2009 年度春期　応用数学 I・情報数学特論　期末試験 (担当:角皆)

実施: 2009 年 7 月 30 日 (木), 13:30 〜 14:30, 8–208 教室

1. 一般的な諸注意

- 学生証を机上に提示すること。学生証を忘れた者は、学務課窓口に行って「臨時学生証 (定期試験用)」を作成してもらうこと。
- 上の場合を含め、入室は試験開始後 20 分まで認める。退室は試験開始後 30 分を過ぎてから終了 10 分前まで認める。
- 机の上に出してよい物は、学生証の他に筆記用具・下敷 (白色かそれに近いもので無地) ・時計 (電卓機能等のないもの) のみ。
- ノート・プリント・参考書等の参照不可。計算機の使用不可。
- 携帯電話等は電源を切って鞄の中にしまっておくこと。くれぐれも鳴らさないこと。時計としての使用も不可。
- 不正の疑いを招く行為は慎むこと。
- 試験開始の指示があるまでは、問題用紙を裏返しておくこと。
- 試験開始後、まづ初めに学生番号・名前を答案用紙に記入すること。学生番号・名前の記入はボールペン・サインペン等で行なうこと。
- 答案用紙の 2 枚目以降が必要な場合は挙手して申し出ること。2 枚目以降にも学生番号・名前の記入を忘れずに。また、全ての用紙の右上に何枚目中の何枚目かを記入すること (n 枚目中の k 枚目なら k/n)。
- 試験時間が終了したら直ちに解答を終了して筆記用具を置き、その後で指示に順って答案を提出すること。

2. 問題について

- 問題番号の順に解答する必要はないが、どこがどの問題か明確に判るようにすること。
- **採点者が読めない答案・意図が伝わらない答案では採点できない。**

3. レポートについて

本授業の評価は本試験とレポートとを合わせて行なうので、本試験の成績が良くても、レポートは提出しなくてはならない。特に、本試験では採り挙げる内容を絞ったので、ここで問われていない内容についてはレポートで答えることが望まれる。

- 期日: **8 月 7 日 (金)20 時頃**まで
- 内容: プリントで配布したような内容、及び授業に関連する内容で、授業内容の理解または発展的な取組みをアピールできるようなもの。
  - ⋆ 問 1–1 は ((1)〜(5) のうち 1 つ以上を) 必修課題とする。
  - ⋆ 問 2–1 は、数学領域以外の理工学専攻の受講者のみ評価対象とする。
  - ⋆ 3 節以降の問題は、全部で 3 つ程度以上を目安に提出せよ。プリントの課題例を全て提出する必要はない。また、課題例になくても関連する内容や自分で調べたり考えたりしたことがあれば、それでも良い。
- 提出方法 :
  - ⋆ 紙媒体: 4–574 室扉のレポートポストに提出。科目名・学生番号・氏名を明記した表紙を付けること。その他、レポートとして常識的な体裁を整えること。
  - ⋆ 電子メイル: 電子メイルでの提出が適切な課題は電子メイルでも良い。初回の授業で配布したプリントに記載したメイルアドレス宛に、メディアセンターの自分のアカウントから提出すること (そうでないとスパムメイルと誤認して消してしまう可能性が高い)。質問などのメイルも歓迎する。
- プリントの課題例を全て提出する必要はない。写して沢山出すくらいなら、少しでも自分でちゃんとやって提出するように。

2009 年度春期　応用数学 I・情報数学特論　期末試験 (担当:角皆)

問 1. $S = \{a, b, c\}$ を情報源アルファベット、$T = \{0, 1\}$ を伝送アルファベットとし、次で定まる符号 (情報源符号化) $\mathcal{C} : S \longrightarrow T^+$ を考える。(1)〜(3) の 各 $\mathcal{C}$ について、次の (a)〜(c) のどれに当てはまるかを答えた上で、その場合に対する問に答えよ。

(a) 一意符号 (一意復号可能符号) でない。
　問: 2 通り以上に復号され得る受信文字列 $\boldsymbol{t} \in T^+$ の例を挙げよ。

(b) 一意符号であるが、瞬時符号 (瞬時復号可能符号) でない。
　問: 瞬時復号可能でないことを例を挙げて示せ。

(c) 瞬時符号である。
　問: 受信文字列 $\boldsymbol{t} = 11010011 \in T^+$ を復号せよ。

$$(1)\ \mathcal{C} : \begin{cases} a \longmapsto 0 \\ b \longmapsto 01 \\ c \longmapsto 11 \end{cases} \qquad (2)\ \mathcal{C} : \begin{cases} a \longmapsto 0 \\ b \longmapsto 10 \\ c \longmapsto 11 \end{cases} \qquad (3)\ \mathcal{C} : \begin{cases} a \longmapsto 0 \\ b \longmapsto 01 \\ c \longmapsto 001 \end{cases}$$

問 2. 生起確率 $P(a) = \dfrac{3}{4}, P(b) = \dfrac{1}{4}$ を持つ情報源 $\mathcal{S} = (S, P), S = \{a, b\}$ について、

(1) 2 元エントロピー $H(\mathcal{S}) = H_2(\mathcal{S})$ を小数第 2 位まで求めよ。但し、$\log_2 3 = 1.585$ としてよい。

(2) 2 次の拡大情報源 $\mathcal{S}^2 = (S^2, P^{\otimes 2})$ に対する Huffman 符号 $\mathcal{C}_2$ を構成し、“1 文字当たりの平均符号長” $L(\mathcal{C}_2)/2$ を小数第 2 位まで求めよ。

(3) (これを解答する場合は (2) は解答しなくても良い。) 3 次の拡大情報源 $\mathcal{S}^3 = (S^3, P^{\otimes 3})$ に対して同様の計算をせよ。

問 3. 3 次の 2 元 Hamming 符号 $\mathcal{H}$ は、例えば次の形のパリティ検査行列

$$H = \begin{pmatrix} 1 & 1 & 0 & a & 1 & 0 & 0 \\ 1 & 1 & 1 & b & 0 & 1 & 0 \\ 1 & 0 & 1 & c & 0 & 0 & 1 \end{pmatrix}$$

で定まる $[7, 4, 3]$-符号である。

(1) 正しい Hamming 符号になるように、$\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ を与えよ。

(2) $\mathcal{H}$ の生成行列の一つで $GH^T = O$ となるような G を求めよ。

(3) $w(\boldsymbol{e}) = 1$ なる $\boldsymbol{e} \in {\boldsymbol{F}_2}^7$ を列挙し、そのシンドローム $\boldsymbol{e}H^T$ との対照表を作れ。

(4) 受信語 $\boldsymbol{y} = (1\ 0\ 1\ 1\ 0\ 1\ 0) \in {\boldsymbol{F}_2}^7$ について、シンドローム $\boldsymbol{y}H^T$ を計算せよ。また、誤りが 1 箇所以内だと仮定して、誤りを訂正して正しい情報語 $\boldsymbol{s} \in {\boldsymbol{F}_2}^4$ を求めよ。

(5) この符号が完全符号である (Hamming の球充填上界式で等号を実現する) ことを確かめよ。

問 4. RSA 暗号方式によって暗号化を行なう。以下、RSA 暗号化の法 (modulus) を N、暗号化指数 (暗号化鍵) を e とし、公開鍵 $(N, e) = (77, 13)$ とする。

(1) 法 N の素因数分解を知らないという前提で、平文 $M = 3$ を暗号化せよ。

(2) 法 N の素因数分解 $77 = 7 \cdot 11$ を知って、復号鍵 (秘密鍵) d を求めよ。また、これを用いて、暗号文 $C = 6$ を復号せよ。

以上

レポートと合わせて評価を行なうので、ここで採り挙げなかった内容についてはレポートで答えることが望まれる。