このノートは「符号理論　デジタルコミュニケーションにおける数学」（日本評論社）の訂正内容を記したものです．証明中の記号は，書籍を参照下さい．

(萩原学 Ver 0.15-0618-01)

1　第２章「符号理論とは」

◆７ページ，７つの項目、「・」の直後

誤：

「情報源」「符号化器」「記録媒体」「メディアの損傷と通信路」「読取機器」「復号器」「終点」

正：

「(情報源)」「(符号化器)」「(記録媒体)」「(メディアの損傷と通信路)」「(読取機器)」「(復号器)」「(終点)」

2　第３章「集合論」

◆１６ページ，例 3.9

誤：

ユークリッドの原理

正：

アルキメデスの原理

それに伴い，索引のア行に「アルキメデスの原理　16」を追加．ヤ行から「ユークリッドの原理　16」を削除．

◆２０ページ，定義３．１７

誤：

A, B, C を集合，$f : A \to B$ と $f' : B \to C$ を写像とする：集合 A から C への写像を以下で定義する：

$$a \to f'(f(a)).$$

正：

A, B, C を集合，$f : A \to B$ と $f' : B \to C$ を写像とする．集合 A から C への写像を以下で定義する：

$$a \mapsto f'(f(a)).$$

◆２２ページ，下から１行目

誤：

読者自信

正：
読者自身

◆２３ページ，上から１２行目
誤：
読者自信

正：
読者自身

◆２４ページ，補題 3.24
誤：
「B をその定義域」

正：
「B をその値域」

◆２７ページ，例 3.31，上から 1 行目，
誤：

- $m \leqq n$ のときには濃度に関して $\#[m,n]_{\mathbb{Z}} = n - m$ が従う．

正：

- $m \leqq n$ のときには濃度に関して $\#[m,n]_{\mathbb{Z}} = n - m + 1$ が従う．

3　第４章「確率と典型系列」

◆３２ページ，例 4.3（一様分布），下から２，３行目
誤：
なぜならもう 1 つの条件は，

正：
もう 1 つの条件は，

◆３４ページ，例 4.5，下から 2 行目
誤：

$$\Pr_{P'}[|X-4|>1] = \sum_{x\in\{0,1\}} P'(x) = 1+0 = 1.$$

正：

$$\Pr_{P'}[|X-4|>1] = \sum_{x\in\{0,1,3\}} P'(x) = 1+0+0 = 1.$$

◆3 6 ページ，一番最後の文
誤：
複数

正：
複数

◆3 7 ページ，定義　4.11
誤：
任意の部分集合 $A_1, A_2, \ldots, A_n \subset \mathcal{X}$ に対して

正：
任意の部分集合 $A_1, A_2, \ldots, A_n \subset \mathbb{R}$ に対して

◆3 9 ページ，例　4.13
誤：
実際に確かめよう．まず

$$\Pr_P[P_1 \in \{0\}, P_2 \in \{0\}] = P(0,0) = 0.1$$

である．他方

$$\Pr_{P_1}[P_1 \in \{0\}] = P_1(0) = 0.3, \qquad \Pr_{P_2}[P_2 \in \{0\}] = P_2(0) = 0.2$$

である．よって

$$\Pr_P[P_1 \in \{0\}, P_2 \in \{0\}] = 0.1,$$
$$\Pr_{P_1}[P_1 \in \{0\}] \times \Pr_{P_2}[P_2 \in \{0\}] = 0.06$$

が従う．特に，それらの生起確率は異なる．

正：
実際に確かめよう．まず

$$P(0,0) = 0.1$$

である．他方

$$P_1(0) = 0.3, \qquad P_2(0) = 0.2$$

である．よって

$$P(0,0) = 0.1, \qquad P_1 \times P_2(0,0) = 0.06$$

が従う．特に，それらの生起確率は異なる．

◆4 3 ページ，補題　4.21（チェビシェフの不等式）
誤：
確率変数 X，その分散 σ と

正：
確率変数 X，その分散 σ^2 と

◆５２ページ，補題 4.33

誤：

$$|B_P(n,\epsilon)| \leqq \exp[n(H(P)+\epsilon)]$$

正：

$$|B_P(n,\epsilon)| \leqq \exp_2[n(H(P)+\epsilon)]$$

◆５３ページ，補題 4.34

誤：

$$x \in B_P(n,\epsilon) \iff P^n(x) \neq 0 \quad \text{かつ} \quad \left|-\frac{1}{n}\log P^n(x) - H(P)\right| \leqq \epsilon.$$

正：

$$x \in B_P(n,\epsilon) \iff P^n(x) \neq 0 \quad \text{かつ} \quad \left|-\frac{1}{n}\log_2 P^n(x) - H(P)\right| \leqq \epsilon.$$

◆５５ページ，下から９、１０行目，補題　4.35 の証明

誤：

$$\mathrm{Pr}_{P'^n}\left[\left|-\frac{1}{n}\log P'^n - H(P)\right| \geqq \epsilon\right] \leqq \frac{\sigma^2}{\epsilon^2 n}$$

が従う．ただし，σ は確率変数 $-\log_2 P'$ の分散を表す．

正：

$$\mathrm{Pr}_{P'^n}\left[\left|-\frac{1}{n}\log_2 P'^n - H(P)\right| \geqq \epsilon\right] \leqq \frac{\sigma^2}{\epsilon^2 n}$$

が従う．ただし，σ^2 は確率変数 $-\log_2 P'$ の分散を表す．

4　第５章「通信路符号化定理」

◆５８ページ，下から５行目

誤：

二元対象通信路

正：

二元対称通信路

◆５９ページ，上から４行目の式
誤：

$$-\frac{1}{9}\log_2\frac{1}{9}-\frac{8}{9}\log_2\frac{8}{9}\fallingdotseq 0.5.$$

正：

$$1-\left(-\frac{1}{9}\log_2\frac{1}{9}-\frac{8}{9}\log_2\frac{8}{9}\right)\fallingdotseq 0.5.$$

◆５９ページ，下から４行目
誤：
本書では，信路を

正：
本書では，通信路を

◆６５ページ，下から６行目
誤：
ところで,「分布

正：
ところで，分布

◆６７ページ，定義５．１２（同時典型系列）
３行目
誤：同時分布に対する典型系列の集合 $B_{P,W}(n,\epsilon)$ を

正：誤：同時分布に対する典型系列の集合 $B_J(n,\epsilon)$ を

◆６７ページ，定義５．１２（同時典型系列）
誤：$B_{P,W}(n,\epsilon):=\{(x,y)\in B_J(n,\epsilon)\mid x\in B_P(n,\epsilon)$ かつ $y\in B_{PW}(n,\epsilon)\}$

正：$B_J(n,\epsilon):=\{(x,y)\in B_{P,W}(n,\epsilon)\mid x\in B_P(n,\epsilon)$ かつ $y\in B_{PW}(n,\epsilon)\}$

◆６８ページ，補題５．１４の証明、７行目
誤：もしくは $(x,y)\notin B_{P,PW}(n,\epsilon)$

正：もしくは $(x,y)\notin B_{P,W}(n,\epsilon)$

◆通信路の記号
通信路の入力の長さ n を意識した記述 W^n という記号が、本書中に何度か用いられています。これらは、W と記述するほうが正確です。あえて長さを意識したい時に W^n と書いていることを、ご注意頂ければと思います。
具体的には、５章中では 69, 75, 81, 82, 83, 84, 85, 86, 87, 89, 90 ページです。

◆７３ページ，一番最後の文
誤：第２章で述べた符号化率

正：本章第 1 節で述べた符号化率

◆７７ページ，定義５．２３（典型集合復号）
誤：$W(|) : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}$

正：$W(|) : \mathcal{Y} \times \mathcal{X} \to \mathbb{R}$

◆７９ページ，補題５．２４の証明
下から５、６行目
誤：
分布 P^n が P の直積分布であることに注意して，写像 f の像ごとに右辺を変形すれば

正：
写像 f の像ごとに右辺を変形すれば

◆７９ページ，補題５．２４の証明
誤：

$$\left(\sum_{f(1)\in\mathcal{X}^n} P(f(1))\right)\left(\sum_{f(2)\in\mathcal{X}^n} P(f(2))\right)\times\cdots\times\left(\sum_{f(|\mathcal{M}|)\in\mathcal{X}^n} P(f(|\mathcal{M}|))\right)$$

正：

$$\left(\sum_{f(1)\in\mathcal{X}^n} P^n(f(1))\right)\left(\sum_{f(2)\in\mathcal{X}^n} P^n(f(2))\right)\times\cdots\times\left(\sum_{f(|\mathcal{M}|)\in\mathcal{X}^n} P^n(f(|\mathcal{M}|))\right)$$

◆７９ページ，補題５．２４の証明
下から２行目
誤：P が分布であるから
正：P^n が分布であるから

5　第６章「通信路符号化逆定理」

◆通信路の記号
通信路の入力の長さ n を意識した記述 W^n という記号が、本書中に何度か用いられています。これらは、W と記述するほうが正確です。あえて長さを意識したい時に W^n と書いていることを、ご注意頂ければと思います。
具体的には、６章中では、95, 113, 117, 122, 123 ページです。
◆１０２ページ，例６．１３
$V(|)$ の値.

誤：

$$\begin{pmatrix} V(0|0) & V(1|0) \\ V(0|1) & V(1|1) \end{pmatrix} := \begin{pmatrix} \frac{1}{3} & \frac{2}{3} \\ \frac{2}{7} & \frac{5}{7} \end{pmatrix}$$

正：

$$\begin{pmatrix} V(0|0) & V(1|0) \\ V(0|1) & V(1|1) \end{pmatrix} := \begin{pmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{2}{7} & \frac{5}{7} \end{pmatrix}$$

書籍１２３ページ〜１２５ページに跨る「通信路符号化逆定理の証明」にはテクニカルな誤りがありました．以下，その証明の修正，および，関連する補題をまとめています．

証明中の記号は，書籍を参照下さい．

Proof. [通信路符号化逆定理の証明]　まずいくつか準備をする．

通信路容量 $\mathcal{C}_W$ に対し，$R > \mathcal{C}_W$ を満たし，符号化率として取りうる勝手な値 $R \in \mathcal{R}$ を選ぶ．その上で，

$$\delta := \min\{2g^{-1}(\gamma)^2, \frac{R - C_W}{2}\}$$

とおく．ただし，g^{-1} は写像 $g : [0, \frac{1}{2}] \to [0, \frac{1}{2}]$ であり $g(x) := -x\log_2 x$ の逆写像を，そして $\gamma := \min\{\frac{1}{8}, \frac{R-C_W}{2(|\mathcal{X}||\mathcal{Y}|+|\mathcal{Y}|)}\}$ を表す．このノートで後述する補題 5.9 により，δ は正の実数であることが示される．

符号長として用いる整数 n を次の条件を満たすように選ぶ：

$$\frac{(n+1)^{|\mathcal{X}|+|\mathcal{X}||\mathcal{Y}|}}{\exp_2[n\delta]} < \epsilon, . \tag{1}$$

かつ，$\exp_2[nR]$ が整数であるとする．これらの条件は δ が正であることから，n を十分に大きくすれば満足できる [1]．メッセージ集合を，濃度が $|\mathcal{M}| = \exp_2[nR]$ を満たす集合として定める．

さて，復号誤り率の上界をタイプ一定符号の議論へ帰着すれば (書籍：補題 6.29)，

$$\bar{s}(W, f, \phi) \leqq (n+1)^{|\mathcal{X}|} \max_{P \in \mathcal{P}_n} \bar{s}(W, f_P, \phi)$$

と表せる．タイプ一定符号の復号誤り率の上界 (書籍： 補題 6.28) を用いて，右辺を変形すれば，δ の選び方から

$$\begin{aligned}
&\bar{s}(W, f, \phi) \\
&\quad \leqq (n+1)^{|\mathcal{X}|} \\
&\qquad \times \max_{P \in \mathcal{P}_n} \frac{(n+1)^{|\mathcal{X}||\mathcal{Y}|}}{\exp_2\left[n \min_{V(\,|\,)} \left\{ D(V||W|P) + \left| \frac{\log_2 |\mathcal{M}|}{n} - I(P,V) \right|^+ \right\}\right]} \\
&\quad = \frac{(n+1)^{|\mathcal{X}|+|\mathcal{X}||\mathcal{Y}|}}{\exp_2[n \min_{P \in \mathcal{P}_n} \min_{V(\,|\,)} \{D(V||W|P) + |R - I(P,V)|^+\}]} \\
&\quad \leqq \frac{(n+1)^{|\mathcal{X}|+|\mathcal{X}||\mathcal{Y}|}}{\exp_2[n\delta]}
\end{aligned} \tag{2}$$

と表せる．符号長 n の選び方（(1) 式）から，

$$\bar{s}(W, f, \phi) < \epsilon$$

を得た． □

[1] $n > \frac{4\exp_2\left[\frac{|\mathcal{X}|+|\mathcal{X}||\mathcal{Y}|}{\delta}\right]}{\epsilon}$ とすればよい．

以下，先の証明に関連する補題を述べる．

Lemma 5.1. 関数 $g : [0, \frac{1}{2}] \to [0, \frac{1}{2}]$ を $g(x) := -x\log_2 x$ と定義する．

このとき，$g(x)$ は全単射写像．つまり，逆写像 $g^{-1} : [0, \frac{1}{2}] \to [0, \frac{1}{2}]$ が定義できる．

そして，$0 \leqq x_1, x_2 \leqq \dfrac{1}{2}$ に対して，次が従う．

$$x_1 < x_2 \iff g(x_1) < g(x_2)$$

Proof. 高校生程度の微分の知識で確認できる．演習問題とする． □

次に挙げる補題に対し，$P = Q$ の場合を考えると，書籍中の補題 6.22 でのべた最初の主張となっている．

Lemma 5.2 (ダイバージェンスのチェイン則)**.** $\mathcal{X}_1, \mathcal{X}_2$ を有限集合，P と Q を $\mathcal{X}_1$ 上の分布，$V(\ |\ ), W(\ |\ )$ を $\mathcal{X}_1$ から $\mathcal{X}_2$ への通信路，$P_{P,V}, P_{Q,W}$ を $\mathcal{X}_1 \times \mathcal{X}_2$ 上の分布とする．ただし，任意の $x_1 \in \mathcal{X}_1, x_2 \in \mathcal{X}_2$ に対して，

$$P_{P,V}(x_1, x_2) = P(x_1)V(x_2|x_1), P_{Q,W}(x_1, x_2) = Q(x_1)W(x_2|x_1)$$

を満たすとする．

このとき，以下が従う．

$$D(P_{P,V}||P_{Q,W}) = D(P||Q) + D(V||W|P).$$

Proof. ざっくりと計算方法を述べる．

まずダイバージェンスと同時分布の定義から，

$$\begin{aligned} D(P_{P,V}||P_{Q,W}) &= \sum_{x_1 \in \mathcal{X}_1, x_2 \in \mathcal{X}_2} (P_{P,V}(x_1, x_2)\log_2 P_{P,V}(x_1, x_2) - P_{P,V}(x_1, x_2)\log_2 P_{Q,W}(x_1, x_2)) \\ &= \sum_{x_1 \in \mathcal{X}_1, x_2 \in \mathcal{X}_2} (P(x_1)V(x_2|x_1)\log_2 P(x_1)V(x_2|x_1) \\ &\qquad -P(x_1)V(x_2|x_1)\log_2 Q(x_1)W(x_2|x_1)) \end{aligned}$$

対数関数の性質などを使い，整理すると，

$$\begin{aligned} D(P_{P,V}||P_{Q,W}) &= \sum_{x_1 \in \mathcal{X}_1, x_2 \in \mathcal{X}_2} (P(x_1)V(x_2|x_1)\log_2 P(x_1) - P(x_1)V(x_2|x_1)\log_2 Q(x_1)) \\ &\qquad + \sum_{x_1 \in \mathcal{X}_1, x_2 \in \mathcal{X}_2} (P(x_1)V(x_2|x_1)\log_2 V(x_2|x_1) - P(x_1)V(x_2|x_1)\log_2 W(x_2|x_1)) \\ &= \sum_{x_1 \in \mathcal{X}_1} (\{P(x_1)V(x_2|x_1)\log_2 P(x_1) - P(x_1)\log_2 Q(x_1)\} \sum_{x_2 \in \mathcal{X}_2} V(x_2|x_1)) \\ &\qquad + \sum_{x_1 \in \mathcal{X}_1} P(x_1)(\sum_{x_2 \in \mathcal{X}_2} V(x_2|x_1)\log_2 V(x_2|x_1) - V(x_2|x_1)\log_2 W(x_2|x_1)) \end{aligned}$$

条件付きダイバージェンス，ダイバージェンスの定義を用いて，

$$\begin{aligned} D(P_{P,V}||P_{Q,W}) &= \sum_{x_1\in\mathcal{X}_1}\{P(x_1)V(x_2|x_1)\log_2 P(x_1) - P(x_1)\log_2 Q(x_1)\} \\ &\quad + D(V||W|P) \\ &= D(P||Q) + D(V||W|P) \end{aligned}$$

を得た．□

ダイバージェンスのチェイン則の応用を述べる．

Lemma 5.3. $\mathcal{X},\mathcal{Y}$ を有限集合，P を $\mathcal{X}$ 上の分布，$V(\,|\,),W(\,|\,)$ を $\mathcal{X}$ から $\mathcal{Y}$ への通信路とする．

このとき，以下が従う．

$$D(P_{PV}||P_{PW}) \leqq D(V||W|P)$$

Proof. ここの証明では，補題5.2を用いる．まず，その為の準備を述べる．$P_{P,V}, P_{PV}$ に対して，関数 $\bar{V}:\mathcal{X}\times\mathcal{Y}\to\mathbb{R}$ を以下で定義する．任意の $x\in\mathcal{X}, y\in\mathcal{Y}$ に対して，

$$\bar{V}(x|y) := \begin{cases} \dfrac{P_{P,V}(x,y)}{P_{PV}(y)} & (P_{PV}(y)\neq 0) \\ \dfrac{1}{|\mathcal{X}|} & (P_{PV}(y)=0) \end{cases}$$

このとき，$\bar{V}(\,|\,)$ は $\mathcal{Y}$ から $\mathcal{X}$ への通信路となる．さらに，関数 $\bar{P}_{P,V}:\mathcal{Y}\times\mathcal{X}\to\mathbb{R}$ を

$$\bar{P}_{P,V}(y,x) := P_{P,V}(x,y)$$

と定義する．同様に，$\bar{P}_{P,W}, \bar{W}(\,|\,)$ を定義する．このとき，

$$\bar{P}_{P,V}(y,x) = P_{PV}(y)\bar{V}(x|y), \bar{P}_{P,W}(y,x) = P_{PW}(y)\bar{W}(x|y)$$

が従う．これで補題5.2を適用する準備ができた．補題中の記号 $\mathcal{X}_1,\mathcal{X}_2,P,V(\,|\,),P_{P,V},Q,W(\,|\,),P_{Q,W}$ を，それぞれ，$\mathcal{Y},\mathcal{X},P_{PV},\bar{V}(\,|\,),\bar{P}_{P,V},P_{PW},\bar{W}(\,|\,),\bar{P}_{P,W}$ とすれば，

$$D(\bar{P}_{P,V}||\bar{P}_{P,W}) = D(P_{PV}||P_{PW}) + D(\bar{V}||\bar{W}|P_{PV})$$

が従う．とくにダイバージェンスの非負性から

$$D(\bar{P}_{P,V}||\bar{P}_{P,W}) \geqq D(P_{PV},P_{PW})$$

が成り立つ．

他方，$\bar{P}_{P,V},\bar{P}_{P,W}$ の定義から，$D(\bar{P}_{P,V}||\bar{P}_{P,W}) = D(P_{P,V}||P_{P,W})$ が従う．条件付きダイバージェンスの性質より $D(P_{P,V}||P_{P,W}) = D(V||W|P)$ と表せる．

以上を組み合せて，

$$D(V||W|P) = D(P_{P,V}||P_{P,W}) = D(\bar{P}_{P,V}||\bar{P}_{P,W}) \geqq D(P_{PV}||P_{PW})$$

を得た．□

一度，話がそれて，条件付きダイバージェンスと関連を持つ補題を述べる．

Lemma 5.4. a を実数であり，$0 \leqq a \leqq 1$ を満たすとする．関数 $F_a : (0,1) \to \mathbb{R}$ を $F_a(x) := a\log_2 \frac{a}{x} + (1-a)\log_2 \frac{1-a}{1-x} - 2(a-x)^2$ と定義する．
このとき，任意の $0 < x_0 < 1$ に対して，次が従う．

$$F_a(x_0) \geqq 0.$$

Proof. 演習問題とする．高校程度の微分の知識で示せる． □

Pinsker の不等式と呼ばれるものは幾つか異なるものが知られる．ここでは，代表的なものの一つを述べる．

Lemma 5.5 (Pinsker の不等式)**.** $\mathcal{X}$ を有限集合，P, Q を $\mathcal{X}$ 上の分布とする．
このとき，次が従う．

$$\sqrt{\frac{D(P||Q)}{2}} \geqq \max_{x\in\mathcal{X}}|P(x) - Q(x)|.$$

Proof. $x_0 \in \mathcal{X}$ として，

$$|P(x_0) - Q(x_0)| = \max_{x\in\mathcal{X}}|P(x) - Q(x)|$$

をみたすものを選ぶ．これは，$\mathcal{X}$ が有限集合であるから可能である．
続いて，集合 $\{1,2\}$ 上の分布 $\bar{P}$ を，$\bar{P}(1) := P(x_0), \bar{P}(2) := 1 - P(x_0)$ と定義する．次に，$\{1,2\}$ から $\mathcal{X}$ への通信路 $\bar{V}(\,|\,)$ を

$$\bar{V}(x|a) := \begin{cases} 1 & (a = 1, x = x_0) \\ \dfrac{P(x)}{1 - P(x_0)} & (a = 2, x \neq x_0) \\ 0 & (\text{それ以外}) \end{cases}$$

と定義する．最後に，$\{1,2\} \times \mathcal{X}$ 上の分布 $\bar{P}_{P,V}$ を

$$\bar{P}_{P,V}(a,x) := \begin{cases} P(x_0) & (a = 1, x = x_0) \\ P(x) & (a = 2, x \neq x_0) \\ 0 & (\text{それ以外}) \end{cases}$$

と定義する．
以上の準備のもと，ダイバージェンスのチェイン則（補題 5.2）が適用できることに注意しよう．さらに，ダイバージェンスの非負性から

$$D(\bar{P}_{P,V}||\bar{P}_{Q,W}) = D(\bar{P}||\bar{Q}) + D(\bar{V}||\bar{W}|P) \geqq D(\bar{P}||\bar{Q})$$

が従う．
ダイバージェンスと $\bar{P}, \bar{Q}$ の定義により，

$$\begin{aligned} D(\bar{P}||\bar{Q}) \quad = \quad & P(x_0)\log_2 P(x_0) + (1 - P(x_0))\log_2(1 - P(x_0)) \\ & -P(x_0)\log_2 Q(x_0) - (1 - P(x_0))\log_2(1 - Q(x_0)) \end{aligned}$$

と表せる．$Q(x_0)$ は $0 < Q(x_0) \leqq 1$ を満たすことに注意しよう．

ここで，$Q(x_0) = 1$ か否かで場合分けする．$Q(x_0) = 1$ であれば，$D(\bar{P}||\bar{Q}) = \infty$ であることに注意すれば，

$$D(P||Q) \geqq D(\bar{P}||\bar{Q}) = \infty > 2(\max_{x\in\mathcal{X}}|P(x) - Q(x)|)^2$$

が成り立つのは，最右の項が有限の値であることからわかる．また，$Q(x_0) \neq 1$ であれば，$0 < Q(x_0), 1 - Q(x_0) < 1$ である．他方，

$$D(\bar{P}||\bar{Q}) = P(x_0)\log_2\frac{P(x_0)}{Q(x_0)} + (1 - P(x_0))\log_2\frac{1 - P(x_0)}{1 - Q(x_0)}$$

と表せる．そこで，右辺に補題 5.4 を適用すれば，

$$\begin{aligned} D(\bar{P}||\bar{Q}) &\geqq 2(P(x_0) - Q(x_0))^2 \\ &= 2(\max_{x\in\mathcal{X}}|P(x) - Q(x)|)^2. \end{aligned}$$

よって，主張を得た． □

以下は，解析学でいう，一様連続性の議論である．

Lemma 5.6. α を $0 \leqq \alpha \leqq \dfrac{1}{4}$ を満たす実数，x_1, x_2 を $0 \leqq x_1, x_2 \leqq 1$ を満たす実数とする．

このとき，$|x_1 - x_2| \leqq \alpha$ であれば，$|g(x_1) - g(x_2)| \leqq g(\alpha)$ が従う．

Proof. 関数 $g'(x) : \mathbb{R}_{\geqq 0}$ を

$$g'(x) := g(x + \alpha) - g(x)$$

と定義する．このとき，$g'(x)$ は単調減少関数である．

よって，$0 \leqq x \leqq 1 - \alpha$ において，$|g'(x)|$ の最大値は $\max\{|g'(0)|, |g'(1 - \alpha)|\}$ と表せる．特に，$|g'(0)| = g(\alpha), |g'(1 - \alpha)| = g(1 - \alpha)$ であることに注意．

また，$0 \leqq \alpha \leqq \dfrac{1}{4}$ であれば，簡単な計算で $g(\alpha) \geqq g(1 - \alpha)$ が確かめられる．

以上から，

$$|g(x_1) - g(x_2)| \leqq g(\alpha)$$

を得た． □

これまでの議論をもちいて，エントロピーや相互情報量に関する評価を与える．

Lemma 5.7. $\mathcal{X}, \mathcal{Y}$ を有限集合，P を $\mathcal{X}$ 上の分布，$V(\ |\ ), W(\ |\ )$ を $\mathcal{X}$ から $\mathcal{Y}$ への通信路とする．

$D(V||W|P) \leqq 1/8$ であれば，次が従う．

1. $|H(P,V) - H(P,W)| \leqq |\mathcal{X}||\mathcal{Y}|g(\sqrt{\dfrac{D(V||W|P)}{2}})$
2. $|H(PV) - H(PW)| \leqq |\mathcal{Y}|g(\sqrt{\dfrac{D(V||W|P)}{2}})$

3. $|I(P,V) - I(P,W)| \leqq (|\mathcal{X}||\mathcal{Y}| + |\mathcal{Y}|)g(\sqrt{\frac{D(V||W|P)}{2}})$

Proof. 1．に関して：Pinsker の定理 5.5 より，$D(V||W|P) \leqq \frac{1}{8}$ であれば

$$|P_{P,V}(x,y) - P_{P,W}(x,y)| \leqq \sqrt{\frac{D(V||W|P)}{2}} \leqq \frac{1}{4}$$

が従うことに注意しよう．ただし，$x \in \mathcal{X}, y \in \mathcal{Y}$ を表す．

エントロピーの定義と絶対値の性質から，

$$\begin{aligned} |H(P,V) - H(P,W)| &= |\sum_{x\in\mathcal{X},y\in\mathcal{Y}} g(P_{P,V}(x,y)) - \sum_{x\in\mathcal{X},y\in\mathcal{Y}} g(P_{P,W}(x,y))| \\ &\leqq \sum_{x\in\mathcal{X},y\in\mathcal{Y}} |g(P_{P,V}(x,y)) - g(P_{P,W}(x,y))| \end{aligned}$$

が従う．

上で注意した通り，$|P_{P,V}(x,y) - P_{P,W}(x,y)| \leqq \sqrt{\frac{D(V||W|P)}{2}}$ かつ $|P_{P,V}(x,y) - P_{P,W}(x,y)| \leqq \frac{1}{8}$ が従う．そこで補題 5.6 を用いて整理すれば，

$$|H(P,V) - H(P,W)| \leqq \sum_{x\in\mathcal{X},y\in\mathcal{Y}} g(\sqrt{\frac{D(V||W|P)}{2}}) = |\mathcal{X}||\mathcal{Y}|g(\sqrt{\frac{D(V||W|P)}{2}})$$

を得た．

2．に関して:受信アルファベット上の分布に対するダイバージェンスの上限（補題5.3）より，$D(P_{PV}||P_{PW}) \leqq D(V||W|P)$ が従う．先と同様に $D(V||W|P) \leqq \frac{1}{8}$ であれば

$$|P_{PV}(y) - P_{PW}(y)| \leqq \sqrt{\frac{D(V||W|P)}{2}} \leqq \frac{1}{4}$$

が従う．ただし，$y \in \mathcal{Y}$ を表す．

エントロピーの定義と絶対値の性質から，

$$\begin{aligned} |H(PV) - H(PW)| &= |\sum_{y\in\mathcal{Y}} g(P_{PV}(y)) - \sum_{y\in\mathcal{Y}} g(P_{PW}(y))| \\ &\leqq \sum_{y\in\mathcal{Y}} |g(P_{PV}(y)) - g(P_{PW}(y))| \end{aligned}$$

が従う．

上で注意した通り，$|P_{PV}(y) - P_{PW}(y)| \leqq \sqrt{\frac{D(V||W|P)}{2}}$ かつ $|P_{PV}(y) - P_{PW}(y)| \leqq \frac{1}{8}$ が従う．そこで補題 5.6 を用いて整理すれば，

$$|H(PV) - H(PW)| \leqq \sum_{y\in\mathcal{Y}} g(\sqrt{\frac{D(V||W|P)}{2}}) = |\mathcal{Y}|g(\sqrt{\frac{D(V||W|P)}{2}})$$

を得た．

３．に関して：相互情報量の定義より，

$$\begin{aligned}|I(P,V)-I(P,W)| &= |H(P)+H(PV)-H(P,V)-H(P)-H(PW)+H(P,W)| \\ &= |H(PV)-H(PW)-H(P,V)+H(P,W)|\end{aligned}$$

が従う．絶対値の性質と１．２．を用いて，

$$\begin{aligned}|I(P,V)-I(P,W)| &\leqq |H(PV)-H(PW)|+|H(P,V)-H(P,W)| \\ &\leqq |\mathcal{X}||\mathcal{Y}|g(\sqrt{\frac{D(V||W|P)}{2}})+|\mathcal{Y}|g(\sqrt{\frac{D(V||W|P)}{2}}) \\ &= (|\mathcal{X}||\mathcal{Y}|+|\mathcal{Y}|)g(\sqrt{\frac{D(V||W|P)}{2}})\end{aligned}$$

を得た． □

Lemma 5.8. $\mathcal{X},\mathcal{Y}$ を有限集合，P を $\mathcal{X}$ 上の分布，$V(\ |\ ),W(\ |\ )$ を $\mathcal{X}$ から $\mathcal{Y}$ への通信路とする．C_W を通信路 $W(\ |\ )$ の通信路容量，R を実数であり $R > C_W$ であるとする．

$$D(V||W|P) \leqq \frac{1}{8}$$

かつ

$$D(V||W|P) \leqq 2\{g^{-1}(\frac{R-C_W}{2(|\mathcal{X}||\mathcal{Y}|+|\mathcal{Y}|)})\}^2$$

であれば，次が従う．

$$|R-I(P,V)|^+ \geqq \frac{R-C_W}{2}$$

Proof. 仮定 $D(V||W|P) \leqq \frac{1}{8}$ から，補題 5.7 を用いて，

$$I(P,V) \leqq I(P,W)+(|\mathcal{X}||\mathcal{Y}|+|\mathcal{Y}|)g(\sqrt{\frac{D(V||W|P)}{2}})$$

が従う．通信路容量 C_W の定義にもとづき右辺を変形すれば，

$$I(P,V) \leqq C_W+(|\mathcal{X}||\mathcal{Y}|+|\mathcal{Y}|)g(\sqrt{\frac{D(V||W|P)}{2}})$$

と表せる．これらの議論と $|\ |^+$ の定義から，

$$|R-I(P,V)|^+ \geqq |R-C_W-(|\mathcal{X}||\mathcal{Y}|+|\mathcal{Y}|)g(\sqrt{\frac{D(V||W|P)}{2}})|^+ \qquad (3)$$

が従う．

以下，もう一つの仮定，$D(V||W|P) \leqq 2\{g^{-1}(\frac{R-C_W}{2(|\mathcal{X}||\mathcal{Y}|+|\mathcal{Y}|)})\}^2$ に注目する．
両辺を 2 で割ってから，の平方をとれば，

$$\sqrt{\frac{D(V||W|P)}{2}} \leqq g^{-1}(\frac{R-C_W}{2(|\mathcal{X}||\mathcal{Y}|+|\mathcal{Y}|)})$$

と表せる．補題 5.1 により，

$$g(\sqrt{\frac{D(V||W|P)}{2}}) \leqq \frac{R-C_W}{2(|\mathcal{X}||\mathcal{Y}|+|\mathcal{Y}|)}$$

が従う．そこで，式 (3) に適用すれば，

$$|R-I(P,V)|^+ \geqq |R-C_W-\frac{R-C_W}{2}|^+ = \frac{R-C_W}{2}$$

を得た． □

Lemma 5.9. $\mathcal{X},\mathcal{Y}$ を有限集合，P を $\mathcal{X}$ 上の分布，$V(\ |\ ),W(\ |\ )$ を $\mathcal{X}$ から $\mathcal{Y}$ への通信路とする．C_W を通信路 $W(\ |\ )$ の通信路容量，R を実数であり $R > C_W$ であるとする．
$\gamma := \min\{\frac{1}{8}, \frac{R-C_W}{2(|\mathcal{X}||\mathcal{Y}|+|\mathcal{Y}|)}\}$ とおく．
このとき

$$D(V||W|P) + |R-I(P,V)|^+ \geqq \min\{2g^{-1}(\gamma)^2, \frac{R-C_W}{2}\}$$

が従う．

$$\min\{2g^{-1}(\gamma)^2, \frac{R-C_W}{2}\} > 0$$

に注意せよ．

Proof. $D(V||W|P)$ の大きさに注目し，二つの場合にわけて考察する．
$D(V||W|P) \geqq 2g^{-1}(\gamma)^2$ のとき：

$$\begin{aligned} D(V||W|P) + |R-I(P,V)|^+ &\geqq D(V||W|P) \\ &\geqq 2g^{-1}(\gamma)^2 \\ &\geqq \min\{2g^{-1}(\gamma)^2, \frac{R-C_W}{2}\} \end{aligned}$$

が成立する．
$0 \leqq D(V||W|P) \leqq 2g^{-1}(\gamma)^2$ のとき：補題 5.8 を用いて，

$$\begin{aligned} D(V||W|P) + |R-I(P,V)|^+ &\geqq |R-I(P,V)|^+ \\ &\geqq \frac{R-C_W}{2} \\ &\geqq \min\{2g^{-1}(\gamma)^2, \frac{R-C_W}{2}\} \end{aligned}$$

を得た． □

6　第７章「ハミング符号」

◆１２９ページ，上から１３行目
誤：例をに当てはめよう．

正：例に当てはめよう．

◆１４５ページ、定理７．２７（シンドロームの相違性）の証明
下から２行目、
誤：
ところで，ベクトル e_{n_0} の要素は第 n_0 成分のみが 1 であり，ほかは 0 である．右辺を変形すれば

正：
ところで，ベクトル e_{n_1} の要素は第 n_1 成分のみが 1 であり，ほかは 0 である．右辺を変形すれば

◆１４６ページ、定理７．２７（シンドロームの相違性）の証明
誤：

$$He_{n_1}^T = \begin{pmatrix} h_{1,n_0} \\ h_{2,n_0} \\ \vdots \\ h_{m,n_0} \end{pmatrix} = h_{*,n_0}$$

となり H の第 n_0 列と一致する．「行列 H のどの列もベクトルとしてすべて異なる」と仮定しているから，どの $1 \leqq n_0 \leqq n$ に対しても $He_{n_0}^T$ は異なる．
残る一重誤りはゼロベクトル $\mathbf{0}$ である．ゼロベクトルのシンドロームを計算すれば，$H\mathbf{0}^T = \mathbf{0}^T$ が従う．我々は行列 H に対して「行列 H のどの列も要素に 1 つ以上 1 をもつ」という構造を仮定している．よってどの $1 \leqq n_0 \leqq n$ に対しても

$$He_{n_0}^T \neq \mathbf{0}^T = H\mathbf{0}^T$$

が従う．以上から主張を得た．

正：

$$He_{n_1}^T = \begin{pmatrix} h_{1,n_0} \\ h_{2,n_0} \\ \vdots \\ h_{m,n_0} \end{pmatrix} = h_{*,n_1}$$

となり H の第 n_1 列と一致する．「行列 H のどの列もベクトルとしてすべて異なる」と仮定しているから，どの $1 \leqq n_1 \leqq n$ に対しても $He_{n_1}^T$ は異なる．
残る一重誤りはゼロベクトル $\mathbf{0}$ である．ゼロベクトルのシンドロームを計算すれば，$H\mathbf{0}^T = \mathbf{0}^T$ が従う．我々は行列 H に対して「行列 H のどの列も要素に 1 つ以上 1 をもつ」という構造を仮定している．よってどの $1 \leqq n_1 \leqq n$ に対しても

$$He_{n_1}^T \neq \mathbf{0}^T = H\mathbf{0}^T$$

が従う．以上から主張を得た．

7　第８章「最小距離復号のＮＰ完全性」

◆１８７ページ，定理８．４０（帰着の推移性）の証明
下から３行目
誤：
帰着関数 f_{32} を計算するチューリング機械 T_{31} を

正：
帰着関数 f_{31} を計算するチューリング機械 T_{31} を

◆１８９ページ，補題８．４３
誤：
1. $e \leqq t$ を満たさなければ，

正：
1. $\mathrm{wt}(e) \leqq t$ を満たさなければ，

8　第９章「LDPC 符号と sum-product 復号法」

別ファイルを参照。

URL：http://manau.jp/codingBook/correctionChapter9.pdf

9　第１０章「リード・ソロモン符号とユークリッド復号法」

◆２６４ページ，補題１０．４８の証明
下から２行目、
誤：
各 $\deg r_{l_0}(X)$ は非負整数，もしくは，∞ しか取りえない．

正：
各 $\deg r_{l_0}(X)$ も非負整数しか取りえない．

◆２６５ページ，補題１０．４８の証明
上から２行目、
誤：
もし $r_l(X) \geqq 0$ であれば，

正：
もし $\deg r_l(X) \geqq 0$ であれば，

◆２６８ページ，定理１０．５０（誤り位置の検出）
４行目以降、
誤：
多項式 $e(X) \in \mathbb{F}[X]$ を，次数が n 次未満であり，ゼロでない係数は t 個以下とする．$e(X)$ の非ゼロの係数をもつ次数の集合を $\mathcal{E}$ とする．そして，多項式 $\sigma(X) \in \mathbb{F}[X]$ を

$$\sigma(X) := \prod_{n_2 \in \mathcal{E}} (1 - a^{n_2} X)$$

と定義する．

以上の記号のもと，次の (1)∼(3) が従う．

(1)　$\sigma(X)$ は，以下の条件 (A)∼(D) を満たす．

(A)　$\sigma(0) = 1$.
(B)　$\deg \sigma(X) \leqq t$.

ここで，多項式 $S(X) \in \mathbb{F}[X]$ を以下で定義しよう：

$$S(X) := \sum_{n_1=0}^{2t-1} e(a^{n_1+1}) X^{n_1}.$$

そのうえで，次が成り立つ．

(C)　各 $t \leqq n_0 < 2t$ に対し，積 $\sigma(X)S(X)$ の n_0 次の係数は 0.
(D)　$\sigma(X)S(X)$ の $t-1$ 次以下の式を $\eta(X)$ と表せば，$\sigma(X)$ と $\eta(X)$ を同時に割り切る $\mathbb{F}$ 上の多項式は定数のみ．

正：
多項式 $e(X) \in \mathbb{F}[X]$ を，$\deg e < n$ であり，ゼロでない係数は t 個以下とする．$e(X)$ の非ゼロの係数をもつ次数の集合を $\mathcal{E}$ とする．

ここで，多項式 $S(X) \in \mathbb{F}[X]$ を以下で定義する：

$$S(X) := \sum_{n_1=0}^{2t-1} e(a^{n_1+1}) X^{n_1}.$$

多項式　$\overline{\sigma}(X)$　に対する条件 (A)∼(D) を以下で定義する．

(A)　$\overline{\sigma}(0) = 1$.
(B)　$\deg \overline{\sigma}(X) \leqq t$.
(C)　各 $t \leqq n_0 < 2t$ に対し，積 $\overline{\sigma}(X)S(X)$ の n_0 次の係数は 0.
(D)　$\overline{\sigma}(X)S(X)$ の $t-1$ 次以下の式を $\eta(X)$ と表せば，$\overline{\sigma}(X)$ と $\eta(X)$ を同時に割り切る $\mathbb{F}$ 上の多項式は定数のみ．

多項式 $\sigma(X) \in \mathbb{F}[X]$

$$\sigma(X) := \prod_{n_2 \in \mathcal{E}} (1 - a^{n_2} X)$$

に関して、(1) が従う.

(1)　$\sigma(X)$ は条件 (A)∼(D) を満たす.

◆２７０ページ，定理１０．５０（誤り位置の検出）の証明
上から６行目、
誤：

$$\sum_{n_2' \in \mathcal{E}} e_{n_2'} \left(\prod_{n_2 \in \mathcal{E} \setminus \{n_2'\}} (1 - a^{n_2} X) \right) (a^{n_2'} - a^{(2t+1)n_2'}) X^{2t}$$

正：

$$\sum_{n_2' \in \mathcal{E}} e_{n_2'} \left(\prod_{n_2 \in \mathcal{E} \setminus \{n_2'\}} (1 - a^{n_2} X) \right) (a^{n_2'} - a^{(2t+1)n_2'} X^{2t})$$

◆２７２ページ，注意１０．５１
下から２行目、
誤：
この等式から，$R_1(X) = b(X)R(X)$ が従う.

正：
この等式から，$R'(X) = b(X)R(X)$ が従う.

◆２７３ページ，定理１０．５２

誤：

$$-\frac{\eta(a^{-n_2})}{\sigma'(a^{-n_2})} = e_{n_2}.$$

正：

$$-\frac{\eta(a^{-n_2})}{\sigma(a^{-n_2})'} = e_{n_2}.$$

◆２７４ページ，定義１０．５４（ユークリッド復号法）
手順７.
誤：

$$e_{n_0} := \begin{cases} -\dfrac{\eta(a^{n_0})}{\sigma'(a^{n_0})} & (n_0 \in \mathcal{E}) \\ 0 & (n_0 \notin \mathcal{E}) \end{cases}$$

正：

$$e_{n_0} := \begin{cases} -\dfrac{\eta(a^{n_0})}{\sigma'(a^{n_0})} & (\sigma(a^{-n_0}) = 0) \\ 0 & (\sigma(a^{-n_0}) \neq 0) \end{cases}$$

◆２７５ページ，補題１０．５５
下から２行目の左辺
誤：deg$\sigma(X)$

正：deg$T_l(X)$

◆２７６ページ，補題１０．５５の証明
１行目、式（１０．１０）の左辺
誤：deg$\sigma(X)$

正：deg$T_l(X)$

◆２７７ページ，上から５行目，
誤：

$$T_l(X)S(X) = -a(X)X^{2t} + r_l(X)$$

正：

$$T_l(X)S(X) = -R_l(X)X^{2t} + r_l(X)$$

◆２７８ページ，上から６行目，

誤：

$$T_l(X)S(X) + a(X)X^{2t} = r_l(X) = b(X)\eta(X)$$

正：

$$T_l(X)S(X) + R_l(X)X^{2t} = r_l(X) = b(X)\eta(X)$$