20R13302 佐野　海徳

3.1

(a) 符号長は 2^4-1、情報量は 15 - 4 = 11 である。よって、この条件を満たすパリティ検査行列が求めるハミング符号である。$\begin{pmatrix} 1&1&0&1&0&1&0&1&0&1&1&1&0&0&0 \\ 0&1&0&1&1&0&1&0&1&0&1&0&1&0&0 \\ 0&0&1&0&1&0&1&1&0&1&1&0&0&1&0 \\ 0&0&1&1&0&1&1&0&1&0&1&0&0&0&1 \end{pmatrix}$ が求める行列である。

(b) 受信語を r とし、r から得られるシンドロームは $s=(1010)^t$ であり、これは上で求めたパリティ検査行列の第 8 列目に等しい。よって推定誤りベクトルを $\hat{e}=(000000010000000)$ とすると求める推定符合語は (000000010000010) である。

3.2

(a) ハミング重みの定義よりその符号語の非ゼロの成分の数がハミング重みに等しいから、$A_0=1, A_1=0, A_2=0, A_3=7, A_4=7, A_5=0, A_6=0, A_7=1$, だから、$A(X)=1+7X^3+7X^4+X^7$,$A(X,Y)=X^7+7X^4Y^3+7X^3Y^4+Y^7$ である。

(b)(a) と同様にして $B_0=1, B_2=0, B_3=0, B_4=7, B_5=0, B_6=0, B_7=0$ だから、$B(X)=1+7X^4$,$B(X,Y)=X^7+7X^3Y^4$ である。

(c)$\frac{1}{16}A(X+Y,X-Y)=\frac{1}{16}\{(X+Y)^7+7(X+Y)^4(X-Y)^3+7(X+Y)^3(X-Y)^4+(X-Y)^7\}$ である。ここで $(X+Y)^7=X^7+7X^6Y+21X^5Y^2+35X^4Y^3+35X^3Y^4+21X^2Y^5+7XY^6+Y^7$, $7(X+Y)^4(X-Y)^3=7X^7+7X^6Y-21X^5Y^2-21X^4Y^3+21X^3Y^4+3X^2Y^5-7XY^6-7Y^7$,$7(X+Y)^3(X-Y)^4=7X^7-7X^6Y-21X^5Y^2+21X^4Y^3+21X^3Y^4-3X^2Y^5-7XY^6+7Y^7$, $(X-Y)^7=X^7-7X^6Y+21X^5Y^2-35X^4Y^3+35X^3Y^4-21X^2Y^5+7XY^6-Y^7$ であり、これらを全部足しあげると $16X^7+112X^3Y^4$ だから、$\frac{1}{16}A(X+Y,X-Y)=X^7+7X^3Y^4=B(X,Y)$ が確かに成り立った。

3.3

(a)　$(1100)G=(1100101)$ である。

(b) 受信語を r とするとシンドローム s は Hr で求められる。こうして求めると $s=(011)^t$ である。s と H の 2 列目が一致しているので $\hat{e}=(0100000)$。よって求める符号語は $r-\hat{e}=(1010111)$。

3.9

(a)ba という操作は問題 pdf の一番右の状態になる操作である。また、a は 4 回、b は 2 回行うともとに戻す操作である。これを実現する最小の a^ib^j は a = 3,b = 1 である。

(b)ba に対して ab はどのような操作かというと、右から 3 番めの状態を作る操作である。よって $ab\neq ba$ であるから反例が存在し可換ではない。

(c)$G=e, a^1b^0, a^2b^0, a^3b^0, a^0b^1, a^1b^1, a^2b^1, a^3b^1$ である。

(d)

(e) 演算表より ab。

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	b	a^3b	a^2b	a^3b
a^2	a^2	a^3	e	a	a^3b	b	ab	a^2b
a^3	a^3	e	a	a^2	ab	a^2b	a^3b	b
b	b	ab	a^2b	a^3b	e	a	a^2	a^3
ab	ab	a^2b	a^3b	b	a^3	e	a	a^2
a^2b	a^2b	a^3b	b	a	a^2	a^3	e	ab
a^3b	a^3b	b	ab	a^2b	a	a^2	a^3	e

3.10

(a) が成り立つとき定義より $gN = Ng$ だから両辺に $g^(-1)$ をかけて、なおかつ結合則が成立することから $gNg^-1 = N$。また、(b) が成り立つということはすべての元 $n \in N$ に対して演算が N の中で閉じている、つまり $gng^-1 \in N$ が成り立つ。　また、(c) が成り立つとき定義より (a) であるから、$(a) \to (b) \to (c) \to (a)$ であり、証明された。