Mathematics for Computer Science

Prof. dr.hab. Viorel Bostan

Technical University of Moldova

viorel.bostan@adm.utm.md

Lecture 4


WEB-АГЕНТСТВО “АШОТ”+
ТАКОЙ ДИДЖИТОВКА ДЕЛАЕМ, БРАТ,
КАЙФУЕШ!*
+7 (495) 730-74-79 (СПРОСИТЬ РУДИКА)
*РОЛИК-ШМОЛИК ТОЖЕ УМЕЕМ

Logic Problem

I am going to give you a problem.

If you have heard this problem before and know its solution, recognize it honestly.

The person who answers correctly, receives a bonus point!

PROBLEM. There is an island, divided in two halves.

People living on one half, are always telling the truth, while people on the other half are pathological liars, so they are always lying.

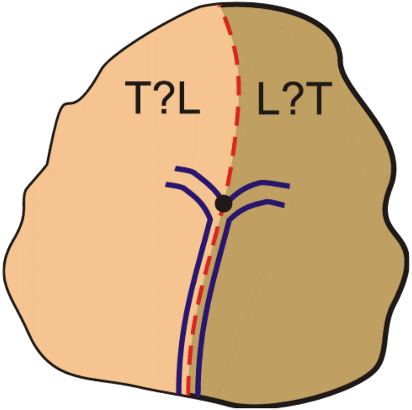
Truth-tellers and liars are never visiting the other half of the island.

Let us suppose that people on the island are answering to any question by only "YES" or "NO".

A road goes exactly through the middle of our strange island and a man sits at the road intersection.

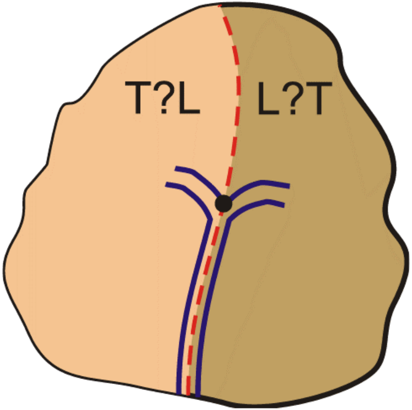
Suppose you are a postman, who have to deliver a letter to say John truth-teller.

Logic Problem



What question (only one) should you ask the man sitting at the intersection, in order to determine where you should go, to the left or to the right?

Logic Problem



Last Lecture Summary

- Proving implications $P \Rightarrow Q$:
  - directly;
  - by contrapositive;
  - by contradiction;
  - by cases.
- Proving Iff, $P \Leftrightarrow Q$.
- Do not reason backwards!
- Formalizing propositional logic:
  - Language $\mathcal{L}_P$;
  - Logic formula;
  - Set of sub-formulas;
  - Precedence rules;
- Truth assignment and Truth tables;
- Tautology and Contradiction.

Logical deductions

Logical deductions or **inference rules** are used to combine axioms and true propositions to construct more true propositions.

Definition

A set of formulas Σ implies formula φ, if every truth assignment which satisfies Σ, also satisfies φ. It is written as $\Sigma \models \varphi$ or $\dfrac{\Sigma}{\varphi}$.

Example.
Consider inference rule
$\{\alpha, \alpha \to \beta\} \models \beta$

or

$$\frac{\alpha, \alpha \to \beta}{\beta}$$

Indeed, the truth table for $\alpha \to \beta$ is

α	β	$\alpha \to \beta$
T	T	T
T	F	F
F	T	T
F	F	T

Logical deductions

Logical deductions or **inference rules** are used to combine axioms and true propositions to construct more true propositions.

Definition

A set of formulas Σ implies formula φ, if every truth assignment which satisfies Σ, also satisfies φ. It is written as $\Sigma \models \varphi$ or $\dfrac{\Sigma}{\varphi}$.

Example.
Consider inference rule
$\{\alpha, \alpha \to \beta\} \models \beta$

or

$$\frac{\alpha, \alpha \to \beta}{\beta}$$

Indeed, the truth table for $\alpha \to \beta$ is

α	β	$\alpha \to \beta$
T	T	T
T	F	F
F	T	T
F	F	T

Logical deductions

Logical deductions or **inference rules** are used to combine axioms and true propositions to construct more true propositions.

Definition

A set of formulas Σ implies formula φ, if every truth assignment which satisfies Σ, also satisfies φ. It is written as $\Sigma \models \varphi$ or $\dfrac{\Sigma}{\varphi}$.

Example.
Consider inference rule
$\{\alpha, \alpha \to \beta\} \models \beta$

or

$$\frac{\alpha, \alpha \to \beta}{\beta}$$

Indeed, the truth table for $\alpha \to \beta$ is

α	β	$\alpha \to \beta$
T	T	T
T	F	F
F	T	T
F	F	T

Inference rules: Modus Ponens

Modus Ponens

$$\frac{\alpha,\ \alpha \to \beta}{\beta}$$

Example

$\alpha =$"Today is Wednesday"
$\beta =$"We have Discrete Math class"
$\alpha \to \beta =$"If it is Wednesday, then we have Discrete Math class".

In this case Modus Ponens means:
α is true,
and $\alpha \to \beta$ is true,
implies β is also true.

Inference rules: Modus Tollens

Modus Tollens

$$\frac{\alpha \to \beta,\ \neg\beta}{\neg\alpha}$$

If from α follows β, and β is false, then α is false too.

α	β	$\neg\alpha$	$\neg\beta$	$\alpha \to \beta$
T	T	F	F	T
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

Inference rules: Modus Tollens

Modus Tollens

$$\frac{\alpha \rightarrow \beta,\ \neg\beta}{\neg\alpha}$$

If from α follows β, and β is false, then α is false too.

α	β	$\neg\alpha$	$\neg\beta$	$\alpha \rightarrow \beta$
T	T	F	F	T
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

Modus Tollens

$$\frac{\alpha \to \beta,\ \neg\beta}{\neg\alpha}$$

If from α follows β, and β is false, then α is false too.

α	β	$\neg\alpha$	$\neg\beta$	$\alpha \to \beta$
T	T	F	F	T
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

Consider the truth table for $\oplus$ symbol, called also **exclusive or**:

α	β	$\alpha \oplus \beta$
T	T	F
T	F	T
F	T	T
F	F	F

Modus Ponendo-Tollens

$$\frac{\alpha \oplus \beta,\ \alpha}{\neg\beta}\ , \qquad \frac{\alpha \oplus \beta,\ \beta}{\neg\alpha}$$

If (exactly one) either α or β is true, and one of them is true, then the other one is false.

Inference rules

Modus Tollen-Ponens

$$\frac{\alpha \oplus \beta,\ \neg\alpha}{\beta}, \quad \frac{\alpha \oplus \beta,\ \neg\beta}{\alpha}, \quad \frac{\alpha \vee \beta,\ \neg\alpha}{\beta}, \quad \frac{\alpha \vee \beta,\ \neg\beta}{\alpha}.$$

Transitivity Rule

$$\frac{\alpha \to \beta,\ \beta \to \gamma}{\alpha \to \gamma}$$

Contradiction Rule

$$\frac{\alpha \to \beta,\ \alpha \to \neg\beta}{\neg\alpha}$$

Inference rules

Contrapositive Rule

$$\frac{\alpha \rightarrow \beta}{\neg\beta \rightarrow \neg\alpha}$$

Composed Contrapositive Rule

$$\frac{(\alpha \wedge \beta) \rightarrow \gamma}{(\alpha \wedge \neg\gamma) \rightarrow \neg\beta}$$

Section Rule

$$\frac{\alpha \rightarrow \beta,\ (\beta \wedge \gamma) \rightarrow \delta}{(\alpha \wedge \gamma) \rightarrow \delta}$$

Inference rules

Import Rule

$$\frac{\alpha \rightarrow (\beta \rightarrow \gamma)}{(\alpha \wedge \beta) \rightarrow \gamma}$$

Export Rule

$$\frac{(\alpha \wedge \beta) \rightarrow \gamma}{\alpha \rightarrow (\beta \rightarrow \gamma)}$$

Dilemma Rules

$$\frac{\alpha \rightarrow \gamma,\ \beta \rightarrow \gamma,\ \alpha \vee \beta}{\gamma}, \qquad \frac{\alpha \rightarrow \beta,\ \alpha \rightarrow \gamma,\ \neg\beta \vee \neg\gamma}{\neg\alpha}$$

Inference rules: Dilemma Rule

$$\frac{\alpha \to \gamma,\ \beta \to \gamma,\ \alpha \lor \beta}{\gamma}$$

$$\frac{\alpha \to \gamma,\ \beta \to \gamma,\ \alpha \lor \beta}{\gamma}$$

$$\frac{\alpha \to \gamma,\ \beta \to \gamma,\ \alpha \lor \beta}{\gamma}$$

α	β	γ	$\alpha \to \gamma$	$\beta \to \gamma$	$\alpha \lor \beta$
T	T	T	T	T	T
T	T	F	F	F	T
T	F	T	T	T	T
T	F	F	F	T	T
F	T	T	T	T	T
F	T	F	T	F	T

Logical Deductions

Logical deductions can be written as formulas (that are tautologies):

$$\frac{\alpha \to \beta,\ \alpha}{\beta} \quad \Rightarrow \quad ((\alpha \to \beta) \wedge \alpha) \to \beta$$

α	β	$\alpha \to \beta$	$(\alpha \to \beta) \wedge \alpha$	$((\alpha \to \beta) \wedge \alpha) \to \beta$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Basically, you need to connect the formulas from Σ with conjunction $\wedge$ and then connect them using implication $\to$ with φ.

In other words $\dfrac{\Sigma}{\varphi} \quad \Rightarrow \quad (\Sigma) \to \varphi.$

Examples of wrong logical deductions

$$\frac{\alpha \to \beta,\ \beta}{\alpha}$$

$$\frac{\alpha \to \beta,\ \neg\alpha}{\neg\beta}$$

$$\frac{\alpha \lor \beta,\ \alpha}{\alpha}$$

Soap opera deduction

If Mariana is not the daughter of Don Pedro, then either Jose Ignacio is Mariana's father, or Luis Alberto is not her brother. If Luis Alberto is Mariana's brother, then Mariana is the don Pedro's daughter and Jose Ignacio is lying. If Jose Ignacio is lying then either Luis Alberto is not Mariana's brother, or Jose Ignacio is her father.
Therefore Mariana is the don Pedro's daughter.

Question: Is this logical deduction true?

Consider the following notations:

- $A =$ "Mariana is the daughter of Don Pedro";
- $B =$ "Luis Alberto is not Mariana's brother";
- $C =$ "Jose Ignacio is Mariana's father";
- $D =$ "Jose Ignacio is lying".

Soap opera deduction

- $A =$ "Mariana is the daughter of Don Pedro";
- $B =$ "Luis Alberto is not Mariana's brother";
- $C =$ "Jose Ignacio is Mariana's father";

  If Mariana is not the daughter of Don Pedro, then either Jose Ignacio is Mariana's father, or Luis Alberto is not her brother.

$$\Downarrow$$

$$(\neg A) \quad \rightarrow \quad (C \oplus B)$$

Soap opera deduction

- $A =$ "Mariana is the daughter of Don Pedro";
- $B =$ "Luis Alberto is not Mariana's brother";
- $D =$ "Jose Ignacio is lying".

  If Luis Alberto is Mariana's brother, then Mariana is the don Pedro's daughter and Jose Ignacio is lying.

$$\Downarrow$$

$$(\neg B) \quad \rightarrow \quad (A \wedge D)$$

Soap opera deduction

- $B =$ "Luis Alberto is not Mariana's brother";
- $C =$ "Jose Ignacio is Mariana's father";
- $D =$ "Jose Ignacio is lying".

  If Jose Ignacio is lying then either Luis Alberto is not Mariana's brother, or Jose Ignacio is her father.

$$\Downarrow$$

$$D \quad \rightarrow \quad (B \oplus C)$$

Soap opera deduction

Also, clearly, A and C can not be true simultaneously:

- $A =$ "Mariana is the daughter of Don Pedro";
- $C =$ "Jose Ignacio is Mariana's father".

Therefore,

$$A \oplus C$$

should be added to the list of fomulas.

Thus, our soap opera formula is

$$\underbrace{(\neg A \to (C \oplus B)) \land (\neg B \to (A \land D)) \land (D \to (B \oplus C)) \land (A \oplus C)}_{=K} \to A$$

Need to prove that this formula is true.

We will be using the Contradiction Rule:

$$\frac{\alpha \to G,\ \alpha \to \neg G}{\neg\alpha}$$

So, we will consider that our formula $K \to A$ is false.
Then, if we will be able to find a formula G such that $\alpha =$ "$K \to A$ is false" will imply that G is both false and true,
it will follow that $\neg\alpha$ is true,
in other words K should be true.

Soap opera deduction

$$\underbrace{(\neg A \to (C \oplus B)) \land (\neg B \to (A \land D)) \land (D \to (B \oplus C)) \land (A \oplus C)}_{=K} \to A$$

$$v(K \to A) = F$$

Recall the truth table for implication

α	β	$\alpha \to \beta$
T	T	T
T	F	F
F	T	T
F	F	T

Implication is false, only if the left side (i.e. K) is true. In this case, we will also have that the right side (i.e. A) is false:

$$v(A) = F \tag{G}$$

Soap opera deduction

Therefore,

$$v\left(\underbrace{(\neg A \to (C \oplus B)) \land (\neg B \to (A \land D)) \land (D \to (B \oplus C)) \land (A \oplus C)}_{=K}\right) = T$$

But a conjunction $I \land II \land III \land IV$ has a true value if and only if all its *factors* are having true value. Thus,

$$v\left(\neg A \to (C \oplus B)\right) = T \tag{1}$$

$$v\left(\neg B \to (A \land D)\right) = T \tag{2}$$

$$v\left(D \to (B \oplus C)\right) = T \tag{3}$$

$$v\left(A \oplus C\right) = T \tag{4}$$

Soap opera deduction

According to (G)

$$v(A) = F$$

Then formula

$$v\,(A \oplus C) = T \tag{4}$$

implies

$$v(C) = T \tag{5}$$

α	β	$\alpha \oplus \beta$
T	T	F
T	F	T
F	T	T
F	F	F

Soap opera deduction

According to (G)

$$v(A) = F$$

Then

$$v(\neg A) = T$$

and

$$v\left(\neg A \to (C \oplus B)\right) = T \tag{1}$$

if and only if

$$v\left(C \oplus B\right) = T \tag{6}$$

but since $v(C) = T$, we have

$$v(B) = F \tag{7}$$

Soap opera deduction

Since $v(B) = F$,

$$v(\neg B) = T$$

and

$$v\left(\neg B \to (A \wedge D)\right) = T \tag{2}$$

if and only if

$$v\left(A \wedge D\right) = T$$

which implies

$$v(A) = T$$

Soap opera deduction

In conclusion we supposed that $\alpha = "K \to A$ is false" implies both $G = "A$ is true", and $\neg G = "A$ is false".

By Contradiction Rule

$$\frac{\alpha \to G,\ \alpha \to \neg G}{\neg \alpha}$$

$v(\neg \alpha) = T$.

This means $\neg \alpha = "K \to A$ is true" has true value.

In other words $K \to A$.

Our formula is having true value.

So logical deduction from our soap opera is correct!

Predicate Logic

Up to this moment, we discussed the **Propositional Logic**, or so-called Zero-order Logic.

We need something more, since there are situations in which truthiness of a formula may depend on a variable.

Now, let's move to First-order Logic or **Predicate Logic**.

Definition

A predicate is a proposition whose truth depends on the value of one or more variables.

Example

"n **is a perfect square**" is a predicate whose truth depends on the value of n.

This predicate is true for $n = 4$, since 4 is a prefect square,
but it is false for $n = 8$, since 8 is not a perfect square.

Like other propositions, predicates are often named with a letter. Furthermore, a function-like notation is used to denote a predicate supplied with specific variable values.

For example, we might name our earlier predicate with letter P:

$$P(n) = \text{"}n\text{ is a perfect square"}$$

Now $P(4)$ is true, and $P(5)$ is false.

This notation for predicates is confusingly similar to ordinary function notation.

If P is a predicate, then $P(n)$ is either true or false, depending on the value of n.

On the other hand, if P is an ordinary function, like $n^2 + 1$, then $P(n)$ is a numerical quantity.

Don't confuse these two!

Quantifying a predicate

There are a couple kinds of assertion one commonly makes about a predicate: that it is **sometimes** true and that it is **always** true.

For example, the predicate

$$\text{“}x^2 \geqslant 0\text{”}$$

is always true when x is a real number.

On the other hand, the predicate

$$\text{“}5x^2 - 7 = 0\text{”}$$

is only sometimes true; specifically, when $x = \pm\sqrt{7/5}$.

There are several ways to express the notions of “ **always true**” and “**sometimes true** ” in English.

Quantifying a predicate

Always true

“For all n, $P(n)$ is true. ”

“$P(n)$ is true for every n. ”

“For all x, $x^2 \geq 0$.“

”$x^2 \geq 0$ for every x.”

Sometimes true

"There exists an n such that $P(n)$ is true."

"There exists an x such that $5x^2 - 7 = 0$ "

"$P(n)$ is true for some n ."

"$5x^2 - 7 = 0$ for some x ."

"$P(n)$is true for at least one n ."

Quantifying a predicate

There are symbols to represent **universal** and **existential** quantification, just as there are symbols for "and" ($\wedge$), "implies" ($\Longrightarrow, \rightarrow$), and so forth.

In particular, to say that a predicate $P(n)$ is true for all values of n in some set S, one writes:

$$\forall n \in S \quad P(n)$$

The symbol $\forall$ is read **"for all"**, so this whole expression is read "for all n in S, $P(n)$ is true". To say that a predicate $P(n)$ is true for at least one value of n in S, one writes:

$$\exists n \in S \quad P(n)$$

The backward E is read **"there exists"**. So this expression would be read, "There exists an n in S such that $P(n)$ is true.

Quantifying a predicate

All these sentences quantify how often the predicate is true.

Specifically,

- an assertion that a predicate is always true is called a universal quantification,
- an assertion that a predicate is sometimes true is an existential quantification.

Sometimes the English sentences are unclear with respect to quantification:

> "If you can solve any problem we come up with,
> then you get a 10 for the course."

Quantifying a predicate

The phrase "you can solve any problem we can come up with" could reasonably be interpreted as either a universal or existential quantification:

"you can solve **every** problem we come up with"

"you can solve **at least one** problem we come up with"

Let P be the set of problems and $S(x)$ be the predicate "You can solve problem x", and A be the proposition, "You get a 10 for the course."

Then the 2 different interpretations can be written as follows:

$$(\forall x \in P \quad S(x)) \Rightarrow A$$
$$(\exists x \in P \quad S(x)) \Rightarrow A$$

Mixing Quantifiers

Many mathematical statements involve several quantifiers. For example, Goldbach's Conjecture states:

"Every even integer greater than 2
is the sum of two primes."

Let's write this more verbosely to make the use of quantification more clear:

"For every even integer greater than 2,
there exist primes p and q such that $n = p + q$ "

Let E be the set of even integers greater than 2, and let P be the set of primes. Then we can write Goldbach's Conjecture in logic notation as follows:

$$\forall n \in E \; \exists p \in P \; \exists q \in P \quad n = p + q$$

Swapping the order of different kinds of quantifiers (existential or universal) changes the meaning of a proposition. For another example, let's return to one of our initial, confusing statements:

"Every person has a dream."

This sentence is ambiguous because the order of quantifiers is unclear. Let A be the set of people, let D be the set of dreams, and define the predicate $H(p, d)$ to be "A person p has dream d .". Now the sentence could mean there is a single dream that every person shares:

$$\exists d \in D \quad \forall p \in P \quad H(p, d)$$

Or it could mean that every person has an individual dream:

$$\forall p \in P \quad \exists d \in D \quad H(p, d)$$

Negating Quantifiers

There is a duality between the two kinds of quantifiers. The following two sentences mean the same thing:

"It is not the case that everyone likes to snowboard."

"There exists someone who does not like to snowboard."

In terms of logic notation, this follows from a general equivalence:

$$\neg \forall x \quad P(x)$$
$$\Updownarrow$$
$$\exists x \quad \neg P(x)$$

Negating Quantifiers

Similarly, these sentences mean the same thing:

> "There does not exist anyone who likes skiing over magma."
>
> "Everyone dislikes skiing over magma."

We can express the equivalence in logic notation this way:

$$\neg\exists x \quad Q(x)$$
$$\Updownarrow$$
$$\forall x \quad \neg Q(x)$$

The general principle is that moving a "not" across a quantifier changes the kind of quantifier.

Well Ordering Principle

Every **nonempty** set of **nonnegative integers** has a smallest element.

This principle looks very obvious, but note that it is very restrictive!

- It requires a **nonempty** set: it is false for empty set which does not have the smallest element because it has no elements at all;
- It requires a set of **nonnegative** integers: it is false for the set on negative integers;
- It requires a set of **integers**: is is false for nonnegative rationals.

WOP is used to prove statements that involve predicates on $\mathbb{N}$:

$$P(n) \text{ is true for all } n \in \mathbb{N}.$$

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}, \quad \forall n \in \mathbb{N}.$$

Well Ordering Principle

Need to prove that

$$P(n) \text{ is true for all } n \in \mathbb{N}.$$

using the Well Ordering Principle.

1. Define the set, C, of counterexamples to P being true. Namely, define

$$C = \{n \in \mathbb{N} \mid P(n) \text{ is false } \}$$

2. Use a proof by contradiction and assume that C is nonempty.
3. By the Well Ordering Principle, there will be a smallest element, $n \in C$.
4. Reach a contradiction (somehow) — often by showing how to use n to find another member of C that is smaller than n.
5. Conclude that C must be empty, that is, no counterexamples exist.

Well Ordering Principle

Theorem

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}, \quad \forall n \in \mathbb{N}. \tag{1}$$

Proof.

Proof by contradiction. Assume (1) is false.
It means that there are some numbers $n \in \mathbb{N}$ for which (1) is not true.
Collect them in the set of countrexamples:

$$C = \{n \in \mathbb{N} \mid 1 + 2 + 3 + \cdots + n \neq \frac{n(n+1)}{2}\}.$$

Set C is a nonempty set of nonnegative integers.
By WOP, set C has a minimum element.
Let that element be denoted c.
So, c is the smallest nonnegative number for which (1) is not true.

Well Ordering Principle

Theorem

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}, \quad \forall n \in \mathbb{N}. \tag{1}$$

Proof contd.

c is the smallest nonnegative number for which (1) is not true.
It follows that for number $c - 1$, identity (1) is true:

$$1 + 2 + 3 + \cdots + (c - 1) = \frac{(c-1)c}{2}.$$

Add to both sides of the last identity number c:

$$1 + 2 + 3 + \cdots + (c - 1) + c = \frac{(c-1)c}{2} + c.$$

Theorem

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}, \quad \forall n \in \mathbb{N}. \tag{1}$$

Proof contd.

$$\begin{aligned} 1 + 2 + 3 + \cdots + (c-1) + c &= \frac{(c-1)c}{2} + c \\ &= \frac{c^2 - c + 2c}{2} \\ &= \frac{c(c+1)}{2}, \end{aligned}$$

which means that for c, identity (1) also holds.

Contradiction! Therefore, the set C must be empty.

That is, identity (1) is true for any number $n \in \mathbb{N}$. $\square$

Lecture 4 Summary

- Inference Rules (Deductions);
- Predicate Logic:
- Notion of predicate;
- Universal quantifier $\forall$;
- Existential quantifier $\exists$;
- Order of quantifiers;
- Negating a quantifier;
- Well Ordering Principle.

Next lecture will start with a test.

Homework 2 is due ...

Theorem

The less you know, the more money you make.

Proof.

We know that (axioms)

1. Time is Money.
2. Knowledge is Power.

Therefore, mathematically speaking,

$$\text{Time} = \text{Money}, \tag{2}$$

$$\text{Knowledge} = \text{Power}. \tag{3}$$

Proof contd.

Also, from Physics we know that

$$\text{Power} = \frac{\text{Work}}{\text{Time}}. \tag{4}$$

By simple substitution of formulas (2) and (3) into expression (4) we get

$$\begin{aligned}
\text{Knowledge} &= \frac{\text{Work}}{\text{Money}}, \\
\text{Knowledge} \cdot \text{Money} &= \text{Work}, \\
\text{Money} &= \frac{\text{Work}}{\text{Knowledge}}.
\end{aligned}$$

It follows that as Knowledge goes to 0, Money goes to infinity. □