International Journal of Engineering, Science and Mathematics
Vol. 5,Issue 1, March2016,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

# STUDY OF GENERALIZED CODE IN GAUSSIAN CHANNEL AND REED SOLOMON CODE-A REVIEW

**Vijay Kumar**[*]

## Abstract

In this paper an attempt is being made to study generalization of codes in Gaussian channel and Reed Solomon Code. Here we will learn about communication over a channel of practical interest, in which the transmitted signal is subjected to Gaussian noise. This paper deals with the general principles behind error correcting codes (Reed- Solomon Codes) and their algorithms for encoding using these codes, and for decoding with error correction. R.S. Codes are non-binary cyclic codes that represent a subclass of Bose-Chaudhuri-Hocquenghem (BCH) codes. These Codes are most frequently used digital error control codes in the world.

Gaussian Channel is an alphabet channel and time discrete channel which is a good model for communication as well as the basis of radio and satellite links etc. Shannon's determination of the capacity of the linear Gaussian channel is a challenge to succeeding generations of researchers and this capacity is to be infinite (maximum) of the mutual information between input and output. Gaussian Channel can be easily converted into a discrete binary symmetric channel with crossover probability. In practice these ideas are used to convert continuous channel into discrete channel, the main advantage of discrete channel is ease of processing of the output signal for error correction.

***Keywords:***

Gaussian Channel;
Reed Solomon code;
Bose-Chaudhuri-Hocquenghem (BCH) codes.

## 1. Gaussian Channel

The most important continuous alphabet channel is the Gaussian channel depicted in figure 1. This is a time discrete channel with output $Y_i$ at time i, where $Y_i$ is the sum of the input Xi and the noise $Z_i$; The noise $Z_i$ is drawn i.i.d. from a Gaussian distribution with variance N. Thus

$$Yi = Xi + Zi, \qquad Zi \sim N\ (0, N).$$

[*] Vijay Kumar, Assistant Professor-Mathematics, Beant College of Engineering and Technology (BCET), Gurdaspur

The noise Zi is assumed to be independent of the signal Xi. This channel is a good model for some common communication channels. Without further conditions, the capacity of this channel may be infinite. If the noise variance is zero, then the receiver receives the transmitted symbol perfectly. Since X can take on any real value, the channel can transmit an arbitrary real number with no error if the noise variance is non-zero and there is no constraint on the input, we can choose an infinite subset of inputs arbitrarily far apart, so that they are distinguishable at the output with arbitrarily small probability of error. Such a scheme has an infinite capacity as well. Thus if the noise variance is zero or the input is unconstrained, the capacity of the channel is infinite.

The most common limitation of the input is an energy or power constraint. We assume an average power constraint. For any codeword $(x_1, x_2\ldots, x_n)$ transmitted over the channel, we require

$$\frac{1}{n}\sum_{i=1}^{n} x_i^2 \le p$$

This communication channel models many practical channels including radio and satellite links. The additive noise in such channels may be due to a variety of causes. However, by the central limit theorem, the cumulative effect of a large number of small random effects will be approximately normal, so the Gaussian assumption is valid in a large number of situations.

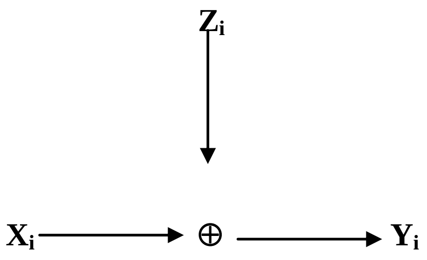

**Figure 1: The Gaussian Channel**

We first analyze a simple suboptimal way to use this channel. Assume that we want to send I bit over the channel in 1 use of the channel. Given the power constraint, the best that we can do is to send one of two levels $+\sqrt{P}$ or $-\sqrt{P}$. The receiver looks at the corresponding received Y and tries to decide which of the two levels was sent. Assuming both levels are equally likely (this would be the case if we wish to send exactly 1 bit of information), the optimum decoding rule is to decide that $+\sqrt{P}$ was sent if $Y > 0$ and decide $-\sqrt{P}$ was sent if $Y < 0$. The probability of error with such a decoding scheme is

$$
\begin{aligned}
P_e &= \frac{1}{2}\Pr\left(Y < 0 \,\middle|\, X = +\sqrt{P}\right) + \frac{1}{2}\Pr\left(Y > 0 \,\middle|\, X = -\sqrt{P}\right) \\
&= \frac{1}{2}\Pr\left(Z < -\sqrt{P} \,\middle|\, X = +\sqrt{P}\right) + \frac{1}{2}\Pr\left(Z > \sqrt{P} \,\middle|\, X = -\sqrt{P}\right) \\
&= \Pr\,(Z > \sqrt{P}) \\
&= 1 - \varphi\left(\sqrt{\frac{P}{N}}\right)
\end{aligned}
$$

Where $\phi$ (x) is the cumulative normal function

$$\varphi(x) = \int \frac{1}{\sqrt{2\pi}} e^{\frac{t^2}{2}} \, dt$$

Using such a scheme, we have converted the Gaussian Channel into a discrete binary symmetric channel with crossover probability P. Similarly, by using a four level input signal, we can convert the Gaussian channel into a discrete four input channel. In some practical modulation schemes, similar ideas are used to convert the continuous channel into a discrete channel. The main advantage of a discrete channel is ease of processing of the output signal for error correction, but some information is lost in the quantization.

We now define the (information) capacity of the channel as the maximum of the mutual information between the input and output over all distributions on the input that satisfy the power constraint.

The information capacity of the Gaussian channel with power constraint P is

$$C = \max_{p\,(x) : E\, x^2 \le p} I(X : Y)$$

We can calculate the information capacity as follows: Expanding I (X; Y), we have

$$
\begin{aligned}
I\ (X;\ Y) &= h(Y) - h\ (Y|\ X) \\
&= h\ (Y - h\ (X + Z|\ X) \\
&= h\ (Y) - h\ (Z|\ X) \\
&= h\ (Y) - h\ (Z)
\end{aligned}
$$

Since Z is independent of X. Now, h (Z) = $\frac{1}{2}$ log 2$\pi$eN. Also,

$$EY^2 = E(X + Z)^2 = EX^2 + 2EXEZ + EZ^2 = P + N$$

Since X and Z are independent and EZ = 0. Given $EY^2$ = P + N the entropy of Y is bounded by $\frac{1}{2}$ log 2$\pi$e (P + N) (the normal maximize the entropy for a given variance).

Applying this result to bound the mutual information, we obtain

$$I(X;\ Y) = h\ (Y) - h\ (Z)$$

$$\leq \frac{1}{2} \log 2\pi e\,(P + N) - \frac{1}{2} \log 2\pi e N$$

$$= \frac{1}{2} \log \left(1 + \frac{P}{N}\right)$$

Hence the information capacity of the Gaussian channel is

$$C = \max_{p(x):\,Ex^2 \leq P} I\,(X;Y) = \frac{1}{2} \log \left(1 + \frac{P}{N}\right)$$

and the maximum is attained when X – MO, P. We will now show that this capacity is also the supremum of the achievable rates for the channel. The arguments are similar to the arguments for a discrete channel.

## 2. Reed-Solomon Code

A Reed-Solomon for RS code over GF(q) is a BCH code of length N = q – 1 of course q is never 2. Thus the length is the number of nonzero elements in the ground field. We shall use N, K and D to denote the length dimension and minimum distance (using capital letters to distinguish them from the parameters of the binary codes which will be constructed later).

Since $x^{a-1}-1 = \prod_{\theta \in GF_{(q)}} (x - \beta)$ the minimal polynomial of α' is simply $M^{th}$ (x) = x - α'. Therefore an RS code of length q – 1 and designed distance δ has generator polynomial

$$g\,(x) = (x - \alpha^{b})\,(x - \alpha^{b+1})\ \ldots.\ (x - \alpha^{b+\delta-2}). \qquad (1)$$

Usually, but not always, b = 1.

Examples. (1) As usual take GF (4) = {0, 1, α, β = $\alpha^2$} with $\alpha^2 + \alpha + 1 = 0$. The RS code over GF (4) with N = 3 and designed distance 2 has g (x) = x - α. The $4^2$ code words are shown as follows:

| | | | |
|---|---|---|---|
| 000 | 1α0 | β0α | βα1 |
| 01α | αβ0 | 10β | 111 |
| 0αβ | β10 | 1βα | ααα |
| 0β1 | α01 | α1β | βββ |

(Fig. 1)

(2) The RS code over GF (5) with N = 4 and designed distance 3. We take α = 2 as the primitive element of GF(5), so that

g (x) = (x - α) (x - α2) = (x – 2) (x – 4) = x2 + 4x + 3

Some of the 25 code words are 3410, 2140, 1320, 0341, 1111 ……

The dimension of an RS code is $K = N - \deg g(x) = N - \delta + 1$. The minimum distance D is by the BCH bound at least $\delta = N - K + 1$. However it can't be greater than this. Therefore

$$D = N - K + 1$$

and RS codes are maximum distance separable. It follows that the Hamming weight distribution of any RS code.

**RS codes are important for several reasons:**

(i) They are the natural codes to use when a code is required of length less than the size of the field. For, being MDS, they the highest possible minimum distance.

(ii) They are convenient for building other codes as we shall see. For example they can be mapped into binary codes with surprisingly high minimum distance. They are also used to constructing concatenated and Justesen codes.

(iii) They are useful for correcting bursts of errors.

Examples:

1. Using the basis 1, $\alpha$ for GF (4) over GF(2). 0 maps into 00, 1 into 10, $\alpha$ 01, $\alpha 2$ 11. Then the [3, 2, 2] RS code over GF (4) of Fig. 1 becomes the [6, 4, 2] binary code of Fig. 2.

| | | | |
|---|---|---|---|
| 000000 | 100100 | 110001 | 110110 |
| 001001 | 011100 | 100011 | 101010 |
| 000111 | 111000 | 101101 | 010101 |
| 001110 | 010010 | 011011 | 111111 |

(Fig. 2)

2. Let c = (c0, c1……… cN-1) belong to an [N, K,D] RS code over GF(2m). Replace each ci by the corresponding binary m-tuple and add an overall parity check an each m-tuple. The resulting binary code has parameters.

$$n = (m + 1)(2m - 1), \quad k = mK. \qquad d \geq 2D = 2(2m - K) \qquad (2)$$

For any K = 1, ….2m – 2. The same construction applied to the extended RS code gives

$$[(m+1)2m, mK, d \geq 2(2m - K + 1)] \qquad (3)$$

binary codes, for K = 1…… 2m – 1

e.g. From the [15, 10, 6] and [16, 10, 7] codes over GF(24) we obtain [75, 40, 12] and [80, 40, 14] binary codes. Even though slightly better codes exist – we shall construct and [80, 40, 16] quadratic residue code.

3. Using the basis 1, $\alpha$, $\alpha 6$ for GC(23) over GF (2) the mapping is

| | | |
|---|---|---|
| $0 \rightarrow$ 000, | $\alpha 2 \rightarrow$ 101, | $\alpha 5 \rightarrow$ 011 |
| $1 \rightarrow$ 100, | $\alpha 3 \rightarrow$ 110, | $\alpha 6 \rightarrow$ 001 |
| $\alpha \rightarrow$ 010, | $\alpha 4 \rightarrow$ 111, | |

Consider the [7, 5, 3] RS code over GF (23) with generator polynomial

$$gN(x) = (x + \alpha 5)\ (x + \alpha n)$$
$$= \alpha 4 + \alpha x - x2$$

It is surprising that this is mapped onto the [21, 15, 3] binary BCH code with generator polynomial

$$g2\ (y) = M(t)\ (y) = 1 + y + y2 + y4 + y6.$$

For g1 (x) itself is mapped onto the vector

111, 010, 100, 000, 000, 000, 000

Which is g2(y). Also ag1(x) is mapped onto yg2(y), a2g1(x) onto y2g2(y), xg1(x) onto y3g2(y) and so on.

This is the only known, nontrivial, example of a cyclic code mapping in this way onto a cyclic code!

## Objectives of the study

To discuss

(1) the coding capacity of mismatched Gaussian Channels.

(2) how the errors in Gaussian Channels centered around the mutual information between the input and the output of a channel, and the minimum mean-square error in estimating the input given the output.

(3) encoding and decoding of RS codes by different manners

(4) power Inequality in Gaussian Channels

## 3. Mismatched Gaussian Channels

Here we shall discuss the coding capacity of mismatched Gaussian Channels. A message X subject to the power constraint is given by

$$\int_0^T X_t^2\, dt \le P_0 T, \qquad a.s. \qquad (1)$$

Where $P_0$ is a positive constant. This channel is an example of a mismatched time-continuous Gaussian feedback channel. It is said to be mismatched because the power constraint is not expressed in terms of the covariance of the noise process N, = $\int_0^t a(s)\, dW_s$, but in terms of the covariance of some other noise process, namely, $N_t = W_t$.

Mismatched channels can arise in jamming situations, in problems where there is insufficient knowledge of the environment, or where one prefers to use a constraint not expressed in terms of the channel noise. General results on the information capacity for such channels have been obtained by Baker 1983.

Here we are interested in evaluating the coding capacity of mismatched Gaussian channels. Here the main result is Theorem 1:

*Theorem 1:*

$$\frac{1}{2}\log\left(1+\frac{P_0}{\lambda_1}\right)\le C_0 \le \frac{1}{2}\log\left(1+\frac{P_0}{\lambda_2}\right)$$

Mutual information is defined in the usual way: it is infinite if the joint measure μxy induced by the two-dimensional process (X, Y) is not absolutely continuous with respect to the product measure μx × μy; otherwise, it is calculated by

$$J\,(\mu_{xy}) = \int_{X\times Y}\left[\log\frac{d\mu_{xy}}{d\mu_x\otimes\mu_y}(x,y)\right]d\mu_{xy}\,(x,y).$$

The information capacity, defined as sup I (μxy) subject to some constraint on X, is typically calculated with an average power constraint. The concept of coding capacity requires a constraint on the power of the (nonrandom) signal paths in-cluded in the codeword set. Thus the constraint $E\|x\|^2 \le P$, for example, is applicable for calculating information capacity, where $\|.\|$ is the RKHS(Reproducing Kernel Hilbert Space) of the channel noise. The corresponding constraint for coding capacity would be $\|x\|^2 \le P$, for each codeword x in the signal set.

When situations $\lambda_1 = \lambda_2$ , we get an exact expression for the coding capacity. An important example is when L = $\sum_n \alpha_n e_n \otimes e_n$, where $\{e_n, n \ge 1\}$ is a complete orthonormal sequence (CONS) in H and $\{\alpha_n, n \ge 1\}$ is a bounded sequence of positive numbers, bounded away from zero, then $\lambda_1 = \lambda_2, = \lim_{n\to\infty} \alpha_n$, and Theorem 1 gives an exact expression for coding capacity. This is the framework for the information capacity treatment. In particular, if $\tilde{\mu}_N$ is a Gaussian measure on $B_T$ which is mutually absolutely continuous with respect to $\tilde{\mu}_N$ and $\tilde{H}$ is the RKHS of $\tilde{\mu}_N$. Then, in the situation of Example 1, J*J = $I_H$ + S, where $I_N$ is the identity on H and S is Hilbert-Schmidt. It then follows that $\lambda_1 = \lambda_2 = 1$ and the coding capacity is the same as in the matched channel. Theorem 1: Which represents an extension of the coding capacity results of McKeague (1984) in two directions: to mismatched Gaussian channels and to nonwhite Gaussian channels, respectively. As an illustration of Theorem 1 we note that the coding capacity of the channel in the example is given by

$$C_0 \le \frac{1}{2}\log\left(\frac{1+p_0}{\lambda_2}\right)$$

## 4. Errors in Gaussian Channels

Here we centered around the mutual information between the input and the output of a channel, and the minimum mean-square error (MMSE) in estimating the input given the output. The output is a relationship between the mutual information and Minimum mean square error that holds regardless of the input distribution, as long as the input-output pair are related through additive Gaussian noise. For example the simplest scalar real-valued Gaussian channel with an arbitrary fixed input distribution. Let the signal-to-noise ratio (SNR) of the channel be denoted by snr. Both the input-output mutual information and the Minimum Mean square error are monotone functions of the SNR, denoted by I (snr) and mmse (snr), respectively. This paper finds that the mutual information in nats and the Minimum Mean square error satisfy the following relationship regardless of the input statistics:

$$\frac{d}{dsnr} I\,(snr) = \frac{1}{2}\, mmse(snr) \qquad (1)$$

Simple as it is, the identity (I) was unknown before this work. It is trivial that one can compute the value of one monotone function given the value of another (e.g., by simply composing the inverse of the latter function with the former); what is quite surprising here is that the overall transformation (1) not only is strickingly simple but is also independent of the input distribution. In fact, this relationship and its variations hold under arbitrary input signaling and the broadest settings of Gaussian channel, including discrete-time and continuous-time channels, either in scalar or vector versions.

In a wider context, the mutual information and mean-square error are at the core of information theory and estimation theory, respectively. The input-output mutual information is an indicator of how much coded information can be pumped through a channel reliably given a certain input signaling, whereas the MMSE measures how accurately each individual input sample can be recovered using the channel output. Interestingly, (1) shows the strong relevance of mutual information to estimation and filtering and provides a noncoding operational characterization for mutual information. Thus, not only is the significane of an identity like (1) self-evident, but the relationship is intriguing and deserves through exposition.

## 5. Decoding of Reed Solomon Codes

It is shown that if an RS code is encoded by means of the Chinese remainder theorem, then decoding can be accomplished in a different manner from the usual decoding procedure for the cyclic RS codes Berlekamp (1968). This decoding method uses the Berlekamp algorithm, yet the roots of the error locator polynomial need not be found as in the Chien search nor the values of the errors determined. Instead, in this method, the calculation of the syndrome is more complicated, and a polynomial division must be accomplished. For low-rate codes, which correct a large number of errors, the total number of Galois field calculations may be less. It is also shown how this method is applicable to RS codes with less information symbols than the full length code.

RS codes constructed by means of the Chinese remainder theorem have the interesting property that each symbol in the encoded word is determined solely by the information symbols. Symbols can be discarded from an encoded word, reducing the distance of the word. If the distance of the full length codeword is 2t + 1, up to 2t symbols can be discarded. Each discarded symbol lowers the distance by one. This property may be useful in certain circumstances. For instance, Mandelbaum (1971) proposes a generalization to Tong' s burst-trapping technique (1969), which makes use of codewords with discardable redundancy. The resulting system can be used with more general channels.

It is also shown that how RS codes encoded by the Chinese remainder theorem in a different manner Mandelbaum (1968) can be decoded by finding the syndromes, solving a system of 2t linear equations, and executing a polynomial division. These codes have less information symbols than the full length RS code.

## 6. Decoding of Reed–Solomon with Alternant Codes

Here the main focus is on linear codes so that the set of codewords form a linear subspace of $\sum^N$. Reed–Solomon codes are a classical, and commonly used, construction of linear error-correcting codes that yield $[N = n, K = k + 1.\ D = n - k]_q$ codes for any $k < n \le q$. The alphabet for such a code is a finite field F. The message specifies a polynomial of degree at most k over F in some formal variable x (by giving its coefficients). The mapping C maps this code to its evaluation at distinct values of x chosen from F (hence it needs $q = |F| \ge n$). The distance property follows immediately from the fact that two degree k polynomials can agree in at most places.

The decoding problem for an $[N, K, D]_q$ code is the problem of finding a codeword in $\sum^N$ that is within a distance of e from a "received" word $R \in \sum^N$. In particular, it is interesting to study the error rate $e \overset{def}{=} e/N$ that can be corrected as a function of the information rate $k \overset{def}{=} K/N$. For a family of Reed–Solomon codes of constant message rate and constant error rate, the two brute-force approaches to the decoding problem (compare with all codewords, or look at all words in the vicinity of the received word) take time exponential in . It is, therefore, a nontrivial task to solve the decoding problem in polynomial time in . Surprisingly, a classical algorithm due to Peterson (1960) manages to solve this problem in polynomial time, as long as $e < \frac{N-K+1}{2}$ (i.e. achieves e = ( 1 – k) /2). Faster algorithms, with running time O($N^2$) or better, are also well known: in particular, the classical algorithms of Berlekamp and Massey (1968) achieve such running time bounds. It is also easily seen that if $c \geq \frac{N-K+1}{2}$ then there may exist several different codewords within distance of a received word, and so the decoding algorithm cannot possibly always recover the "correct" message if it outputs only one solution.

7. **Power Inequality in Gaussian Channels**

The differential entropy of the probability density function f(x) given by

$$h(X) = -\int_{-\infty}^{\infty} f(x)\,(u) \log fx\,(u)\, du \qquad (1)$$

The variance of a Gaussian random variable with the same differential entropy is maximum and equal to the variance when the random variable is Gaussian, and thus, the essence of is that the sum of independent random variables tends to be "more Gaussian" than or both of the individual components. In theory of communication (1948) Claude Shannon put forth the inequality

$$\exp(2h\,(X_1 + \ldots.. + X_n)) \geq \sum_{i=1}^{n} \exp(2h\,(X_i)) \qquad (2)$$

for n independent random variables.

The first proof of (1) was given by Stam (1959), based on an identity commumicated to him by N.G De Bruijn, which couples Fisher's information with Shannon's differential entropy.

Capitalizing on the relationship between mutual information and minimum mean-square error (MMSE) for additive Gaussian channels, this note gives a simpler proof of the entropy-power inequality (EPI) based on an elementary estimation-theoretic reasoning which sidesteps invoking Fisher's information. In a follow-up to this work, we use the MMSE to give simple proofs of two variations of the EPI, namely, Costa's strengthened EPI in which one of the variables is Gaussian Costa (1985), and a generalized EPI for linear transforms of a random vector due to Zamir and Feder (1993).

Following a simple "noise-incemental" argument, Guo & Shamai (2005) shows that regardless of the distribution of X we can write

$$\frac{d}{d\gamma} I\,(X : \sqrt{\gamma}\; X + N) = \frac{1}{2}\, mmse\,(X, \gamma) \tag{3}$$

Where N ~ N (0, 1) is standard Gaussian independent of X, and the MMSE of estimating X in unit-variance additive Gaussian noise is

$$mmse\,(X, \gamma) \quad \left\{(\mathrm{X} - \mathrm{E}\,\{\mathrm{X} \middle| \sqrt{\gamma}\; X + N\})^2 \right\}$$

Here γ is understood as the (gain of the ) signal-to-noise ratio of the Gaussian channel whose input is X.

A direct consequence of (3) is the represen-tation of the differential entropy of a random variable with variance $\sigma_x^2$ as

$$h(X) = \frac{1}{2}\log(2\pi e \sigma_x^2) - \frac{1}{2}\int_0^\infty \frac{\sigma_X^2}{1+\gamma\sigma_X^2} - mmse(X,\gamma)\, d\gamma \tag{4}$$

Thus, the nongaussianness of X (divergence of f(x) with respect to the Gaussian density with identical first and second moments) is given by one half of the integral of the difference of MMSEs achievable by a Gaussian input with variance $\sigma_x^2$ and by X, respectively.

For a unit variance X, (4) reduces to

$$h(X) = \frac{1}{2}\log(2\pi e) - \frac{1}{2}\int_0^\infty \frac{1}{1+\gamma} -- mmse(X,\gamma)\, d\gamma \tag{5}$$

It is amusing (and useful) to note that (5) holds even if X does not have unit variance: simply observe that

$$\log \sigma_x^2 = \int_0^\infty \frac{\sigma_X^2}{1+\gamma\sigma_X^2} - \frac{1}{1+\gamma}\, d\gamma \tag{6}$$

Note that whenever mmse (X, γ) = 0 (1/γ) (as in the case of a discrete random variable, where it vanishes exponentially), (4) indicates that h (X) = - ∞.

Since (5) expresses the differential entropy of an arbitrary random variable in terms of the MMSE of its estimation when observed in Gaussian noise, (1) can be seen as a relationship between the MMSEs (integrated over signal-to-noise ratios) of the sum and of the individual random variables.

## 8. Conclusion

In this general study, we can see that how the errors in Gaussian Channels centered around the mutual information between the input and the output of a channel, and the minimum mean-square error in estimating the input given the output. Also, we see that how the encoding and decoding of RS codes by different manners will take place. R.S. Codes are natural codes to use when a code is required of length less than the size of the field and also, the R.S. codes are the convenient codes for building other codes.

## References

[1] Berlekamp E.R., " Algebraic Coding Theory". New York; McGraw-Hill,1968.

[2] "Bounded distance +1 soft-decision Reed-solomon decoding, " IEEE Trans. Inform. Theory, Vol. 42, pp. 704-720. May 1996.

[3] Blahut R.E. "Theory and Practice of Error Control Codes". Reading, MA:Addison-Wesley,1983.

[4] H. Cohen, H., "A Course in Computational Algebraic Number Theory", GTM 138.Berlin, Germany: Springer Verlag, 1993.

[5] "Error - correcting codes for list decoding, " IEEE Trans. Inform. Theory, Vol. 37, pp. 5-12. 1991.

[6] Feng G.L. and Tzeng K.K.,“ A generalization of the Berlekamp-Massey algorithm for multisequence shift register synthesis with application to decoding cyclic codes,” IEEE Trans. Inform. Theory, Vol. 37, pp.1274-1287, 1991.

[7] Forney G.D., "Generalized minimum distance decoding, " IEEE Trans. Inform. Theory, Vol. IT-12, pp. 125-131, 1966.

[8] Hoholdt T., Van Lint J. H. and Pellikaan R., "Algebraic geometry codes, " in Handbook of Coding Theory, V.S. Pless, W.C. Huffamn, And R.A. Brualdi, Eds Amsterdam, the Netherlands: Elsevier.

[9] Justesen J., "Bounds on list decoding of MDS Codes, " unpublished manuscript, Apr.1998.

[10] Peterson W.W., "Encoding and error-correction procedures for Bose-Chaudhuri codes, " IRE Trans. Inform. Theory, Vol. IT-6, pp. 459-470, 1960.

[11] Roth R.M. and Ruckenstein G., "Efficient decoding of Reed-Solomon codes beyond half the minimum distance, "submitted to IEEE Trans. Inform. Theory, Aug. 1998.

[12] Shokrollahi M. A. and Wasserman H., " Decoding algebraic-geometric codes beyond the error-correction bound, " in Proc. 29th Annu. ACM Symp. Theory of Computing, 1998, pp. 241-248.

[13] Sidelnikov V.M., "Decoding Reed-Solomon codes beyond (d-1) = 2 and zeros of multivariate polynomials, " Probl. Inform. Transm., Vol. 30, No. 1, pp. 44-59, 1994.

[14] Stichtenoth H., " Algebraic Function Fields and Codes". Berlin, Germany: Springer-Vaelag, 1993.

[15] Sudan ., "Decoding of Reed-solomon codes beyond the error-correction bound, " J. Complexity, Vol. 13, No.1,pp. 180-193,1997.

[16] "Decoding of Reed-solomon codes beyond the error-correction diameter, " in Proc. 35th Annu. Allerton Conf. Communication, control and computing, 1997.

[17] Van Lint J.H., "Introduction to Coding Theory. New York: Springer-Verlag,1982.

[18] L. Welch and E.R. Berlekamp, "Error correction of algebraic block codes, " U.S. Patent 4 633 470, Dec. 1986.

[19] Peterson W.W. and Weldon, Jr. E.J., Error-Correcting Codes, second edition Cambridge, Mass.: M.I.T. Press, 1972.

[20] Justesen J., "A class of constructive asymptotically good algebraic codes," IEEE Trans. Inform. Theory, Vol. IT-1 and pp.652-656, Sept. 1972.

[21] Zyablov V.V., "on estimation of complexity of construction of binary linear concatenated codes," Probl, Peredach. Inform., Theory, Vol. 7, No.1, 1971.

[22] Weldon Jr. E.J., " Justeen's construction-the low rate case, " IEEE Trans. Inform. Theory, Vol. IT-19,pp. 711-713, Sept., 1973.

[23] Gulliwer T.A., " Self-reciprocal polynomials and generalized fermat numbers, " IEEE Trans. Inform. Theory, Vol. 38, pp. 1149-1154, May, 1992.

[24] Massey J.L., "Reversible codes, " Inform. Contr., Vol, 7, pp. 369-380, 1964.

[25] Wolf J.K., "Adding two information symbols to certain nonbinary BCH codes and some applications, " BellSyst. Tech. J., Vol. 48,pp. 2005-2024, 1969.

[26] Berlekamp E.R., "Algebraic Coding Theory", second edition Laguna Hills, CA: Aegean Park, 1984.

[27] Chien R.T., "Cyclic Decoding Procedures for Bose-Chaudhuri-Hoc-quenghem codes, " IEEE Trans. Inform. Theory, Vol. IT-10, pp. 357-363, 1964.

[28] Elias P., " Error-correcting codes for list decoding, " IEEE Trans. Inform. Theory, Vol. 37, pp. 5-12, 1991.