Discrete Structures	Prelim 1 sample questions
CS2800	Selected problems from past exams

1. True/false. For each of the following statements, indicate whether the statement is true or false. Give a one or two sentence explanation for your answer.

   (a) A proof that starts "Choose an arbitrary $y \in \mathbb{N}$, and let $x = y^2$" is likely to be a proof that $\forall y \in \mathbb{N}, \forall x \in \mathbb{N}, \ldots$.

   (b) The set of real numbers ($\mathbb{R}$) is countable.

   (c) The set of rational numbers ($\mathbb{Q}$) is countable.

   (d) Recall that $[X \to Y]$ denotes the set of functions with domain X and codomain Y. Let $f : 2^S \to [S \to \{0, 1\}]$ be given by $f : X \mapsto h$ where $h : S \to \{0, 1\}$ is given by $h : s \mapsto 0$. f is one-to-one.

   (e) f as just defined is onto.

2. Prove the following claim using induction: for any $n \geq 0$, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

3. Complete the following diagonalization proof:

   Claim: $X = [\mathbb{N} \to \mathbb{N}]$ is uncountable.

   Proof: We prove this claim by contradiction. Assume that X is countable. Then there exists a function F : **FILL IN** that is **FILL IN**.

   Write $f_0 = F(0)$, $f_1 = F(1)$, and so on. We can write the elements of X in a table:

	0	1	2	$\cdots$
f_0	$f_0(0)$	$f_0(1)$	$f_0(2)$	$\cdots$
f_1	$f_1(0)$	$f_1(1)$	$f_1(2)$	$\cdots$
$\vdots$	$\vdots$	$\vdots$		$\ddots$

   Let f_D : **FILL IN** be given by $f_D : x \mapsto$ **FILL IN**

   Then **FILL IN**

   This is a contradiction because **FILL IN**.

4. Compute $10101b + 101b$ (recall that b indicates the strings of digits should be interpreted as integers using the binary representation). Express your answer in both binary and decimal.

5. Suppose you are given a function $f : \mathbb{N} \to \mathbb{N}$, and are told that $f(1) = 1$ and for all n, $f(n) \leq 2f(\lfloor n/2 \rfloor) + 1$.

   Use strong induction on n to prove that for all $n \geq 2$, $f(n) \leq 2n \log_2 n$.

   You may write log to indicate $\log_2$. Here is a reminder of some facts about $\lfloor x \rfloor$ and $\log x$:

   - $\lfloor x \rfloor \leq x$
   - $\log 1 = 0$, $\log 2 = 1$
   - $\log(x/2) = \log x - 1$
   - $\log(2^x) = x$
   - $\log(x^2) = 2 \log x$
   - if $x \leq y$ then $\log x \leq \log y$

6. In this problem, we are working mod 7, i.e. $\equiv$ denotes congruence mod 7 and $[a]$ is the equivalence of a mod 7.

   (a) What are the units of $\mathbb{Z}_7$? What are their inverses?

(b) Compute $[2]^{393}$.

7. Which of the following sets are countably infinite and which are not countably infinite? Give a one to five sentence justification for your answer.

   (a) The set Σ^* containing all finite length strings of 0's and 1's.

   (b) The set $2^{\mathbb{N}}$ containing all sets of natural numbers.

   (c) The set $\mathbb{N} \times \mathbb{N}$ containing all pairs of natural numbers.

   (d) The set $[\mathbb{N} \to \{0, 1\}]$ containing all functions from $\mathbb{N}$ to $\{0, 1\}$.

   Be sure to include enough detail:

   - If listing elements, be sure to clearly state how you are listing them;
   - If diagonalizing, be sure it is clear what your diagonal construction is;
   - If providing a function, make sure it is clear what the output is on a given input.

8. Use Euler's theorem and repeated squaring to efficiently compute $8^n \mod 15$ for $n = 5$, $n = 81$ and $n = 16023$. Hint: you can solve this problem with 4 multiplications of single digit numbers. Please fully evaluate all expressions for this question (e.g. write 15 instead of $3 \cdot 5$).

9. For any function $f : A \to B$ and a set $C \subseteq A$, define $f(C) = \{f(x) \mid x \in C\}$. That is, $f(C)$ is the set of images of elements of C. Prove that if f is injective, then $f(C_1 \cap C_2) = f(C_1) \cap f(C_2)$ for all $C_1, C_2 \subseteq A$.

   (*Hint:* one way to prove this is from the definition of set equality: $A = B$ iff $A \subseteq B$ and $B \subseteq A$.)

10. The Fibonacci numbers $F_0, F_1, F_2, \ldots$ are defined inductively as follows:

$$\begin{aligned} F_0 &= 1 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2} \quad \text{for } n \geq 2 \end{aligned}$$

   That is, each Fibonacci number is the sum of the previous two numbers in the sequence. Prove by induction that for all natural numbers n (including 0):

$$\sum_{i=0}^{n} F_i \;=\; F_{n+2} - 1$$

11. Prove by induction that for any integer $n \geq 3$, $n^2 - 7n + 12$ is non-negative.

12. (a) Recall Bézout's identity from the homework: for any integers n and m, there exist integers s and t such that $gcd(n, m) = sn + tm$. Use this to show that if $gcd(k, m) = 1$ then $[k]$ is a unit of $\mathbb{Z}_m$.

    (b) Use part (a) to show that if p is prime, then $\phi(p) = p - 1$.

    (c) Use Euler's theorem to compute $3^{38} \mod 37$ (note: 37 is prime).

13. To disprove $\exists x, \neg\forall y, \neg\exists z, \neg F(x, y, z)$, what would you need to show?

    (a) $\exists x, \exists y, \exists z, F(x, y, z)$

    (b) $\exists x, \exists y, \exists z, \neg F(x, y, z)$

    (c) $\forall x, \forall y, \forall z, F(x, y, z)$

    (d) $\forall x, \forall y, \forall z, \neg F(x, y, z)$

14. (a) Write the definition of "$f : A \to B$ is injective" using formal notation ($\forall$, $\exists$, $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $=$, $\neq$, $\ldots$).

(b) Similarly, write down the definition of "$f : A \to B$ is surjective".

(c) Write down the definition of "A is countable". You may write "f is surjective" or "f is injective" in your expression. (Note: we gave two slightly different definitions of countable in lecture; we will accept either answer).

15. Recall that the composition of two functions $f : B \to C$ and $g : A \to B$ is the function $f \circ g : A \to C$ defined as $(f \circ g)(x) = f(g(x))$. Prove that if f and g are both injective, then $f \circ g$ is injective.

16. For each of the following functions, indicate whether the function f is injective, whether it is surjective, and whether it is bijective. Give a one sentence explanation for each answer.

    (a) $f : \mathbb{N} \to \mathbb{N}$ given by $f : x \to x^2$

    (b) $f : \mathbb{R} \to \mathbb{R}$ given by $f : x \to x^2$

    (c) $f : X \to [Y \to X]$ given by $f : x \mapsto h_x$ where $h_x : Y \to X$ is given by $h_x : y \mapsto x$.

17. A chocolate bar consists of n identical square pieces arranged in an unbroken rectangular grid. For instance, a 12-piece bar might be a 3×4, 2×6 or 1×12 grid. A single snap breaks the bar along a straight line separating the squares, into two smaller rectangular pieces. Prove that regardless of the initial dimensions of the bar, any n-piece bar requires exactly $n - 1$ snaps to break it up into individual squares.

18. Briefly and clearly identify the errors in each of the following proofs:

    (a) **Proof that 1 is the largest natural number:** Let n be the largest natural number. Then n^2, being a natural number, is less than or equal to n. Therefore $n^2 - n = n(n-1) \le 0$. Hence $0 \le n \le 1$. Therefore $n = 1$.

    (b) **Proof that 2 = 1:** Let $a = b$.

$$\begin{aligned} \Rightarrow \quad && a^2 &= ab \\ \Rightarrow \quad && a^2 - b^2 &= ab - b^2 \\ \Rightarrow \quad && (a+b)(a-b) &= b(a-b) \\ \Rightarrow \quad && a + b &= b \end{aligned}$$

    Setting $a = b = 1$, we get $2 = 1$.

    (c) **Proof that $(a+b)(a-b) = a^2 - b^2$:**

$$\begin{aligned} \text{To prove:} \quad && (a+b)(a-b) &= a^2 - b^2 \\ \Rightarrow \quad && a^2 - ab + ab - b^2 &= a^2 - b^2 \\ \Rightarrow \quad && a^2 - b^2 &= a^2 - b^2 \end{aligned}$$

    ... which is true, hence the result is proved.

19. Prove that $7^m - 1$ is divisible by 6 for all positive integers m.

20. Prove that

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$$

    for all positive integers n.

21. Prove by induction that the sum of the interior angles of a convex[1] polygon with n sides (and hence n vertices) is $180(n-2)$ degrees. You may use the fact that the sum of the interior angles of a triangle is 180 degrees. You do not need to prove straightforward geometrical facts rigorously (check with us if unsure).

[1] A polygon is convex if, for all vertices p and q of the polygon, the line joining p and q lies entirely within the polygon.

22. Suppose that Alice sends the message a to Bob, encrypted using RSA. Suppose that Bob's implementation of RSA is buggy, and computes $k^{-1} \mod 4\phi(m)$ instead of $k^{-1} \mod \phi(m)$. What decrypted message does Bob see? Justify your answer.

23. (a) What are the units of $\mathbb{Z}$ mod 12?

    (b) What are their inverses?

    (c) What is $\phi(12)$?

24. (a) Let $[X \to Y]$ denote the set of all functions with domain X and codomain Y. Give a function f from $[X \to Y] \times [Y \to Z]$ to $[X \to Z]$.

    (b) Is your function injective? Is it surjective? Is it bijective?

    (c) Based on your function, what can you conclude about the relationship between the cardinality of $[X \to Y] \times [Y \to Z]$ and the cardinality of $[X \to Z]$?