

北海道大学 大学院情報科学研究科  
複合情報学専攻 修士課程入学試験

平成 22 年 8 月 18 日(水) 15:30~17:30

専門科目 2

受験上の注意

- 本問題冊子には、小論文の問題が短題と長題の計二題ある。それぞれについて解答せよ。ただし、短題については、(A)から(D)の四間の小間のうちから一問を選択し、解答せよ。
- 選択問題チェック票に受験番号を記入し、選択した短題に印を付け、解答用紙とともに提出すること。
- 解答用の答案用紙は2枚である。この他に下書き用の草案紙2枚を配付する。
- すべての答案用紙に、受験番号、選択した問題番号(例えば、短題(A)、長題など)を必ず記入すること。
- 解答は、問題ごとに別々の答案用紙に記入すること(裏面を使用してもよい。答案用紙が不足したり、破損したりした場合には試験監督員に申し出て受け取ること)。
- 解答が複数枚にわたる時は、1/2、2/2のように答案用紙にページ番号を必ず付すこと、及び受験番号、選択した問題番号を各ページに記入すること。
- 問題冊子、草案紙は持ち帰り、選択問題チェック票とすべての答案用紙を提出すること。
- 机の上に置いてよいものは、筆記用具(鉛筆、消しゴム、鉛筆削りなど)、時計、および特に指示があったもののみである。時計は計時機能のみを使用し、アラームの使用を禁ずる。携帯電話等は電源を切っておくこと。電卓、電子辞書などは使用不可である。

短題

以下の小問(A)～(D)の中から一題を選択し、300字程度で解答せよ。

- (A) 公開鍵暗号方式のひとつである RSA 暗号について、暗号化と複号の手順を説明し、これら手順と暗号化鍵を公開しても、RSA 暗号の安全性が確保される理由を分かりやすく説明せよ。
- (B) 人工知能の基礎となっている探索技術に関連して、(1) 一般的探索アルゴリズム、並びにその特殊ケースといえる(2) 幅優先探索(breadth-first search)、(3) 深さ優先探索(depth-first search)、及び(4) 反復深化探索(iterative deepening search)について概略を説明せよ。その際、以下のキーワードを使用すること。  
【キーワード】初期状態、ノード、探索木、展開、オペレータ、目標状態、経路、キュー、スタック、深さ制限探索
- (C) 「メタヒューリスティクス」について、具体的なアルゴリズムの例をあげつつ、簡潔に説明せよ。また、それをどのような場合に用いるべきか、用いるべきではないかについて説明せよ。
- (D) 多くの自然現象や社会現象が、スケールフリー性（ベキ乗則）に従うことが観察されている。このスケールフリー性について具体的に説明せよ。その際、以下のキーワードを使用すること。  
【キーワード】分布関数、特徴値、ベキ乗関数

$$\begin{array}{r}
 550 \\
 450 \\
 22 \\
 9 \\
 3
 \end{array}
 \begin{array}{r}
 4 \\
 5 \\
 6 \\
 7 \\
 8 \\
 9 \\
 10 \\
 11 \\
 12 \\
 13
 \end{array}
 \begin{array}{r}
 72 \\
 \times 20 \\
 \hline
 440
 \end{array}$$

長題

学習へのコンピュータ支援に関して、以下の二項目を含め、1000 字程度で論述せよ。

(1) ICT を利用した学習は、伝統的な講義だけの学習と比べてどのようなメリットがありうるか、基本的なものを列挙しなさい。

(2) 協調学習を支援する Web アプリケーションを構築する場合、どのようなシステムが考えられるか、基本的な機能と、あなたの提案で狙いとする特徴的な機能に分けて書きなさい。後者については、その機能が協調学習に対してどのような意味で有効なのかを言及すること。

参考

ICT: 情報通信技術 (Information and Communications Technology)

協調学習：協調学習は、複数の人たちがグループに参加して、適切なタイミングで知的資源の紹介を受けながら、協調的に問題解決することにより、「分散しつつ協調して知性が発揮できる個人の育成」を目指すものである。これは、「教師から学生個人への知識の伝達」が中心と考えられる伝統的な学習と対比してとらえることができる。

16  
×10  
320