CSC3001: Discrete Mathematics

Midterm Exam (Fall 2020)

Instructions:

1. This exam is 120 minute long, and worth 100 points.
2. This exam has 12 pages, consisting of 6 questions, all to be attempted. **Write down your full working in this exam paper**.
3. Calculator is NOT allowed.
4. This exam is in closed book format. No books, dictionaries or blank papers to be brought in except one page of A4 size paper note which you can write anything on both sides. Any cheating will be given **ZERO** mark.
5. As a bonus of reading this instruction, here is a hint for Question 5: induction.

Student Number: ____________________ **Name:** _______________

1. (*18 points*) Suppose that you are given one "**NOT**", three "**AND**"s, and one "**OR**" of the following electronic components:

<table>
<tr><th>Type of Gate</th><th>Symbolic Representation</th><th>Action</th></tr>
<tr><td>NOT</td><td>
</td><td><table><tr><th>Input</th><th>Output</th></tr><tr><td>P</td><td>R</td></tr><tr><td>1</td><td>0</td></tr><tr><td>0</td><td>1</td></tr></table></td></tr>
<tr><td>AND</td><td>
</td><td><table><tr><th colspan="2">Input</th><th>Output</th></tr><tr><td>P</td><td>Q</td><td>R</td></tr><tr><td>1</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>0</td><td>0</td><td>0</td></tr></table></td></tr>
<tr><td>OR</td><td>
</td><td><table><tr><th colspan="2">Input</th><th>Output</th></tr><tr><td>P</td><td>Q</td><td>R</td></tr><tr><td>1</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>0</td><td>0</td><td>0</td></tr></table></td></tr>
</table>

Design a circuit so that it has the following input/output table.

P	Q	R	output
1	1	1	0
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	1
0	0	1	1
0	0	0	0

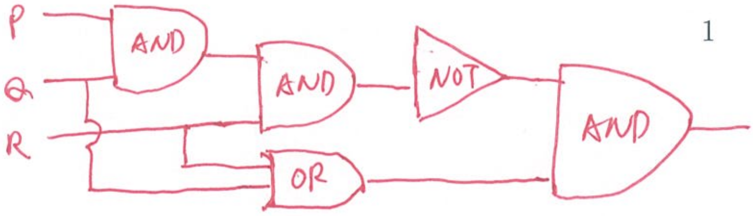
Solution.

$$\overline{P\wedge Q\wedge R}\wedge\overline{P\wedge\overline{Q}\wedge\overline{R}}\wedge\overline{\overline{P}\wedge\overline{Q}\wedge R} \quad 3$$

$$=\overline{P\wedge Q\wedge R}\wedge(\overline{P}\vee Q\vee R)\wedge(P\vee Q\vee R) \quad 3$$

$$=\overline{P\wedge Q\wedge R}\wedge((\overline{P}\wedge P)\vee(Q\vee R)) \quad 3$$

$$=\overline{P\wedge Q\wedge R}\wedge(Q\vee R) \quad 3$$



6

2. (*20 points*) Solve the congruence equation

$$609x \equiv 1 \pmod{2020}$$

Solution. Note that $2020 = 4 \cdot 5 \cdot 101$. By Chinese Remainder Theorem the above equation is equivalent to

3 3

5 $$\begin{cases} 609x \equiv 1 \pmod 4 \\ 609x \equiv 1 \pmod 5 \\ 609x \equiv 1 \pmod{101} \end{cases} \Rightarrow \begin{cases} x \equiv 1 \pmod 4 \\ 4x \equiv 1 \pmod 5 \\ 3x \equiv 1 \pmod{101} \end{cases} \Rightarrow \begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 4 \pmod 5 \\ x \equiv 34 \pmod{101} \end{cases}$$

Let $x_1, x_2, x_3 \in \mathbb{Z}$ be such that

2 2

$$505x_1 \equiv 1 \pmod 4, \quad 404x_2 \equiv 1 \pmod 5, \quad 20x_3 \equiv 1 \pmod{101}$$

2 $$\Rightarrow x_1 \equiv 1 \pmod 4, \quad x_2 \equiv 4 \pmod 5, \quad x_3 \equiv -5 \pmod{101}$$

By Chinese Remainder Theorem we have

$$x = 505 \cdot 1 \cdot 1 + 404 \cdot 4 \cdot 4 + 20 \cdot (-5) \cdot 34 \equiv 1549 \pmod{2020}$$ 3

3. (*11 points*) Prove that $15n + 4$ and $10n + 3$ are coprime for any $n \in \mathbb{N}$.
Solution.

$$15n + 4 = (10n + 3) \cdot 1 + (5n + 1)$$ 5

$$10n + 3 = (5n + 1) \cdot 2 + 1$$ 5

Thus, $\mathsf{gcd}(15n + 4, 10n + 3) = 1$. 1

4. (*11 points*) Suppose there are $m + n$ coins along a line where m of them with head facing up and the other n coins with tail facing up. Can we can flip over pairs of adjacent coins so that all the coins have their heads facing up? Discuss for which case we cannot; and for the cases we can, describe a method to flip the coins.
Solution. There are three different cases:

1. $\{H, H\} \to \{T, T\}$
2. $\{H, T\} \to \{T, H\}$
3. $\{T, T\} \to \{H, H\}$ 2

so the number of T is always changed by 0 or ± 2 for each move. Thus, this is only possible when m, n are both even. 4
If m, n are both even, we may flip the coins as follows:

1. Search for T from left to right along the line. 1
2. If no T found, then we are done. Otherwise, flip the first T and its right neighbor. 1

3. If the right neighbor is T, then return to step 1. Otherwise, the right neighbor becomes T after the flip. Then we return to step 2.

Note that this procedure will push all T to the right end, and n is even, so we will eventually have all H facing up.

5. (*20 points*) Let $\{F_n\}$ be defined by $F_1 = 3, F_2 = 4$ and $F_{n+2} = F_n + F_{n+1}$. Prove that $\mathsf{gcd}(F_n, F_{n+1}) = 1$ for all $n \in \mathbb{Z}^+$.

Proof. Set

$$P(n) = \text{"}\mathsf{gcd}(F_k, F_{k+1}) = 1,\ \forall k \le n\text{"}$$

If $k = 1$, we have $\mathsf{gcd}(F_1, F_2) = 1$; if $k = 2$, we have $F_3 = F_1 + F_2 = 7$, and so $\mathsf{gcd}(F_2, F_3) = 1$. Thus, $P(1)$ and $P(2)$ both hold.
Assume $P(m)$ holds for some $m \ge 2$. Then $m - 1 \ge 1$. Consider $n = m + 1$ and denote $g = \mathsf{gcd}(F_{m+1}, F_{m+2})$. Then

$$g \mid F_{m+2} - F_{m+1} = F_m$$

Since $g \mid F_{m+1}$, we have

$$g \mid F_{m+1} - F_m = F_{m-1} \quad \Rightarrow \quad g \mid \mathsf{gcd}(F_{m-1}, F_m) = 1 \quad \Rightarrow \quad g = 1$$

Therefore, $\mathsf{gcd}(F_n, F_{n+1}) = 1$ for all $n \in \mathbb{Z}^+$. □

6. (*20 points*) Let $n \in \mathbb{Z}^+$. Denote by r_n the number of n-bit binary strings that do not contain a substring "001". Use **generating function** to find the recurrence relation and the closed form of r_n. (**Note:** Full mark will be given **ONLY** if you use generating function. You may use the notations $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$.)

Solution. Consider the two cases of n-bit strings that do not contain a substring "001".

① **The first bit is 0:**

- i) If the second bit is 0, then the remaining bits would have to be 0. So there is only one such a string.
- ii) If the second bit is 1, then the remaing string is a $(n-2)$-bit string that does not contain a substring "001". So there are r_{n-2} of such strings.

.

② **The first bit is 1:** Then the remaining string is a $(n-1)$-string that does not contain a substring "001". So there are r_{n-1} of such strings.

Hence, $r_n = r_{n-2} + r_{n-1} + 1$. Let $f(x) = \sum_{n=0}^{\infty} r_n x^n$ with $r_0 := 1$. Then

$$\begin{aligned} f(x) &= r_0 + r_1 x + \ldots + r_n x^n + \ldots \\ &= 1 + (r_0 + 1)x + (r_0 + r_1 + 1)x^2 + \ldots + (r_{n-2} + r_{n-1} + 1)x^n + \ldots \\ &= (1 + x + x^2 + \ldots) + x(r_0 + r_1 x + \ldots) + x^2(r_0 + r_1 x + \ldots) \\ &= \frac{1}{1-x} + (x + x^2) f(x) \end{aligned}$$

So

$$
\begin{aligned}
f(x) &= \frac{1}{1-x} \cdot \frac{1}{1-x-x^2} \\
&= (1+x+x^2+\ldots) \cdot \frac{1}{\sqrt{5}} \left(\frac{\alpha}{1-\alpha x} - \frac{\beta}{1-\beta x} \right) \qquad 2 \\
&= \frac{1}{\sqrt{5}} (1+x+x^2+\ldots) \left[\alpha(1+\alpha x+\alpha^2 x^2+\ldots) - \beta(1+\beta x+\beta^2 x^2+\ldots) \right] \\
&= \frac{1}{\sqrt{5}} (1+x+x^2+\ldots) \left[(\alpha-\beta) + (\alpha^2-\beta^2)x + \ldots + (\alpha^{n+1}-\beta^{n+1})x^n + \ldots \right] \qquad 1
\end{aligned}
$$

and we have

$$
r_n = \frac{1}{\sqrt{5}} \sum_{i=1}^{n+1} (\alpha^i - \beta^i) = \frac{1}{\sqrt{5}} \left(\sum_{i=1}^{n+1} \alpha^i - \sum_{i=1}^{n+1} \beta^i \right) = \frac{1}{\sqrt{5}} \left(\frac{\alpha^{n+1}-1}{\alpha-1}\alpha - \frac{\beta^{n+1}-1}{\beta-1}\beta \right) \qquad 3
$$

which is simplified to

$$
r_n = \left(\frac{2}{\sqrt{5}} + 1 \right) \alpha^n - \left(\frac{2}{\sqrt{5}} - 1 \right) \beta^n - 1 \qquad 2
$$