Chapter 8
Algebraic Geometry Codes

8.1 Introduction

In order to meet channel capacity, as Shannon postulated, long error-correction codes with large minimum distances need to be found. A large effort in research has been dedicated to finding algebraic codes with good properties and efficient decoding algorithms. Reed–Solomon (RS) codes are a product of this research and have over the years found numerous applications, the most noteworthy being their implementation in satellite systems, compact discs, hard drives and modern, digitally based communications. These codes are defined with non-binary alphabets and have the maximum achievable minimum distance for codes of their lengths. A generalisation of RS codes was introduced by Goppa using a unique construction of codes from algebraic curves. This development led to active research in that area so that currently the complexity of encoding and decoding these codes has been reduced greatly from when they were first presented. These codes are algebraic geometry (AG) codes and have much greater lengths than RS codes with the same alphabets. Furthermore these codes can be improved if curves with desirable properties can be found. AG codes have good properties and some families of these codes have been shown to be asymptotically superior as they exceed the well-known Gilbert–Varshamov bound [16] when the defining finite field $\mathbb{F}_q$ has size $q \geq 49$ with q always a square.

8.2 Motivation for Studying AG Codes

Aside from their proven superior asymptotic performance when the field size $q^2 > 49$, AG codes defined in much smaller fields have very good parameters. A closer look at tables of best-known codes in [8, 15] shows that algebraic geometry codes feature as the best-known linear codes for an appreciable range of code lengths for

M. Tomlinson et al., *Error-Correction Coding and Decoding*,
Signals and Communication Technology,
DOI 10.1007/978-3-319-51103-0_8

different field sizes q. To demonstrate a comparison the parameters of AG codes with shortened BCH codes in fields with small sizes and characteristic 2 is given. AG codes of length n, dimension k have minimum distance $d = n-k-g+1$ where g is called the genus . Notice that $n-k+1$ is the distance of a maximum distance (MDS) separable code. The genus g is then the Singleton defect s of an AG code. The Singleton defect is simply the difference between the distance of a code and the distance some hypothetical MDS code of the same length and dimension. Similarly a BCH code is a code with length n, dimension k, and distance $d = n-k-s+1$ where s is the Singleton defect and number of non-consecutive roots of the BCH code.

Consider Table 8.1, which compares the parameters of AG codes from three curves with genera 3, 7, and 14 with shortened BCH codes with similar code rates. At high rates, BCH codes tend to have better minimum distances or smaller Singleton defects. This is because the roots of the BCH code with high rates are usually cyclically consecutive and thus contribute to the minimum distance. For rates close to half, AG codes are better than BCH codes since the number of non-consecutive roots of the BCH code is increased as a result of conjugacy classes. The AG codes benefit from the fact that their Singleton defect or genus remains fixed for all rates. As a consequence AG codes significantly outperform BCH codes at lower rates. However, the genera of curves with many points in small finite fields are usually large and as the length of the AG codes increases in $\mathbb{F}_8$, the BCH codes beat AG codes in performance. Tables 8.2 and 8.3 show the comparison between AG and BCH codes in fields $\mathbb{F}_{16}$ and $\mathbb{F}_{32}$, respectively. With larger field sizes, curves with many points and small genera can be used, and AG codes do much better than BCH codes. It is worth noting that Tables 8.1, 8.2 and 8.3 show codes in fields with size less than 49.

8.2.1 Bounds Relevant to Algebraic Geometry Codes

Bounds on the performance of codes that are relevant to AG codes are presented in order to show the performance of these codes. Let $A_q(n,d)$ represent the number of codewords in the code space of a code $\mathscr{C}$ with length n, minimum distance d and defined over a field of size q. Let the information rate be $R = k/n$ and the relative minimum distance be $\delta = d/n$ for $0 \leq \delta \leq 1$, then

$$\alpha_q(\delta) = \lim_{n\to\infty} \frac{1}{n} A_q(n, \delta n)$$

which represents the k/n such that there exists a code over a field of size q that has d/n converging to δ [18]. The q-ary entropy function is given by

$$H_q(x) = \begin{cases} 0, & x = 0 \\ x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x), & 0 < x \leq \theta \end{cases}$$

Table 8.1 Comparison between BCH and AG codes in $\mathbb{F}_8$

Rate	AG code in $\mathbb{F}_{2^3}$	Number of points	Genus	Shortened BCH code in $\mathbb{F}_{2^3}$	BCH code in $\mathbb{F}_{2^3}$
0.2500	[23, 5, 16]	24	3	[23, 5, 12]	[63, 45, 12]
0.3333	[23, 7, 14]	24	3	[23, 7, 11]	[63, 47, 11]
0.5000	[23, 11, 10]	24	3	[23, 10, 8]	[63, 50, 8]
0.6667	[23, 15, 6]	24	3	[23, 14, 6]	[63, 54, 6]
0.7500	[23, 17, 4]	24	3	[23, 16, 5]	[63, 56, 5]
0.8500	[23, 19, 2]	24	3	[23, 18, 4]	[63, 58, 4]
0.2500	[33, 8, 19]	34	7	[33, 7, 16]	[63, 37, 16]
0.3333	[33, 11, 16]	34	7	[33, 11, 14]	[63, 41, 14]
0.5000	[33, 16, 11]	34	7	[33, 15, 12]	[63, 45, 12]
0.6667	[33, 22, 5]	34	7	[33, 22, 7]	[63, 52, 7]
0.7500	[33, 24, 3]	34	7	[33, 24, 6]	[63, 54, 6]
0.2500	[64, 16, 35]	65	14	[64, 16, 37]	[63, 15, 37]
0.3333	[64, 21, 30]	65	14	[64, 20, 31]	[63, 19, 31]
0.5000	[64, 32, 19]	65	14	[64, 31, 22]	[63, 30, 22]
0.6667	[64, 42, 9]	65	14	[64, 42, 14]	[63, 41, 14]
0.7500	[64, 48, 3]	65	14	[64, 48, 11]	[63, 47, 11]

Table 8.2 Comparison between BCH and AG codes in $\mathbb{F}_{16}$

Rate	AG code in $\mathbb{F}_{2^4}$	Number of points	Genus	Shortened BCH code in $\mathbb{F}_{2^4}$	BCH code in $\mathbb{F}_{2^4}$
0.2500	[23, 5, 18]	24	1	[23, 4, 11]	[255, 236, 11]
0.3333	[23, 7, 16]	24	1	[23, 6, 10]	[255, 238, 10]
0.5000	[23, 11, 12]	24	1	[23, 10, 8]	[255, 242, 8]
0.6667	[23, 15, 8]	24	1	[23, 14, 6]	[255, 246, 6]
0.7500	[23, 17, 6]	24	1	[23, 16, 5]	[255, 248, 5]
0.8500	[23, 19, 4]	24	1	[23, 18, 4]	[255, 250, 4]
0.2500	[64, 16, 43]	65	6	[64, 16, 27]	[255, 207, 27]
0.3333	[64, 21, 38]	65	6	[64, 20, 25]	[255, 211, 25]
0.5000	[64, 32, 27]	65	6	[64, 32, 19]	[255, 223, 19]
0.6667	[64, 42, 17]	65	6	[64, 41, 13]	[255, 232, 13]
0.7500	[64, 48, 11]	65	6	[64, 47, 10]	[255, 238, 10]
0.8500	[64, 54, 5]	65	6	[64, 53, 7]	[255, 244, 7]
0.2500	[126, 31, 76]	127	20	[126, 30, 57]	[255, 159, 57]
0.3333	[126, 42, 65]	127	20	[126, 41, 48]	[255, 170, 48]
0.5000	[126, 63, 44]	127	20	[126, 63, 37]	[255, 192, 37]
0.6667	[126, 84, 23]	127	20	[126, 84, 24]	[255, 213, 24]
0.7500	[126, 94, 13]	127	20	[126, 94, 19]	[255, 223, 19]

Table 8.3 Comparison between BCH and AG codes in $\mathbb{F}_{32}$

Rate	AG code in $\mathbb{F}_{2^4}$	Number of points	Genus	Shortened BCH code in $\mathbb{F}_{2^4}$	BCH code in $\mathbb{F}_{2^4}$
0.2500	[43, 10, 33]	44	1	[43, 10, 18]	[1023, 990, 18]
0.3333	[43, 14, 29]	44	1	[43, 14, 16]	[1023, 994, 16]
0.5000	[43, 21, 22]	44	1	[43, 20, 13]	[1023, 1000, 13]
0.6667	[43, 28, 15]	44	1	[43, 28, 9]	[1023, 1008, 9]
0.7500	[43, 32, 11]	44	1	[43, 32, 7]	[1023, 1012, 7]
0.8500	[43, 36, 7]	44	1	[43, 36, 5]	[1023, 1016, 5]
0.2500	[75, 18, 53]	76	5	[75, 18, 30]	[1023, 966, 30]
0.3333	[75, 25, 46]	76	5	[75, 24, 27]	[1023, 972, 27]
0.5000	[75, 37, 34]	76	5	[75, 36, 21]	[1023, 984, 21]
0.6667	[75, 50, 21]	76	5	[75, 50, 14]	[1023, 998, 14]
0.7500	[75, 56, 15]	76	5	[75, 56, 11]	[1023, 1004, 11]
0.8500	[75, 63, 8]	76	5	[75, 62, 8]	[1023, 1010, 8]
0.2500	[103, 25, 70]	104	9	[103, 25, 42]	[1023, 945, 42]
0.3333	[103, 34, 61]	104	9	[103, 33, 38]	[1023, 953, 38]
0.5000	[103, 51, 44]	104	9	[103, 50, 28]	[1023, 970, 28]
0.6667	[103, 68, 27]	104	9	[103, 68, 19]	[1023, 988, 19]
0.7500	[103, 77, 18]	104	9	[103, 76, 15]	[1023, 996, 15]
0.8500	[103, 87, 8]	104	9	[103, 86, 10]	[1023, 1006, 10]

The asymptotic Gilbert–Varshamov lower bound on $\alpha_q(\delta)$ is given by,

$$\alpha_q(\delta) \geq 1 - H_q(\delta) \quad \text{for } 0 \leq \delta \leq \theta$$

The Tsfasman–Vladut–Zink bound is a lower bound on $\alpha_q(\delta)$ and holds true for certain families of AG codes, it is given by

$$\alpha_q(\delta) \geq 1 - \delta - \frac{1}{\sqrt{q} - 1} \quad \text{where } \sqrt{q} \in \mathbb{N}/0$$

The supremacy of AG codes lies in the fact that the TVZ bound ensures that these codes have better performance when q is a perfect square and $q \geq 49$.

The Figs. 8.1, 8.2 and 8.3 show the R vs δ plot of these bounds for some range of q.

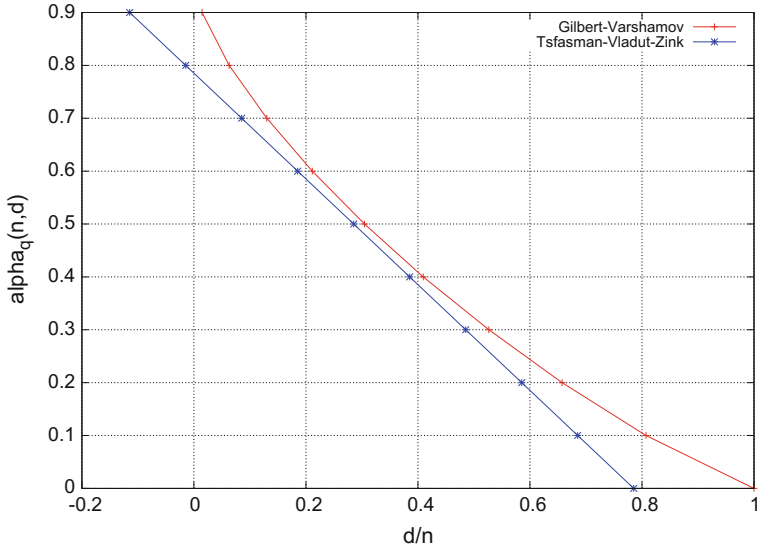

Fig. 8.1 Tsfasman–Vladut–Zink and Gilbert–Varshamov bound for $q = 32$

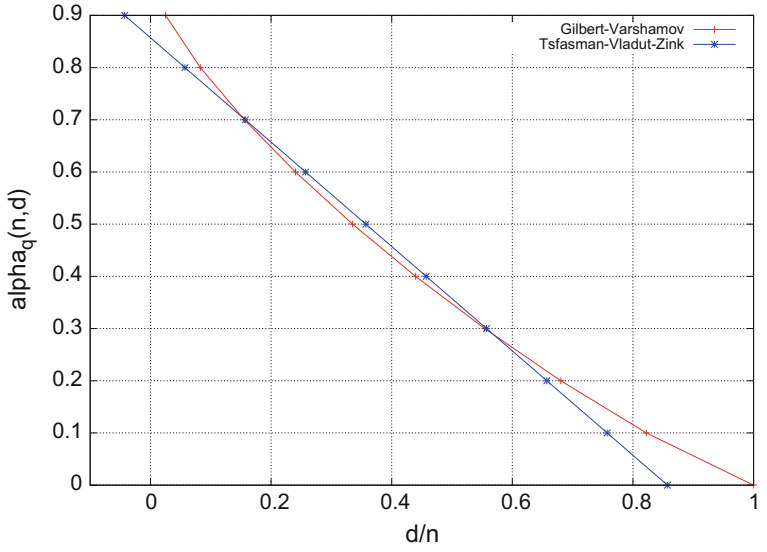

Fig. 8.2 Tsfasman–Vladut–Zink and Gilbert–Varshamov bound for $q = 64$

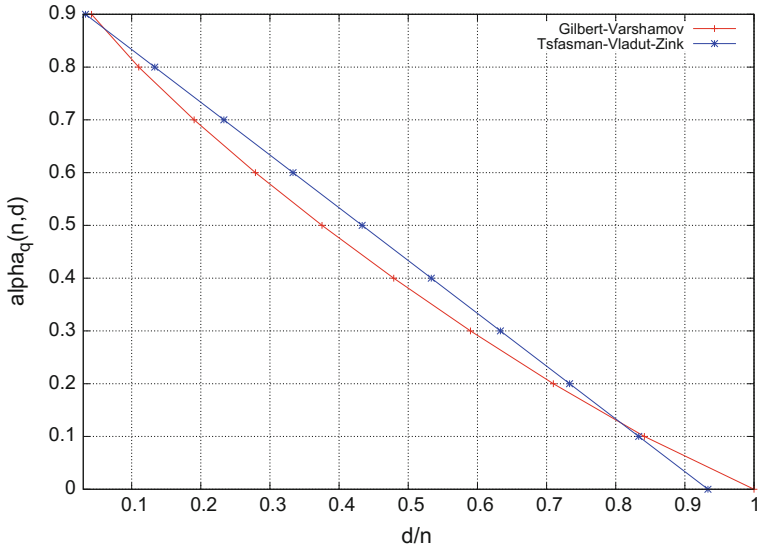

Fig. 8.3 Tsfasman–Vladut–Zink and Gilbert–Varshamov bound for $q = 256$

8.3 Curves and Planes

In this section, the notion of curves and planes are introduced. Definitions and discussions are restricted to two-dimensional planes and all polynomials are assumed to be defined with coefficients in the finite field $\mathbb{F}_q$. The section draws from the following sources [2, 12, 17, 18]. Let $f(x, y)$ be a polynomial in the bivariate ring $\mathbb{F}_q[x, y]$.

Definition 8.1 (*Curve*) A curve is the set of points for which the polynomial $f(x, y)$ vanishes to zero. Mathematically, a curve $\mathscr{X}$ is associated with a polynomial $f(x, y)$ so that $f(P) = \{0 | P \in \mathscr{X}\}$.

A curve is a subset of a plane. There are two main types of planes; the affine plane and the projective plane. These planes are multidimensional, however, we restrict our discussion to two-dimensional planes only.

Definition 8.2 (*Affine Plane*) A two-dimensional affine plane denoted by $\mathbb{A}^2(\mathbb{F}_q)$ is a set of points,

$$\mathbb{A}^2(\mathbb{F}_q) = \{(\alpha, \beta) : \alpha, \beta \in \mathbb{F}_q\} \tag{8.1}$$

which has cardinality q^2.

A curve $\mathscr{X}$ is called an affine curve if $\mathscr{X} \subset \mathbb{A}^2(\mathbb{F}_q)$.

Definition 8.3 (*Projective Plane*) A two-dimensional projective plane $\mathbb{P}^2(\mathbb{F}_q)$ is the algebraic closure of $\mathbb{A}^2$ and is defined as the set of equivalence points,

$$\mathbb{P}^2(\mathbb{F}_q) = \{(\alpha : \beta : 1) : \ \alpha, \beta \in \mathbb{F}_q\} \bigcup \{(\alpha : 1 : 0) : \ \alpha \in \mathbb{F}_q\} \bigcup \{(1 : 0 : 0)\}.$$

A curve $\mathscr{X}$ is said to lie in the projective plane if $\mathscr{X} \subset \mathbb{P}^2(\mathbb{F}_q)$. The points in the projective plane are called equivalence points since for any point $P \in \mathbb{P}^2(\mathbb{F}_q)$,

$$\text{if } f(x_0, y_0, z_0) = 0, \quad \text{then } f(\alpha x_0, \alpha y_0, \alpha z_0) = 0 \qquad \alpha \in \mathbb{F}_q^*, \ P = (x_0 : y_0 : z_0)$$

because $f(x, y, z)$ is homogeneous. The colons in the notation of a projective point $(x : y : z)$ represents this equivalence property.

The affine polynomial $f(x, y)$ is in two variables, in order to define a projective polynomial in three variables, *homogenisation* is used,

$$f(x, y, z) = z^d f\left(\frac{x}{z}, \frac{y}{z}\right) \qquad d = \text{Degree of } \ f(x, y)$$

which turns $f(x, y)$ into a homogeneous[1] polynomial in three variables. An n-dimensional projective polynomial has $n + 1$ variables. The affine space $\mathbb{A}^2(\mathbb{F}_q)$ is a subset of $\mathbb{P}^2(\mathbb{F}_q)$ and is given by,

$$\mathbb{A}^2(\mathbb{F}_q) = \{(\alpha : \beta : 1) : \ \alpha, \beta \in \mathbb{F}_q\} \subset \mathbb{P}^2(\mathbb{F}_q).$$

A projective curve can then be defined as a set of points,

$$\mathscr{X} = \{P : f(P) = 0, \ P \in \mathbb{P}^2(\mathbb{F}_q)\}.$$

Definition 8.4 (*Point at Infinity*) A point on a projective curve $\mathscr{X}$ that coincides with any of the points of $\mathbb{P}^2(\mathbb{F}_q)$ of the form,

$$\{(\alpha : 1 : 0) : \ \alpha \in \mathbb{F}_q\} \cup \{(1 : 0 : 0)\}$$

i.e. points $(x_0 : y_0 : z_0)$ for which $z_0 = 0$ is called a point at infinity.

A third plane, called the bicyclic plane [1], is a subset of the $\mathbb{A}^2(\mathbb{F}_q)$ and consists of points,

$$\{(\alpha, \beta) : \alpha, \beta \in \mathbb{F}_q \setminus \{0\}\}.$$

This plane was defined so as to adapt the Fourier transform to AG codes since the inverse Fourier transform is undefined for zero coordinates.

Example 8.1 Consider the two-dimensional affine plane $\mathbb{A}^2(\mathbb{F}_4)$. Following the definition of $\mathbb{A}^2(\mathbb{F}_4)$ we have,

[1] Each term in the polynomial has degree equal to d.

$$\begin{array}{cccc} (0,0) & (0,1) & (1,0) & (1,1) \\ (1,\alpha) & (\alpha,1) & (1,\alpha^2) & (\alpha^2,1) \\ (\alpha^2,\alpha) & (\alpha,\alpha^2) & (0,\alpha^2) & (0,\alpha) \\ (\alpha^2,0) & (\alpha,0) & (\alpha^2,\alpha^2) & (\alpha,\alpha) \end{array}$$

where α is the primitive element of the finite field $\mathbb{F}_4$. The two-dimensional projective plane $\mathbb{P}^2(\mathbb{F}_4)$ is given by,

Affine Points				Points at Infinity	
$(0:0:1)$	$(0:1:1)$	$(1:0:1)$	$(1:1:1)$	$(0:1:0)$	$(1:0:0)$
$(1:\alpha:1)$	$(\alpha:1:1)$	$(1:\alpha^2:1)$	$(\alpha^2:1:1)$	$(\alpha:1:0)$	
$(\alpha^2:\alpha:1)$	$(\alpha:\alpha^2:1)$	$(0:\alpha^2:1)$	$(0:\alpha:1)$	$(\alpha^2:1:0)$	
$(\alpha^2:0:1)$	$(\alpha:0:1)$	$(\alpha^2:\alpha^2:1)$	$(\alpha:\alpha:1)$	$(1:1:0)$	

Definition 8.5 (*Irreducible Curve*) A curve associated with a polynomial $f(x, y, z)$ that cannot be reduced or factorised is called *irreducible*.

Definition 8.6 (*Singular Point*) A point on a curve is singular if its evaluation on all partial derivatives of the defining polynomial with respect to each indeterminate is zero.

Suppose f_x, f_y, and f_z denote partial derivatives of $f(x, y, z)$ with respect to x, y, and z respectively. A point $P \in \mathscr{X}$ is singular if,

$$\frac{\partial f(x,y,z)}{\partial x} = f_x, \frac{\partial f(x,y,z)}{\partial y} = f_y, \frac{\partial f(x,y,z)}{\partial z} = f_z$$
$$f_x(P) = f_y(P) = f_z(P) = 0.$$

Definition 8.7 (*Smooth Curve*) A curve $\mathscr{X}$ is nonsingular or smooth does not contain any singular points.

To obtain AG codes, it is required that the defining curve is both irreducible and smooth.

Definition 8.8 (*Genus*) The genus of a curve can be seen as a measure of how many bends a curve has on its plane. The genus of a smooth curve defined by $f(x, y, z)$ is given by the Plücker formula,

$$g = \frac{(d-1)(d-2)}{2}, \quad d = \text{Degree of } f(x, y, z)$$

The genus plays an important role in determining the quality of AG codes. It is desirable for curves that define AG codes to have small genera.

Example 8.2 Consider the Hermitian curve in $\mathbb{F}_4$ defined as,

$$f(x, y) = x^3 + y^2 + y \quad \text{affine}$$
$$f(x, y, z) = x^3 + y^2 z + y z^2 \quad \text{projective via homogenisation}$$

It is straightforward to verify that the curve is irreducible. The curve has the following projective points,

$$(0:0:1) \quad (0:1:1) \quad (\alpha:\alpha:1) \quad (\alpha:\alpha^2:1)$$
$$(\alpha^2:\alpha:1) \quad (\alpha^2:\alpha^2:1) \quad (1:\alpha:1) \quad (1:\alpha^2:1) \quad (0:1:0)$$

Notice the curve has a single point at infinity $P_\infty = (0:1:0)$. One can easily check that the curve has no singular points and is thus smooth.

8.3.1 Important Theorems and Concepts

The length of an AG code is utmost the number of points on the defining curve. Since it is desirable to obtain codes that are as long as possible, it is desirable to know what the maximum number of points attainable from a curve, given a genus is.

Theorem 8.1 (Hasse–Weil with Serre's Improvement [2]) *The Hasse–Weil theorem with Serre's improvement says that the number of rational points*[2] *of an irreducible curve, n, with genus g in* $\mathbb{F}_q$ *is upper bounded by,*

$$n \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

Curves that meet this bound are called *maximal* curves. The Hermitian curves are examples of maximal curves. Bezout's theorem is an important theorem, and is used to determine the minimum distance of algebraic geometry codes. It describes the size of the set which is the intersection of two curves in the projective plane.

Theorem 8.2 (Bezout's Theorem [2]) *Any two curves* $\mathscr{X}_a$ *and* $\mathscr{X}_b$ *with degrees of their associated polynomials as m and n respectively, have utmost* $m \times n$ *common roots in the projective plane counted with multiplicity.*

Definition 8.9 (*Divisor*) A divisor on a curve $\mathscr{X}$ is a formal sum associated with the points of the curve.

$$D = \sum_{P \in \mathscr{X}} n_p P$$

where n_p are integers.

[2] A rational point is a point of degree one. See Sect. 8.4 for the definition of the degree of point on a curve.

A zero divisor is one that has $n_p = 0$ for all $P \in \mathscr{X}$. A divisor is called effective if it is not a zero divisor. The support of a divisor is a subset of $\mathscr{X}$ for which $n_p \neq 0$. The degree of a divisor is given as,

$$deg(D) = \sum_{P \in \mathscr{X}} n_p \, deg(P)$$

For simplicity, it is assumed that the degree of points $P \in \mathscr{X}$, i.e. $deg(P)$ is 1 (points of higher degree are discussed in Sect. 8.4). Addition of two divisors $D_1 = \sum_{P \in \mathscr{X}} n_p P$ and $D_2 = \sum_{P \in \mathscr{X}} \acute{n}_p P$ is so defined,

$$D_1 + D_2 = \sum_{P \in \mathscr{X}} (n_p + \acute{n}_p) P.$$

Divisors are simply book-keeping structures that store information on points of a curve. Below is an example the intersection divisor of two curves.

Example 8.3 Consider the Hermitian curve in $\mathbb{F}_4$ defined as,

$$f_1(x, y, z) = x^3 + y^2 z + y z^2$$

with points given in Example 8.2 and the curve defined by

$$f_2(x, y, z) = x$$

with points

$$(0 : 0 : 1) \; (0 : 1 : 1) \; (0 : \alpha : 1) \; (0 : \alpha^2 : 1) \; (0 : 1 : 0)$$

These two curves intersect at 3 points below all with multiplicity 1,

$$(0 : 0 : 1) \; (0 : 1 : 0) \; (0 : 1 : 1).$$

Alternatively, this may be represented using a divisor D,

$$D = (0 : 0 : 1) + (0 : 1 : 0) + (0 : 1 : 1)$$

with n_p the multiplicity, equal to 1 for all the points. Notice that the two curves meet at exactly $deg(f_1) deg(f_2) = 3$ points in agreement with Bezout's theorem.

For rational functions with denominators, points in divisor with $n_p < 0$ are poles. For example, $D = P_1 - 2P_2$ will denote an intersection divisor of two curves that have one zero P_1 and pole P_2 with multiplicity two in common. Below is the formal definition of the field of fractions of a curve $\mathscr{X}$.

Definition 8.10 (*Field of fractions*) The field of fractions $\mathbb{F}_q(\mathscr{X})$ of a curve $\mathscr{X}$ defined by a polynomial $f(x, y, z)$ contains all rational functions of the form

$$\frac{g(x, y, z)}{h(x, y, z)}$$

with the restriction that $g(x, y, z)$ and $h(x, y, z)$ are homogeneous polynomials that have the same degree and are not divisible by $f(x, y, z)$.

A subset (Riemann–Roch space) of the field of fractions of $\mathscr{X}$ meeting certain conditions are evaluated at points of the curve $\mathscr{X}$ to form codewords of an AG code. Thus, there is a one-to-one mapping between rational functions in this subset and codewords of an AG code. The Riemann–Roch theorem defines this subset and gives a lower bound on the dimension of AG codes. The definition of a Riemann–Roch space is given.

Definition 8.11 (*Riemann–Roch Space*) The Riemann–Roch space associated with a divisor D is given by,

$$L(D) = \{t \in \mathbb{F}_q(\mathscr{X}) | (t) + D \geq 0\} \cup 0$$

where $\mathbb{F}_q(\mathscr{X})$ is the field of fractions and (t) is the intersection divisor[3] of the rational function t and the curve $\mathscr{X}$.

Essentially, the Riemann–Roch space associated with a divisor D is a set of functions of the form t from the field of fractions $\mathbb{F}_q(\mathscr{X})$ such that the divisor sum $(t) + D$ has no poles, i.e. $(t) + D \geq 0$.

The rational functions in $L(D)$ are functions from the field of fractions $\mathbb{F}_q(\mathscr{X})$ that must have poles only in the zeros (positive terms) contained in the divisor D, each pole occurring with utmost the multiplicity defined in the divisor D and most have zeros only in the poles (negative terms) contained in the divisor D, each zero occurring with at least the multiplicity defined in the divisor D.

Example 8.4 Suppose a hypothetical curve $\mathscr{X}$ has points of degree one,

$$\mathscr{X} = \{P_1, P_2, P_3, P_4\}$$

We choose a divisor $D = 2P_1 - 5P_2$ with degree -3, and define a Riemann–Roch space $L(D)$. If we randomly select three functions t_1, t_2, and t_3 from the field of fractions $\mathbb{F}_q(\mathscr{X})$ such that they have divisors,

$$(t_1) = -3P_1 + 5P_2 + 4P_4 \ (t_2) = 2P_1 + 4P_2 \ (t_3) = -P_1 + 8P_2 + P_3.$$

$t_1 \notin L(D)$ since $(t_1) + D = -P_1 + 4P_4$ contains negative terms or poles. Also, $t_2 \notin L(D)$ since $(t_2) + D = 4P_1 - P_2$ contains negative terms. However, $t_3 \in L(D)$ since $(t_3) + D = P_1 + 3P_2 + P_3$ contains no negative terms. Any function $t \in \mathbb{F}_q(\mathscr{X})$ is also in $L(D)$ if it has a pole at P_1 with multiplicity at most 2 (with no other poles in common with $\mathscr{X}$) and a zero at P_2 with multiplicity at least 5.

[3] An intersection divisor is a divisor that contains information on the points of intersection of two curves.

The Riemann–Roch space is a vector space (with rational functions as elements) thus, a set of basis functions. The size of this set is the dimension of the space.

Theorem 8.3 (Riemann Roch Theorem [2]) *Let $\mathscr{X}$ be a curve with genus g and D any divisor with degree $(D) > 2g - 2$, then the dimension of the Riemann–Roch space associated with D, denoted by $l(D)$ is,*

$$l(D) = degree(D) - g + 1$$

Algebraic geometry codes are the image of an evaluation map of a Riemann–Roch space associated with a divisor D so that

$$L(D) \rightarrow \mathbb{F}_q^n$$

$$t \rightarrow (t(P_1), t(P_2), \ldots, t(P_n))$$

where $\mathscr{X} = \{P_1, P_2, \ldots, P_n, P_x\}$ is a smooth irreducible projective curve of genus g defined over $\mathbb{F}_q$. The divisor D must have no points in common with a divisor T associated with $\mathscr{X}$, i.e. it has support disjoint from T. For example, if the divisor T is of the form

$$T = P_1 + P_2 + \cdots + P_n$$

then, $D = mP_x$.

Codes defined by the divisors T and $D = mP_x$ are called one-point AG codes (since the divisor D has a support containing only one point), and AG codes are predominantly defined as so since the parameters of such codes are easily determined [10].

8.3.2 Construction of AG Codes

The following steps are necessary in order to construct a generator matrix of an AG code,

1. Find the points of a smooth irreducible curve and its genus.
2. Choose divisors D and $T = P_1 + \cdots + P_n$. From the Riemann–Roch theorem determine the dimension of the Riemann–Roch space $L(D)$ associated with divisor D. This dimension $l(D)$ is the dimension of the AG code.
3. Find $k = l(D)$ linearly independent rational functions from $L(D)$. These form the basis functions of $L(D)$.
4. Evaluate all k basis functions on the points in the support of T to form the k rows of a generator matrix of the AG code.

Example 8.5 Consider again the Hermitian curve defined in $\mathbb{F}_4$ as,

$$f(x, y, z) = x^3 + y^2z + yz^2$$

1. In Example 8.2 this curve was shown to have 8 affine points and one point at infinity. The genus of this curve is given by the Plücker formula,

$$g = \frac{(r-1)(r-2)}{2} = 1$$

   where $r = 3$ is the degree of $f(x, y, z)$.
2. Let $D = 5P_\infty$ where $P_\infty = (0\colon 1\colon 0)$ and T be the sum of all 8 affine points. The dimension of the Riemann–Roch space is then given by,

$$l(5P_\infty) = 5 - 1 + 1 = 5$$

   thus, the AG code has dimension $k = 5$.
3. The basis functions for the space $L(5P_\infty)$ are

$$\{t_1, \ldots, t_k\} = \left\{1, \frac{x}{z}, \frac{x^2}{z^2}, \frac{y}{z}, \frac{xy}{z^2}\right\}$$

   By examining the basis, it is clear that $t_1 = 1$ has no poles, thus, $(t_1) + D$ has no poles also. Basis functions with denominator z have $(t_i) = S - P_\infty$, where S is a divisor of the numerator. Thus, $(t_i) + D$ has no poles. Basis functions with denominator z^2 have $(t_j) = S - 2P_\infty$, where S is a divisor of the numerator. Thus, $(t_j) + D$ also has no poles.
4. The generator matrix of the Hermitian code defined with divisor $D = 5P_\infty$ is thus,

$$G = \begin{bmatrix} t_1(P_1) & \cdots & t_1(P_n) \\ \vdots & \ddots & \vdots \\ t_k(P_1) & \cdots & t_k(P_n) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & \alpha^2 & \alpha^2 & 1 \\ 0 & 1 & 0 & 0 & 0 & \alpha^2 & \alpha & 0 \\ 0 & 0 & 1 & 0 & 0 & \alpha & 1 & \alpha \\ 0 & 0 & 0 & 1 & 0 & \alpha & 0 & \alpha^2 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Example 8.6 Consider the curve defined in $\mathbb{F}_8$ as,

$$f(x, y, z) = x$$

1. This curve is a straight line and has 8 affine points of the form $(0 : \beta : 1)$ and one point at infinity $(0 : 1 : 0)$. The curve is both irreducible and smooth. The genus of this curve is given by the Plücker formula,

$$g = \frac{(r-1)(r-2)}{2} = 0$$

where $r = 1$ is the degree of $f(x, y, z)$. Clearly, the genus is zero since the curve is straight line and has no bends.
2. Let $D = 5P_\infty$, where $P_\infty = (0\colon 1\colon 0)$ and T be the sum of all 8 affine points. The dimension of the Riemann–Roch space is then given by,

$$l(5P_\infty) = 5 - 0 + 1 = 6$$

thus, the AG code has dimension $k = 6$.
3. The basis functions for the space $L(5P_\infty)$ are

$$\{t_1, \ldots, t_k\} = \left\{1, \frac{y}{z}, \frac{y^2}{z^2}, \frac{y^3}{z^3}, \frac{y^4}{z^4}, \frac{y^5}{z^5}\right\}$$

By examining the basis, it is clear that $t_1 = 1$ has no poles, thus, $(t_1) + D$ has no poles also. Basis functions with denominator z have $(t_1) = S - P_\infty$ where $S = (0 : 0 : 1)$ is a divisor of the numerator. The denominator polynomial z evaluates to zero at the point at infinity P_∞ of the divisor D, thus, $(t_1) + D$ has no poles. Basis functions with denominator z^2 have $(t_2) = S - 2P_\infty$ where $S = 2 \times (0 : 0 : 1)$ is a divisor of the numerator. The denominator polynomial z^2 evaluates to zero at the point at infinity P_∞ of the divisor D with multiplicity 2, thus, $(t_2) + D$ has no poles. Basis functions with denominator z^3 have $(t_3) = S - 3P_\infty$ where $S = 3 \times (0 : 0 : 1)$ is a divisor of the numerator. Thus, $(t_3) + D$ also has no poles. And so on.
4. The generator matrix of the code defined with divisor $D = 5P_\infty$ is thus,

$$G = \begin{bmatrix} t_1(P_1) & \cdots & t_1(P_n) \\ \vdots & \ddots & \vdots \\ t_k(P_1) & \cdots & t_k(P_n) \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & 1 \\ 0 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 & 1 \\ 0 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 & 1 \\ 0 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 & 1 \\ 0 & \alpha^5 & \alpha^3 & \alpha & \alpha^6 & \alpha^4 & \alpha^2 & 1 \end{bmatrix}$$

Clearly, this is a generator matrix of an extended Reed–Solomon code with parameters $[3, 6, 8]_8$.

Theorem 8.4 (From [2]) *The minimum distance of an AG code is given by,*

$$d \geq n - degree(D)$$

Thus, the Hermitian code defined by $D = 5P_\infty$ is a $[8, 5, 3]_4$ code. The dual of an AG code has parameters [17],

$$\text{Dimension, } k^\perp = n - degree(D) + g - 1$$
$$\text{Distance, } d^\perp \geq degree(D) - 2g + 2$$

8.4 Generalised AG Codes

Algebraic geometry codes and codes obtained from them feature prominently in the databases of best-known codes [8, 15] for an appreciable range of code lengths for different field sizes q. Generalised algebraic geometry codes were first presented by Niederreiter et al. [21], Xing et al. [13]. A subsequent paper by Ozbudak and Stichtenoth [14] shed more light on the construction. AG codes as defined by Goppa utilised places of degree one or rational places. Generalised AG codes however were constructed by Xing et al. using places of higher degree (including places of degree one). In [20], the authors presented a method of constructing generalised AG codes which uses a concatenation concept. The paper showed that best-known codes were obtainable via this construction. In [4] it was shown that the method can be effective in constructing new codes and the authors presented 59 codes in finite fields $\mathbb{F}_4$, $\mathbb{F}_8$ and $\mathbb{F}_9$ better than the codes in [8]. In [11], the authors presented a construction method based on [20] that uses a subfield image concept and obtained new binary codes as a result. In [19] the authors presented some new curves as well as 129 new codes in $\mathbb{F}_8$ and $\mathbb{F}_9$.

8.4.1 Concept of Places of Higher Degree

Recall from Chap. 8 that a two-dimensional affine space $\mathbb{A}^2(\mathbb{F}_q)$ is given by the set of points

$$\{(\alpha, \beta) : \alpha, \beta \in \mathbb{F}_q\}$$

while its projective closure $\mathbb{P}^2(\mathbb{F}_q)$ is given by the set of equivalence points

$$\{\{(\alpha : \beta : 1)\} \cup \{(\alpha : 1 : 0)\} \cup \{(1 : 0 : 0)\} : \alpha, \beta \in \mathbb{F}_q\}.$$

Given a homogeneous polynomial $F(x, y, z)$, a curve $\mathscr{X}/\mathbb{F}_q$ defined in $\mathbb{P}^2(\mathbb{F}_q)$ is a set of distinct points

$$\mathscr{X}/\mathbb{F}_q = \{T \in \mathbb{P}^2(\mathbb{F}_q) : F(T) = 0\}$$

Let $\mathbb{F}_{q^\ell}$ be an extension of the field $\mathbb{F}_q$, the Frobenius automorphism is given as

$$\begin{aligned} &\phi_{q,\ell} : \mathbb{F}_{q^\ell} \to \mathbb{F}_{q^\ell} \\ &\phi_{q,\ell}(\beta) = \beta^q \qquad \beta \in \mathbb{F}_{q^\ell} \end{aligned}$$

and its action on a projective point $(x : y : z)$ in $\mathbb{F}_{q^\ell}$ is

$$\phi_{q,\ell}((x : y : z)) = (x^q : y^q : z^q).$$

Definition 8.12 (*Place of Degree from* [18]) A place of degree ℓ is a set of ℓ points of a curve defined in the extension field $\mathbb{F}_{q^\ell}$ denoted by $\{T_0, T_1, \ldots, T_{\ell-1}\}$ where each $T_i = \phi^i_{q,l}(T_0)$. Places of degree one are called rational places.

Example 8.7 Consider the curve in $\mathbb{F}_4$ defined as,

$$F(x, y, z) = x$$

The curve has the following projective rational points (points of degree 1),

$$\begin{array}{l} (0:0:1)\ (0:1:1)\ (0:\alpha:1)\ (0:\alpha^2:1) \\ (0:1:0) \end{array}$$

where α is the primitive polynomial of $\mathbb{F}_4$. The curve has the following places of degree 2,

$$\begin{array}{cc} \{(0:\beta:1), (0:\beta^4:1)\} & \{(0:\beta^2:1), (0:\beta^8:1)\} \\ \{(0:\beta^3:1), (0:\beta^{12}:1)\} & \{(0:\beta^6:1), (0:\beta^9:1)\} \\ \{(0:\beta^7:1), (0:\beta^{13}:1)\} & \{(0:\beta^{11}:1), (0:\beta^{14}:1)\} \end{array}$$

where β is the primitive element of $\mathbb{F}_{16}$.

8.4.2 Generalised Construction

This section gives details of the construction of generalised AG codes as described in [21]. Two maps that are useful in the construction of generalised AG codes are now described. Observe that $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^\ell}$ for all $\ell \geq 2$. It is then possible to map $\mathbb{F}_{q^\ell}$ to an ℓ-dimensional vector space with elements from $\mathbb{F}_q$ using a suitable basis. The map π_ℓ is defined as such,

$$\pi_\ell : \mathbb{F}_{q^\ell} \rightarrow \mathbb{F}_q^\ell$$
$$\pi_\ell(\beta) = (c_1\, c_2 \ldots c_\ell) \qquad \beta \in \mathbb{F}_{q^\ell},\ c_i \in \mathbb{F}_q.$$

Suppose $(\gamma_1, \gamma_2, \ldots, \gamma_\ell)$ forms a suitable basis of the vector space $\mathbb{F}_q^\ell$, then $\beta = c_1\gamma_1 + c_2\gamma_2 + \cdots + c_\ell\gamma_\ell$. Finally, the map $\sigma_{\ell,n}$ is used to represent an encoding map from an ℓ-dimensional message space in $\mathbb{F}_q$ to an n-dimensional code space,

$$\sigma_{\ell,n} : \mathbb{F}_q^\ell \rightarrow \mathbb{F}_q^n$$

with $\ell \leq n$.

A description of generalised AG codes as presented in [4, 13, 21] is now presented. Let $F = F(x, y, z)$ be a homogeneous polynomial defined in $\mathbb{F}_q$. Let g be the genus of a smooth irreducible curve $\mathscr{X}/\mathbb{F}_q$ corresponding to the polynomial F. Also, let $P_1, P_2, \ldots, P_r$ be r distinct places of $\mathscr{X}/\mathbb{F}_q$ and $k_i = deg(P_i)$ (deg is degree of). W is a divisor of the curve $\mathscr{X}/\mathbb{F}_q$ such that

$$W = P_1 + P_2 + \cdots + P_r$$

and another divisor G such that the two do not intersect.[4] Specifically, the divisor $G = m(Q - R)$ where $deg(Q) = deg(R) + 1$ for arbitrary[5] divisors Q and R. As mentioned earlier, associated with the divisor G is a Riemann–Roch space $\mathscr{L}(G)$ with $m = deg(G)$) an integer, $m \geq 0$. From the Riemann–Roch theorem (Theorem 8.3) it is known that the dimension of $\mathscr{L}(G)$ is given by $l(G)$ and

$$l(G) \geq m - g + 1.$$

Also, associated with each P_i is a q-ary code C_i with parameters $[n_i, k_i = deg(P_i), d_i]_q$ with the restriction that $d_i \leq k_i$. Let

$$\{f_1, f_2, .., f_k : f_l \in \mathscr{L}(G)\}$$

denote a set of k linearly independent elements of $\mathscr{L}(G)$ that form a basis. A generator matrix for a generalised AG code is given as such,

$$M = \begin{bmatrix} \sigma_{k_1,n_1}(\pi_{k_1}(f_1(P_1))) & \cdots\cdots & \sigma_{k_r,n_r}(\pi_{k_r}(f_1(P_r))) \\ \sigma_{k_1,n_1}(\pi_{k_1}(f_2(P_1))) & \cdots\cdots & \sigma_{k_r,n_r}(\pi_{k_r}(f_2(P_r))) \\ \vdots & \ddots & \vdots \\ \sigma_{k_1,n_1}(\pi_{k_1}(f_k(P_1))) & \cdots\cdots & \sigma_{k_r,n_r}(\pi_{k_r}(f_k(P_r))) \end{bmatrix}$$

[4] This is consistent with the definition of AG codes. The two divisors should have no points in common.

[5] These are randomly chosen places such that the difference between their degrees is 1 and G does not intersect W.

where $f_l(P_i)$ is an evaluation of a polynomial and basis element f_l at a place P_i, π_{k_i} is a mapping from $\mathbb{F}_{q^{k_i}}$ to $\mathbb{F}_q$ and σ_{k_i,n_i} is the encoding of a message vector in $\mathbb{F}_q^{k_i}$ to a code vector in $\mathbb{F}_q^{n_i}$. This is a 3 step process. The place P_i is first evaluated at f_l resulting in an element of $\mathbb{F}_q^{k_i}$. The result is then mapped to a vector of length k_i in the subfield $\mathbb{F}_q$. Finally, this vector is encoded with code with parameters $[n_i, k_i, d_i]_q$.

It is desirable to choose the maximum possible minimum distance for all codes C_i so that $d_i = k_i$ [21]. The same code is used in the map σ_{k_i,n_i} for all points of the same degree k_i, i.e. the code C_j has parameters $[n_j, j, d_j]_q$ for a place of degree j. Let A_j be an integer denoting the number of places of degree j and B_j be an integer such that $0 \leq B_j \leq A_j$.

If t is the maximum degree of any place P_i that is chosen in the construction, then the generalised AG code is represented as a

$$C_1(k; t; B_1, B_2, \ldots, B_t; d_1, d_2, \ldots, d_t).$$

Let $[n, k, d]_q$ represent a linear code in $\mathbb{F}_q$ with length n, dimension k, and minimum distance d, then a generalised AG code is given by the parameters [21],

$$\begin{aligned} k &= l(G) \geq m - g + 1 \\ n &= \sum_{i=1}^{r} n_i = \sum_{j=1}^{t} B_j n_j \\ d &\geq \sum_{i=1}^{r} d_i - g - k + 1 = \sum_{j=1}^{t} B_j d_j - g - k + 1. \end{aligned}$$

Below are two examples showing the construction of generalised AG codes.

Example 8.8 Let $F(x, y, z) = x^3 + xyz + xz^2 + y^2z$ [21] be a polynomial in $\mathbb{F}_2$. The curve $\mathscr{X}/\mathbb{F}_2$ has genus $g = 1$ and $A_1 = 4$ places of degree 1 and $A_2 = 2$ places of degree 2.

Table 8.4 gives the places of $\mathscr{X}/\mathbb{F}_2$ up degree 2. The field $\mathbb{F}_{2^2}$ is defined by a primitive polynomial $s^2 + s + 1$ with α as its primitive element. Points

$$R = (1 : a^3 + a^2 : 1)$$

as a place of degree 4 and

$$Q = (1 : b^4 + b^3 + b^2 : 1)$$

as a place of degree 5 are also chosen arbitrarily while a and b are primitive elements of $\mathbb{F}_{2^4}$ (defined by the polynomial $s^4 + s^3 + s^2 + s + 1$) and $\mathbb{F}_{2^5}$ (defined by the polynomial $s^5 + s^2 + 1$),g respectively. The divisor W is

$$W = P_1 + \cdots + P_6.$$

Table 8.4 Places of $\mathscr{X}/\mathbb{F}_2$

#	P_i	$deg(P_i)$
P_1	$(0:1:0)$	1
P_2	$(0:0:1)$	1
P_3	$(1:0:1)$	1
P_4	$(1:1:1)$	1
P_5	$\{(\alpha:1:1), (\alpha^2:1:1)\}$	2
P_6	$\{(\alpha:\alpha+1:1), (\alpha^2:\alpha:1)\}$	2

The basis of the Riemann–Roch space $\mathscr{L}(2D)$ with $D = Q - R$ and $m = 2$ is obtained with computer algebra software MAGMA [3] as,

$$\begin{aligned} f_1 &= (x^7 + x^3 + x)/(x^{10} + x^4 + 1)y \\ &\quad + (x^{10} + x^9 + x^7 + x^6 + x^5 + x + 1)/(x^{10} + x^4 + 1) \\ f_2 &= (x^8 + x^7 + x^4 + x^3 + x + 1)/(x^{10} + x^4 + 1)y \\ &\quad + (x^8 + x^4 + x^2)/(x^{10} + x^4 + 1) \end{aligned}$$

For the map σ_{k_i,n_i} the codes; c_1 a $[1, 1, 1]_2$ cyclic code for places of degree 1 and c_2 a $[3, 2, 2]_2$ cyclic code places of degree 2 are used. For the map π_2 which applies to places of degree 2, a polynomial basis $[\gamma_1, \gamma_2] = [1, \alpha]$ is used. Only the first point in the place P_i for $deg(P_i) = 2$ in the evaluation of f_1 and f_2 at P_i is utilised. The generator matrix M of the resulting $[10, 2, 6]_2$ generalised AG code over $\mathbb{F}_2$ is,

$$M = \begin{bmatrix} 1\,1\,0\,1\,0\,1\,1\,0\,1\,1 \\ 0\,0\,1\,1\,1\,1\,0\,1\,0\,1 \end{bmatrix}$$

Example 8.9 Consider again the polynomial

$$F(x, y, z) = x^3 + xyz + xz^2 + y^2z$$

with coefficients from $\mathbb{F}_2$ whose curve (with genus equal to 1) has places up to degree 2 as in Table 8.4. An element f of the Riemann–Roch space defined by the divisor $G = (R - Q)$ with

$$Q = (a : a^3 + a^2 : 1)$$

and

$$R = (b : b^4 + b^3 + b^2 + b + 1 : 1)$$

where a and b primitive elements of $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^5}$ (since the curve has no place of degree 3) respectively, is given by,

$$f = (x^3x + x^2z^2 + z^4)y/(x^5 + x^3z^2 + z^5) + (x^5 + x^4z + x^3z^2 + z^3x^2 + xz^4 + z^5)/(x^5 + x^3z^2 + z^5)$$

Evaluating f at all the 5 places P_i from the Table 8.4 and using the map $\pi_{\deg(P_i)}$ that maps all evaluations to $\mathbb{F}_2$ results in,

$$[\ \overbrace{1 \mid 1 \mid 0 \mid 1}^{f(P_i)\ |_{\deg(P_i)=1}} \quad \underbrace{1 \mid \alpha^2}_{f(P_i)\ |_{\deg(P_i)=2}}\ ]$$

This forms the code $[6, 1, 5]_4$.[6] In $\mathbb{F}_2$ this becomes,

$$[\ 1 \mid 1 \mid 0 \mid 1 \mid \underbrace{1\ 0}_{1} \mid \underbrace{1\ 1}_{\alpha^2}\ ]$$

which forms the code $[8, 1, 5]_2$. Short auxiliary codes $[1, 1, 1]_2$ to encode $f(P_i)\ |_{\deg(P_i)=1}$ and $[3, 2, 2]_2$ to encode $f(P_i)\ |_{\deg(P_i)=2}$ are used. The resulting codeword of a generalised AG code is,

$$[\ 1 \mid 1 \mid 0 \mid 1 \mid 1\ \ 0\ \ 1 \mid 1\ \ 1\ \ 0\ ].$$

This forms the code $[10, 1, 7]_2$.

Three polynomials and their associated curves are used to obtain codes in $\mathbb{F}_{16}$ better than the best-known codes in [15]. The three polynomials are given in Table 8.5, while Table 8.6 gives a summary of the properties of their associated curves (with $t = 4$). w is the primitive element of $\mathbb{F}_{16}$. The number of places of degree j, A_j, is determined by computer algebra system MAGMA [3]. The best-known linear codes from [15] over $\mathbb{F}_{16}$ with $j = d_j$ for $1 \leq j \leq 4$ are

$$[1, 1, 1]_{16} \quad [3, 2, 2]_{16} \quad [5, 3, 3]_{16} \quad [7, 4, 4]_{16}$$

which correspond to C_1, C_2, C_3 and C_4, respectively. Since $t = 4$ for all the codes in this paper and

$$[d_1, d_2, d_3, d_4] = [1, 2, 3, 4]$$

The representation $C_1(k; t; B_1, B_2, \ldots, B_t; d_1, d_2, \ldots, d_t)$ is shortened as such,

$$C_1(k; t; B_1, B_2, \ldots, B_t; d_1, d_2, \ldots, d_t) \equiv C_1(k; B_1, B_2, \ldots, B_t).$$

Tables 8.7 to 8.9 show improved codes from generalised AG codes with better minimum distance than codes in [15]. It is also worth noting that codes of the form

[6] From Bezout's $d_{min} = n - m = n - k - g + 1$.

Table 8.5 Polynomials in $\mathbb{F}_{16}$

$F_1 = x^5 + y^4z + yz^4$
$F_2 = x^{16} + x^4y^{15} + x^4 + xy^{15} + w^4y^{15} + w^4$
$F_3 = x^{28} + wx^{20} + x^{18} + w^{10}x^{17} + w^{10}x^{15} + w^4x^{14} + w^3x^{13} + w^3x^{12} + wx^{11} + x^{10} + w^{11}x^9 + w^{12}x^8 + w^{14}x^7 + w^{13}x^6y^2 + w^9x^6y + w^6x^6 + w^2x^5y^2 + w^{13}x^5y + w^{14}x^5 + w^{14}x^4y^4 + w^7x^4y^2 + w^6x^4y + w^9x^4 + w^8x^3y^4 + w^{11}x^3y + w^4x^3 + w^{11}x^2y^4 + w^{11}x^2y^2 + wx^2y + w^5x^2 + w^8xy^4 + w^6xy^2 + w^9xy + w^{11}y^8 + y^4 + w^2y^2 + w^3y$

Table 8.6 Properties of $\mathscr{X}_i/\mathbb{F}_{16}$

Curve	Genus	A_1	A_2	A_3	A_4	Reference
$\mathscr{X}_1$	6	65	0	1600	15600	
$\mathscr{X}_2$	40	225	0	904	16920	[5]
$\mathscr{X}_3$	13	97	16	1376	15840	[6] via [9]

Table 8.7 New codes from $\mathscr{X}_1/\mathbb{F}_{16}$

Codes	k Range	Description	#
$[70, k, d \geq 63 - k]_{16}$	$10 \leq k \leq 50$	$C_1(k; [65, 0, 1, 0])$	41

Table 8.8 New codes from $\mathscr{X}_2/\mathbb{F}_{16}$

Code	k Range	Description	#
$[232, k, 190 - k]$	$102 \geq k \geq 129$	$C_1(k; [225, 0, 0, 1])$	28
$[230, k, 189 - k]$	$100 \geq k \geq 129$	$C_1(k; [225, 0, 1, 0])$	30
$[235, k, 192 - k]$	$105 \geq k \geq 121$	$C_1(k; [225, 0, 2, 0])$	17

$C_1(k; N, 0, 0, 0)$ are simply Goppa codes (defined with only rational points). The symbol # in the Tables 8.7 to 8.9 denotes the number of new codes from each generalised AG code $C_1(k; B_1, B_2, \ldots, B_t)$. The tables in [7] contain curves known to have the most number of rational points for a given genus. The curve $\mathscr{X}_2/\mathbb{F}_{16}$ is defined by the well-known Hermitian polynomial [5].

Table 8.9 New codes from $\mathscr{X}_3/\mathbb{F}_{16}$

Codes	k Range	Description	#
$[102, k, 88 - k]$	$8 \leq k \leq 66$	$C(k; [97, 0, 1, 0])$	59
$[103, k, 89 - k]$	$8 \leq k \leq 68$	$C(k; [97, 2, 0, 0])$	61
$[106, k, 91 - k]$	$k = 8$	$C(k; [97, 3, 0, 0])$	1

8.5 Summary

Algebraic geometry codes are codes obtained from curves. First, the motivation for studying these codes was given. From an asymptotic point of view, some families of AG codes have superior performance than the previous best known bound on the performance of linear codes, the Gilbert–Varshamov bound. For codes of moderate length, AG codes have better minimum distances than their main competitors, non-binary BCH codes with the same rate defined in the same finite fields. Theorems and definitions as a precursor to AG codes was given. Key theorems are Bezout's and Riemann–Roch. Examples using the well-known Hermitian code in a finite field of cardinality 4 were then discussed. The concept of place of higher degrees of curves was presented. This notion was used in the construction of generalised AG codes.

References

1. Blahut, R.E.: Algebraic Codes on Lines, Planes and Curves. Cambridge (2008)
2. Blake, I., Heegard, C., Hoholdt, T., Wei, V.: Algebraic-geometry codes. IEEE Trans. Inf. Theory **44**(6), 2596–2618 (1998)
3. Bosma, W., Cannon, J.J., Playoust, C.P.: The Magma algebra system I: The user language **24**, 235–266 (1997)
4. Ding, C., Niederreiter, H., Xing, C.: Some new codes from algebraic curves. IEEE Trans. Inf. Theory **46**(7), 2638–2642 (2000)
5. Garcia, A., Quoos, L.: A construction of curves over finite fields. ACTA Arithmetica **98**(2), (2001)
6. van der Geer, G., van der Vlugt, M.: Kummer covers with many points. Finite Fields Appl. **6**(4), 327–341 (2000)
7. van der Geer, G., et al.: Manypoints: A Table of Curves with Many Points (2009). http://www.manypoints.org
8. Grassl, M.: Code Tables: Bounds on the Parameters of Various Types of Codes (2007). http://www.codetables.de
9. Grassl, M.: Private Communication (2010)
10. Lachaud, G., Tsfasman, M., Justesen, J., Wei, V.W.: Introduction to the special issue on algebraic geometry codes. IEEE Trans. Inf. Theory **41**(6), 1545 (1995)
11. Leung, K.H., Ling, S., Xing, C.: New binary linear codes from algebraic curves. IEEE Trans. Inf. Theory **48**(1), 285–287 (2002)
12. Massimo, G.: Notes on Algebraic-geometric Codes. Lecture Notes (2003). http://www.math.kth.se/math/forskningsrapporter/Giulietti.pdf
13. Niederreiter, H., Xing, C., Lam, K.Y.: A new construction of algebraic-geometry codes. Appl. Algebra Eng. Commun. Comput. **9**(5), (1999)
14. Ozbudak, F., Stichtenoth, H.: Constructing codes from algebraic curves. IEEE Trans. Inf. Theory **45**(7) (1999)
15. Schimd, W., Shurer, R.: Mint: A Database for Optimal Net Parameters (2004). http://mint.sbg.ac.at
16. Tsfasman, M., Vladut, S., Zink, T.: On Goppa codes which are better than the Varshamov-Gilbert bound. Math. Nacr. **109**, 21–28 (1982)
17. Van-Lint, J.: Algebraic geometry codes. In: Ray-Chaudhari, D. (ed.) Coding theory and design theory: Part I: Coding Theory, p. 137. Springer, New York (1990)
18. Walker, J.L.: Codes and Curves. American Mathematical Society, Rhode Island (2000)

19. Xing, C., Ling, S.: A class of linear codes with good parameters from algebraic curves. IEEE Trans. Inf. Theory **46**(4), 1527–1532 (2000)
20. Xing, C., Niederreiter, H., Lam, K.: A generalization of algebraic-geometry codes. IEEE Trans. Inf. Theory **45**(7), 2498–2501 (1999a)
21. Xing, C., Niederreiter, H., Lam, K.Y.: Constructions of algebraic-geometry codes. IEEE Trans. Inf. Theory **45**(4), 1186–1193 (1999b)