情報理論　期末試験

以下の文の(1)～(60)に入るべき用語を選択肢から選び、記号を記述せよ。ただし、一つの設問で選択肢が使われるのは1回だけとは限らない（1点×60）。

1. 現代の情報通信では、まず人間が使う文字や画像などを0と1の組み合わせ、すなわち(1)に置き換える。この置き換えの処理のことを(2)という。つぎに、第三者に情報を読み取られることを防ぐための処理(3)を行い、最後に情報の送信の過程で起こった変化を検出したり、変化前の状態に戻したりするための処理(4)を行う。

［ア］暗号化　［イ］記号　［ウ］ハフマン符号
［エ］通信路符号化　［オ］情報源符号化　［カ］符号

2. 情報を送るときは、まず人間が使う文字などにあたる(5)から 0 と 1 の組み合わせへの置き換えを行う。ひとつの(5)の置き換えの結果として得られる 0 と 1 の並びのことを(6)という。通信の効率は(5)と(6)の対応の決め方によって決まり、すべての(5)に対して同じ長さの(6)を割り当てる方法のことを(7)と呼ぶ。情報源での(5)の出現率が偏っている場合は、出現率の高い(5)に割り当てる(6)のビット数を(8)し、出現率が低いもの割り当てるのはその逆になるようにすれば効率を上げられる。

［ア］等長符号　［イ］シンボル　［ウ］符号語
［エ］コンパクト符号　［オ］多く　［カ］少なく

3. 情報源符号化において、平均符号長の値がもっとも(9)符号、すなわち効率が最も(10)符号のことを(11)という。ハフマン符号も(11)のひとつであり、出現率の最も(12)シンボルを結合させる処理を繰り返して符号の木を作ることで得られる。

［ア］コンパクト符号　［イ］小さい　［ウ］良い
［エ］悪い　［オ］木　［カ］大きい

4. シンボルが 2 種類しかない場合に、シンボルの組み合わせをシンボルのように扱い、それらに等長符号を割り当てたものを(13)と呼ぶ。そのかわりにハフマン符号を割り当てたものは(14)と呼ばれる。一般に(13)よりも(14)の方が平均符号長が(15)、効率が(16)。

［ア］良い　［イ］短く　［ウ］固定長ランレングス符号
［エ］悪い　［オ］長く　［カ］ランレングスハフマン符号

5. 第三者に傍受された際に情報が洩れることを防ぐため、そのままでは読めない形に置き換えることを(17)という。置き換え前の文を平文 （読みは(18)）、置き換えたものを(19)という。(17)にはいろいろな方法があるが、(17)の処理とその逆の処理に同じ鍵を使うタイプのものを(20)という。

［ア］ひらぶん　［イ］共通鍵暗号　［ウ］暗号化
［エ］へいぶん　［オ］公開鍵暗号　［カ］暗号文

6. RSA 暗号は(21)の一種であり、暗号化、復号にはそれぞれ 2 つの数値を使う。暗号化の鍵のうちの一つは、まず 2 つの(22)を決め、それらの積 n と、それぞれから 1 を引いた値の(23)である L を求め、L と互いに素で、L より(24)正の整数のリストの中から選んで決める。

［ア］共通鍵暗号　［イ］小さい　［ウ］最小公倍数
［エ］公開鍵暗号　［オ］素数　［カ］最大公約数

7. 事象系とは、(25)とそれが起こる確率を重複・不足のないようにまとめたものであり、行列の形で表わされる。(25)が起こったことで増える情報量は、それが起こる確率の(26)に比例する。事象系全体での情報量の平均値をとったものを(27)と呼ぶ。事象系に含まれる事象がおこる確率がすべて等しいときに(27)の値は(28)になる。

［ア］指数　［イ］最小　［ウ］事象
［エ］エントロピー　［オ］対数　［カ］最大

8. 1 つのサイコロを振り、出た目を調べて「3 以下」「4 以上」という事象から事象系 X、「偶数」「奇数」という事象から事象系 Y をつくると、X の結果が確定している場合は Y の事象の確率が変わる。このとき、これらの事象系には(29)という。また、この変化した確率のことを(30)という。「事象 x_s が起こったことが確定しているときの事象 y_e」は(31)のように記述する。一方の事象系の結果が確定しているときのもう一方の事象系のエントロピーを(32)と呼ぶ。

［ア］$x_s|y_e$　［イ］相関がある　［ウ］条件付き確率
［エ］$y_e|x_s$　［オ］相関がない　［カ］条件付きエントロピー

9. 設問 8 の 2 つの事象系 X, Y を組み合わせ、「3 以下かつ偶数」のような事象から事象系を作ることができる。このような事象系を(33)という。この場合(33)の事象の数は(34)になる。(33)のエントロピーは(35)と呼ばれ、このケースでは(35)の値は元になった事象系のエントロピーの和(36)。

［ア］に等しい　［イ］結合事象系　［ウ］4 つ
［エ］より小さい　［オ］統合事象系　［カ］結合エントロピー

10. 符号 (0 または 1) が通信路を通る過程で別のものに変わってしまうことを(37)、どちらであるかわからなくなってしまうことを(38)という。通信路の性質の表現のしかたとして、図で表わしたものを(39)、行列で表わしたものを(40)という。

［ア］通信路行列　［イ］通信路図　［ウ］消失
［エ］通信路線図　［オ］変化　［カ］不明

11. 通信路への入力からなる事象系を X、出力からなる事象系を Y とし、それらのエントロピーを図で表わすと、その(41)にあたる相互情報量 $I(X,Y)$ が「実質的に通信路を通った情報」であり、この値が大きいほど多くの情報が通ったことになる。$I(X,Y)$ は X の性質と(42)の性質の両方に依存する。X をいろいろに変えて $I(X,Y)$ が(43)になったときの値を(44)と呼ぶ。これは通信路の性能を表わす指標として使われる。

［ア］通信路　　［イ］条件付き確率　　［ウ］最大
［エ］通信路容量　　［オ］重なり部分　　［カ］最小

12. 情報源符号を 1 ビットずつ奇数回ずつ繰り返して送る手法を(45)という。この手法で 3 回ずつ繰り返すとき、例えば受信者が「010」を受け取った場合に、変化が起きたと判定して再送信を要求する手法を(46)、受け取ったものだけを使って情報源符号は「0」であったと判定する手法を(47)という。一般に、(46)の方が(47)よりも誤り率は(48)。

［ア］誤り検出　　［イ］大きい　　［ウ］重複符号
［エ］誤り訂正　　［オ］小さい　　［カ］反復符号

13. パリティ検査符号では、k ビットの情報源符号に対して 1 ビットの検査符号を加える。$k=4$ で情報源符号が「1101」の場合は、加わる検査符号は(49)になる。単純なパリティ検査符号では(50)はできないが、水平垂直パリティ検査符号、すなわち情報源符号を縦横に並べ、その(51)にパリティ検査符号を加える手法を使えば、$(k+1)^2$ ビットの塊の中の誤りが(52)個以下なら(50)ができる。

［ア］誤り検出　　［イ］右と下　　［ウ］0
［エ］誤り訂正　　［オ］2　　［カ］1

14. 符号多項式とは符号の「0」「1」を多項式の係数に置き換えたものであり、例えば「1101」は(53)になる。符号多項式の演算は、1+1 が(54)になること以外は通常のものと変わらない。多項式 $G(x)=x^2+1$ を使って検査符号を加える場合は、1 ブロックあたりの検査符号は(55)ビットになる。受信者は受け取った符号を区切って符号多項式に置き換え、$G(x)$ で割って(56)ときに誤りがないものと判定する。

［ア］x^2+x+1　　［イ］割り切れる　　［ウ］0
［エ］x^3+x^2+1　　［オ］割り切れない　　［カ］2

15. 符号多項式を使った検査符号で $k=4$ のときは、情報源符号「1000」「0100」「0010」「0001」につく検査符号をあらかじめ求めておけば、一般の情報源符号につく検査符号はそれらのそれぞれの桁の(57)で求められる。(57)は記号(58)で表わされる。また、1 ブロックの情報源符号が 4 ビット、検査符号が 3 ビットのケースでは、検査符号と情報源符号からなる(59)つの等式が常に成り立つ。これを使えば、1 ブロックに含まれる誤りが(60)つまでなら誤り訂正ができる。

［ア］2　　［イ］$\oplus$　　［ウ］排他的論理和
［エ］3　　［オ］1　　［カ］直積