情報学専攻入学者選抜試験

情報科学

問題冊子

注意事項

1. 試験開始の合図があるまで、この問題冊子の中を見てはいけません。

2. 問題冊子は、表紙を含めて全部で 10 ページあります。試験開始後に問題冊子のページ数を確認して、落丁又は印刷が不鮮明な場合は直ちに申し出てください。

3. 解答は解答用紙に記入してください。問題冊子に記入しても採点されません。

4. 問題冊子、解答冊子は切り離さずにすべて提出してください。

5. ４分野から２分野を選んで解答してください。

情報と数理

（問１）

$g(x)=1+x+x^4$ の$\mathbb{Z}_2$上の根をαとしてα^5 ∈ $\mathbb{GF}(2^4)$の最小多項式を求めよ。ただし、$\mathbb{Z}_2$は2を法とする剰余体とし、$\mathbb{GF}(2^4)$は要素数2のガロア体とする。

（問２）

単純グラフとその補グラフのどちらかは連結であることを証明せよ。

計算機構成論

（問１）

同期式順序回路で構成されたプロセッサの処理速度に関する以下の問に答えなさい。

（１） このプロセッサにおいて、除算命令の実行に要するクロック数は、８クロックである。このプロセッサの動作クロックが 100MHz である時、除算命令の実行時間を求めなさい。

（２） プロセッサの構造・構成をそのままにして処理速度を上げるためには動作クロックの周波数を高くすれば良いが、その周波数には上限が存在する。このプロセッサにおいて動作クロックの上限は何によって決まるのか説明しなさい。

（問２）

分岐先番地を直接指定する絶対ジャンプ命令の他に、分岐先番地をプログラムカウンタからの相対値で指定する相対ジャンプ命令を持つプロセッサを仮定する。また、条件付き分岐ならびに無条件分岐をすべて絶対ジャンプ命令を用いて書いたサブルーチン A と、すべて相対ジャンプ命令を用いて書いたサブルーチン B があるとする。ただし、絶対ジャンプ命令と相対ジャンプ命令の OP コード長、分岐先番地を即値指定するオペランド長、命令全体の命令語長はどれも同じであるものとする。以下の問に答えなさい。

（１） 絶対ジャンプ命令と相対ジャンプ命令について、バイナリコード（機械語コード）の視点から違いを説明しなさい。

（２） サブルーチン A とサブルーチン B がそれぞれ実行されたとき、機能，振る舞いが同じだとすると、バイナリコード以外、サブルーチン A と B は何が異なるのか説明しなさい。

（３） 相対ジャンプ命令が用意されている理由を説明しなさい。

OS とネットワーク

（問１）

複数プロセスが共有資源（shared resources）を利用しようとする場合には、確実に排他制御（mutual exclusion）を行う必要がある。共有資源の利用可能量を保持する変数が管理されているとき、この変数の更新を複数プロセスに許す場合には、クリティカルセクション（critical section）を定義して、その中に２つ以上のプロセスが入らないように制御することによって排他制御を実現することになる。

（1） 代表的な排他制御方式に関する以下の説明文中、ア～オの空欄を適切な用語で埋めなさい。イとウには、アルファベット１文字からなる名前が入る。

> Dekker のアルゴリズムは、特別な命令やハードウェアの助けを必要とせずソフトウェアのみで実現可能であるという利点はある。その一方で、関係プロセスがこの規約を守らない場合は排他制御に失敗するほか、たとえ規約を守っていたとしても、資源の確保を待つプロセスが優先権をひたすらチェックし続ける［ア］が生じることがあり、CPU 資源を無駄にする恐れがある。
>
> セマフォ（semaphore）は、クリティカルセクションに入りたいときにプロセスが行う［イ］操作と、出るときに行う［ウ］操作を用いる。［イ］操作は、共有資源をひとつ確保し、共有資源に空きがない場合にはこのプロセスを［エ］状態に移行させる。一方、［ウ］操作は共有資源をひとつ解放するとともに、［エ］状態のプロセスが存在する場合は、ひとつを［オ］状態に移行させる。この方式で［ア］が発生することはないが、２つの操作を行わずに共有資源へアクセスすることを禁止することはできず、その場合には排他制御に失敗する。

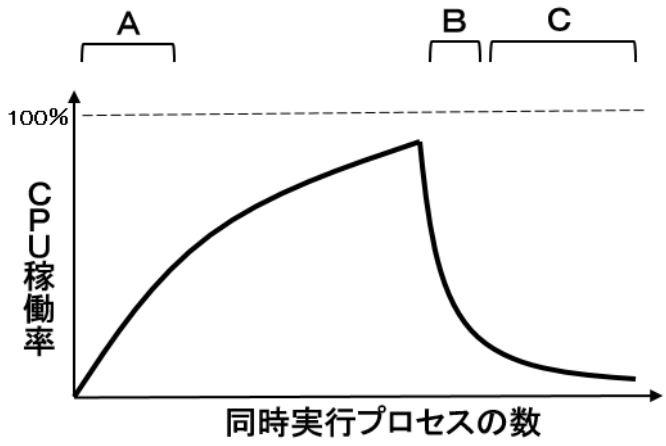
（2） モニタ（monitor）は、オブジェクト指向の概念に基づいて共有資源をカプセル化することで排他制御を実現する。

① この方式が Dekker のアルゴリズム、およびセマフォの欠点を補える理由を説明しなさい。

② モニタを提供するプログラミング言語には、排他制御をするために要請される言語仕様がある。それはどのようなことか説明しなさい。

（問２）

パーソナルコンピュータ上で、同時に実行しているプロセス数と CPU 稼働率との関係を調査すると、多くの場合は下のグラフのようになる。次の問いに答えなさい。



（１） A 部は、同時実行プロセスが少ない場合であっても、CPU 稼働率はそれほど上がらないことを表している。それはなぜか説明しなさい。

（２） B 部は、同時実行プロセス数がある数を超えると、一気に CPU 稼働率が下がることを表している。それはなぜか説明しなさい。

（３） C 部は、実行プロセスが多数あるにもかかわらず、ほとんどその実行ができない状況になっていることを表している。この状態を何と呼ぶか答えなさい。

（問３）

オペレーティングシステムが提供するファイルシステムでは、各ファイルに対して、そのファイルが保持するデータそのもの以外に、オペレーティングシステムやユーザが利用する目的で、様々な属性情報が管理されている。次の例を参考に、利用目的を３つ挙げ、それぞれについてどのような属性情報を管理しているか答えなさい。

例：　異なるデータをユーザが識別できるように、ファイル名を管理する

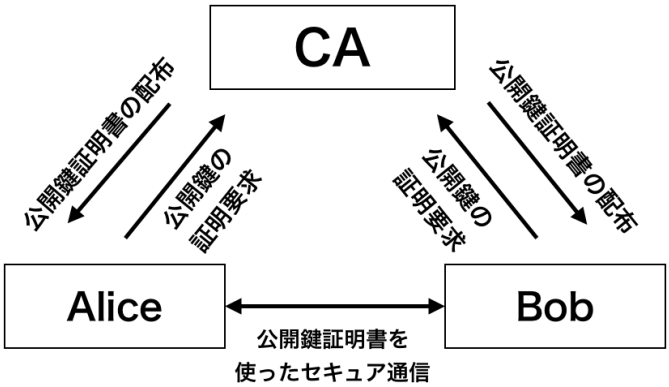
（問４）

異なる場所に設置されたクライアントとサーバの間で、次のような条件で通信を行う場合にかかる応答時間が何秒となるか答えなさい。ただし、クライアントの送信処理の始まりから受信処理が終了するまでを応答時間とし、距離による遅延は考慮しないものとする。

クライアント-サーバ間の伝送速度	20M ビット/秒
伝送効率	80%
送信データ量	アップロード 2M バイト ダウンロード 4M バイト
サーバの処理時間	送受信を合計して 0.2 秒
クライアントの処理時間	送受信を合計して 0.2 秒

（問５）

以下の図は公開鍵暗号基盤（PKI）における CA とユーザ間の関係についての概要を示したものである。図中の「公開鍵の証明要求」「公開鍵証明書の配布」「公開鍵証明書を使ったセキュア通信」の３つの動作について、以下の問いに答えなさい。



（１）　**「公開鍵の証明要求」**について、なぜ利用者（Alice や Bob）は CA に公開鍵を証明してもらう必要があるのか。簡潔に説明しなさい。

（２）　**「公開鍵証明書の配布」**について、誰が誰に対してどのような作業を行うのか。公開鍵証明書の作成方法に着目して説明しなさい。

（３）　**「公開鍵証明書を使ったセキュア通信」**で行われる一連の作業について説明しなさい。説明にあたっては、公開鍵証明書の検証、および通信の暗号化・復号に誰のどの鍵を用いる必要があるのかを明記すること。

知能システム

（問１）

人間以外の「ボット」が人間向けのサービスにアクセスすることを避けるために、CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) と呼ばれる一種のチューリングテストが Web サービスのリクエスト時を中心に広く用いられている。

これについて以下の問題に解答せよ。

（注）著作権上問題のない画像に差し替えています

（１）「チューリングテスト」とは何か。最も適切な説明がされているものを１つ選べ。

(a) 計算可能な問題のクラスがいかなる構造をもっているかを調べるテストのこと。

(b) チューリングマシンがそのテープにある初期状態に対して有限時間で停止するかを調べるテストのこと。

(c) あるマシンが知的であるかどうかを調べるためのテストのこと。

（２）CAPTCHA の機能について、次の用語をすべて用いて適切に説明せよ。

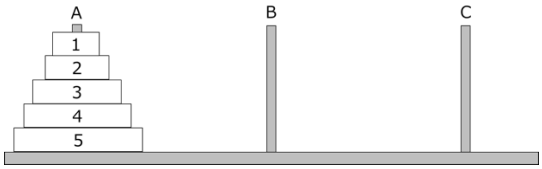
人間	知性	テスト	情報セキュリティ技術	判定

（３）（２）で述べた機能について、その機能が実効性をもつための条件、限界とその解決方法を知能システムの発展の観点から論ぜよ。

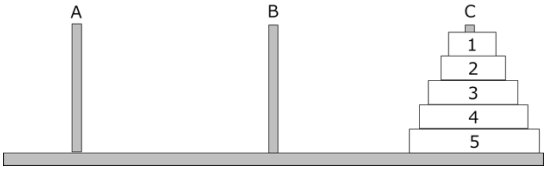
（問２）

ある知的な問題を、計算機に解かせるための方法について考える。

3 本の棒（左から順に A, B, C と呼ぶ）と、5 枚の円盤（小さい順に 1, 2, 3, 4, 5 と呼ぶ）からなるパズルがある。真横から見ると、初期状態では、棒 A に円盤 1, 2, 3, 4, 5 が、大きな円盤が一番下になるよう順番に刺さっている（下図左; 初期状態）。これら 5 枚の円盤を棒 C に、大きな円盤が一番下になるよう順番に刺さった状態にしたい（下図右; 目標状態）。このとき、棒 B は円盤の一時的な置き場所として使用できる。ただし、円盤を移動させる手数は最小限にとどめたい。このパズルでは、円盤は一度に 1 枚しか移動できない。また、小さな円盤の上に大きな円盤を乗せることはできない。このパズルは、円盤の枚数を 6 枚、7 枚、…N 枚と増加させていった場合にも、同様の手続きとルールで解くことができる。



初期状態



目標状態

円盤を 5 枚用いた場合の初期状態から目標状態へ至るまでの各円盤の動きを書き出した結果、以下のように 31 手を要した。

1手目.円盤1: A → C
2手目.円盤2: A → B
3手目.円盤1: C → B
4手目.円盤3: A → C
5手目.円盤1: B → A
6手目.円盤2: B → C
7手目.円盤1: A → C
8手目.円盤4: A → B
9手目.円盤1: C → B
10手目.　円盤2: C → A
11手目.　円盤1: B → A
12手目.　円盤3: C → B
13手目.　円盤1: A → C
14手目.　円盤2: A → B
15手目.　円盤1: C → B
16手目.　円盤5: A → C
17手目.　円盤1: B → A
18手目.　円盤2: B → C
19手目.　円盤1: A → C
20手目.　円盤3: B → A
21手目.　円盤1: C → B
22手目.　円盤2: C → A
23手目.　円盤1: B → A
24手目.　円盤4: B → C
25手目.　円盤1: A → C
26手目.　円盤2: A → B
27手目.　円盤1: C → B
28手目.　円盤3: A → C
29手目.　円盤1: B → A
30手目.　円盤2: B → C
31手目.　円盤1: A → C

（1）　上記の実行結果を見ると、3 手目で円盤 2 枚の山が棒 B に、7 手目で円盤 3 枚の山が 棒 C に、15 手目で円盤 4 枚の山が棒 B にできている。円盤 N 枚でこのパズルを解く場合、最大の円盤 N が棒 A から棒 C へ移動する直前のタイミングで棒 B にできている山には　何枚の円盤があると言えるか、N を用いて答えよ。

（2）　（1）のように、同じような構造の問題に対して繰り返し同じ手続きを適用していくことで問題全体を解こうとするアルゴリズムの名称を答えよ。

（3）　円盤 2 枚を用いた場合の最少手数は 3 手、3 枚を用いた場合の最少手数は 7 手、4 枚を用いた場合の最少手数は 15 手だと言う。100 枚の円盤からなる上記のパズルを人間が 1 人で解くことはできるか、あるいは解くことができないか。「解くことができる」、「解くことができない」の 2 つの選択肢のうちいずれかに丸を付けたうえで、そのように考えた理由を具体的に説明しなさい。なお、1 手にかかる操作時間は 1 秒とする。