佐野　海徳　20R13302 ICT.C209

K.1

(a) 符号長は 12、最小距離は 100001011001 と 001101010010 の組、あるいは 111010001100 と 110110110101 の組における 6 である。符号化率は $\frac{1}{12}\log_2|4| = \frac{1}{6}$ である。

(b) 受信語 $\vec{r}$ とのハミング距離が最小になる符号語 $\vec{c}$ を複合結果とする複合法である最小距離復号法における復号結果のこと。正確には $\vec{c}^{(MD)}\vec{r} = \arg\min_{\vec{c}\in C} d(\vec{c},\vec{r})$ で定義される。

(c)$\vec{c_t}^{(BD)}(\vec{r}) = \vec{c} \in C(d(\vec{c},\vec{r}) \leq t$ となる符号語が唯一存在する) $\vec{c_t}^{(BD)}(\vec{r})$ =error (そんな符号語は存在しないため復号失敗) が定義である。

佐野　海徳　20R13302 ICT.C209

K.2

(a) 講義資料の定理 3.9 より、ハミング限界は線形とは限らない (n,M,d) 符号が存在するための必要条件を与える。

(b)

佐野　海徳　20R13302 ICT.C209

K.3

(a) C_1 において (1,1) + (1,1) = (0,0) だが、(0,0) は C_1 に存在しないので二元線形符号とはならない。C_2 において、これは二元線形符号である。次元は

(b) 左辺を計算すると $\begin{pmatrix} x_1 \\ x_1+x_3+x_4 \\ x_1+x_2+x_3+x_4 \\ x_4 \end{pmatrix}$ である。右辺の値から、$x_1 = 1, x_4 = 0$ は自明。これを用いると $x_2 = 0, x_3 = 1$ も同様にしてわかる。

(c)C = {000,111} である。000 に何をかけても 0 であるから、111 と内積を取って 0 になるベクトルを考えると、長さ 3 で 1 を偶数個含むものが当てはまる。よって、$C^{\perp} = \{000, 011, 101, 110\}$ である。

(b) 佐野　海徳　20R13302 ICT.C209

K.4

(a)4 × 4 の対角行列の右に H の 1 4 行目を転置したものを書いたものが G であるから
$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$ である。

(b)uG を計算すると、求める符号語は (1010011) である。

(c)

(d) 受信語を r とする。Hr^t を計算すると、(010) である。これは H の第六列に等しい。よって、推定誤りベクトルを $\hat{e} = (0000010)$ として、推定送信語を求めると、$\hat{c} = r - \hat{e} = (1111111)$ である。よって求める推定符号語は (1111111)。

(e)H のどの二列を取り出して計算しても $(000)^t$ とは異なるため、最小距離は 3 以上である。

(f)1 列目、2 列目、3 列目を取り出して計算すると、$(000)^t$ となる。よって、これらは線形従属であり最小距離は 3 以下である。

(g)69p 最後

佐野海徳　20R13302 ICT.C209

K.5

(a)1 つめは加法単位元を 0 とし、逆元は任意の元 x に対して-x を取ることで x-x = 0 を満たすので,-x, 結合性については任意の元 a,b,c∈ $\mathbb{Q}$ に対し (a + b) + c = a + b + c = a + (b + c) が成り立つので成立。よって単位元 0 と逆元-x が存在して、結合性も満たすので群となる。2 つめに対して、結合則を考えると、任意の元 $a, b, c \in \mathbb{R}$ に対して $(a \times b) \times c = ab \times c = abc, a \times (b \times c) = a \times bc = abc$ が成立するので成立。よってこれは群であり、乗法単位元を 1, 乗法逆元を $\frac{1}{x}$ とする群である。3 つめに関しては、正則でない行列には逆行列が存在しないので逆元が存在しない。よって、これは群にならない。4 つめは後で考える。

e, e' を単位元とする。e, e' が単位元であることから $ee' = e', ee' = e$ となる。よって、$e' = e$ であり、単位元は一意に存在する。

(b.2)a', a'' を a の逆元とする。このとき、逆元の存在から、$a'a = e$ となる。両辺に右から a'' をかけると、(左辺)$a'' = (a'a)a'' = a'(aa'') = a'e = a'$、(右辺)$a'' = ea'' = a''$ となり、結局 $a' = a''$ だから、逆元は一意に存在する。

(c)$99221 = 97343 \times 1 + 1878, 97343 = 1878 \times 51 + 1565, 1878 = 1565 \times 1 + 313, 1565 = 313 \times 5 + 0$ だから、求める最大公約数は 313。

佐野海徳　20R13302 ICT.C209

K.6

(a) 1 つ目の式は $1+1=0$, 2 つ目の式は $(1+x^2+x^3)+(1+x+x^2)=x+x^3$,3 つめの式は $(1-x)(1+x)=1-x^2$,4 つめの式に対して $(1+x)(ax^5+bx^4+cx^3+dx^2+ex+f)+g=x^6+x^2+1$ という式を考える (a,b,c,d,e,f,g は 0 か 1 のどちらか)。(左辺) $=ax^6+(a+b)x^5+(b+c)x^4+(c+d)x^3+(d+e)x^2+(e+f)x+(f+g)$ であり、右辺と係数を比較すると、a $=1$,b $=1$,c $=1$,d $=1$,e $=0$,f $=0$,g $=1$ となる。よって、商は $x^5+x^4+x^3+x^2$, あまりは 1 である。

(b.1)

A. $[010]+[010]=(x^2\times x^2)modp(X)=x^3+x$。

B. $ax^3+bx^2+c(a,b,c\in\mathbb{F}_2)$ である式を $p(x)$ でわった余りを考えると、$(b-a)x^2-ax-c$ である。$b-a=1, a=0, c=0$ を満たすのは $a=0, b=1, c=0$ である。よって、[010] が求めるものである。

C.

(c)p は素数なので $gcd(a,p)=1$。よって、$y,z\in\mathbb{Z}$ が存在して $ay+pz=1$ となる。これより、[a][y] $=$ [1] となって、この $[y]\in\mathbb{Z}/<p>$ が [a] の逆元である。

佐野　海徳　20R13302 ICT.C209

K.7

(a).1 符号長は 5、次元は 3、$\mathbb{F}$ 上の線形符号では符号化率は $\frac{k}{n}$ が成り立つので $\frac{3}{5}$。最小距離は $n-k+1=5-3+1=3$。

(a).2 定義より各項を計算し、mod7 で剰余をとると、$\mathrm{G}=\begin{pmatrix}1&1&1&1&1\\0&1&2&3&4\\0&1&4&2&2\end{pmatrix}$

(a).3 (4,0,3)G $=(4.4+3,4+3\times4,4+3\times2,4+3\times2)=(4,0,2,3,3)$。