COMPUTER SCIENCE TRIPOS Part Ib

Monday 3 June 2002 1.30 to 4.30

Paper 3

Answer **five** *questions.*
Submit the answers in five **separate** *bundles, each with its own cover sheet. On each cover sheet, write the numbers of* **all** *attempted questions, and circle the number of the question attached.*

You may not start to read the questions printed on the subsequent pages of this question paper until instructed that you may do so by the Invigilator

1 Compiler Construction

(*a*) Give a diagram showing the phases of a typical compilation system for a language like C which produces a directly executable fully-linked binary file as output. For each phase, describe in a paragraph what it does (mentioning possible implementation techniques) and give a brief overview of the data-structures used for its input and output indicating whether they would normally reside in a file or in memory. (Do not specify details of any files used to automate the writing of any of the above phases.) [16 marks]

(*b*) Indicate how a typical Java implementation might differ and explain what is meant by *just-in-time compilation*. [4 marks]

2 Introduction to Security

(*a*) (*i*) Explain the collision resistance requirement for the hash function used in a digital signature scheme. [4 marks]

(*ii*) Show how the DES block cipher can be used to build a 64-bit hash function. Is the result collision resistant? [4 marks]

(*b*) A sequence of plaintext blocks $P_1, \ldots, P_8$ is encrypted using DES into a sequence of ciphertext blocks. Where an IV is used, it is numbered C_0. Owing to a transmission error, one bit in ciphertext block C_3 changes its value, and as a consequence, the receiver obtains after decryption a corrupted plaintext block sequence $P'_1, \ldots, P'_8$. For the following modes of operation, how many bits do you expect to be wrong in each block P'_i?

(*i*) Cipher block chaining. [2 marks]

(*ii*) 64-bit output feedback. [2 marks]

(*c*) (*i*) Explain the *Feistel principle* used by block ciphers such as DES and its purpose. [4 marks]

(*ii*) Using a given pseudo-random function $F : \{0,1\}^{100} \to \{0,1\}^{100}$, construct a pseudo-random permutation $P : \{0,1\}^{300} \to \{0,1\}^{300}$ by extending the Feistel principle appropriately. [4 marks]

3 Data Structures and Algorithms

Some languages allow the user to allocate and free space explicitly using calls such as `malloc(size)` and `free(ptr)`. The blocks of space are typically allocated from a large region that you can assume is a vector.

(*a*) Discuss the issues that must be considered when deciding how to implement such space allocation functions. [6 marks]

(*b*) Outline the design of a standard algorithm for space allocation using the first fit strategy, and outline an algorithm based on the binary buddy system in which block sizes are rounded up to the next power of 2. [7 marks each]

4 Computer Design

For each of the following, explain the difference between:

(*a*) analogue computer and digital computer; [4 marks]

(*b*) data-flow and control-flow model of computation; [4 marks]

(*c*) little endian and big endian; [4 marks]

(*d*) latency and bandwidth of data transmission; [4 marks]

(*e*) spatial locality and temporal locality of data. [4 marks]

5 Continuous Mathematics

Consider the trigonometric series

$$\frac{a_0}{2} + \sum_{r=1}^{\infty} (a_r \cos rx + b_r \sin rx)$$

where $a_0, a_1, a_2, \ldots$ and $b_1, b_2, \ldots$ are constants and suppose that $f(x)$ is a periodic function of x with period 2π.

(a) State expressions for the constants a_0, a_r, b_r $(r = 1, 2, \ldots)$ so that the trigonometric series forms the *Fourier series* of $f(x)$ over the interval $-\pi < x \leqslant \pi$. Such expressions are then known as the *Fourier coefficients* of $f(x)$. [4 marks]

(b) State the *Dirichlet conditions* on the function $f(x)$ for it to be represented by its Fourier series at all points in the interval $-\pi < x \leqslant \pi$ at which the function $f(x)$ is continuous. [2 marks]

(c) Determine simplified expressions for the Fourier coefficients when the function $f(x)$ is an even function of x. [3 marks]

(d) Consider the function $f(x)$ which is periodic with period 2π and is defined by $f(x) = x^2$ in the interval $-\pi < x \leqslant \pi$. Does the function $f(x)$ satisfy the Dirichlet conditions? Briefly justify your answer. [2 marks]

(e) Determine the Fourier series for this function $f(x)$. [6 marks]

(f) By substituting a suitable value for x in the Fourier series show that

$$\frac{\pi^2}{12} = \sum_{r=1}^{\infty} \frac{(-1)^{r+1}}{r^2}.$$

[3 marks]

6 Computation Theory

(*a*) Explain how each number $e \in \mathbb{N}$ can be decoded uniquely as a register machine program $Prog_e$. [6 marks]

(*b*) What would it mean for a register machine to *decide the halting problem*? [4 marks]

(*c*) Prove that such a register machine cannot exist. (You may assume the existence of suitable register machines for copying registers and manipulating lists of numbers so long as you specify their behaviour clearly.) [10 marks]

7 Numerical Analysis I

(*a*) Consider a version of the Brown model in which the significand of a floating-point number is represented as $d_0.d_1d_2\ldots d_{p-1}$. Explain the parameters β, p, $e_{\max}$, $e_{\min}$ of the model. [3 marks]

(*b*) Describe the layout of bits in IEEE single precision and give the values of the above four parameters. [5 marks]

(*c*) IBM System/370 single precision uses the same total number of bits, and a similar method for storing negative exponents. However, there are 7 bits for the exponent, and all bit patterns represent numbers. Given $\beta = 16$, deduce the values of the remaining three parameters for this floating-point implementation. [5 marks]

(*d*) If $\beta = 10, p = 3$ how should 6.789, 6.785, 6.755 be rounded using the "round to even" method? [3 marks]

(*e*) Now consider $\beta = 2$, $p = 8$ on a machine with just one guard digit. How should the following be rounded using "round to even"?

$$0\,1\,1\,0\,1\,0\,1\,1\,0$$
$$1\,0\,1\,1\,1\,0\,1\,0\,1$$
$$1\,1\,0\,1\,0\,0\,0\,1\,1$$
$$0\,1\,1\,1\,1\,1\,1\,1\,1$$

[4 marks]

8 Computer Graphics and Image Processing

(*a*) Describe an algorithm which draws a Bezier cubic curve to a specified tolerance using straight lines. [7 marks]

(*b*) Describe an algorithm for clipping a line against a rectangle. [8 marks]

(*c*) A Bezier cubic curve could be clipped and drawn using the algorithm in (*a*) to produce straight lines and the algorithm in (*b*) to do the clipping. Describe a more efficient algorithm which draws a Bezier cubic curve clipped against a rectangle. [5 marks]

END OF PAPER