Generalized Reed-Solomon codes from algebraic geometry

Citation for published version (APA):
van Lint, J. H., & Springer, T. A. (1987). Generalized Reed-Solomon codes from algebraic geometry. *IEEE Transactions on Information Theory*, *33*(3), 305-309. https://doi.org/10.1109/TIT.1987.1057320

DOI:
10.1109/TIT.1987.1057320

Document status and date:
Published: 01/01/1987

Document Version:
Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Generalized Reed–Solomon Codes from Algebraic Geometry

J. H. VAN LINT AND T. A. SPRINGER

Abstract—A few years ago Tsfasman *et al.*, using results from algebraic geometry, showed that there is a sequence of codes which are generalizations of Goppa codes and which exceed the Gilbert–Varshamov bound. We show that a similar sequence of codes (in fact, the duals of the previous codes) can be found by generalizing the construction of Reed–Solomon codes. Our approach has the advantage that it uses less complicated concepts from algebraic geometry.

I. Introduction

In 1982 Tsfasman *et al.* [19] published a paper with an extremely exciting result, namely, the existence of a sequence of codes which generalize the idea of Goppa codes (cf. [15, p. 108]) over $\mathbb{F}_q$ (with $q = p^{2r}$) and the minimum distances of which *exceed the Gilbert–Varshamov bound* for $q \geq 49$. For this paper they received the IEEE Information Theory Group Paper Award for 1983. Since the results depend heavily on methods and results from algebraic geometry, or more particularly, the theory of algebraic curves, the paper was not easily accessible to many coding theorists.

Since then, several expository papers have appeared [1], [6]–[8], [10], [14], [16], [18] which have made the main idea considerably clearer. This paper is another attempt to simplify the situation by taking a different approach. The Goppa codes are considered as generalizations of Reed–Solomon (RS) codes. This avoids the use of differentials and residues. It is likely that Tsfasman *et al.* are aware of this easier approach (cf., e.g., [13]). Actually, our codes are the *duals* of the codes described in [19]; cf. Section VII. We remark that in 1975 Delsarte [3] observed the strong connection between the original Goppa codes and Reed–Solomon codes.

In Section II we repeat the definition of an extended Reed–Solomon code over $\mathbb{F}_q$ and then *reformulate* this definition in terminology which leads in a natural way to the generalization. In Section III we list the definitions and results from algebraic geometry which we need, and we give a few examples. The reader who is not familiar with algebraic geometry should nevertheless be able to read this section. Section IV gives the "*generalized Reed–Solomon*" *codes*. We obtain the parameters of these codes (dimension, minimum distance) and in Section V we only briefly go into the asymptotics which show that these codes exceed the Gilbert–Varshamov bound (since the calculations are exactly the same as those in [18]).

In Section VI we treat an example. We regret that difficulties remain; for example, it is not possible (yet) to explain the projective curves (which are used in the construction) in an elementary way.

Section VII requires knowledge of the original approach. We show that the two sequences of codes are duals.

II. Reed–Solomon Codes

We repeat one of the standard descriptions of an extended Reed–Solomon code over $\mathbb{F}_q$ (cf. [15, p. 85]). Let $\mathbb{F}_q = \{\alpha_0, \alpha_1, \cdots, \alpha_{q-1}\}$. Consider the set L of all polynomials $f(x)$ of degree $< k$ in $\mathbb{F}_q[x]$. The code C of length $n = q$ is defined by

$$C := \{c = (f(\alpha_0), f(\alpha_1), \cdots, f(\alpha_{q-1})) | f(x) \in L\}. \tag{2.1}$$

Since a polynomial of degree l has at most l zeros in $\mathbb{F}_q$, we see that C has minimum distance $d = n - k + 1$, which is the best possible, i.e., C is a maximum distance separable (MDS) code (cf. [15, p. 54]). Therefore, C is a good starting point for a sequence of good codes.

We now reformulate this definition in terminology which will make the generalization quite natural. Let F be the algebraic closure of $\mathbb{F}_q$. Consider the projective line X over F. As usual, points on X are described by homogeneous coordinates (x, y) where (x, y) and $(\lambda x, \lambda y), 0 \neq \lambda \in F$, denote the same point. Points on X with coordinates in $\mathbb{F}_q$ are called *rational* points. Of course, they are the points

$$P_i := (\alpha_i, 1), \qquad 0 \leq i \leq q-1$$

and

$$Q := (1, 0)$$

(the so-called point at infinity). Let $\mathscr{L}$ be the set of rational functions on X which are defined at each P_i, with coefficients in $\mathbb{F}_q$, and which have a pole of order less than k in the point Q and no other poles.

A rational function has the form $a(x, y)/b(x, y)$, where $a(x, y)$ and $b(x, y)$ are homogeneous polynomials of the

Manuscript received September 26, 1985; revised August 18, 1986. This work was partially presented at the 1985 IEEE Symposium, Brighton, England.

J. H. van Lint is with the Department of Mathematics and Computing Science, Eindhoven University of Technology, PO Box 513, 5600 MB, Eindhoven, The Netherlands.

T. A. Springer is with the Department of Mathematics, University of Utrecht, Budapestlaan 6, Utrecht, The Netherlands.

IEEE Log Number 8611420.

same degree. If L is the set defined, then we clearly have

$$\mathscr{L} = \{f(x/y) | f(x) \in L\}.$$

Therefore, the code C, defined by (2.1), is also given by

$$C = \left\{ \left(f(P_0), f(P_1), \cdots, f(P_{q-1}) \right) | f \in \mathscr{L} \right\}. \quad (2.2)$$

III. Facts from Algebraic Geometry

Most of what we shall need can be found in introductory textbooks on algebraic geometry, e.g., in [5]. For a more algebraic approach see [2]. Let F, as before, be the algebraic closure of $\mathbb{F}_q$. Let X be an irreducible nonsingular *projective curve* in N-dimensional projective space over F (we do not give a precise definition since we hope the concept is intuitively clear). Let g be the *genus* of X (cf. [5, p. 196]; for the reader who is not familiar with the term genus, it suffices to know that it is an integer which, for a given curve, can be calculated). We give a few simple examples.

Example A: In the plane $\mathbb{C}^2$ consider the curve with equation $y^2 - x^3 + x = 0$ (see Fig. 1 for the real points of this curve). We embed $\mathbb{C}^2$ in projective space $\mathbb{P}^2$ with homogeneous coordinates (x, y, z). Our curve X now has the equation $f(x, y, z) = y^2z - x^3 + xz^2 = 0$; the original representation is obtained by taking $z = 1$. In general, let X be a nonsingular irreducible curve in $\mathbb{P}^2$ defined by an equation $f(x, y, z) = 0$, where f is a homogeneous polynomial of degree d. Then the genus of X is $\frac{1}{2}(d-1)(d-2)$; so the example of Fig. 1 has genus 1 (cf. [5, p. 199]). In particular, the projective line $\mathbb{P}^1$ considered as a curve in $\mathbb{P}^2$ has genus 0; it has the equation $y = 0$.

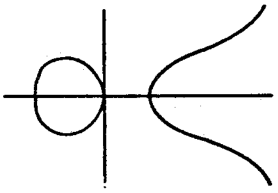

Fig. 1

Example B: Our second example is given only because it has strong connections to the geometry which is the foundation of the remarkable codes of Section IV. (This example can be skipped.) An *elliptic curve* X in $\mathbb{P}^2$ is defined by a cubic equation of the form

$$4x^3 - axz^2 - bz^3 - y^2z = 0$$

(we assume that the characteristic p of F is not 2 or 3 and, furthermore, that $\Delta = a^3 - 27b^2 \neq 0$).

Over $\mathbb{C}$ these curves are dealt with via the theory of elliptic functions. As in Example A, we have a curve of genus 1. Elliptic curves are particularly interesting because they can be given the structure of an Abelian group (cf. [5, p. 124]). Choose $(0,0,1)$ as zero element. Addition is defined as follows: if $\xi \in X, \eta \in X$, then $-(\xi + \eta)$ is the third point of intersection of the line through ξ and η with X. This group structure plays an essential role in the analysis of the so-called "supersingular" elliptic curves which lead to Theorem 1.

We return to the essentials which we shall use. Let X be a curve as before. A *divisor* D on X is simply a formal sum

$$D = \sum n_p \cdot P$$

where P runs through the points of X, $n_p \in \mathbb{Z}$, and $n_p = 0$ for all but finitely many points P. The integer $\sum n_p$ is called the *degree* of D.

Let f be a rational function (not identically 0) defined on the curve X. If $P \in X$, we say that f has *order n* ($n > 0$) in P if f has a zero of multiplicity n in P, and we say f has order $-n$ if P is a pole of order n for f. If f is defined at P and $f(P) \neq 0$, then the order of f in P is 0. We give an example.

Example C: Consider the algebraic closure F of $\mathbb{F}_4$ and let X be the curve in $\mathbb{P}^2$ with equation $x^3 + y^3 + z^3 = 0$. Consider the point $Q = (0,1,1)$ on X, and let f be the rational function $x/(y+z)$. To understand the behavior of f at Q, we shall have to represent the function differently. To this end, we observe that on the curve X we have $(y + z) = x^3/(y^2 + yz + z^2)$.

Therefore, f can be given by

$$f(x, y, z) = (y^2 + yz + z^2)/x^2.$$

Since the numerator of this expression is not zero in Q, it is clear why we say that f has order -2 in Q. Similarly, f has order 1 in the points $(0, \omega, 1)$, $(0, \bar{\omega}, 1)$, where we use the notation $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$.

If $D = \sum n_p P$ is a divisor, then we define the linear space $\mathscr{L}(D)$ of rational functions on X to be the set of all functions f such that the order of f at each point P of X is $\geq -n_p$. It is easy to see [5, p. 192] that

$$\mathscr{L}(D) = \{0\} \text{ if the degree of } D \text{ is negative.} \quad (3.1)$$

The main theorem used in the proof is the *Riemann-Roch theorem* [5, p. 210] and in fact the weaker version known as Riemann's theorem [5, p. 196] suffices. This theorem tells us the dimension $l(D)$ of the space $\mathscr{L}(D)$:

$$l(D) \geq \text{degree}\,(D) - g + 1, \quad (3.2)$$

with equality if degree $(D) > 2g - 2$.

In the application in the next section the divisor D will have $n_p \neq 0$ only for points P which are rational (i.e., they have coordinates in $\mathscr{F}_q$). In this case there is an analog of $\mathscr{L}(D)$ which is a vector space over $\mathbb{F}_q$ (rational functions which have values in $\mathbb{F}_q$ at the points where $n_p \neq 0$). It is known that (3.1) and (3.2) remain valid in that case (cf., e.g., [20, ch. VIII, theorem 10] or [2]). The results treated above are enough to understand the construction in Section IV. For the asymptotics of Section V we need an actual sequence of projective curves X. If the curve X has $n+1$ rational points and genus g, then we define

$$\gamma := g/n.$$

The following theorem was proved in [19].

Theorem 1: Let $q = p^{2r}$. There exists a sequence of curves over $\mathbb{F}_q$ such that

$$\gamma \to (q^{1/2} - 1)^{-1} =: \bar{\gamma} \text{ for } n \to \infty.$$

We remark that Drinfeld and Vlădut [4] have shown that $\liminf \gamma \geq (q^{1/2} - 1)^{-1}$, ($q$ arbitrary). Thus we cannot improve on the theorem. (Also see [12], [16], [18].)

IV. Generalized Reed–Solomon Codes

Again let X be an irreducible nonsingular projective curve in $\mathbb{P}^N$, and let $P_1, P_2, \cdots, P_n$ and Q be the *rational* points on X. We choose an integer m such that

$$2g - 2 < m < n. \tag{4.1}$$

Generalizing (2.2) we define a code C over $\mathbb{F}_q$ by

$$C := \{(f(P_1), \cdots, f(P_n)) | f \in \mathscr{L}(mQ)\} \tag{4.2}$$

where the space $\mathscr{L}(mQ)$ is taken over $\mathbb{F}_q$.

If a codeword is $\mathbf{0}$, then the corresponding function f is in the space $\mathscr{L}(mQ - \Sigma_{i=1}^n P_i)$, and then (3.1) implies that $f = 0$. Therefore, the code C has the same dimension as the space $\mathscr{L}(mQ)$. So we find from (3.2) and (4.1) that

$$k := \dim C = m - g + 1. \tag{4.3}$$

Similarly, if a codeword has weight w, i.e., $f(P_i) = 0$ for $n - w$ values of i, then the corresponding function f is in a space $\mathscr{L}(D)$ where D is a divisor of degree $m - n + w$. Therefore, (3.1) shows that the minimum distance d of C satisfies

$$d \geq n - m. \tag{4.4}$$

In this way we have given the construction and the parameters of a large class of codes.

How good a code from this class is depends on the choice of the curve X. If we take X to be the projective line $\mathbb{P}$, then we find our starting point of Section II.

V. Asymptotics

In the construction of Section IV let X run through the sequence of projective curves mentioned in Theorem 1. For each curve X we can still choose m according to (4.1). We thus obtain a sequence of codes. We are interested in the asymptotic behavior of the rate $R := k/n$ and the parameter $\delta := d/n$ as n tends to infinity. From (4.3) and (4.4) we find

$$R = k/n > \frac{m}{n} - \gamma \geq 1 - \gamma - \delta. \tag{5.1}$$

The Gilbert–Varshamov bound states that a sequence of codes exists such that

$$\lim_{n \to \infty} \sup R \geq 1 - H_q(\delta) \tag{5.2}$$

where

$$H_q(x) := x \log_q(q - 1) - x \log_q x - (1 - x) \log_q(1 - x)$$

for

$$0 < x < (q - 1)/q.$$

From (5.1) we find

$$\lim_{n \to \infty} \sup R \geq 1 - \bar{\gamma} - \delta. \tag{5.3}$$

An easy calculation shows that if $q \geq 49$, the line given by the right-hand side of (5.3) intersects the curve given by the right-hand side of (5.2). For the details we refer to [18]. If the points of intersection correspond to $\delta = \delta_1$ resp. $\delta = \delta_2$, then for values of δ between these bounds our sequence of codes exceeds the Gilbert–Varshamov bound.

VI. An Example

The introductory example in Section II was the "curve" $\mathbb{P}$ of genus 0. We now consider as an example a plane curve, which in a sense is the next member of our sequence. Let $q = r^2$ be a square (as before). If we consider $\mathbb{F}_q$ as a quadratic extension of $\mathbb{F}_r$, then $\bar{x} := x^r$ is the conjugate of x. Consider the curve X in $\mathbb{P}^2$ with equation

$$x^{r+1} + y^{r+1} + z^{r+1} = 0, \text{ i.e., } x\bar{x} + y\bar{y} + z\bar{z} = 0, \tag{6.1}$$

a so-called Hermitean curve. For $q = 4$, the Example C of Section III is of type (6.1). As remarked in Example A of Section III, this curve has genus $g = \frac{1}{2}r(r - 1) = \frac{1}{2}(q - \sqrt{q})$.

To apply our theory we must now calculate the number of rational points of X. (This is well-known; cf. [11, p. 102].) In this case this is an easy exercise. If $z = 0$, then in (6.1) we may take $y = 1$, and we find $r + 1$ solutions for x. If none of x, y, z are 0, then we may take $z = 1$. Let α be primitive in $\mathbb{F}_q$. If $\beta \in \mathbb{F}_q \setminus \{0, 1\}$, then $\beta = \alpha^{i(r+1)}$ and hence $y^{r+1} = \beta$ has $r + 1$ solutions. Fixing β similarly yields $r + 1$ solutions for x. So X has $(r - 2)(r + 1)^2 + 3(r + 1)$ rational points, i.e., x has $q\sqrt{q} + 1$ rational points. As in (4.1) we take

$$q - \sqrt{q} < m < q\sqrt{q}. \tag{6.2}$$

By the method of Section IV we find a code C with length $n = q\sqrt{q}$, dimension $k = m - g + 1$, and minimum distance $d \geq n - m = n - k - g + 1$.

Although this code is no longer MDS, it is usually better than the corresponding RS code with the same rate. For instance, if we take $q = 16$, then a rate $\frac{1}{2}$ extended RS code (length 16) has $d = 9$ and the code treated above with rate $\frac{1}{2}$ (i.e., $m = 37$) has length 64 and $d = 27$. On practically any channel this is a far better code.

Let us now look at (6.1) for the case $q = 4$. We write $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$. The nine rational points of X are given as

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	Q
x	1	1	1	1	1	1	0	0	0
y	0	0	0	$\bar{\omega}$	ω	1	$\bar{\omega}$	ω	1
z	$\bar{\omega}$	ω	1	0	0	0	1	1	1

In this case $g = 1$. First we take $m = 2$. By (4.3) the code C has dimension 2. We must find two functions which are a basis of $\mathscr{L}(2Q)$. One of them is the function which is identically 1, which yields $\mathbf{1}$ as a basis vector for C. The other function must be defined on X with exception of Q, where it has a pole of order 2. In Example C of Section III we saw that $x/(y+z)$ is such a function. This yields the following generator for C

$$G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \omega & \bar{\omega} & 1 & \omega & \bar{\omega} & 1 & 0 & 0 \end{pmatrix},$$

and indeed, we see that $d = 6$ as predicted by (4.4). Similarly, if we take $m = 3$, then we must add a row to G_2, corresponding to a function which has a pole of order 3 in Q. We leave it to the reader to check (see Section III, Example C) that $y/(y+z)$ is such a function. So we find the generator

$$G_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \omega & \bar{\omega} & 1 & \omega & \bar{\omega} & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & \omega & \bar{\omega} \end{pmatrix}.$$

Now $d = 5$ in accordance with (4.4).

VII. The Dual Codes

Consider the code C defined in Section IV. Let the functions $\phi_0 = 1, \phi_1, \cdots, \phi_{k-1}$ be a basis of $\mathscr{L}(mQ)$. Then

$$G = \begin{pmatrix} 1 & 1 & \text{-------} & 1 \\ \phi_1(P_1) & \phi_1(P_2) & \text{-------} & \phi_1(P_n) \\ \phi_{k-1}(P_1) & \phi_{k-1}(P_2) & \text{-------} & \phi_{k-1}(P_n) \end{pmatrix}$$

is a generator matrix for C. Let $s := m - 2g + 1$. Consider s columns of G corresponding to $P_{i_1}, \cdots, P_{i_s}$. By (3.2)

$$l\left(mQ - \sum_{\nu=1}^{s} P_{i_\nu}\right) = m - s - g + 1 = g.$$

This means that the solutions $(\lambda_0, \cdots, \lambda_{k-1})$ of the equations

$$\sum_{j=0}^{k-1} \lambda_j \phi_j(P_{i_\nu}) = 0, \nu = 1, \cdots, s$$

form a space of dimension g.

Therefore, any s columns of G have rank $k - g$, i.e., rank s. So any s columns of G are independent. We have proved that the dual $C^\perp$ of C has minimum distance $d' \geq s + 1$. Clearly, $C^\perp$ has dimension $n - k$.

Consider the asymptotic behavior of the parameters $R' := (n-k)/n$ and $\delta' := d'/n$ for the sequence of codes $C^\perp$ corresponding to the sequence treated in Section V. By the inequalities derived earlier we have

$$R' + \delta' \geq 1 - \gamma,$$

i.e., the sequence of dual codes also exceeds the Gilbert–Varshamov bound! We now compare our codes with those defined in [19]. To understand the following, the reader must be familiar with more algebraic geometry than summarized in Section III. The codes of [19] are also defined by considering the curve X of Section IV. Let $P_1, P_2, \cdots, P_n, Q$ be as before.

We consider $\Omega(\Sigma P_i - mQ)$, the space of *differentials* on X with a zero of multiplicity $\geq m$ at Q and regular except possibly in the points P_i, where a pole of order 1 may occur.

If W is a canonical divisor, then

$$\Omega(\Sigma P_i - mQ) \cong \mathscr{L}(W + \Sigma P_i - mQ)$$

and so by the Riemann–Roch theorem this space has dimension $n - m + g - 1$. In [19] a code C^* is defined by taking as codewords the vectors

$$\Psi = \Psi(\omega) := \left(\operatorname{res}_{P_1}(\omega), \cdots, \operatorname{res}_{P_n}(\omega)\right)$$

where $\omega \in \Omega(\Sigma P_i - mQ)$.

Again, the Riemann–Roch theorem shows that C^* also has dimension $n - m + g - 1$, i.e., it has the same dimension as the code $C^\perp$ treated earlier. Exactly as in Section IV it is shown that C^* has minimum distance $d^* \geq m - 2g + 2$. As remarked in the introduction, we shall show that C^* and $C^\perp$ are equal. Since these two codes have the same dimension, it suffices to show that a word $c \in C$ and a word $\Psi \in C^*$ have inner product 0. Let c correspond to $f \in \mathscr{L}(mQ)$. Then $f\omega$ is a differential in $\Omega(\Sigma P_i)$. By the residue theorem (cf. [9, p. 248]) the sum of the residues of this differential is zero. Because ω has poles of order at most 1 we have

$$0 = \sum_{i=1}^{n} \operatorname{res}_{P_i}(f\omega) = \sum_{i=1}^{n} f(P_i) \cdot \operatorname{res}_{P_i}(\omega) = \sum_{i=1}^{n} c_i \Psi_i,$$

i.e., $(c, \Psi) = 0$. The reader who is familiar with [19] will have seen that we did not introduce a new class of codes. Hopefully, the reader who has more difficulty with the necessary algebraic geometry will consider our approach easier to grasp. The task of constructing the sequence of Theorem 1 in a more elementary way remains.

Acknowledgment

The authors thank H. J. Tiersma for his assistance with Section VII.

References

[1] T. Beth, "Some aspects of coding theory between probability, algebra, combinatorics and complexity theory," in *Combinatorial Theory*, Lecture Notes in Mathematics, vol. 969. New York: Springer.

[2] C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, Mathematical Surveys, vol. VI. New York: Amer. Math. Soc., 1951.

[3] P. Delsarte, "On subfield subcodes of modified Reed–Solomon codes," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 575–576, 1975.

[4] V. D. Drinfeld and S. G. Vlădut, "On the number of points of an algebraic curve" (Russian), *Functional Anal. Appl.*, vol. 17, pp. 68–69, 1983.

[5] W. Fulton, *Algebraic Curves*. Reading: Benjamin Cummings, 1969.

[6] V. D. Goppa, "Codes on algebraic curves," *Soviet Math. Doklady*, vol. 24, pp. 170–172, 1981.

[7] ——, "Algebraic-geometric codes," *Math. USSR Isvestiya*, vol. 21, pp. 75–91, 1983.

[8] ——, "Codes and information," *Russian Math. Surveys*, vol. 39, pp. 87–141.

[9] R. D. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52. New York: Springer Verlag, 1977.

[10] J. W. P. Hirschfeld, "Linear codes and algebraic curves," in *Geometrical Combinatorics*, F. C. Holroyd and R. J. Wilson, Eds. Boston, MA: Pitman, 1984.

[11] ——, *Projective Geometries over Finite Fields*. Oxford Univ. Press, 1979.

[12] Y. Ihara, "Some remarks on the number of rational points of algebraic curves over finite fields," *J. Fac. Sci. Tokyo*, vol. 28, pp. 721–729, 1982.

[13] G. L. Katsman, M. A. Tsfasman, and S. G. Vlădut, "Modular curves and codes with a polynomial construction," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 353–355, 1984.

[14] G. Lachaud, "Les codes geometriques de Goppa," *Séminaire Bourbaki*, no. 641, 1985.

[15] J. H. van Lint, *Introduction to Coding Theory*, Graduate Texts in Mathematics, vol. 86. New York: Springer-Verlag, 1982.

[16] Y. I. Manin, "What is the maximum number of rational points on a curve over $\mathbb{F}_2$?" *J. Fac. Sci. Tokyo*, vol. 28, pp. 715–720, 1981.

[17] J. P. Serre, "Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini," *C. R. Acad. Sc. Paris*, vol. 296, pp. 397–402, 1983.

[18] M. A. Tsfasman, "Goppa codes that are better than the Varshamov–Gilbert bound," *Probl. Inform. Transmission*, vol. 18, pp. 163–165, 1982.

[19] M. A. Tsfasman, S. G. Vlădut, and T. Zink, "Modular curves, Shimura curves and Goppa codes better than the Varshamov–Gilbert bound," *Math. Nachr.*, vol. 109, pp. 21–28, 1982.

[20] A. Weil, *Foundations of Algebraic Geometry*, vol. 29. New York: A.M.S. Colloquium Publ., 1946 and 1962.