0$ mod $q-1$, we have

$$\sum_{P\in\mathbb{A}^{m+1}(\mathbb{F}_q)} F(P) = (q-1) \sum_{P\in\mathbb{P}^{m}(\mathbb{F}_q)} F(P) + F(0).$$

and left side vanishes by Lemma 4.2 . □

We are now ready for the main theorem of this section:

Theorem 4.4 . *Let* $\mu = m(q-1)-\nu$. *Then*

$$PC_\nu(m,q)^\perp = PC_\mu(m,q) \quad \textit{for } \nu \neq 0 \textit{ mod } (q-1) \tag{11}$$

$$PC_\nu(m,q)^\perp = \overline{PC_\mu(m,q)} \quad \textit{for } \nu = 0 \textit{ mod } (q-1) \tag{12}$$

where $\overline{PC_\mu(m,q)} = span_{\mathbb{F}_q}\{\underline{1}, PC_\mu(m,q)\}$ (*i.e.* $PC_\mu(m,q)$ "*extended*").

Proof :

Assume $\nu \neq 0 \bmod q-1$:

Let $\underline{c}_\nu = (F_1(P_1),\ldots,F_1(P_n)) \in PC_\nu(m,q)$ and $\underline{c}_\mu = (G_1(P_1),\ldots,G_1(P_n)) \in PC_\mu(m,q)$. Then $deg(F_1G_1) = m(q-1) < (m+1)(q-1)$ and from Lemma 4.3, we get that $<\underline{c}_\nu, \underline{c}_\mu> = 0$. Thus, $PC_\nu(m,q)^\perp \supseteq PC_\mu(m,q)$.

Now consider the dimensions:

$$dim\ PC_\nu(m,q) = \sum_{\substack{x \leq \nu \\ x \equiv_{q-1} \nu}} d(x,m,q) \quad \text{and} \quad dim\ PC_\mu(m,q) = \sum_{\substack{x \leq \mu \\ x \equiv_{q-1} \mu}} d(x,m,q)$$

where $\mu = m(q-1)-\nu$, and using Lemma 4.1, we get

$$dim\ PC_\nu(m,q) + dim\ PC_\mu(m,q)$$

$$= \sum_{\substack{x \leq \nu \\ x \equiv_{q-1} \nu}} d(x,m,q) + \sum_{\substack{x \leq m(q-1)-\nu \\ x \equiv_{q-1} \nu}} d(x,m,q)$$

$$= \sum_{\substack{x \leq \nu \\ x \equiv_{q-1} \nu}} d(x,m,q) + \sum_{\substack{0 < x < (m+1)(q-1)-\nu \\ x \equiv_{q-1} \nu}} d(x,m,q)$$

$$= \sum_{\substack{x \leq \nu \\ x \equiv_{q-1} \nu}} d(x,m,q) + \sum_{\substack{0 < x < (m+1)(q-1)-\nu \\ x \equiv_{q-1} \nu}} d((m+1)(q-1)-x,m,q)$$

$$= \sum_{\substack{x \leq \nu \\ x \equiv_{q-1} \nu}} d(x,m,q) + \sum_{\substack{\nu < x < (m+1)(q-1) \\ x \equiv_{q-1} \nu}} d(x,m,q) = \frac{q^{m+1}-1}{q-1}.$$

Hence, $PC_\nu(m,q)^\perp = PC_\mu(m,q)$.

Assume $\nu = 0 \bmod q-1$:

Computations like before shows that

$$dim\ PC_\nu(m,q) + dim\ PC_\mu(m,q) = \sum_{\substack{0<x\le\nu \\ x\equiv_{q-1}\nu}} d(x,m,q) + \sum_{\substack{0<x\le\mu \\ x\equiv_{q-1}\mu}} d(x,m,q) = \frac{q^{m+1}-1}{q-1} - 1.$$

Now extend the code $PC_\mu(m,q)$ with the all-one vector corresponding to evaluation of the constant polynomial 1, and call the extended code $\overline{PC_\mu(m,q)}$. Then we have

$$dim\ PC_\nu(m,q) + dim\ \overline{PC_\mu(m,q)} = \frac{q^{m+1}-1}{q-1}.$$

Let $\underline{c}_\nu = (F_1(P_1),\ldots,F_1(P_n)) \in PC_\nu(m,q)$ and $\underline{c}_\mu = (G_1(P_1),\ldots,G_1(P_1)) \in PC_\mu(m,q)$. Then, $deg(F_1G_1) = m(q-1) < (m+1)(q-1)$ and from Lemma 4.3, we get that $<\underline{c}_\nu, \underline{c}_\mu + \lambda\underline{1}> = <\underline{c}_\nu, \underline{c}_\mu> + <\underline{c}_\nu, \lambda\underline{1}> = 0$.
This proves the theorem. □

Remark 4.5. In [4, Th. 3.2.1] a result equivalent with (12) is proved. However, the notation in [4] differs a little, since in [4] the all-one vector is included by definition of the nonprimitive GRM codes and has to be removed to get the dual code (instead of added).

5. Cyclic Projective Reed-Muller codes.

Kasami et. al. [2] showed that the GRM codes (with one coordinate dropped) are cyclic and also precisely descibed the roots of the corresponding generator-polynomial. In [4] Delsarte et. al. showed that the cyclic properties of GRM codes are related to the possibility of a cyclic arrangement of the points of $\mathbb{A}^m(\mathbb{F}_q)\setminus\{0\}$. Following the idea in [4], we get the following projective analogy:

Let α be a primitive element of $\mathbb{F}_{q^{m+1}}$ and let $m(x)=\sum_{i=0}^{m+1}\epsilon_i x^i$, $\epsilon_{m+1}=1$, be the minimal polynomial of α. Let M_α be the matrix

$$M_\alpha = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & & \cdots & & 1 \\ -\epsilon_0 & & \cdots & & -\epsilon_m \end{bmatrix}.$$

$<M_\alpha>$ is the subgroup of $GL(m+1,q)$ generated by M_α and $|<M_\alpha>| = q^{m+1}-1$. Then 1-1 maps are established

$$\mathbb{A}^{m+1}(\mathbb{F}_q)\setminus\{\underline{0}\} \quad \leftrightarrow \quad \mathbb{F}^*_{q^{m+1}} \quad \leftrightarrow \quad <M_\alpha>$$

$$(a_0, a_1, \ldots, a_m) \quad \mapsto \quad \alpha^i=\sum_{j=0}^{m} a_j\alpha^j \quad \mapsto \quad M^i_\alpha.$$

These $1-1$ maps naturally induces $1-1$ maps on quotients

$$\mathbb{P}^m(\mathbb{F}_q) \quad \leftrightarrow \quad \mathbb{F}^*_{q^{m+1}}/\mathbb{F}^*_q \quad \leftrightarrow \quad <M_\alpha>/Z$$

$$(a_0 : a_1 : \ldots : a_m) \quad \mapsto \quad \overline{\alpha^i} = \overline{\sum_{j=0}^{m} a_j \alpha^j} \quad \mapsto \quad \overline{M_\alpha^i} \ ,$$

where $Z = \{ \lambda I \mid \lambda \in \mathbb{F}_q^* \} \leq GL(m+1, q)$.

If $(n, q-1) = 1$, $n = (q^{m+1}-1)/(q-1)$, another natural cyclic description of $\mathbb{P}^m(\mathbb{F}_q)$ arises. Consider the subgroup $<M_\alpha^{q-1}> \leq <M_\alpha> \leq GL(m+1,q)$, with order $|<M_\alpha^{q-1}>| = n$ and since $(n, q-1) = 1$, we have natural $1-1$ maps as before

$$\mathbb{P}^m(\mathbb{F}_q) \quad \leftrightarrow \quad \mathbb{F}_{q^{m+1}}^* \Big/ \mathbb{F}_q^* \quad \leftrightarrow \quad <\mathrm{M}_\alpha^{q-1}>$$

$$(a_0 : a_1 : \ldots : a_m) \quad \mapsto \quad \alpha^{(q-1)i} = \sum_{j=0}^{m} a_j \alpha^j \quad \mapsto \quad M_\alpha^{(q-1)i} \ ,$$

where $(a_0 : a_1 : \ldots : a_m)$ is the unique representative for a projective point that correspond to $\alpha^{(q-1)i}$ for some i (such i exist since $(n, q-1) = 1$). Remark that M_α^{q-1} correspond to the minimal polynomial for $\beta = \alpha^{q-1}$ and for that reason we let $M_\beta = M_\alpha^{q-1}$.

<u>Example</u> . Consider $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2-2x-1)$ and let α be a primitive element.
Then $1 = \alpha^0$, $x = \alpha^1$, $2x+1 = \alpha^2$, $2x+2 = \alpha^3$, $2 = \alpha^4$, $2x = \alpha^5$, $x+2 = \alpha^6$, $x+1 = \alpha^7$ and the natural identification of $\mathbb{P}^1(\mathbb{F}_3)$ induced from $\mathbb{A}^2(\mathbb{F}_3)$ is

$\mathbb{P}^1(\mathbb{F}_3) \quad (a_0 : a_1) \ \mapsto \ \overline{a_0 + a_1 x} \in \mathbb{F}_9^* / \mathbb{F}_3^*$

$\mathbb{P}^1(\mathbb{F}_3) = \Big\{ (1:0), (0:1), (1:2), (1:1) \Big\}$

$\mathbb{F}_9^* / \mathbb{F}_3^* = \Big\{ \{1,2\}, \{x, 2x\}, \{2x+1, x+2\}, \{2x+2, x+1\} \Big\}$

$= \Big\{ \{\alpha^0, \alpha^4\}, \{\alpha^1, \alpha^5\}, \{\alpha^2, \alpha^6\}, \{\alpha^3, \alpha^7\} \Big\}$

The second cyclic description is not valid here, since $(4,2) \neq 1$.
($<\beta> = \{1, \alpha^2, \alpha^4, \alpha^6\}$ corresponds to (1:0) and (1:2) only).

Example . Consider $\mathbb{F}_{27} = \mathbb{F}_3[x]/(x^3 - x^2 - 2)$ and let α be a primitive element in $\mathbb{F}_{27}^*$.

$\mathbb{F}_{27}^* / \mathbb{F}_3^* = \left\{ \{\alpha^0, \alpha^{13}\}, \{\alpha^1, \alpha^{14}\}, \ldots, \{\alpha^{12}, \alpha^{25}\} \right\} \simeq \mathbb{P}^2(\mathbb{F}_3)$ and

$<\beta> = <\alpha^2> = \{\alpha^0, \alpha^2, \ldots, \alpha^{24}\}$ gives a set of representatives for points in $\mathbb{P}^2(\mathbb{F}_3)$.

Theorem 5.1 . *If* $\nu = 0 \ mod \ q-1$ *or* $(n, q-1) = 1$, *then* $PC_\nu(m,q)$ *is equivalent to a cyclic code.*

Proof :

Using the cyclic arrangement of the points in $\mathbb{P}^m(\mathbb{F}_q)$ described above, we have:

$$P_1, P_2 = MP_1, \ldots, P_n = M^{n-1}P_1,$$

where $M = M_\alpha$ in case $\nu = 0 \bmod q-1$ and $M = M_\beta$ in case $(n, q-1) = 1$. Observing that $M_\alpha^n P_1 = \mu P_1$ for some $\mu \in \mathbb{F}_q^*$, $M_\beta^n P_1 = P_1$ and $F(\lambda P_1) = \lambda^\nu F(P_1) = F(P_1)$, when $deg(F) = \nu = 0 \bmod q-1$, we find that

$$C = \{(F(P_1), \ldots, F(P_n)) \mid F(X_0, \ldots, X_m) \in \mathbb{F}_q[X_0, X_1, \ldots, X_m]_h^\nu\}$$

$$= \{(F(P_1), \ldots, F(M^{n-1}P_1)) \mid F(X_0, \ldots, X_m) \in \mathbb{F}_q[X_0, X_1, \ldots, X_m]_h^\nu\}$$

is a cyclic code :

Consider the linear transformation on $\mathbb{P}^m(\mathbb{F}_q)$ given by M:

Let $F \in \mathbb{F}_q[X_0,\ldots,X_m]_h^\nu$ and define $G(\underline{X}) = F(M\underline{X})$.

Then $G \in \mathbb{F}_q[X_0,\ldots,X_m]_h^\nu$ and $G(P_i) = F(P_{i+1})$ for $i = 1,\ldots,n-1$ and $G(P_n) = F(MP_n) = F(P_1)$.

Hence, $(F(P_2),\ldots,F(P_n),F(P_1)) = (G(P_1),\ldots,G(P_n))$ and C is cyclic. C only differs from $PC_\nu(m, q)$ by permutations of coordinates, so they are equivalent. □

From Theorem 5.1 we know that for $\nu = 0 \bmod q-1$ or $(n, q-1) = 1$, $PC_\nu(m,q)$ is a cyclic code of length $n = (q^{m+1}-1)/(q-1)$. Therefore, it has a 1-variabel description as an ideal in $\mathbb{F}_q[x]/(x^n-1)$ generated by some polynomial $g(x)$. Like before let α be a primitive element of $\mathbb{F}_{q^{m+1}}$. Then all roots of x^n-1 lies in $\mathbb{F}_{q^{m+1}}$ and are powers of $\beta = \alpha^{q-1}$.

In the case $\nu = 0 \bmod q-1$, Theorem 5.1 have been treated in [2] and [4]. Let $h = \sum_{i=0}^{m} h_i q^i$, $h_i \in \mathbb{Z}_+$, and define the q-weight of h to be $w_q(h) = \sum_{i=0}^{m} h_i$. As a special case of [2, Cor. 7], we have

Theorem 5.2 . *Assume $\nu = 0$ mod $q-1$. Then,*

$$\beta^j = \alpha^{(q-1)j} \text{ is a root in } g(x) \ (0 \le j < n) \quad \Leftrightarrow$$

$$w_q((q-1)j) \le (m+1)(q-1)-\nu-1.$$

□

In parallel to the Theorem 5.2 it is possible to characterize the roots of the cyclic PRM codes in case $(n, q-1) = 1$. First a central lemma inspired by the corresponding affine version in [4].

Lemma 5.3 . *Let* $F(\underline{X}) \in \mathbb{F}_q[X_0,\ldots,X_m]_h^\nu$ *and let* $B=(b_0:\ldots:b_m)\in \mathbb{P}^m(\mathbb{F}_{q^{m+1}})$. *Assume* $w_q(h)\le (m+1)(q-1)-\nu-1$ *and* $(w_q(h)+\nu)=0 \bmod q-1$. *Then*

$$\sum_{P\in\mathbb{P}^m(\mathbb{F}_q)} F(P)(<P,B>)^h = 0$$

where $<P,B> = \sum_{i=0}^{m} p_i b_i$ *for* $P=(p_0:\ldots:p_m)$.

Proof :

$$(<P,B>)^h = \Big(\sum_{i=0}^{m} p_i b_i\Big)^{\sum_{j=0}^{m} h_j q^j} = \prod_j \Big((\sum_i p_i b_i)^{q^j}\Big)^{h_j} = \prod_j \Big(\sum_i p_i (b_i)^{q^j}\Big)^{h_j} =$$

$$\sum_{k_0,\cdots,k_m} Q_{k_0,\cdots,k_m}(B) p_0^{k_0}\cdots p_m^{k_m} ,$$

where $Q_{k_0,\cdots,k_m}(B)$ is a polynomial in $b_0,\ldots,b_m$ and $\sum_j k_j = \sum_j h_j = w_q(h)$. Therefore,

$$\sum_{P\in\mathbb{P}^m(\mathbb{F}_q)} F(P)(<P,B>)^h = 0,$$

from Lemma 4.3, ($deg(F) + w_q(h) < (m+1)(q-1)$). □

Notation . For $0\le j< q^{m+1}-1$, $n=\frac{q^{m+1}-1}{q-1}$ let J denote the set of $q-1$ representatives for j mod n less than $q^{m+1}-1$, i.e.

$$J = \{h \bmod (q^{m+1}-1) \mid h=j+kn,\ k=0,1,\ldots,q-2\}.$$

Furthermore, define

$$S_\mu = \{j \mid j=j_0+j_1q+j_2q^2+\cdots+j_mq^m,\ 0\le j_i\le q-1,$$

$$\sum_{i=0}^{m} j_i = \mu \bmod q-1 \quad \text{and} \quad \sum_{i=0}^{m} j_i \le \mu \}$$

$$R_\nu = \{ j \bmod n \mid 0 \le j < q^{m+1}-1,\ \exists j' \in J:$$
$$w_q(j') \le (m+1)(q-1)-\nu-1 \ \wedge \ (w_q(j')+\nu) = 0 \bmod q-1 \}$$

Theorem 5.4 . *Assume* $(n, q-1) = 1$. *Then*

$$\beta^j = \alpha^{(q-1)j} \text{ is a root in } g(x)\ (0 \le j < n) \quad \Leftrightarrow \quad j \in R_\nu.$$

Proof : The "if"-part: Let $c(x) = \sum_{i=1}^{n} c_i x^i$ be the polynomial corresponding to the codeword $(c_0, \ldots, c_n) \in PC_\nu(m,q)$. The cyclic describtion of $\mathbf{P}^m(\mathbf{F}_q)$ gives that $c_i = F(M_\beta^i P_1)$, where $F(\underline{X})$ is the corresponding $(m+1)$-variable polynomial. Let $j \in R_\nu$ and let $j' \in J$ have the property

$$w_q(j') \le (m+1)(q-1)-\nu-1 \ \wedge \ (w_q(j')+\nu) = 0 \bmod q-1.$$

Now $\alpha^{(q-1)j'} = \alpha^{(q-1)j}$ is a root of $g(x)$ if and only if $c(\alpha^{(q-1)j'}) = 0$:

$$c(\alpha^{(q-1)j'}) = \sum_i F(M_\beta^i P_1)\left(\alpha^{(q-1)j'}\right)^i = \sum_i F(M_\beta^i P_1)(\alpha^{i(q-1)})^{j'} =$$

$$\sum_i F(M_\alpha^{i(q-1)} P_1)(<P_1 M_\alpha^{i(q-1)}, \underline{\alpha}>)^{j'}, (\underline{\alpha} = (1, \alpha, \ldots, \alpha^m)).$$

Now from Lemma 5.3 the "if"-part is clear.

The "only if"-part: We want to show that the number of roots already found are equal to $dim(PC_\nu(m,q)^\perp)$.

First observe that $R_\nu \supseteq \{ j \bmod n \mid j \in S_\mu \}$. If $0 \le j < q^{m+1}-1$, such that $(j \bmod n) \in R_\nu$, then $j \bmod n = j' \bmod n$ and $j' \in S_\mu$, so $R_\nu = \{ j \bmod n \mid j \in S_\mu \}$.

Since $(n, q-1) = 1$, we have $(m+1, q-1) = 1$. Therefore, if $j_1 \in S_\mu$, and

$j_2 = j_1 + kn$, $0 \le k < q-1$, then $w_q(j_2) \neq w_q(j_1) \bmod q-1$ and $j_2 \notin S_\mu$. It follows that $|S_\mu| = |\{j \bmod n \,|\, j \in S_\mu\}| = |R_\nu|$. Now $|S_\mu| = dim(PC_\nu(m,q)^\perp)$ and the "only if"-part follows. □

Remark. A proof of Theorem 5.2 similar to the proof above can easily be done.

Example . Let $q=3$, $m=2$, i.e. $n=13$ and $(n, q-1)=1$.

The cyclotomic cosets are

$n=13$:	$n=26$ (subscript = 3-weight):
$\{ 0 \}$	$\{ 0 \}_0$
$\{ 1, 3, 9 \}$	$\{ 1, 3, 9 \}_1$
$\{ 2, 6, 5 \}$	$\{ 2, 6, 18 \}_2$
$\{ 4, 12, 10 \}$	$\{ 4, 12, 10 \}_2$
$\{ 7, 8, 11 \}$	$\{ 5, 15, 19 \}_3$
	$\{ 7, 21, 11 \}_3$
	$\{ 8, 24, 20 \}_4$
	$\{ 13 \}_3$
	$\{ 14, 16, 22 \}_4$
	$\{ 17, 25, 23 \}_5$

$\nu = 1$: Then by Theorem 3.6 $PC_1(2,3)$ has parameters $k=3$ and $d=9$. Theorem 5.4 gives the following conditions for β^j being a root:

$$w_3(j) \le 4 \ \wedge \ w_3(j) + 1 = 0 \bmod 2$$

i.e

$$w_3(j) = 1 \vee 3 .$$

i.e

$$j \in R_1 = \{0, 1, 3, 9, 2, 6, 5, 7, 8, 11\}$$

So $$g(x) = \prod_{j \in R_1} (x - \beta^j)$$

is the generatorpolynomium for a cyclic code equivalent to $PC_1(2,3)$.
The (simple) BCH-bound gives $d \geq 6$.

$\nu = 2$: Then by Theorem 3.6 $PC_2(2,3)$ has parameters $k = 6$ and $d = 6$.
Theorem 5.4 gives the following conditions for β^j being a root:

$$w_3(j) \leq 3 \ \wedge \ w_3(j) + 2 = 0 \bmod 2$$

i.e

$$w_3(j) = 0 \vee 2 .$$

i.e

$$j \in R_2 = \{0, 2, 6, 5, 4, 12, 10\}$$

So $$g(x) = \prod_{j \in R_2} (x - \beta^j)$$

is the generatorpolynomium for a cyclic code equivalent to $PC_2(2,3)$.
The (simple) BCH-bound gives $d \geq 4$.
Since $\nu = 0 \bmod 2$, we can also use another representation and Theorem 5.2 gives the following conditions for β^j being a root:

$$w_3(2j) \leq 3 \ \wedge \ w_3(2j) = 0 \bmod 2$$

i.e

$$w_3(2j) = 0 \vee 2.$$

i.e

$$2j \in S_2 = \{0, 2, 6, 18, 4, 12, 10\}$$

i.e

$$j \in K_2 = \{0, 1, 3, 9, 2, 6, 5\}$$

So

$$g(x) = \prod_{j \in K_2} (x - \beta^j)$$

is the generatorpolynomium for a cyclic code equivalent to $PC_2(2,3)$.
The (simple) BCH-bound gives $d \geq 5$.

$\nu = 3$: Then by Theorem 3.6 $PC_3(2,3)$ has parameters $k = 10$ and $d = 3$.
Theorem 5.4 gives the following conditions for β^j being a root:

$$w_3(j) \leq 2 \quad \wedge \quad w_3(j) + 3 = 0 \bmod 2$$

i.e

$$w_3(j) = 1.$$

i.e

$$j \in R_3 = \{1, 3, 9\}$$

So

$$g(x) = \prod_{j \in R_3} (x - \beta^j)$$

is the generatorpolynomium for a cyclic code equivalent to $PC_3(2,3)$.
The (simple) BCH-bound gives $d \geq 2$.

Observe that (Th. 4.4) $PC_1(2,3)^{\perp} = PC_3(2,3)$ and that $PC_2(2,3) \subseteq PC_2(2,3)^{\perp}$.

Example . $m = 2$, $q = 4$, $n = 21$. $(n, q-1) \neq 1$.
We have cyclic codes for $\nu = 0 \bmod 3$ $(0 \leq \nu \leq 6)$.

The cyclotomic cosets are

$n = 21$:

$\{ 0 \}$
$\{ 1, 4, 16 \}$
$\{ 2, 8, 11 \}$
$\{ 3, 12, 6 \}$
$\{ 5, 20, 17 \}$
$\{ 7 \}$
$\{ 9, 15, 18 \}$
$\{ 10, 19, 13 \}$
$\{ 14 \}$

$n = 63$ (subscript = 4-weight):

$\{ 0 \}_0$ $\{ 21 \}_3$
$\{ 1, 4, 16 \}_1$ $\{ 22, 25, 37 \}_4$
$\{ 2, 8, 32 \}_2$ $\{ 23, 29, 53 \}_5$
$\{ 3, 12, 48 \}_3$ $\{ 26, 41, 38 \}_4$
$\{ 5, 20, 17 \}_2$ $\{ 27, 45, 54 \}_5$
$\{ 6, 24, 33 \}_3$ $\{ 30, 57, 39 \}_6$
$\{ 7, 28, 49 \}_4$ $\{ 31, 61, 55 \}_7$
$\{ 9, 36, 18 \}_3$ $\{ 42 \}_6$
$\{ 10, 40, 34 \}_4$ $\{ 43, 46, 58 \}_7$
$\{ 11, 44, 50 \}_5$ $\{ 47, 62, 59 \}_8$
$\{ 13, 52, 19 \}_4$
$\{ 14, 56, 35 \}_5$
$\{ 15, 60, 51 \}_6$

$\nu = 3$: Then by Theorem 3.6 $PC_3(2,4)$ has parameters $k = 10$ and $d = 8$. Theorem 5.2 gives the following conditions for β^j being a root:

$$w_4(3j) \leq 5 \ \wedge \ w_4(3j) = 0 \bmod 3$$

i.e

$$w_4(3j) = 0 \vee 3.$$

i.e

$$3j \in S_3 = \{ 0, 3, 12, 48, 6, 24, 33, 9, 36, 18, 21 \}$$

i.e

$$j \in K_3 = \{ 0, 1, 4, 16, 2, 8, 11, 3, 12, 6, 7 \}$$

So

$$g(x) = \prod_{j \in K_3} (x - \beta^j)$$

is the generatorpolynomium for a cyclic code equivalent to $PC_3(2,4)$.
The (simple) BCH-bound gives $d \geq 6$

Remark . It is easy to show (by direct check) that the linear code $PC_1(1,3)$ of length 4, dimension 3 and minimum distance 2 is not a cyclic code for any choice of representation of points in $\mathbb{P}^1(\mathbb{F}_3)$.

6. Acknowledgements.

At the workshop in Coding Theory and Algebraic Geometry, C.I.R.M., Marseille, may 1989, M. Tsfasman asked the question about the minimum distance in algebraic geometry terms and generously shared his ideas with the participants. His remarks encouraged the author to work on the problem.

The author would like to thank Tom Høholdt and Jens Peter Pedersen from the group in codingtheory at The Technical University of Copenhagen, Math. Inst. for stimulating discussions on the subject. Also thanks to the anonymous referees for their comments and advice.

7. References.

[1] : T. Kasami, S. Lin and W. W. Peterson : "New Generalizations of the Reed-Muller Codes Part I: Primitive Codes, *IEEE*, *IT*-14, no.2, 1968.

[2] : E. J. Weldon: "New Generalizations of the Reed-Muller Codes Part II: Nonprimitive Codes, *IEEE*, *IT*-14, no.2, 1968.

[3] : T. Kasami, S. Lin and W. W. Peterson : "Polynomial Codes", *IEEE*, *IT*-14, no.6, 1968.

[4] : P. Delsarte, J. M. Goethals, F. J. MacWilliams : "On Generalized Reed-Muller Codes and Their Relatives", *Information and Control* 16, pp.403-442, 1970.

[5] : S. G. Vladut, Y. I. Manin : "Linear Codes and Modular Curves", *J. Soviet Math.* 30, pp. 2611-2643, 1985.

[6] : G. Lachaud : "Projective Reed-Muller codes", in *Lect. Notes in Comp. Sci.* 311, Springer, 1988.

[7] : G. Lachaud : "The parameters of Projective Reed-Muller Codes", *Discrete Mathematics* 81 (1990) pp. 217-221.

[8] : S. Lang, *Algebra*, Addison Wesley, New York 1965.

[9] : I. F. Blake, R. C. Mullin, *The Mathematical Theory of Coding*, Academic Press, New York 1975.

8. Tables.

Tables over parameters of projective Reed-Muller codes $PC_\nu(m,q)$ are listed for small values of q and m. The degree ν is denoted by "deg" in the table. Codes which are equivalent to cyclic codes because of Theorem 5.2 are indicated in table by a "x", and those because of Theorem 5.4 by a "•".

TABLE

q = 3 , m = 2 , n = 13 •
deg = 1 k = 3 d = 9
deg = 2 k = 6 d = 6 x
deg = 3 k = 10 d = 3
deg = 4 k = 12 d = 2 x

q = 3 , m = 3 , n = 40
deg = 1 k = 4 d = 27
deg = 2 k = 10 d = 18 x
deg = 3 k = 20 d = 9
deg = 4 k = 29 d = 6 x
deg = 5 k = 36 d = 3
deg = 6 k = 39 d = 2 x

q = 3 , m = 4 , n = 121 •
deg = 1 k = 5 d = 81
deg = 2 k = 15 d = 54 x
deg = 3 k = 35 d = 27
deg = 4 k = 60 d = 18 x
deg = 5 k = 86 d = 9
deg = 6 k = 105 d = 6 x
deg = 7 k = 116 d = 3
deg = 8 k = 120 d = 2 x

q = 3 , m = 5 , n = 364
deg = 1 k = 6 d = 243
deg = 2 k = 21 d = 162 x
deg = 3 k = 56 d = 81
deg = 4 k = 111 d = 54 x
deg = 5 k = 182 d = 27
deg = 6 k = 252 d = 18 x
deg = 7 k = 308 d = 9
deg = 8 k = 342 d = 6 x
deg = 9 k = 358 d = 3
deg =10 k = 363 d = 2 x

q = 3 , m = 6 , n = 1093 •
deg = 1 k = 7 d = 729
deg = 2 k = 28 d = 486 x
deg = 3 k = 84 d = 243
deg = 4 k = 189 d = 162 x
deg = 5 k = 350 d = 81
deg = 6 k = 546 d = 54 x
deg = 7 k = 743 d = 27
deg = 8 k = 903 d = 18 x
deg = 9 k = 1009 d = 9
deg =10 k = 1064 d = 6 x
deg =11 k = 1086 d = 3
deg =12 k = 1092 d = 2 x

q = 4 , m = 2 , n = 21
deg = 1 k = 3 d = 16
deg = 2 k = 6 d = 12
deg = 3 k = 10 d = 8 x
deg = 4 k = 15 d = 4
deg = 5 k = 18 d = 3
deg = 6 k = 20 d = 2 x

q = 4 , m = 3 , n = 85 •
deg = 1 k = 4 d = 64
deg = 2 k = 10 d = 48
deg = 3 k = 20 d = 32 x
deg = 4 k = 35 d = 16
deg = 5 k = 50 d = 12
deg = 6 k = 64 d = 8 x
deg = 7 k = 75 d = 4
deg = 8 k = 81 d = 3
deg = 9 k = 84 d = 2 x

q = 4 , m = 4 , n = 341 •
deg = 1 k = 5 d = 256
deg = 2 k = 15 d = 192
deg = 3 k = 35 d = 128 x
deg = 4 k = 70 d = 64
deg = 5 k = 116 d = 48
deg = 6 k = 170 d = 32 x
deg = 7 k = 225 d = 16
deg = 8 k = 271 d = 12
deg = 9 k = 305 d = 8 x
deg =10 k = 326 d = 4
deg =11 k = 336 d = 3
deg =12 k = 340 d = 2 x

q = 4 , m = 5 , n = 1365
deg = 1 k = 6 d =1024
deg = 2 k = 21 d = 768
deg = 3 k = 56 d = 512 x
deg = 4 k = 126 d = 256
deg = 5 k = 237 d = 192
deg = 6 k = 392 d = 128 x
deg = 7 k = 582 d = 64
deg = 8 k = 783 d = 48
deg = 9 k = 972 d = 32 x
deg =10 k = 1128 d = 16
deg =11 k = 1239 d = 12
deg =12 k = 1308 d = 8 x
deg =13 k = 1344 d = 4
deg =14 k = 1359 d = 3
deg =15 k = 1364 d = 2 x

q = 5 , m = 2 , n = 31 •
deg = 1 k = 3 d = 25
deg = 2 k = 6 d = 20
deg = 3 k = 10 d = 15
deg = 4 k = 15 d = 10 x
deg = 5 k = 21 d = 5
deg = 6 k = 25 d = 4
deg = 7 k = 28 d = 3
deg = 8 k = 30 d = 2 x

q = 5 , m = 3 , n = 156
deg = 1 k = 4 d = 125
deg = 2 k = 10 d = 100
deg = 3 k = 20 d = 75
deg = 4 k = 35 d = 50 x
deg = 5 k = 56 d = 25
deg = 6 k = 78 d = 20
deg = 7 k = 100 d = 15
deg = 8 k = 120 d = 10 x
deg = 9 k = 136 d = 5
deg =10 k = 146 d = 4
deg =11 k = 152 d = 3
deg =12 k = 155 d = 2 x

q = 5 , m = 4 , n = 781 •
deg = 1 k = 5 d = 625
deg = 2 k = 15 d = 500
deg = 3 k = 35 d = 375
deg = 4 k = 70 d = 250 x
deg = 5 k = 126 d = 125
deg = 6 k = 200 d = 100
deg = 7 k = 290 d = 75
deg = 8 k = 390 d = 50 x
deg = 9 k = 491 d = 25
deg =10 k = 581 d = 20
deg =11 k = 655 d = 15
deg =12 k = 710 d = 10 x
deg =13 k = 746 d = 5
deg =14 k = 766 d = 4
deg =15 k = 776 d = 3
deg =16 k = 780 d = 2 x

q = 7 , m = 2 , n = 57
deg = 1 k = 3 d = 49
deg = 2 k = 6 d = 42
deg = 3 k = 10 d = 35
deg = 4 k = 15 d = 28
deg = 5 k = 21 d = 21
deg = 6 k = 28 d = 14 x
deg = 7 k = 36 d = 7

deg = 8 k = 42 d = 6
deg = 9 k = 47 d = 5
deg =10 k = 51 d = 4
deg =11 k = 54 d = 3
deg =12 k = 56 d = 2 x

q = 7 , m = 3 , n = 400
deg = 1 k = 4 d = 343
deg = 2 k = 10 d = 294
deg = 3 k = 20 d = 245
deg = 4 k = 35 d = 196
deg = 5 k = 56 d = 147
deg = 6 k = 84 d = 98 x
deg = 7 k = 120 d = 49
deg = 8 k = 159 d = 42
deg = 9 k = 200 d = 35
deg =10 k = 241 d = 28
deg =11 k = 280 d = 21
deg =12 k = 315 d = 14 x
deg =13 k = 344 d = 7
deg =14 k = 365 d = 6
deg =15 k = 380 d = 5
deg =16 k = 390 d = 4
deg =17 k = 396 d = 3
deg =18 k = 399 d = 2 x

q = 8 , m = 2 , n = 73 •
deg = 1 k = 3 d = 64
deg = 2 k = 6 d = 56
deg = 3 k = 10 d = 48
deg = 4 k = 15 d = 40
deg = 5 k = 21 d = 32
deg = 6 k = 28 d = 24
deg = 7 k = 36 d = 16 x
deg = 8 k = 45 d = 8
deg = 9 k = 52 d = 7
deg =10 k = 58 d = 6
deg =11 k = 63 d = 5
deg =12 k = 67 d = 4
deg =13 k = 70 d = 3
deg =14 k = 72 d = 2 x

q = 8 , m = 3 , n = 585 •
deg = 1 k = 4 d = 512
deg = 2 k = 10 d = 448
deg = 3 k = 20 d = 384
deg = 4 k = 35 d = 320
deg = 5 k = 56 d = 256
deg = 6 k = 84 d = 192
deg = 7 k = 120 d = 128 x
deg = 8 k = 165 d = 64
deg = 9 k = 214 d = 56
deg =10 k = 266 d = 48
deg =11 k = 319 d = 40
deg =12 k = 371 d = 32
deg =13 k = 420 d = 24
deg =14 k = 464 d = 16 x
deg =15 k = 501 d = 8
deg =16 k = 529 d = 7
deg =17 k = 550 d = 6
deg =18 k = 565 d = 5
deg =19 k = 575 d = 4
deg =20 k = 581 d = 3
deg =21 k = 584 d = 2 x

q = 9 , m = 2 , n = 91 •
deg = 1 k = 3 d = 81
deg = 2 k = 6 d = 72
deg = 3 k = 10 d = 63
deg = 4 k = 15 d = 54
deg = 5 k = 21 d = 45
deg = 6 k = 28 d = 36
deg = 7 k = 36 d = 27
deg = 8 k = 45 d = 18 x
deg = 9 k = 55 d = 9
deg =10 k = 63 d = 8
deg =11 k = 70 d = 7
deg =12 k = 76 d = 6
deg =13 k = 81 d = 5
deg =14 k = 85 d = 4
deg =15 k = 88 d = 3
deg =16 k = 90 d = 2 x

q = 9 , m = 3 , n = 820
deg = 1 k = 4 d = 729
deg = 2 k = 10 d = 648
deg = 3 k = 20 d = 567
deg = 4 k = 35 d = 486
deg = 5 k = 56 d = 405
deg = 6 k = 84 d = 324
deg = 7 k = 120 d = 243
deg = 8 k = 165 d = 162 x
deg = 9 k = 220 d = 81
deg =10 k = 280 d = 72
deg =11 k = 344 d = 63
deg =12 k = 410 d = 54
deg =13 k = 476 d = 45
deg =14 k = 540 d = 36
deg =15 k = 600 d = 27
deg =16 k = 654 d = 18 x
deg =17 k = 700 d = 9
deg =18 k = 736 d = 8
deg =19 k = 764 d = 7
deg =20 k = 785 d = 6
deg =21 k = 800 d = 5
deg =22 k = 810 d = 4
deg =23 k = 816 d = 3
deg =24 k = 819 d = 2 x

q = 11 , m = 2 , n = 133 •
deg = 1 k = 3 d = 121
deg = 2 k = 6 d = 110
deg = 3 k = 10 d = 99
deg = 4 k = 15 d = 88
deg = 5 k = 21 d = 77
deg = 6 k = 28 d = 66
deg = 7 k = 36 d = 55
deg = 8 k = 45 d = 44
deg = 9 k = 55 d = 33
deg =10 k = 66 d = 22 x
deg =11 k = 78 d = 11
deg =12 k = 88 d = 10
deg =13 k = 97 d = 9
deg =14 k = 105 d = 8
deg =15 k = 112 d = 7
deg =16 k = 118 d = 6
deg =17 k = 123 d = 5
deg =18 k = 127 d = 4
deg =19 k = 130 d = 3
deg =20 k = 132 d = 2 x

q = 13 , m = 2 , n = 183
deg = 1 k = 3 d = 169
deg = 2 k = 6 d = 156
deg = 3 k = 10 d = 143
deg = 4 k = 15 d = 130
deg = 5 k = 21 d = 117
deg = 6 k = 28 d = 104
deg = 7 k = 36 d = 91
deg = 8 k = 45 d = 78
deg = 9 k = 55 d = 65
deg =10 k = 66 d = 52
deg =11 k = 78 d = 39
deg =12 k = 91 d = 26 x
deg =13 k = 105 d = 13
deg =14 k = 117 d = 12
deg =15 k = 128 d = 11
deg =16 k = 138 d = 10
deg =17 k = 147 d = 9
deg =18 k = 155 d = 8
deg =19 k = 162 d = 7
deg =20 k = 168 d = 6
deg =21 k = 173 d = 5
deg =22 k = 177 d = 4
deg =23 k = 180 d = 3
deg =24 k = 182 d = 2 x

q = 16 , m = 2 , n = 273
deg = 1 k = 3 d = 256
deg = 2 k = 6 d = 240
deg = 3 k = 10 d = 224
deg = 4 k = 15 d = 208

deg = 5 k = 21 d = 192
deg = 6 k = 28 d = 176
deg = 7 k = 36 d = 160
deg = 8 k = 45 d = 144
deg = 9 k = 55 d = 128
deg =10 k = 66 d = 112
deg =11 k = 78 d = 96
deg =12 k = 91 d = 80
deg =13 k = 105 d = 64
deg =14 k = 120 d = 48
deg =15 k = 136 d = 32 x
deg =16 k = 153 d = 16
deg =17 k = 168 d = 15
deg =18 k = 182 d = 14
deg =19 k = 195 d = 13
deg =20 k = 207 d = 12
deg =21 k = 218 d = 11
deg =22 k = 228 d = 10
deg =23 k = 237 d = 9
deg =24 k = 245 d = 8
deg =25 k = 252 d = 7
deg =26 k = 258 d = 6
deg =27 k = 263 d = 5
deg =28 k = 267 d = 4
deg =29 k = 270 d = 3
deg =30 k = 272 d = 2 x

q = 32 , m = 2 , n = 1057 •
deg = 1 k = 3 d =1024
deg = 2 k = 6 d = 992
deg = 3 k = 10 d = 960
deg = 4 k = 15 d = 928
deg = 5 k = 21 d = 896
deg = 6 k = 28 d = 864
deg = 7 k = 36 d = 832
deg = 8 k = 45 d = 800
deg = 9 k = 55 d = 768
deg =10 k = 66 d = 736
deg =11 k = 78 d = 704
deg =12 k = 91 d = 672
deg =13 k = 105 d = 640
deg =14 k = 120 d = 608
deg =15 k = 136 d = 576
deg =16 k = 153 d = 544
deg =17 k = 171 d = 512
deg =18 k = 190 d = 480
deg =19 k = 210 d = 448
deg =20 k = 231 d = 416
deg =21 k = 253 d = 384
deg =22 k = 276 d = 352
deg =23 k = 300 d = 320
deg =24 k = 325 d = 288
deg =25 k = 351 d = 256
deg =26 k = 378 d = 224
deg =27 k = 406 d = 192
deg =28 k = 435 d = 160
deg =29 k = 465 d = 128
deg =30 k = 496 d = 96
deg =31 k = 528 d = 64 x
deg =32 k = 561 d = 32
deg =33 k = 592 d = 31
deg =34 k = 622 d = 30
deg =35 k = 651 d = 29
deg =36 k = 679 d = 28
deg =37 k = 706 d = 27
deg =38 k = 732 d = 26
deg =39 k = 757 d = 25
deg =40 k = 781 d = 24
deg =41 k = 804 d = 23
deg =42 k = 826 d = 22
deg =43 k = 847 d = 21
deg =44 k = 867 d = 20
deg =45 k = 886 d = 19
deg =46 k = 904 d = 18
deg =47 k = 921 d = 17
deg =48 k = 937 d = 16
deg =49 k = 952 d = 15
deg =50 k = 966 d = 14
deg =51 k = 979 d = 13
deg =52 k = 991 d = 12
deg =53 k = 1002d = 11
deg =54 k = 1012d = 10
deg =55 k = 1021d = 9
deg =56 k = 1029d = 8
deg =57 k = 1036d = 7
deg =58 k = 1042d = 6
deg =59 k = 1047d = 5
deg =60 k = 1051d = 4
deg =61 k = 1054d = 3
deg =62 k = 1056d = 2 x

4 Codes from certain algebraic function fields with many rational places

Reprint of [PS90].

CODES FROM CERTAIN ALGEBRAIC FUNCTION FIELDS WITH MANY RATIONAL PLACES

JENS PETER PEDERSEN & ANDERS BJÆRT SØRENSEN

I. Introduction

Geometric Goppa codes are linear error-correcting codes constructed from algebraic curves [1], [2], [3]. The parameters of a geometric Goppa code from an algebraic curve can be determined or estimated, when the genus and the number of rational points of the curve is known. Curves with low genus and many rational points yields good codes.

In [4], Hansen and Stichtenoth constructed an algebraic curve in the projective plane over the finite field F_q, $q = 2^{2n+1}$, with $q^2 + 1$ F_q-rational points and a low genus, and used this curve to construct a family of geometric Goppa codes. The purpose of this paper is to extend the results and proofs of Hansen and Stichtenoth to projective planes over F_q, where q is an arbitrary prime power. However, instead of using the language of algebraic curves, we use the language of algebraic function fields in one variable, cf. [5] (see also [6] for a function field approach to geometric Goppa codes).

In section II, we define a function field $F = \mathsf{F}_q(x_1, x_2)$ in one variable over F_q. We prove, that F has $q^2 + 1$ F_q-rational places, i.e. places of degree one, and we compute the genus of F. In section III, we find a basis of the vector space associated to the place at infinity. This is used in section IV, where we construct a family of geometric Goppa codes. Furthermore, we prove, that the dual codes are in the same family.

II. The Function Field

Throughout the paper $\mathsf{F}_q(x_1)$ denotes the rational function field over the finite field F_q. In [4], Hansen and Stichtenoth considered the function field $\mathsf{F}_q(x_1, x_2)/\mathsf{F}_q$, defined by the absolutely irreducible polynomial

$$h(x_1, x_2) = x_2^q + x_2 + x_1^{q_0}(x_1^q + x_1) = 0,$$

where $q_0 = 2^n$ and $q = 2^{2n+1}$. This function field has $q^2 + 1$ F_q-rational places and genus $q_0(q - 1)$. Inspired by this, we define the following function field.

DEFINITION 1. *Let q be a prime power, and let q_0^2 be a divisor of q, $1 \leqq q_0 < \sqrt{q}$. Define the function field $F = \mathsf{F}_q(x_1, x_2)/\mathsf{F}_q$ by*

$$h(x_1, x_2) = x_2^q - x_2 - x_1^{q_0}(x_1^q - x_1) = 0. \tag{1}$$

THEOREM 1. *Let F be defined as in definition 1.*

(1) *F has q^2+1 F_q-rational places. Exactly one of the F_q-rational places is a place at infinity.*
(2) *$h(x_1,x_2)$ is absolutely irreducible, and F is an extension of $\mathsf{F}_q(x_1)$ of degree q, $[F:\mathsf{F}_q(x_1)]=q$.*
(3) *F has genus $g=q(q-1)/(2q_0)$.*

PROOF: (1) and (2) are proved in lemma 2, and (3) in lemma 3. □

LEMMA 2. *$[F:\mathsf{F}_q(x_1)]=q$, $h(x_1,x_2)$ is absolutely irreducible, and F has q^2+1 F_q-rational places, including exactly one place, P_∞, at infinity.*

PROOF: Let Q_∞ be the place at infinity of $\mathsf{F}_q(x_1)$, and let P_∞ be a place of F above Q_∞. ν_∞ is the discrete valuation at P_∞. From [5] and (1), we have

$$[F:\mathsf{F}_q(x_1)]=\sum_{P \text{ above } Q_\infty} e_P d_P \leqq q, \tag{2}$$

where e_P is the ramification index and d_P the relative degree of P above Q_∞. x_1^{-1} is a local parameter at Q_∞, implying that $\nu_\infty(x_1^{-1})=e_{P_\infty}\leqq q$. Now

$$\nu_\infty(x_1)=-e_{P_\infty}<0.$$

From $h(x_1,x_2)$ we get

$$\nu_\infty(x_2)=-\frac{e_{P_\infty}}{q}(q+q_0).$$

Define the functions

$$\begin{aligned} v &= x_2^{q/q_0}-x_1^{q/q_0+1} \\ w &= x_2^{q/q_0}x_1^{q/q_0^2-1}+v^{q/q_0}. \end{aligned} \tag{3}$$

By using (1), we obtain $v^{q_0}=x_2-x_1^{q_0+1}$ and $w^{q_0}=x_1^{q/q_0-q_0}x_2+v$, and by using the restriction on q_0 we get

$$\begin{aligned} \nu_\infty(v) &= -e_{P_\infty}\left(1+\frac{1}{q_0}\right) \\ \nu_\infty(w) &= -\frac{e_{P_\infty}}{q}\left(\frac{q^2}{q_0^2}-q+\frac{q}{q_0}+1\right). \end{aligned} \tag{4}$$

(4) implies $q|e_{P_\infty}$, which combined with (2) gives us $[F:\mathsf{F}_q(x_1)]=e_{P_\infty}=q$, and that P_∞ is the only place above Q_∞. Hence, $h(x_1,x_2)$ is absolutely irreducible.

Furthermore, since $e_{P_\infty}=q$, (2) implies $d_{P_\infty}=1$, and P_∞ is a F_q-rational place of F. Finally, for any fixed $x_1\in\mathsf{F}_q$, $h(x_1,x_2)$ has q different solutions of x_2 in F_q. Hence, above any F_q-rational place $Q\neq Q_\infty$ of $\mathsf{F}_q(x_1)$, there is q F_q-rational places of F. Thus, F has q^2+1 F_q-rational places. □

LEMMA 3. *F has genus $g = q(q-1)/(2q_0)$.*

PROOF: Let v and w be defined as in (3). From the proof of lemma 2, we have

$$\begin{aligned}
\nu_\infty(x_1) &= -q \\
\nu_\infty(x_2) &= -(q+q_0) \\
\nu_\infty(v) &= -\left(q + \frac{q}{q_0}\right) \\
\nu_\infty(w) &= -\left(\frac{q^2}{q_0^2} - q + \frac{q}{q_0} + 1\right).
\end{aligned}$$

Hence, a local parameter at P_∞ is

$$u = \frac{x_1^{q/q_0^2-2} v}{w}.$$

We use the Riemann-Hurwitz-Zeuthen formula [7],

$$2g - 2 = -2[F : \mathbf{F}_q(x_1)] + \deg R, \tag{5}$$

where R is the different of F, to compute the genus g. Let G be the group of automorphisms of F, which fixes $\mathbf{F}_q(x_1)$. Since $[F : \mathbf{F}_q(x_1)] = q$, the order of G is q. The elements of G are

$$\sigma \; : \quad \begin{cases} x_1 \mapsto x_1 \\ x_2 \mapsto x_2 + \alpha, \qquad \alpha \in \mathbf{F}_q \end{cases}$$

The higher ramification groups, G_i, is defined by

$$G_i = \{\sigma \in G \mid \nu_\infty(\sigma(u) - u) \geqq i+1\}.$$

By simple computations we get $\nu_\infty(\sigma(u) - u) = q/q_0 + 2$ for all $\sigma \in G$, $\sigma \neq 1$. Hence,

$$\begin{aligned}
|G_i| &= q, \qquad i = 0, 1, \ldots, q/q_0 + 1 \\
|G_i| &= 1, \qquad\qquad i \geqq q/q_0 + 2.
\end{aligned}$$

By [7], the degree of the different is

$$\deg R = \sum_{i=0}^{\infty} (|G_i| - 1) = (q-1)\left(\frac{q}{q_0} + 2\right). \tag{6}$$

Substituting (6) in (5) proves the lemma. □

The degree of the different could alternatively have been computed as $\nu_\infty\left(\frac{dt}{du}\right)$, where $t = x_1^{-1}$ is the local parameter at Q_∞ of $\mathbf{F}_q(x_1)$, and u is the local parameter at P_∞ of F [8]. We get

$$\frac{du}{dx_1} = -x_1^{q/q_0^2-2} \, \frac{x_1^{-1} vw + x_1^{-1} v^{q/q_0+1} + x_1^{q/q_0} w}{w^2},$$

and

$$\nu_\infty\left(\frac{du}{dx_1}\right) = -\left(2\,\frac{q(q-1)}{2q_0} - 2\right). \tag{7}$$

Since $\frac{dt}{dx_1} = -x_1^{-2}$ and $\frac{du}{dt} = -x_1^2 \frac{du}{dx_1}$, we get

$$\deg R = \nu_\infty\left(\frac{dt}{du}\right) = -\nu_\infty\left(\frac{du}{dt}\right) = (q-1)\left(\frac{q}{q_0} + 2\right),$$

as above in (6).

III. The Vector Space $L(mP_\infty)$

Let G be a divisor, and let $\mathrm{div}(f)$ denote the divisor of f. By definition

$$L(G) = \{f \in F \mid \mathrm{div}(f) \geqq -G\}.$$

$L(G)$ is a vector space over $\mathbf{F}_q$, and $\dim(L(G))$ denotes the dimension of $L(G)$ over $\mathbf{F}_q$.

Let P_∞ be the $\mathbf{F}_q$-rational place of F at infinity. In the following we are going to determine a basis for $L(mP_\infty)$ for any m, and thereby determine $\dim(L(mP_\infty))$.

Define the functions

$$\begin{aligned} f_0 &= 1 \\ f_q &= x_1 \\ f_{q+q_0} &= x_2 \\ f_{q+q/q_0} &= v \\ f_{q^2/q_0^2-q+q/q_0+1} &= w, \end{aligned} \tag{8}$$

where v and w are defined as in (3). By definition these functions are regular outside P_∞, and from the proof of lemma 3, we have

$$\nu_\infty(f_i) = -i, \qquad i \in \left\{0, q, q+q_0, q+\frac{q}{q_0}, \frac{q^2}{q_0^2} - q + \frac{q}{q_0} + 1\right\}.$$

Let $\mathcal{P}$ be the additive monoid, generated by the pole orders of the f_i's, i.e.

$$\mathcal{P} = \left\langle 0, q, q+q_0, q+\frac{q}{q_0}, \frac{q^2}{q_0^2} - q + \frac{q}{q_0} + 1 \right\rangle.$$

Let $j \in \mathcal{P}$. Then

$$j = a_1 q + a_2(q+q_0) + a_3\left(q + \frac{q}{q_0}\right) + a_4\left(\frac{q^2}{q_0^2} - q + \frac{q}{q_0} + 1\right),$$

where the a_i's are non-negative integers, i.e. $a_i \in \mathbf{N}_0$. Define the functions f_j by

$$f_j = f_q^{a_1} f_{q+q_0}^{a_2} f_{q+q/q_0}^{a_3} f_{q^2/q_0^2-q+q/q_0+1}^{a_4}. \tag{9}$$

We observe, that f_j is regular outside P_∞, and that $\nu_\infty(f_j) = -j$.

THEOREM 4.

$$|\mathbf{N}_0 \setminus \mathcal{P}| = \frac{q(q-1)}{2q_0} = g.$$

In order to prove theorem 4, we need lemma 5 and 6 below, and some notation, namely the additive monoids

$$\begin{aligned} \mathcal{H} &= \left\langle 0, q, q+q_0, q+\frac{q}{q_0} \right\rangle \\ \mathcal{U} &= \left\langle 0, \frac{q}{q_0}, \frac{q}{q_0}+1, \frac{q}{q_0}+\frac{q}{q_0^2} \right\rangle \\ \mathcal{U}' &= \left\langle 0, \frac{q}{q_0}, \frac{q}{q_0}+1 \right\rangle \end{aligned}$$

LEMMA 5. *Let $m \in \mathbb{N}_0$. There are uniquely determined integers c, s, such that*

$$m = cq_0 + s\left(\frac{q^2}{q_0^2} - q + \frac{q}{q_0} + 1\right), \qquad 0 \leqq s < q_0.$$

If m is represented in this form, then

$$m \notin \mathcal{P} \iff c \notin \mathcal{U}$$

PROOF: The unique representation of m is trivial, since $(q_0, q^2/q_0^2 - q + q/q_0 + 1) = 1$. Furthermore, it is easily seen, that $c \in \mathcal{U}$ implies $m \in \mathcal{P}$.
Assume $m \in \mathcal{P}$. Note, that m then can be written as

$$m = t_1 + t_2\left(\frac{q^2}{q_0^2} - q + \frac{q}{q_0} + 1\right), \qquad t_1 \in \mathcal{H}, \quad t_2 \geqq 0.$$

Put $t_2 = aq_0 + s$, where $a \geqq 0$ and $0 \leqq s < q_0$. Then

$$\begin{aligned} m - s\left(\frac{q^2}{q_0^2} - q + \frac{q}{q_0} + 1\right) &= t_1 + aq_0\left(\frac{q^2}{q_0^2} - q + \frac{q}{q_0} + 1\right) \\ &= t_1 + aq_0\left(\frac{q^2}{q_0^2} - q\right) + a(q + q_0) \\ &= t_1 + aq_0\left(\frac{q}{q_0^2} - 1\right)q + a(q + q_0) \in \mathcal{H} \end{aligned}$$

Since $\mathcal{H} = q_0\mathcal{U}$, we get

$$m - s\left(\frac{q^2}{q_0^2} - q + \frac{q}{q_0} + 1\right) = q_0 c, \qquad c \in \mathcal{U}. \ \square$$

LEMMA 6.

$$|\mathbb{N}_0 \setminus \mathcal{U}| = \frac{q}{2q_0^2}\left(q_0(q_0 - 1) + \frac{q}{q_0} - q_0\right).$$

PROOF: Let

$$\mathbb{N}_{i,j} = \left\{ i\frac{q}{q_0} + j\frac{q}{q_0^2}, \ldots, i\frac{q}{q_0} + (j+1)\frac{q}{q_0^2} - 1 \right\}.$$

Then

$$\mathbb{N}_0 = \bigcup_{j=0}^{q_0 - 1} \bigcup_{i=0}^{\infty} \mathbb{N}_{i,j},$$

and since $\mathbb{N}_{i_1,j_1} \cap \mathbb{N}_{i_2,j_2} = \emptyset$ for $(i_1, j_1) \neq (i_2, j_2)$ we get

$$|\mathbb{N}_0 \setminus \mathcal{U}| = \sum_{j=0}^{q_0 - 1} \sum_{i=0}^{\infty} |\mathbb{N}_{i,j} \setminus \mathcal{U}| = N_1 + N_2, \tag{10}$$

where

$$N_1 = \sum_{j=0}^{q_0-1} \sum_{i=j}^{\infty} |\mathsf{N}_{i,j} \setminus \mathcal{U}|$$

$$N_2 = \sum_{j=0}^{q_0-1} \sum_{i=0}^{j-1} |\mathsf{N}_{i,j} \setminus \mathcal{U}|.$$

Before we proceed, we observe that

$$\begin{aligned} \mathsf{N}_0 \setminus \mathcal{U}' &= \bigcup_{s=0}^{q/q_0-2} \left\{ s\frac{q}{q_0} + (s+1), \ldots, (s+1)\frac{q}{q_0} - 1 \right\} \\ &= \bigcup_{s=0}^{q/q_0-2} S_s, \end{aligned} \tag{11}$$

where $S_{s_1} \cap S_{s_2} = \emptyset$ if $s_1 \neq s_2$.
Assume $i \geqq j$. We have

$$\mathsf{N}_{i,j} = \left\{ j\left(\frac{q}{q_0} + \frac{q}{q_0^2}\right) + (i-j)\frac{q}{q_0}, \ldots, j\left(\frac{q}{q_0} + \frac{q}{q_0^2}\right) + (i-j)\frac{q}{q_0} + \frac{q}{q_0^2} - 1 \right\}.$$

Hence,

$$|\mathsf{N}_{i,j} \setminus \mathcal{U}| = \left| \left\{ (i-j)\frac{q}{q_0}, \ldots, (i-j)\frac{q}{q_0} + \frac{q}{q_0^2} - 1 \right\} \setminus \mathcal{U}' \right|.$$

By (11) we have, that $|\mathsf{N}_{i,j} \setminus \mathcal{U}| = 0$ if $i - j \geqq q/q_0^2 - 1$. We use (11) for $0 \leqq i - j \leqq q/q_0^2 - 2 \Longleftrightarrow j \leqq i \leqq q/q_0^2 + j - 2$, and get

$$\begin{aligned} |\mathsf{N}_{i,j} \setminus \mathcal{U}| &= \left| \left\{ (i-j)\frac{q}{q_0} + (i-j+1), \ldots, (i-j)\frac{q}{q_0} + \frac{q}{q_0^2} - 1 \right\} \right| \\ &= \frac{q}{q_0^2} - (i-j+1), \qquad j \leqq i \leqq \frac{q}{q_0^2} + j - 2. \end{aligned}$$

Thus,

$$N_1 = \sum_{j=0}^{q_0-1} \sum_{i=j}^{q/q_0^2+j-2} \left(\frac{q}{q_0^2} - i + j - 1 \right) = \frac{q}{2q_0^2}\left(\frac{q}{q_0} - q_0 \right). \tag{12}$$

Assume $i < j < q_0$. We have

$$\mathsf{N}_{i,j} = \left\{ i\left(\frac{q}{q_0} + \frac{q}{q_0^2}\right) + (j-i)\frac{q}{q_0^2}, \ldots, i\left(\frac{q}{q_0} + \frac{q}{q_0^2}\right) + (j-i+1)\frac{q}{q_0^2} - 1 \right\}.$$

Hence,

$$|\mathsf{N}_{i,j} \setminus \mathcal{U}| = \left| \left\{ (j-i)\frac{q}{q_0^2}, \ldots, (j-i+1)\frac{q}{q_0^2} - 1 \right\} \setminus \mathcal{U}' \right|.$$

Again we use (11) by observing that

$$\left\{ (j-i)\frac{q}{q_0^2}, \ldots, (i-j+1)\frac{q}{q_0^2} - 1 \right\} \subset S_0,$$

for all legal values of i and j. Thus,

$$|\mathbb{N}_{i,j} \setminus \mathcal{U}| = \frac{q}{q_0^2}, \qquad i < j < q_0,$$

and we get

$$N_2 = \sum_{j=0}^{q_0-1} \sum_{i=0}^{j-1} \frac{q}{q_0^2} = \frac{q}{2q_0}(q_0 - 1). \tag{13}$$

Substituting (12) and (13) in (10) proves the lemma. □

PROOF OF THEOREM 4: Let $m \in \mathbb{N}_0$. From lemma 5 we have, that m can be uniquely represented as

$$m = cq_0 + s\left(\frac{q^2}{q_0^2} - q + \frac{q}{q_0} + 1\right), \qquad 0 \leqq s < q_0.$$

Assume $c \geqq 0$. By lemma 5 $m \notin \mathcal{P} \iff c \notin \mathcal{U}$. From lemma 6 we know, that c can be chosen among $\frac{q}{2q_0^2}(q_0(q_0-1) + q/q_0 - q_0)$ elements. Therefore q_0 possible choices of s produces

$$\frac{q}{2q_0}\left(q_0(q_0-1) + \frac{q}{q_0} - q_0\right) \tag{14}$$

elements $m \notin \mathcal{P}$.
Assume $c < 0$. Note that

$$1 \leqq m = cq_0 + s\left(\frac{q^2}{q_0^2} - q + \frac{q}{q_0} + 1\right)$$

$$\Downarrow$$

$$1 \leqq s \leqq q_0 - 1.$$

Let $s \in \{1, 2, \ldots, q_0 - 1\}$. Then

$$1 \leqq m = cq_0 + s\left(\frac{q^2}{q_0^2} - q + \frac{q}{q_0} + 1\right)$$

$$\Downarrow$$

$$-sq_0\left(\frac{q^2}{q_0^3} - \frac{q}{q_0} + \frac{q}{q_0^2}\right) \leqq cq_0 + (s-1)$$

$$\Downarrow$$

$$-s\left(\frac{q^2}{q_0^3} - \frac{q}{q_0} + \frac{q}{q_0^2}\right) \leqq c.$$

Conversely,

$$-s\left(\frac{q^2}{q_0^3} - \frac{q}{q_0} + \frac{q}{q_0^2}\right) \leqq c < 0$$

$$\Downarrow$$

$$0 \leqq cq_0 + s\left(\frac{q^2}{q_0^2} - q + \frac{q}{q_0}\right).$$

Hence, for any $s \in \{1, 2, \ldots, q_0 - 1\}$, there are precisely $s\left(\frac{q^2}{q_0^3} - \frac{q}{q_0} + \frac{q}{q_0^2}\right)$ elements $m \notin \mathcal{P}$ with $c < 0$. Thus, in this case we obtain

$$\sum_{s=1}^{q_0-1} s\left(\frac{q^2}{q_0^3} - \frac{q}{q_0} + \frac{q}{q_0^2}\right) = \frac{q_0(q_0-1)}{2}\left(\frac{q^2}{q_0^3} - \frac{q}{q_0} + \frac{q}{q_0^2}\right) \tag{15}$$

elements $m \notin \mathcal{P}$.
Adding (14) and (15) proves the theorem. □

For any $\mathbf{F}_q$-rational place P of a function field of genus g, there are exactly g numbers, $0 < m_1 < \cdots < m_g < 2g$, such that $L(m_i P) = L((m_i - 1)P)$. These m_i's are called the Weierstrass gaps at P [9]. For any $j \in \mathbf{N}_0$, which is not a Weierstrass gap, there exists a function f in the function field, which is regular outside P and with $-\nu_P(f) = j$. Now, let $y_{i_0}, y_{i_1}, \ldots$ be an infinite series of functions, where y_{i_j} has no poles outside P, $-\nu_P(y_{i_j}) = i_j$, $i_{j-1} < i_j$, and let

$$U_P = \{i_j \mid j = 0, 1, \ldots\}. \tag{16}$$

The y_{i_j}'s are linearly independent, since their pole orders are mutually different. Then, if

$$|\mathbf{N}_0 \setminus U_P| = g, \tag{17}$$

we have that

$$\{y_{i_j} \mid i_j \in U_P, i_j \leqq m\}$$

is a basis for $L(mP)$. We use this in the proof of theorem 7, where we find a basis for $L(mP_\infty)$.

THEOREM 7. *Let f_j be defined as in (9), $j \in \mathcal{P}$. Then $L(mP_\infty)$ has as basis the elements in the set*

$$B_m = \{f_j \mid j \in \mathcal{P},\ j \leqq m\}.$$

PROOF: The theorem is trivially true for $m \leqq 0$, so we assume $m > 0$. Observe that the f_j's form a series as above. As in (16), $\mathcal{P}$ is the set of pole orders at P_∞ of the f_j's. By theorem 4, we have that $|\mathbf{N}_0 \setminus \mathcal{P}| = g$. The condition in (17) is satiesfied, and the theorem is thereby proved. □

COROLLARY 8. *The Weierstrass gaps of the $\mathbf{F}_q$-rational place P_∞ of F, are the elements of the set $\mathbf{N}_0 \setminus \mathcal{P}$.*

IV. The Codes

Let $P_1, \ldots, P_n$ be $\mathbf{F}_q$-rational places of a function field. Define the divisor $D = P_1 + \cdots + P_n$, and choose the divisor G, such that the supports of D and G are disjoint. Then the geometric Goppa code $C_L(D, G)$, associated with D and G (cf. [1], [2]), is the image of the $\mathbf{F}_q$-linear map ϕ, given by

$$\begin{aligned} \phi: \quad & L(G) \to \mathbf{F}_q^n \\ & f \mapsto \big(f(P_1), \ldots, f(P_n)\big). \end{aligned}$$

$C_L(D, G)$ is a linear $[n, k, d]$ code over $\mathbf{F}_q$, where n denotes the length, k the dimension and d the minimum distance.

THEOREM 9. *Let F be the function field defined in definition 1. Let P_∞ be the $\mathbf{F}_q$-rational place at infinity, and let $P_1, \ldots, P_{q^2}$ be the rest of the $\mathbf{F}_q$-rational places of F. Define $D = P_1 + \cdots + P_{q^2}$ and $G = mP_\infty$, $m \geqq 0$. Let $\mathcal{C}_m$ be the geometric Goppa code $C_L(D, G)$. Then $\mathcal{C}_m$ is a linear $[n, k, d]$ code over $\mathbf{F}_q$ with $n = q^2$. If $m < q^2$, then*

$$k = |\{j \in \mathcal{P} \mid j \leqq m\}|$$
$$d \geqq q^2 - m.$$

Furthermore, if $q(q-1)/q_0 - 2 < m < q^2$, then

$$k = m + 1 - \frac{q(q-1)}{2q_0}.$$

PROOF: n is trivial, and k was determined in theorem 7. ϕ is injective for $m < q^2$, and since $\deg(\mathrm{div}(f)) = 0$, any $f \in L(G)$ is zero in at most m $\mathbf{F}_q$-rational places. Hence, a codeword has weight at least $q^2 - m$. □

Any code $\mathcal{C}_m$ of theorem 9 is easily constructed. In theorem 7, we found a basis B_m for $\mathcal{C}_m$, and therefore, the codewords, corresponding to the elements of B_m, form a generator matrix of $\mathcal{C}_m$.

It is well-known, that the dual code of a geometric Goppa code also is a geometric Goppa code [2]. Moreover, it can be shown [6], that if ω is a differential, such that

$$\nu_{P_i}(\omega) = -1 \text{ and } \mathrm{res}_{P_i}(\omega) = 1 \text{ for all } P_i \in \mathrm{supp}\ D, \tag{18}$$

then

$$C_L(D, D - G + \mathrm{div}(\omega))^\perp = C_L(D, G),$$

where $\mathcal{C}^\perp$ denotes the dual code of $\mathcal{C}$.

THEOREM 10. *(Notation as in theorem 9).*

$$\mathcal{C}_m^\perp = \mathcal{C}_{q^2+2g-2-m}.$$

PROOF: Let ω be the differential

$$\omega = \frac{dx_1}{x_1 - x_1^q}.$$

Since x_1 only has poles at P_∞, we have from the proof of lemma 2,

$$\mathrm{div}(x_1 - x_1^q) = \sum_{i=1}^{q^2} P_i - q^2 P_\infty = D - q^2 P_\infty.$$

From (7), we have

$$\nu_\infty(dx_1) = \nu_\infty\left(\frac{dx_1}{du} du\right) = 2g - 2.$$

Furthermore, $\nu_{P_i}(dx_1) = 0$ for all $P_i \neq P_\infty$, since P_i is unramified. Alltogether we get

$$\mathrm{div}(\omega) = (2g - 2 + q^2)P_\infty - D.$$

As noted above, $P_i \neq P_\infty$ is unramified, implying that $x_1 - \alpha$ is a local parameter at P_i for some $\alpha \in \mathbf{F}_q$. Hence,

$$\begin{aligned}\mathrm{res}_{P_i}(\omega) &= \mathrm{res}_{P_i}\left(\frac{dx_1}{x_1 - x_1^q}\right) \\ &= \mathrm{res}_{P_i}\left(\left(-\prod_{\beta \neq \alpha}(\alpha - \beta)^{-1}\right)\frac{1}{x_1 - \alpha}\, d(x_1 - \alpha)\right) \\ &= 1.\end{aligned}$$

ω satiesfies the conditions of (18), and the theorem is proved. □

COROLLARY 11. *If $\mathbf{F}_q$ is of characteristic 2, then $\mathcal{C}_m$ is self-dual, if and only if $m = q^2/2 + g - 1$. If $\mathbf{F}_q$ is of odd characteristic, $\mathcal{C}_m$ cannot be self-dual.*

V. Discussion

We have defined a function field with $q^2 + 1$ $\mathbf{F}_q$-rational places. The definition of the function field, the results and the proofs, is inspired by the work of Hansen and Stichtenoth [4]. However, in [4] it is proved, that the function field F with $q_0 = 2^n$, $q = 2^{2n+1}$ and genus $g = q_0(q-1)$, has as many $\mathbf{F}_q$-rational places as possible for a function field of this genus. This was proved by using a bound of Serre [10]. In the extended case, as we have studied in this paper, it has not been possible to apply this bound.

References

1. V. D. Goppa, *Codes on Algebraic Curves*, Soviet Math. Dokl. **24** (1981), 170–172.
2. V. D. Goppa, *Algebraico-geometric Codes*, Math. U.S.S.R. Izvestiya **21** (1983), 75–91.
3. V. D. Goppa, "Geometry and Codes," Kluwer Academic Publishers, Dordrecht Boston London, 1988.
4. J. P. Hansen and H. Stichtenoth, *Group Codes on Certain Algebraic Curves with many Rational Points*, AAECC (1990) (to appear).
5. C. Chevalley, "Introducion to the Theory of Algebraic Functions of one Variable," American Mathematical Society, New York, 1951.
6. H. Stichtenoth, *Self-dual Goppa Codes*, J. Pure Appl. Algebra **55** (1988), 199–211.
7. J. P. Serre, "Corps Locaux," Hermann, Paris, 1962.
8. R. Hartshorne, "Algebraic Geometry," Springer-Verlag, New York Heidelberg Berlin, 1977.
9. W. Fulton, "Algebraic Curves," Benjamin Cummings, Reading, 1969.
10. J. P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Série I **296** (1983), 397–402.

MAT-REPORT NO. 1990-11
ISSN 0904-7611

5 Weighted Reed-Muller codes

Revised version of [Sø91a].

Weighted Reed-Muller Codes

Anders Bjært Sørensen

-

Abstract

A generalization of the Reed-Muller codes, the weighted Reed-Muller codes, is presented. The codeparameters are estimated and the duals are shown to be weighted Reed-Muller codes, too. It is shown how the minimum distance of certain algebraic geometry codes in many cases can be determined exactly or an upper bound can be found, using subcodes which are weighted Reed-Muller codes.

Keywords: Error-correcting codes, Reed-Muller codes, finite projective geometry, algebraic geometry codes.

1 Introduction

The socalled generalized Reed-Muller codes were introduced by Kasami, Lin and Peterson [1,3] and Weldon [2] about 1970. The multivariable approach [4] and the introduction of algebraic geometry codes in the eighties inspired Lachaud [5] to introduce the projective Reed-Muller codes. Their parameters and cyclic structure were determined in [6] by the author. In this paper, we generalize some of the results of [6] by the presentation of socalled weighted Reed-Muller codes.

In section 2, we define the affine and projective version of the weighted Reed-Muller codes, the WARM-codes and WPRM-codes, and we determine their code parameters (for the minimum distance in the projective case we give only an estimate). In section 3, we show that the dual of an WARM-code is again a WARM-code and that the dual of a WPRM-code is almost a WPRM-code. In section 4, we show that a certain class of algebraic geometry codes is in fact WARM-codes, and as an example we show that the curve used by Pellikaan et.al. in [7] as a basis to prove that all linear codes are weakly algebraic geometric, gives codes which are WARM-codes. Hence, the minimum distance of these codes are determined. Furthermore, we study the Hansen-Stichtenoth codes [10, 11] and we give an upper bound of the minimum distance using maximal WARM-subcodes.

2 Weighted affine and projective Reed-Muller codes

2.1 The definition

Let $\mathbf{F}_q$ be the finite field with q elements, q a prime power. By $\mathbf{A}^m(\mathbf{F}_q)$ resp. $\mathbf{P}^m(\mathbf{F}_q)$ we mean the m-dimensional affine resp. projective space defined over $\mathbf{F}_q$. We will often just write $\mathbf{A}^m$ and $\mathbf{P}^m$. $\mathbf{F}_q[X_1, \ldots, X_m]$ is the ring of polynomials in m variables with coefficients in $\mathbf{F}_q$. If we attach to each variable X_i a natural number w_i, called the *weight* of X_i, we speak about the ring of weighted polynomials, $W\mathbf{F}_q[X_1, \ldots, X_m]$. If all weights are 1 (trivial weights), we have just the usual polynomial ring. The weighted degree of $F \in W\mathbf{F}_q[X_1, \ldots, X_m]$, is defined as $deg_w(F) = deg_w(F(X_1, \ldots, X_m)) = deg(F(X_1^{w_1}, \ldots, X_m^{w_m})$, where deg is the usual degree. We will without loss of generality always assume that the weights are ordered $w_1 \leq w_2 \leq \cdots \leq w_m$.

The general set-up in the affine case is the following: Consider the evaluation map

$$\phi : W\mathbf{F}_q[X_1, \ldots, X_m] \rightarrow (\mathbf{F}_q)^{q^m}$$

given by

$$\phi(F) = (\ldots, F(P_i), \ldots),$$

where P_i runs through $\mathbf{A}^m(\mathbf{F}_q)$.

The W is actually not needed in this definition, since we don't use the weights. We will in the following therefore sometimes omit it.

The definition of the affine Reed-Muller code, (also called the generalized Reed-Muller code in the litterature) $ARM(\nu, m, q)$, of order ν and length q^m is now:

$$ARM(\nu, m, q) = \phi(V(\nu)),$$

where

$$V(\nu) = \{F \in \mathbf{F}_q[X_1, \ldots, X_m] \mid deg(F) \leq \nu\},$$

where $1 \leq \nu \leq m(q-1)$.

Definiton 1 Given natural number ω and weights $\{w_i\}_{i=1}^m$ corresponding to the ring of weighted polynomials $W\mathbf{F}_q[X_1, \ldots, X_m]$.

The *Weighted Affine Reed-Muller Code, $WARM(\omega, m, q)$* of weighted order ω, and length q^m, corresponding to the weights $\{w_i\}_{i=1}^m$, is defined as

$$WARM(\omega, m, q) = \phi(V_w(\omega)),$$

where

$$V_w(\omega) = \{F \in W\mathbf{F}_q[X_1, \ldots, X_m] \mid deg_w(F) \leq \omega\}.$$

The set-up in the projective case is the following: Consider the evaluation map

$$\psi : W\mathbf{F}_q[X_0, \ldots, X_m] \rightarrow (\mathbf{F}_q)^n$$

given by

$$\psi(F) = (\ldots, F(P_i), \ldots),$$

where $\{P_i\}$ is an arbitrary, but fixed, set of representatives of the points in $\mathbf{P}^m(\mathbf{F}_q)$ and $n = (q^{m+1} - 1)/(q - 1)$.

Like before we will omit the W, when suitable.

The definition of the projective Reed-Muller code $PRM(\nu, m, q)$ of order ν and length n is:

$$PRM(\nu, m, q) = \psi(U(\nu))$$

where

$$U(\nu) = \{F \in \mathbf{F}_q[X_0, \ldots, X_m] \mid deg(F) = \nu,\ F \text{ homogeneous}\} \cup \{0\},$$

where $1 \leq \nu \leq m(q - 1)$.

Definiton 2 Given natural numbers ω, s and weights $\{w_i\}_{i=0}^m$ corresponding to the ring of weighted polynomials $W\mathbf{F}_q[X_0, \ldots, X_m]$. Let $0 \leq \omega \leq (q-1)\sum_{i=0}^m w_i, 0 < s < q$.

The *Weighted Projective Reed-Muller Code*, $WPRM(\omega, s, m, q)$ of weighted order ω, normal order equivalent to s mod $(q - 1)$ and length $(q^m - 1)/(q - 1)$, corresponding to the weights $\{w_i\}_{i=0}^m$, is defined as

$$WPRM(\omega, \nu, m, q) = \psi(U_w(\omega)),$$

where

$$U_w(\omega) = \{F \in W\mathbf{F}_q[X_0, \ldots, X_m] \mid deg_w(F) \leq \omega, deg(F) \equiv s \bmod (q-1)\} \cup \{0\},$$

2.2 The codeparameters

First some convenient notation and some useful lemmas.

For a polynomial F in $\mathbf{F}_q[X_1, \ldots, X_m]$, we will by $\overline{F}$ denote the reduced form of F. That is the polynomial of lowest degree equivalent to F modulo the ideal $(X_i^q - X_i, i = 1, \ldots, m)$. For any subset M of $\mathbf{F}_q[X_1, \ldots, X_m]$, the set $\overline{M}$ denotes the set of reduced elements of M.

Lemma 3 *For $F \in \mathbf{F}_q[X_1, \ldots, X_m]$ and $G \in \mathbf{F}_q[X_0, \ldots, X_m]$, G homogeneous, we have*

1. $\forall P \in \mathbf{A}^m : F(P) = \overline{F}(P)$.
2. $\forall P \in \mathbf{P}^m : G(P) = \overline{G}(P)$.
3. *If* $F(P) = 0, \forall P \in \mathbf{A}^m$ *then* $\overline{F} = 0$
4. *If* $G(P) = 0, \forall P \in \mathbf{P}^m$ *then* $\overline{G} = 0$

Proof: 1. and 2. is obvious. 3. is proved in [8] and 4. follows from 3.

Lemma 4 *Consider the evaluation maps ϕ resp. ψ defined in the previous section and their restriction to some $\mathbf{F}_q$-linear subspace V resp. U*

$$\phi : W\mathbf{F}_q[X_1, \ldots, X_m] \supseteq V \rightarrow (\mathbf{F}_q)^{q^m}$$

$$\psi : W\mathbf{F}_q[X_0, \ldots, X_m] \supseteq U \rightarrow (\mathbf{F}_q)^{n}$$

where $n = (q^{m+1} - 1)/(q - 1)$.

Then

1. *$ker(\phi) = \{F \in V \,|\, \overline{F} = 0\}$.*
2. *$ker(\psi) = \{G \in U \,|\, \overline{G} = 0\}$.*
3. *$\phi_{|\overline{V}}$ is injective, $\phi(V) = \phi(\overline{V})$ and $V/ker(\phi) \simeq \overline{V}$.*
4. *$\psi_{|\overline{U}}$ is injective, $\psi(U) = \psi(\overline{U})$ and $U/ker(\psi) \simeq \overline{U}$.*

Proof: Easy consequences of Lemma 3.

Definiton 5 Given a natural numbers ω, ν and a set of weights $\{w_i\}_{i=\epsilon}^{m}$ (ordered), such that $1 \leq \nu \leq m(q-1)$ and $1 \leq \omega \leq (q-1)\sum_{i=\epsilon}^{m} w_i$. Here, $\epsilon = 1$ in the affine case and $\epsilon = 0$ in the projective case.

We define for a fixed weighted degree ω the interesting interval of normal degrees. Let

$$\nu_{max}(\omega) = Q_\epsilon(q-1) + R_\epsilon,$$

where

$$Q_\epsilon = max\{Q \,|\, \omega \geq \sum_{i=\epsilon}^{Q-1+\epsilon} (q-1)w_i\}$$

and

$$R_\epsilon = max\{R \,|\, \omega \geq \sum_{i=\epsilon}^{Q_\epsilon-1+\epsilon} (q-1)w_i + Rw_{Q_\epsilon+\epsilon}\}.$$

Furthermore, let

$$\nu_{min}(\omega) = Q'(q-1) + R',$$

where

$$Q' = max\{Q \,|\, \omega \geq \sum_{i=m-Q+1}^{m} (q-1)w_i\}$$

and

$$R' = max\{R \,|\, \omega \geq \sum_{i=m-Q'+1}^{m} (q-1)w_i + Rw_{m-Q'}\}.$$

Next, we define for a fixed normal degree ν the interesting interval of weighted degrees. Let

$$\omega_{max}(\nu) = \sum_{i=m-Q+1}^{m} (q-1)w_i + Rw_{m-Q},$$

and

$$\omega_{min}(\nu) = \sum_{i=\epsilon}^{Q-1+\epsilon} (q-1)w_i + (R+1)w_{Q+\epsilon} - 1,$$

where $\nu = Q(q-1) + R, 0 \leq R < q,$

Lemma 6 We observe that

1. $\nu_{max}(\omega)$ *is the maximal normal degree of a reduced polynomial of weighted degree less than or equal to* ω.
2. $\nu_{min}(\omega)$ *is the maximal normal degree such that all reduced polynomials of normal degree less than are equal this degree, has weighted degree less than or equal* ω.
3. $\omega_{max}(\nu)$ *is the maximal weighted degree of a reduced polynomial of normal degree less than or equal* ν.
4. $\omega_{min}(\nu)$ *is the maximal weighted degree such that all reduced polynomials of weighted degree less than are equal this degree, has normal degree less than or equal* ν.

The defined numbers has the following charateristic properties

5. $\nu_{max}(\omega) = min\{\nu \,|\, \omega \leq \omega_{min}(\nu)\}$
6. $\nu_{min}(\omega) = max\{\nu \,|\, \omega \geq \omega_{max}(\nu)\}$
7. $\omega_{max}(\nu) = min\{\omega \,|\, \nu \leq \nu_{min}(\omega)\}$
8. $\omega_{min}(\nu) = max\{\omega \,|\, \nu \geq \nu_{max}(\omega)\}$
9. $\omega \geq \omega_{max}(\nu) \Leftrightarrow \nu \leq \nu_{min}(\omega)$
10. $\omega \leq \omega_{min}(\nu) \Leftrightarrow \nu \geq \nu_{max}(\omega)$

Proof: For a given weighted degree ω, the corresponding normal degres $\nu_{min}(\omega)$ and $\nu_{max}(\omega)$ are found simply by constructing a monomial of lowest resp. highest possible normal degree, which has weighted degree less than or equal ω.

Since the weighted degrees are ordered ($\leq$) these monomials are on the form

$$X_{m-Q'}^{R'} \prod_{i=m-Q'+1}^{m} X_i^{q-1}, \text{and}$$

$$X_{Q_\epsilon+\epsilon}^{R_\epsilon} \prod_{i=\epsilon}^{Q_\epsilon-1+\epsilon} X_i^{q-1},$$

where $Q', Q_\epsilon, R', R_\epsilon$ are defined in definition 5.

For a given normal degree ν, the weighted degrees $\omega_{min}(\nu)$ and $\omega_{max}(\nu)$ are found by building monomials from top resp. from botton of normal degree ν. Remark that $\omega_{min}(\nu)$ is not just the weighted degree of the polynomial of degree ν constructed from the botton, but this weighted degree plus $w_{Q+\epsilon} - 1$.

Now statements 1.-4. is clear. Using the picture of filling in from top or bottom easily establishes the following

$$\omega < \omega_{max}(\nu) \Leftrightarrow \nu > \nu_{min}(\omega)$$
$$\omega > \omega_{min}(\nu) \Leftrightarrow \nu < \nu_{max}(\omega)$$

From this follows 5.-10..

Lemma 7 *Notation as above. Then the following holds*

1. $WARM(\omega_{min}(\nu), m, q) \subseteq ARM(\nu, m, q) \subseteq WARM(\omega_{max}(\nu), m, q)$
2. $ARM(\nu_{min}(\omega), m, q) \subseteq WARM(\omega, m, q) \subseteq ARM(\nu_{max}(\omega), m, q)$
3. $WPRM(\omega_{min}(\nu), \nu \bmod (q-1), m, q) \subseteq PRM(\nu, m, q) \subseteq WPRM(\omega_{max}(\nu), \nu \bmod (q-1), m, q)$
4. $PRM(\nu_{min}(\omega) - T', m, q) \subseteq WPRM(\omega, s, m, q) \subseteq PRM(\nu_{max}(\omega) - T, m, q)$

where $T = (R_0 - s) \bmod (q-1)$ *and* $T' = (R' - s) \bmod (q-1)$.

Proof: Use the interpretation given in lemma 6, 1. to 4. and 1. to 3. follows immediately. In 4. one has to be careful that the normal degree is equivalent to s modulo $(q-1)$.

It is well-known (see [1,4]) that the $ARM(\nu, m, q)$-code is a $[q^m, k, d]$-code with

$$k = |\{(e_1, \ldots, e_m) | \sum_{i=1}^{m} e_i \leq \nu, 0 \leq e_i \leq q-1, e_i \in \mathbf{N_0}\}|$$

and

$$d = (q-R)q^{m-Q-1},$$

where $\nu = Q(q-1) + R, 0 \leq R < q-1, 0 \leq Q \leq m-1$.

Somewhat similar holds for the $WARM(\omega, m, q)$-code:

Theorem 8 *Given a natural number* ω *and a corresponding set of (ordered) weights* $\{w_i\}_{i=1}^m$, *such that* $\omega \leq (q-1)\sum_{i=1}^m w_i$. *The* $WARM(\omega, m, q)$*-code is a* $\mathbf{F}_q$*-linear* $[q^m, k, d]$ *code with*

$$k = |\{(e_1, \ldots, e_m) | \sum_{i=1}^{m} w_i e_i \leq \omega, 0 \leq e_i < q, e_i \in \mathbf{N_0}\}|$$

and

$$d = q^{m-Q-1}(q-R),$$

where Q *and* R *is given by* $\nu_{max}(\omega) = Q(q-1) + R, 0 \leq R < (q-1)$.

Proof: From lemma 4, it is clear that we only have to study $\overline{V(\omega)}$. The following set of monomials

$$\{\prod_{i=1}^{m} X_i^{e_i} \mid \sum_{i=1}^{m} w_i e_i \leq \omega, 0 \leq e_i < q\}$$

is a basis of $\overline{V(\omega)}$ and the expression for the dimension then follows immediately.

Consider the polynomial

$$G = \prod_{\beta \neq \lambda_1} (X_1 - \beta) \prod_{\beta \neq \lambda_2} (X_2 - \beta) \cdots \prod_{\beta \neq \lambda_Q} (X_Q - \beta) \prod_{\beta \in \Lambda} (X_{Q+1} - \beta),$$

where $\lambda_i \in \mathbf{F}_q, \Lambda = \{\mu_1, \ldots, \mu_R\}, \mu_i \in \mathbf{F}_q$ all distinct.

G is a polynomial in $\overline{V(\omega)}$ of highest possible normal degree. Furthermore G is zero at all points of $\mathbf{A}^m(\mathbf{F}_q)$, except in points on the form

$$(\lambda_1, \ldots, \lambda_Q, \mu, z_{Q+2}, \ldots, z_m)$$

where $\lambda_i \in \mathbf{F}_q, \mu \notin \Lambda$, and z_j chosen free in $\mathbf{F}_q$. There is exactly $q^{m-Q-1}(q-R)$ such non-zeros and therefore, we get an upper bound on the minimum distance

$$d \leq q^{m-Q-1}(q-R)$$

From the multivariable description of affine Reed-Muller codes (see [4],[6]) it is known that at a polynomial of degree $(q-1)Q + R$ can have at most $q^m - q^{m-Q-1}(q-R)$ zeros and equality follows.

Remark 9 Notice that the proof above together with Lemma 7 (*2.*) immediately gives that the parameters of the $WARM(\omega, m, q)$-code is worse than those of the $ARM(\nu_{max}(\omega), m, q$ code, since the minium distances are equal, but the dimension of $WARM(\omega, m, q)$-code are less than that of $ARM(\nu_{max}(\omega), m, q)$.

In other words, the optimal weights are the trivial ones.

In [6], it is shown that the $PRM(\nu, m, q)$-code is a $[n, k, d]$-code with

$$k = |\{(e_1, \ldots, e_m) | \sum_{i=1}^{m} e_i \equiv \nu \bmod (q-1), 0 \leq e_i \leq q-1\}|$$

and

$$n = \frac{q^{m+1}-1}{q-1} \text{ and } d = (q-R')q^{m-Q'-1},$$

where $\nu - 1 = Q'(q-1) + R', 0 \leq R' < q-1, 0 \leq Q' \leq m-1$.

For the $WPRM(\omega, s, m, q)$-code, we have:

Theorem 10 *Given natural numbers ω, s and a set of (ordered) weights $\{w_i\}$, such that $1 \leq \omega \leq (q-1)\sum_{i=1}^{m} w_i, 0 < s < q$. Define*

$$Q^* = max\{Q \mid \omega \geq (q-1)\sum_{i=0}^{Q-1} w_i + w_Q + (s-1)w_{Q+1}\},$$

$$Q^{**} = max\{Q \mid \omega \geq (q-1)\sum_{i=0}^{Q-1} w_i + sw_Q\}.$$

The $WPRM(\omega, s, m, q)$-code is a $\mathbf{F}_q$-linear $[n, k, d]$ code with

$$k = |\{(e_0, \ldots, e_m) \mid \sum_{i=0}^{m} w_i e_i \leq \omega, \sum_{i=0}^{m} e_i \equiv \nu \bmod (q-1), 0 \leq e_i < q\}|$$

and

$$n = \frac{q^{m+1}-1}{q-1} \text{ and } q^{m-Q^{**}-1}(q-s+1) < d \leq q^{m-Q^{*}-1}(q-s+1).$$

Proof: From lemma 4 it is clear that we only have to study $\overline{U_w(\omega)}$. The following set of monomials

$$\{\prod_{i=0}^{m} X_i^{e_i} | \sum_{i=0}^{m} w_i e_i \leq \omega, \sum_{i=0}^{m} e_i \equiv s \bmod (q-1), 0 \leq e_i < q\}$$

is a basis for $\overline{U_w(\omega)}$. The expression for the dimension then follows immediately.

Consider the polynomial

$$G = X_{Q^*} \prod_{i=0}^{Q^*-1} (X_i^{q-1} - X_{Q^*+1}^{q-1}) \prod_{j=1}^{s-1} (\lambda_j X_{Q^*} - X_{Q^*+1})$$

where $\lambda_j \in \mathbf{F}_q$, are distinct. Since

$$deg_w(\overline{G}) = \sum_{i=0}^{Q^*-1} (q-1)w_i + w_{Q^*} + (s-1)w_{Q^*+1}$$

by definition of Q^*, we have $\overline{G} \in \overline{U_w(\omega)}$. G is zero at all points of $\mathbf{P}^m(\mathbf{F}_q)$, except in points on the form

$$(0 : \cdots : 0 : 1 : \lambda : z_{Q^*+2} : \cdots : z_m),$$

$\lambda \neq \lambda_j, j = 1, \ldots, s-1$ and z_j chosen freely in $\mathbf{F}_q$. There is exactly $q^{m-Q^*-1}(q-s+1)$ such non-zeros and we therefore get an upper bound on the minimum distance

$$d \leq q^{m-Q^*-1}(q-s+1)$$

From the rojective Reed-Muller codes (see [6]), it is known that a reduced polynomial of degree $(q-1)r+s+1$ can have at most $(q^{m+1}-1)/(q-1) - q^{m-r-1}(q-s)$ zeros. Now $\overline{G}$ is not necessarily a polynomial in $\overline{U_w(\omega)}$ of highest possible normal degree equivalent to s modulo $(q-1)$, so we are at the moment only able to give a lower bound by replacing Q^* with Q^{**}.

Remark 11 As in the affine case we immediately from Lemma 7 (*4.*) conclude that the optimal weights for $WPRM$-codes are the trivial ones. That means that also here no good new codes are produced.

3 The dual of weighted Reed-Muller codes

In this section, we will show that the dual of a *WARM*-code is again a *WARM*-code and that this almost hold for *WPRM*-codes, too. We recall from [6] that the same situation happened for *PRM*-codes. For *ARM*-codes this have been know since for a long time (see [4]).

Definiton 12 Let

$$d(\nu, m, q) = \mid \{(e_1, \ldots, e_m) | 0 \leq e_i < q, \sum_{i=1}^{m} e_i = \nu\} \mid$$

$$d_w(\omega, m, q) = |\{(e_1, \ldots, e_m) \mid \sum_{i=1}^{m} e_i w_i = \omega, 0 \leq e_i < q\}|,$$

$$d_w(\omega, s, m, q) = |\{(e_0, \ldots, e_m) \mid \sum_{i=0}^{m} e_i w_i = \omega, \sum_{i=0}^{m} e_i \equiv s \bmod (q-1), 0 \leq e_i < q\}|,$$

$$\omega_{M,\epsilon} = (q-1)\sum_{i=\epsilon}^{m} w_i, \nu_{M,\epsilon} = (m+1-\epsilon)(q-1).$$

Lemma 13 *The following holds*

1. $d(\nu, m, q) = d(\nu_{M,1} - \nu, m, q),.$
2. $d_w(\omega, m, q) = d_w(\omega_{M,1} - \omega, m, q).$
3. $d_w(\omega, s, m, q) = d_w(\omega_{M,0} - \omega, q-1-s, m, q).$
4. $q^m = \sum_{0 \leq x \leq \nu} d(x, m, q) + \sum_{0 \leq x \leq \nu_{M,1} - \nu - 1} d(x, m, q).$
5. $q^m = \sum_{0 \leq x \leq \omega} d_w(x, m, q) + \sum_{0 \leq x \leq \omega_{M,1} - \omega - 1} d_w(x, m, q).$
6. $\frac{q^{m+1}-1}{q-1} = \sum_{0 \leq x \leq \omega} d_w(x, s, m, q) + \sum_{0 \leq x \leq \omega_{M,0} - \omega - 1} d_w(x, s, m, q) - \delta_{0,s}$, *where* $\delta_{0,s} = 0$, *when* $s \neq 0$, *and* $\delta_{0,0} = 1$.

Proof: 1.-3. follows using the 1-1 correspondance between $\prod_i X_i^{e_i}$ and $\prod_i X_i^{q-1-e_i}$. 4. 5. and 6. can easily be proved using the same technics as in [6,Lemma 4.1].

Theorem 14 *The dual of a weighted Reed-Muller code are given as*

1. $WARM(\omega, m, q)^{\perp} = WARM(\omega_{M,1} - \omega - 1, m, q).$
2. $WPRM(\omega, s, m, q)^{\perp} = WPRM(\omega_{M,0} - \omega - 1, q-1-s, m, q)$, *when* $s \neq 0$.
3. $WPRM(\omega, 0, m, q)^{\perp} = WPRM(\omega_{M,0} - \omega - 1, 0, m, q)^*$,
   where C^* *is the shortned code of* C, *defined by* $C^* = span\{\mathbf{v}_2, \ldots, \mathbf{v}_k\}$ *where* $C = span\{\mathbf{1}, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ *and* $\mathbf{1}$ *means the vector* $(1, \ldots, 1)$.

Proof: Using [6, Lemma 4.2 and 4.3], it is clear that it is enough to prove that the dimensions add to q^m resp. $(q^{m+1}-1)/(q-1)$. This follows, however, immediately from Lemma 13, (*4.-6.*). Like in the projective Reed-Muller case one has to be careful in the case when the normal degree is 0 modulo $(q-1)$. The constants then have to by counted only once.

4 Weighted Reed-Muller codes and algebraic-geometric codes

In this section we study the *WARM*-codes from a algebraic geometric point of wiew. Goppa introduced the algebraic geometry approach to coding theory about 1980 by the following beautiful construction (see [9]):

Let C be a projective, nonsingular, absolutely irreducible curve defined over $\mathbf{F}_q$ with functionfield $\mathbf{F}_q(C)$ and of genus g. Let $D = \sum_{i=1}^{n} P_i$, and G be two divisors defined over $\mathbf{F}_q$ such that G and D have disjoint support, the P_i's distinct $\mathbf{F}_q$-rational points on C. We define a $\mathbf{F}_q$-linear evaluation map

$$\alpha_L : L(G) \rightarrow \mathbf{F}_q^n.$$

by $\alpha_L(f) = (\ldots, f(P_i), \ldots)$.

As usual $L(G) = \{f \in \mathbf{F}_q(C) \mid div(f) \geq -G\}$ and the corresponding algebraic-geometric code $C_L(C, D, G)$ is now

$$C_L(C, D, G) = \alpha_L(L(G)).$$

Let us now specialize to the following situation:

- $C \subset \mathbf{P}^m$
- $G = \omega Q$, Q a $\mathbf{F}_q$-rational point on $C, \omega \in \mathbf{N}$.
- $D = \sum_{i=1}^{q^m} P_i, P_i \in \mathbf{P}^m \backslash H$.

where H is a hyperplane, and $Q \in H$. Denote the coordinates of $\mathbf{P}^m$ by x_i, and assume w.l.o.g. that $H = Z(x_0)$. Let us call a curve with these properties an *affine covering curve.*

Let us now consider linear systems of monomials in the affine coordinatefunctions $y_i = x_i/x_0, i = 1, \ldots, m$. That means, we consider vectorspaces generated by monomials on the form

$$\prod_{i=1}^{m} y_i^{e_i}, e_i \in \mathbf{N}.$$

For a given finite set of such monomials, the vectorspace generated by these monomials is a subspace of a $L(nQ)$ for n large enough (larger than the maximal pole order in Q of

the basismonomials). When the linear system generates a $L(nQ)$ for some n, the linear system is said to be *complete.*

Given a $L(\omega Q)$, we can associate to it, a linear system, taking monomials of coordinatefunctions that has poleorder less than or equal ω as a basis. To a maximal such linear system we associate a weighted affine Reed-Muller code, namely

$$WARM(\omega, m, q)$$

where the weights are $w_i = |v_Q(y_i)|, i = 1, \ldots, m$, the discrete valuation corresponding to Q denoted by v_Q. It is the maximal $WARM$-code, which is a subcode of $\alpha_L(L(\omega Q))$.

When our linear system is complete, i.e when $L(\omega Q)$ is spanned by functions on the form $\prod_{i=1}^{m} y_i^{e_i}$, we in fact have an algebraic-geometric code given as a $WARM$-code.

Example 15 *(The Pellikaan-Shen-van Wee Curve.)* The curve C used in [7] is given by the complete intersections of hypersurfaces

$$x_i^{q+1} - x_i^2 x_0^{q-1} + x_{i+1} x_0^q - x_{i+1}^q x_0 = 0,$$

where $i = 1, \ldots, m-1$. C is almost a curve on the form given above. It goes through all $\mathbf{F}_q$-rational points in $\mathbf{P}^m \backslash H$, where $H = Z(x_0)$. It intersects the hyperplane H in exactly one point Q, but is highly singular in that point (and that is the only singularity). It is shown in [7] that there lies only one smooth point above Q on the normalization of C. If we identify Q and the q^2 points in $\mathbf{P}^m \backslash H$ with their preimage on the normalization, (saving notation, see [7] for a precise describtion) and likewise with the coordinate functions $y_i = x_i/x_0$, we are now in a situation like above - we can think of C as an affine covering curve.

Let v_Q denotes the discrete valuation at Q. In [7] it is shown that

$$v_Q(y_i) = -q^{m-i}(q+1)^{i-1}.$$

It is furthermore shown that

$$L(\omega Q) = span\{\prod_{i=1}^{m} y_i^{e_i} \mid v_Q(\prod_{i=1}^{m} y_i^{e_i}) \geq -\omega\}$$

The linear system is complete and if we define weights $\{q^{m-i}(q+1)^{i-1}\}_{i=1}^{m}$, we have that the corresponding code $\alpha_L(L(\omega Q))$ now is

$$WARM(\omega, m, q).$$

Thereby the minimum distance is also found, but as noted in remark 9 the code itself is actually not interesting, since there exists a Reed-Muller code with the same minimum distance and length, but with a higher dimension, namely $ARM(\nu_{max}(\omega), m, q)$.

In general, a linear system of the form described above is not complete, but is a subspace of some $L(\omega Q)$-space. The minimumdistance of the corresponding WARM-code then gives an upper bound for the minimum distance of the algebraic -geometric code C_L. The Riemann-Roch theorem gives a lower bound of the minimum distance of the algebraic -geometric code.

Example 16 *(The Hansen-Stichtenoth Curve)* We consider the curve, C, given by the affine equation

$$x_2^q - x_2 - x_1^{q_0}(x_1^q - x_1) = 0,$$

where $q = p^{2n+i}, q_0 = p^n, n \in \mathbf{N}_0, i \in \mathbf{N}$.

This curve has the properties considered above. It has q^2+1 $\mathbf{F}_q$-rational points, where exactly one point, Q, lies in the hyperplane (line) at infinity, and the rest, P_i, covers the affine plane $\mathbf{A}^2(\mathbf{F}_q)$.

Using the construction above we get codes $C_L(C, \omega Q, D)$ of length $n = q^2$, dimension $k = dim(\alpha_L(L(\omega Q))$ and minimum distance $d \geq q^2 - \omega$.

In [11] it is shown that the functions

$$g_1 = f_q = \frac{x_1}{x_0}, g_2 = f_{q+q_0} = \frac{x_2}{x_0},$$

$$g_3 = f_{q+q/q_0} = x_2^{q/q_0} - x_1^{q/q_0+1}, g_4 = f_{q^2/q_0^2-q+q/q_0+1} = x_2^{q/q_0} x_1^{q/q_0-1} + f_{q+q/q_0}^{q/q_0},$$

"generate" the vectorspace $L(\omega Q)$ in the following sense:

$$L(\omega Q) = span \{ \prod_{i=1}^{4} g_i^{e_i} \mid \sum_{i=1}^{4} e_i w_i \leq \omega \},$$

where the weights w_i are the subindex of the f-function corresponding to g_i.

It is clear that

$$WARM(\nu_{max}(\omega), 2, q) \subseteq C_L(C, \omega Q, D)$$

and therefore the minimum distance of $WARM(\nu_{max}(\omega), 2, q)$ is an upper bound for the minimum distance of $C_L(C, \omega Q, D)$.

The minimum distance for the $WARM(\nu_{max}(\omega), 2, q)$-code with the weights q and $q + q_0$ is

$$d = (q - b)q^{1-a}, \tag{1}$$

where

$$a = 0, \text{ for } \omega \leq q(q-1) \text{ and } a = 1 \text{ for } q(q-1) < \omega \leq (q-1)(2q + q_0 - 1)$$

and

$$b = \lfloor \frac{\omega - q(q-1)}{q + q_0} \rfloor \text{ for } a = 1 \text{ and } b = \lfloor \frac{\omega}{q} \rfloor \text{ for } a = 0.$$

This is infact the exact minimum distance for $\omega = q(q-c), c = 1, \ldots, q$, since here the minimum distance coincides with the lower bound

$$d \geq q^2 - \omega,$$

deduced from the Riemann-Roch Theorem. By complete computersearch it is shown ([12]) that for other values of ω, (1) is not the exact minimum distance of the Hansen-Stichtenoth codes.

5 Acknowledgements

This work were done during a visit at RISC-LINZ, Austria. The author would like to thank the whole faculty at RISC for their hospitality.

6 References

[1.] T.Kasami, S.Lin, W.W.Peterson : New Generalizations of the Reed-Muller Codes Part I: Primitive Codes, *IEEE, IT-14, no. 2, 1968.*

[2.] E.J.Weldon : New Generalizations of the Reed-Muller Codes Part II: Nonprimitive Codes, *IEEE, IT-14, no. 2, 1968.*

[3.] T.Kasami, S.Lin, W.W.Peterson : Polynomial Codes, *IEEE, IT-14, no. 6, 1968.*

[4.] P.Delsarte, J.M.Goethals, F.J.MacWilliams : On Generalized Reed-Muller Codes and Their Relatives,*Information and Control 16, pp. 403-442, 1970.*

[5.] G.Lachaud : The parameters of Projective Reed-Muller Codes, *Discrete Mathematics 81 (1990), pp. 217-221*

[6.] A.B.Sørensen : Projective Reed-Muller Codes, to appear in IEEE-Trans. on Inf. Theory, november 1991.

[7.] R.Pellikaan, B.Z.Shen, G.J.M.van Wee : Which linear codes are algebraic -geometric?, to appear in IEEE-IT.

[8.] S.Lang, *Algebra*, Addison Wesley, New York 1965.

[9.] V.D.Goppa, *Geometry and Codes*, Mathematics and its application, Soviet series 24, Kluwer Ac. Publ.,Dordrecht, The Netherlands, 1989.

[10.] J.P.Hansen, H.Stichtenoth : Group Codes on Certain Algebraic Curves with many rational points, *AAECC, vol.1, no.1, pp. 67-77, 1990.*

[11.] J.P.Pedersen, A.B. Sørensen, Codes from Certain Algebraic Functionfields with many Rational Places, *MAT-REPORT NO. 1990-11, Matematisk Institut, Danmarks Tekniske Højskole, June 1990.*

[12.] A. Holm, Masters Thesis, Matematisk Institut, Aarhus Universitet, 1990

6 A note on algorithms deciding rationality and absolutely irreducibility based on the number of rational solutions

Revised version of [Sø91b].

A note on algorithms deciding rationality and absolutely irreducibility based on the number of rational solutions

Anders Bjært Sørensen

-

Abstract

In this note, we focus on known results concerning the number of rational solutions of a polynomial defined over a finite field, and show how this information carries a lot of geometrical information on the zeroset.

It turns out that qualitative characteristica as rationality and absolutely irreducibility are reflected in the number of solutions over finite fields. We explain how we get an outline of new interesting algorithms using this fact.

We explicitely give algorithms that partially detects non-rationality of an algebraic curve defined over a finite field and we discuss an outline for a probabilistic algorithm finding the number of absolutely irreducible factors of a multivariable polynomial defined over a finite field. This algorithm can be lifted to an algorithm finding the number of irreducible factors and the number of absolutely irreducible factors of a multivariable polynomial defined over the rational numbers.

1 Introduction

In this paper we try to use information on the number of rational points on hypersurfaces to build algorithms that detects non-rationality and absolutely irreducibility. This approach is as far as the author knows new, but also not at all fully developed. The aim here is also to present some results theoretically and computationally that hopefully will encourage other people to work along these ideas.

Two main ideas compromises this paper. First, we try to solve problems like rationality and absolutely irreducibility detecting consequences of these properties (sufficient and necessary) and not by actually using methods used in solving bigger problems, like genuscomputation and factorization. The methods presented here cannot be extended to these bigger and more difficult problems. And this should not be so. From a complexity point of view, it should be easier to detect rationality/nonrationality resp. absolutely irreduciblity than to find the genus (in case of a curve) resp. factorize.

The other idea is to use reduction modulo a prime whenever possible. This is a well-known princip used in factorizationalgorithms as the Berlekamp-Hensel algorithm and

solves the traditionally big problem of uncontrolled coefficient-growth. However it is also typically difficult to apply reductionmethods. We will in this paper only discuss the reductionproces/lifting in the part concerning absolutely irreducibility.

In section 2 the question about rationality of algebraic curves defined over a finite field is treated. The corresponding problem for curves defined over the rational numbers including the reductionprocess, we hope to address in near future.

In section 3 we give an outline of an absolutely irreducibility test for polynomials with coefficients in finite fields or in the rational numbers. Examples are given that indicate the possibilities of this approach.

2 Rationality

Curves. Let $\mathbf{F}_q$ be the finite field with q elements, q a prime power. For a nonsingular projective curve X defined over $\mathbf{F}_q$ (i.e. the defining equations defined over $\mathbf{F}_q$) the famous Weil-conjectures (now proved!) gives a lot of information on the number of $\mathbf{F}_q$-rational solutions (points on X).

If we by N_m denote the number of F_{q^m}-rational solutions (points on X), we define the Zetafunction of X

$$Z(t) = Z(X, \mathbf{F}_q)(t) = exp\,(\sum_{m=1}^{\infty} N_m \frac{t^m}{m}).$$

The Weil-conjectures now tells

Theorem 2.1 (Weil) *The Zetafunction of X is a rational function*

$$Z(t) = \frac{P(t)}{(1-t)(1-qt)},$$

and the numerator satisfies

$$P(t) \in \mathbf{Z}(t), \quad P(t) = \prod_{i=1}^{2g}(1-\alpha_i t)$$

$$\alpha_i \in \mathbf{C}, \quad \alpha_i \alpha_{2g+1-i} = q, \quad |\alpha_i| = \sqrt{q},$$

where g is the genus of X.

A proof of this theorem can be found in [FJ]. We will in this paper mainly use the following corollary.

Corollary 2.2

$$N_m = 1 + q^m - \textstyle\sum_{i=1}^{2g} \alpha_i^m \tag{1}$$

$$| N_m - (1+q^m) | \leq 2g\,\sqrt{q^m} \tag{2}$$

$$N_m = 1 + q^m, \quad m = 1, \ldots, g \quad \Rightarrow \quad N_{2g} = 1 + q^{2g} + 2gq^g \tag{3}$$

Example 2.3 Consider the nonsingular elliptic curve (genus = 1) $Y^2Z - X^3 - X^2Z - XZ^2 = 0$ over $\mathbf{F}_7$. It is easy to count the number of projective $\mathbf{F}_7$-rational solutions. It turns out to be 8. Over $\mathbf{F}_{7^2}$ we find 64 points. This illustrates (3) in the corollary.

Remark 2.4 For singular curves nothing as nice as the above theorem 2.1 holds. The zetafunction will still be a rational function, but the degrees of the polynomials will now be dependent on the singular structure and not just of the genus. For a fixed genus, curves exist with the number of rational points arbitrarily big.

We see that we can use corollary 2.2 to give an algorithm deciding rationality of nonsingular curves:

Algorithm RATIONAL-1

INPUT: X nonsingular curve defined over $\mathbf{F}_q$, a upper bound $gb(X)$ of the genus of X.

OUTPUT: Answer to the question: Is X rational or not ?

1. Compute N_1
2. **if** $N_1 \neq 1 + q$ **then Return**('Not rational') **fi**
3. $i := 1$
4. **while** $N_i = 1 + q^i$ **and** $i < 2gb(X)$ **do**
   $i := i + 1$;
   Compute N_i;
   if $N_i \neq 1 + q^i$ **then Return**('Not rational') **fi**
   od
5. **Return**('Rational').

Remark 2.5 The algorithm is correct, since from corollary 2.2 (2) we have that $N_i \neq 1 + q^i \Rightarrow g > 0$. The two "Not rational"-Return's are therefore correct. The while-loop is correct since, if we complete the loop and go to step 5, we have $N_i = 1 + q^i$ for $i = 1, \ldots, 2gb(X)$. It follows that $N_{2g} = 1 + q^{2g}$ and from corollary 2.2 (3) the conclusion in step 5 is correct. Termination of the algorithm is obvious.

Remark 2.6 This algorithm has no practical interest in the shown form, since the knowledge of nonsingularity and some explicitely given equations necessary for the computation of N_i , will typically give enough information to decide rationality without this algorithm. For instance explicitely given nonsingular plane curves at once gives us the genus via the genusformula. The same happens for complete intersections.

Let us now consider singular curves. Any singular curve has a unique non-singular model and non-singular $\mathbf{F}_q-$rational points on the singular curve are in 1-1 correspondance with $\mathbf{F}_q-$rational points on the non-singular model. Counting $\mathbf{F}_q-$rational points on the singular curve therefore gives good information on the number of $\mathbf{F}_q-$ rational points on its non-singular model.

The algorithm RATIONAL-1 can be modified such that it detects non-rationality for a big class of "difficult" curves (i.e. curves with bad singularities). For this we need some information on the blowing-up of singularities - but we do not want too much information (then we know the genus already). We want to give reasonable good estimates on the number of $\mathbf{F}_q-$rational points on the nonsingular model - good enough to exclude many nonrational cases using corollary 2.2.

Algorithm RATIONAL-2 below describes such a modification.

Let N_i^* be the number of non-singular $\mathbf{F}_{q^i}-$rational points on X, let Δ_i be a bound on the difference between N_i^* and the number of $\mathbf{F}_{q^i}-$rational points, N_i, on the non-singular model of X.

Algorithm RATIONAL-2

INPUT: X a curve defined over $\mathbf{F}_q$, an upper bound $gb(X)$ of the genus of X.

OUTPUT: Answer to the question: Is X non-rational or maybe rational ?

1. Compute N_1^* and Δ_1
2. **if** $|N_1^* - (1+q)| > \Delta_1$ **then Return** ("Not rational") **fi**
3. $i := 1$
4. **while** $|N_i^* - (1+q^i)| \leq \Delta_i$ **and** $i < 2gb(X)$ **do**
   $i := i+1$;
   Compute N_i^* and Δ_i;
   if $|N_i^* - (1+q^i)| > \Delta_i$ **then Return**("Not rational") **fi**
   od
5. **Return**("Special analysis needed").

Remark 2.7 The correctness and termination of version 2 follows immediately from the correctness and termination of version 1. The differensbound Δ_i can of course as a refinement be devided into an upper and a lower bound and the refined algorithm is stright forward to write down.

Example 2.8 Consider the plane curve C defined by $(X^2+Y^2-Z^2)^3 + 27X^2Y^2Z^2 + XZ^5 - Z^6 = 0$. The numbers, N_1^* and $N_{1,sing}$, of $\mathbf{F}_p-$ rational nonsingular points and $\mathbf{F}_p-$rational singular points for small primes are found to be

p	5	7	11	13	17	19
N_1^*	3	8	3	13	23	27
$N_{1,sing}$	2	0	0	4	2	0

The trivial upper genus bound is 10. Concerning the differens Δ_1, we can immediately give the following general bounds.

Each singularity P defined over $\mathbf{F}_p$ corresponds to at most m_P nonsingular $\mathbf{F}_p$-rational points on the nonsingular model, where m_P is the multiplicity of the point and at least r_P nonsingular $\mathbf{F}_p$-rational points on the nonsingular model, where r_P is the number of distinct tangentlines at P defined over $\mathbf{F}_p$.

Using the algorithm (step 2.) we conclude for $p = 11, 27$ nonrationality, since $\Delta_1 = 0$. For $p = 7$, we have no conclusion, since the curve here shows rational behaviour. For $p = 5$, we have two singularities $(2 : 1 : 0)$ and $(3 : 1 : 0)$, both cusps of multiplicity 2 with 1 tangent defined over $\mathbf{F}_5$. We have no conclusion from this information, since each singularity could contribute with 1 or 2 non-singular rational points. Further analysis is necessary. For $p = 17$, however, we have nonrationality, since the number of nonsingular points already exceeds $1 + p$. For $p = 13$, we have no conclusion at a first glance.

For $p = 7$, computations in $\mathbf{F}_{49}$ shows 54 non-singular solutions and 2 singular solutions (cusps of multiplicity 2 at infinity $Z = 0$). Therefore, in step 4 we detect non-rationality for $p = 7$.

For $p = 5$, computations in $\mathbf{F}_{25}$ shows 25 non-singular solutions and 2 singular solutions (the two already found over $\mathbf{F}_5$). Non-rationality is immediate, since we have more than 26 smooth $\mathbf{F}_{25}$-rational solutions on the smooth model.

For $p = 13$, the four singularities consists of two doublepoints $(11 : 1 : 1)$ and $(11 : 12 : 1)$ with two conjugated tangents defined over $\mathbf{F}_{13^2}$, and two cusps $(5 : 1 : 0)$ and $(8 : 1 : 0)$ of multiplicity 2. All together they contribute with at least 2 nonsingular $\mathbf{F}_{13}$−rational points on the smooth model. Therefore, we have at least 15 non-singular $\mathbf{F}_{13}$−rational points and we conclude non-rationality.

Example 2.9 Consider the plane curve C defined by $(X^2 + Y^2 - Z^2)^3 + 27X^2Y^2Z^2 = 0$. The numbers, N_1^* and $N_{1,sing}$, of $\mathbf{F}_p-$ rational nonsingular points and $\mathbf{F}_p$−rational singular points for small primes are found to be

p	5	7	11	13	17	19
N_1^*	0	4	8	0	12	16
$N_{1,sing}$	10	4	4	10	10	4

From none of the computed numbers we are able to conclude non-rationality using the algorithm. This is not surprising, since the curve is a socalled astroid - a well-known rational curve over the rationals. It has six cusps and four ordinary doublepoints and good reduction for all primes greater than or equal 5.

From the numbers computed and looking at tangentcones one sees that for $p = 5, 13, 17$ all singularities are defined over the groundfield - for $p = 7, 11, 19$ only cusps are defined

over $\mathbf{F}_p$. For $p = 5, 17$, we have six cusps giving one rational point each and four doublepoints with tangents defined over a quadratic extension. For $p = 13$, we have the tangents to the doublepoints defined over the groundfield and therefore contributing with eight rational points.

Example 2.10 Consider the spacecurve C defined by $X^2 - XZ - YU = 0, YZ - XU - ZU = 0$. It is (over the rationals) a well-known elliptic quartic, i.e. genus 1. This is reflected in the number of rationals points over finite fields as shown in

p	5	7	11	13	17	19
N_1^*	8	8	12	8	16	12
$N_{1,sing}$	0	0	0	0	0	0

For $p = 5, 13, 17$, we immediately conclude non-rationality.

For $p = 7, 11, 19$, we have rational behaviour. Computing the number of rational solutions in a quadratic extension of $\mathbf{F}_7, \mathbf{F}_{11}$ and $\mathbf{F}_{19}$ gives $64, 144$ and 400 non-singular rational solutuions. In the first loop of step 4. we return with a "non-rational". Since we already knew that the genus (over the rational numbers) is 1, the computed numbers are just what corollar 2.2 (3) predicted for genus 1 curves.

Remark 2.11 An algorithm deciding rationality of plane algebraic curves defined over the rational numbers are being developed. It is based on the above algorithm together with a reduction modulo a prime. We hope to present this in near future.

Remark 2.12 In the case of higher dimensional varieties the situation is more complicated and just the fact that we don't have a unique non-singular model in dimension greater than 1 shows that the algorithms doesn't generalize - new ideas have to be introduced. Also the Weil-conjectures are much more complicated and even in the codimension 1 case (nonsingular hypersurfaces) where rather explicit formulas are known (see [IR]), counting the number of rational points, just like in the above algorithms, gives almost no information.

3 Absolutely irreducibility

First some heuristic principles that detecs many absolutely irreducible polynomials. It is based on lemmas taken from [PS] and [SCH].

Lemma 3.1 *Let K be a field. Let $F(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$. Let $F_H(x_0, \ldots, x_n)$ be the homogenization of F w.r.t. x_0. If for all $(a_0, \ldots, a_n) \in \overline{K}^{n+1} \setminus \{\underline{0}\}$ such that $F_H(a_0, \ldots, a_n) = 0$ we have*

$$\frac{\partial F_H}{\partial x_i}(a_0, \ldots, a_n) \neq 0, i = 0, \ldots, n$$

then F is absolutely irreducible.

In geometrical terms the lemma states the fact that non-singularity for a projective connected algebraic set over the algebraic closure ensures irreducibility. When the defining polynomial is reducible the different components have to meet (connectedness is obvious) in points in which all derivatives vanishes. This criterion of course does not apply to singular, absolutely irreducible polynomials and is furthermore impossible to use in practise except in special cases, since we have to check for solutions in the algebraic closure.

Lemma 3.2 *Let K be a perfect field and let $F \in K[x_1, \ldots, x_n]$, irreducible over K. There exists a finite Galois extension M of K such that F factorizes uniquely*

$$F = \lambda \prod_{i=1}^{k} F_i$$

where $[M : K] = k, \lambda \in K, F_1, \ldots, F_k \in M[x_1, \ldots, x_n]$, absolutely irreducible, $deg(F_i) = deg(F)/k, i = 1, \ldots, k$ and all $F_i's$ are conjugated.

This lemma gives us a heuristic criterion that in many cases makes it possible to extend irreducibility to absolutely irreducibility. Unfortunately it is not exhausting - there exists absolutely irreducible polynomials for which the criterion does not apply. The criterion says that if there exists just one non-singular solution over the groundfield - then the polynomial is absolutely irreducible. Or in other words: All solutions over the groundfield have to be singular when the polynomial is not absolutely irreducible. Precisely stated

Corollary 3.3 *Let K be a perfect field and let $F \in K[x_1, \ldots, x_n], n \geq 2$, irreducible over K. If there exists $(a_1, \ldots, a_n) \in K^n$ such that*

$$F(a_1, \ldots, a_n) = 0 \text{ and } \frac{\partial F}{\partial x_i}(a_1, \ldots, a_n) \neq 0, \text{ for some } i \in \{1, \ldots, n\}$$

then F is absolutely irreducible.

Proof: Let the notation be as in lemma 3.2. It is clear that a zero $(a_1, \ldots, a_n)$ of F is a zero of one of the $F_i's$ in the factorization of F in some minimal Galois extension. Now, the $F_i's$ are here all conjugated with each other, so $(a_1, \ldots, a_n)$ has to be a zero of all $F_i's$. Hence $\frac{\partial F}{\partial x_i}(a_1, \ldots, a_n) = 0, i = 1, \ldots, n$. So in the reducible case a zero of F in the groundfield must vanish on all derivatives. If not, F is absolutely irreducible.

Remark 3.4 In case of the rational numbers it is easy to construct examples, where the corollary does not apply: For instance $F(x, y) = x^2 + y^2 + 1$. No rational solutions and irreducible over $\mathbf{Q}$ and $\overline{\mathbf{Q}}$. In the case of finite fields the corollary is much stronger. In fact, for a given absolutely irreducible polynomial defined over $\mathbf{F}_q$ there always exists an extension, where the corollary applies. This follows from theorem 3.8 below, since the singular points are a closed subvariety of codimension at least 1.

Bivariate polynomials. Let us consider the bivariate case in more detail. Let us look at a polynomial $F(x,y) \in \mathbf{F}_q[x,y], deg(F) = d$. We will in the following identify F with its homogenization F_H and work projectively.

Assume F is absolutely irreducible. We denote by $N_i(F)$ the number of projective non-singular $\mathbf{F}_{q^i}-$rational solutions to $F = 0$ and by g_F the genus of $Z(F)$. Assume that the number of rational points on the non-singular model is $N_i(F) + \Delta_i(F)$. Corollar 2.2 gives

$$1 + q^i - 2g_F(\sqrt{q})^i - \Delta_i(F) \leq N_i(F) \leq 1 + q^i + 2g_F(\sqrt{q})^i.$$

If F is irreducible over $\mathbf{F}_q$, but not absolutely irreducible, we have from lemma 3.2 that F factors over $\mathbf{F}_{q^k}$ into k factors $\{F_j\}_{j=1}^k$ all conjugated, absolutely irreducible and of degree d/k. Each factor satisfies

$$1 + q^k - 2g_{F_j}(\sqrt{q})^k - \Delta_k(F_j) \leq N_k(F_j) \leq 1 + q^k + 2g_{F_j}(\sqrt{q})^k, j = 1, \ldots, k.$$

From this and corollary 3.3, we deduce the following property on $N_i(F)$

$$N_i(F) = 0,\ i = 1, \ldots, k-1,\ N_k(F) \leq k(1 + q^k + 2g_{F_j}(\sqrt{q})^k) - 1.$$

Assume F is reducible and squarefree over $\mathbf{F}_q$ and assume F factors over $\mathbf{F}_q$ as

$$F = \prod_{j=1}^{t} G_j \prod_{j=1}^{s} H_j,$$

where the t factors G_j are absolutely irreducible, and the s factors H_j of degree d_j, each factors into e_j absolutely irreducible factors $H_{j,l}$ of degree d_j/e_j over $\mathbf{F}_{q^{e_j}}$. Combining the previous inequalities we get

$$N_i(F) \leq \sum_{j=1}^{t}(1 + q^i + 2g_{G_j}(\sqrt{q})^i) + \sum_{j, e_j | i} e_j(1 + q^i + 2g_{H_{j,l}}(\sqrt{q})^i) - 1.$$

We deduce from the above inequalities

Theorem 3.5 *Let $F(x,y) \in \mathbf{F}_q[x,y]$. Let $N_j(F)$, be the number of projective $\mathbf{F}_{q^j}-$rational non-singular solutions of $F = 0$ and let $gb(F)$ be an upper bound on the possible genus of $Z(F)$ in the absolutely irreducible case. If*

$$0 < N_1(F) < 1 + q - 2gb(F)\sqrt{q} - \Delta_1(F) \text{ or } N_1(F) > 1 + q + 2gb(F)\sqrt{q},$$

then F is reducible over $\mathbf{F}_q$.

Assume F is irreducible over $\mathbf{F}_q$. If for some $j > 1$

$$0 < N_j(F) < 1 + q^j - 2gb(F)(\sqrt{q})^j - \Delta_j(F) \text{ or } N_j(F) > 1 + q^j + 2gb(F)(\sqrt{q})^j,$$

then F is reducible over $\mathbf{F}_{q^k}$ with k factors, k a divisor of j.

Remark 3.6 If F is reducible over $\mathbf{F}_q$, with at least two factors absolutely irreducible over $\mathbf{F}_q$, this fact can be detected for $q > (9/4)d^4$. This follows from the inequality

$$1 + q + d^2\sqrt{q} < 2(1 + q - 2\frac{1}{2}(\frac{d}{2})^2\sqrt{q} - (\frac{d}{2})^2) - (\frac{d}{2})^2,$$

where we use the upper bounds $(1/2)d^2$ for the genus and d^2 for the differens Δ_1 of a plane curve of degree d.

Example 3.7 Let $F(x,y) = -2x^2y^2 - x^5 - x^4 - 3x^3 + 3y^4 - 3y^2x^3 - 3y^2x + 2y^2 - 2x^2 - 2x$. The following tabel shows the number N_1 of non-singular solutions and the number S_1 of singular solutions for primefields

p	5	7	11	13	17	19	23	29	31	37	41	43	47	53
N_1	10	16	28	22	30	36	40	46	64	66	78	92	88	106
S_1	2	0	0	4	2	0	0	4	4	2	6	0	4	2

We see that we can apply theorem 3.5 with upper bound $6 - S_1$ on the genus. In case $p = 31, 41, 47$ we detect reducibility over $\mathbf{F}_p$. In fact by construction $f = (x^2 + 3y^2 + 2)(y^2 - x^3 - x^2 - x)$. For the other p in the table, theorem 3.5 does not apply.

Multivariable polynomials. For nonsingular hypersurfaces the theory of zetafunctions (see[IR]) gives information on the number of rational points. However, we are interested in arbitrary hypersurfaces and let us recall the following more general theorem [SCH, V.Th.5A].

Theorem 3.8 *Let $F(x_1, \ldots, x_n) \in \mathbf{F}_q[x_1, \ldots, x_n], n \geq 2$ absolutely irreducible, and N_m be the number of $\mathbf{F}_{q^m}$−rational projective points. Then, for $m \to \infty$, we have*

$$N_m = (q^m)^{n-1} + O((q^m)^{n-(3/2)}).$$

It has been known for a long time that absolutely irreducibility of a polynomial defined over the rational numbers, $\mathbf{Q}$, carries over to almost all reductions modulo a prime p. Schmidt [SCH] gives a bound due to Ostrowski such that reduction modulo primes bigger that the bound preserves absolutely irreducibility. This fact together with theorem 3.8 gives immediately the following ([SCH, V,Cor.5C])

Theorem 3.9 *Let $F(x_1, \ldots, x_n) \in \mathbf{Q}[x_1, \ldots, x_n], n \geq 2$, absolutely irreducible, and $N(p)$ be the number of solutions in $(\mathbf{F}_p)^n$ to $F \equiv 0 \bmod p, p$ a prime. Then for $p \to \infty$ we have*

$$N(p) = p^{n-1} + O(p^{n-(3/2)}).$$

The above two theorems 3.8 and 3.9 are the basis of two similar absolutely irreducibility tests. We state

Theorem 3.10 *Let $F(x_1,\ldots,x_n) \in \mathbf{F}_q[x_1,\ldots,x_n], n \geq 2$, squarefree, and let N_m be the number of $\mathbf{F}_{q^m}-$rational projective solutions. Then*

$$\lim_{m\to\infty} \frac{N_m}{(q^m)^{n-1}} = k$$

where k is the number of absolutely irreducible factors of F.

Proof: Let F factor into k absolutely irreducible factors over some finite extension of $\mathbf{F}_q$. N_m, for $m >> 0$ is then the sum of the number of solutions for each absolutely irreducible factor subtracted by the number of solutions in common, loosely speaking. The intersection of the irreducible factors is an algebraic set of dimension at most $n-2$. The number of solutions on a variety of dimension d is $(q^m)^d + O((q^m)^{d-(1/2)})$ ([SCH, VI. Th.7A]). This subtraction therefore does not influence the leading term $(q^m)^{n-1}$ in theorem 3.8. Using theorem 3.8 for each factor and adding afterwards gives the theorem.

Theorem 3.11 *Let $F(x_1,\ldots,x_n) \in \mathbf{Q}[x_1,\ldots,x_n], n \geq 2$, squarefree, and let $N(p)$ be the number of solutions in $(\mathbf{F}_p)^n$ to $F \equiv 0 \bmod p, p$ a prime. Then*

$$\lim_{p\to\infty} \; inf(\frac{N(p)}{p^{n-1}}) = \textit{number of abs. irr. factors def. over } \mathbf{Q}$$

$$\lim_{p\to\infty} \; sup(\frac{N(p)}{p^{n-1}}) = \textit{number of abs. irr. factors.}$$

Proof: The theorem relies on the following two facts concerning a given irreducibel polynomial f over $\mathbf{Q}$ in one variable.

1. There exists infinitely many primes p such that $f \bmod p$ factors complitely into linear factors over $\mathbf{F}_p$ (see [GB]).

2. There exists infinitely many primes such that $f \bmod p$ has no linear factors over goundfield $\mathbf{F}_p$ (see [FJ]).

Assume F factorizes as

$$F = \prod_{i=1}^{k} F_i \text{ over } \mathbf{Q}$$

and each F_i factorizes as

$$F_i = \prod_{j=1}^{l_i} F_{i,j} \text{ over } \overline{\mathbf{Q}}.$$

From the theorem of the primitive element it follows that there exists a simple, finite extension $\mathbf{Q}(\alpha)$ such that all absolutely irreducible factors $F_{i,j}$ are defined over $\mathbf{Q}(\alpha)$. Let f be the minimal polynomial for α.

Now we use theorem 3.9 on the infinite set of primes where f by reduction has no linear factors over the groundfield $\mathbf{F}_p$, and we get that for these primes all irreducible F_i remains irreducible after reduction. For this infinite number of primes the reduction of F has exactly k factors. Now only those F_i which are absolutely irreducible over

$\mathbf{Q}$ contributes to the limit in the theorem. The other irreducible, but non-absolutely irreducible, factors can only have rational solutions in their singular points according to corollary 3.3 and this fact by the choice of primes also holds after reduction. The first part of the conclusion then follows.

Likewise the second part follows from theorem 3.9 now using the infinite set of primes where $f \bmod p$ factors completely into linear factors over the groundfield. For these primes all irreducible, but non-absolutely irreducible factors F_i, will after reduction each contribute with l_i absolutely factors defined over the groundfield $\mathbf{F}_p$. The second part then follows.

Remark 3.12 It would be very interesting to find a probabilistic absolutely irreducibilitytest based on the two last theorems. Examples shown below indicates that efficient algorithms may be obtained. Some statistical evidens of this fact would also be interesting.

Example 3.13 Let

$$F(x,y) = 2x^{13}-x^{11}y^4-2x^{10}y^3+x^8y^7-2x^6y+2x^5y^{10}+x^4y^5-x^3y^{14}+2x^3y^4-2x^2y^{13}-xy^8+y^{17}.$$

Computing the number of affine solutions for primes up to 191 show the following picture:

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
N	3	5	7	27	19	47	59	71	81	53	167	141	153	169	183
$\frac{N}{p}$	1.5	1.7	1.4	3.9	1.7	3.6	3.5	3.7	3.5	1.8	5.4	3.8	3.7	3.9	3.9

p	53	59	61	67	71	73	79	83	89	97	101	103	107	109
N	103	115	235	263	277	419	459	163	349	567	199	603	211	429
$\frac{N}{p}$	1.9	1.9	3.9	3.9	3.9	5.7	5.8	2.0	3.9	5.8	2.0	5.9	2.0	3.9

p	113	127	131	137	139	149	151	157	163	167	173	179	181	191
N	441	749	261	535	547	295	891	623	645	659	343	355	719	755
$\frac{N}{p}$	3.9	5.9	2.0	3.9	3.9	2.0	5.9	4.0	4.0	3.9	2.0	2.0	4.0	4.0

The four limitpoints 2, 4 and 6 are understandable when the factorization over $\mathbf{Q}$ are found

$$F(x,y) = (x-y)(2x^2-y^4)(x^2+xy+y^2)(x^8-xy+y^{10})$$

and compared with the absolute factorization

$$F(x,y) = (x-y)(\sqrt{2}x-y^2)(\sqrt{2}x+y^2)(x-\gamma y)(x-\gamma^2 y)(x^8-xy+y^{10})$$

where γ is a third root of unity. The limit 2 comes from primes where 2 is not a square in $\mathbf{F}_p$ and also x^2+x+1 does not split. 4 comes when one of these conditions, but not both are fulfillied and 6 from primes where everything splits in the groundfield.

Example 3.14 Let

$$F(x,y) = x^{1555}y^{6332} + x^{1255}y^{5721} + x^{1234}y^{5678} + x^{444}y^{1110} + x^{333}y^{688} + x^{321}y^{654} + x^{144}y^{499} + x^{123}y^{456} + x^{33}y^{77} + x^{21}y^{43} + x^{12}y^{34} + 1$$

Computing the number of affine solutions of $F = 0$ over $\mathbf{F}_p$ for primes from 53 to 101 gives the following result

p	53	59	61	67	71	73	79	83	89	97	101
N	105	134	116	123	129	178	142	159	174	201	199
$\frac{N}{p}$	1.98	2.27	1.90	1.84	1.82	2.44	1.80	1.92	1.96	2.07	1.97

The example is computed using the MAPLE (V 4.3) computer algebra system. Using stright forward implementation, i.e. test by evaluation the p^2 possible affine solutions, it took 207 seconds for $p = 101$ and 57 seconds for $p = 53$ to find the shown results (APOLLO-10000 workstation). The only refinement used were MAPLE's built-in fast exponentiation mod$p$. MAPLE uses more than 20 hours (!) to factorize F over $\mathbf{Z}$ into

$$f = (x^{1234}y^{5678} + x^{123}y^{456} + x^{12}y^{34} + 1)(x^{321}y^{654} + x^{21}y^{43} + 1)$$

(on APOLLO-1000).

The interesting question now is: With what probability could we conclude the existence of two absolutely irreducible factors defined over $\mathbf{Q}$ from the numbers shown?

Generally it is interesting to know more about the distribution of the number of solutions when p varies and when we go to extensions $\mathbf{F}_{p^i}$.

4 Acknowledgements

The author would like to thank the faculty at RISC-LINZ, Austria for their hospitality. Without the nice research atmosphere in Schloss Hagenberg and the computer facilities including the MAPLE computer algebra system (University of Waterloo) this work would not have been possible.

5 References

[FJ] M. D. Fried, M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Bd. 11 (A Series of Modern Surveys in Mathematics), Springer-Verlag, 1986.

[GB] I. Gerst, J. Brillhart, On the prime divisors of polynomials, *American Mathematical Monthly, march 1971.*

[IR] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory* GTM 84, Springer-Verlag, 1982.

[PS] J. P. Pedersen, A. B. Sørensen, *Function Fields and Codes*, lecture notes, Technical University of Denmark, 1991.

[SCH] W. M. Schmidt, *Equations over Finite Fields, An Elementary Approach*, LNM 536, Springer-Verlag 1976.

Sammenfatning på dansk

Denne afhandling indeholder forfatterens forskningsresultater opnået i perioden 1.7.89 til 1.11.91. Til opnåelse af Ph.D. graden i matematik er afhandlingen indleveret til det naturvidenskablige fakultet ved Aarhus Universitet til bedømmelse.

Denne afhandling er støttet af et kandidatstipendium fra Statens Naturvidenskabelige Forskningsråd under titlen "Algebraisk geometri over endelige legemer". Forskerakademiet har støttet ophold i Moskva og Linz og "Kulturaftalen DK-USSR" har støttet opholdet i Moskva.

Afhandlingen bygger på 5 artikler skrevet i perioden 1.7.89 til 1.11.91. Artiklerne er

[Sø89a] A. B. Sørensen, *A "Full degeneration"-lemma for hypersurfaces in $P(q,n)$*, Preprint Series no. 5, 1989, Matematisk Institut, Aarhus Universitet. Revised version submitted to Discrete Mathematics.

[Sø89b] A. B. Sørensen, *Projective Reed-Muller codes*, Preprint Series no. 11, 1989, Matematisk Institut, Aarhus Universitet. Revised version to appear in IEEE Trans. on Inf. Theory, nov. 91.

[PS90] J. P. Pedersen, A. B. Sørensen,*Codes From Certain Algebraic Function Fields With Many Rational Places*, MAT-REPORT NO. 1990-11, Matematisk Institut, Danmarks Tekniske Højskole, June 1990.

[Sø91a] A. B. Sørensen, *Weighted Reed-Muller Codes*, RISC-Linz Series no. 91-36.0 august 1991, submitted to IEEE Trans. on Inf. Theory.

[Sø91b] A. B. Sørensen, *A Note on Algorithms Deciding Rationality and Absolutely Irreducibility Based on the Number of Rational Solutions*, RISC-Linz Series no 91-37.0, august 1991.

Disse artikler danner baggrund for kapitlerne 2-6 i nævnte rækkefølge. Med hensyn til [Sø89a] (kapitel 2) og [Sø89b] (kapitel 3) er det reviderede udgaver, der er medtaget. I kapitel 4 er [PS90] reproduceret, og kapitler 5 og 6 er reproduktioner af [Sø91a] og [Sø91b] med enkelte rettelser.

I **kapitel 1** præsenterer vi relevant, bagvedliggende teori og sætter de opnåede resultater ind i en større sammenhæng. Vi lægger vægt på de nyeste resultater og beskriver hermed den aktuelle udvikling indenfor området. Et nyt eksempel og en formodning er medtaget.

Bortset fra kapitel 1 falder afhandlingen i to dele. En første større del omfattende kapitel 2-5, der omhandler anvendelsen af algebraisk og projektiv geometri over endelige legemer indenfor teorien for fejl-korrigerende koder. Den anden del (kapitel 6) omhandler algoritmer i computer algebra og konstruktiv algebraisk geometri.

I **kapitel 2** giver vi et bevis for det såkaldte "Full degeneration-lemma". Givet en codimension-1 algebraisk mængde i $\mathbf{P}^n$ defineret over et endeligt legeme $\mathbf{F}_q, q$ en primtalspotens, og af lav grad $d, d \leq q$. "Full degeneration-lemmaet" siger, at den algebraiske mængde med det maximale antal rationale punkter er d forskellige hyperplaner gennem et fælles $\mathbf{P}^{n-2}$. Vi sammenligner, for q et kvadrat, den fundne øvre grænse med grænsen, der kommer fra Weil-formodningerne, og viser at den maximale grad af en glat plan kurve, for hvilke Weil-grænsen kan realiseres, er den samme som den øvre grænse, Serre, ved at anvende Weil-formodningerne, bemærker i [Se83]. Vores metode er hovedsaglig kombinatorisk. En udvidet udgave af kapitel 2 er indsendt til Discrete Mathematics for publikation.

I **kapitel 3** er resultaterne fra kapitel 2 generaliseret til enhver grad. Beviset for "Full degeneration lemmaet" er nu baseret på resultater fra kodningsteori om Reed-Muller koder. De projektive Reed-Muller koder introduceres og deres parametre bestemmes eksakt (her svarer minimumsafstanden til den øvre grænse i "Full degeneration-lemmaet." Det vises desuden, at en delklasse af de projektive Reed-Muller koder er cykliske. Disse generaliserede resultater besvarer fuldstændigt spørgsmålet rejst i bogen af Tsfasman og Vălduţ (Algebraic-geometric codes, Mathematics and its Application **58**, Kluwer Ac. Publ. Dordrecht, The Netherlands, 1991, Problem 1.2.9).
Kapitel 3 bliver publiceret i IEEE Transactions on Information Theory, nov. 1991.

I **kapitel 5** generaliseres Reed-Muller koderne til vægtede Reed-Muller koder. De vægtede Reed-Muller koders egenskaber studeres, kodernes parametre estimeres, de duale koder karakteriseres og deres forbindelse til algebraisk geometri koder diskuteres. Den sidstenævnte forbindelse var motivationen for at introducere disse koder. Dette kapitel er indsendt til IEEE Trans on Inf. Theory for publikation.

I **kapitel 4** (skrevet sammen med J. P. Pedersen) undersøger vi Hansen-Stichtenoth koderne i vilkårlig karakteristik (i [HS90] var kun karakteristik 2 undersøgt). Vi bestemmer antallet af rationale punkter, genus og basis for vektorrummet af rationale funktioner med foreskreven pol i uendeligt. Alle resultater fra [HS90] generaliserer til vilkårlig karakteristik pånær maximalitetsegenskaben af kurverne med hensyn til Weils eksplicitte formler.

I **kapitel 6** konstruerer vi en algoritme til detektion af rationalitet af algebraiske kurver defineret over endelige legemer, baseret på konsekvenser af Weil-formodningerne. Vi diskuterer modifikationer med henblik på mulig anvendelse i praksis. Vi fremlægger en ide til en probabilistisk absolut irreducibilitetstest for multivariable polynomier over $\mathbf{Q}$ byggende på antallet af rationale punkter på hyperflader.

Konklusion Antallet af rationale punkter på algebraiske kurver (varieteter) er af interesse i mange problemkredse i moderne matematik - både i teoritiske og anvendelsesorienterede sammenhænge. Deres store betydning indenfor anvendelse af algebraiske kurver i

teorien for fejl-korrigerende koder er veletableret. Gode koder fås fra algebraiske kurver med mange rationale punkter relativt til genus. Resultatet om minimumsafstanden af de projektive Reed-Muller koder har sin geometriske fortolkning i "Full degeneration lemmaet." Tilsyneladende indeholder antallet af rationale punkter også information, der kan bruges indenfor computer algebra og konstruktiv algebraisk geometri.

På denne måde bliver rationale punkter og deres kardinalitet forbindelsen mellem de to dele i denne afhandling, og det er forfatterens overbevisning, at flere interessante anvendelser af antallet af rationale punkter vil dukke frem.