Concept of field

Group Let G be a set of elements with following properties:

- Closure: For binary operation $\star$, $c = a \star b$ with c uniquely defined and $a, b, c \in G$.
- Associative: $a \star (b \star c) = (a \star b) \star c$
- Identity element: For $a, e \in G$, $a \star e = e \star a = a$
- Inverse: $a \star a' = a' \star a = e$
- Commutative group: When $a \star b = b \star a$

Proof for uniqueness of e: $e' = e' \star e = e$

Proof for uniqueness of a':

$a' = a' \star e = a' \star (a \star a'') = (a' \star a) \star a'' = a''$

G=0,1 with modulo-2 addition $\oplus$

Other examples: modulo-m addition, modulo-p multiplication with prime p $1, 2, \ldots, p-1$

FIELD: A set of element $F, +, \cdot$ is called field if:

- F is commutative group under addition where identity element is Zero.

- Non-Zero elements of F is commutative group under multiplication where identity element is 1.

- Distributive $\cdot$ over $+$

  $a \cdot (b + c) = a \cdot b + a \cdot c$

Finite fields are known as Galois field. For prime p, $GF(p^m)$ is extended field. Characteristic of finite field λ is obtained from $\sum_{i=1}^{\lambda} 1 = 0$

Example: Binary field 0,1 with $\lambda = 2$

Cyclic group: Smallest n such that $a^n = 1$ If powers of an element constitute the whole group.

Example: The element is called primitive. 3 is primitive element of $GF(7)$

Binary field arithmetic

Polynomial $f(x) = f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n$ with f_i= 0 or 1 for $0 \leq i \leq n$

Largest power of x with non-zero coefficient gives the degree.

Add or Subtract polynomials over $GF(2)$ satisfy commutative, associative, distributive properties.

Division $\frac{f(x)}{g(x)}$ gives quotient $q(x)$ and remainder $r(x)$ Degree of $r(x) < g(x)$

If $r(x) = 0$, $g(x)$ is a factor of $f(x)$

If a is a root, $(x + a)$ divides $f(x)$.

If $f(x)$ has even no of terms, $f(x)$ is divisible by $(x + 1)$

$p(x)$ is irreducible, if it is not divisible by any polynomial of lesser degree. $x^2 + x + 1$, $x^3 + x + 1$, $x^4 + x + 1$ are irreducible.

Binary field arithmetic

Any irreducible polynomial of degree m divides $x^{2^m-1}+1$.

Ex. x^3+x+1 divides x^7+1.

$p(x)$ is primitive if smallest n for $p(x)$ that divides x^n+1 is $n=2^m-1$.

Ex. x^4+x+1 is primitive. $x^4+x^3+x^2+x+1$ is irreducible but divides x^5+1.

Squaring of $f(x)$ gives

$$f^2(x) = (f_0 + f_1 x + \ldots + f_n x^n)^2$$

$$= f_0^2 + f_0(f_1 x + \ldots) + f_0(f_1 x + \ldots) + (f_1 x + \ldots)^2$$

$$= f_0^2 + (f_1 x + \ldots)^2$$

$= f_0^2 + (f_1 x)^2 + \ldots + (f_n x^n)^2$

$= f_0 + f_1 x^2 + f_2 (x^2)^2 + \ldots$

Therefore, we have $f^2(x) = f(x^2)$ and in general,, $[f(x)]^{2^l} = f(x^{2^l})$

Roots and conjugates: If β, an element from extension field of $GF(2)$, is a root of $f(x)$, then β^{2^l} is also a root.

Since $[f(x)]^{2^l} = f(x^{2^l})$ putting $x = \beta$ $[f(\beta)]^{2^l} = f(\beta^{2^l})$ and β is a root implies $f(\beta) = 0$ and $f(\beta^{2^l}) = 0$ so that $\beta^{2^l})$ is also a root, called conjugates of β.

Ex. $f(x) = 1+x^3+x^4+x^5+x^6$ Then $\alpha, \alpha^2, \alpha^4, \alpha^8 \in GF(2^4)$ are all roots of $f(x)$

Now, $\beta^{2^m-1} = 1$ gives roots of $x^{2^m-1} + 1$ The $2^m - 1$ non-zero elements of $GF(2^m)$ form all roots of $x^{2^m-1} + 1$.

Minimal polynomial: $\phi(x)$ of smallest degree over $GF(2)$ such that $\phi(\beta) = 0$

It is irreducible: If $\phi(x) = \phi_1(x)\phi_2(x)$, say, then if $\phi(\beta) = 0$ $\phi_1(\beta) = 0$ or $\phi_2(\beta) = 0$ implying there exists polynomial for smaller degree that meets the condition. i.e $\phi(x)$ is not minimal.

Divisibility: Consider $f(x)$ over $GF(2)$, $\phi(x)$ is minimal for some β and β is root of $f(x)$ then $\phi(x)$ divides $f(x)$.

Let $f(x) = q(x)\phi(x)+r(x)$. For the root $x = \beta$, $f(\beta) = \phi(\beta) = 0$ so that $r(x) = 0$ which proves the divisibility. When $f(x)$ is irreducible, $f(x)$ and $\phi(x)$ are same. Then, $\phi(x)$ divides $x^{2^m}+x$ from conjugates concept.

Consider $f(x) = \prod_{i=0}^{e-1} (x+\beta^{2^i})$ where $\beta \in GF(2^m)$ such that $\beta^{2^e} = \beta$ with e as smallest non negative integer. $f(x)$ so constructed is irreducible

polynomial over $GF(2)$. This can be shown considering that its coeeficients can be only 0 or 1 and there are no factors.

$[f(x)]^2$ would have terms $(x+\beta^{2^i})^2$ i.e.

$$[f(x)]^2 = \prod_{i=0}^{e-1}(x^2+\beta^{2^{i+1}})$$

$$[f(x)]^2 = \prod_{i=1}^{e}(x^2+\beta^{2^i})$$

$$[f(x)]^2 = \prod_{i=1}^{e-1}(x^2+\beta^{2^i})(x^2+\beta^{2^e})$$

Since $\beta^{2^e} = \beta$;

$$[f(x)]^2 = \prod_{i=0}^{e-1}(x^2+\beta^{2^i})$$

Therefore, $[f(x)]^2 = f(x^2)$

Let $f(x) = f_0 + f_1 x + f_2 x^2 + \ldots + f_e x^e$

Then $[f(x)]^2 = \sum f_i^2 x^{2i}$

and from $f(x^2) = \sum f_i x^{2i}$

we conclude $f_i^2 = f_i$

This can only happen when $f_i = 0/1$

So, $f(x)$ has coefficients from $GF(2)$ only.

Suppose it is not irreducible so that $f(x) = a(x)b(x)$

Since $f(\beta) = 0$ either $a(\beta) = 0$ or $b(\beta) = 0$

Then conjugates of β are also roots and $a(x)$ or $b(x)$ would be of degree e and would match with $f(x)$.

Therefore, $f(x)$ must be irreducible.

Constructing $GF(2^m)$ and its arithmetic

In a finite field $GF(q)$, a nonzero element a is said to be Primitive if the order of a is $q-1$.

Therefore the power of the primitive element generate all the nonzero element of $GF(q)$.

To construct elements of $GF(2^m)$ start from primitive polynomial of degree m; with α as root of $p(x)$. Powers of α generate all non-zero elements of $GF(2^m)$. Order of α is 2^m-1

Ex. Consider $\beta = \alpha^7$ in $GF(2^4)$ Powers of $\beta^{0\ldots15}$ generate all non-zero elements, $\alpha^{15} = 1$ Conjugates of β are $(\alpha^7)^2$, $\beta^{2^2} = \alpha^{13}$, $\beta^{2^3} = \alpha^{11}$. α^7 is primitive of $GF(2^7)$

If β is an element of order n in $GF(2^m)$ [i.e. $\beta^n = 1$], all conjugates of β are of order n.

Ex. Consider α^5 in $GF(2^4)$. Its conjugate is α^{10} Order of them is $n = 3$ Their minimal polynomial is x^2+x+1 whose degree is a factor of $m = 4$.

$Conj(\alpha^3) = \alpha^6; \alpha^9; \alpha^{12}$ all have order $n = 5$

To construct elements of $GF(2^4)$ start from primitive polynomial of degree 4; $p(x) = x^4 + x + 1$.

Set $p(\alpha) = 0$ so that $\alpha^4 = 1 + \alpha$ is the identity used to represent polynomials

Power representation $0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}$. It is good for $\cdot$ operation.

Tuple representation $f_0 + f_1\alpha + f_2\alpha^2 + f_3\alpha^3$. It is good for $+$ operation.

$< f_0, f_1, f_2, f_3 >$ representation is used for coding.

Power	Polynomial	4-tuple
0	0	0000
1	1	1000
α	α	0100
α^2	α^2	0010
α^3	α^3	0001
α^4	$1+\alpha$	1100
α^5	$\alpha+\alpha^2$	0110
α^6	$\alpha^2+\alpha^3$	0011
α^7	$1+\alpha+\alpha^3$	1101
α^8	$1+\alpha^2$	1010
α^9	$\alpha+\alpha^3$	0101
α^{10}	$1+\alpha+\alpha^2$	1110
α^{11}	$\alpha+\alpha^2+\alpha^3$	0111
α^{12}	$1+\alpha+\alpha^2+\alpha^3$	1111
α^{13}	$1+\alpha^2+\alpha^3$	1011
α^{14}	$1+\alpha^3$	1001

Conjugate roots	Minimal Polynomial
0	x
1	$x+1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	x^4+x+1
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$x^4+x^3+x^2+x+1$
α^5, α^{10}	x^2+x+1
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	x^4+x^3+1

Computations involving $GF(2^m)$ arithmetic

For $m = 4$; solve the system $X + \alpha^7 Y = \alpha^2$ and $\alpha^{12} X + \alpha^8 Y = \alpha^4$

Applying Cramer's rule, $X = \frac{\alpha^{10}+\alpha^{11}}{\alpha^8+\alpha^{19}}$ and $Y = \frac{\alpha^{14}+\alpha^4}{\alpha^8+\alpha^{19}}$

Simplifying, $X = \alpha^9$ and $Y = \alpha^4$.

Polynomial with coefficients in $GF(2^m)$: Consider $f(X) = X^2 + \alpha^7 X + \alpha = 0$. Substituing, $f(\alpha^6) = 0$ and $f(\alpha^{10}) = 0$ are roots.

Then, we can write $f(X) = (X+\alpha^6)(X+\alpha^{10})$.

Vector Space

V is a set of elements on which $+$ is defined, F is a field. $\cdot$ is defined between elements of F and V.

V is a vector space over field F if

- V is a commutative group under $+$
- Closure: For any $a \in F$ and $v \in V$, $a \cdot v \in V$
- Distributive: $a \cdot (u + v) = a \cdot u + a \cdot v$ and $(a + b) \cdot v = a \cdot v + b \cdot v$
- Associative: $(a \cdot b) \cdot v = a \cdot (b \cdot v)$
- Identity element: $1 \cdot v = v$ and $v + 0 = v$

Elements of V are called vectors and elements of F are called scalars. The $+$ is vector addition and the $\cdot$ is scalar multiplication.

Properties of Additive inverse: $(-c) \cdot v = c \cdot (-v) = -(c \cdot v)$

Ex. Ordered sequence of n components

$(a_0, a_1, \ldots, a_{n-1})$ with $a_i = 0/1$

V_n denotes all 2^n distinct n-tuples.

Define $u + v = (< u_i + v_i >)$ This is an n-tuple over $GF(2)$; implies closure.

Then, $v + v = (0, 0, \ldots, 0) = 0$ gives the additive identity element.

Therefore, V_n is commutative group under $+$

Next, $a \cdot v_i$ with scalar gives closure. $a = 1$ gives identity element. Other laws are also satisfied.

Thus, V_n of all n-tuples form vector space over $GF(2)$.

When a subset S of V is vector space over F, S is called **subspace** of V.

For $u, v \in S$; $u + v \in S$ and for $a \in F$, $u \in S$; $a \cdot u \in S$ (closure under $\cdot$)

Let $v_1, v_2, \ldots, v_k$ be k vectors in V and $a_1, a_2, \ldots, a_k$ be k scalars from F.

Then $a_1 v_1 + a_2 v_2 + \ldots + a_k v_k$ is a linear combination of $v_1, v_2, \ldots, v_k$

Now, sum of two such linear combinations is also a linear combination. Product of a scalar

and a linear combination is again one of the linear combinations.

Hence, the set of all linear combinations of k such vectors would form a subspace of V.

A set of vectors **spans** Vif every vector in V is a linear combination of the vectors in that set.

At least one such set B exists and is called the **basis** of V.

Cardinality of B gives the **dimension** of the vector space V.

Ex. Consider n-tuple $< e_i >$ with one non-zero element in the i^{th} position. $< e_i >$ spans V_n since all its 2^n n-tuples can be generated as all possible linear combinations of $< e_i >$. These are linearly independent, forms the basis of V_n and its dimension is n.

Dual of subspace Let $u = c_1v_1 + \ldots + c_kv_k$ form a k-dimensional subspace S of V_n with 2^k vectors.

Define **inner product** as $u.v = u_0v_0 + u_1v_1 + \ldots + u_{n-1}v_{n-1}$ Now, $u.v = 0$ implies u and v are orthogonal.

For the inner product, $u.v = v.u$; $u.(v + w) = (u.v) + (u.w)$; $(au).v = a(u.v)$

S is subspace of V_n and S_d a subset of V_n such that for $u \in S$ and $v \in S_d$; $u.v = 0$

S_d is non-empty since $(0, 0, \ldots, 0) \in S_d$. For $v, w \in S_d$; $u.(v+w) = 0+0 = 0$ implies $v+w \in S_d$. Then $a.v = 0/v \in S_d$

These closure properties are enough to show that S_d is a subspace of V_n and S_d and S are called duals to each other.

Now $dim(S) = k$; $dim(S_d) = n - k$ so that $dim(S) + dim(S_d) = n$

Ex. $3 - d$ subspace of V_5:

$(00000), (11100), (01010), ((10001),$

$(10110), (01101), (11011), (00111)$

S_d has vectors $(00000), (101010),$

$(01110), (11011).$

Spanned by $(10101), (01110)$

so that $dim(S_d) = 2$

Matrices

The $k \times n$ matrix G over $GF(2)$ is rectangular array with k rows and n columns. g_{ij} is element from $GF(2)$ with $0 \leq i < k$ and $0 \leq j < n$.

If k rows of G are linearly independent, then 2^k linear combinations of the rows form a $k - dim$ subspace of V_n - called the row space of G.

Elementary row operations include interchange, addition and we get another matrix G' over $GF(2)$: both give same row space.

For any $k \times n$ matrix G with k linearly independent rows, there exists an $(n-k) \times n$ matrix H over $GF(2)$ with $n-k$ linearly independent rows such that for any row $g_i.h_j = 0$ Row space of G is null space of H.

Ex.

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

and $G' = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$

by adding third row to first and interchanging second and third.

Row space of both:

$(000000), (100101), (010011), (001110),$

$(110110), (101011), (011101), (111000)$

which is a 3-d subspace of V_6.

Row space of this G is Null space of

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Matrices can be added: $[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}]$

Multiplication requires $c_{ij} = a_i.b_j = \sum_{t=0}^{n-1} a_{it}.b_{tj}$

Dimensionwise: $(k \times n).(n \times l) = (k \times l)$

Transpose of $G = G^T$ is $n \times k$ matrix.

Identity matrix I_k is of dimension $k \times k$.

Submatrix can be a matrix where rows/columns of G is omitted.

Generalize to entries from GF(q) where q is some power of a prime.

Linear block code

Definition: An (n, k) code with length n and 2^k code words is linear iff its 2^k code words form a k-dimensional subspace of the vector space of all n-tuples over the field $GF(2)$.

This implies that a binary block code is linear iff modulo-2 sum of two code words is also a code word (closure property).

This linear block code $\mathcal{C}$ being k-d subspace of V_n, we can find k linearly independent code words $g_0, g_1, \ldots, g_{k-1}$ in $\mathcal{C}$ such that every code word $v \in \mathcal{C}$ is a linear combination of these k code words.

$v = u_0 g_0 + u_1 g_1 + \ldots + u_{k-1} g_{k-1}$ where $u_i = 0/1$ for $0 \leq i < k$.

These linearly independent code words can be the rows of a $k \times n$ matrix G so that $v = u.G$. Rows of G generate / span the linear code $\mathcal{C}$.

Systematic structure of code: $n-k$ redundant part followed by k bit message part.

Generator matrix: G then takes the form $[P(k \times n-k)I(k \times k)]$ with P the parity-checking part and I the identity matrix.

So, $v_{n-k+i} = u_i$ for $0 \leq i < k$ and $v_j = u_0 p_{0j} + \ldots + u_{k-1} p_{k-1,j}$ for $0 \leq j < n-k$.

$$G = \begin{bmatrix} p_{00} & p_{01} & \cdots & p_{0,n-k-1} & 1 & 0 & \ldots & 0 \\ p_{10} & p_{11} & \cdots & p_{1,n-k-1} & 0 & 1 & \ldots & 0 \\ \vdots & & & & & & & \\ p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} & 0 & 0 & \ldots & 1 \end{bmatrix}$$

Parity check matrix $H = [I_{n-k} P^T]$ its row space is orthogonal to G.

$$H = \begin{bmatrix} 1 & 0 & \dots & 0 & p_{00} & p_{10} & \cdots & p_{k-1,0} \\ 0 & 1 & \dots & 0 & p_{01} & p_{11} & \cdots & p_{k-1,1} \\ \vdots & & & & & & & \\ 0 & 0 & \dots & 1 & p_{0,n-k-1} & p_{1,n-k-1} & \cdots & p_{k-1,n-k-1} \end{bmatrix}$$

$(n-k) \times n$ matrix with $(n-k)$ linearly independent rows. $v.H^T = 0$ The 2^{n-k} linear combinations of H form $(n, n-k)$ linear code $\mathcal{C}_d$ which is the dual of $\mathcal{C}$.

$\mathcal{C}_d$ is the null space of $\mathcal{C}$ i.e. for any $v \in \mathcal{C}$, $w \in \mathcal{C}_d$, $v.w = 0$.

Parity check of $\mathcal{C}$ = Generator of $\mathcal{C}_d$. $g_i.h_j = p_{ij} + p_{ij} = 0$ for all i, j so that inner product $G.H^T = 0$.

$v.H^T = 0$ leads to same parity check equations $v_j + u_0 p_{0j} + \ldots + u_{k-1} p_{k-1,j} = 0$.

Ex: Consider (7,4) linear code.

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Then, we can write:

$v_6 = u_3$

$v_5 = u_2$

$v_4 = u_1$

$v_3 = u_0$

$v_2 = u_1 + u_2 + u_3$

$v_1 = u_0 + u_1 + u_2$

$v_0 = u_0 + u_2 + u_3$

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Syndrome and error detection

Received sequence $r = v + e$ where v is the transmitted sequence and e is the error vector.

or, $e = r + v$ with $e_i = 1$ for $r_i \neq v_i$ and $e_i = 0$ for $r_i = v_i$.

Now, $s = r \cdot H^T = (s_0, s_1, \ldots, s_{n-k-1}$ is the syndrome of r.

Then $s = 0$ iff r is codeword and else $s \neq 0$.

$s_{n-k-1} = r_{n-k-1} + r_{n-k} p_{0,n-k-1} + \ldots + r_{n-1} p_{k-1,n-k-1}$

For the $(7, 4)$ linear block code,

$s_0 = r_0 + r_3 + r_5 + r_6$

$s_1 = r_1 + r_3 + r_4 + r_5$

$s_2 = r_2 + r_4 + r_5 + r_6$

and now consider $s = e.H^T$

Find the error pattern from simultaneous equations involving e, not r.

Consider one with single error bit = 1, others zero. Then generate $v^* = r + e^*$ selected error pattern, and correct error. Else ask for retransmission.

We have $n - k$ linear equations involving e so that the n-tuple e has 2^k solutions i.e. 2^k error patterns are involved.

Ex. s = (111) 16 error patterns generate s. Choose e = (0000010) Let v = (1001011) and r = (1001001) so that s = (111) and $v^* = r + e^*$ = (1001011)

Minimum distance

Distance $d(v, w)$ is no of places where w and v differ. The triangle inequality is $d(v, w) + d(w, x) \geq d(v, x)$

Hamming weight $\mathcal{W}(v)$ of v is no of 1's so that $d(v, w) = \mathcal{W}(v + w)$

Minimum distance $d_{min} = min[d(v, w) : v, w \in \mathcal{C}, v \neq w]$

Since $v + w \in \mathcal{C}$ we write

$d_{min} = min[\mathcal{W}(x) : x = v + w \in \mathcal{C}, x \neq 0]$

This gives the concept of minimum weight

$\mathcal{W}_{min} \doteq d_{min}$

The $(7, 4)$ linear block code has minimum weight or minimum distance $= 3$. This relates to its parity check matrix.

For each codeword of Hamming weight l, $\exists l$ columns of H such that their vector sum is zero and converse.

$H = [h_0, h_1, \ldots, h_{n-1}]$ with i-th column being h_i. Let $v_{i_1}, v_{i_2}, \ldots, v_{i_l}$ be the non-zero columns of V.

Then, $V.H^T = 0$ implies $v_{i_1}h_{i_1} + v_{i_2}h_{i_2} + \ldots + v_{i_l}h_{i_l} = 0$ i.e. $h_{i_1} + h_{i_2} + \ldots + h_{i_l} = 0$

Conversely, suppose $h_{i_1} + h_{i_2} + \ldots + h_{i_l} = 0$. Then, $x.H^T = x_{i_1}h_{i_1} + x_{i_2}h_{i_2} + \ldots + x_{i_l}h_{i_l} = 0$

Then, $x.H^T = 0$ where x has l non-zero components. This implies $x \in \mathcal{C}$

In other words, For each code of Hamming weight l, there exist l columns of H such that, the vector sum of these columns is equal to the zero.

Conversely , if there exist l column of H whose vector sum is the zero vector, there exist a code vector of Hamming weight of l in $\mathcal{C}$.

The minimum distance of a linear block code is equal to the minimum weight of its nonzero code words.

Let $\mathcal{C}$ be an (n, k) linear code with parity check matrix H. If no $(d-1)$ or fewer columns add to zero, $\mathcal{W}_{min} = d$

and minimum weight or distance of $\mathcal{C}$ is equal to the smallest no of columns of H adding to zero.

In the $(7,4)$ linear block code, the $0,2,6$ -th columns add to zero. Hence, $d_{min} = 3$

Given d_{min}, no error pattern of $d_{min} - 1$ or fewer errors can change one code vector into another. The received vector is not a code-word, hence the error is detectable. So, error detecting capability is $d_{min} - 1$.

There are $2^n - 1$ error patterns, out of which $2^k - 1$ correspond to the valid code words. Hence, there are $2^n - 2^k$ detectable error patterns.

Let there be A_i codewords of weight i in $\mathcal{C}$, this is called weight distribution of the code. Then, probability of undetected error is

$P_{uE} = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}$ where p is the transition probability in a BSC.

$A_1 = A_2 = \ldots = A_{d_{min}-1} = 0$ For the $(7,4)$ code, $A_0 = A_7 = 1$ and $A_3 = A_4 = 7$ so that $P_{uE} = 7p^3(1-p)^4 + 7p^4(1-p)^3 + p^7$

When $p = 10^{-2}$, the error prob is about 7×10^{-6}.

Let t be a positive integer such that $2t+1 \leq d_{min} \leq 2t+2$ to cover both odd and even. Let v, r be the transmitted and received pair and w be another valid codeword. Then, $d(v,r) + d(w,r) \geq d(v,w)$ from triangle inequality over HD. Suppose t' errors occur in v, so that $d(v,r) = t'$

$d(v,w) \geq d_{min} \geq 2t+1$ being valid codewords. Hence, $d(w,r) \geq 2t+1-t'$.

When $t' \leq t$; $d(w,r) > t$. So, r is closer to v in HD than top any other code vector w in $\mathcal{C}$.

For BSC, $P(r|v) > P(r|w)$ for $w \neq v$. Based on maximum likelihood decoding, r decodes into v and therefore errors are corrected.

For $l > t$ errors, consider $d(v, w) = d_{min}$ and consider two error patterns e_1, e_2 such that $e_1 + e_2 = v + w$ and e_1, e_2 have no common 1's.

Now, suppose $r = v + e_1$. Then, $d(v, r) = \mathcal{W}(v + r) = \mathcal{W}(e_1)$. Now, v, w are codewords.

Then, $d(w, r) = \mathcal{W}(w + r) = \mathcal{W}(w + v + e_1) = \mathcal{W}(e_2)$.

Now, let $\mathcal{W}(e_1) > t$. Then, it follows that $\mathcal{W}(e_2) \leq t + 1$

Then, $d(v, r) \geq d(w, r)$ and incorrect decoding occurs using maximum likelihood.

Hence, $t = \frac{\lfloor (d_{min} - 1) \rfloor}{2}$ is the t-error correcting code. This is random error correcting capability.

Hamming codes

$n = 2^m - 1$; $k = 2^m - m - 1$; $n - k = m$; $t = 1$; $d_{min} = 3$

$H = [I_m|Q]$ i.e all non-zero m-tuples are taken as columns. Q has columns with HW $= 2$ or above.

Order of columns does not affect weight distribution or distance property.

$G = [Q^T|I_{2^m-m-1}]$

No two columns of H add to zero. Presence of all tuples ensure that $h_i + h_j = h_l$ are found as columns. Hence, $h_i + h_j + h_l = 0$ which implies $d_{min} = 3$.

These are single error correcting perfect codes.

Delete any l columns of H to get H' dimension $(m \times 2^m - m - l - 1)$

Deleting even weight columns gives $H' = [I_m|Q'$ which is $m \times 2^{m-1}$ matrix.

For odd weights, no 3 columns will add to zero. Hence, $d_{min} = 4$. From I_m 3 columns can be found such that $h_i + (h_j + h_l + h_s) = 0$. This is called the shortened Hamming code.