CS201 · Discrete Mathematics

Midterm Assignment

刘乐奇 / 12011327

April 13, 2022

1 Q1

1. Incorrect.

Step	*Reason*
1. $(\neg p \wedge (p \rightarrow q)) \rightarrow \neg q$	*Premise*
2. $\neg(\neg p \wedge (\neg p \vee q)) \vee \neg q$	*Useful law*
3. $(p \vee (p \wedge \neg q)) \vee \neg q$	*Double negation law & De Morgen's law*
4. $((p \vee p) \wedge (p \vee \neg q)) \vee \neg q$	*Distributive law*
5. $(p \wedge (p \vee \neg q)) \vee \neg q$	*Idempotent law*
6. $(p \vee \neg q) \wedge ((p \vee \neg q) \vee \neg q)$	*Distributive law*
7. $(p \vee \neg q) \wedge (p \vee (\neg q \vee \neg q))$	*Associative law*
8. $(p \vee \neg q) \wedge (p \vee \neg q)$	*Idempotent law*
9. $(p \vee \neg q)$	*Idempotent law*

   It is a contingency.

2. Correct.
   On the left hand side:

Step	*Reason*
1. $(p \vee q) \rightarrow r$	*Premise*
2. $\neg(p \vee q) \vee r$	*Useful law*
3. $(\neg p \wedge \neg q) \vee r$	*De Morgen's law*

   On the right hand side:

Step	*Reason*
1. $(p \rightarrow r) \wedge (q \rightarrow r)$	*Premise*
2. $(\neg p \vee r) \wedge (\neg q \vee r)$	*Useful law*
3. $(\neg p \wedge \neg q) \vee r$	*Distributive law*

   Therefore, they are equivalent.

3. Correct.
   For any number $y \in \mathbb{R}$, if $y \neq 0$, there always exists a reciprocal x of y such that $xy = 1$.

4. Correct.
   Take $n = 1, m = 2$ such that $n^2 + m^2 = 5$. So $\exists n \exists m(n^2 + m^2 = 5)$ in the domain of $\mathbb{Z}$ is T.

2 Q2

1. Let propositions p: you finished your homework; q: you can answer this question. Then Premise 1 is $\neg p \rightarrow \neg q$; Premise 2 is p; Conclusion is q.
   We want to know if $((\neg p \rightarrow \neg q) \wedge p) \rightarrow q$ is a tautology.

Step	*Reason*
1. $((\neg p \rightarrow \neg q) \wedge p) \rightarrow q$	*Premise*
2. $\neg(p \vee q) \vee q$	*Useful law & Double negation law*
3. $(\neg p \wedge \neg q) \vee q$	*De Morgen's law*
4. $(\neg p \vee q) \wedge (\neg q \vee q)$	*Distributive law*
5. $(\neg p \vee q) \wedge T$	*Negation law*
6. $(\neg p \vee q)$	*Identity law*

It is a contingency, not a tautology. Therefore, the argument form is invalid.

2. Let predicates $P(x)$: student x has submitted his or her homework; $Q(x)$: student x can get 100 in the final exam. Domain is the students in this class. Then Premise 1 is $\forall xP(x) \to \forall xQ(x)$; Premise 2 is $\exists x\neg P(x)$; Conclusion is $\neg\forall xQ(x)$.
We want to know if $((\forall xP(x) \to \forall xQ(x)) \wedge (\exists x\neg P(x))) \to (\neg(\forall xQ(x)))$ is a tautology.

Step	*Reason*
1. $((\forall xP(x) \to \forall xQ(x)) \wedge (\exists x\neg P(x))) \to (\neg\forall xQ(x))$	*Premise*
2. $((\forall xP(x) \to \forall xQ(x)) \wedge \neg\forall xP(x)) \to (\neg\forall xQ(x))$	*De Morgen's law for quantifier*
3. $\neg((\neg\forall xP(x) \vee \forall xQ(x)) \wedge \neg\forall xP(x)) \vee (\neg\forall xQ(x))$	*Useful law*
4. $((\forall xP(x) \wedge \neg\forall xQ(x)) \vee \forall xP(x)) \vee (\neg\forall xQ(x))$	*Double negation law*
5. $((\forall xP(x) \vee \forall xP(x)) \wedge (\neg\forall xQ(x) \vee \forall xP(x))) \vee (\neg\forall xQ(x))$	*Distributive law*
6. $(\forall xP(x) \wedge (\neg\forall xQ(x) \vee \forall xP(x))) \vee (\neg\forall xQ(x))$	*Idempotent law*
7. $(\forall xP(x) \vee \neg\forall xQ(x)) \wedge ((\neg\forall xQ(x) \vee \forall xP(x)) \vee \neg\forall xQ(x))$	*Distributive law*
8. $(\forall xP(x) \vee \neg\forall xQ(x)) \wedge (\neg\forall xQ(x) \vee \neg\forall xQ(x) \vee \forall xP(x))$	*Commutative law*
9. $(\forall xP(x) \vee \neg\forall xQ(x)) \wedge (\neg\forall xQ(x) \vee \forall xP(x))$	*Idempotent law*
10. $\forall xP(x) \vee \neg\forall xQ(x)$	*Idempotent law*

It is a contingency, not a tautology. Therefore, the argument form is invalid.

3 Q3

Step	*Reason*
1. $(\neg r \vee (p \wedge \neg q)) \to (r \wedge p \wedge \neg q)$	*Premise*
2. $\neg(\neg r \vee (p \wedge \neg q)) \vee (r \wedge p \wedge \neg q)$	*Useful law*
3. $(r \wedge (\neg p \vee q)) \vee (r \wedge p \wedge \neg q)$	*De Morgen's law* & *Double negation law*
4. $r \wedge ((\neg p \vee q) \vee (p \wedge \neg q))$	*Associative law* & *De Morgen's law*
5. $r \wedge (\neg p \vee ((q \vee p) \wedge (q \vee \neg q)))$	*Associative law* & *De Morgen's law*
6. $r \wedge (\neg p \vee ((q \vee p) \wedge T))$	*Negation law*
7. $r \wedge (\neg p \vee (q \vee p))$	*Identity law*
8. $r \wedge (T \vee q)$	*Commutative law* & *Associative law*
9. $r \wedge T$	*Domination law*
10. r	*Identity law*

By Addition rule of inference, we have

$$r \to (r \vee s)$$

that is,

$$(\neg r \vee (p \wedge \neg q)) \to (r \wedge p \wedge \neg q) \to (r \vee s)$$

which is what we need to prove.

4 Q4

1. Let $A = \{1, 1\}, B = \{2, 2\}$, then $A \times B = \{(1, 2)\}, B \times A = \{(2, 1)\}$. We have $\mathcal{P}(A \times B) = \{\emptyset, (1, 2)\} \neq \mathcal{P}(B \times A) = \{\emptyset, (2, 1)\}$

2. By definition, we have $A \oplus B = (A \cap \overline{B}) \cup (B \cap \overline{A})$. Then

$$
\begin{aligned}
&(A \oplus B) \oplus B \\
&= ((A \cap \overline{B}) \cup (B \cap \overline{A})) \oplus B && \textit{By definition} \\
&= (\overline{(A \cap \overline{B}) \cup (B \cap \overline{A})} \cap B) \cup (((A \cap \overline{B}) \cup (B \cap \overline{A})) \cap \overline{B}) && \textit{By definition} \\
&= ((\overline{A} \cup B) \cap (\overline{B} \cup A) \cap B) \cup (((A \cap \overline{B}) \cup (B \cap \overline{A})) \cap \overline{B}) && \textit{De Morgen's law} \\
&= ((\overline{A} \cup B) \cap ((\overline{B} \cup A) \cap B)) \cup (((A \cap \overline{B}) \cup (B \cap \overline{A})) \cap \overline{B}) && \textit{Associative law} \\
&= ((\overline{A} \cup B) \cap ((\overline{B} \cap B) \cup (A \cap B))) \cup (((A \cap \overline{B}) \cap \overline{B}) \cup ((B \cap \overline{A}) \cap \overline{B})) && \textit{Distributive law} \\
&= ((\overline{A} \cup B) \cap (\emptyset \cup (A \cap B))) \cup (((A \cap \overline{B}) \cap \overline{B}) \cup ((B \cap \overline{A}) \cap \overline{B})) && \textit{Complement law} \\
&= ((\overline{A} \cup B) \cap (A \cap B)) \cup (((A \cap \overline{B}) \cap \overline{B}) \cup ((B \cap \overline{A}) \cap \overline{B})) && \textit{Identity law} \\
&= (((\overline{A} \cup B) \cap A) \cap B) \cup ((A \cap (\overline{B} \cap \overline{B})) \cup ((B \cap \overline{B}) \cap \overline{A})) && \textit{Associative law} \\
&= (((\overline{A} \cup B) \cap A) \cap B) \cup ((A \cap \overline{B}) \cup ((B \cap \overline{B}) \cap \overline{A})) && \textit{Idempotent law} \\
&= (((\overline{A} \cap A) \cup (B \cap A)) \cap B) \cup ((A \cap \overline{B}) \cup ((B \cap \overline{B}) \cap \overline{A})) && \textit{Distributive law} \\
&= ((\emptyset \cup (B \cap A)) \cap B) \cup ((A \cap \overline{B}) \cup (\emptyset \cap \overline{A})) && \textit{Complement law} \\
&= ((\emptyset \cup (B \cap A)) \cap B) \cup ((A \cap \overline{B}) \cup \emptyset) && \textit{Domination law} \\
&= ((B \cap A) \cap B) \cup (A \cap \overline{B}) && \textit{Identity law} \\
&= (B \cap B \cap A) \cup (A \cap \overline{B}) && \textit{Commutative law} \\
&= (B \cap A) \cup (A \cap \overline{B}) && \textit{Idempotent law} \\
&= A \cap (B \cup \overline{B}) && \textit{Distributive law} \\
&= A \cap U && \textit{Complement law} \\
&= A && \textit{Identity law}
\end{aligned}
$$

3. $\forall y \in f(S \cap T), \exists x \in S \cap T \subseteq S$ (or T, equivalently), we have $y = f(x)$, i.e., $f(S \cap T) \subseteq f(S) \cap f(T)$. But reversely, $\forall y \in f(S) \cap f(T), \exists x \in S$ (or T), we have $y = f(x) \in S$ (or T). However, we cannot guarantee that $x \in S \cap T$. Therefore, $f(S \cap T) \subset f(S) \cap f(T)$.

4. For any $x \in f^{-1}(S \cap T)$, there exists $y \in s \cap T \subseteq S$ (or T, equivalently) such that $y = f(x)$, i.e., $f^{-1}(S \cap T) \subseteq f^{-1}(S) \cap f^{-1}(T)$. For any $x \in f^{-1}(S) \cap f^{-1}(T)$, there exists $y \in S$ or $y \in T$ such that $y = f(x)$, i.e., $f^{-1}(S) \cap f^{-1}(T) \subseteq f^{-1}(S \cap T)$. Therefore, $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$

5 Q5

For any infinite set A, then we can extract an element a_1 from A, a_2 from $A - \{a_1\}$, a_3 from $A - \{a_1, a_2\}$,...,a_{n+1} from $A - \{a_1, a_2, ..., a_n\}$ and so on. Then there at least a sequence $S = \{a_1, a_2, ..., a_n\}$ is countable, i.e., $|A| \geq |S|$. However, for any sequence S, we have $|S| = |\mathbb{Z}^+|$, i.e., $|A| \geq |\mathbb{Z}^+|$. Therefore, there is no infinite set A such that $|A| < |\mathbb{Z}^+|$.

6 Q6

$$(\log n)^{\log \log n}, \log(n^n), n^2(\log n)^{20}, n^{20}, 2^n, (n!)^5$$

For $k = 2^{64}, C = 1$, we have

$$(\log n)^{\log \log n} \leq C \log(n^n)$$

whenever $n > k$. Therefore, $(\log n)^{\log \log n} = O(\log(n^n))$.

7 Q7

From the question we can get the system of linear congruences as below

$$\begin{aligned}
x &\equiv 1(mod\ 2)\\
x &\equiv 0(mod\ 3)\\
x &\equiv 1(mod\ 4)\\
x &\equiv 4(mod\ 5)\\
x &\equiv 3(mod\ 6)\\
x &\equiv 0(mod\ 7)\\
x &\equiv 1(mod\ 8)\\
x &\equiv 0(mod\ 9)
\end{aligned}$$

Since $gcd(2,4,8) = 2, gcd(3,9) = 3$, we can simplify it. After simplification, we have

$$\begin{aligned}
x &\equiv 4(mod\ 5)\\
x &\equiv 3(mod\ 6)\\
x &\equiv 0(mod\ 7)\\
x &\equiv 1(mod\ 8)\\
x &\equiv 0(mod\ 9)
\end{aligned}$$

Since $x \equiv 4(mod\ 5)$, we have $\exists k \in \mathbb{Z}, x = 4 + 5k$. Substitute into $x \equiv 3(mod\ 6)$, we have

$$\begin{aligned}
&4 + 5k \equiv 3(mod\ 6)\\
\implies\ &k \equiv 25(mod\ 6)\ (since\ 5 \times 5 \equiv 1(mod\ 6))
\end{aligned}$$

Similarly, $\exists t \in \mathbb{Z}, k = 25 + 6t \implies x = 129 + 30t$. Substitute into $x \equiv 0(mod\ 7)$, we have

$$\begin{aligned}
&129 + 30t \equiv 0(mod\ 7)\\
\implies\ &t \equiv 16(mod\ 7)\ (since\ 4 \times 30 \equiv 1(mod\ 7))
\end{aligned}$$

Then, $\exists s \in \mathbb{Z}, t = 16 + 7s \implies x = 609 + 210s$. Substitute into $x \equiv 1(mod\ 8)$, we have

$$\begin{aligned}
&609 + 210s \equiv 1(mod\ 8)\\
\implies\ &210s \equiv 0(mod\ 8)
\end{aligned}$$

then by definition, we have $8|210s$, i.e., $4|105s$. Since $gcd(4,105) = 1$, then by the property of division, we have $4|s$, i.e., $\exists l \in \mathbb{Z}, s = 4l \implies x = 609 + 840l$. Substitute into $x \equiv 0(mod\ 9)$, we have

$$\begin{aligned}
&609 + 840l \equiv 0(mod\ 9)\\
\implies\ &840l \equiv 3(mod\ 9)
\end{aligned}$$

then by definition, we have $9|840l - 3$, i.e., $3|280l - 1 \implies 280l \equiv 1(mod\ 3)$. Since $280 \times 93 \equiv 1(mod\ 3)$, we have

$$l \equiv 93(mod\ 3)$$

Therefore, $\exists r \in \mathbb{Z}, l = 93 + 3r \implies x = 78729 + 2520r = 609 + 2520(r + 31)$. Thus the solution is $x \equiv 609(mod\ 2520)$.

8 Q8

1. Since (a and b are integers, just for short)

$$33^{15} \equiv (32+1)^{15} \equiv 32^{15} + a32^{14} \cdot 1 + \ldots + b32 \cdot 1^{14} + 1^{15} \equiv 1^{15} \equiv 1(mod\ 32)$$

then $(33^{15} \mod 32)^3 \mod 15 = 1^3 \mod 15 = 1$.

2. By Euclidean algorithm, we have

$$\begin{aligned} 1638 &= 7 \times 210 + 168 \\ 210 &= 1 \times 168 + 42 \\ 168 &= 4 \times 42 \end{aligned}$$

So $gcd(210, 1638) = 42$.

3. Since $gcd(34, 89) = 1$, $34y \equiv 1(mod\ 89)$ has solution.

$$\begin{aligned} 89 &= 2 \times 34 + 21 \\ 34 &= 1 \times 21 + 13 \\ 21 &= 1 \times 13 + 8 \\ 13 &= 1 \times 8 + 5 \\ 8 &= 1 \times 5 + 3 \\ 5 &= 1 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 2 &= 2 \times 1 \end{aligned}$$

we have $q = [2, 1, 1, 1, 1, 1, 1, 2]$ and $s = [1, 0, 0, 0, 0, 0, 0, 0], t = [0, 1, 0, 0, 0, 0, 0, 0]$. By iterating $s_i := s_{i-2} - s_{i-1}q_{i-1}$ and $t_i := t_{i-2} - t_{i-1}q_{i-1}$, we can get $s_8 = 13, t_8 = -34$. So the inverse of 34 modulo 89 is -34.
Therefore, $x \equiv 77 \times (-34) \equiv 52(mod\ 89)$.

4. It is to find the solution of $3^{1000} \mod 10$. (a and b are integers, just for short)

$$3^{1000} \equiv 9^{500} \equiv (10-1)^{500} \equiv 10^{500} + a10^{499}(-1) + \ldots + b10(-1)^{499} + (-1)^{500} \equiv (-1)^{500} \equiv 1(mod\ 10)$$

So the last decimal digit of 3^{1000} is 1.

9 Q9

Let $m = kt$, t is odd, then

$$2^m + 1 = (2^k + 1)(2^{k(t-1)} - 2^{k(t-2)} + \ldots - 2^k + 1)$$

Suppose m has an odd factor greater than one, then let $t = 2s + 1, s \geq 1$. We have

$$2^m + 1 = (2^k + 1)(2^{ks} - 2^{k(2s-1)} + \ldots - 2^k + 1)$$

For $s = 1$, $2^m + 1 = (2^k + 1)(2^{2k} - 2^k + 1)$ is not a prime. For $s > 1$, we have $k = \frac{m}{2s+1} < m$, so $2^k + 1 < 2^m + 1$, $2^k + 1$ is a factor of $2^m + 1$, leading a contradiction.

10 Q10

1. Valid.
$(p-1)(q-1) = 88 \times 60 = 5280$, which satisfies $gcd(e, (p-1)(q-1)) = 1$. $ed = 61 \times 4501 = 274561 = 52 \times 5280 + 1$, so $ed \equiv 1(mod\ (p-1)(q-1))$. Therefore, this pair of public key (n, e) and private key d is valid.

2. Invalid.
$(p-1)(q-1) = 88 \times 60 = 5280$, which satisfies $gcd(e, (p-1)(q-1)) = 1$. $ed = 89 \times 4501 = 400589 = 75 \times 5280 + 4589$, so $ed \equiv 4589(mod\ (p-1)(q-1))$, not satisfy the requirement. Therefore, this pair of public key (n, e) and private key d is invalid.

3. Invalid.
$(p-1)(q-1) = 88 \times 60 = 5280$, $gcd(e, (p-1)(q-1)) = 30$, not satisfy the requirement. Therefore, this pair of public key (n, e) and private key d is invalid.

11 Q11

For the first time, I try to use shift cipher to solve this problem.

```
#include <iostream>
#include <cstring>
using namespace std;
int main()
{
    string s = "qy qaq iloiyu uiwx lwhc oiu lwgc i nat ah srasalizcu yae vcjcp gvao oriz yae pc mavvi mcz";
    int len = s.length();

    for (int j = 1; j < 26; j++)
    {
        for (int i = 0; i < len; i++)
        {
            if(s[i]-'a' >= 0 && s[i]-'a' <= 25)
                cout.put('a'+(s[i]-'a'+j)%26);
            else
                cout.put(s[i]);
        }
        cout << endl;
    }
    return 0;
}
```

Unfortunately, it failed.

Then, I made a guess to solve this problem. (Color does not mean anything). I started from $yea'pc$ and

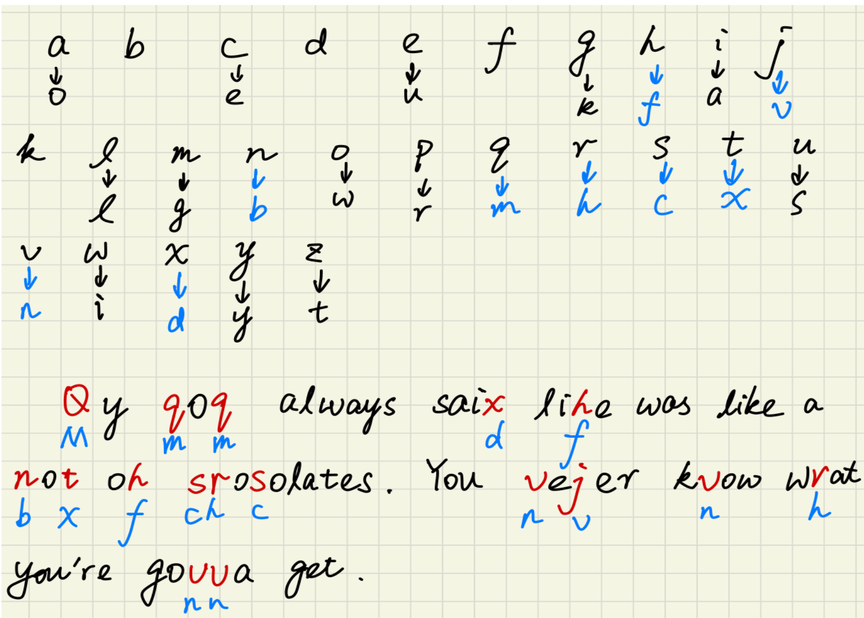

Figure 1: Q11

guessed it may be $you're$. Then I found that i for a word is much probable to be a. Since I had confirmed y is what, then Qy is pretty like to be My and qaq is to be mom. ah is of coming after that, and so on. During the guess, I noticed that l and y do not change before and after the encryption, which means $f(12) = 12$ and $f(25) = 25$. Thus, I had a guess, maybe the encryption function is in the form of

$f(p) = (ap + b) \mod 26$. After that, I tried to use $12 \equiv 12a + b (mod\, 26)$ and $25 \equiv 25a + b (mod\, 26)$ to solve the function. After tested some special cases, I found with $a = 5, b = -22$, the function can be used to decryption. Therefore, I solved for an inverse function of that and the encryption function is as

$$f(p) = 21p + 462 \mod 26$$

It worked well.