Reflections on the "Decoding of Algebraic-Geometric Codes up to the Designed Minimum Distance"

Gui-Liang Feng, Member IEEE, and T. R. N. Rao, Fellow IEEE

The Why, What, and How of Algebraic-Geometric Codes

We begin this exposition by looking back at two key developments: (i) reduction of the Shannon problem to the Hamming problem, and (ii) reduction of the Hamming problem to the Riemann problem. During the late 1940's, Shannon and Hamming developed two different approaches for coding discrete information in the presence of noise. Shannon proposed a general model for a noisy channel, in which distortions are described by the conditional probabilities of the transformation of one word into another. He proved an important coding theorem on the possibility of transmitting information in such a way that the probability of error tends to zero as the word length increases. Unfortunately, the statistical description of the channel does not indicate how to construct optimal codes. Therefore, the problem of constructing such codes in Shannon's model has not been accomplished in practice. However, beginning with the very simple parity checks already used in the first computers, Hamming arrived at the idea of error-correcting codes. He proposed a geometrical model in which distortions are described by the distance between words, defined as the number of symbols by which the words differ from each other. The problem of constructing an optimal code in this model reduces to that of the densest possible packing of spheres. To solve this problem, a variety of methods were applied from logic, combinatorics, number theory, algebra, geometry, and topology. The concept of a code associated with an algebraic curve gradually crystallized, and Riemann-Roch theorem became the basic computational tool. The problem of constructing good codes was thus reduced to the analysis of algebraic curves [1].

Why AG codes?

There exist several important classes of linear codes, which have been extensively studied. A linear code of finite length can be defined as the null space of a parity matrix $\mathbf{H}$. A linear code with length n over $\mathbf{F}_q$ is a linear subspace of ${\mathbf{F}_q}^n$. The notation $[n,k,d]$ is commonly used to represent a code of length n with dimension k and minimum distance d. For such a code, the *information rate* and the *relative minimum distance rate*, are given by $R = k/n$ and $\delta = d/n$ respectively.

A sequence of linear codes $\{C_m\}_{m=1}^{\infty} = \{[n_m, k_m, d_m]\}_{m=1}^{\infty}$ over $\mathbf{F}_q$, such that the code length $n_m \to \infty$ when $m \to \infty$, is said to be *asymptotically good*, if the information rates R_m and the relative minimum distance rates δ_m are bounded away from zero.

Let us consider the q-ary entropy function defined as follows:

$$H_q(x) \equiv x \cdot \log_q(q-1) - x \cdot \log_q x - (1-x) \cdot \log_q(1-x).$$

Since $\log_2(2-1) = 0$, when $q = 2$, the binary entropy function is reduced to

$$H_2(x) \equiv -x \cdot \log_2 x - (1-x) \cdot \log_2(1-x).$$

$R_{GV}(\delta) \equiv 1 - H_q(\delta)$ is called the *Gilbert−Varshamov curve.* It is known that $R_{GV}(0) = 1$ and $R_{GV}(\frac{q-1}{q}) = 0$. For more than thirty five years, for a fixed δ_m, the best lower asymptotic bound on R_m has been referred to as the *Gilbert − Varshamov* bound, which can be simply described as follows:

Gilbert-Varshamov bound : Suppose $0 \le \delta \le \frac{q-1}{q}$. Then there exists an infinite sequence of $[n, k, d]$ q-ary linear codes with $d/n \equiv \delta$ and rate $R \equiv k/n$ satisfying the following condition:

$$R \ge 1 - H_q(\delta) \text{ for } all\ n.$$

Finding asymptotically good codes, especially a sequence of linear codes, which meet or exceed the Gilbert-Varshamov bound, has been a very active area of research for the past thirty five years. Unfortunately, many known linear codes are asymptotically bad codes. It was previously shown that there exist long Goppa codes which meet the Gilbert-Varshamov bound. However a solution for finding these long Goppa codes has not yet appeared. In 1972, Justesen gave a construction of explicit asymptotically good codes by using *concatenated codes* [5]. For this work, he received the 1972 Browder J. Thompson prize. However, these codes achieve a lower bound which is below the *Gilbert−Varshamov* (GV) bound.

It is desirable to construct asymptotically good codes of longer code length for a designed minimum distance, which meet or exceed the Gilbert-Varshamov bound. To this extent considerable research efforts have been made, which investigated a new approach to construct linear codes, especially using the rational points of algebraic-geometric curves as code locations.

What are AG codes?

The most important development in the theory of error-correcting codes in recent years was the introduction of methods from algebraic geometry to construct good codes. The ideas are based on generalizations of the so-called *Goppa codes.* The "classical" Goppa codes were already a great improvement on codes known at that time. V. D. Goppa [2-4] discovered an amazing connection between the theory of algebraic curves over a finite field $\mathbf{F}_q$ and the theory of error-correcting block q-ary codes. His efforts of many years in searching for possible generalizations of Reed-Solomon codes, BCH codes and classical Goppa codes, culminated in the development of *algebraic geometric* (AG) codes. The codes constructed by choosing a family of points from a curve and a space of rational functions of this curve, are said to be algebraic-geometric codes. These codes are also known as *geometric Goppa codes*, and can be considered to be a generalization from the Reed-Solomon codes on an affine line to the codes on arbitrary irreducible non-singular curves. In this context, it is to be noted that all linear codes can be described as AG codes.

Algebraic-geometric codes opened new and rather exciting possibilities in coding theory and related topics. They have very good code parameters (like code dimension, minimum distance rate δ, and information rate R), and offer flexibility in the choice of these parameters. For a long time there was serious doubt whether it would be possible to give an explicit algebraic construction of a sequence of codes such that both R and δ are bounded away from zero.

A very sensational development in the theory of AG codes was presented in a paper, [6], by Tsfasman, Vladut and Zink in 1982. In this paper, the idea of codes from algebraic curves was combined with some recent results from algebraic geometry, to produce a sequence of polynomially constructive error-correcting codes over $\mathbf{F}_q$. This led to a new lower bound, the *Tsfasman-Vladut-Zink* (TVZ) bound, on the information rate of good codes, which is better than the GV bound when $q \geq 49$. For this paper, the authors received the IEEE Information Theory Group Paper Award in 1983.

The novice reader should realize that the GV-bound could not be improved until 1982, and was believed by many researchers to be the best possible lower bound. Several binary coding experts still feel that for linear codes over $\mathbf{F}_2$, it is not possible to achieve any improvement of the GV bound. Furthermore, there exists no known explicit or simple (or with a polynomial complexity of length n and a lower degree) construction of a sequence of codes meeting this bound.

In 1984, Katsman, Tsfasman and Vladut [7] gave a construction which uses a class of codes over a fixed field $GF(p^2)$, $p^2 \geq 49$, and meeting the TVZ bound. However, the time complexity of construction of these codes is very high.

For any desired minimum distance, codes of longer length can be constructed using the principles based on AG curves. The basic computational tool for determining the minimum distance of these codes is the Riemann-Roch theorem. We shall now discuss the construction of AG codes from algebraic-geometric curves.

How to construct AG codes?

Reed-Solomon codes can be regarded as a special type of AG codes. For these codes, the points on an affine plane line can be considered as the code locations. However, the number of points is limited by the number of elements in the field. We illustrate the construction of Reed-Solomon code by considering an example over $GF(2^2)$. The line $y = 0$ contains four points (0, 0), (1, 0), (α, 0) and (α^2, 0). Using these four points, we can construct Reed-Solomon code of length 4. The *basis* of ${\mathbf{F}_q}^n$ ($= {\mathbf{F}_4}^4$) comprises the following four vectors:

$$\begin{array}{rcl} 1 & \leftrightarrow & (1,1,1,1) \\ x & \leftrightarrow & (0,1,\alpha,\alpha^2) \\ x^2 & \leftrightarrow & (0,1,\alpha^2,\alpha) \\ x^3 & \leftrightarrow & (0,1,1,1). \end{array}$$

These vectors can be regarded as the evaluated vectors of the monomials { 1, x, x^2, x^3 } at these four points. By considering the first $r \leq 3$ vectors (i.e., monomials) of the basis as a parity check matrix, we can define the Reed-Solomon code $\mathbf{C}_r$ over $GF(2^2)$. In general, the code $\mathbf{C}_r$ has the minimum distance $r+1$. For example, we define the parity check matrix of the first $r = 2$ vectors as follows:

$$\mathbf{H}_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 \end{bmatrix}$$

The Reed-Solomon code defined by this parity check matrix has the minimum distance $r+1 = 3$.

Now we give a simple example illustrating the construction of AG codes from Hermitian curves in a two-dimensional affine space. Consider a Hermitian curve defined as follows:

$$x^3 + y^2 + y = 0 \text{ over } GF(2^2).$$

The roots (i.e., rational points) of this curve are given as follows: $(x_1, y_1) = (0, 0)$, $(x_2, y_2) = (0, 1)$, $(x_3, y_3) = (1, \alpha)$, $(x_4, y_4) = (1, \alpha^2)$, $(x_5, y_5) = (\alpha, \alpha)$, $(x_6, y_6) = (\alpha, \alpha^2)$, $(x_7, y_7) = (\alpha^2, \alpha)$, and $(x_8, y_8) = (\alpha^2, \alpha^2)$. These rational points constitute a location set LS, whose elements also denote the locations of a linear code. Each $f(x, y)$ is associated with an evaluated vector, evaluated on these rational points as: $f(x, y) \leftrightarrow (f(x_1, y_1), f(x_2, y_2), f(x_3, y_3), f(x_4, y_4), f(x_5, y_5), f(x_6, y_6), f(x_7, y_7), f(x_8, y_8))$. Then the monomials $\{ 1, x, y, x^2, xy, y^2, xy^2, y^3 \}$ are associated with the following evaluated vectors:

$$\begin{array}{ccc}
1 & \leftrightarrow & (1,1,1,1,1,1,1,1) \\
x & \leftrightarrow & (0,0,1,1,\alpha,\alpha,\alpha^2,\alpha^2) \\
y & \leftrightarrow & (0,1,\alpha,\alpha^2,\alpha,\alpha^2,\alpha,\alpha^2) \\
x^2 & \leftrightarrow & (0,0,1,1,\alpha^2,\alpha^2,\alpha,\alpha) \\
xy & \leftrightarrow & (0,0,\alpha,\alpha^2,\alpha^2,1,1,\alpha) \\
y^2 & \leftrightarrow & (0,1,\alpha^2,\alpha,\alpha^2,\alpha,\alpha^2,\alpha) \\
xy^2 & \leftrightarrow & (0,0,\alpha^2,\alpha,1,\alpha^2,\alpha,1) \\
y^3 & \leftrightarrow & (0,1,1,1,1,1,1,1).
\end{array}$$

By considering the first r vectors, (i.e., the first r monomials), we can define the parity matrix of the code $\mathbf{C}_r$. For example, the parity matrix obtained by the first 5 vectors is as shown below, and defines the code $\mathbf{C}_5$.

$$\mathbf{H}_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha^2 & \alpha & \alpha \\ 0 & 0 & \alpha & \alpha^2 & \alpha^2 & 1 & 1 & \alpha \end{bmatrix}.$$

In general, by considering the first r vectors, (i.e., the first r monomials of the sequence H), as a parity check matrix $\mathbf{H}_r$, we can define codes $\mathbf{C}_r$ with length n and the points of LS

as the code locations. The minimum distance of these codes can be determined by using the Riemann-Roch theorem, i.e., $d(\mathbf{C}_r) \geq r\text{-}g+1$, where g is the genus of the curve. By choosing a larger set of rational points, we can construct AG codes of larger code lengths.

Let us consider the following curve in a three-dimensional space over $GF(2^2)$:

$$\left\{ \begin{array}{l} x^3 + y^2 + y = 0 \\ y^3 + z^2 + z = 0. \end{array} \right.$$

This curve has $4 \times 2 \times 2 = 16$ rational points, and from these rational points we can construct AG codes over $GF(2^2)$, up to length 16.

If we consider curves, surfaces or other varieties in high-dimensional spaces, we get an increase in the number of rational points and thus can construct AG codes of larger code lengths.

Decoding AG Codes up to the Designed Minimum Distance

The construction and decoding of AG codes are two important problems of study in the development of the theory of algebraic-geometric codes. Good code constructions are very important. Moreover, it is desirable and essential to derive simple decoding procedures which can correct as many errors as possible. The algebraic decoding of block codes by first determining an error-locator polynomial and subsequently evaluating its zeroes which yield the error locations, was presented by Peterson in 1960 for binary BCH codes, and extended by Gorenstein and Zierler to q-ary BCH codes. By generalizing their idea to AG codes, in 1989, Justesen, Larsen, Jensen, Havemose and Hoholdt [8] published the first decoding procedure for a class of AG codes based on plane curves. This decoding procedure is a generalization of the Peterson's decoding procedure for AG codes on plane curves, and can correct up to $\lfloor (d^* - g - 1)/2 \rfloor$ errors, where d^* is the designed minimum distance of the code and g is the genus of the curve involved in the construction. For this paper, they received the IEEE Information Theory Group Paper Award in 1991.

Subsequent research based on this approach resulted in several improvements. Skorobogatov and Vladut [9] generalized their ideas and gave a decoding procedure for AG codes derived from arbitrary algebraic curves, which can correct any $\lfloor (d^* - g - 1)/2 \rfloor$ or fewer errors. In their paper, Skorobogatov and Vladut also presented a modified algorithm which corrects more errors, though in general, not up to the designed minimum distance. Independently, Krachkovskii proved the same result, but his work was only published as a preprint in Russian [10]. Using profound results from algebraic geometry, Pellikaan [11] gave a decoding procedure which can correct up to $\lfloor (d^* - 1)/2 \rfloor$ errors. However, his decoding procedure is very complex and is not efficient. Justesen et al. [12], improved on their original decoding procedure in several ways and gave a new decoding procedure for AG codes from arbitrary regular plane curves, which can correct up to $\lfloor (d^* - g/2 - 1)/2 \rfloor$ errors. Porter, Shen and Pellikaan [13] proposed a decoding procedure using an extra place, and Duursma [14] suggested a decoding procedure which uses a special divisor. Unfortunately, all these decoding procedures can not correct up to $\lfloor (d^* - 1)/2 \rfloor$ errors, which is the error-correcting capacity of AG codes. During the past few years, the problem of decoding AG codes up to $\lfloor (d^* - 1)/2 \rfloor$ errors has become very active and to a large extent has remained intangible.

In 1991, we gave a generalized Peterson's decoding procedure which looks simple and can correct up to $\lfloor (d^* - 1)/2 \rfloor$ errors for the AG codes $C_\Omega(D, G)$, where $G = mQ$ [15]. Similar to the previous decoding algorithms, this decoding procedure also uses the technique of solving systems of linear equations and can be explained purely in terms of linear algebra, in the same manner by which one can abstract from AG codes to linear codes. But we add a majority voting scheme to determine the value of the next unknown syndrome, until the error locator polynomial can be uniquely determined, or until the values of all the unknown syndromes can be determined. At about the same time, Ehrhard independently found another decoding algorithm which can also decode AG codes up to the designed minimum distance, but only for the case of $d^* \geq 6g$, [16].

It is well-known that the decoding of Reed-Solomon codes is equivalent to solving a system of special non-linear equations with one variable. Peterson's decoding procedure reduces this problem to finding a linear dependence of the initial columns for the syndrome matrix, i.e., finding an error locator polynomial, and solving the error locator equation. However, the correctness depends on the fact that the syndrome matrix can be decomposed into a product of three matrices, i.e., $\mathbf{S} = \mathbf{XEY}$, where $\mathbf{E}$ is a diagonal matrix, and $\mathbf{X}$ is a full rank matrix. We must mention that some of the entries of matrix $\mathbf{S}$ are unknown. Hence we can only find the partial linear dependent relations of columns of $\mathbf{S}$. Using the Vandermonde matrix in the decoding of Reed-Solomon codes, $\mathbf{X}$ is guaranteed to be a full rank matrix, whose rank is given by the number of errors. Thus, from the partial linear dependent relations of columns of the syndrome matrix $\mathbf{S}$, we can find the same linear dependent relations of the corresponding columns of the unknown matrix $\mathbf{Y}$, i. e., we can find the functions that must be satisfied by all the error locations. Hence, from the syndrome matrix $\mathbf{S}$, we need to find the partial linear dependent relations of the columns. Furthermore, from these partial linear dependent relations, i.e., error-locator polynomials, we can determine the error locations. The error magnitudes can be determined by solving a system of linear equations. Similarly, the decoding of AG codes is equivalent to solving a system of special non-linear equations with several variables. We can also use the Peterson's decoding procedure to reduce it to solving some linear problems. However, in the case of AG codes with a non-zero genus g, the matrix $\mathbf{X}$ is not guaranteed to be a full rank matrix. Thus, the partial linear dependent relations of the columns of the syndrome matrix $\mathbf{S}$ may not represent the linear dependent relations of the corresponding columns of matrix $\mathbf{Y}$. Hence, these partial linear dependent relations can not be used to directly determine the error locations.

Our idea considers the fact that all the fully linear dependent relations of columns of $\mathbf{S}$ will also be satisfied by the error locations, i.e., these fully linear dependent relations also represent the error locator polynomials. However, some of the partial linear dependent relations of columns of $\mathbf{S}$ may not be the fully linear dependent relations of the same columns, because $\mathbf{X}$ is not a full rank matrix. Hence, we refer to the partial linear relations of the columns of the syndrome matrix $\mathbf{S}$ as *candidate* linear dependent relations of the columns of $\mathbf{S}$, and also of the corresponding columns of $\mathbf{Y}$. However, it is very difficult to determine the fully linear dependent relations of the columns of $\mathbf{S}$. We rationalized that if this candidate linear dependent relation is a fully linear dependent relation, then the value of the next unknown syndrome that can be uniquely determined by extending the candidate linear dependent relation to this unknown syndrome will be a *true* syndrome value, provided there is no column leader at its previous columns in the same row. The next unknown syndrome satisfying this condition is called a *candidate next unknown syndrome*. Fortunately, we were able to prove that among the candidate next unknown syndromes, the number of true values of the syndromes is greater than the number of false values of these syndromes. This enabled us to determine the true values of the next unknown syndromes, using the majority voting scheme. Thus, instead of determining the true candidate linear dependent relations, we determine the true candidate next unknown syndromes. The error vector can be determined in either of the following two ways: (i) by determining the values of all the unknown syndromes and then using the Fourier inverse transform to obtain the error vector, (i.e. Blahut's decoding approach), or (ii) by finding the values of the next g unknown syndromes, determining the error locator polynomial and further calculating the error magnitudes to obtain the error vector, (i.e. Berlekamp-Massey's approach). The second approach is possible because if $r + g$ syndromes are known, the partial linear dependent relations of columns of matrix $\mathbf{S}$ also denote the fully linear dependent relations of the columns of matrix $\mathbf{S}$, i. e., they represent the linear dependent relations of the corresponding columns of matrix $\mathbf{Y}$. Using either of these two approaches, we can correct errors up to the designed minimum distance. The complexity is $O(n^3)$, similar to the complexity of solving a system of linear equations with n variables. When the syndrome matrix $\mathbf{S}$ satisfies some conditions, (e. g. it is a Hankel matrix, or a block-Hankel matrix, or a Hankel-block-Hankel matrix), the complexity will be further reduced [17,18].

Improved AG Codes without Algebraic-Geometric Curves

For a long time AG codes were thought to be very difficult for engineers to understand, because they are based on the theory of algebraic geometry or algebraic geometric curves. This area has become very active recently due to its utility in solving many important problems. Unfortunately however, it also requires special mathematical knowledge and skills. After the introduction of AG codes, though several papers and books dealing with these codes have been published, these codes are still not clearly understood by many engineers. The current AG codes have many good advantages and are more efficient than the Reed-Solomon codes. However, we believe that the current AG codes can be further improved. Some of the questions of major concern to engineers include (i) the development of techniques and methods to simplify the understanding of AG codes, and (ii) the improvement of the current AG codes to yield more efficient codes.

Justesen et. al. [8], made a significant contribution to the understanding of algebraic-geometric codes. Their approach involves the use of monomials of two variables instead of rational functions in three variables, for deriving the current AG codes from affine plane curves. Blahut [19] gave a simple interpretation of AG codes derived without the use of algebraic-geometric curves. He demonstrated that some codes derived from Klein curves can be considered to be the weighted sums of Reed-Solomon codes.

It is common knowledge that a linear code with length n over a field is a linear subspace in an n-dimensional affine space over this field. A set of n linearly independent vectors of this n-dimensional affine space can be used to construct a sequence of linear codes. For instance, let $n = 2^m$ with the field being GF(2^m). Furthermore, let a monomial x^i represent the evaluated vector (0^i, 1^i, α^i, ..., $\alpha^{(n-2)i}$), where 0^0 expresses a value 1, for $0 \leq i \leq n-1$. Then { 1, x, ..., x^{n-1} } is a set of linearly independent vectors. The first r vectors define a Reed-Solomon code. For the parity check matrix of this code, a lower bound of the minimum distance can be easily determined by using the Vandermonde matrix. It is therefore very important to choose the n linearly independent vectors such that a lower bound of the minimum distance of the code defined by a subset of the vector sequence can be easily determined. For the Reed-Solomon codes defined by the first r monomials (i.e., vectors) from the sequence { 1, x, ..., x^{n-1} }, a lower bound of the minimum distance can be determined by using the Vandermonde matrix, and thus Reed-Solomon codes can be easily constructed. For the AG code over GF(2^4) defined by the first r monomials (i.e., evaluated vectors) from the sequence { 1, x, y, x^2, xy, ..., x^4y^{11}, y^{12}, y^{13}, y^{14}, y^{15} }, a lower bound of the minimum distance can be determined by using the Reimann-Roch theorem and we can construct Hermitan codes over GF(2^4).

¿From the majority voting scheme for decoding AG codes up to the designed minimum distance, it can be easily realized that a lower bound δ_{FR}, called Feng-Rao bound [20], can be derived by simply calculating the number of the next unknown syndromes in the syndrome matrix, instead of using the Reimann-Roch theorem. This implies that the new decoding scheme can be considered to be a new method for determining a lower bound of the minimum distance. This method does not require the use of the theory of algebraic-geometry. Thus, a sequence of linearly independent vectors which need not be derived from irreducible non-singular curves, can also be used to construct linear codes, and their designed minimum distance can be easily determined by simply calculating the number of the next unknown syndromes in the syndrome matrix. This is the basic idea used for deriving the *improved geometric Goppa codes* without using algebraic-geometric curves [21-22]. The improvement of the improved geometric Goppa codes over the current AG codes is essentially two-fold: (i) the location set whose elements define the code locations, need not consist of only rational points from irreducible and non-singular curves - these points can be derived from curves, surfaces, hyperplanes or other varieties; (ii) the monomial sequence H need not be made from the *first* r monomials.

This procedure leads to the definition of a location set whose elements need to satisfy a certain set of equations. These elements may be derived from surfaces, curves or other varieties, and do not necessarily have to be points on irreducible non-singular algebraic curves. This adds to the flexibility in the choice of code parameters of these AG codes.

Apart from us, several eminent researchers including Pellikaan, Wei, Heegard, Saints, and Hoholdt, are currently pursuing active research work in this area. Though the current emphasis of research is towards constructing AG codes without using the theory of algebraic-geometric curves, we feel that with the combined use of the concepts from algebraic coding theory and the insights provided by the theory of algebraic-geometry, it will be possible to witness in the near future, the construction of very simple AG-like codes which are more efficient than the current AG codes.

Some Afterthoughts

Our decoding procedure which is based on the majority voting scheme, finds many interesting applications. For instance, the decoding procedure can be extended to handle the AG codes $C_\Omega(D,G)$, where $G = \sum m_i Q_i$, as considered by Duursma [23]. It can also be used in decoding binary cyclic codes up to the true minimum distance, as demonstrated by Feng and Tzeng [24]. Furthermore, we have also applied the majority voting scheme to the erasures-and-errors decoding of AG codes [25].

We now discuss some fascinating implementation details. Decoding of AG codes up to $\lfloor (d^* - g - 1)/2 \rfloor$ errors has been successfully done in the past by several researchers, using various approaches which include solving a system of linear equations, defining and solving the key equations, using Grobner bases, using Sakata's algorithm, and so on. By applying the majority voting scheme in the decoding procedure, and using the technique of solving a set of linear equations, we can decode AG codes up to the designed minimum distance. Some researchers have recently applied this majority voting scheme in decoding procedure while using some of the other above mentioned approaches, and were also successful in decoding AG codes up to the designed minimum distance [26-29].

Using faster computing algorithms, decoding of AG codes can be improved. For example, in a collaborative research effort with Wei and Tzeng [17], by using a fast algorithm for the Hankel-Block-Hankel matrices to implement the majority voting scheme, we have derived a fast decoding procedure with complexity $O(n^{7/3})$, for the AG codes from the affine plane curves. In [18], we generalized this decoding procedure to the AG codes from m-dimensional affine spaces and obtained a decoding procedure with complexity $O(n^{3-2/(m+1)})$. Using the Sakata algorithm and the majority voting scheme, Sakata, Justesen, and Hoholdt [26] have derived a new decoding procedure for AG codes with the same complexity, $O(n^{3-2/(m+1)})$.

Based on the idea of the majority voting scheme, a new approach has been developed for determining a lower bound of the minimum distance. This new approach does not make use of the Reimann-Roch theorem. More general linear codes with some efficient parameters have been constructed. Some of them are called improved geometric Goppa codes, and some are known as AG codes derived without using the theory of algebraic geometry. Recently, research work dealing with the construction of asymptotically good linear codes exceeding the GV bound or the TVZ bound, especially over small finite fields such as GF(4) and GF(8), has become very active, [30]. It is extremely difficult to construct binary linear codes exceeding the GV bound. However, we strongly believe that in the not-too-distant future, many significant results will appear in this area of research.

References

[1] V. D. Goppa: Codes and Information: Russian Math. Surveys, Vol.39, No. 1, pp. 87-141, 1984.

[2] V. D. Goppa: Codes associated with divisors: Problemy Peredachi Informatsii 13 (1977) 33-39.

[3] V. D. Goppa: Codes on algebraic curves: Soviet math. Dokl. 24 (1981) 75-91.

[4] V. D. Goppa: Algebraic-geometric codes: Math. USSR Izvestiya 21 (1983) 75-91.

[5] J. Justesen: A class of constructive asymptotically good algebraic codes: IEEE Trans. Infor. Theory, Vol. IT-18, pp. 652-656, 1972.

[6] M. A. Tsfasman, S. G. Vladut, and T. Zink: Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound: Math. Nachr. 104 (1982) 13-28.

[7] G. L. Katsman, M.A. Tsfasman and S. G. Vladut: Modular curves and codes with a polynomial construction: IEEE Trans. Infor. Theory, Vol. IT-30, pp. 353-355, March 1984.

[8] J. Justesen, K. J. Larsen, H. Elbrond Jensen, A. Havemose, and T. Hoholdt: Construction and decoding of a class of algebraic geometry codes: IEEE Trans. Infor. Theory, Vol. IT-35, pp. 811-821, July 1989.

[9] A. N. Skorobogatov and S. G. Vladut: On decoding of algebraic geometric codes: IEEE Trans. Infor. Theory, Vol. IT-36, pp. 1051-1060, Sept. 1990.

[10] V. Yu. Krachkovskii: Decoding of codes on algebraic curves: Odessa, preprint 1988.

[11] R. Pellikaan: On a decoding algorithm for codes on maximal curves: IEEE Trans. Infor. Theory, Vol. IT-35, pp. 1228-1232, Nov. 1989.

[12] J. Justesen, K. J. Larsen, H. Elbrond Jensen, and T. Hoholdt: Fast decoding of codes from algebraic plane curves: IEEE Trans. Infor. Theory, Vol. IT-38, pp. 111-119, Jan. 1992.

[13] S. C. Porter, B.-Z. Shen, and R. Pellikaan: Decoding geometric Goppa codes using an extra place: IEEE Trans. on Information Theory, vol IT-38, No. 6, pp. 1663-1676, Nov. 1992.

[14] I. M. Duursma: Algebraic decoding using special divisors: IEEE Trans. on Infor. Theory. Vol. IT-39, pp. 694-698, March 1993.

[15] G.L. Feng and T.R.N. Rao: Decoding Algebraic Geometric Codes up to the Design Minimum Distance: Presented at AAECC-9, 1991 and IEEE Trans. on Infor. Theory. Vol. IT-39, No.1, pp. 37-45, Jan. 1993.

[16] D. Ehrhard: Achieving the designed error capacity in decoding algebraic-geometric code: IEEE Trans. on Infor. Theory. Vol. IT-39, No.3, pp. 743-751, May. 1993.

[17] G.L. Feng, V.K. Wei, T.R.N. Rao, and K.K. Tzeng: Simplified Understanding and Efficient Decoding of a Class of Algebraic-Geometric Codes: IEEE Trans. on Infor. Theory. Vol. IT-40, No.4, pp. 981-1002, July 1994.

[18] G.L. Feng and T.R.N. Rao: A Class of Algebraic Geometric Codes from Curves in High-Dimensional Projective Spaces: Lecture Notes in Computer Science, 673 pp. 132-146, May, 1993.

[19] R. E. Blahut: AG codes without AG: presented at 1992 IEEE Information Theory Workshop, Salvador da Bahia, Brazil, June 1992.

[20] C. Kirfel and R. Pellikaan: The minimum distance of codes in an array comming from telescopic semigroups: reprint, May 1993.

[21] G.L. Feng and T.R.N. Rao: A Simple Approach for Construction of Algebraic-Geometric Codes from Affine Plane Curves: IEEE Trans. on Infor. Theory. Vol. IT-40, No.4, pp. 1003-1012, July 1994.

[22] G.L. Feng and T.R.N. Rao: Improved Geometric Goppa Codes: to appear in IEEE Trans. on Infor. Theory. 1995.

[23] I. M. Duursma: Majority coset decoding: IEEE Trans. on Infor. Theory. Vol. IT-39, pp. 1067-1071, May 1993.

[24] G.L. Feng and K. K. Tzeng: A New Procedure for Decoding Cyclic and BCH Codes up to Actual Minimum Distance: IEEE Trans. on Infor. Theory. Vol. IT-40, No.5, pp. 1364-1374, Sept., 1994.

[25] G.L. Feng and T.R.N. Rao: Erasures-and-errors decoding of algebraic-geometric codes: Proceedings of 1993 IEEE Infor. Theory Workshop pp.911-912, June 1993.

[26] S. Sakata, J. Justesen, Y. Madelung, H. E. Jensen, and T. Hoholdt: Fast decoding of algebraic-geometric codes up to half the designed minimum distance: Proceedings of 1993 IEEE Infor. Theory Workshop pp.921-922, June 1993.

[27] S. Sakata, H. E. Jensen, and T. Hoholdt: Generalized Berlekamp-Massey decoding of algebraic geometry codes up to half the Feng-Rao bound: Proceedings of 1994 IEEE ISIT pp.154, June 1994.

[28] B.Z. Shen and K.K. Tzeng: Decoding geometric Goppa codes up to designed minimum distance by solving a key equation in a ring: Proceedings of 1994 IEEE ISIT pp.155, June 1994.

[29] K. Saints, I. Rubion, and C. Heegard: Decoding algebraic-geometric codes using Grobner bases: Proceedings of 1994 IEEE ISIT pp.156, June 1994.

[30] A. Garcia and H. Stichtenoth: A tower of Aritin-Schreier extensions of function fields attaining the Drinfed-Vladut bound: reprinted Dec 1994.