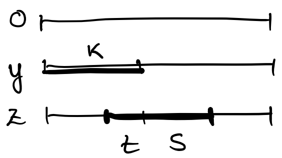
1. (a) $\binom{n}{w}$

(b)



$t+s = i \leftarrow d(z,x)$

$k-t+s = j \leftarrow d(z,y)$

$\therefore \quad s = \frac{i+j-k}{2} \;;\; t = i-s = \frac{i-j+k}{2}$

$p_{ij}^{k} = \binom{k}{t}\binom{n-k}{s}$ if s is integer and 0 o/w

If $k=0$, then $x=y$, and $p_{ii}^{0} = \binom{n}{i}$; $p_{ij}^{0} = 0$ if $i \neq j$

2. (a) $\binom{n}{w}2^w$

(b) $\sum_{\substack{i=0 \\ \text{even}}}^{n} \binom{n}{i}2^i$;

$-1 = (1-2)^n = \sum (-1)^i \binom{n}{i} 2^i = \underbrace{\sum_{i \text{ even}} \binom{n}{i}2^i}_{a} - \underbrace{\sum_{i \text{ odd}} \binom{n}{i}2^i}_{b}$

$\therefore \quad a = b-1$

Also $3^n = (1+2)^n = a+b = 2b-1$

$\therefore \quad b = \frac{3^n+1}{2}$ and $\boxed{a = \frac{3^n-1}{2}}$

3. $C_1\ [n, 0, ?]$ $\quad G = \text{empty}$; $H = I_n$

$C_2\ [n, n, 1]$ $\quad G = I_n$; $H = \text{empty}$

$C_3\ [n, 1, n]$ $\quad G_3 = [1\,1 \dots 1]$; $H_3 = \begin{array}{c} n \\ \begin{bmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & & & & & & \\ 1 & 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix} \end{array} n-1$.

$C_4\ [n, n-1, 2]$ $\quad G = H_3$; $H = G_3$

4. (a) If you know Lagrange's theorem, then that's it. If not, then note that the subset $C_0 = \{x \in C \mid x_i = 0\}$ is a linear subcode of C. Now take $y \in C$ s.t. $y_i = 1$ and consider the set $C_1 = \{x + y \mid x \in C_0\}$. You will quickly conclude that $|C_0| = |C_1|$, and since $|C_0| + |C_1| = |C|$, $|C_0| = \frac{|C|}{2}$

(b) Suppose that $[n, k, d]$ are the parameters of the code C. We note that upon shortening, the distance cannot decrease. The length of C_1 is $n-1$; $\dim C_1 = \dim C - 1 = k-1$, and the distance is $\geq d$

The parity-check matrix of C_1 is obtained by discarding from H the last column.

To obtain the generator matrix G_1, perform row operations in G to remove all but a single 1 in the last column. Then discard the row with this 1 and the last column.

5.
$$S(x) := \sum_{y \in C} (-1)^{x_1 y_1 + \dots + x_n y_n}$$

The vectors $y \in C$ s.t. $\sum_{i=1}^{n} x_i y_i = 0$ form an $\mathbb{F}_2$-linear space.

Since $x \notin C^\perp$, there is a vector $y \in C$ s.t. $\sum_{i=1}^{n} x_i y_i = 1$, so for every $y \in C$ with $\sum_{i=1}^{n} x_i y_i = 0$ there is a vector $\bar{y} \in C$ with $\sum_{i=1}^{n} x_i \bar{y}_i = 1$.

Thus the terms in the sum $S(x)$ split evenly between 0 and 1, and so $S(x) = 0$.

6 (a) Since $d(x,y) = d(0, y-x)$, we may argue in terms of the norm (Hamming weight), and must show that

$$|x+y| \leq |x| + |y|$$

which is straightforward.

10. Let $x_1 = (111000\ldots0)$; $x_2 = (001110\ldots0)$, then $x = x_1 - x_2$ is a codevector of Hamming weight 4; if $Hx_1^T = Hx_2^T$, then $Hx^T = 0$, contradicting the fact that the distance of the code is 5.

11. Let C be a linear code in $\mathcal{X}_n$ and $x \notin C$ be a vector. The set $x + C = \{x + y : y \in C\}$ is called a coset of C in $\mathcal{X}_n$. It is easily seen that for different x_1, x_2 the cosets $x_1 + C$ and $x_2 + C$ either coincide, or are disjoint. Thus if $\dim C = k$, there are 2^{n-k} cosets. In each coset we choose a vector of the smallest Hamming weight and call it the coset leader.

Since all the vectors of weight one are coset leaders, the matrix H does not contain identical columns.

For 000110 to be a coset leader we need that the sum of the columns $h_4 + h_5$ be different from any of the columns h_1, h_2, h_3, h_6 (o/w 000110 would be in a coset with leader of wt. 1).

The matrix

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

satisfies these conditions (there are other possibilities)

Problem 31. Let β be a root of f. We have $f(x)(x-1) = x^5 - 1$, so β is a primitive 5th degree root of unity. In other words, $\mathbf{ord}\,(\beta) = 5$.

[Alternatively, we have $\beta^5 = \beta^4.\beta = (\beta^3 + \beta^2 + \beta + 1)\beta = 1$.]

Therefore β is not primitive in $\mathbb{F}_{16}$, and so f is not a primitive polynomial. Now let α be a root of $x^4 + x + 1$, $\alpha \in \mathbb{F}_{16}$. We can take $\beta = \alpha^3$.

The elements $\beta^3, \beta^2, \beta, 1$ are linearly independent over $\mathbb{F}_2$ because f is irreducible. So let us construct $\mathbb{F}_{16}$ taking them as a basis.

We obtain

β^3	β^2	β	1		α^3	α^2	α	1	
0	0	0	0	0	0	0	0	0	0
0	0	0	1	1	0	0	0	1	1
0	0	1	0	β	1	0	0	0	α^3
0	1	0	0	β^2	1	1	0	0	α^6
1	0	0	0	β^3	1	0	1	0	α^9
0	0	1	1	$\beta+1$	1	0	0	1	α^{14}
0	1	0	1	β^2+1	1	1	0	1	α^{13}
0	1	1	0	$\beta^2+\beta$	0	1	0	0	α^2
1	0	0	1	β^3+1	1	0	1	1	α^7
1	0	1	0	$\beta^3+\beta$	0	0	1	0	α
1	1	0	0	$\beta^3+\beta^2$	0	1	1	0	α^5
0	1	1	1	$\beta^2+\beta+1$	0	1	0	1	α^8
1	0	1	1	$\beta^3+\beta+1$	0	0	1	1	α^4
1	1	0	1	$\beta^3+\beta^2+1$	0	1	1	1	α^{10}
1	1	1	0	$\beta^3+\beta^2+\beta$	1	1	1	0	α^{11}
1	1	1	1	$\beta^3+\beta^2+\beta+1$	1	1	1	1	α^{12}

For instance, to compute $\beta + 1$ as a power of α we write $\beta + 1 = \alpha^3 + 1 = \alpha^{14}$ etc.

(c) α^{14} is a primitive element in $\mathbb{F}_{16}$ since $(14, 15) = 1$. Its minimal polynomial is $m_7 = x^4 + x^3 + 1$ (verify directly that $m_7(\beta + 1) = 0$!)

(32) a). $F_4 = \{0, 1, w, \bar{w}\}$

$w = \alpha^i \in \mathbb{F}_4$

$ord(\alpha^i) = 3$ since $ord(\alpha^i) = \dfrac{ord(\alpha)}{gcd(ord(\alpha^i), i)}$

$gcd(15, i) = 5$

$i = 5, 10$.

Let $w = \alpha^5$, $\bar{w} = \alpha^{10}$. (or $w = \alpha^{10}$, $\bar{w} = \alpha^5$) $\alpha^4 = \alpha + 1$

$+$	0	1	w	$\bar{w}$
0	0	1	w	$\bar{w}$
1	1	0	$\bar{w}$	w
w	w	$\bar{w}$	0	1
$\bar{w}$	$\bar{w}$	w	1	0

$1 + w = 1 + \alpha^5 = \alpha^2 + \alpha + 1 = \bar{w}$

$1 + \bar{w} = 1 + \alpha^{10} = \alpha^2 + \alpha = w$

$w + \bar{w} = \alpha^5 + \alpha^{10} = 1$

$\cdot$	0	1	w	$\bar{w}$
0	0	0	0	0
1	0	1	w	$\bar{w}$
w	0	w	$\bar{w}$	1
$\bar{w}$	0	$\bar{w}$	1	w

$w \cdot w = \alpha^{10} = \bar{w}$

$\bar{w} \cdot \bar{w} = \alpha^{20} = \alpha^5 = w$

$w \cdot \bar{w} = \alpha^{15} = 1$

b). $f(x) = x^2 + wx + 1$ can not be divided by

x

$x + 1$

$x + w$

$x + \bar{w}$

hence $f(x)$ is irreducible.

c) $\beta^2+\omega\beta+1=0$

or $\beta^2=\omega\beta+1$

$\beta,\ \beta^2=\omega\beta+1,\ \beta^3=\omega\beta^2+\beta=\omega(\omega\beta+1)+\beta$

$=\bar{w}\beta+w+\beta=w\beta+w$

$\beta^4=w\beta^2+w\beta=w^2\beta+w+w\beta=\beta+w$

$\beta^5=\beta^2+\beta w=1$

$ord(\beta)=5$

β is not primitive in $\mathbb{F}_{16}$

d) Since $ord(\beta)=5$, $3|i$.

Since $\beta^2+w\beta+1=0$

if $\beta=\alpha^3$ $\beta^2+w\beta+1=\alpha^6+\alpha^8+1=\alpha^3\neq 0$

if $\beta=\alpha^6$ $\beta^2+w\beta+1=\alpha^{12}+\alpha^{11}+1=0 \Rightarrow i=6$

e). $\forall(\lambda,\mu)\in\mathbb{F}_4$

$\lambda\beta+\mu=0$ iff $\lambda=\mu=0$

Hence $\{\beta,1\}$ form a basis of $\mathbb{F}_{16}$ over $\mathbb{F}_4$.

Since $\beta=\alpha^6,\ \bar{W}=\alpha^{10},\ \beta^2=w\beta+1$	representation in the basis $(\beta,1)$
$\alpha=\beta\cdot\bar{w}$	$(\bar{w},0)$
$\alpha^2=\beta^2\cdot\bar{w}^2=(w\beta+1)\cdot w=w^2\beta+w=\bar{w}\beta+w$	$(\bar{w},w)$
$\alpha^3=\beta\bar{w}\cdot(\bar{w}\beta+w)=w(w\beta+1)+\beta=w\beta+w$	(w,w)
$\alpha^4=\beta\bar{w}(w\beta+w)=(w\beta+1)+\beta=\bar{w}\beta+1$	$(\bar{w},1)$
$\alpha^5=\beta\bar{w}(\bar{w}\beta+1)=w(w\beta+1)+\beta\bar{w}=w$	$(0,w)$
$\alpha^6=\beta\bar{w}\cdot w=\beta$	$(1,0)$
$\alpha^7=\beta\bar{w}\cdot\beta=\bar{w}(w\beta+1)=\beta+\bar{w}$	$(1,\bar{w})$
$\alpha^8=\beta\bar{w}(\beta+\bar{w})=\bar{w}(w\beta+1)+\beta w=\bar{w}\beta+\bar{w}$	$(\bar{w},\bar{w})$
$\alpha^9=\beta\bar{w}(\bar{w}\beta+\bar{w})=w(w\beta+1)+w\beta=\beta+w$	$(1,w)$
$\alpha^{10}=\beta\bar{w}(\beta+w)=\bar{w}(w\beta+1)+\beta=\bar{w}$	$(0,\bar{w})$

$\alpha^{11} = \beta\bar{w}\cdot\bar{w} = w\beta$ $(w, 0)$

$\alpha^{12} = \beta\bar{w}\cdot w\beta = w\beta+1$ $(w, 1)$

$\alpha^{13} = \beta\bar{w}\cdot(w\beta+1) = (w\beta+1)+\bar{w}\beta = \beta+1$ $(1,1)$

$\alpha^{14} = \beta\bar{w}\cdot(\beta+1) = \bar{w}(w\beta+1)+\beta\bar{w} = w\beta+\bar{w}$ $(w,\bar{w})$

1 $(0,1)$

0 $(0,0)$

f). Monic irreducible polynomial of degree ≤ 2 over $\mathbb{F}_4$:

$$\begin{cases} x \quad x+1 \quad x+w \quad x+\bar{w} \\ x^2+wx+1 \quad x^2+\bar{w}x+1, \quad x^2+x+w, \quad x^2+x+\bar{w}, \quad x^2+wx+w, \quad x^2+\bar{w}x+\bar{w} \end{cases}$$

element in $\mathbb{F}_{16}$	Minimal polynomial
0	x
1	$x+1$
α	x^2+x+w
α^2	$x^2+x+\bar{w}$
α^3	$x^2+\bar{w}x+1$
α^4	x^2+x+w
α^5	$x+w$
α^6	x^2+wx+1
α^7	x^2+wx+w
α^8	$x^2+x+\bar{w}$
α^9	x^2+wx+1
α^{10}	$x+\bar{w}$
α^{11}	$x^2+wx+\bar{w}$
α^{12}	$x^2+\bar{w}x+1$
α^{13}	x^2+wx+w
α^{14}	$x^2+wx+\bar{w}$

Problem 34. (a) The number of primitive elements in $\mathbb{F}_{32}$ equals the number of integers between 1 and 30 that are coprime with 31, i.e., 30.

(b) We need to show that none of the polynomials $x, x+1, x^2+1, x^2+x+1$ divide f. Since f has no roots in $\mathbb{F}_2$, only the last two polynomials remain. We can write

$$f = (x^2+x+1)(x^3+x^2)+1 = (x^2+1)(x^3+x+1)+1,$$

proving that f is irreducible.

(c) No, because $\mathbb{F}_{32}$ does not contain elements of order less than 31.

(d) No because 2^4-1 is not a divisor of 2^5-1 (or because of (c)).

(e) We have

$$\prod_{i=0}^{4}(x-\alpha^i) = x^5 + (1+\alpha+\alpha^2+\alpha^3+\alpha^4)x^4 + (\alpha+\alpha^2+\alpha^6+\alpha^7)x^3$$
$$+(\alpha^3+\alpha^4+\alpha^8+\alpha^9)x^2 + (\alpha^6+\alpha^7+\alpha^8+\alpha^9+\alpha^{10})x + \alpha^{10}$$
$$= x^5 + \alpha^{15}x^4 + \alpha^{21}x^3 + \alpha^{23}x^2 + \alpha^{21}x + \alpha^{10}.$$

(f) We have $\alpha^4+\alpha^3+\alpha = \alpha^9$, so the logarithm equals 9.

(g) By (a) γ is a primitive element, so its minimal polynomial is of degree 5.

(h) Since γ is not a root of a polynomial of degree 4 or less, the elements $1, \gamma, \gamma^2, \gamma^3, \gamma^4$ are linearly independent over $\mathbb{F}_2$.

(i) We compute $\alpha^8 = \alpha^3+\alpha^2+1$, getting (1,0,1,1,0) as the coordinates with respect to the basis $(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$.