Cubo Matemática Educacional
Vol. 3., N° 1, ENERO 2001

Algebraic curves, differential geometry in positive characteristic and error-correcting codes

E. Ballico

Dept. of Mathematics, Univesità di Trento
38050 Povo (TN) - Italy
e-mail: ballico@science.unitn.it

1 Introduction

The oldest problem in Algebra is solving polynomial equations. The main aim of Algebraic Geometry is the study of the common zeros of finitely many polynomials equations in several variables. In the geometric part of Algebraic Geometry one often uses differenti als, derivatives and other tools from Differential Geometry. However, if we want to work over a field, **K**, of positive characteristic (for instance a finite field) several pathologies arise for the following reason. If $p := \mathrm{char}(\mathbf{K}) > 0$, the $d(x^p)/dx = p\,x^{p-1} = 0$ (because $p = 0$) and hence the non-constant function x^p has identically zero derivative. We will say much more on these strange phenomena in section 3. Finding solutions of polynomial equations over finite fields is important for some applications to coding theory, in particular for the construction and study of linear codes. The aim of section 4 is to try to explain some of the connections between these two topics. Previously, several applications of number theory and algebra to coding theory were known; after all most codes are connected with a finite field. In the references we listed several books (most of them brand new), a few surveys and a very small part of the recent preprints on the subject. Using the web it is easy to find a huge number of recent preprints on this topic and hence to see the popularity of this topic among researchers (mostly pure mathematicians). For an example of quantum error correcting code for quantum computers (if any in the near future!), see page 50 of [CG]. In section 2 we review a few well-known properties of algebraic curves, stressing their arithmetic (e.g. counting the number of their points if the base field is finite) and the fundamental trichotomy between curves of genus 0, curves of genus 1 and curves of genus at least two.

2 Algebraic Curves

Let X be a smooth projective curve defined over a field L. One should think about X as a one-dimensional object, say the generalization of the notions of lines, ellipses, parabolas and hyperbolas. The main discrete invariant of X is its genus, g. The genus is a non negative integer. Indeed, every line, every ellipse, every parabola and every hyperbola corresponds to a smooth curve of genus 0. If the field L is the complex number field $\mathbf{C}$, then we may endowe the complex points, $X(\mathbf{C})$, of X with the euclidean topology. With this topology $X(\mathbf{C})$ is a compact connected orientable two-dimensional topological manifold. $X(\mathbf{C})$ has a unique $\mathbf{C}^\infty$ structure. The algebraic structure on X induces a complex structure, i.e. $X(\mathbf{C})$ is a Riemann Surface. Viceversa, every compact connected Riemann Surface is associated to a unique smooth projective curve defined over the field $\mathbf{C}$. The topological or differentiable classification of all orientable compact connected two-dimensional manifolds is very well-known: every such T is homeomorphic (or diffeomorphic) to a sphere with g handles and g is exactly the genus of X [St]; we have $H_1(T,\mathbb{Z}) \cong \mathbb{Z}^{\oplus 2g}$ and this may be used to define the integer g, i.e. the genus; even the fundamental group $\pi_1(T,P)$ of T is uniquely determined by the genus. Viceversa, $\pi_1(T,P)$ may be used to define the genus, g, because it has $2g$ generators $a_1, b_1, a_2, b_2, ..., a_g, b_g$ with a unique relation $\prod_{1\le i\le g} a_i b_i a_i^{-1} b_i^{-1} = 1$. If $g = 0$, then $X(\mathbf{C})$ is topologically a sphere and the associated Riemann Surface is just $\mathbf{CP}^1$. If $g = 1$, then the Riemann Surface $X(\mathbf{C})$ is called an elliptic curve and the associated topological manifold is a two-dimensional torus $S^1 \times S^1$. There is a deep difference between the 3 cases: $g = 0$, g= 1 or $g \geq 2$. On the topological side, this may be seen looking at their universal covering spaces: $\mathbf{CP}^1$ is simply connected, the universal covering of an elliptic curve is $\mathbf{C}$ as a Riemann Surface (i.e. it has no non-constant holomorphic function), while the universal covering of a smooth curve of genus $g \geq 2$ is biholomorphic to the unit disk $\Delta := \{z \in \mathbf{C} : |z| < 1\}$ ([F], Th. IV.4.5); the last assertion is a famous theorem proved in 1907 independently by Poincaré and Koebe. If a smooth curve defined over an arbitrary field is seen as a plane curve of a certain degree, we have a lot of informations about its genus. Here we need to work with the projective plane $\mathbf{P}^2$, not the affine plane, because a smooth affine curve may have singularities at infinity: think about two parallel affine lines. A smooth plane curve of degree d has genus $(d-1)(d-2)/2$. In particular it has genus 0 if and only if $d = 1$ or $d = 2$ (lines and smooth conics) and it has genus 1 if and only if $d = 3$. If the degree d plane curve Y has some singularities, then the genus, g, of its smooth model is at most $(d-1)(d-2)/2$ and the integer $(d-1)(d-2)/2 - g$ depends only on the number and type of the singularities of Y; for instance if Y has only ordinary nodes and ordinary cusps as singularities, then $(d-1)(d-2)/2 - g$ is the number of singular points of Y.

The three cases $g = 0$,g= 1 and $g \geq 2$ are completely different from several points of view (see [L] for the higher dimensional case and for complex analytic methods, [Ma] for more from the point of view of the arithmetic of algebraic curves). Here we will consider them from the point of view of points defined on certain small field. Let X be a smooth projective curve defined over a field L. If L is algebraically closed, the set X(L) of points of X defined over L is infinite. What happens if L is not algebraically closed ? The set

$X(L)$ may be empty. For instance the plane conic $x^2 + y^2 + 1 = 0$ (or in homogeneous coordinates $x^2 + y^2 + z^2 = 0$) is defined over $\mathbf{R}$ but it has no real point. The most important object associated to X is its canonical line bundle K_X and its dual (i.e. the tangent bundle TX of X). We have $\deg(K_X) = 2g - 2$ and $\deg(TX) = 2 - 2g$. These line bundles are defined over L. If $g = 1$, both are trivial and not very interesting. Line bundles of positive degree may be used to embed the curve in a projective space. If $g = 0$ indeed TX embeds X as a plane conic and the embedding is defined over L. Hence if $g, = 0$ we may see X as a plane conic. As the example of the real conic without real points just given shows, we may have $X(L) = \phi$. Since $\mathbf{P}^1$ is defined over any field, there is at least one genus 0 curve with $X(L) \neq \phi$. We have $\mathbf{P}^1(L) = \mathbf{L} \cup \{\infty\}$. In particular if L is infinite $\mathbf{P}^1(L)$ is infinite, while if L is finite we have $\#(\mathbf{P}^1(L)) = \#(L) + 1$. The next result shows that these are the only two possibilities for the integers $\#(X(L))$ for any smooth curve X with genus 0 defined over a finite field L.

Proposition 2.1. *Let X be a smooth projective curve of genus 0 defined over the field L. If $X(L) \neq \phi$ the X is isomorphic over L to* $\mathbf{P}^1$.

Proof. See X as a plane conic and take $P \in X(L)$. Thus $P \in P^2(L)$ and for every $Q \in P^2(L)$ with $Q \neq P$ there is a unique line $\langle PQ \rangle$ containing P and Q and this line is defined over L. Take any line D of $\mathbf{P}^2$ defined over L and with $P \notin D$. We have $D \cong \mathbf{P}^1$ over L. For every $Q \in D$ the line $\langle PQ \rangle$ intersects the conic X in P and in another point, Q'. If Q is defined over L, then Q' is defined over L because a degree 2 polynomial $f(x) \in L[x]$ with coefficient in L and with one root defined over L has both solutions defined over L. Viceversa, for every $Q' \in (X \backslash \{P\})$ the line $\langle PQ' \rangle$ intersects D in a unique point, Q; if $Q' \in X(L)$, then $\langle PQ' \rangle$ is defined over L and hence Q is defined over L. To the point $P \in X(L)$ we associate as line $\langle PP \rangle$ (which is not defined) the tangent line $T_P X$ to X at P. Since $P \in X(L)$ even $T_P X$ is defined over L because the coefficients of its equation are obtain taking derivatives from the coefficients of the equation of X and the coordinates of P; both may be taken as elements of L. This construction (called the stereographic projection of X from P onto D) induces the isomorphism of X and $\mathbf{P}^1$ and it is defined over L.

In particular by 2.1 over any algebraically closed field there is a unique smooth genus 0 curve: $\mathbf{P}^1$.

Example 2.2. Let X be a genus 1 smooth projective curve defined over the field L and assume $X(L) \neq \phi$. X may be seen as a plane cubic curve $X = \{f(x,y,z) = 0\} \subset \mathbf{P}^2$ with f degree 3 polynomial with coefficients in L. Take $P \in X(L)$ and consider the line $T_P X$ tangent to X at P. If P is a flex for X, i.e. if $T_P X$ has order of contact 3 with X at P, we are stuck. However, if P is not a flex of X we may find another point, Q, of $X(L)$ in the following way. The restriction of $f(x,y,z)$ to $T_P X$ is a degree 3 polinomial, f, on the line $T_P X$ with coefficients in L and with a double root, P, defined over L. Hence f has all three roots defined over L. Since P is not a flex of X, f has at P exactly a double root, i.e. the other root of f defines a point $Q \in X(L)$ with QP. If Q is a flex of X, we stop. If Q is not a flex of X we may continue and find other points of $X(L)$. This is called the tangent method. Similarly, if we know $P, Q \in X(L)$ with $P \neq Q$, the line $\langle PQ \rangle$ is defined over L. If this line is not tangent to the cubic X at P or at Q, then it intersects X at a point different from P and from Q and defined over L. This is called the chordal method.

If we know $O \in X(L)$ with O flex point of the plane cubic X, then we may define in the following way a composition law which make $X(L)$ an abelian group for which O is the zero element. Fix $P, Q \in X(L)$. It is easier to define $-(P+Q)$ for this law. It is the unique point, R, of $X(L)$ such that the points P, Q are collinear; here if $P = Q$ we take as R the third intersection point of the line with X; hence $3P$ is zero if and only if P is a flex point of the cubic X. Now we need to define $-A$ for any $A \in X(L)$. If $A = O$, set $-A = O$. If $A \neq O$, let $-A$ be the third point of intersection of the cubic X with the line $\langle AO \rangle$ which is defined over L.

The fundamental trichotomy (genus 0 or 1 or ≥ 2) is deeply related to $X(L)$ if L is a finite extension of Q or of a function field $\mathbf{F}_q(x)$ in one variables over $\mathbf{F}_q$; here $\mathbf{F}_q$ denotes the field with q elements and q must be a power of a prime. If $g = 0$ by 2.1 either $X(L) = \phi$ or $X(L) \cong \mathbf{L} \cup \{\infty\}$ is infinite. If $g = 1$ and L is a finite extension of Q either $X(L) = \phi$ or $X(L)$ is a finitely generated abelian group (Mordell (1922) - Weil (1928) theorem). If $g \geq 2$, then $X(L)$ is finite; this is a famous theorem of Faltings (1983) for L finite extension of Q and a famous theorem of Grauert (1966) and Manin (1963) for L finitely generated extension of $\mathbf{C}$ or of $\mathbf{F}_p$.

Now we will give a proof due to Ax of a classical theorem of Chevalley - Warning (see [Gr], p. 11, or [Ax]. For the proof we need the following two lemmas.

Lemma 2.3. *Let L be any field and u: $\mathbf{F}_q^* \to L^*$ be any non-trivial homomorphism between the multiplicative groups of the two fields. Then $\sum_{x \in \mathbf{F}_q^*} h(x) = 0$.*

Proof. By hypothesis there is $y \in \mathbf{F}_q^*$ such that $h(y) \neq 0$. Since the multiplication by y is a bijection of onto itself, we have $\sum_{x \in \mathbf{F}_q^*} h(x) = \sum_{x \in \mathbf{F}_q^*} h(xy) = (\sum_{x \in \mathbf{F}_q^*} h(x))h(y)$. Since L has no zero-divisor and $h(y) \neq 1$, this implies
$\sum_{x \in \mathbf{F}_q^*} h(x) = 0$.

Lemma 2.4. *For every integer $m > 0$ we have $\sum_{x \in \mathbf{F}_q} x^m = -1$ if $q-1$ divides m and $\sum_{x \in \mathbf{F}_q} x^m = 0$ if $q-1$ does not divide m.*

Proof. The function $x \mapsto x^m$ is a homomorphism of the multiplicative group $\mathbf{F}_q^*$ into itself. Since $\mathbf{F}_q^*$ is a cyclic group of order $q-1$, this homomorphism is the identity if and only if m is divisible by $q-1$. If m is divisible by $q-1$ the sum is $q-1$ because 0 goes to 0 and $\#(\mathbf{F}_q^*) = q-1$. If m is not divisible by m, use lemma 2.3.

Theorem 2.5. (Chevalley - Warning) *Let f be a polynomial in n variables with coefficients in the finite field $\mathbf{F}_q$ with $q = p^e$, $e \geq 1$. Set $d := deg(f)$. Let $N(f)$ be the number of distinct zeros of f in $\mathbf{F}_q$. If $n > d$, then $N(f) \equiv 0 \; mod(p)$.*

Proof. We have $\#(\mathbf{F}_q^n) = q^n \equiv 0 \; mod(p)$. Let $N(f)'$ be the residue class of $N(f) \; mod(p)$. Since $\mathbf{F}_q^*$ is a cyclic group of order $q-1$, for every $n-$ple x$\in \mathbf{F}_q^n$ we have $1 - f(x)^{q-1} = 1$ if $f(x) = 0$ and $1 - f(x)^{q-1} = 0$ if $f(x) \neq 0$. Thus, taking the sum $\sum$ of all elements of $\mathbf{F}_q^n$ we obtain $N(f)' = \sum(1 - f(x)^{q-1}) = -\sum f(x)^{q-1}$. We will see the last sum,

$\mathbf{S}(f)$, as an element of $\mathbf{F}_q$ and we must prove that this element is zero if $deg(f) < n$. Since $deg(f(x)^{q-1}) = d(q-1)$, $\mathbf{S}(f)$ is a $\mathbf{F}_q$-linear combitation of terms $\mathbf{S}(m)$ with m monomial of degree $d(q-1)$ in n variables $x_1, ..., x_n$. Thus it is sufficient to prove that $\mathbf{S}(m) = 0$ for every monomial m of degree $d(q-1)$. If $m = x_1^{a_1} .....x_n^{a_n}$, then $\mathbf{S}(m) = \prod_{1 \leq i \leq n} \sum_{x_i \in \mathbf{F}_i} x_i^{a_i}$. Since $d < n$, at least one exponent, say a_i is at most $q-1$. By Lemma 2.4 the i-th factor of $\mathbf{S}(m)$ is 0 and hence we conclude.

In Projective Geometry homogeneous polynomials are the main topic. Hence it is worthwhile to single-out the following corollary of Theorem 2.5.

Corollary 2.6. *Let f be a homogeneous polynomial in n variables with coefficients in the finite field* $\mathbf{F}_q$. *Set* $d := deg(f)$. *If* $n > d$, *then* f *has a non-trivial zero, i.e. a zero* $\neq (0, ...0)$.

Proof. Since f is homogeneous, it has (0,....,0) as a zero. By Theorem 2.5 f must have at least $p-1$ other zeros, where $p := char(\mathbf{F}_q)$.

Now we summarize some results on the integers $\#(X(L))$ when X is a smooth curve defined over a finite field. Let X be a smooth projective geometrically irreducible curve of genus g defined over $\mathbf{F}_q$. A. Weil proved that $|\#(X(\mathbf{F}_q)) - q - 1| \leq 2g(q)^{1/2}$ (the so-called Riemann's hypothesis for curves). Ihara [Ih] proved that, when g is large compared to q, this bound can be significantly improved. Set $n := \#(X(\mathbf{F}_q))$. Given X and a so-called linear system $|L|$ on X one can construct a linear code over $\mathbf{F}_q$ (see [M1] , [LV] or [MV]). This code is a matrix on vectors in the space $\mathbf{F}_q^n$. Thus the larger is n, the better is the code. This explains one reason for the interest in finding X with large $\#(X(\mathbf{F}_q))$. If $q = p^e$ and $x = p^f$ with $f \geq e$, then $\mathbf{F}_x$ is an extension of $\mathbf{F}_q$. The curve X is defined even over $\mathbf{F}_x$, too, and hence the integer $\#(X(\mathbf{F}_x))$ is defined. We may consider the set $\mathbf{S}(q,g)$ of all integers $\#(X(\mathbf{F}_q))$, where q is fixed while X varies among all smooth curves of genus g defined over $\mathbf{F}_q$. Let $\mathbf{N}_q(g)$ be the minimum of $\mathbf{S}(q,g)$. Set $A(q) := limsup_{g \to \infty} \mathbf{N}_q(g)/g$. We used $\mathbf{N}_q(g)/g$ in the definition of $A(q)$ by Weil's extimate $|\#(X(\mathbf{F}_q)) - q - 1| \leq 2g(q)^{1/2}$. Serre proved that $A(q) > 0$ for every q [Se]. Drinfeld and Vladut proved that $A(q) \leq (q)^{1/2} - 1$ for every q [DV]. Several people independently proved that if q is a square, then $A(q) = (q)^{1/2} - 1$ (see for instance [GS]). Thus a general upper bound for $A(q)$ is known but, unless q is a square, nobody knows the exact value of $A(q)$. We stress that this was started before the applications to coding theory: the theory is nice, the results are amusing and it was a big help to be able say in the introduction of the paper that " this paper improves a Theorem of Serre " (see lines 15-20 of the first column of the interview with J.-P. Serre listed as [CF]). This seems to be occured quite often in the interraltions between pure and applied mathematics. However, sometimes applied mathematics (and quite often theoretical physics) had applications to pure mathematics.

3 Differential Geometry in positive characteristic

If $f(x_0, ..., x_n)$ is a polynomial in $n+1$ variables over a field $\mathbf{K}$, one can take the partial derivatives $\partial f / \partial x_i$ just formally imposing the following rules: $\partial(x_i)/\partial x_i = 1$ $\partial(x_j)/\partial x_i =$

0 if $i \neq j$. $\partial(c)/\partial x_i = 0$ for every $c \in K$ (i.e. the elements of **K** are constants) and the Leibniz rule $\partial(uv)/\partial x_i = u\partial(v)/\partial x_i + v\partial(u)/\partial x_i$ for all polynomials u, v. In this way one can use differentials and similar stuff even in Algebraic Geometry. However, if $char(\mathbf{K}) = p > 0$, then a strange phenomenon occurs. By Leibniz rule we obtain $\partial(f^p)/\partial x_i = pf^{p-1}(\partial(f)/\partial x_i) = 0$ (just because $p = 0$) for every polynomial f. This means that there are non-constant polynomials such that all their partial derivatives are identically zero. Using derivatives as in Differential Topology one can define tangent spaces, differentials of regular maps between smooth varieties and so on. However, if $char(\mathbf{K}) = p > 0$ we have just seen the existence of non-constant maps (say $f^p : K^{\oplus(n+1)} \to K$ for any polynomial f) such that their differentials are identically zero.

Now we will introduce a famous example.

Example 3.1. (The Fermat hypersurface). We fix a base field **K** with $char(\mathbf{K}) = p > 0$. Consider the homogeneous polynomial $f_{n,m} \in K[x_0, ..., x_n]$ defined by $f_{n,m}(x_0, ..., x_n) = \sum_{0 \leq i < n} x_i^m$. Let $X(n, m, p)$ the hypersurface $\{f_{n,m} = 0\}$ of the projective space $\mathbf{P}^n$ (over **K**). If m is divisible by p we have $f_{n,m} = f_{n,m/p^p}$. Hence if m is divible by p the hypersurface $X(n, m, p)$ is just $X(n, m/p, p)$ counted with multiplicity p. Iterating this trick we see that it is sufficient to study the Fermat hypersurfaces $X(n, m, p)$ for all m with $(m, p) = 1$. First we well check that every such hypersurface is smooth. Take $P \in X(n, m, p)$, say $P = (a_0, ..., a_n)$, with $a_i \neq 0$ for at least one index i and $(m, p) = 1$. We have $\partial(f_{n,m})/\partial x_i(P) = m\ a_i^{m-1} \neq 0$ (by the assumption $(m, p) = 1$). Thus the hypersurface $X(n, m, p)$ is smooth at P; here we use as in Differential Topology the Jacobian criterion or Inverse Function Theorem to check if a zero-locus of a $\mathbf{C}^\infty$ function is smooth.

In [Be] A. Beauville proved the following stricking characterization of smooth hypersurfaces of $\mathbf{P}^n$, $n \geq 3$, such that all their general hyperplane section are isomorphic. It is quite easy to prove that in characteristic 0 the only possible ones are the hyperplanes and the hyperquadrics, and this explains the restriction $d \geq 3$ in the statement.

Theorem 3.2. [Be] *Let $X \subset \mathbf{P}^n$, $n \geq 3$, be a smooth hypersurface of degree $d \geq 3$. The following conditions are equivalent:*

(i) All smooth hyperplane sections of X are isomorphic;

(ii) for every $P \in \mathbf{P}^n$ the polar divisor of P in X, i.e. the set of all $Q \in X$ such that the tangent hyperplane $T_Q X$ contains P is a hyperplane section of X;

(iii) $char(\mathbf{K}) > 0$, $d-1$ is a power of $char(\mathbf{K})$ and all the partial derivatives $\partial f/\partial x_i, 0 \leq i \leq n$, of the equation f of X are powers of linear forms;

(iv) $p = char(\mathbf{K}) > 0$, $d - 1$ is a power, q, of $char(\mathbf{K})$ and X is projectively equivalent to the Fermat hypersurface $X(n, q+1, p)$.

Fix an algebraically closed field **K** and let $Y \subset \mathbf{P}^2$ an irreducible curve defined over **K**. We consider the following bad properties which Y may have.

(a) Every smooth point of Y is a flex point, i.e. for every $P \in Y_{reg}$ the tangent line to Y at P has order of contact at least 3 with Y at P.

(b) Every tangent line of Y is bitangent (or worse), i.e. for a general $P \in Y_{reg}$ there is $Q \in Y_{reg}$ such that $Q \neq P$ and $Q \in T_P Y$.

(c) There is $O \in \mathbf{P}^2$ such that $O \in T_P Y$ for every $P \in Y_{reg}$; if such point O exists, Y is called a strange curve and O is called the strange point of Y.

Obviously for (c) we have to exclude the case Y a line, because every point of a line D would be a strange point for D.
The properties (a), (b) and (c) may be stated for any irreducible curve Y of $\mathbf{P}^n, n \geq 3$. For an irreducible curve $D \subset \mathbf{P}^n$, $n \geq 3$, with D spanning $\mathbf{P}^n$, a further pathology in principle could arise:

(d) A general secant line to D is trisecant (or worst), i.e. if you take two general points P, Q of D, the line $\langle PQ \rangle$ meets D at least in another point; more generally, if you take $n-1$ general points $P_1, ..., P_{n-1}$ of D, their linear span $\langle P_1, ..., P_{n-1} \rangle$ is a codimension two linear subspace of $\mathbf{P}^n$; if the linear space $\langle P_1, ..., P_{n-1} \rangle$ contains at least another point of D, D is called very strange.

It is known that (a), (b), (c) and (d) are not possible if $char(\mathbf{K}) = 0$ (see 3.3 for a proof for pathology (c)), but that there are examples if $char(\mathbf{K}) > 0$. Here we summarize a few results and examples concerning the pathologies (a), (b), (c) and (d).

(3.3) Let $Y \subset \mathbf{P}^n$ be a strange curve with O as strange point. The linear projection from O into $\mathbf{P}^{n-1}$ has differential everywhere zero. Thus by Sard's Theorem in characteristic 0 these map must be constant, i.e. either Y is a line or $char(\mathbf{K}) > 0$. Assume $char(\mathbf{K}) = 2$ and consider the smooth plane conic $X = \{x_0 x_1 + x_2^2 = 0\}$. Since $char(\mathbf{K}) = 2, \partial(x_2^2)/\partial x_2 = 0$. Thus for every $P \in X$, say $P = (a_0, a_1, a_2)$ the tangent line $T_P X$ has equation $a_0 x_1 + a_1 x_0 = 0$ and hence it contains the point $O := (0;0;1)$. Thus O is a strange point of X. Lluiss proved that this is the only example of smooth strange curve $X \subset \mathbf{P}^n$, $n \geq 2$, which is not a line; the proof of Lluiss' Theorem given in [L] gives the following generalization: smooth conic in characteristic 2 are the only strange curves (apart from the lines) which have only "very mild singularities" (e.g. only ordinary double points). However, if we allow bad singularities, then for every prime p there is a huge number of strange singular curves defined in characteristic p. The possible equations of all strange plane curves are given in [BH], § 3.

(3.4) A very strange curve is strange ([R], Lemma 1.1). In particular Luiss' Theorem stated in 3.3 shows that there is no smooth very strange curve in $\mathbf{P}^n$, $n \geq 3$, and no very strange curve exists in characteristic 0 (see 3.3). Every very strange curve has pathology (a) ([R], Prop. 2.1). For examples of very strange curves for all integers $n \geq 3$ and all prime p, see [R], Example 1.2.

(3.5) Let $X \subset \mathbf{P}^n$ be a smooth curve such that for a general $P \in X$ the tangent line $T_P X$ intersects X at least at another point. H. Kaji proved that X must have genus 0 or genus 1 and that only very few elliptic curves admit an embedding in $\mathbf{P}^n$ with such property. The construction of the examples in the genus 1 case made in [Ka] is very delicate. Kaji's Theorem implies that no smooth plane curve has pathology (b).

(3.6) Pathology (a) cannot arise in characteristic 0, but for all integers $n \geq 2$ and all primes p there are examples of integral (and even smooth) curves in $\mathbf{P}^n$ with pathology (a); the curve is called non-reflexive if it has pathology (a) (see [K], Ch. I, for examples and a nice historical introduction).

4 Goppa codes

Information theory was created by C. E. Shannon around 1948. Its aim is the improvement or the preservation of transmission signals in space or in time. Usually, a signal to be transmitted must be encoded and then, at the arrival, must be decoded. Hence coding theory is fundamental. The theory was developed following two distinct approaches.

Shannon started the study of the probabilistic approach and proved the existence of codes whose transmission rate is as near as you want to the capacity of the transmission channel and which make as small as you want the probability of errors. However, his theorem is not constructive and gives no idea for the construction of such good codes. Golay and Hamming started an algebraic approach for the explicit construction of efficient codes. Choose your preferred mathematical theory. There are good chances that it was used to construct codes. One may construct error correcting codes using several algebraic tools (for instance finite groups of permutations), algebraic and geometrical methods related to finite fields, finite geometries, combinatorics, trees, packing of spheres, and so on.

The main problems of coding theory are optimization problems. It is desiderable to achieve simultaneously a high transmission speed and a large fraction of correctable errors whereby the coding and decoding algorithms should admit simple machine realization and have a short working time. Of course, all these demands are contradictory. The mathematical theory of asymptotic properties of codes establishes the bounds of the achievable. A very important problem for the real life is generating good codes by means of algorithms which are fast. The computational aspects of the implementation of the algebro-geometric Goppa codes (finding a good curve X, a good " linear system " on X and finding points on X) are studied in [MV], Ch. II. These data may be constructed in polynomial time. However, it turns out that Goppa codes corresponding to a certain class of curves (the so - called modular curves) have good asymptotic parameters only for sufficiently large q, where q is the number of elements of the field which is the base for your code. In particular with these curves one cannot obtain good binary codes ($q = 2$).

An error-control code is a mapping of one set of sequences, say of " symbols ", into another set, by means of the controlled addition of redundancy in such a way that the additional redundancy can be used to detect and/or correct any errors which may occur during storage or transmission of the sequences. The aim is to protect the information contained in the original sequence as much possible, but to retrieve as efficiently as possible the informations from the trasmited data (decoding). To make efficiently this part it is essential to put some structure on these data, otherwise one would have to storage everything. Some codes are bases on group theory, but here we will consider only codes bases on linear algebra, the so-called linear codes. A linear code over the finite field $\mathbf{F}_q$ with q elements is a linear subspace, V, of $(\mathbf{F}_q)^n$; if it has dimension k, it is called a $[n,k]$−code.

The Hamming distance $d(x,y)$ of two elements $x := (x_1, ..., x_n)$ and $y := (y_1, ..., y_n)$ of $(\mathbf{F}_q)^n$ is the number of indices i with $x_i \neq y_i$. If any two elements of V are sufficiently distant for the Hamming metric, then a certain number of transmission errors may be detected. For instance if $d(x,0) \geq 2k + 1$ for all $x \in (V \setminus \{0\})$ and we receive an element

$y \in (\mathbf{F}_q)^n$ with $d(y, V) \leq k$, there is a unique $z \in V$ for which $d(y, z) = d(y, V)$ and we may consider that z was the true message. In this sense we have an error-correcting code. A linear $[n, k]-$code V over $\mathbf{F}_q$ is just the image of a linear map $L : (\mathbf{F}_q)^k \rightarrow (\mathbf{F}_q)^n$ with $rank(L) = k$ and L just corresponds to a $k \times n$ matrix A with elements of $\mathbf{F}_q$ as coefficients and $rank(A) = k$. Around 1980 a visionary Russian electrical engineer discovered that the theory of algebraic curves (and their jacobians) over finite fields can be used to construct valuable codes, now named Goppa codes ([G1]). These codes where proved to give better asymptotic bounds on the asymptotic properties of codes than the conjectural ones made by coding theorists ([TVZ]) and this created an enormous turmoil among coding theorists and compelled them to study algebraic curves.

We recall very briefly the definition and the main properties of the Goppa codes which may be defined without using Algebraic Geometry ([LV], pp. 22-24). Fix a monic polynomial $g(x) \in \mathbf{F}_{q^n}[x]$, say $g(x) = \sum_{0 \leq i \leq t} g_i x^i$ and n distinct elements $L := (c_0, ..., c_{t-1})$ of $(\mathbf{F}_q)^n$. We assume $g_t \neq 0$, i.e. set $t := deg(g(x))$. The Goppa code $\Gamma(L, g)$ with Goppa polynomial $g(x)$ is the set of all words $(c_0, c_1, ..., c_{n-1}) \in (\mathbf{F}_q)^n$ such that $\sum_{0 \leq i \leq n-1} c_i/(x - g_i) \equiv 0 \ mod(g(x))$, i.e. such that the numerator of the left hand side of the congruence (written as $a(x)/b(x)$ with $a(x)$ and $b(x)$ polynomials) is divisible by $g(x)$. The parity check matrix for the Goppa code $\Gamma(L, g)$ is the $t \times n$ matrix $H = (h_{ij})$ with $h_{ij} = h_{j-1} g_{j-1}^i$. By [LV], Theorems 5.6 and 5.7 at p. 23, the Goppa code $\Gamma(L, g)$ has dimension at least $n - mt$ and minimum distance at least $t + 1$; if $g(x)$ has no multiple root, then $\Gamma(L, g)$ has minimum distance at least $2t + 1$. It is proven in [LV], p. 24, that Goppa codes have the following very nice property. To state it we need to introduce the entropy function H_q. Set $H_q(0) := 0$ and for $0 < x < (q - 1)/q$ set $H_q(x) := x \ log_q(q - 1) - x \ log_q x - (1 - x) \ log_q(1 - x)$, where log_q is the logarithm in base q. There exists a sequence of Goppa codes over $\mathbf{F}_q$ with information rate tending to $1 - H_q(\delta)$, i.e. whose rate tends to the so - called Gilbert - Varshamov bound.

These Goppa codes correspond to the genus 0 case of the following more general construction [LV], pp. 55-65). Let X be a smooth projective geometrically irreducible curve of genus g defined over $\mathbf{F}_q$. Fix n distinct points $P_1, ..., P_n$ of and set $D := P_1 + ... + P_n$. Thus D is a positive divisor of degree n. Let G be a positive divisor whose support is disjoint from D and $L(G)$ be the corresponding complete linear system. The linear map $\alpha : L(G) \rightarrow (\mathbf{F}_q)^n$ defined by $\alpha(f) := (f(P_1), ..., f(P_n))$ define a linear code $C(D, G)$: the Goppa code associated to X, D and G. The dimension $dim(Im(\alpha))$ of the code $C(D, G)$ is given by $dim(Im(\alpha)) = dim(L(G)) - dim(Ker(\alpha)) = dim(L(G)) - dim(L(G - D))$. Since $L(G - D) = \{0\}$ if $deg(G) < deg(D) = n$, we have $dim(Im(\alpha)) = dim(L(G))$ if $deg(G) < n$. If a word $\alpha(f)$ has $n - d$ coordinates $\neq 0$, say $f(P_{i_1}) = ... = f(P_{i_{n-d}}) = 0$, then the divisor $(f) + G - P_{i_1} - ... - P_{i_{n-d}}$ is effective, where (f) is the principal divisor associated to the rational function f. Hence, taking degrees, we obtain $deg(G) - n + d \geq 0$. Thus the minimum distance of $C(G, D)$ is at least $n - deg(G)$.

Referencias

[Ax] **J. Ax**, *Zeros of polynomials over finite fields*, Am. J. Math. 86, 255-261, (1964).

[BH] **V. Bayer and A. Hefez**, *Strange curves*, Comm. Algebra 19, 3041-3059, (1991).

[Be] **A. Beauville**, *Sur les hypersurfaces dont les sections hyperplanes sont à module constant*, in: The Grothendieck Festschrift Volume I, pp. 121-133, Progress in Math. 86, Birkhäuser, (1990).

[CK] **R. Calderbank and W. M. Kantor**, *The geometry of two-weight codes*, Bull. London Math. Soc. 18, 97-122, (1986).

[CFM] **A. Campillo, J. I. Farran and C. Munuera**, *On the parameters of algebraic geometry codes related to Arf semigroups*, preprint math. NT/9911025.

[CG] **N. Cerf and N. Gisin**, *Les promesses de l' information quantique*, La Recherche 237 , 46-53, (2000).

[DV] **V. G. Drinfeld and S. G. Vladut**, *Number of points of an algebraic curve*, Functional Analysis 17 (1983), 53-54; English translation of Funksional'-nyi Analiz i Ego Prilozhenia 17, 68-69, (1983).

[F] **J. I. Farran**, *Rational points, genus and asymptotic behaviour in reduced algebraic curves over finite fields*, preprint math. AG/9910149.

[GS] **A. Garcia and H. Stichtenoth**, *A tower of Artin-Schreier extensions of functions fields attaining the Drinfeld-Vladut bound*, Invent. Math. 121, 211-222, (1995).

[G1] **V. D. Goppa**, *Codes on algebraic curves*, Soviet Math. Dokl. 24 (1981), 170-172; English translation of Dokl. Akad. Nauk SSSR 259, 1289-1290, (1981).

[Gr] **M. J. Greenberg**, *Lectures on forms in many variables*, W. A. Benjamin, Inc., (1969).

[G2] **V. D. Goppa**, *Geometry and Codes, Mathematics and its Applications*, vol. 24, Kluwer, Dordrecht, (1991).

[HLP] **T. Hoholdt, J. H. van Lint and R. Pellikaan**, *Algebraic Geometry Codes*, in: Handbook of Coding Theory, V. Pless, W. C. Huffman and R. A. Brualdi, Eds., pp. 871-961 (vol. 1), Elsevier, Amsterdam, (1998).

[Ih] **Y. Ihara**, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo 28, 721-724, (1991).

[Ka] **H. Kaji**, *On the Gauss map of space curves in characteristic p*, II, Compositio Math. 78, 261-269, (1991).

[K] **S. L. Kleiman**, *Tandency and duality*, in: Proceedings of the 1984 Vancouver Conference in Algebraic Geometry, pp. 163-225, CMS Conference Proceedings, vol. 6, (1986).

[KWZ] **A. Kresch, J. L. Wetherell and M. E. Zieve**, *Curves of every genus with many points, I: abelian and toric families*, preprint math. AG/9912069.

[L] **D. Laksov**, *Indecomposability of the restricted tangent bundle*, Astérisque 87/88, 207-219, (1981).

[La] **S. Lang**. *Hyperbolic and diophantine analysis*, Bull. Amer. Math. Soc. 14, 159-205, (1986).

[LV] **J. H. van Lint and G. van der Geer**, *Introduction to coding theory and algebraic geometry*, Birkhäauser, (1988).

[MV] **Y. I. Manin and S. G. Vladut**, *Linear codes and modular curves*, J. Soviet Math. 30. 2611-2643, (1985).

[Ma] **B. Mazur**, *Arithmetic on curves*, Bull. Amer. Math. Soc. 14, 207-259, (1986).

[M1] **C. Moreno**, *Algebraic Curves over Finite Fields*, Cambridge Tracts in Math. vol. 97, Cambridge University Press, Cambridge, (1991).

[M2] **C. Moreno**, Review of Ref. [Pr], Bull. Amer. Math. Soc. 36, 399-404, (1999).

[Pr] **O. Pretzel**, *Codes and algebraic curves*, Oxford Lecture Series in Mathematics and Its Applications, Clarendon Press, Oxford, (1998).

[R] **J. Rathmann**, *The uniform position principle for curves in characteristic p*, Math. Ann. 276, 565-579, (1987).

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

[St] **S. A. Stepanov**, *Codes on Algebraic Curves*, Kluwer Academic Publishers, (1999).

[S] **H. Stichtenoth**, *Algebraic Functions Fields and Codes*, Springer Universitext, Springer, (1993).

[Sti] **J. Stillwell**, *Classical Topology and Combinatorial Group Theory*, Graduate Texts in Math. 75, Springer-Verlag, (1980).

[TVZ] **M. A. Tsfaman, S. G. Vladut and Th. Zink**, *On Goppa codes which are better than the Varshamov - Gilbert bound*, Math. Nachr. 109, 21-28, (1982).