Lecture 1
บท: Mathematics as a Language for Computer

วิชา: 819605 Discrete Mathematics

อาจารย์ผู้สอน: ปพนธีร์ แย้มโชติ | วิศวกรรมคอมพิวเตอร์ | ภาคปลาย ปีการศึกษา 2568

ประกาศ: ตกลงร่วมกันเพื่อหาวันเรียนชดเชย สำหรับกลุ่ม (H01)

เนื่องด้วยวันอังคารของกลุ่ม H01 จะชนวันหยุดเยอะมาก (3 มีนาคม, 7, 14 เมษายน, และ 5 พฤษภาคม) ทำให้เราเหลือวันเรียนแค่ 13 ครั้ง จึงจำเป็นต้องหาวันชดเชย 2 วัน เพื่อให้เรียนได้ครบ 15 ครั้ง (เพราะเนื้อหาเยอะ) โดยจะมี 4 ทางเลือก

1. เรียนออนไลน์ทั้ง ๆ ที่วันหยุด (อาจารย์ทำงานทุกวันไม่มีวันหยุดครับ)
2. หาวันชดเชยวันเสาร์หรือวันอาทิตย์ (อาจารย์คิดว่ามีคนทำงานวันธรรมดาอยู่เยอะ)
3. เข้าเรียนของกลุ่ม I01 วันพุธ
4. เรียนกับวิดีโอ

เป้าหมายการเรียนรู้ของเอกสารประกอบนี้

1. แยกให้ได้ว่าประโยคใดเป็น **ประพจน์**
2. แยกบทบาท **สิ่งที่อ้าง** (claim) ออกจาก **เหตุผล/การอ้างอิง** (reason/justification)
3. ใช้โครงร่างการพิสูจน์มาตรฐาน: **ข้อกล่าวอ้าง** $\rightarrow$ **แนวคิด** $\rightarrow$ **พิสูจน์** $\rightarrow$ QED
4. เขียนการพิสูจน์ “ถ้า...แล้ว...” แบบสั้น ๆ ด้วยโครงตัวอย่างโดย **แกะนิยาม** แล้วใช้ให้ถูกต้อง
5. ตรวจข้อผิดพลาดในบทพิสูจน์: หา **จุดที่ผิดกฎ** พร้อมระบุเหตุผลได้และแก้ไขให้ถูก
6. สร้างนิสัย “ลองคิดแย้งดูก่อน” เพื่อปฏิเสธข้อความแบบ **สำหรับทุก...** ด้วย **ตัวอย่างค้าน** (counterexample)

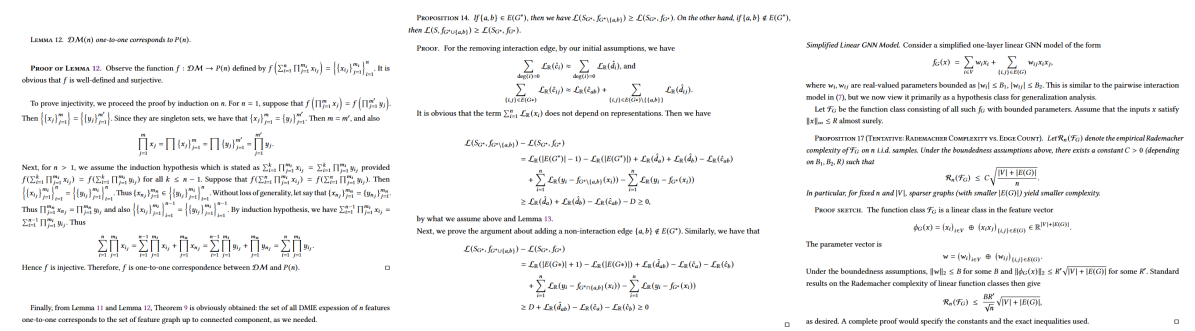
คำถามตั้งต้นของรายวิชา Discrete Mathematics เทอมนี้

1. ทำไมคณิตศาสตร์สำหรับคอมพิวเตอร์ถึงไม่ใช่คณิตศาสตร์แบบคำนวณ แต่เป็นคณิตศาสตร์แบบให้เหตุผล
2. คิดยังไงกับคำพูดที่ว่า "โปรแกรม/ฟังก์ชันทำงานได้ถูกต้อง เพราะผ่านทุก test case ที่ตั้งไว้หมดแล้ว"
3. คำนวณเลขเก่งแล้วจะทำอะไรในคอมพิวเตอร์ได้เก่งบ้าง

ตัวอย่างคอมพิวเตอร์แบบที่ผมเรียนมา (เรียนคอม หนีไม่พ้นคณิตศาสตร์นะครับ)

เพราะเราเรียนไปเป็นนักพัฒนา ผู้ออกแบบ ไม่ใช่ผู้ใช้งาน

(1) งานวิจัย ป.เอก ทาง machine learning ของผม



Lemma 12. *$\mathcal{DM}(n)$ one-to-one corresponds to $P(n)$.*

Proof of Lemma 12. Observe the function $f : \mathcal{DM} \to P(n)$ defined by $f\left(\sum_{i=1}^{n} \prod_{j=1}^{n_i} x_{ij}\right) = \left\{\{x_{ij}\}_{j=1}^{n_i}\right\}_{i=1}^{n}$. It is obvious that f is well-defined and surjective.

To prove injectivity, we proceed the proof by induction on n. For $n = 1$, suppose that $f\left(\prod_{j=1}^{m} x_j\right) = f\left(\prod_{j=1}^{m'} y_j\right)$. Then $\left\{\{x_j\}_{j=1}^{m}\right\} = \left\{\{y_j\}_{j=1}^{m'}\right\}$. Since they are singleton sets, we have that $\{x_j\}_{j=1}^{m} = \{y_j\}_{j=1}^{m'}$. Then $m = m'$, and also

$$\prod_{j=1}^{m} x_j = \prod \{x_j\}_{j=1}^{m} = \prod \{y_j\}_{j=1}^{m'} = \prod_{j=1}^{m'} y_j.$$

Next, for $n > 1$, we assume the induction hypothesis which is stated as $\sum_{i=1}^{k} \prod_{j=1}^{n_i} x_{ij} = \sum_{i=1}^{k} \prod_{j=1}^{n_i} y_{ij}$ provided $f(\sum_{i=1}^{k} \prod_{j=1}^{n_i} x_{ij}) = f(\sum_{i=1}^{k} \prod_{j=1}^{n_i} y_{ij})$ for all $k \leq n-1$. Suppose that $f(\sum_{i=1}^{n} \prod_{j=1}^{n_i} x_{ij}) = f(\sum_{i=1}^{n} \prod_{j=1}^{n_i} y_{ij})$. Then $\left\{\{x_{ij}\}_{j=1}^{n_i}\right\}_{i=1}^{n} = \left\{\{y_{ij}\}_{j=1}^{n_i}\right\}_{i=1}^{n}$. Thus $\{x_{n_j}\}_{j=1}^{n_n} \subseteq \left\{\{y_{ij}\}_{j=1}^{n_i}\right\}_{i=1}^{n}$. Without loss of generality, let say that $\{x_{n_j}\}_{j=1}^{n_n} = \{y_{n_j}\}_{j=1}^{n_n}$. Thus $\prod_{j=1}^{n_n} x_{n_j} = \prod_{j=1}^{n_n} y_{ij}$ and also $\left\{\{x_{ij}\}_{j=1}^{n_i}\right\}_{i=1}^{n-1} = \left\{\{y_{ij}\}_{j=1}^{n_i}\right\}_{i=1}^{n-1}$. By induction hypothesis, we have $\sum_{i=1}^{n-1} \prod_{j=1}^{n_i} x_{ij} = \sum_{i=1}^{n-1} \prod_{j=1}^{n_i} y_{ij}$. Thus

$$\sum_{i=1}^{n} \prod_{j=1}^{n_i} x_{ij} = \sum_{i=1}^{n-1} \prod_{j=1}^{n_i} x_{ij} + \prod_{j=1}^{n_n} x_{nj} = \sum_{i=1}^{n-1} \prod_{j=1}^{n_i} y_{ij} + \prod_{j=1}^{n_n} y_{nj} = \sum_{i=1}^{n} \prod_{j=1}^{n_i} y_{ij}.$$

Hence f is injective. Therefore, f is one-to-one correspondence between $\mathcal{DM}$ and $P(n)$. □

Finally, from Lemma 11 and Lemma 12, Theorem 9 is obviously obtained: the set of all DMIE expression of n features one-to-one corresponds to the set of feature graph up to connected component, as we needed.

Proposition 14. *If $\{a, b\} \in E(G^*)$, then we have $\mathcal{L}(S_{G^*}, f_{G^*\setminus\{a,b\}}) \geq \mathcal{L}(S_{G^*}, f_{G^*})$. On the other hand, if $\{a, b\} \notin E(G^*)$, then $\mathcal{L}(S, f_{G^*\cup\{a,b\}}) \geq \mathcal{L}(S_{G^*}, f_{G^*})$.*

Proof. For the removing interaction edge, by our initial assumptions, we have

$$\sum_{\deg(i)=0} \mathcal{L}_{\mathbb{R}}(\hat{t}_i) = \sum_{\deg(i)=0} \mathcal{L}_{\mathbb{R}}(\hat{d}_i), \text{ and}$$

$$\sum_{\{i,j\}\in E(G*)} \mathcal{L}_{\mathbb{R}}(\hat{t}_{ij}) \approx \mathcal{L}_{\mathbb{R}}(\hat{e}_{ab}) + \sum_{\{i,j\}\in E(G*)\setminus\{\{a,b\}\}} \mathcal{L}_{\mathbb{R}}(\hat{d}_{ij}).$$

It is obvious that the term $\sum_{i=1}^{n} \mathcal{L}_{\mathbb{R}}(x_i)$ does not depend on representations. Then we have

$$\begin{aligned}
\mathcal{L}(S_{G^*}, f_{G^*\setminus\{a,b\}}) &- \mathcal{L}(S_{G^*}, f_{G^*}) \\
&= \mathcal{L}_{\mathbb{R}}(|E(G^*)| - 1) - \mathcal{L}_{\mathbb{R}}(|E(G^*)|) + \mathcal{L}_{\mathbb{R}}(\hat{d}_a) + \mathcal{L}_{\mathbb{R}}(\hat{d}_b) - \mathcal{L}_{\mathbb{R}}(\hat{e}_{ab}) \\
&\quad + \sum_{i=1}^{n} \mathcal{L}_{\mathbb{R}}(y_i - f_{G^*\setminus\{a,b\}}(x_i)) - \sum_{i=1}^{n} \mathcal{L}_{\mathbb{R}}(y_i - f_{G^*}(x_i)) \\
&\geq \mathcal{L}_{\mathbb{R}}(\hat{d}_a) + \mathcal{L}_{\mathbb{R}}(\hat{d}_b) - \mathcal{L}_{\mathbb{R}}(\hat{e}_{ab}) - D \geq 0,
\end{aligned}$$

by what we assume above and Lemma 13.

Next, we prove the argument about adding a non-interaction edge $\{a, b\} \notin E(G^*)$. Similarly, we have that

$$\begin{aligned}
\mathcal{L}(S_{G^*}, f_{G^*\cup\{a,b\}}) &- \mathcal{L}(S_{G^*}, f_{G^*}) \\
&= \mathcal{L}_{\mathbb{R}}(|E(G*)| + 1) - \mathcal{L}_{\mathbb{R}}(|E(G*)|) + \mathcal{L}_{\mathbb{R}}(\hat{d}_{ab}) - \mathcal{L}_{\mathbb{R}}(\hat{e}_a) - \mathcal{L}_{\mathbb{R}}(\hat{e}_b) \\
&\quad + \sum_{i=1}^{n} \mathcal{L}_{\mathbb{R}}(y_i - f_{G^*\cap\{a,b\}}(x_i)) - \sum_{i=1}^{n} \mathcal{L}_{\mathbb{R}}(y_i - f_{G^*}(x_i)) \\
&\geq D + \mathcal{L}_{\mathbb{R}}(\hat{d}_{ab}) - \mathcal{L}_{\mathbb{R}}(\hat{e}_a) - \mathcal{L}_{\mathbb{R}}(\hat{e}_b) \geq 0
\end{aligned}$$

□

Simplified Linear GNN Model. Consider a simplified one-layer linear GNN model of the form

$$f_G(x) = \sum_{i\in V} w_i x_i + \sum_{\{i,j\}\in E(G)} w_{ij} x_i x_j,$$

where w_i, w_{ij} are real-valued parameters bounded as $|w_i| \leq B_1, |w_{ij}| \leq B_2$. This is similar to the pairwise interaction model in (7), but we now view it primarily as a hypothesis class for generalization analysis.

Let $\mathcal{F}_G$ be the function class consisting of all such f_G with bounded parameters. Assume that the inputs x satisfy $\|x\|_\infty \leq R$ almost surely.

Proposition 17 (Tentative: Rademacher Complexity vs. Edge Count). *Let $\mathcal{R}_n(\mathcal{F}_G)$ denote the empirical Rademacher complexity of $\mathcal{F}_G$ on n i.i.d. samples. Under the boundedness assumptions above, there exists a constant $C > 0$ (depending on B_1, B_2, R) such that*

$$\mathcal{R}_n(\mathcal{F}_G) \leq C\sqrt{\frac{|V| + |E(G)|}{n}}$$

In particular, for fixed n and $|V|$, sparser graphs (with smaller $|E(G)|$) yield smaller complexity.

Proof sketch. The function class $\mathcal{F}_G$ is a linear class in the feature vector

$$\phi_G(x) = (x_i)_{i\in V} \oplus (x_i x_j)_{\{i,j\}\in E(G)} \in \mathbb{R}^{|V|+|E(G)|}.$$

The parameter vector is

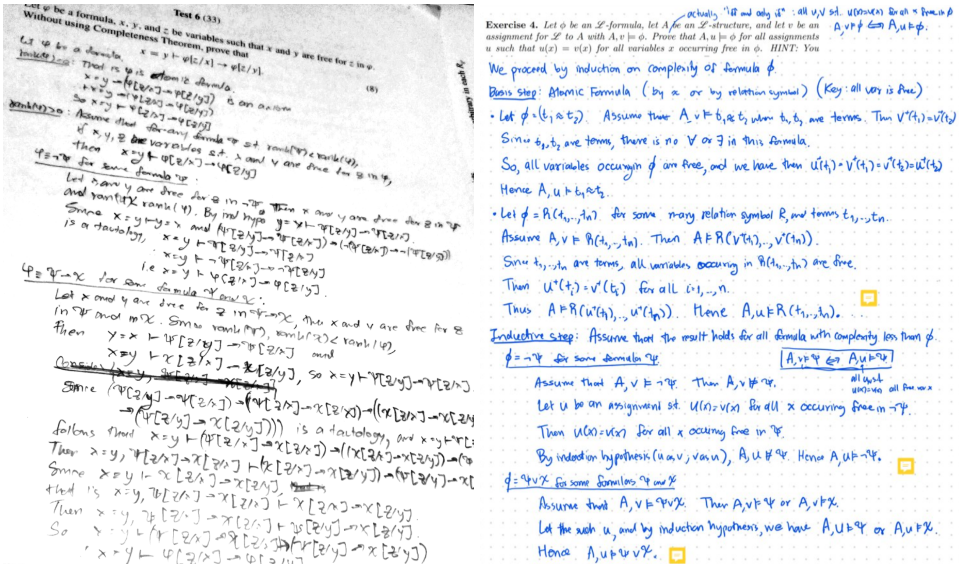
$$w = (w_i)_{i\in V} \oplus (w_{ij})_{\{i,j\}\in E(G)}.$$

Under the boundedness assumptions, $\|w\|_2 \leq B$ for some B and $\|\phi_G(x)\|_2 \leq R'\sqrt{|V| + |E(G)|}$ for some R'. Standard results on the Rademacher complexity of linear function classes then give

$$\mathcal{R}_n(\mathcal{F}_G) \leq \frac{BR'}{\sqrt{n}}\sqrt{|V| + |E(G)|},$$

as desired. A complete proof would specify the constants and the exact inequalities used. □

(2) วิชา AI: ข้อสอบ/การบ้านหัวข้อ First Order Logic ป.ตรี / ป.โท



Test 6 (33)

Let ϕ be a formula, x, y, and z be variables such that x and y are free for z in ϕ. Without using Completeness Theorem, prove that

$$x = y \vdash \phi[z/x] \to \phi[z/y]$$

(8)

Exercise 4. *Let ϕ be an $\mathcal{L}$-formula, let A be an $\mathcal{L}$-structure, and let v be an assignment for $\mathcal{L}$ to A with $A, v \models \phi$. Prove that $A, u \models \phi$ for all assignments u such that $u(x) = v(x)$ for all variables x occurring free in ϕ. HINT: You*

We proceed by induction on complexity of formula ϕ

Basis step: Atomic Formula (by $\approx$ or by relation symbol) (Key: all vars is free)

- Let $\phi = (t_1 \approx t_2)$. Assume that $A, v \models t_1 \approx t_2$ where t_1, t_2 are terms. Then $V^A(t_1) = V^A(t_2)$
  Since t_1, t_2 are terms, there is no $\forall$ or $\exists$ in this formula.
  So, all variables occurring in ϕ are free, and we have then $u^A(t_1) = v^A(t_1) = v^A(t_2) = u^A(t_2)$
  Hence $A, u \models t_1 \approx t_2$.
- Let $\phi = R(t_1, \ldots, t_n)$ for some n-ary relation symbol R, and terms $t_1, \ldots, t_n$.
  Assume $A, v \models R(t_1, \ldots, t_n)$. Then $A \models R(v^A(t_1), \ldots, v^A(t_n))$.
  Since $t_1, \ldots, t_n$ are terms, all variables occuring in $R(t_1, \ldots, t_n)$ are free.
  Then $u^A(t_i) = v^A(t_i)$ for all $i = 1, \ldots, n$.
  Thus $A \models R(u^A(t_1), \ldots, u^A(t_n))$. Hence $A, u \models R(t_1, \ldots, t_n)$.

Inductive step: Assume that the result holds for all formula with complexity less than ϕ.

$\phi = \neg\psi$ for some formula $\neg\psi$. $\boxed{A, v \models \neg\psi \iff A, u \models \neg\psi}$

Assume that $A, v \models \neg\psi$. Then $A, v \not\models \psi$.

Let u be an assignment st. $u(x) = v(x)$ for all x occuring free in $\neg\psi$.

Then $u(x) = v(x)$ for all x occuring free in ψ.

By induction hypothesis (u and v, v and u), $A, u \not\models \psi$. Hence $A, u \models \neg\psi$.

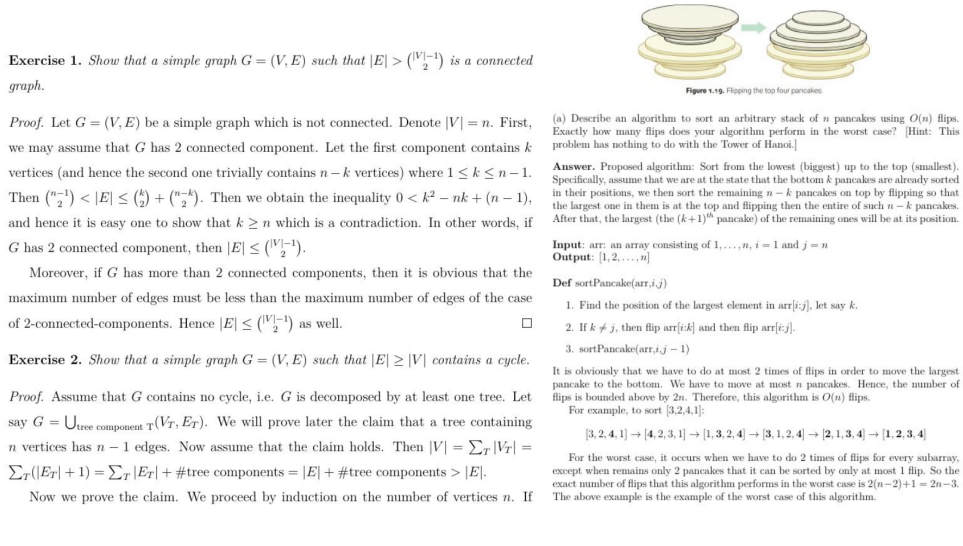
$\phi = \psi \vee \chi$ for some formulas ψ and χ

Assume that $A, v \models \psi \vee \chi$. Then $A, v \models \psi$ or $A, v \models \chi$.

Let the such u, and by induction hypothesis, we have $A, u \models \psi$ or $A, u \models \chi$.

Hence $A, u \models \psi \vee \chi$.

(3) การบ้านตอนผมเรียนวิชา algorithm



Exercise 1. *Show that a simple graph $G = (V, E)$ such that $|E| > \binom{|V|-1}{2}$ is a connected graph.*

Proof. Let $G = (V, E)$ be a simple graph which is not connected. Denote $|V| = n$. First, we may assume that G has 2 connected component. Let the first component contains k vertices (and hence the second one trivially contains $n-k$ vertices) where $1 \leq k \leq n-1$. Then $\binom{n-1}{2} < |E| \leq \binom{k}{2} + \binom{n-k}{2}$. Then we obtain the inequality $0 < k^2 - nk + (n-1)$, and hence it is easy one to show that $k \geq n$ which is a contradiction. In other words, if G has 2 connected component, then $|E| \leq \binom{|V|-1}{2}$.

Moreover, if G has more than 2 connected components, then it is obvious that the maximum number of edges must be less than the maximum number of edges of the case of 2-connected-components. Hence $|E| \leq \binom{|V|-1}{2}$ as well. □

Exercise 2. *Show that a simple graph $G = (V, E)$ such that $|E| \geq |V|$ contains a cycle.*

Proof. Assume that G contains no cycle, i.e. G is decomposed by at least one tree. Let say $G = \bigcup_{\text{tree component } T}(V_T, E_T)$. We will prove later the claim that a tree containing n vertices has $n-1$ edges. Now assume that the claim holds. Then $|V| = \sum_T |V_T| = \sum_T(|E_T| + 1) = \sum_T |E_T| + \#\text{tree components} = |E| + \#\text{tree components} > |E|$.

Now we prove the claim. We proceed by induction on the number of vertices n. If

Figure 1.19. Flipping the top four pancakes.

(a) Describe an algorithm to sort an arbitrary stack of n pancakes using $O(n)$ flips. Exactly how many flips does your algorithm perform in the worst case? [Hint: This problem has nothing to do with the Tower of Hanoi.]

Answer. Proposed algorithm: Sort from the lowest (biggest) up to the top (smallest). Specifically, assume that we are at the state that the bottom k pancakes are already sorted in their positions, we then sort the remaining $n-k$ pancakes on top by flipping so that the largest one in them is at the top and flipping then the entire of such $n-k$ pancakes. After that, the largest (the $(k+1)^{th}$ pancake) of the remaining ones will be at its position.

Input: arr: an array consisting of $1, \ldots, n$, $i = 1$ and $j = n$
Output: $[1, 2, \ldots, n]$

Def sortPancake(arr,i,j)

1. Find the position of the largest element in arr$[i:j]$, let say k.
2. If $k \neq j$, then flip arr$[i:k]$ and then flip arr$[i:j]$.
3. sortPancake(arr,i,$j-1$)

It is obviously that we have to do at most 2 times of flips in order to move the largest pancake to the bottom. We have to move at most n pancakes. Hence, the number of flips is bounded above by $2n$. Therefore, this algorithm is $O(n)$ flips.

For example, to sort [3,2,4,1]:

$$[3, 2, \mathbf{4}, 1] \to [\mathbf{4}, 2, 3, 1] \to [1, \mathbf{3}, 2, \mathbf{4}] \to [\mathbf{3}, 1, 2, \mathbf{4}] \to [\mathbf{2}, 1, \mathbf{3}, \mathbf{4}] \to [\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}]$$

For the worst case, it occurs when we have to do 2 times of flips for every subarray, except when remains only 2 pancakes that it can be sorted by only at most 1 flip. So the exact number of flips that this algorithm performs in the worst case is $2(n-2)+1 = 2n-3$. The above example is the example of the worst case of this algorithm.

ข้อตกลงของรายวิชา

ข้อตกลงสำคัญ

- **ข้อตกลง:** $\mathbb{N} = \{0, 1, 2, \dots\}$ เรานับ 0 เป็นจำนวนนับ
- **ต้องระบุเอกภพ/โดเมน (universe/domain) ให้ชัดเจน** เมื่อเขียน "สำหรับทุก x" หรือ "ให้ n เป็นจำนวนเต็ม"

A. นิยาม + ตัวอย่างการพิสูจน์ต้นแบบ

นิยาม: ประพจน์ (Proposition)

Definition 1. **ประพจน์** คือประโยคที่มีค่าความจริงแน่นอนว่า **จริง** หรือ **เท็จ** (แต่ไม่เป็นทั้งสองอย่างพร้อมกัน)

นิยาม: Predicate / open sentence

Definition 2. **Predicate** คือประโยคที่มีตัวแปร (เช่น $P(n)$) ซึ่งจะกลายเป็นประพจน์ได้ก็ต่อเมื่อ เรากำหนดค่าตัวแปร หรือใส่ตัวบ่งปริมาณ (เช่น "สำหรับทุก $n \in \mathbb{Z}$")

นิยาม: การพิสูจน์ (มุมมองของรายวิชา)

Definition 3. **การพิสูจน์** คือชุดของบรรทัดข้อความที่เรียงต่อกัน โดยแต่ละบรรทัดต้องมีเหตุผลรองรับ เช่น มาจากนิยาม ข้อเท็จจริงที่พิสูจน์แล้ว หรือการอ้างตรรกะที่ถูกต้อง และต้อง **ตรวจสอบได้** ว่าแต่ละบรรทัดตามมาจากอะไร

แบบฝึกหัด: เป็นประพจน์หรือไม่?

ทำเครื่องหมายว่า "เป็นประพจน์หรือไม่" ถ้าเป็นประพจน์ให้ทำเครื่องหมายว่า "จริง/เท็จ" ด้วย

(A1) $2 + 3 = 5$ เป็นประพจน์? ☐ใช่ ☐ไม่ใช่ จริง/เท็จ? ☐ T ☐ F

(A2) "กรุงเทพฯเป็นเมืองหลวงของประเทศไทย" เป็นประพจน์? ☐ใช่ ☐ไม่ใช่ จริง/เท็จ? ☐ T ☐ F

(A3) $x^2 - 3x + 2 = 0$ เป็นประพจน์? ☐ใช่ ☐ไม่ใช่ จริง/เท็จ? ☐ T ☐ F

(A4) "กรุณาปิดประตู" เป็นประพจน์? ☐ใช่ ☐ไม่ใช่ จริง/เท็จ? ☐ T ☐ F

(A5) "n เป็นจำนวนเฉพาะ" เป็นประพจน์? ☐ใช่ ☐ไม่ใช่ จริง/เท็จ? ☐ T ☐ F

คำถามเพิ่ม: สำหรับข้อความที่ไม่ใช่ประพจน์ เราทำอย่างไรได้บ้างให้กลายเป็นประพจน์
(2 แนวคิด: (1) กล่าวถึง 1 ตัวอย่าง และ (2) กล่าวถึงกลุ่มของหลายตัวอย่าง (จำกัดตัว / มีไม่จำกัดตัว))

นิยาม: จำนวนคู่/จำนวนคี่ในจำนวนเต็ม

Definition 4. ให้ $n \in \mathbb{Z}$

$$\begin{aligned} n \text{ เป็นจำนวนคู่} &\iff \exists k \in \mathbb{Z} : \ n = 2k, \\ n \text{ เป็นจำนวนคี่} &\iff \exists k \in \mathbb{Z} : \ n = 2k + 1. \end{aligned}$$

วิธีการใช้นิยามที่มีตัวบ่งปริมาณ there exist ($\exists$)

วันนี้ให้ใช้วิธีจำ pattern การอ้างเหตุผลไปก่อนนะครับ ครั้งที่ 2 และ 3 เราจะมาทำความเข้าใจการพิสูจน์แบบต่าง ๆ กันโดยละเอียด (อาจารย์จะสมมติว่าผู้เรียนทุกคนมีความรู้วิชาตรรกศาสตร์เบื้องต้นตอน ม.ปลาย กันมาแล้ว แต่ถ้าใครยัง แนะนำให้ไป self-learning เตรียมตัวมาก่อน)

ทฤษฎีบทตัวอย่าง: โครงสร้างพิสูจน์ที่ควรเลียนแบบ

Theorem 5. สำหรับทุกจำนวนเต็ม n ถ้า n เป็นจำนวนคี่ แล้ว n^2 เป็นจำนวนคี่

Proof idea. ใช้นิยามของ "จำนวนคี่": ถ้า n คี่ แปลว่ามี $k \in \mathbb{Z}$ บางตัวที่ทำให้ $n = 2k + 1$ จากนั้นทำ n^2 ให้อยู่ในรูป $2(\dots) + 1$ เพื่อสรุปว่าเป็นคี่ตามนิยาม

Proof. ให้ $n \in \mathbb{Z}$ และสมมติว่า n เป็นจำนวนคี่ ตามนิยามของจำนวนคี่ จะมี $k \in \mathbb{Z}$ ที่ทำให้ $n = 2k + 1$ ดังนั้น

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

ให้ $m = 2k^2 + 2k$ ซึ่งเป็นจำนวนเต็ม จะได้ $n^2 = 2m + 1$ จึงสรุปว่า n^2 เป็นจำนวนคี่ตามนิยาม $\square$

แบบฝึกหัดอ่านพิสูจน์: ในพิสูจน์ข้างบน ให้ชี้

1. จุดที่เป็นการระบุเอกภพสัมพัทธ์
2. จุดที่เป็น "สมมติฐาน" (assumption)
3. จุดที่เรา "อ้างถึงนิยาม"
4. จุดที่เรา "เลือกพยาน" (witness) ของ $\exists$ (ตัวบ่งปริมาณการมีอยู่)

B. คลินิกพิสูจน์: ดีบักพิสูจน์ที่ผิด

กติกา (สำคัญมาก)

เมื่อบอกว่า "ผิด" ต้องชี้ให้ได้ว่า **บรรทัดแรกที่ผิดกฎคือบรรทัดไหน** และ**ผิดเพราะอะไร** (การระบุเหตุผลที่ผิดได้สำคัญกว่าระบุจุดที่ผิด)

พิสูจน์ที่ผิด #1

Claim 6. ถ้า n^2 เป็นจำนวนคู่ แล้ว n เป็นจำนวนคู่ $\quad (n \in \mathbb{Z})$

พิสูจน์ของนักศึกษา (มีข้อผิดพลาด):

1. สมมติว่า n^2 เป็นจำนวนคู่
2. ดังนั้น $n^2 = 2k$ สำหรับจำนวนเต็ม k บางตัว
3. จึงได้ $n = \sqrt{2k}$
4. ซึ่งจะได้ว่า $n = 2\sqrt{\frac{k}{2}}$
5. เลือก $m = \sqrt{\frac{k}{2}}$ ดังนั้น n เป็นจำนวนคู่

Exercise 7 (หาบรรทัดแรกที่ผิดกฎ).

(B1) วงกลม **บรรทัดแรก** ที่ไม่สามารถให้เหตุผลได้ (จริง ๆ มีผิดหลายที่)

(B2) อธิบายว่า **ทำไม** จึงผิด

(B3) แนวทางแก้:

- พิสูจน์แบบ **ปฏิเสธสลับเงื่อนไข** (contrapositive): ถ้า n เป็นคี่ แล้ว n^2 เป็นคี่
- ใช้เหตุผลเรื่อง "ถ้า n คี่ $\Rightarrow n = 2k + 1$" แล้วคูณ/ยกกำลังสอง

ลองเขียนพิสูจน์ (ใช้การอ้างทฤษฎีที่พิสูจน์มาแล้วได้)

พิสูจน์ที่ผิด #2 (โดเมนไม่ชัด / ขาดพยาน)

Claim 8. สำหรับทุกจำนวน x ถ้า x เป็นจำนวนคี่ แล้ว $x + 1$ เป็นจำนวนคู่

Exercise 9 (แก้ "ข้อความ" ก่อนแก้ "พิสูจน์").

(B5) ข้อความข้างบนคลุมเครือ เพราะคำว่า "จำนวน" หมายถึงอะไร? ควรอยู่ในโดเมนไหน ($\mathbb{Z}$? $\mathbb{R}$? $\mathbb{N}$?)
ข้อความที่แก้แล้ว:

(B6) จากนั้นเขียนพิสูจน์ที่ถูกต้องโดยใช้นิยามจำนวนคี่/คู่

C. Activity: ลองเขียนพิสูจน์ด้วยตนเองด้วยการเลียนแบบตัวอย่าง

แบบฝึกหัด: เติมโครงร่างพิสูจน์

Exercise 10. Claim. สำหรับทุกจำนวนเต็ม n ถ้า n เป็นจำนวนคู่ แล้ว n^2 เป็นจำนวนคู่
Proof idea. :

Proof. ให้ $n \in \mathbb{Z}$ และสมมติว่า n เป็นจำนวนคู่
ตามนิยามของจำนวนคู่ จะมี _____ $\in \mathbb{Z}$ ที่ทำให้ $n =$ _____
ดังนั้น

$$n^2 = (_____)^2 = _____ = 2(_____)$$

จึงสรุปว่า n^2 เป็นจำนวนคู่ตามนิยาม □

ลองเขียนเอง: พิสูจน์ให้สะอาด ไม่มีขั้นกระโดด

ขั้นตอนทำงาน

(1) ร่างเดี่ยว 10 นาที ส่งใน assignment $\longrightarrow$ (2) อาจารย์เลือกแชร์ขึ้นจอแบบ blind ผู้ส่ง $\longrightarrow$ (3) ลองหาจุดผิด

Exercise 11. Claim. สำหรับทุกจำนวนเต็ม n ถ้า n หารด้วย 4 ลงตัว แล้ว n เป็นจำนวนคู่

Definition 12 (นิยามเพิ่มเติมประกอบการเขียนพิสูจน์).
จำนวนเต็ม n จะหารด้วย 4 ลงตัว ก็ต่อเมื่อ มีจำนวนเต็ม k ที่ทำให้ $n = 4k$

Proof idea. :

Proof. :

D. สรุปแพตเทิร์น + ล่าตัวอย่างโต้แย้ง + Exit Ticket

สรุปแพตเทิร์น (เก็บไว้ใช้ทุกสัปดาห์)

(1) การพิสูจน์อิมพลิเคชัน "ถ้า P แล้ว Q"

$$\text{สมมติ } P \longrightarrow \text{ใช้นิยาม/ข้อเท็จจริงที่รู้} \longrightarrow \text{สรุป } Q$$

(2) แกะนิยาม / ประกอบนิยาม
ตัวอย่าง:

$$n \text{ เป็นจำนวนคู่} \iff \exists k \in \mathbb{Z} : \ n = 2k.$$

แกะนิยาม = แทนคำว่า "เป็นจำนวนคู่" ด้วยรูป $\exists k \in \mathbb{Z} : n = 2k$ และ **เลือกพยาน** ให้ชัดเจน
ประกอบนิยาม = ทำให้ได้รูปตามนิยาม แล้วจึงสรุปสมบัตินั้น

ความหมายของ implication

ใจความสำคัญ (อ่านให้จบก่อนทำโจทย์)

$P \to Q$ แปลว่า ``**ทุกครั้งที่ P จริง จะต้องทำให้ Q จริงด้วย**''
พูดแบบโลกคอม: **ถ้าอินพุตอยู่ในเงื่อนไข P (precondition) แล้วผลลัพธ์ต้องเป็นไปตาม Q (postcondition)**

เมื่อไหร่ที่ $P \to Q$ เป็นเท็จ? (สำคัญมาก)

อิมพลิเคชัน $P \to Q$ **เป็นเท็จได้แค่กรณีเดียว** คือ

ดังนั้น **การหักล้าง** ข้อความรูป $P \to Q$ ทำได้โดย

ความจริงแบบ ``ว่าง'' (vacuous truth): ทำไมบางทีมันดูแปลก?

ถ้า P **เท็จ** แล้ว $P \to Q$ จะ **ถือว่าเป็นจริง** (ไม่ว่า Q จะจริงหรือเท็จ)
เพราะประโยคนี้ให้สัญญาเฉพาะ ``กรณีที่ P เกิดขึ้น'' เท่านั้น
ตัวอย่าง: ``ถ้า 1 เป็นจำนวนคู่ แล้ว $2 + 2 = 5$'' เป็น **จริงในเชิงตรรกะ** เพราะส่วนหน้า 1 เป็นคู่ **เท็จ**

เทียบกับการพิสูจน์ในห้องเรียน

เวลาเราพิสูจน์ $P \to Q$ เราทำตามแพตเทิร์นนี้:

สมมติ P $\longrightarrow$ **ใช้เหตุผล/นิยาม/ข้อเท็จจริง** $\longrightarrow$ **สรุป Q**

ข้อควรจำ: **การพิสูจน์ไม่ได้พยายามทำให้ P จริง** แต่พยายามแสดงว่า **ถ้าเกิด P ขึ้นจริง ๆ แล้ว Q ต้องตามมา**

คำพูดภาษาไทย/อังกฤษที่มักแปลเป็นสัญลักษณ์ผิด

ให้ P, Q เป็นประพจน์

- ``P **only if** Q'' $\equiv$ $P \to Q$
- ``P **if** Q'' $\equiv$ $Q \to P$
- ``Q **whenever** P'' $\equiv$ $P \to Q$

ทริกจำ: ``P only if Q'' = Q เป็น **เงื่อนไขจำเป็น** ของ P (ถ้าไม่มี Q ก็ห้ามมี P)

สมมูลที่ใช้บ่อย (ไว้ใช้สัปดาห์หน้า): contrapositive

$$P \to Q \quad \text{สมมูลกับ} \quad \neg Q \to \neg P$$

หลายครั้งพิสูจน์ $\neg Q \to \neg P$ ง่ายกว่า (เช่น เรื่องคู่/คี่)

แบบฝึกหัดสั้น (ทำในห้อง/ทำเองได้)

1. ให้ P = "n เป็นจำนวนคู่" และ Q = "n^2 เป็นจำนวนคู่"
   $P \to Q$ แปลว่าอะไร

2. ถ้าจะทำให้ $P \to Q$ **เป็นเท็จ** ต้องหา n แบบไหน?
   อธิบายเป็นรูป: ต้องทำให้ P _____ แต่ Q _____

3. พิจารณาประโยค: ``ถ้า n เป็นจำนวนคี่ แล้ว n หารด้วย 2 ลงตัว''
   เลือก $n = 2$ แล้วตอบว่า ประโยคนี้ ``จริงหรือเท็จ'' **สำหรับ** $n = 2$? เพราะอะไร?

4. ทำไม ``ผ่านทุก test case ที่เราลอง'' จึงยังไม่พอจะสรุปว่า $\forall$ input, (program ทำงานได้ถูกต้อง) ?

5. เราสามารถอธิบายคำกล่าวว่า "เครื่องมือที่ห่วย เอาไปใช้วัดผลอะไรไม่ได้เลย" ด้วย implication ได้อย่างไร

ล่าตัวอย่างโต้แย้ง (Counterexample) กรณีข้อความไม่จริง

จงปฏิเสธข้อความต่อไปนี้:

$$\textbf{(CE)} \quad \forall n \in \mathbb{Z},\ (n^2 \text{ เป็นจำนวนคู่}) \to (n \text{ หารด้วย } 4 \text{ ลงตัว})$$

Exercise 13 (หาตัวอย่างโต้แย้ง). เลือก $n =$ _____ คำนวณ $n^2 =$ _____
อธิบาย 1 ประโยคว่าทำไม n นี้จึงทำให้ (CE) เป็นเท็จ

Exit Ticket (2 นาที)

เป้าหมายการเรียนรู้ของเอกสารประกอบนี้

1. ✓ แยกให้ได้ว่าประโยคใดเป็น **ประพจน์**
2. ✓ แยกบทบาท **สิ่งที่อ้าง** (claim) ออกจาก **เหตุผล/การอ้างอิง** (reason/justification)
3. ✓ ใช้โครงร่างการพิสูจน์มาตรฐาน: **ข้อกล่าวอ้าง** $\rightarrow$ **แนวคิด** $\rightarrow$ **พิสูจน์** $\rightarrow$ **QED**
4. ✓ เขียนการพิสูจน์ "ถ้า...แล้ว..." แบบสั้น ๆ ด้วยโครงตัวอย่างโดย **แกะนิยาม** แล้วใช้ให้ถูกต้อง
5. ✓ ตรวจข้อผิดพลาดในบทพิสูจน์: หา **จุดที่ผิดกฎ** พร้อมระบุเหตุผลได้และแก้ไขให้ถูก
6. ✓ สร้างนิสัย "ลองคิดแย้งดูก่อน" เพื่อปฏิเสธข้อความแบบ **สำหรับทุก...** ด้วย **ตัวอย่างค้าน** (counterexample)

(1) **ประพจน์** ต่างจาก **เพรดิเคต/ประโยคเปิด** อย่างไร?

(2) สิ่งใดบ้างที่เราสามารถใช้ในการอ้างเหตุผลในการเขียนพิสูจน์

(3) ในการพิสูจน์ "ถ้า P แล้ว Q" เรา **สมมติอะไร** ตอนเริ่ม และต้อง **สรุปอะไร** ตอนจบ?

(4) อะไรทำให้ "หนึ่งบรรทัด" ในพิสูจน์ **ถูกกฎ/ตรวจสอบได้**? ยกตัวอย่างเหตุผลที่ยอมรับได้ 1 อย่าง

การบ้าน (สัปดาห์ที่ 1)

คำสั่งสำคัญ และใช้กับทุกการบ้านและข้อสอบ: รับงานที่เขียนด้วยลายมือเท่านั้น (จะเขียนในกระดาษแล้วถ่ายรูปแล้วทำเป็น pdf หรือจะเขียนใน tablet ก็ได้ แต่ขอเป็นไฟล์ pdf 1 ไฟล์เท่านั้น)

งานเขียนเชิงเหตุผล (เน้น "ตรวจสอบได้")

1. พิสูจน์ว่า สำหรับทุกจำนวนเต็ม a, b ถ้า a และ b เป็นจำนวนคู่ แล้ว $a + b$ เป็นจำนวนคู่
   (เกณฑ์สำคัญ: ต้องใช้นิยามจำนวนคู่ และระบุพยานให้ชัดเจน)

2. จงยกตัวอย่างโต้แย้งให้แต่ละข้อความต่อไปนี้ และเขียนอธิบาย 1 ประโยคว่าทำไมใช้ได้

   (a) $\forall n \in \mathbb{Z},\ (n \text{ เป็นจำนวนคี่}) \to (n \text{ หารด้วย } 3 \text{ ลงตัว})$

   (b) $\forall p \in \mathbb{Z},\ (p \text{ เป็นจำนวนเฉพาะ}) \to (p \text{ เป็นจำนวนคี่})$

3. ข้อผิดพลาดของบทพิสูจน์ด้านล่างเกี่ยวข้องกับการพูดถึงตัวบ่งปริมาณ for all "สำหรับ...ใด ๆ" แต่ขั้นตอนการให้เหตุผลถูกแล้ว จงบอกสาเหตุที่ผิด พร้อมกับแก้ไขให้ถูกต้อง
   "สำหรับจำนวนเต็ม n ใด ๆ ถ้า n เป็นจำนวนคู่ แล้ว n^2 จะเป็นจำนวนคู่"

   พิสูจน์. สำหรับจำนวนเต็ม n ใด ๆ จะได้ว่า จะมีจำนวนเต็ม k ที่ทำให้ $n = 2k$
   เพราะฉะนั้น สำหรับจำนวนคู่ n ใด ๆ และจำนวนเต็ม k ใด ๆ จะได้ว่า

   $$\begin{aligned} n^2 &= (2k)^2 \\ &= 4k^2 \\ &= 2(2k^2) \end{aligned}$$

   ดังนั้น สำหรับจำนวนเต็ม m ใด ๆ ที่ $m = 2k^2$ จะได้ว่า $n^2 = 2m$
   เพราะฉะนั้น สำหรับจำนวนเต็มคู่ n และจำนวนเต็ม m ใด ๆ จะได้ว่า $n^2 = 2m$ จึงได้ว่า n^2 เป็นจำนวนคู่ $\square$