Rendiconti
Accademia Nazionale delle Scienze detta dei XL
Memorie di Matematica e Applicazioni
125° (2009), Vol. XXXI, fasc. 1, pagg. 75-88

J. W. P. HIRSCHFELD

The Number of Points on a Curve, and Applications Arcs and Curves: the Legacy of Beniamino Segre

Dedicated to the memory of Beniamino Segre
on the centenary of his birth 16.02.1903 – 22.10.1977

ABSTRACT. — Curves defined over a finite field have various applications, such as

(*a*) the construction of good error-correcting codes,
(*b*) the correspondence with arcs in a finite Desarguesian plane,
(*c*) the Main Conjecture for maximum-distance-separable (MDS) codes.

Bounds for the number of points of such a curve imply results in these cases.

For plane curves, there is a variety of bounds that can be considered, such as the Hasse–Weil bound (1934/1948), the Stöhr–Voloch bound (1986), as well as bounds that depend on the plane embedding. Curves that achieve these bounds can sometimes be characterised.

Segre applied bounds for the number of points on a curve to obtain bounds on the sizes of complete arcs. He also considered plane Fermat curves that achieve the Hasse–Weil bound. Various of these results and their applications are surveyed.

1. - INTRODUCTION

Here are three problems.

(I) What is the size of a complete arc in $\mathrm{PG}(2,q)$?
(II) How many points are there on a curve over $\boldsymbol{F}_q$?
(III) Is the Main Conjecture for MDS codes true?

Related to all of these, Segre wrote several influential papers.

(*) Indirizzo dell'Autore: J. W. P. Hirschfeld, Department of Mathematics, University of Sussex, Brighton BN1 9RF, United Kingdom.
e-mail: jwph@sussex.ac.uk

A.M.S. Classification: 51E21 - 11G20 - 94B27.

1955 Curve razionali normali e k-archi negli spazi finiti,
Ann. Mat. Pura Appl. **39** (1955), 357–379.
1959 Le geometrie di Galois,
Ann. Mat. Pura Appl. **48**, 1–97.
1964 Arithmetische Eigenschaften von Galois-Räumen I,
Math. Ann. **154**, 195–256.
1967 Introduction to Galois geometries,
Atti Accad. Naz. Lincei Mem. **8**, 133–236.

2. - The number of points on a curve

The problem of finding the number of points over a finite field has been studied for many years.

Gauss (1801) solved the problem of finding the number of solutions (x, y) in the following cases:

1. $ax^3 - by^3 \equiv 1 \pmod{p}$ when $p \equiv 1 \pmod{3}$;
2. $ax^4 - by^4 \equiv 1 \pmod{p}$ when $p \equiv 1 \pmod{4}$.

To begin with a simple example, let $F = X^3 + Y^3 + Z^3$ and write the field

$$\boldsymbol{F}_7 = \{0, 1, 2, 3, -3, -2, -1 \mid 7 = 0\}.$$

Since, in $\boldsymbol{F}_7$, an element x satisfies $x^3 = 0, 1, -1$, so the zeros of F in PG$(2, 7)$ are

$$\begin{array}{lll} (0,1,-1), & (0,1,-2), & (0,1,3), \\ (1,0,-1), & (1,0,-2), & (1,0,3), \\ (1,-1,0), & (1,-2,0), & (1,3,0). \end{array}$$

Hence the number of zeros is $N_1 = 9$. The number of zeros of F over $\boldsymbol{F}_{49}$ is $N_2 = 63$.

If the same question is considered when F is over $\boldsymbol{F}_2, \boldsymbol{F}_4, \boldsymbol{F}_{16}$, the numbers of zeros are

$$N_1 = 3, \quad N_2 = 9, \quad N_4 = 9.$$

THEOREM 2.1 (Hasse–Weil [11, 12, 39]): *For a non-singular curve $\mathcal{C}$ of genus g defined over $\boldsymbol{F}_q$, let N_i be the number of its points rational over $\boldsymbol{F}_{q^i}$. Then*

$$\exp\Big(\sum N_i T^i / i\Big) = \frac{f(T)}{(1-T)(1-qT)}.$$

where $f \in \boldsymbol{Z}[T]$ with $\deg f = 2g$. *This implies that*

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

This last inequality can be improved.

THEOREM 2.2 (Serre [32]):

$$N_1 \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor = S_g.$$

THEOREM 2.3 Ihara [24]):

$$N_1 \leq q + 1 - \frac{1}{2}g + \left\{2\left(q + \frac{1}{8}\right)g^2 + (q^2 - q)g\right\}^{\frac{1}{2}}.$$

2.1. *The Hermitian curve*

EXAMPLE 2.4: When q is a square, the ternary Hermitian form

$$F = X^{\sqrt{q}+1} + Y^{\sqrt{q}+1} + Z^{\sqrt{q}+1},$$

is unique up to a projectivity, and defines the Hermitian curve $\mathcal{U}_{2,q} = \boldsymbol{v}(F)$. Its genus is $g = \frac{1}{2}(q - \sqrt{q})$, and the number of its rational points is $N_1 = q\sqrt{q} + 1$, attaining the Hasse–Weil upper bound.

See [21] and [27] for characterisations of $\mathcal{U}_{2,q}$.

Write $N_q(g) = \max N_1$, taken over all non-singular curves $\mathcal{C}$ of genus g over $\boldsymbol{F}_q$.

EXAMPLE 2.5: A case in which $N_q(g)$ is strictly less than S_g is the following. A plane non-singular curve $\mathcal{C}^4$ of degree 4 over $\boldsymbol{F}_7$ has at most 20 points; that is, $N_7(3) = 20 < 23 = S_3$.

Segre studied in [30, 31] the number of zeros of varieties given by an equation

$$F(X_1, X_2, \ldots, X_r) = G(Y_1, Y_2, \ldots, Y_r),$$

where F and G are homogeneous forms of degree n over $\boldsymbol{F}_q$, and

$$q = nt + 1.$$

This leads to formulas for the number of zeros in the case that F is diagonal and $G = 0$. In particular, as one case, if $q = p^b,\ q \equiv 1 \pmod 4$, and q is square, then the quartic curve, given by

$$F = X_0^4 + a_1 X_1^4 + a_2 X_2^4,$$

has

$$N_1 = q + 1 \pm 2\sqrt{q},\ q + 1 \pm 6\sqrt{q},$$

giving one curve among many attaining the Hasse–Weil upper bound, as well as one attaining the Hasse–Weil lower bound.

3. - Plane curves

As an application of the Hasse–Weil theorem, there is the following result, providing an upper bound in a form required in connection with plane arcs.

Theorem 3.1 (Segre [31]): *Let a plane curve $\mathcal{C}^d$ of degree d over $\boldsymbol{F}_q$ with no linear components have N_0 non-singular points. If*

$$\sqrt{q} > d - 1,$$

then

$$N_0 < d(q + 2 - d).$$

This can be improved subject to a further restriction.

Theorem 3.2 (Hirschfeld–Korchmáros [19]): *Let $\mathcal{C}^d$ be a plane irreducible curve. If*

$$\sqrt{q} > \frac{1}{2}\, d + 2,$$

then

$$N_0 \leq d(q + 2 - d).$$

with equality if and only if $\mathcal{C}^d$ is isomorphic to the Hermitian curve $\mathcal{U}_{2,q}$.

For a plane curve $\mathcal{F}$ defined over $\boldsymbol{F}_q$, there are different definitions of the 'number of points' on $\mathcal{F}$. So far, the number N_1 has been considered. Let this number also be written C_q. Then the numbers C_q, M_q, $\hat{M}_q$, B_q are the following:

$$\begin{aligned} C_q &= \#\, \boldsymbol{F}_q\text{-points on a non-singular model of } \mathcal{F};\\ M_q &= \#\text{ points on } \mathcal{F} \text{ in } \mathrm{PG}(2,q);\\ \hat{M}_q &= \#\text{ points on } \mathcal{F} \text{ in } \mathrm{PG}(2,q) \text{ counted with multiplicity};\\ B_q &= \#\text{ branches of } \mathcal{F} \text{ centred at an } \boldsymbol{F}_q\text{-point}. \end{aligned}$$

It follows that

(1) $C_q \leq B_q \leq \hat{M}_q$;
(2) for $\mathcal{F}$ non-singular, $C_q = B_q = M_q = \hat{M}_q$.

Theorem 3.3 (Stöhr–Voloch [34]): *Let $\mathcal{C}^d$ be a plane irreducible curve of degree d over $\boldsymbol{F}_q$ with q odd such that not all points are inflexions. Then*

$$C_q \leq \frac{1}{2} d(q + 1 - d) = V.$$

PROOF: Consider the number of points $P = (x, y, z)$ on $\mathcal{C}^d$ such that the Frobenius image $P^q = (x^q, y^q, z^q) \in \ell_P$, the tangent at P. □

REMARK 3.4: To compare these bounds, it should be noted that, for $d \geq \frac{1}{2}\sqrt{q} + 3$,

$$V \leq S_g.$$

4. - CLASSICAL CURVES

Let $\mathcal{C} = \mathcal{C}^n$ be an absolutely irreducible plane curve of degree n, which is a (possibly singular) plane model of a projective, geometrically irreducible, non-singular, algebraic curve $\mathcal{X}$ defined over $\boldsymbol{F}_q$. To each point of $\mathcal{X}$ there corresponds a *place* or a *branch* of $\mathcal{C}$; associated to each place is a unique tangent. If P is a place of $\mathcal{C}$ and $\alpha = m_P(\mathcal{C})$ is the minimum of the intersection numbers $I(P, l \cap \mathcal{C})$ for all lines l through P and so the multiplicity of P on $\mathcal{C}$, then α is the *order* of P. The tangent l_P at P is the unique line for which $I(P, l_P \cap \mathcal{C}) > \alpha$ and $\beta = I(P, l_P \cap \mathcal{C}) - \alpha$ is the *class* of P. With respect to the linear system Σ of lines of $\mathrm{PG}(2, \overline{\boldsymbol{F}}_q)$, a point with *order sequence* $(0, r, s)$ is viewed as a branch of order $\alpha = r$ and class $\beta = s - r$.

If $\mathcal{C}$ is not the locus of the points of inflexion, the order sequence of a generic point is $(0, 1, 2)$ and $\mathcal{C}$ is said to be *classical for* Σ.

If $\mathcal{C}$ is non-classical, then the order sequence at a generic point is $(0, 1, p^v)$, with $p^v > 2$, or, equivalently, the order sequence of $\mathcal{X}$ with respect to γ_n^2, the linear series cut out by lines.

For any curve $\mathcal{C}$, whether classical or non-classical, only a finite number of points have a different order sequence from the generic one. In the case that $\mathcal{C} = \mathcal{U}_{2,q}$ with degree $\sqrt{q} + 1$,

$$(0, r, s) = \begin{cases} (0, 1, \sqrt{q} + 1) & \text{for } P \text{ rational,} \\ (0, 1, \sqrt{q}) & \text{for } P \text{ generic.} \end{cases}$$

The curve $\mathcal{C}$ is *Frobenius classical* if $P^q \notin l_P$, apart from a finite number of places; so it is *Frobenius non-classical* if $P^q \in l_P$. If the order sequence at P is $(0, 1, p^v)$, then the *Frobenius order sequence* at P is

$$(0, v) \quad \text{with} \quad v = 1 \text{ or } p^v.$$

Then $\mathcal{C}$ is Frobenius classical if $v = 1$ and Frobenius non-classical if $v = p^v$.

THEOREM 4.1 (Stöhr–Voloch [34]): *Let $\mathcal{C}^d$ be a plane irreducible curve of degree d over $\boldsymbol{F}_q$. Then*

$$C_q \leq \frac{1}{2}\{d(d-3)v + (q+2)d\}.$$

The most general form of this theorem is the following.

THEOREM 4.2 (Stöhr–Voloch [34]): *Suppose that*

(a) $\mathcal{C}$ *is an irreducible curve of genus* g;
(b) γ_d^n *is a linear series on* $\mathcal{C}$ *of dimension* n *and order* d;
(c) *the order sequence on* $\mathcal{C}$ *is* $(\varepsilon_0, \ldots, \varepsilon_n)$;
(d) *the Frobenius order sequence on* $\mathcal{C}$ *is* $(\nu_0, \ldots, \nu_{n-1})$.

Then

$$C_q \leq \frac{1}{n}\{(2g-2)(\nu_0 + \ldots + \nu_{n-1}) + (q+n)d\}\,.$$

THEOREM 4.3 (Hefez–Voloch [13]): *Suppose that*

(a) $\mathcal{C}$ *is a plane non-singular curve of degree* d;
(b) $\mathcal{C}$ *is Frobenius non-classical.*

Then

$$C_q = d(q-d+2)$$

An example of this is the Hermitian curve $\mathcal{U}_{2,q}$.

If a projective curve over $\boldsymbol{F}_q$ has affine equation $f(X,Y)=0$, then f divides $H(f)$, where

$$H(f) = f_{XX}{f_Y}^2 - 2f_{XY}f_Xf_Y + f_{YY}{f_X}^2, \tag{4.1}$$

if and only if there exist non-zero polynomials $s, z_0, z_1, z_2 \in \boldsymbol{F}_q[X,Y]$ with z_i not divisible by f such that, for a power p^ν, with $\nu \geq 1$, of the characteristic p of $\boldsymbol{F}_q$,

$$s(X,Y)f(X,Y) = z_0(X,Y)^{p^\nu} + z_1(X,Y)^{p^\nu}X + z_2(X,Y)^{p^\nu}Y; \tag{4.2}$$

see [9]. For $p^\nu \leq q$, the necessary and sufficient conditions in order that the plane curve $\mathcal{C}$ with equation $f(X,Y)=0$ be Frobenius non-classical are (4.3) together with (4.2), where

$$t(X,Y)f(X,Y) = z_0(X,Y) + z_1(X,Y)\,X^{q/p^\nu} + z_2(X,Y)\,Y^{q/p^\nu}. \tag{4.3}$$

Note that if the Frobenius non-classical projective curve is non-singular, then $p^\nu \leq \sqrt{q}$.

A plane curve over $\boldsymbol{F}_q$ may have singular points at which the tangents do not lie over $\boldsymbol{F}_q$. These give branch points that are not counted as $\boldsymbol{F}_q$-points on a non-singular model. As an example, a plane cubic curve with an isolated double point has $q+3$ branch points but only $q+1$ points on a twisted cubic, the non-singular model. The next two theorems give results that include such points.

THEOREM 4.4 ([20]): *Let* $\mathcal{C}$ *be the projective plane curve of degree* d *and genus* g *given by* $f(X,Y)=0$, *where* $f(X,Y)$ *is an absolutely irreducible polynomial with coefficients in* $\boldsymbol{F}_q$.

(i) *If* $f \nmid H(f)$, *then*

$$B_q \leq \frac{1}{2}\{(2g-2) + (q+2)d\}. \tag{4.4}$$

(ii) *If* $f \mid H(f)$ *and* $I(P, \mathcal{C} \cap \ell_P) = p^v$, *then*

$$B_q \leq \frac{1}{2}\{p^v(2g-2) + (q+2)d\}. \tag{4.5}$$

THEOREM 4.5 ([20]): *If* (a) $\mathcal{C}$ *is Frobenius non-classical and* (b) $p \nmid m_P(\mathcal{C})$ *for all points* P *of* $\mathcal{C}$, *then*

$$B_q \geq (q-1)d - (2g-2), \tag{4.6}$$

and equality holds if and only if every singular branch of $\mathcal{C}$ *is centred at a point of* $\mathrm{PG}(2,q)$.

EXAMPLE 4.6: Let $q = p^3$, with p an odd prime, and

$$g(X,Y) = (X^p + X)^p + (X^{p+1} + 1)^p X - Y^{p^2+p+1}.$$

Then $\mathcal{C}$ is a projective non-singular Frobenius non-classical plane curve with $\varepsilon = v = p$, Garcia [8]. In fact, both (4.2) and (4.3) hold for

$$s(X,Y) = t(X,Y) = 1, \qquad z_0(X,Y) = X^p + X,$$
$$z_1(X,Y) = X^{p+1} + 1, \qquad z_2(X,Y) = -Y^{p+1}.$$

This shows that the exceptional case (ii) in Theorem 4.4 occurs. Also, the number of $\boldsymbol{F}_q$-rational points of $\mathcal{C}$ is $(p^2+p+1)(p^3-p^2-p+1)$, by Theorem 4.3.

Now, let $\bar{\pi} : \mathcal{C} \to \mathcal{C}^*$ be the rational map defined by $(1,x,y) \mapsto (z_0, z_1, z_2)$. Then $\mathcal{C}^*$ is the dual curve of $\mathcal{C}$. The main properties of $\mathcal{C}^*$ are as follows:

(i) $\mathcal{C}^*$ is a projective singular plane curve defined over $\boldsymbol{F}_q$ birationally equivalent to $\mathcal{C}$;

(ii) $\mathcal{C}^*$ has degree $p^3 + 2p^2 + 2p + 1 = (p^2+p+1)(p+1)$, and genus $g = (p^2+p)(p^2+p-1)/2$;

(iii) $\mathcal{C}^*$ is a Frobenius non-classical plane curve with $\varepsilon = v = p^2$;

(iv) $\mathcal{C}^*$ has only one non-linear branch; it is centred at an $\mathbf{F}_{p^3}$-rational point and has order $p+1$.

Applying Theorem 4.5, we obtain that

$$\begin{aligned} B_{p^3} &= (p^2+p+1)(p+1)(p^3-1) - (p^2+p+1)(p^2+p-2) \\ &= (p^2+p+1)(p-1)(p^3+2p^2+p-1). \end{aligned}$$

In the case $p = 3$, this gives $B_{27} = 1222$, $N_{27} = 208$.

5. - SEGRE'S THEOREM

The following four notions are equivalent for $n \geq k$:

1. (CODING THEORY) a *maximum distance separable* (MDS) linear code C of length n, dimension k and hence minimum distance $d = n - k + 1$, that is, an $[n, k, n-k+1]_q$ code over $\boldsymbol{F}_q$;

2. (MATRIX THEORY) a $k \times (n-k)$ matrix A with entries in $\boldsymbol{F}_q$ such that every minor is non-zero;

3. (VECTOR SPACE) a set K' of n vectors in $V(k,q)$, the vector space of k dimensions over $\boldsymbol{F}_q$, with any k linearly independent;

4. (PROJECTIVE SPACE) an *n-arc* in $PG(k-1,q)$, that is, a set K of n points with at most $k-1$ in any hyperplane of the projective space of $k-1$ dimensions over $\boldsymbol{F}_q$.

To show the equivalence of these four concepts, consider a generator matrix G for such a code C in canonical form:

$$\begin{matrix} & & & & & n & & \\ k & \begin{bmatrix} 1 & 0 & \dots & 0 & a_{11} & \dots & a_{1,n-k} \\ 0 & 1 & \dots & 0 & a_{21} & \dots & a_{2,n-k} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & a_{k1} & \dots & a_{k,n-k} \end{bmatrix} \end{matrix} = G.$$

Since C has minimum distance $n-k+1$, any linear combination of the rows of G has at most $k-1$ zeros; that is, considering the columns of G as a set K' of n vectors in $V(k,q)$, any k are linearly independent. Regarding the columns of G as a set K of points of $\mathrm{PG}(k-1,q)$ means that no k lie in a hyperplane; equivalently, any k points of K are linearly independent. This, in turn, implies that every minor of A is non-zero.

For given k and q, let $M(k,q)$ be the maximum value of n for such a code. Then

$$M(k,q) = k+1 \text{ for } q \leq k.$$

A suitable set of vectors in $V(k,q)$ is

$$(1,0,\dots,0),\ (0,1,0,\dots,0),\ \dots,(0,\dots,0,1),(1,1,\dots,1);$$

that is, for $q \leq k$, every element of $V(k,q)$ is a linear combination of at most $k-1$ of these $k+1$ vectors.

The Main Conjecture MC_k for MDS Codes, always taking $q > k$, is the following.

CONJECTURE 5.1:

$$M(k,q) = \begin{cases} q+2 & \text{for } k=3 \text{ and } k=q-1 \text{ both with } q \text{ even}, \\ q+1 & \text{in all other cases.} \end{cases}$$

It will be convenient to have the notation $m(k-1,q) = M(k,q)$.

Since the problem involves linear dependence, the projective space setting is more economical than the vector space setting, since the redundant scalars are factored out.

A *normal rational curve* in $\mathrm{PG}(r,q)$ is the projective image of the curve

$$\mathcal{T}_r = \{(1,t,\dots,t^r) \mid t \in \boldsymbol{F}_q \cup \{\infty\}\}.$$

Segre [28] enunciated three problems:

I. For given k and q, what is the maximum value of n such that an n-arc exists in the space $\mathrm{PG}(k-1,q)$? What are the n-arcs corresponding to this value of n?

II. Are there values of k and q with $q > k$ such that every $(q+1)$–arc of $\mathrm{PG}(k-1,q)$ is a normal rational curve?

III. For given k and q with $q > k$, what are the values of n ($\leq q$) such that each n–arc is contained in a normal rational curve of $\mathrm{PG}(k-1,q)$? In how many such curves is the n–arc contained?

An n–arc is *complete* if it is maximal with respect to inclusion; that is, it is not contained in an $(n+1)$–arc. Implicit in Problem III is Problem IV, which may be expressed as follows.

IV. What are the values of n for which a complete n–arc exists in $\mathrm{PG}(k-1,q)$? In particular, what is the size of the second largest complete arc in $\mathrm{PG}(k-1,q)$?

From above, $m(r,q)$ is the maximum size of an arc in $\mathrm{PG}(r,q)$; also, let $m'(r,q)$ denote the size of the second largest complete arc in $\mathrm{PG}(r,q)$. Then an n–arc in $\mathrm{PG}(r,q)$ with $n > m'(r,q)$ is contained in an $m(r,q)$–arc. This is an important inductive tool.

THEOREM 5.2 (Segre [29]): *Let $\mathcal{K}$ be a k-arc in* $\mathrm{PG}(2,q)$*, and let $\mathcal{K}'$ be its dual.*

(i) *The $kt = k(q+2-k)$ tangents through the points of $\mathcal{K}$ lie on an algebraic envelope Γ' whose dual curve Γ is of degree t or $2t$ according as q is even or odd.*

(ii) *The envelope Γ' contains no bisecant of $\mathcal{K}$ and so no pencil with vertex P in $\mathcal{K}$.*

(iii) *For q odd, the t tangents to $\mathcal{K}$ through a point P of $\mathcal{K}$ each count twice in the intersection of Γ' with the pencil $\mathscr{L}_P$ of lines through P. Dually, each line l of $\mathcal{K}'$ is a tangent at t distinct points of Γ.*

(iv) *For q odd, Γ' may contain components of multiplicity two, but does not consist entirely of double components.*

(v) *The arc $\mathcal{K}$ is incomplete if and only if Γ' has a rational linear component.*

This theorem enables bounds to be obtained for the size of a complete arc by comparing the number of tangents to the arc with a bound for the number of lines in an algebraic envelope or, equivalently, the number of rational points on an algebraic curve. The difficulty is that the curve here is not necessarily irreducible. For details of the argument, see [16, Chapter 10], where details of the theorems in the next section may also be found.

6. - BOUNDS FOR ARCS AND MDS CODES

THEOREM 6.1 (Bose [1]):

$$m(2,q) = \begin{cases} q+1, & q \text{ odd;} \\ q+2, & q \text{ even.} \end{cases}$$

THEOREM 6.2 (Segre [31]):

$$m'(2,q) \le \begin{cases} q - \frac{1}{4}\sqrt{q} + \frac{7}{4}, & q \text{ odd;} \\ q - \sqrt{q} + 1, & q \text{ even.} \end{cases}$$

THEOREM 6.3 ([7], [2], [26], [3]):

$$m'(2,q) = q - \sqrt{q} + 1, \quad q = 2^b,\ q \textit{ square},\ q > 4.$$

Equality in Theorem 6.3 is obtained by taking a cyclic projectivity $\mathfrak{T}$ of $\mathrm{PG}(2,q)$, that is, a projectivity acting as a single cycle on its points and so of order q^2+q+1. As

$$q^2 + q + 1 = (q + \sqrt{q} + 1)(q - \sqrt{q} + 1),$$

the orbits of the group $\langle \mathfrak{T}^{q+\sqrt{q}+1} \rangle$ have size $q - \sqrt{q} + 1$. These orbits are complete arcs for q square with $q > 4$.

CONJECTURE 6.4: For $q = p^b,\ q$ square, $q > 9$,

$$m'(2,q) = q - \sqrt{q} + 1.$$

Apart from the case q even, Conjecture 6.4 is also true for $q = 25$.

THEOREM 6.5 (Voloch [37], [38]): *For* $q = p^b$,

$$m'(2,q) \le \begin{cases} \frac{44}{45}q + \frac{8}{9}, & \text{for } q = p; \\ q - \frac{1}{4}\sqrt{pq} + \frac{29}{16} + 1, & \text{for } b \text{ odd},\ b \ge 3,\ p > 2; \\ q - \sqrt{2q} + 2, & \text{for } b \text{ odd},\ b \ge 3,\ p = 2. \end{cases}$$

THEOREM 6.6 ([17]): *For* $q = p^b,\ p \ge 5$,

$$m'(2,q) \le q - \frac{1}{2}\sqrt{q} + 5.$$

THEOREM 6.7 ([18]): *Let* $q = p^b$ *with* $p \ge 3$, *and let* $q = 3^{2e}$ *when* $p = 3$. *If* $q \ge 23^2$ *and* $q \ne 3^6$ *or* 5^5, *then*

$$m'(2,q) \le q - \frac{1}{2}\sqrt{q} + \frac{5}{2}.$$

Also,

$$m'(2,q) \le \begin{cases} q - 22 & \text{when} \quad q = 5^5; \\ q - 9 & \text{when} \quad q = 3^6; \\ q - 9 & \text{when} \quad q = 23^2; \\ q - 5 & \text{when} \quad q = 19^2. \end{cases}$$

Similar methods also allow a bound for $m''(2,q)$, the size of the third largest complete arc in $\mathrm{PG}(2,q)$.

THEOREM 6.8 ([19]): *For $q = 2^b$, q square,*

$$m''(2,q)\begin{cases} \leq q - 2\sqrt{q} + 6 & \text{for } q \geq 64; \\ = 12 & \text{for } q = 16. \end{cases}$$

Each bound for $m'(2,q)$ implies a result about the Main Conjecture; see [22] for details.

7. - GOPPA'S CONSTRUCTION OF A LINEAR CODE

Let $\mathcal{V}$ be an algebraic curve defined over $\boldsymbol{F}_q$. Let

$$\mathcal{P} = (P_1, \ldots, P_n)$$

be an ordered set of rational point points P_i of $\mathcal{V}$. Let

$$D = P_1 + \ \ldots + P_n,$$

with $P_i \neq P_j$ for $i \neq j$, be the associated divisor. Let

$$E = \sum_{j=1}^{s} m_j Q_j,$$

with $m_j \geq 0$ and $\sum m_j = m$, be an $\boldsymbol{F}_q$ -divisor such that, with $\mathcal{Q} = \{Q_j \mid j = 1, \ldots, s\}$,

$$\mathcal{P} \cap \mathcal{Q} = \emptyset.$$

Let $L(E) =$ be the space of functions associated to E. The evaluation map θ at $\mathcal{P}$ is

$$\theta : L(E) \longrightarrow \left(\mathbf{F}_q\right)^n,$$

given by

$$f \longmapsto (f(P_1), \ldots, f(P_n)).$$

Now,

$$\text{im } \theta = C = C(D,E).$$

is an *algebraic geometry* code.

The Riemann–Roch theorem leads to the following result.

THEOREM 7.1 (Goppa [10]): *The code $C = C(D,E)$ is an $[n,k,d]_q$ code with information rate $R = k/n$ and relative distance $\delta = d/n$. If $n > m > 2g - 2$, then*

(i) $k = m - g + 1$;
(ii) $d \geq n - m$;
(iii) $n - k + 1 - g \leq d \leq n - k + 1$;
(iv) $R + \delta \geq 1 - (g-1)/n$.

EXAMPLE 7.2: Let $F = Z$ and $E = mP_\infty$, where $P_\infty = (0,1,0)$. Also, with $\boldsymbol{F}_q = \{t_1, \ldots, t_q\}$,

$$\mathcal{P} = ((1,t_1,0), \ldots, (1,t_q,0)).$$

So,

$$n = q, \quad k = m+1, \quad d = n-k+1 = n-m,$$

and

$$G = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ t_1 & t_2 & \ldots & t_q \\ \vdots & \vdots & & \vdots \\ t_1^m & t_2^m & \ldots & t_q^m \end{bmatrix} \begin{matrix} 1 \\ Y/X \\ \vdots \\ Y^m/X^m \end{matrix}.$$

This is a Reed–Solomon code and is MDS.

Under the equivalence of an $[n,k,d]_q$ code and a projective $[n,k]$ system of n points in $PG(k-1,q)$ with at most $n-d$ in a hyperplane, this case gives q points in $PG(m,q)$ on a normal rational curve . The system can be extended to include the point $(0,0,\ldots,0,1)$, the remaining rational point on the normal rational curve, and the code can be extended to the MDS code C' by adding the transpose of this vector as an extra column of G. For C',

$$n = q+1, \quad k = m+1, \quad d = n-m = q+2-k = n-k+1.$$

EXAMPLE 7.3: Take $q = 4$ and $F = X^3 + Y^3 + Z^3$. With

$$\begin{array}{lll} P_0 = (0,1,1), & P_1 = (0,1,\omega), & P_2 = (0,1,\omega^2), \\ P_3 = (1,0,1), & P_4 = (1,0,\omega), & P_5 = (1,0,\omega^2), \\ P_6 = (1,1,0), & P_7 = (1,\omega,0), & P_8 = (1,\omega^2,0), \end{array}$$

let $E = 3P_0$ and let $\mathcal{P} = \{P_1, \ldots, P_8\}$. The genus $g = 1$ and $C(D,E)$ has parameters

$$n = 8, \quad k = 3, \quad 5 \le d \le 6.$$

Then, with the functions given evaluated at $P_1, \ldots, P_8$,

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & \omega^2 & \omega & 1 & \omega_2 & \omega \\ \omega & \omega^2 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{matrix} 1 \\ X/(Y+Z) \\ Y/(Y+Z). \end{matrix}$$

As the last row of G reveals a word of weight 5, so $d = 5$. So $C(D,E)$ is an $[8,3,5]$ code.

Theorem 7.1 leads to the question of asymptotic values of R and the related question of asymptotic values of g/n. Let

$$A^+(q) = \limsup_{g\to\infty} N_q(g)/g,$$

$$A^-(q) = \liminf_{g\to\infty} N_q(g)/g.$$

The Hasse–Weil theorem implies that $A^+(q) \leq 2\sqrt{q}$. It was shown by Drinfeld and Vlăduţ [5], using the zeta function, that

$$A^+(q) \leq \sqrt{q} - 1,$$

with equality for q square, [24], [36]. In the other direction, it is now known that

$$A^-(q) > 0;$$

see [6].

REFERENCES

[1] R. C. Bose, *Mathematical theory of the symmetrical factorial design*, Sankhyā, **8** (1947), 107-166.

[2] E. Boros - T. Szönyi, *On the sharpness of theorem of B. Segre*, Combinatorica, **6** (1986), 261-268.

[3] A. Cossidente, *New proof of the existence of* $(q^2 - q + 1)$*−arcs in* $PG(2, q^2)$, J. Geom., **53** (1995), 37-40; Addendum, J. Geom., **59** (1997), 32-33.

[4] A. Cossidente - G. Korchmáros, *The algebraic envelope associated to a complete arc*, Recenti Progressi in Geometria, Rend. Circ. Mat. Palermo Suppl., **51** (1998), 9-24.

[5] V. G. Drinfeld - S. G. Vlăduţ, *The number of points of an algebraic curve*, Functional Anal. Appl., **17** (1983), 53-54.

[6] N. D. Elkies - E. W. Howe - A. Kresch - B. Poonen - J. L. Wetherell, *Curves of every genus with many points. II. Asymptotically good families*, Duke Math. J., **122** (2004), 399-422.

[7] J. C. Fisher - J. W. P. Hirschfeld - J. A. Thas, *Complete arcs in planes of square order*, Combinatorics '84, Ann. Discrete Math., **30**, North Holland, 1986, pp. 243-250.

[8] A. Garcia, *The curves* $y^n = f(x)$ *over finite fields Arch. Math.*, **54** (1990), 36-44.

[9] A. Garcia - J. F. Voloch, *Wronskians and linear independence in fields of prime characteristic*, Manuscripta Math., **59** (1987), 457-469.

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

[11] H. Hasse, *Beweis des Analogons der Riemannsche Vermutung für die Artinschen und F.K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen*, Vorl. Mitt. Nachr. Ges. Wiss. Göttingen I, **42** (1933), 253-262.

[12] H. Hasse, *Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern*, Abh. Math. Sem. Univ., **10** (1934), 325-348.

[13] A. Hefez - J. F. Voloch, *Frobenius nonclassical curves*, Arch. Math., **54** (1990), 263-273.

[14] A. Hefez - J. F. Voloch, *Correction to: "Frobenius nonclassical curves"*, Arch. Math., **57** (1991), 416.

[15] J. W. P. Hirschfeld, *Finite Projective Spaces Of Three Dimensions*, Oxford University Press, Oxford, 1985.

[16] J. W. P. Hirschfeld, *Projective Geometries Over Finite Fields*, Second edition, Oxford University Press, Oxford, 1998.

[17] J. W. P. Hirschfeld - G. Korchmáros, *On the embedding of an arc into a conic in a finite plane*, Finite Fields Appl., **2** (1996), 274-292.

[18] J. W. P. Hirschfeld - G. Korchmáros, *On the number of rational points on an algebraic curve over a finite field*, Bull. Belg. Math. Soc. Simon Stevin, **5** (1998), 313-340.

[19] J. W. P. Hirschfeld - G. Korchmáros, *Arcs and curves over a finite field Finite*, Fields Appl., **5** (1999), 393-408.

[20] J. W. P. HIRSCHFELD - G. KORCHMÁROS, *On the number of solutions of an equation over a finite field*, Bull. London Math. Soc., **33** (2001), 16-24.
[21] J. W. P. HIRSCHFELD - L. STORME - J. A. THAS - J. F. VOLOCH, *A characterization of Hermitian curves*, J. Geom., **41** (1991), 72-78.
[22] J. W. P. HIRSCHFELD - L. STORME, *The packing problem in statistics, coding theory and finite projective spaces: update 2001*, Finite Geometries, Developments in Mathematics, Kluwer, Boston, 2001, pp. 201-246.
[23] J. W. P. HIRSCHFELD - J. A. THAS, *General Galois Geometries*, Oxford University Press, Oxford, 1991.
[24] Y. IHARA, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math., **28** (1981), 721-724.
[25] B. C. KESTENBAND, *Unital intersections in finite projective planes*, Geom. Dedicata, **11** (1981), 107-117.
[26] B. C. KESTENBAND, *A family of complete arcs in projective planes*, Colloq. Math., **57** (1989), 59-67.
[27] H. G. RÜCK - H. STICHTENOTH, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math., **457** (1994), 185-188.
[28] B. SEGRE, *Curve razionali normali e k-archi negli spazi finiti*, Ann. Mat. Pura Appl., **39** (1955), 357-379.
[29] B. SEGRE, *Le geometrie di Galois*, Ann. Mat. Pura Appl., **48** (1959), 1-97.
[30] B. SEGRE, *Arithmetische Eigenschaften von Galois-Räumen I*, Math. Ann., **154** (1964), 195-256.
[31] B. SEGRE, *Introduction to Galois geometries*, Atti Accad. Naz. Lincei Mem., **8** (1967), 133-236.
[32] J.-P. SERRE, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C.R. Acad. Sci. Paris Sér. I, **296** (1983), 397-402.
[33] H. STICHTENOTH, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.
[34] K. O. STÖHR - J. F. VOLOCH, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc., **52** (1986), 1-19.
[35] J. A. THAS, *Complete arcs and algebraic curves in $PG(2,q)$*, J. Algebra, **106** (1987), 451-464.
[36] M. A. TSFASMAN - S. G. VLĂDUŢ - T. ZINK, *Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound Math. Nachr.,* **109** (1982), 21-28.
[37] J. F. VOLOCH, *On the completeness of certain plane arcs*, European J. Combin., **8** (1987), 453-456.
[38] J. F. VOLOCH, *Arcs in projective planes over prime fields*, J. Geom., **38** (1990), 198-200.
[39] A. WEIL, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann, Paris, 1948.

Direttore responsabile: Prof. A. BALLIO - Autorizz. Trib. di Roma n. 7269 dell'8-12-1959
«Monograf» - Via Collamarini, 5 - Bologna