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号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。

(d)d を偶奇で場合分けすると、$2t < d$ は $\lfloor d_c \rfloor = \begin{cases} d_o(d = 2d_o + 1) \\ d_e(d = 2d_e + 2) \end{cases}, \frac{d}{2} = \begin{cases} d_o + \frac{1}{2} \\ d_e + 1(d = 2d_e + 2) \end{cases}$。

ここから $t < \frac{d}{2}$ は $\lfloor \frac{d-1}{2} \rfloor$ と同値。つまり、各符号語から $\frac{d}{2}$ より小さい半径にある受信語の集合に交わりがないので、$\frac{d}{2}$ より少ない数の誤りは訂正できると言える。ここで逆に異なる 2 つの符号語 $\vec{c_1}, \vec{c_2}$ の $\frac{d}{2}$ より小さい半径に共通して含まれる受信語 $\vec{r}$ が存在したと仮定すると d を符号 C の最小距離として $d \geq d(\vec{c_1}, \vec{c_2})$

$\geq d(\vec{c_1}, \vec{r}) + f(\vec{r}, \vec{c_2})$

$\geq \frac{d}{2} + \frac{d}{2} = d$ で d = d となり矛盾が起こる。

次に半径 t の限界距離符号は $t \leq \lfloor \frac{d-1}{2} \rfloor + 1$ に対して $\lfloor \frac{d-1}{2} \rfloor$ 個より多い誤りを訂正できないことがあると示す。最小距離を d を与える符号語のペアを $\vec{c_1}, vecc_2$ とする。符号語 $\vec{c_1}$ を送信し、$\vec{c_1}$ の中で $\vec{c_2}$ と異なる d 個の要素のうち t 個が $\vec{c_2}$ の要素に変わった受信語 $\vec{r}$ を受信したとする。このとき $d(\vec{r}, \vec{c_1}) = t, d(\vec{r}, \vec{c_2}) = d - t$ である。$\lfloor \frac{d-1}{2} \leq \frac{d-2}{2}$ だから $d(\vec{r}, \vec{c_1}) = t \leq \lfloor \frac{d-1}{2} \rfloor + 1 \leq \frac{d-2}{2} + 1 \leq \frac{d}{2}$ つまり $t \leq \frac{d}{2}$ となる。これより $t = d(\vec{r}, \vec{c_1}) \leq d - t = d(\vec{r}, \vec{c_2})$ をえる。これは $\vec{r}$から半径 t 以内に少なくとも 2 つの符号語$\vec{c_1}, \vec{c_2}$ が存在することを意味するので、復号エラーとなる。つまり、誤り訂正能力から $t \geq \lfloor \frac{d-1}{w} \rfloor$ ならば半径 t の限界距離復号は任意の符号語 $c \in C$ を送信した場合に t 個の任意の誤りを訂正できるから $2t < d$ となる t に対して $d(\vec{c}, \vec{r})$ となる符号語 $\vec{c}$ は存在するとしたら一意である。

佐野　海徳　20R13302 ICT.C209

K.2

(a)C の各符号語からハミング距離 t 以下のベクトル全体は互いに交わりがない。実際、交わりがあると仮定すると、最小距離が d であることに矛盾。したがってユニオン限界を投資機で満たし、$\#\cup\{\vec{c}\in C\}B(\vec{c},t)=\sigma_{\vec{c},C}\#B(\vec{c},t)=|C|V_2(n,t)$ が成り立つ。よって左辺の集合は $\mathbb{F}_2^n$ に含まれるまたは等しいので $2^n\leq|C|V_2(n,t)$ となる。ので $M\geq\frac{2^n}{V_2(n,t)}, t=\lfloor\frac{d-1}{2}\rfloor$ が成り立つ。よってこれは必要条件を与える。

(b)VG 限界を言い換えると、$M-1<\frac{2^n}{V_2(n,d-1)}$ が成り立つ (M - 1, n,d) 符号に対して、(M - 1,n,d) 符号 C は最大ではない。したがって、C に最小距離を d に保ったまま符号語を一つ増やせる、すなわち (n,M,d) 符号が存在する。よって、これは十分条件である。

(c.1)$B\leq A\frac{4}{3}\pi r^3$

(c.2) 容器に A 個の球雨が入っているとすると、このとき各球から距離 r 以下の空間には互いに交わりがないのでユニオン限界を等式で満たし、すべての球が占有する空間の体積は各球の体積の和に等しい。更にすべての球が専有する空間の体積は容器の体積を超えないので $B\leq A\frac{4}{3}\pi r^3$ となる。最大充填でも上の議論は成り立つので $B\leq A(B,r)\frac{4}{3}\pi r^3$ となる。

佐野　海徳　20R13302 ICT.C209

K.3

(a)C_1 は零ベクトルが含まれていないので線形符号でない。C_2 は二元線形符号であり、次元は3、生成行列は $\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$ である。最小距離は 1、符号化率は $\frac{3}{5}$ である。

(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。

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) 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)。

(d) 符号長は 7。次元は 4。符号化率は $\frac{k}{n} = \frac{4}{7}$。

(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) 問題のハミング符号 C は $(n - 2^3 - 1, M = 2^{2^m - 1 - m}, d = 3)$ 符号である。さらに d(C)= 3 より、t(C) = 1,$V_2(n, t) = n + 1$ となる。これらはハミング限界を投資機で満たし、C は完全である。よって題意は証明された。

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 つめは群となる。$f, g \in S(x)$ に対して X の異なる 2 元 x,y を取れば f は単射だから $f(x) \neq f(y)$、また g も単射だから $g(f(x)) \neq g(f(y))$、つまり $(g\dot{f})(x) \neq (f\dot{g})(y)$ となり合成写像 $g\dot{f}$ は単射。次に $z \in X$ をとると g は全射。よって g(y) = z を満たす $y \in X$ が存在する。更に f も全射であるから f(x) = y となる $x \in X$ が存在する。よって $z = g(y) = g(f(x)) = (g\dot{f})(x)$ が成り立ち合成写像 $g\dot{f}$ は全射である。したがって $g\dot{f} \in S(X)$。$f, g, h \in S(X)$ に対して $(h\dot{(}g \dots f))(x) = h((g \dots f)(x)) = h(g(f(x)))$、$((h\dot{g})\dot{f})(x) = (h\dot{g})(f(x)) = h(g(f(x)))(x \in X)$ よって結合法則が成立する。X 上の恒等写像 $1_X : x \mapsto x(x \in X)$ は S(X) の元であって $(1_X\dot{f})(x) = 1_X(f(x)) = f(x) = f(1_X(x)) = (f\dot{1}_X)(x)(x \in X)$ すなわち $1_X\dot{f} = f\dot{1}_X = f$ だから 1_X は S(X) は単位元。S(X) の元 f は全単射であるから、逆写像 f^{-1} が存在して f^{-1} が存在して、f^{-1} も全単射。よって $f^{-1} \in S(X)$。$(f^{-1}\dot{f})(x) = f^{-1}(f(x)) = x = f(f^{-1}(x)) = (f\dot{f^{-1}})(x)(x \in X)$。すなわち $f^{-1}\dot{f} = f\dot{f}^{-1} = 1_X$ だから f^{-1} は逆元である。

(b.1)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. $[010]\times[010]=(x^2\times x^2)modp(X)=x^3+x$。

B. [010] と乗算をして [100] となるものなので、計算すると、[011] が答えである。

C.$[011]\times[010]^{-1}=[011]\times[011]=[110]$ である。

(b.2) 計算すると、$[100]\alpha_1+[011]\alpha_2=[010], [100]\alpha_1+[101]\alpha_2=[101]$。これをもとに演算表から条件を満たすものを探すと、$\alpha_1=[100], \alpha_2=[011]$。

(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、G $=\begin{pmatrix} \text{ここ}1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 2 & 2 \end{pmatrix}$。

(a).3 (403)G = (40233)。

(b)$f(X)$ から $(f(\alpha_1),.....f(\alpha_n))$ に移す写像 ϕ は線形全単射であったから、C の非ゼロ符号語は $\vec{x}(f)=(f(\alpha_1),.....f(\alpha_n)))\neq(0,...,0)$ with $f(X)(\neq 0)\in\mathbb{F}_q[X;k]$ と書ける。この非ゼロ符号語の重み、言い換えると $f(\alpha_i)\neq 0$ となる $i(1\geq i\geq n)$ の個数を調べる。零多項式は零符号語となる。つまり、$\phi:\mathbb{F}_q[X;k]\in 0\mapsto(0,...0)\in[F]^n{}_q$ であるから対偶を考えると非零符号語は非零多項式から生成されることがわかる。また、次数 k 未満の非零多項式 $f(X)$ の根の個数は k 未満であることと、$\alpha_1,...,\alpha_n$ が全て異なることから、$f(\alpha_i)=0$ となる i の個数は k 未満であることがわかる。言い換えると $f(\alpha_i)$ の個数は k 未満であることが分かる。言い換えるとm $f(\alpha_i)\neq 0$ となる i の個数は n - k + 1 以上である。こうして $\omega(\vec{x})\leq n-k+1$ が示された。よってこのことから題意が証明された。

佐野　海徳　20R13302 ICT.C209

K.8

(a) 1つ目は巡回符号である。次元は 1, 符号長は 4。2つ目は巡回符号である。次元は 4, 符号長は 4。

(b)(1010) によって生成される巡回符号を列挙すると、(1010), (0101) の 2 つである。

(c)x^4-1 を素因数分解すると、$x^4-1=(x+1)(x-1)(x^2+1)=(x+1)(x+1)(x+1)^2=(x+1)^4$ である。ここで自明なものを除くと $g(X)=1+X,(1+x)^2,(1+x)^3$ の 3 つである。

(e) まず C が線形符号であること、つまり、$c(X),d(X)\in C$ に対して $u(X),v(X)\in\mathbb{F}[X;k]$ が存在して $c(X)=u(X)g(X),d(X)=v(X)g(X)$ と書ける。$a,b\in mathbbF$ に対して $ac(X)+bd(X)=au(X)g(X)+bv(X)g(X)=(au(X)+bv(X))g(X)=au(X)+bv(X)\in\mathbb{F}[X;k]$ となるので $ac(X)+bd(X)\in C$ となる。次に C が巡回性を満たすと示す。右巡回シフトで閉じていることを示せば左巡回シフトでも同じようにできるので右巡回シフトで閉じていることを示せば十分である。言い換えれば $c(X)\in C$ に対して $Xc(X)modX^n-1\in C$ である。modX^n-1 で $Xc(X)\equiv Xc(X)-c_{n-1}(X^n-1)\equiv Xu(X)g(X)-c_{n-1}h(X)g(X)\equiv(Xu(X)-c_{n-1}h(X))g(X)$ が成り立つ。ここで多項式 f(X) の k 次の係数を $coef(f(X);k)$ とかくと $coef(Xu(X);k)=coef(c_{n-1}h(X))=c_{n-1}$ だから、$coef(Xu(X);k)=coef(c_{n-1}h(X))=c_{n-1}$ なので $Xu(X)-c_{n-1}h(X)\in\mathbb{F}[X;k]$ となり、主張が導かれた。

佐野　海徳 20R13302 ICT.C209

K.9

(a)$\alpha^0 = (100), \alpha^1 = (010), \alpha^2 = (001), \alpha^3 = (110), \alpha^4 = (011), \alpha^5 = (111), \alpha^6 = (101)$ となる。ここで、演算表より、$\alpha^{50} = \alpha^{6\times8}\alpha^2 = \alpha^{5\ times4}\alpha^2 = \alpha^{3\times2}\alpha^2 = \alpha^1$、$\alpha^{100} = \alpha^{6\times16}\alpha^4 = \alpha 5 \times 8\alpha^4 = \alpha^{3\times4}\alpha^4 = \alpha^{6\times2}\alpha^4 = \alpha^5\alpha^4 = \alpha^2$ となり、べき表現は $\alpha^1 + \alpha^2$, ベクトル表現は $(010) + (001) = (011) = \alpha^4$。

佐野　海徳 20R13302 ICT.C209

K.10

(a) (1) は a^2,(2) は $a^{2\times2} = a^4$,(3) は $a^{4\times2} = a^8$,(4) は $a^{3\times2} = a^6$,(5) は $a^{6\times2} = a$(12),(6) は $a^{12\times2} = a^9$, (7) は $a^{5\times2} = a^1$0,(8) は $a^{7\times2} = 14$,(9) は $a^{14\times2} = a^1$3,(10) は $a^{13\times2} = a^1$1,(11) は $1 + X + X^4$,(12) は $1 + X + X^2$,(13) は $1 + X^3 + X^4$。

(b) 求める生成多項式は a, a^2, a^3, a^4 を根に含む次数最小のモニック多項式だから g(X) = $(1 + X^2 + X^4)(1 + X + X^2 + X^3 + X^4)$ となる。

(c) 求める生成多項式は $a, a^2, a^3...a^6$ を根に含む次数最小のモニック多項式であるから g(X) = $(1 + X + X^2 + X^3 + X^4)(1 + X + X^4)(1 + X + X^2)$。

佐野　海徳 20R13302 ICT.C209

K.11

あまりに大量のデータを送受信することになると、コンピュータやサーバのメモリリミットに引っかかることがあると思うのですが、メールなどで打てる語数が決まっているというのは頻繁に使用されるサービスであり、多くの人が使用するものであるから 1 つ 1 つのデータを安全にかつすばやく送るためのトレードオフとして仕方のないことなのでしょうか。mod で符号を管理するのはコンピュータ上で扱える数値の最大が決まっているからなのかと考えました。また、HashTable を使うことでも復号というものは実施できるのではないかと考えていますが、こうした理論が存在するということはなにかこちらの方法のほうが Hashtable が大きくなることによるメモリ使用量の増大など、利点があるからなのだろうかとも思っています。