Goppa Codes

Key One Chung

December, 2004

Department of Mathematics, Iowa State University,

Ames, Iowa 50011-2064

email: kochung@iastate.edu

Contents

1 Introduction

1.1 Linear Codes

Definition. *A linear code $C(n,k)$ over a field F is a vector subspace of F^n with dimension k. n is called the length of the code C. The minimum distance of C is $d := \min\{d(x,y)|x,y \in C, x \neq y\}$, where $d(x,y)$ is the Hamming distance. (n,k,d) is called the parameter of C.*

If a basis for C is $\{r_1, \ldots, r_k\}$, then

$$G = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_k \end{pmatrix}$$

is a generator matrix for C, and $C = \{uG|u \in F^k\}$.

What is a good code?

Why are d and k of C important?

- dimension k: the larger, the better

  We may think of each codeword as having k information symbols and $n-k$ checks. So, large k with respect to n makes an efficient code.

- minimum distance d: the larger, the better

  We can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors.

How good can a code be?

1.2 Bounds on Codes

Theorem (Singleton Bound). *Let $C(n,k)$ be a linear code of minimum distance d over $\mathbf{F}_q$. Then, $d \leq n-k+1$.*

Given n, both k and d cannot be large.

Definition. *Let q be a prime power and let n, d be positive integers with $d \leq n$. Then the quantity $A_q(n,d)$ is defined as the maximum value of M such that there is a code over $\mathbf{F}_q$ of length n with M codewords and minimum distance d.*

Let $V_q(n,r)$ denote the number of elements in the ball of radius r centered at x, for any $x \in \mathbf{F}_q^n$. Then, $V_q(n,r) = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i$.

Theorem (Gilbert-Varshamov Bound). $A_q(n,d) \geq q^n / V_q(n,d-1)$.

Asymptotic Bounds

Definition. *Let C be a code over $\mathbf{F}_q$ of length n with q^k codewords and minimum distance d. The information rate of C is $R := k/n$ and the relative minimum distance of C is $\delta := d/n$.*

Note that $0 \leq R, \delta \leq 1$, and C is a good code if both R and δ are close to 1.

Definition. *Let q be a prime power and $\delta \in \mathbf{R}$ with $0 \leq \delta \leq 1$. Then*

$$\alpha_q(\delta) := \limsup_{n \to \infty} \frac{1}{n} \log_q A_q(n, \delta n).$$

$\alpha_q(\delta)$ is the largest R such that there is a sequence of codes over $\mathbf{F}_q$ with relative minimum distance converging to δ and information rate converging to R.

Set $\theta = 1 - 1/q$.

We define a function $H_q(x)$ on $0 \leq x \leq \theta$ by

$$H_q(x) := 0, \text{ if } x = 0$$
$$x \log_q(q-1) - x \log_q x - (1-x)\log_q(1-x), \text{ if } 0 < x \leq \theta.$$

The function H_q is called the *Hilbert entropy function*.

Theorem (Asymptotic Gilbert-Varshamov Bound). *For any δ with $0 \leq \delta \leq \theta$, we have $\alpha_q(\delta) \geq 1 - H_q(\delta)$.*

The Gilbert-Varshamov Bound was the best known lower bound on $\alpha_q(\delta)$ for a full 30 years following its original discovery in 1952. In 1982, the existence of a sequence of codes having better than The Gilbert-Varshamov Bound was first proven by Tsfasman, Vladut, and Zink using Goppa codes.

1.3 Reed-Solomon Codes

Definition. $L_r := \{f \in \mathbf{F}_q[x] | deg(f) \leq r\} \bigcup \{0\}$

Note that L_r is a vector subspace over $\mathbf{F}_q$.

Definition. $\mathbf{F}_q^* = \{\alpha_1, \ldots, \alpha_{q-1}\}$ *and* $1 \leq k \leq q-1$. *Then the Reed-Solomon code* $RS(k,q)$ *is defined to be*

$$RS(k,q) := \{(f(\alpha_1), \ldots, f(\alpha_{q-1})) | f \in L_{k-1}\}.$$

It is an image of a linear transformation $\epsilon : L_{k-1} \rightarrow \mathbf{F}_q^{q-1}$ given by

$$\epsilon(f) = (f(\alpha_1), \ldots, f(\alpha_{q-1})).$$

Parameters of $RS(k,q)$ are $n = q-1$, $dim\, C = k$, and $d = n - k + 1$.

- By singleton bound, given $n = q - 1$ and dimension k, $RS(k, q)$ is the best.
- However, it is a very restrictive class of codes because the length is so small with regard to the alphabet size. (q-1,q)
- In practice, we want to work with codes which are long with respect to the alphabet size.

2 Goppa Codes

2.1 Introduction to Goppa Codes (1981)

1. Choose a finite field $\mathbf{F}_q$.
2. Choose a projective nonsingular plane curve X over $\mathbf{F}_q$.
3. Pick n distinct $\mathbf{F}_q$-rational points

$$\mathcal{P} = \{P_1 \ldots, P_n\} \subset X(\mathbf{F}_q) \text{ on } X.$$

4. Choose a divisor D on X such that $\mathcal{P} \bigcap supp(D) = \emptyset$.
5. Goppa code

$$C(X, \mathcal{P}, D) := \{(f(P_1, \ldots, f(P_n)))|f \in L(D)\} \subset \mathbf{F}_q^n.$$

Note

1. $dim\, C = dim\, L(D)$

2. If $\{f_1, \ldots, f_k\}$ is a basis for $L(D)$ over $\mathbf{F}_q$, then
$$\begin{pmatrix} f_1(P_1) & \cdots & f_1(P_n) \\ \vdots & \ddots & \vdots \\ f_k(P_1) & \cdots & f_k(P_n) \end{pmatrix}$$
is a generator matrix for C.

3. It is the first infinite family of codes whose parameters beats the Gilbert-Varshamov bound.

2.2 Algebraic and Projective Curves

$\overline{k}$ denotes the algebraic closure of the field k.

Definition. *We define the affine place $A^2(k)$ to be the set k^2.*

Definition. *If $f \in k[x, y]$, then the affine(algebraic) curve is defined to be*

$$C_f := \{P \in A^2 | f(P) = 0\}.$$

Let X be an algebraic curve over k. Then,

$$I(X) = \{f \in k[x, y] | f(P) = 0 \text{ for all } P \in X\}$$

is an ideal of $k[x, y]$. The quotient ring $\Gamma(X) = k[x, y]/I(X)$ is called the coordinate ring of X.

Example. $f(x,y) = y - x^2$ and $g(x,y) = y - c \in \mathbf{R}[x,y]$.

In $\mathbf{R}$, if $c > 0$, then we have two intersections.
If $c = 0$, then we have a single intersection of multiplicity 2.

In $\mathbf{C} = \overline{\mathbf{R}}$, $|C_f \bigcap C_g| = 2$.

If $g(x,y) = x - c$, then we have one intersection. However, if we regard C_f and C_g intersect once at "infinity" as well, then $|C_f \bigcap C_g| = 2$.

For given $f(x, y) \in k[x, y]$, we construct the polynomial

$$F(X, Y, Z) = Z^d f(X/Z, Y/Z) \in k[X, Y, Z]$$

where $d = deg(f)$. The polynomial F is called the *homogenization* of f.

Observation

- $f(x_0, y_0) = 0 \Leftrightarrow F(x_0, y_0, 1) = 0$
- For any $\alpha \in k^*$, we have $F(\alpha X, \alpha Y, \alpha Z) = \alpha^d F(X, Y, Z)$.
  So, $F(X_0, Y_0, Z_0) = 0 \Leftrightarrow F(\alpha X_0, \alpha Y_0, \alpha Z_0) = 0$ for all $\alpha \in k^*$.
  $\Rightarrow$ We identify the solutions (X_0, Y_0, Z_0) and $(\alpha X_0, \alpha Y_0, \alpha Z_0)$.
- Since F is homogeneous, $F(0, 0, 0) = 0$.
  $\Rightarrow$ We ignore the solution $(0, 0, 0)$ of $F = 0$.

Definition. *The projective plane is*

$$\mathbf{P}^2(k) := (k^3 \backslash \{(0,0,0)\}) / \sim$$

where $(X_0, Y_0, Z_0) \sim (X_1, Y_1, Z_1)$ *if and only if there is some* $\alpha \in k^*$ *with* $X_1 = \alpha X_0$, $Y_1 = \alpha Y_0$, *and* $Z_1 = \alpha Z_0$. *We write* $(X_0 : Y_0 : Z_0)$ *for the equivalence class of* (X_0, Y_0, Z_0) *in* $\mathbf{P}^2$.

By multiplying through by a unit, we have

$$\mathbf{P}^2(k) = \{(X_0 : Y_0 : 1) | X_0, Y_0 \in k\} \bigcup \{(X_0 : 1 : 0) | X_0 \in k\} \bigcup \{(1 : 0 : 0)\}.$$

Any point of the form $(X : Y : 0)$ is called a *point at infinity*.

Definition. *Let F be the homogenization of f. Then the projective curve of F is*

$$\widehat{C_f} := \{(X_0 : Y_0 : Z_0) \in \mathbf{P}^2(\overline{k}) | F(X_0, Y_0, Z_0) = 0\}.$$

Example. $f(x, y) = y - x^2, g(x, y) = x - c.$ What is $\widehat{C_f} \bigcap \widehat{C_g}$?

$F(X, Y, Z) = Z^2(Y/Z - (x/Z)^2) = YZ - X^2$

$G(X, Y, Z) = X - cZ$

When $Z = 1, Y = X^2$ and $X = c$. So, we have $(c : c^2 : 1)$.

When $z = 0, X = 0 = X^2$. So, we have $(0 : 1 : 0)$.

Therefore, $|\widehat{C_f} \bigcap \widehat{C_g}| = 2$.

Theorem (Bezout's Theorem). *If $f, g \in k[x, y]$ are polynomials of degree d and e respectively, then C_f and C_g intersect in at most de points. Further, $\widehat{C_f}$ and $\widehat{C_g}$ intersect in exactly de points of $\mathbf{P}^2(\overline{k})$, when points are counted with multiplicity.*

2.3 Nonsingularity and the Genus

For coding theory, we only want to work with "nice" curves. Since we have already decided to restrict ourselves to plane curves, the only other restriction we will need is that our curve will be *nonsingular*.

Definition. *Let $f(x,y) \in k[x,y]$. A singular point of C_f is a point $p \in \overline{k} \times \overline{k}$ such that $f(p) = f_x(p) = f_y(p) = 0$. The curve C_f is nonsingular if it has no singular points. If F is the homogenization of f, then $P \in \mathbf{P}^2(\overline{k})$ is a singular point of $\widehat{C_f}$ if $f(P) = F_X(P) = F_Y(P) = F_Z(P) = 0$. The curve $\widehat{C_f}$ is nonsingular if it has no singular points.*

Note. Intuitively, a singular point is a point where the curve does not have a well-defined tangent line, or where it intersects itself.

Definition (Plücker Formula). *Let $f(x,y) \in k[x,y]$ be a polynomial of degree d such that $\widehat{C_f}$ is nonsingular. Then the genus of C_f (or of $\widehat{C_f}$) is defined to be*

$$g := \frac{(d-1)(d-2)}{2}.$$

2.4 Points, Functions, Divisors on Curves

Definition. *Let C be the projective plane curve defined by $F = 0$, where $F \in k[X, Y, Z]$ is a homogeneous polynomial. Let K be an extension field of k. We define a K-rational point on C to be a point $(X_0, Y_0, Z_0) \in \mathbf{P}^2(K)$ such that $F(X_0, Y_0, Z_0) = 0$. $C(K)$ denotes the set of all K-rational points on C.*

Definition. *Let C be a nonsingular projective plane curve. A point of degree n on C over $\mathbf{F}_q$ is a set $P = \{P_0, \ldots, P_{n-1}\}$ of n distinct points in $C(\mathbf{F}_{q^n})$ such that $P_i = \sigma_{q,n}^i(P_0)$ for $i = 1, \ldots, n-1$, where $\sigma_{q,n}^i : \mathbf{F}_{q^n} \to \mathbf{F}_{q^n}$ is the Frobenius automorphism with $\sigma_{q,n}(\alpha) = \alpha^q$.*

Note. Elements of $C(k)$ are called points of degree one or simply rational points.

Example. Let C_0 be the projective plane curve over $\mathbf{F}_3$ corresponding to

$$f(x,y) = y^2 - x^3 - 2x - 2 \in \mathbf{F}_3[x,y].$$

Homogenization; $F(X,Y,Z) = Y^2Z - X^3 - 2XZ^2 - 2Z^3 = 0$

$$\begin{aligned} F_X &= -4Z = 2Z = 0 \\ F_Y &= 2YZ = 0 \\ F_Z &= Y^2 - 4XZ = Y^2 + 2XZ = 0 \end{aligned}$$

$\Rightarrow Z = Y = X = 0$. So, C_0 is nonsingular.

Also, genus $g = \frac{2\cdot 1}{2} = 1$.

Now, let's find points of degree 1(rational points) $C_0(\mathbf{F}_3)$.

$$y^2 - x^3 - 2x - 2 = 0$$

If $x = 0$, then $y^2 = 2$. No such elements in $\mathbf{F}_3$.
If $x = 1$, then $y^2 = 2$. No such elements in $\mathbf{F}_3$.
If $x = 2$, then $y^2 = 2$. No such elements in $\mathbf{F}_3$.

So, no rational points of the type $(X : Y : 1)$.

When $Z = 0$, $-X^3 = 0$. So, $X = 0$.

So, $C_0(\mathbf{F}_3) = \{P_\infty := (0 : 1 : 0)\}$.

To find the points of degree 2, let's compute $C_0(\mathbf{F}_{3^2})$ first.

Note that t^2+1 is irreducible over $\mathbf{F}_3$. Then $\mathbf{F}_9 = \mathbf{F}_3[t]/(t^2+1)$.

Let $\alpha \in \mathbf{F}_9$ corresponding t. Then, $\mathbf{F}_9 = \{a+b\alpha | a, b \in \mathbf{F}_3\}$, where $\alpha^2 = -1 = 2$. When $Z = 1$, $Y^2 - X^3 - 2X - 2 = 0$.

If $X = 0$, $Y^2 = 2 \Rightarrow Y = \alpha$ or $-\alpha = 2\alpha$.

So, $(0:\alpha:1), (0:2\alpha:1) \in C_0(\mathbf{F}_9)$.

By doing similar computation,

$$C_0(\mathbf{F}_9) = \{(0:\alpha:1), (0:2\alpha:1), (1:\alpha:1), (1:2\alpha:1), (2:\alpha:1), (2:2\alpha:1), P_\infty\}.$$

Frobenius map $\sigma_{3,2} : \mathbf{F}_9 \to \mathbf{F}_9; \alpha \mapsto \alpha^3 = 2\alpha$

Then, $\sigma_{3,2}(0:\alpha:1) = (0:2\alpha:1)$.

So, we have one point $Q_1 = \{(0:\alpha:1), (0:2\alpha:1)\}$ of degree 2.

Similarly, $Q_2 = \{(1:\alpha:1), (1:2\alpha:1)\}$, $Q_3 = \{(2:\alpha:1), (2:2\alpha:1)\}$.

So, we have three points of degree two on C_0.

Similarly, $\mathbf{F}_{3^3} = \mathbf{F}_3[t]/(t^3 + 2t + 2)$ and let $w \in \mathbf{F}_{27}$ corresponding to t.

Then, we have

$$C_0(\mathbf{F}_{27}) = \{(w : 0 : 1), (1 + w : 0 : 1), \ldots, (1 + 2w + 2w^2 : 1 + 2w + 2w^2 : 1), P_\infty\}.$$

with 28 $\mathbf{F}_{27}$-rational points.

Also, we see that

$$C_0(\mathbf{F}_{27}) = R_1 \bigcup \cdots \bigcup R_9 \bigcup \{P_\infty\}$$

where $R_1, \ldots, R_9$ are the nine points of degree three on C_0.

For example, $R_1 = \{(w : 0 : 1), (1 + w : 0 : 1), (2 + w : 0 : 1)\}$.

Let C and C' be two projective plane curves over $\mathbf{F}_q$ defined by polynomials of degree d and e respectively. Then, the set of points over $\overline{\mathbf{F}_q}$ where they intersect will cluster into points $P_1, \ldots, P_l$ of varying degrees over $\mathbf{F}_q$, where a point is listed more than once if the intersection of the two curves is with multiplicity greater than one.

Let r_i denote the degree of the point P_i over $\mathbf{F}_q$. Then, we have $de = r_1 + r_2 + \cdots + r_l$. In this case, we write

$$C \bigcap C' = P_1 + \cdots + P_l$$

and call $C \bigcap C'$ the intersection divisor of C and C'.

Definition. • *Let C be a curve defined by over F_q. A divisor D on C over $\mathbf{F}_q$ is an element of the free abelian group on the set of points(of arbitrary degree) on C over $\mathbf{F}_q$.*

Thus every divisor is of the form $D = \sum n_Q Q$, where the n_Q are integers and each Q is a point (of arbitrary degree) on C.

- *If $n_Q \geq 0$ for all Q, we call D effective and write $D \geq 0$.*
- *We define the degree of the divisor $D = \sum n_Q Q$ to be $deg\ D = \sum n_Q deg\ Q$.*
- *the support of the divisor $D = \sum n_Q Q$ is $supp\ D = \{Q | n_Q \neq 0\}$.*

Note $C \bigcap C'$ is an effective divisor of degree de.

Definition. *Let $F(X,Y,Z)$ be the polynomial which defines the nonsingular projective plane curve C over the field $\mathbf{F}_q$. The field of rational functions on C is*

$$\mathbf{F}_q(C) := \left(\left\{ \frac{g(X,Y,Z)}{h(X,Y,Z)} | g,h \in \mathbf{F}_q[X,Y,Z] \text{ hom. same deg} \right\} \bigcup \{0\} \right) / \sim$$

where $g/h \sim g'/h'$ if and only if $gh' - g'h \in \langle F \rangle \subset \mathbf{F}_q[X,Y,Z]$.

Example $F(X,Y,Z) = Y^2Z - X^3 - 2XZ^2 - 2Z^3 \in \mathbf{F}_3[X,Y,Z]$.
Then $X^2/Z^2 = (Y^2 + XZ + Z^2)/XZ$ in $\mathbf{F}_3(C_0)$
since

$$X^2(XZ) - Z^2(Y^2 + XZ + Z^2) = Z(X^3 - ZY^2 - XZ^2 - Z^3) \in \langle F \rangle.$$

Definition. *Let C be a curve defined over $\mathbf{F}_q$ and let $f := g/h \in \mathbf{F}_q(C)$. The divisor of f is defined to be $div(f) := \sum P - \sum Q$, where $\sum P$ is the intersection divisor $C \bigcap C_g$ and $\sum Q$ the intersection divisor $C \bigcap C_h$.*

Note that since $deg(C \bigcap C_g) = deg(C \bigcap C_h)$, we have $deg\ div(f) = 0$.

Definition. *Let D be a divisor on the nonsingular projective plane curve C defined over the field $\mathbf{F}_q$. Then the space of rational functions associated to D is*

$$L(D) := \{f \in \mathbf{F}_q(C) | div(f) + D \geq 0\} \bigcup \{0\}.$$

Note $L(D)$ is a finite dimensional vector space over $\mathbf{F}_q$.

Theorem (Riemann-Roch Theorem). *Let C be a nonsingular projective plane curve of genus g defined over $\mathbf{F}_q$ and let D be a divisor on C. Then $dim\ L(D) \geq deg\ D + 1 - g$. Further, if $deg\ D > 2g - 2$, then*

$$dim\ L(D) = deg\ D + 1 - g.$$

2.5 Good Codes from Algebraic geometry

Theorem. *Let X be a nonsingular, projective plane curve of genus g, defined over $\mathbf{F}_q$. Let $\mathcal{P} \subset X(\mathbf{F}_q)$ be a set of n distinct $\mathbf{F}_q$-rational points on X, and let D be a divisor on X satisfying $2g-2 < deg\ D < n$. Then, Goppa code $C := C(X, \mathcal{P}, D)$ is linear of length n, dimension $k := deg\ D + 1 - g$, and the minimum distance d, where $d \geq n - deg\ D$.*

Note The information rate R of C is $k/n = (deg\ D + 1 - g)/n$ and the relative minimum distance δ of C is $d/n \geq (n - deg\ D)/n$.
We want $R + \delta$ large. We have

$$R + \delta \geq \frac{deg\ D + 1 - g}{n} + \frac{n - deg\ D}{n} = 1 + 1/n - g/n.$$

So, for given genus g, it is better to have large $n \leq |X(\mathbf{F}_q)|$.

How many rational points can a curve of genus g have?

Theorem (Hasse-Weil). *let X be a nonsinguar projective curve of genus g over $\mathbf{F}_q$ and set $N = |X(\mathbf{F}_q)|$. Then*

$$|N - (q+1)| \leq 2g\sqrt{q}.$$

Theorem (Serre). *In the situation of the above theorem, we have*

$$|N - (q+1)| \leq g\lfloor 2\sqrt{q} \rfloor$$

3 McEliece Public Key Cryptosystem

3.1 Idea

Syndrome decoding of linear codes (when considered as a decision problem) is an NP-complete problem if the number of errors is not bounded. However, there are classes of linear codes which have very fast decoding algorithms. The basic idea of the McEliece system is to take one of these linear codes and disguise it so that Oscar, when trying to decrypt a message, is forced to use syndrome decoding, while Bob, who set up the system, can remove the disguise and use the fast decoding algorithm. McEliece suggested using Goppa Codes, which are linear codes with a fast decoding algorithm, in the system, but any linear code with a good decoding algorithm can be used.

3.2 Key Creation

- The private key consists of the matrices (S, G, P), where S is a random, invertible $k \times k$ matrix, P is a random $n \times n$ permutation matrix, and G is the $k \times n$ generator matrix of a Goppa code that corrects up to t errors.

- The public key is the matrix product of the three private matrices, so it is a $k \times n$ matrix $\widehat{G} = SGP$. Additionally, a number $t' \leq t$ has to be advertised which stands for the number of errors that a sender of a message is allowed to add to his message. So the public key is $(\widehat{G}, t')$.

3.3 Encryption

The plain text is dissected into blocks of size k bits. For every block a random error vector of size n that has at most t' entries is chosen and is added to the encoding $\widehat{G}$:

$$c = m\widehat{G} + e$$

3.4 Decryption

The receiver multiplies the cipher text with the inverse of the permutation matrix:

$$c' = cP^{-1} = m\widehat{G}P^{-1} + eP^{-1} = mSG + eP^{-1}$$

Since G is a t error correcting code and eP^{-1} will contain at most the $t' \leq t$ intentional errors, he can quickly Goppa decode into c' and already has the result mS. To get the plain text messages he will then multiply with the inverse of S.

$$m = mSS^{-1}$$

3.5 Security

To be able to use a trap door Goppa code to decipher a message, the inverse matrices of P and S have to be known. If some unauthorized person does not have this information, she will face the problem to solve a linear code. With an average choice of $t \geq 50$ and $n \geq 2^{10}$, this is a very difficult problem.

3.6 Drawbacks

- The size of the public key $\widehat{G}$ is quite large. Using the Goppa code with parameters suggested by McEliece, the public key would consist of 2^{19} bits. This will certainly cause implementation problems.
- The encrypted message is much longer than the plaintext message. This increase of the bandwidth makes the system more prone to transmission errors.

3.7 Discussion

$$m \xrightarrow{\text{encrypt}} c \xrightarrow{\text{encode}} c' \xrightarrow{\text{public line}} c' + e \xrightarrow{\text{decode}} c \xrightarrow{\text{decrypt}} m$$

$$m \xrightarrow{\text{encrypt}} c = m\widehat{G} + e \xrightarrow{\text{public line}} c' = m\widehat{G} + e + e' \xrightarrow{\text{decrypt}} m$$

Assume that we have a Goppa code $C(n, k)$ with the minimum distance $d = 2t + 1$. As we stated, if $t \geq 50$ and $n \geq 2^{10}$, then McEliece Cryptosystem is considered to be fairly secure. However, we need a big key size. We know that cellular phone does not require much security. Therefore, it would be a good problem to find a proper t, t' and n having a little security for cellular phone and not so much big key size. In this case, we can correct up to $t - t'$ errors.

References

[1] J.L. Walker, *Codes and Curves*, American Mathematical Society (2000), 1–44.

[2] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer (1986), 1–44.

[3] P.J. Morandi, *Error Correcting Codes and Algebraic Curves*, Lecture Notes (2001), 3–63, http://emmy.nmsu.edu/ pmorandi/math601f01/LectureNotes.pdf.

[4] B. Cherowitzo , http://www-math.cudenver.edu/ wcherowi/courses/m5410/ctcmcel.html.

[5] http://entropy.stop1984.com/en/mceliece.html.