MA1100T Quick Notes

§1 Logic

1.1 Statement vs. Proposition vs. Predicate

- A **statement** is a sentence.
- A **proposition** is a statement that is either true or false, but not both.
- A **predicate** is an assignment of truth values to elements of some domain.

1.2 Implications

> "On Wednesdays, we wear pink." – *Mean Girls*

Denoted as $p \to q$, if it is Wednesday today, then I should probably wear pink. If it is not Wednesday, it doesn't mean I cannot wear pink, so we have

p	q	$p \to q$
0	1	1

Moreover, $p \to q \equiv \neg p \vee q$.

1.3 Logical Equivalence

- Two propositional formulas are **logically equivalence** if $\forall$ assignment of truth values of propositions, they have the same truth value.
- Two propositional formulas are **not logically equivalence** if $\exists$ assignment of truth values of propositions, they have different truth values.

1.4 If and only if

$$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$$

p	q	$p \leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

1.4.1 Necessity and Sufficiency

- If $p \to q$ then p is **sufficient** for q.
- If $p \leftarrow q$ then p is **necessary** for q.

Example (SJTU Mathematics Contest 2023)
If α: "The equation of a hyperbola is $x^2 - y^2 = a^2$, $a > 0$" and β: "The asymptotes of this hyperbola form and angle of $\pi/2$".

α	β	α implies β?	β implies α?
1	1	True	False since $(x-1)^2 - y^2 = a^2$ also works
1	0	False since β is true	False since the angle equals $\pi/2$
0	1	True, consider $(x-1)^2 - y^2 = a^2$	False since $(x-1)^2 - y^2 = a^2$ also works
0	0	True, consider $x^2 - 4y^2 = a^2$ and $\theta = 52.13°$	True, if $\theta \neq \pi/2$, the equation doesn't have to be $x^2 - y^2 = a^2$

As we can see, "α implies β" is tally to "$\alpha \to \beta$" but "β implies α" does not tally to "$\beta \to \alpha$" so for β, α is **sufficient** but not **necessary**.

1.5 Tautology & Contradiction

- If $F_1 \equiv F_2$, then $F_1 \leftrightarrow F_2$ is a **tautology**.
- If $F_1 \not\equiv F_2$, then $F_1 \leftrightarrow F_2$ is a **contradiction**.

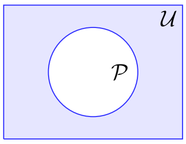
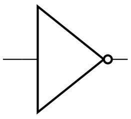
1.6 Useful Denial

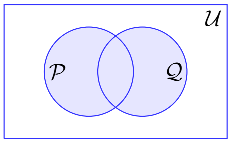
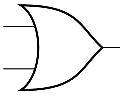
F_2 is a **useful denial** of F_1 iff $F_1 \equiv \neg F_2$.

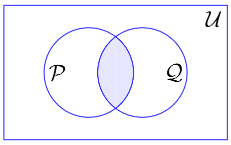
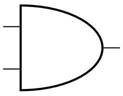
1.7 Boolean Algebra in Words

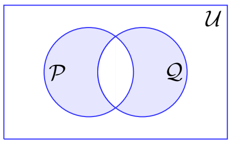
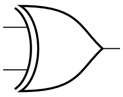
- $p \to q$: shown in §1.2
- $p \wedge \neg p$ is a contradiction: Nothing can be both true and false at the same time.
- $p \vee \neg p$ is a tautology: Something must either be true or false right?
- $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$: Let say if I ask you: "Tea or coffee?". If you want tea but not coffee, then P is true and Q is false, negating lets you drink coffee but not tea, you only drank coffee in the end.
- $\neg(\forall x)(P(x)) \equiv (\exists x)(\neg P(x))$: I don't drink coffee every day, I drank tea on Wednesday.
- $\neg(\exists x)(P(x)) \equiv (\forall x)(\neg P(x))$: Haha you can't find me drinking coffee for all days – I drank tea every day.

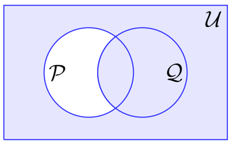
1.8 Boolean, Set Theory, Bitwise Operations, Logic Gates

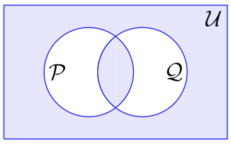
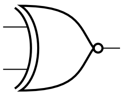
Boolean	Set Theory	Bitwise	Logic Gates
$\neg p$	 $\mathcal{P}^{\complement}$ Complement	NOT $x = \left(2^{\lfloor \log_2 x \rfloor + 1} - 1\right) - x$ `NOT 10110101 = 01001010`	

$p \vee q$	
	$\mathcal{P} \cup \mathcal{Q}$
	Union
		`101101 OR 011001 = 111101`
		`101101`
		`OR 011001`
		`111101`
			

$p \wedge q$	
	$\mathcal{P} \cap \mathcal{Q}$
	Intersection
		`101101 AND 011001 = 001001`
		`101101`
		`AND 011001`
		`001001`
			

$p \oplus q$	
	$\mathcal{P} \triangle \mathcal{Q}$
	Symmetric Difference
		`101101 XOR 011001 = 110100`
		`101101`
		`XOR 011001`
		`110100`
			

$p \to q$	
	$\mathcal{P} \to \mathcal{Q}$
	Implies
		`101101 THEN 011001 = 011011`
		`101101`
		`THEN 011001`
		`011011`	

$p \leftrightarrow q$	
	$\mathcal{P} \leftrightarrow \mathcal{Q}$
	Equivalent
		`101101 XNOR 011001 = 001011`
		`101101`
		`XNOR 011001`
		`001011`
			

1.9 More on Quantifiers

- The **universal quantification** $\forall x P(x)$ states that "**for all** x such that $P(x)$ is true".
- The **existential quantification** $\exists x P(x)$ states that "**there exists** x such that $P(x)$ is true".

1.9.1 Equivalent Formulae on Finite Sets

Let the domain of $P(x)$ be a set with finite cardinality, assign the elements $x_1, x_2, x_3, \ldots, x_k$,

- $\forall x P(x) \equiv \bigwedge_{i=1}^{k} P(x_i)$
- $\exists x P(x) \equiv \bigvee_{i=1}^{k} P(x_i)$

By the inductive process, we can also deduce De Morgan's law.

$$\neg\left(\bigwedge_{i=1}^{k} P(x_i)\right) \equiv \bigvee_{i=1}^{k} (\neg P(x_i))$$

1.9.2 Quantifiers Overloading

Consider the following sentence

"Everyone who takes a break can have a snack."

Let $\mathcal{P}$ be the set of people, and $\mathcal{S}$ be the set of all snacks. We say that $H(p, s)$ equals "person p had snack s". Consider the following formulae:

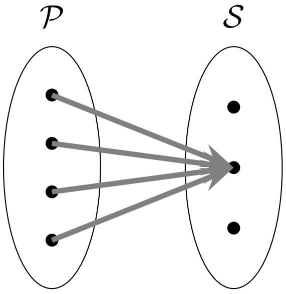
(a)

$$(\exists s)(\forall p) H(p, s)$$

In words, we have

"There exists a snack s (probably KitKat) such that every person p, p ate s."

It is an **all-to-one** situation here.



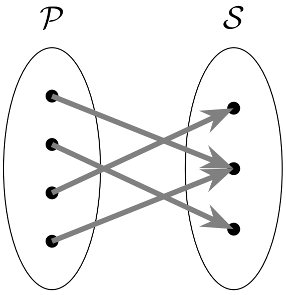
(b)

$$(\forall p)(\exists s)H(p,s)$$

In words, we have

> "For all people p, there exists a snack s such that p ate s."

It is a **one-to-one** situation here.



Moreover, we can stack quantifiers.

- x is irrational: $(\forall p \in \mathbb{Z})(\forall q \in \mathbb{Z})(x \neq p/q) \equiv (\nexists (p,q) \in \mathbb{Z}^2)(x = p/q)$.
- x is rational: $(\exists p \in \mathbb{Z})(\exists q \in \mathbb{Z})(x = p/q) \equiv \neg(\forall (p,q) \in \mathbb{Z}^2)(x \neq p/q)$.

§2 Proofs

No notes GG.

2.1 Tutorial 1

Problem 2.1
In this problem we consider binary logical operators in propositional logic.

1. How many are there?
2. Prove that there are exactly two binary logical operators $\star$ in propositional logic such that $p \ \star (p \vee q)$ is a tautology.

1. $2^{2\times 2} = 16$ of them
2.

p	q	$p \vee q$	$p \star (p \vee q)$
1	1	1	1
1	0	1	1
0	1	1	1
0	0	0	1

Since we know

p	q	$p \star q$
1	1	1
0	1	1
0	0	1

But we don't know the case when p is true and q is false – there are two possibilities, hence there exists two such binary logical operators.

Problem 2.2

Define predicates $P(x)$ and $Q(x)$ with the same domain such that the formulas $\exists x(P(x) \to Q(x))$ and $(\exists x P(x)) \to (\exists x Q(x))$ have different truth values. Be sure to include brief justifications for the truth values of the two formulas (i.e., write down which one is true, which one is false, and why they are each true or false.)

Since $\exists x(P(x) \to Q(x))$ is a *useful denial* of $(\exists x P(x)) \to (\exists x Q(x))$, we have

$$\nexists x(P(x) \to Q(x)) \equiv \forall x(P(x) \wedge \neg Q(x))$$
$$(\exists x P(x)) \to (\exists x Q(x)) \equiv (\nexists x P(x)) \vee (\exists x Q(x))$$

If $\forall x(P(x) \wedge \neg Q(x))$ is true, then $\forall x$, $P(x)$ and $\neg Q(x)$ are true, but this implies $\nexists x P(x)$ and $\exists x Q(x)$ are false, hence $(\nexists x P(x)) \vee (\exists x Q(x)$ is false, no solution.

If $\forall x(P(x) \wedge \neg Q(x))$ is false, then $\nexists x P(x)$ and $\exists x Q(x)$ are false.

Set $P(x)$ be "x is odd" and $Q(x)$ be "x is prime". Let $9 \in \mathcal{U}$ so $\exists x P(x)$. Next choose $4 \in \mathcal{U}$ so $\nexists x Q(x)$ is true and $\forall x(P(x) \wedge \neg Q(x))$ is false.

Therefore an answer is $\boxed{P(x)\text{: "}x\text{ is odd"},\ Q(x)\text{: "}x\text{ is prime"},\ \mathcal{U} = \{4, 9\}}$.

The statement $\exists x(P(x) \to Q(x))$ is true whereas $(\exists x P(x)) \to (\exists x Q(x))$ is false.

Problem 2.3

Same question as the previous, except with the formulas $\forall x(P(x) \vee Q(x))$ and $(\forall x P(x)) \vee (\forall x Q(x))$.

Negating gives

$$\neg(\forall x)(P(x) \vee Q(x)) \equiv \exists x(\neg P(x) \wedge \neg Q(x))$$
$$(\forall x P(x)) \vee (\forall x Q(x)) \equiv (\forall x P(x)) \vee (\forall x Q(x))$$

Assume $\forall x P(x)$ and $\forall x Q(x)$ are false, then $\exists x(\neg P(x) \wedge \neg Q(x))$ is false. This implies that $\forall x(P(x) \vee Q(x))$ is true.

Set $P(x)$ be "x is odd" and $Q(x)$ be "x is prime". Let $9 \in \mathcal{U}$ so $\forall x Q(x)$ is false. Next, choose $4 \in \mathcal{U}$ so $\forall x P(x)$ is false and $\forall x(P(x) \vee Q(x))$ is true.

Therefore an answer is $\boxed{P(x)\text{: “}x\text{ is odd”, } Q(x)\text{: “}x\text{ is prime”, } \mathcal{U} = \{2, 9\}}$.

The statement $\forall x(P(x) \vee Q(x))$ is true whereas $(\forall x P(x)) \vee (\forall x Q(x))$ is false.

Problem 2.4

Prove that if m and n are integers such that mn is even, then either m is even or n is even. In your proof, point out where you are using the following facts (1): every integer is either even or odd; (2) no integer is both even and odd.

We will prove by contradiction. For the sake of contradiction, assume m, n are odd integers by (1). We can express $m = 2k + 1$ and $n = 2\ell + 1$ for some integer k, ℓ. Thus

$$mn = (2k + 1)(2\ell + 1) = 2(2k\ell + k + \ell) + 1$$

which is odd by (2) since it is not divisible by 2.

Problem 2.5

Prove that for every two distinct rational numbers, there is an irrational number in between them. (Recall we proved in lecture that $\sqrt{2}$ is irrational. If you want to claim any other number is irrational, you have to prove your claim first.)

Assume that the two rational numbers are a/b and c/d respectively (a, b, c, d are integers throughout this problem), and that $a/b < c/d$. Choose the number $\frac{a}{b} + \frac{\sqrt{2}}{C}$ for sufficiently large C.

Claim — For some rational number r/s where r, s are coprime integers, and an integer C, the number $\frac{r}{s} + \frac{\sqrt{2}}{C}$ is irrational.

For the sake of contradiction, assume that $\frac{r}{s} + \frac{\sqrt{2}}{C} = \frac{m}{n}$ for some coprime integers m, n. A quick simplification yields

$$2(ns)^2 = C^2(ms - nr)^2$$

This implies that $C(ms - nr)$ is even. In any case, we have $\nu_2\left(2(ns)^2\right)$ is odd but $\nu_2\left(C^2(ms - nr)^2\right)$ is even, hence a contradiction.

Problem 2.6

Prove or disprove: The sum of two irrational numbers is irrational.

Choose $1 \pm \sqrt{2}$, thus $(1 + \sqrt{2}) + (1 - \sqrt{2}) = 2$ is rational.

§3 Induction

3.1 Some Examples

Problem (McCarthy)
Let x be an integer, and

$$f(x) = \begin{cases} x - 10 & x > 100; \\ f(f(x+11)) & x \leq 100 \end{cases}$$

Then $f(x) = 91$ for all $x \leq 101$.

If $90 \leq x \leq 99$, then $f(x) = f(f(x+11)) = f(x+1)$.

If $x = 100$, then $f(100) = f(f(111)) = f(101) = 91$.

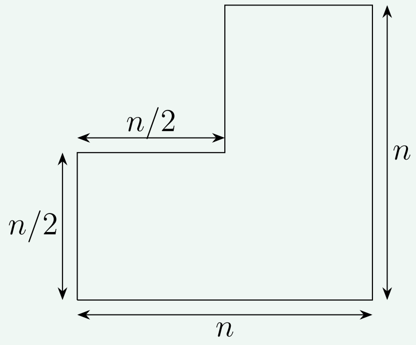
This concludes that for all integers $90 \leq x \leq 100$ we have $f(x) = 91$.

And by the inductive process, let's say $90 - 11k \leq x \leq 100 - 11k$ for some nonnegative integer k. We've proved that case $k = 0$. For other k, $f(f(x)) = f(x+11)$ which can be proved by induction.

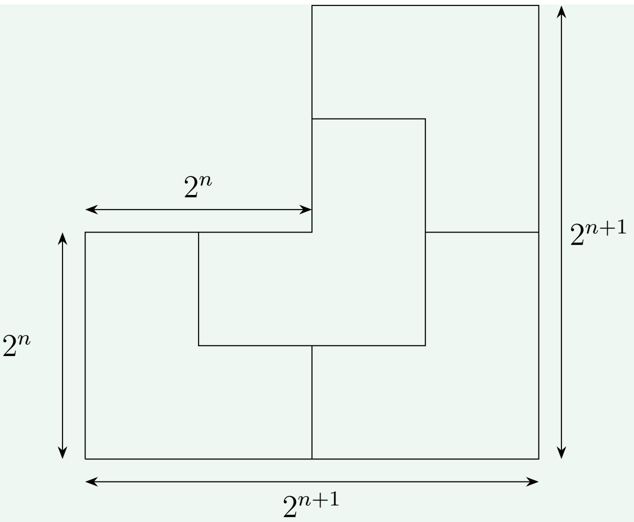
Problem (Golomb, 1965)
Prove that any $2^n \times 2^n$ board with one square removed can be tiled with L-shaped triominoes.

Indeed, we have to use induction twice, as follows:

Claim — Define an *ℓ-block of size n* to be a shape on the board as follows:



then an ℓ-block of size 2^{n+1} can be tiled by ℓ-blocks of size 2^n. A construction can easily show this



Base Case: $n = 1$ is just an L-shaped triomino.
Inductive Step: is shown in the construction above.

Now we have to deal with the entire square.

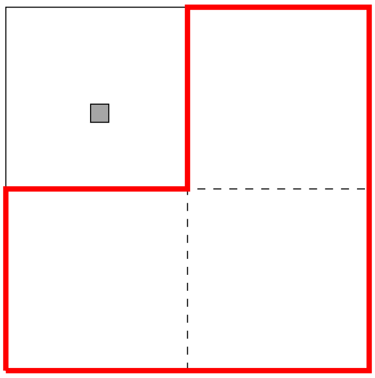
Claim — Any $2^n \times 2^n$ board with one square removed can be tiled with L-shaped triominoes.

We'll proceed by induction.

Assume that for some positive integer n, any $2^n \times 2^n$ board with one square removed can be tiled with L-shaped triominoes.

Base Case: $n = 1$ can be tiled with only one L-shaped triomino.
Inductive Step: Let the square removed be X. Divide the $2^{n+1} \times 2^{n+1}$ board into four equal smaller $2^n \times 2^n$ boards. By the pigeonhole principle, exactly one of the $2^n \times 2^n$ boards must contain X. Let this $2^n \times 2^n$ board be B. The three other $2^n \times 2^n$ boards form an ℓ-block of size 2^{n+1}, which can be tiled.

On the other hand, B can be tiled according to our inductive hypothesis.



3.1.1 A False Induction Proof

> "Assume that for any $n \geq 1$ horses, they have the same color." Taking the first n horses and last n horses, we can conclude that $n+1$ horses have the same color.

The "problem of the problem" lies in the fact that 2 horses, they can have different colors. Hence $P(1) \to P(2)$ does not hold true.

3.1.2 Well-Ordering Principle

Theorem (Well-Ordering Principle)

An **ordered set** is said to be **well-ordered** if each and every nonempty subset has a smallest or least element.

This is the foundation of proof by infinite descent.

3.2 Beyond Induction: Infinite Descent

Problem (IMO 1988)

Let a and b be positive integers such that $ab+1$ divides a^2+b^2. Show that

$$\frac{a^2+b^2}{ab+1}$$

is the square of an integer.

FTSOC, let $\dfrac{a^2+b^2}{ab+1} = k$ for some nonsquare integer k. Rearranging gives

$$a^2 - kab + (b^2 - k) = 0$$

Assume that (a, b) is a solution and WLOG assume $a \geq b$. FTSOC let $a+b$ be minimal. Then (a', b) is also a solution by the quadratic equation in a. By the Vieta's formulas, we have

$$\begin{cases} a + a' = kb \\ aa' = b^2 - k \end{cases}$$

By the first equation, we know that a' is an integer. And by the second equation

$$a' = \frac{b^2-k}{a} \neq 0$$

since $b^2 - k$ cannot equal to 0.

On the other hand, by $a'^2 + b^2 = k(a'b+1)$ implies that $a' > 0$.

Bounding gives

$$a' = \frac{b^2-k}{a} \leq \frac{a^2-k}{a} = a - \frac{k}{a} < a$$

Therefore $a > a'$ which leads to a contradiction by minimality.

3.3 Tutorial 2

Problem 3.1

For each of the following sentences, explain (in one sentence) whether it is true or false. The scope of x and y is taken to be $\mathbb{R}$.

1. $\forall x \exists y (x^2 = y)$
2. $\forall y \exists x (x^2 = y)$
3. $\exists x \forall y (x^2 = y)$
4. $\exists y \forall x (x^2 = y)$
5. $\forall x \forall y (x^2 = y)$
6. $\exists x \exists y (x^2 = y)$

1. True, the value of y is uniquely determined by the value of x^2.
2. False, choose a negative y.
3. False, $x^2 = y$ but $x^2 \neq y + 1$ for every real y.
4. False, if $y = 0$ choose positive x, conversely if $y^2 > 0$ choose $x = 0$.
5. False, $1^2 \neq 0$.
6. True, choose $x = y = 0$.

Problem 3.2

Prove that for every nonzero integer a and b, there is a positive integer c such that a and b both divide c. (Remember, we don't know yet that the lcm exists.) Then prove that there is a smallest positive integer c such that a and b both divide c.

(i) Choose $c = |ab| = |a||b|$.

> **Claim —** For all nonzero integer n and a positive integer m, n divides m if and only if $|n|$ divides m.

If n is positive, then there's nothing to consider.

If $n < 0$ divides m, then m/n is an integer. $|n|/m = -n/m$ which is an integer so $|n|$ divides m.

If $|n|/m = -n/m$ is an integer, then n/m is an integer as well.

So by (i) we know that there exists such c. Moreover, we know that $c/|a|$ and $c/|b|$ are natural numbers. Assume otherwise, c does not have a smallest value, then $c/|a|$ does not have a smallest value, contradicting to the Well-Ordering principle.

Problem 3.3

Use induction to prove that for every n in $\mathbb{N}$, 3 divides $n^3 - n$. (If you want to use facts about division modulo 3 you have to prove them first. The proof I have in mind doesn't use such facts.)

Base Case: $n = 0$, then $n^3 - n = 0 = 3 \times 0$ so 3 divides $n^3 - n$.

Inductive Step: Assume that $n^3 - n$ is divisible by 3 for some n in $\mathbb{N}$. Let $n^3 - n = 3k$ for some integer k. We hope to prove that $(n+1)^3 - (n+1)$ is divisible by 3.

$$\begin{aligned}(n+1)^3 - (n+1) &= n^3 + 3n^2 + 2n \\ &= (n^3 + 3n^2 + 2n + 2(3k)) - 2(3k) \\ &= (3n^3 + 3n^2) - 2(3k) \\ &= 3(n^3 + n^2 - 2k)\end{aligned}$$

Problem 3.4

Define a sequence $\{a_n\}_n$ of real numbers by $a_0 = 0$ and $a_{n+1} = (a_n)^2 + \frac{1}{4}$ for $n \in \mathbb{N}$. Prove that for all n in $\mathbb{N}^+$, we have $0 < a_n < 1$.

It is easy to show that $a_{n+1} > 0$ by $(a_n)^2 + \frac{1}{4} \geq \frac{1}{4} > 0$ for all $n \in \mathbb{N}$.

Claim — $a_n < \frac{1}{2}$ for all $n \in \mathbb{N}$.

We will prove by induction.

Base Case: $a_0 = 0 < \frac{1}{2}$.

Inductive Step: Assume that for some $n \in \mathbb{N}$, we have $a_n < \frac{1}{2}$, we wish to prove that $a_{n+1} < \frac{1}{2}$.

By

$$a_{n+1} = (a_n)^2 + \frac{1}{4} < \left(\frac{1}{2}\right)^2 + \frac{1}{4} = \frac{1}{2}$$

Hence each term $a_n, n \in \mathbb{N}^+$ satisfy $0 < a_n < \frac{1}{2} < 1$.

Problem 3.5

What rule(s) of addition for real numbers (among associativity and commutativity) guarantees that $(a+b)+(c+d) = a+(b+(c+d))$? Use induction to prove that for every $n \in \mathbb{N}^+$ and every sequence of real numbers $\{a_i\}_{i=0}^n$ and $\{b_i\}_{i=0}^n$, we have $\sum_{i=0}^n (a_i+b_i) = \sum_{i=0}^n a_i + \sum_{i=0}^n b_i$. In your proof, specify which rules of addition you use and where.

Left associativity:

$$(a+b)+(c+d) = a+b+(c+d)$$

Right associativity:

$$a+b+(c+d) = a+(b+(c+d))$$

We will proceed by induction.

Base Case: $(a_1)+(b_1) = (a_1+b_1)$ which is obviously true.

Inductive Step: We assume that $\sum_{i=0}^n (a_i+b_i) = \sum_{i=0}^n a_i + \sum_{i=0}^n b_i$, we want

$$\sum_{i=0}^n (a_i+b_i) + (a_{n+1}+b_{n+1}) = \left(\sum_{i=0}^n a_i + a_{n+1}\right) + \left(\sum_{i=0}^n b_i + b_{n+1}\right)$$

Let $p \overset{L}{=} q$ if q can be shown equal to p by using left associativity. Similarly define $p \overset{R}{=} q$ for right associativity and $p \overset{C}{=} q$ for commutativity.

From the right, we have

$$\begin{aligned}\left(\sum_{i=0}^n a_i + a_{n+1}\right) + \left(\sum_{i=0}^n b_i + b_{n+1}\right) &\overset{L}{=} \sum_{i=0}^n a_i + a_{n+1} + \left(\sum_{i=0}^n b_i + b_{n+1}\right) \\ &\overset{R}{=} \sum_{i=0}^n a_i + \left(a_{n+1} + \left(\sum_{i=0}^n b_i + b_{n+1}\right)\right)\end{aligned}$$

While from the left, using our inductive hypothesis, we have

$$\begin{aligned}\sum_{i=0}^n (a_i+b_i) + (a_{n+1}+b_{n+1}) &= \sum_{i=0}^n a_i + \sum_{i=0}^n b_i + (a_{n+1}+b_{n+1}) \\ &\overset{R}{=} \sum_{i=0}^n a_i + \left(\sum_{i=0}^n b_i + (a_{n+1}+b_{n+1})\right) \\ &\overset{C}{=} \sum_{i=0}^n a_i + \left((a_{n+1}+b_{n+1}) + \sum_{i=0}^n b_i\right) \\ &\overset{L}{=} \sum_{i=0}^n a_i + \left(a_{n+1}+b_{n+1} + \sum_{i=0}^n b_i\right)\end{aligned}$$

$$\begin{aligned}&\overset{R}{=} \sum_{i=0}^{n} a_i + \left(a_{n+1} + \left(b_{n+1} + \sum_{i=0}^{n} b_i\right)\right)\\ &\overset{C}{=} \sum_{i=0}^{n} a_i + \left(a_{n+1} + \left(\sum_{i=0}^{n} b_i + b_{n+1}\right)\right)\end{aligned}$$

So we have shown that both sides equal

$$\sum_{i=0}^{n} a_i + \left(a_{n+1} + \left(\sum_{i=0}^{n} b_i + b_{n+1}\right)\right)$$

and therefore we are done.

Problem 3.6

Suppose S is a nonempty subset of $\mathbb{Z}$ which is bounded above by some integer m, i.e., $s < m$ for all $s \in S$. Use well-ordering to prove that S has a largest element.

Step 1: If $m > 0$ then for every element in S, we subtract it by m so that we end up with another set of integers T. If $m \leq 0$ then just let $T = S$. Thus T is a set of nonpositive integers.

Step 2: Similarly, for every element in T, multiply by -1 so that we end up with another set of integers U. Each element in U is nonnegative, hence it is a subset of $\mathbb{N}$.

By the well-ordering principle, U has a smallest element. So T has a largest element and S has a largest element since S, T, U are one to one mappings.

> **Remark.** One can consider the sets of all values $m - s$.

Problem 3.7

Define the predicate $P(n,m)$ to say that there is a finite sequence of positive integers $\{a_i\}_{i=0}^j$ such that

$$\frac{n}{m} = \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_j}}}}.$$

The domain of $P(n,m)$ is the set $\{(n,m) : n,m \in \mathbb{N}^+, n < m\}$. For example, $P(7,9)$ is true, as witnessed by the sequence $a_0 = 1$, $a_1 = 3$, $a_2 = 2$. $P(1,4)$ is true, as witnessed by $a_0 = 4$. (Make sure you understand these computational examples before proceeding.) The goal of this question is to prove that $P(n,m)$ holds for all m and n (in its domain, of course).

1. Suppose $n < m$ are positive integers such that n does not divide m. Prove that there is a largest positive integer a such that $\frac{n}{m} < \frac{1}{a}$.
2. In the context of the previous part, prove that $0 < m - an < n$.
3. Suppose $n < m$ are positive integers such that for all positive integers $n' < n$, $P(n', n)$ holds. Prove that $P(n,m)$ holds.
4. Convince yourself that we have a proof that $P(n,m)$ holds for all m and n.

1. Rearranging gives $a < m/n$, which by Problem 3.6 there is a largest element.

   > **Remark.** By $n/m = 1/a$ we can show that a exists and $a > 0$.

2. For the left part of the inequality, rearranging inequality gives

$$\begin{aligned} a &< m/n \\ an &< m \\ 0 &< m - an \end{aligned}$$

For the right part of the inequality, since m/n is not an integer, there exists a positive integer k such that $k < m/n < k+1$.

If $a < k$ then $a + 1 \leq k < m/n$ which is a contradiction since a is largest positive integer less than m/n. Therefore $k = a$.

Hence

$$\begin{aligned} m/n &< a + 1 \\ m &< an + n \\ m - an &< n \end{aligned}$$

3. By rewriting n/m,

$$\begin{aligned}\frac{n}{m} &= \frac{1}{\frac{m}{n}} \\ &= \frac{1}{a + \frac{m-an}{n}}\end{aligned}$$

   Since $m - an < n$, $P(m - an, n)$ holds. So in this case, let $a_0 = a$, which clearly shows that $P(n, m)$ holds.

4. **Base Case**: A quick check shows that $P(1, 2), P(1, 3), P(2, 3)$ holds.

$$\frac{1}{2} = \frac{1}{1 + \frac{1}{1}} \qquad \frac{1}{3} = \frac{1}{2 + \frac{1}{1}} \qquad \frac{2}{3} = \frac{1}{1 + \frac{1}{2}}$$

   Inductive Step: Now assume that $m = 4$ for example. Then by our induction hypothesis for every integer $2 \leq n < 4$, the statement $P(n, m)$ holds. Assume that for all integers $1 \leq k < n$, $P(k, n)$ holds. Consider $P(k', n + 1)$ where k' is an integer $1 \leq k' < n + 1$. If $n = 1$, choose $a_0 = m$.

   Therefore, we have proved that for all integers $1 \leq n < m$, the statement $P(n, m)$ holds.

§4 Sets

4.1 Fundamental Notations

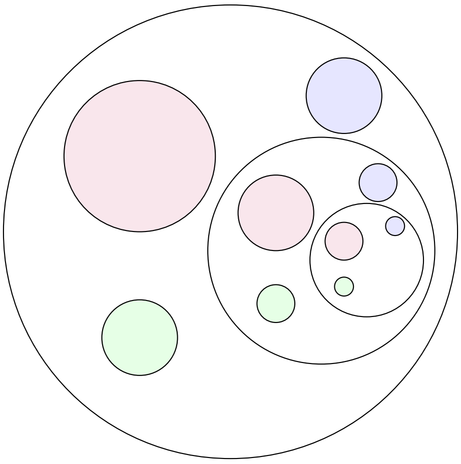
- **Union of Sets**: $\bigcup_{i=0}^{n} A_i =$

4.1.1 Element Chasing

4.2 Russell's Paradox, Zermelo-Fraenkel Set Theory and Axiom of Choice (ZFC)

4.2.1 Russell's Paradox

Consider the set $\mathcal{S}$ that contains ALL sets x that do not contain itself. In other words, $x \notin x$. An illustration below demonstrates how a set can contain itself.



Now, if $\mathcal{S} \in \mathcal{S}$, then $\mathcal{S}$ does not contain itself, by $\mathcal{S}$ is already in $\mathcal{S}$! Contradiction.

However, if $\mathcal{S} \notin \mathcal{S}$, then by negation $\mathcal{S}$ must contain itself. But we cannot find $\mathcal{S}$ in $\mathcal{S}$! Contradiction again.

An analogy by Veritasium on self-referencing paradox is as follows:

> Assume that there's a law in a village that states that the barber has to shave every man who doesn't shave himself. But since the barber is also a man who doesn't shave himself, someone must shave the barber, which is the barber himself! Contradiction.

4.2.2 Zermelo-Fraenkel Set Theory

There are 10 axioms in ZFC. As we proceed, one can progressively lay down the foundations of set theory.

1. **Axiom of extensionality**: $A = B$ if $\forall x((x \in A) \leftrightarrow (x \in B))$
2. **Axiom of empty set**: There is a unique empty set $\varnothing$ (by Extensionality).
3. **Axiom of pairing**: For every two sets A, B, there exists set $C = \{A, B\}$ such that $A \in C$ and $B \in C$.
4. **Axiom of union**: Let A be a set of sets, there exists a set $\bigcup A$ such that the elements in $\bigcup A$ are the elements in the sets in A.

   Now we can have a set of more than 2 elements.

5. **Axiom schema of specification (Aussonderungsaxiom)**: For every formula $\varphi(x)$ and set A, there exists a set S with its elements are the elements x in A such that $\varphi(x)$ holds.
    - **Berry's Paradox**:
6. **Axiom of power set**: For every set A, there exists a set $\mathcal{P}(A)$ whose elements are the subsets of A.
7. **Axiom of infinity**: There exists a set X, such that $\varnothing \in X$ and whenever $x \in X$ we have $x \cup \{x\} \in X$, the **successor** of x.

    Therefore, we can construct the set

    $$\begin{aligned} X_0 &= \varnothing \\ X_1 &= \{\varnothing\} \\ X_2 &= \{\varnothing, \{\varnothing\}\} \\ X_3 &= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} \\ X_4 &= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\} \end{aligned}$$

    This axiom allows us to construct a set with infinitely many elements.
8. **Axiom schema of replacement**: For every formula $\varphi(x, y)$ and set A, if for every $x \in A$ there's a **unique** y such that $\varphi(x, y)$, then there's a set with exactly those y such that there exists some $x \in A$ with $\varphi(x, y)$.
9. **Axiom of foundation**: For every nonempty set (of sets) A, we have an element x such that for every $a \in A$, we have $a \notin x$.

    This, with the axiom of pairing, assures that **no set is an element of itself** $x \notin x$.

4.2.3 Axiom of Choice

4.3 Tutorial 3

Problem 4.1

Let m and n be positive integers. Given a chocolate bar with dimensions m units by n units, your task is to break it down into mn many 1 unit by 1 unit squares. The only operation you can perform is to take a single piece and break it vertically or horizontally. (You can't break multiple pieces in one operation!) Use strong induction to prove that one needs at least $mn - 1$ operations for this task. (Optional: Is $mn - 1$ operations enough?)

Claim — We actually need exactly $mn - 1$ operations.

Assume that after the k'th operation ($k \in \mathbb{N}^+$), we have $P(k)$ pieces. For convention, we also assume $P(0) = 1$. Since after each operation, one of the pieces breaks into two pieces, hence we have

$$P(k+1) = P(k) + 1$$

Claim — $P(k) = k + 1$ for all $k \in \mathbb{N}$.

Base Case: $k = 0$ we have $P(0) = 1$ as defined.

Inductive Step: Assume that $P(k) = k + 1$ holds true for some $k \in \mathbb{N}$, then we have

$$P(k+1) = P(k) + 1 = k + 2$$

as desired.

Problem 4.2

Prove that for all sets A, B and C, we have $(A - B) - C = (A - C) - (B - C)$. (As mentioned in lecture, do not prove this by translating the set identity into a propositional tautology.)

Let a be an element of the set $(A - B) - C$. By set difference we can deduce that $a \in A$ but $a \notin B$ and $a \notin C$.

While on the other hand, $A - C$ is the set of all elements k which $k \in A$ but $k \notin C$. $B - C$ is the set of all elements k which $k \in B$ but $k \notin C$.
Taking the difference $(A - C) - (B - C)$ gives the set of all elements k such that $k \in A$ but $k \notin B$ and $k \notin C$ as desired.

Problem 4.3

Prove that for all sets x and y, the set $\{\{x\}, \{x, y\}\}$ is an element of $\mathcal{P}(\mathcal{P}(\{x, y\}))$.

By the definition of power set, we have

$$\mathcal{P}(\mathcal{P}(\{x,y\})) = \mathcal{P}(\{\varnothing, \{x\}, \{y\}, \{x,y\}\})$$

If the set $\{\{x\}, \{x, y\}\}$ is an element of a power set $\mathcal{P}(\{\varnothing, \{x\}, \{y\}, \{x,y\}\})$, then this set must be a subset of $\{\varnothing, \{x\}, \{y\}, \{x,y\}\}$.

This is true since $\{x\} \in \{\varnothing, \{x\}, \{y\}, \{x,y\}\}$ and $\{x, y\} \in \{\varnothing, \{x\}, \{y\}, \{x,y\}\}$.

Problem 4.4

Prove or disprove: For all sets A, B, C and D, if $A \times B \subseteq C \times D$ then $A \subseteq C$ and $B \subseteq D$.

I claim that this is false.

Consider $A = \varnothing$, $B = \{x\}$, $C = \{y\}$, $D = \{z\}$.

Then $A \times B = \varnothing$, whereas $C \times D = \{(y, z)\}$.

So $A \times B \subseteq C \times D$ but B is not a subset of D since $x \in B$ but $x \notin D$.

Problem 4.5

Prove or disprove: For all sets $\{A_i\}_{i\in I}$ and $\{B_i\}_{i\in I}$, we have $\left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I}(A_i \cup B_i)$.

I claim that this is false.

Consider $I = \{1, 2\}$ and

$$\begin{aligned} A_1 &= \{a\} & A_2 &= \{b\} \\ B_1 &= \{b\} & B_2 &= \{a\} \end{aligned}$$

Then we have

$$\bigcap_{i\in I} A_i = A_1 \cap A_2 = \varnothing$$

$$\bigcap_{i\in I} B_i = B_1 \cap B_2 = \varnothing$$

So we have $\left(\bigcap_{i\in I} A_i\right) \cup \left(\bigcap_{i\in I} B_i\right) = \varnothing$.

But on the other hand,

$$\bigcap_{i\in I}(A_i \cup B_i) = (A_1 \cup B_1) \cap (A_2 \cup B_2) = \{a, b\}$$

which is a counterexample of this statement.

Problem 4.6

Suppose $\{A_i\}_{i\in\mathbb{N}}$ are sets. Prove that

$$\bigcup_{i=0}^{\infty}\bigcap_{j=i}^{\infty} A_j \subseteq \bigcap_{i=0}^{\infty}\bigcup_{j=i}^{\infty} A_j.$$

Let $\mathcal{A} = \bigcup_{i=0}^{\infty}\bigcap_{j=i}^{\infty} A_j$ and $\mathcal{B} = \bigcap_{i=0}^{\infty}\bigcup_{j=i}^{\infty} A_j$. If each of $\bigcap_{j=i}^{\infty} A_j = \varnothing$ for all $i = 0, 1, 2, \ldots$, then $\mathcal{A} = \varnothing$ and we are done.

Assume that for some element a, there exist an index k such that

$$a \in \bigcap_{j=k}^{\infty} A_j$$

This means for every index $N \geq k$, we must have $a \in A_N$.

Now that we want to show $a \in \bigcup_{j=i}^{\infty} A_j$ for all $i = 0, 1, 2, \ldots$.

If $i \leq k$, we have

$$a \in \left(\bigcup_{j=i}^{k-1} A_j\right) \cup A_k \cup \left(\bigcup_{j=k+1}^{\infty} A_j\right)$$

If $i > k$, then we have

$$a \in \bigcup_{j=i}^{\infty} A_j$$

since $i > k$. Hence we have proven that for all $i = 0, 1, 2, \ldots$, $a \in \bigcup_{j=i}^{\infty} A_j$ and therefore $a \in \mathcal{B}$ as desired.

> **Remark.**
>
> - An *index* is a natural number.
> - We define $\bigcup_{i=j}^{k} A_j = \varnothing$ if $k < j$.