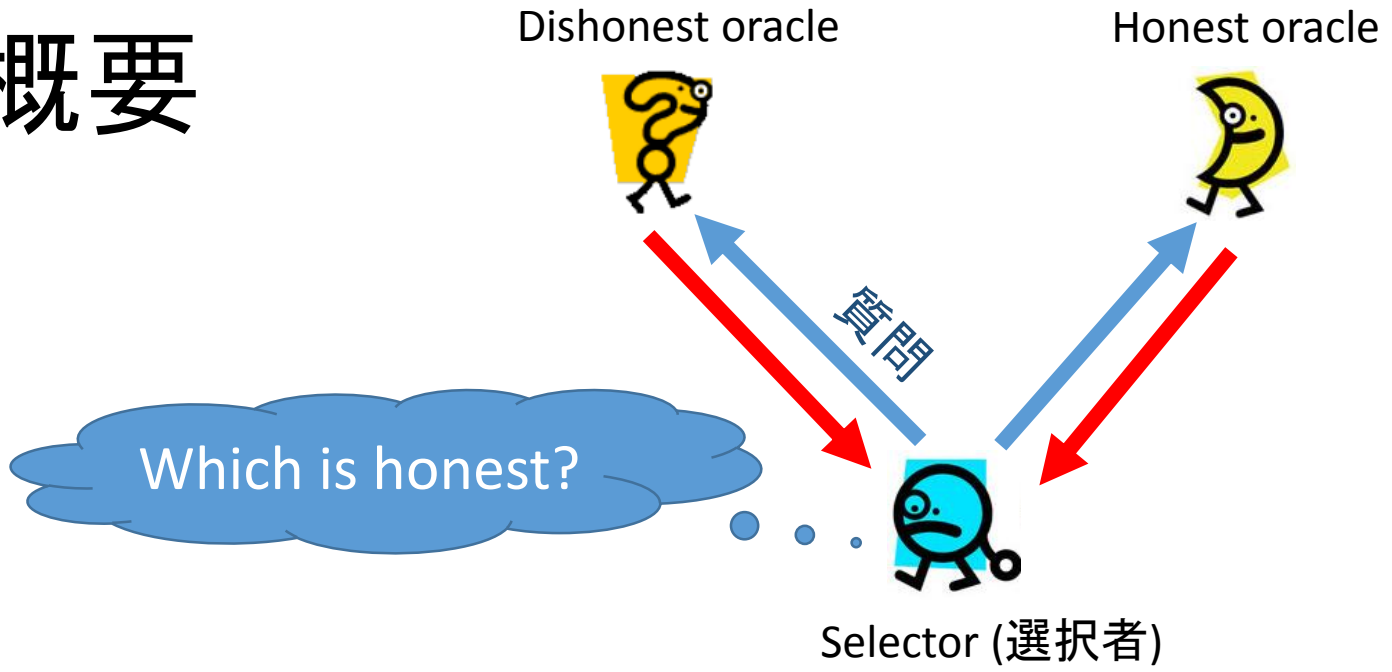
Identifying an Honest $\mathbf{EXP}^{\mathbf{NP}}$ Oracle Among Many (CCC'15)

平原　秀一

東京大学 修士課程2年
ERATOリサーチアシスタント

ERATO感謝祭 Season II 2015年8月4日

概要

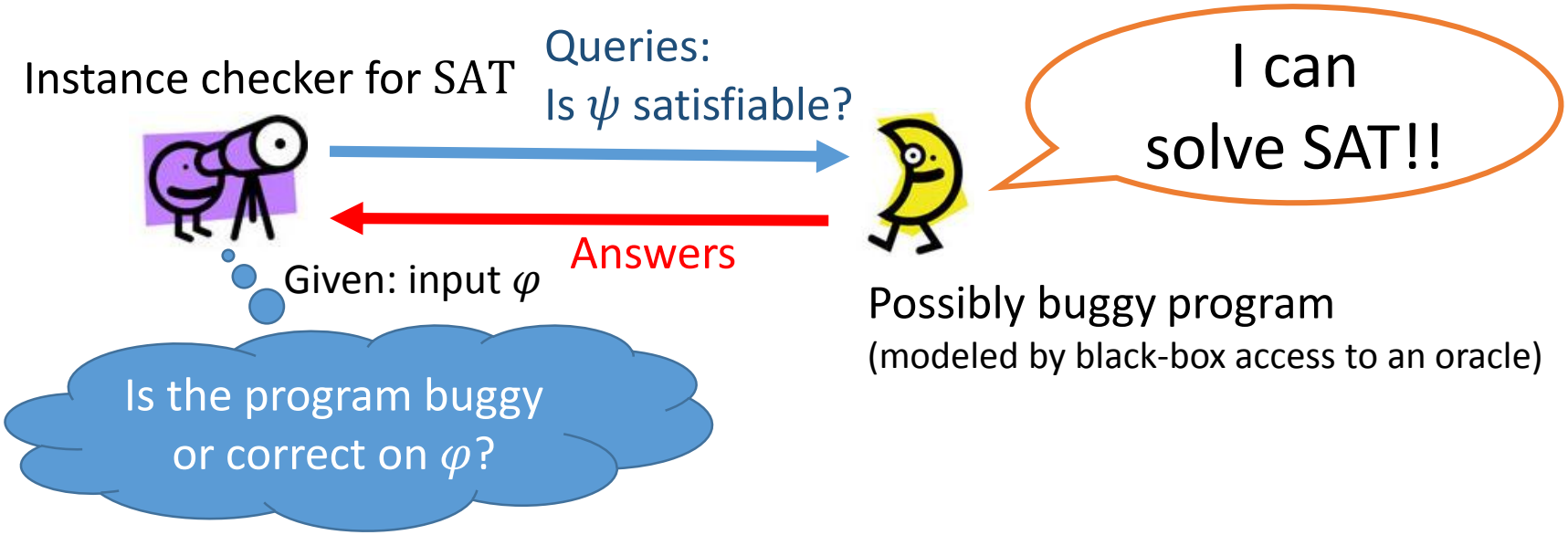


貢献ポイント

1. 選択者という概念を定式化した。
   - 選択者の存在 ⇔ 短いアドバイスの消去
2. $\mathrm{EXP}^{\mathrm{NP}}$完全問題に対する選択者の存在を示した。

背景: Instance checker [Blum & Kannan (1989)]

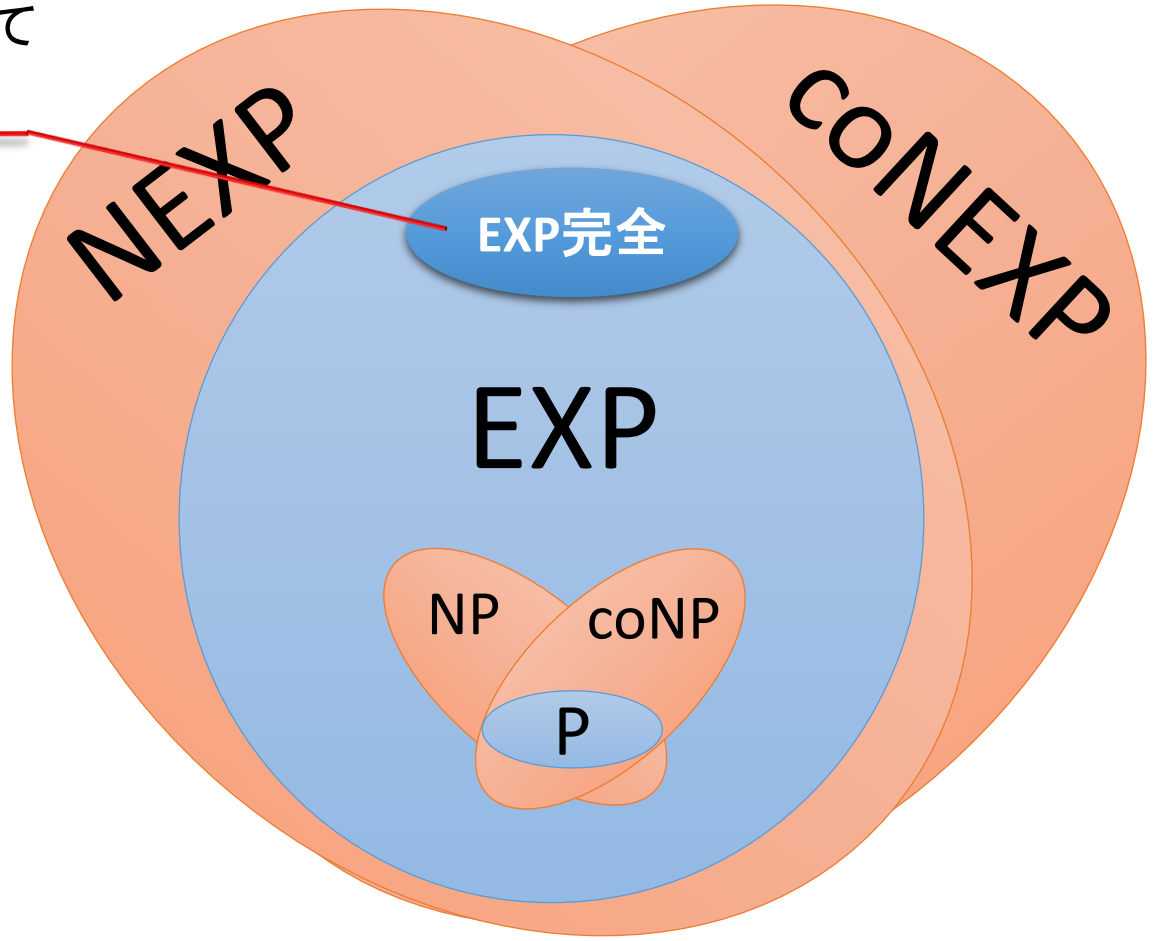
問題Lに対するInstance checker とは、多項式時間の乱択機械であって、与えられたプログラム が与えられたインスタンスφで正しく$L(\varphi)$を計算しているかを(低い誤り確率を許して) 判定するもの。



Instance checkerの存在について

指数時間完全問題に対して
Instance checkerが存在

[Babai, Fortnow & Lund (1991)]

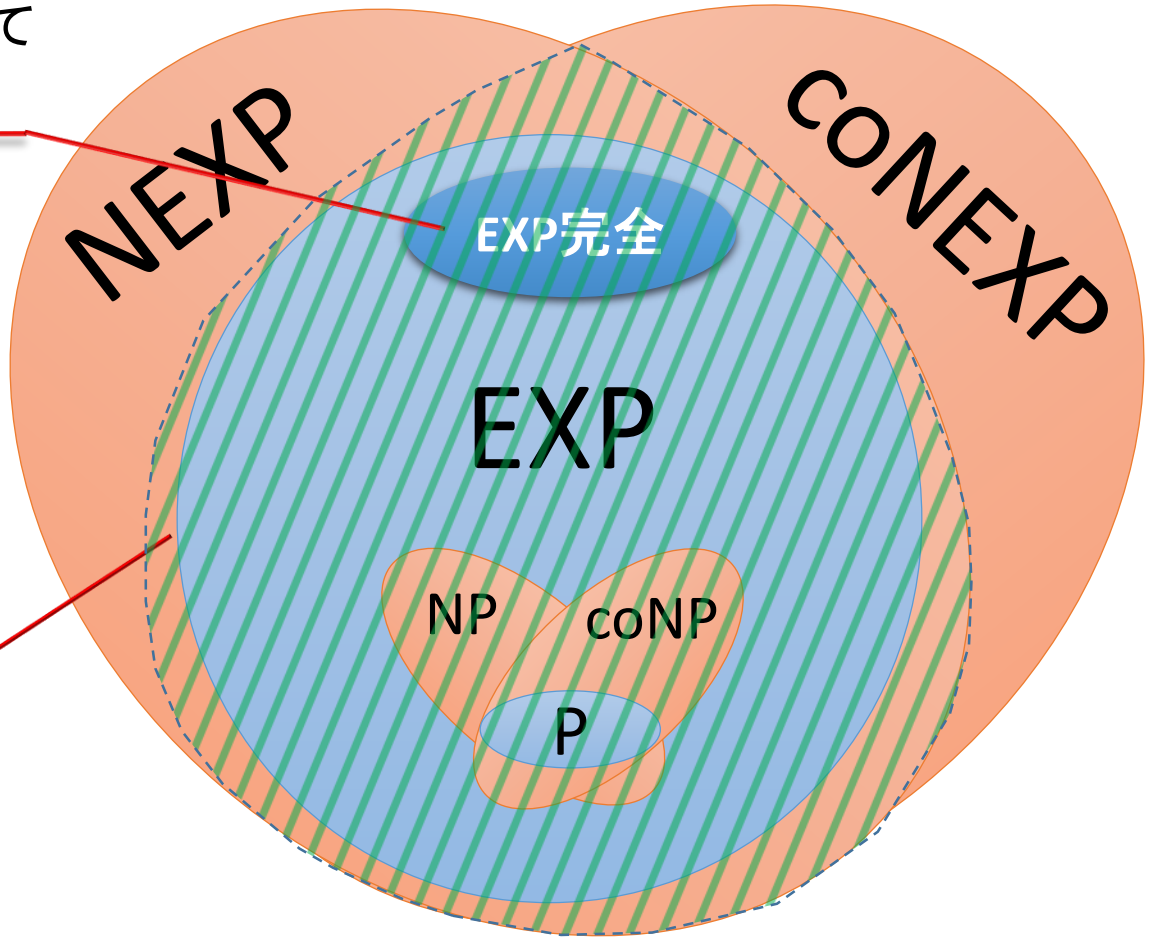


Instance checkerの存在について

指数時間完全問題に対して
Instance checkerが存在

[Babai, Fortnow & Lund (1991)]

Instance checkerは
NEXP ∩ coNEXPにのみ存在



(Probabilistic) Selector for SAT

Given:
1. An input φ, and
2. access to two oracles
   one of which is honest.

Task:

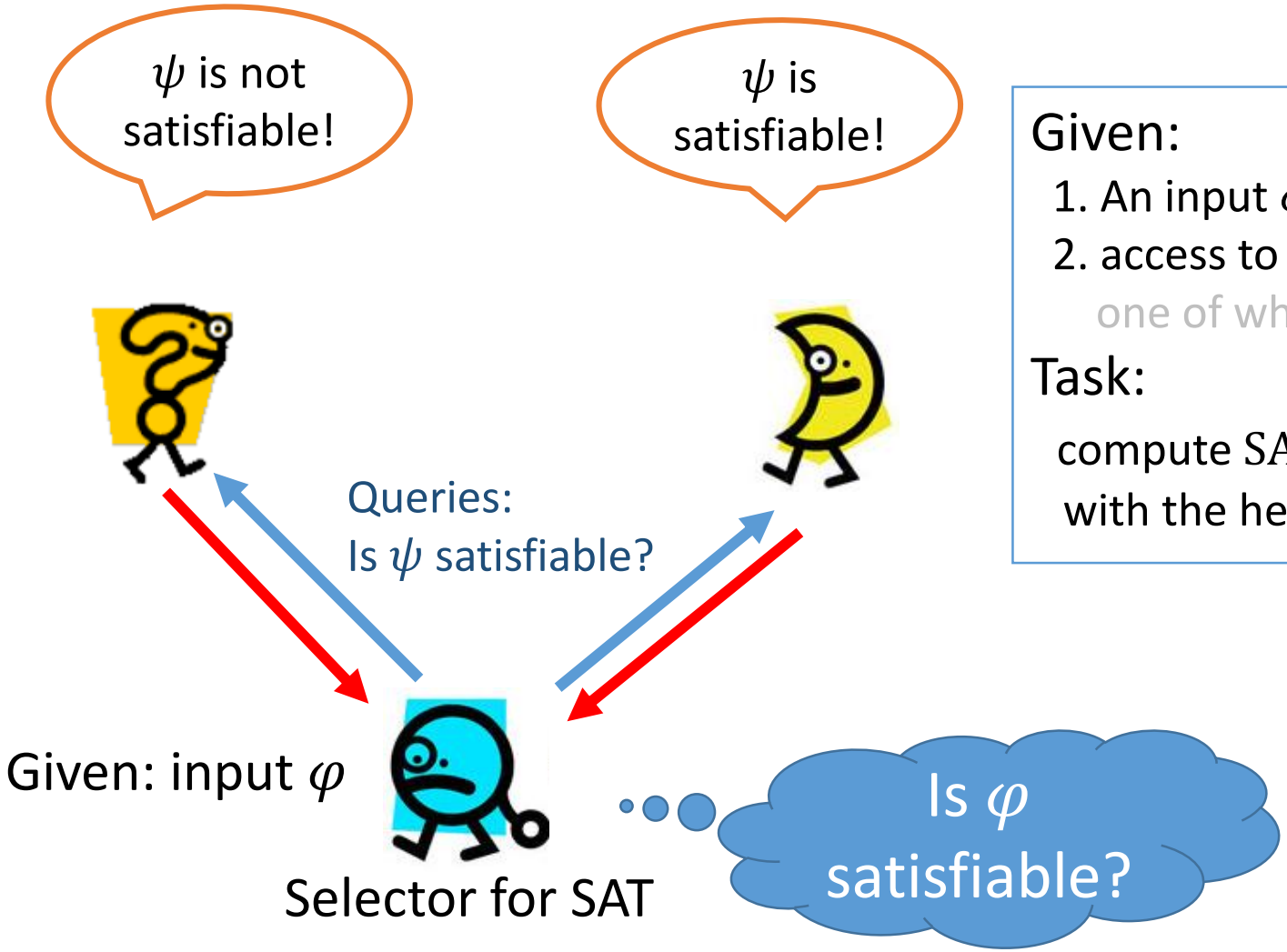
compute $\mathrm{SAT}(\varphi)$
with the help of the oracles

Given: input φ

Selector for SAT

Is φ satisfiable?

(Probabilistic) Selector for SAT



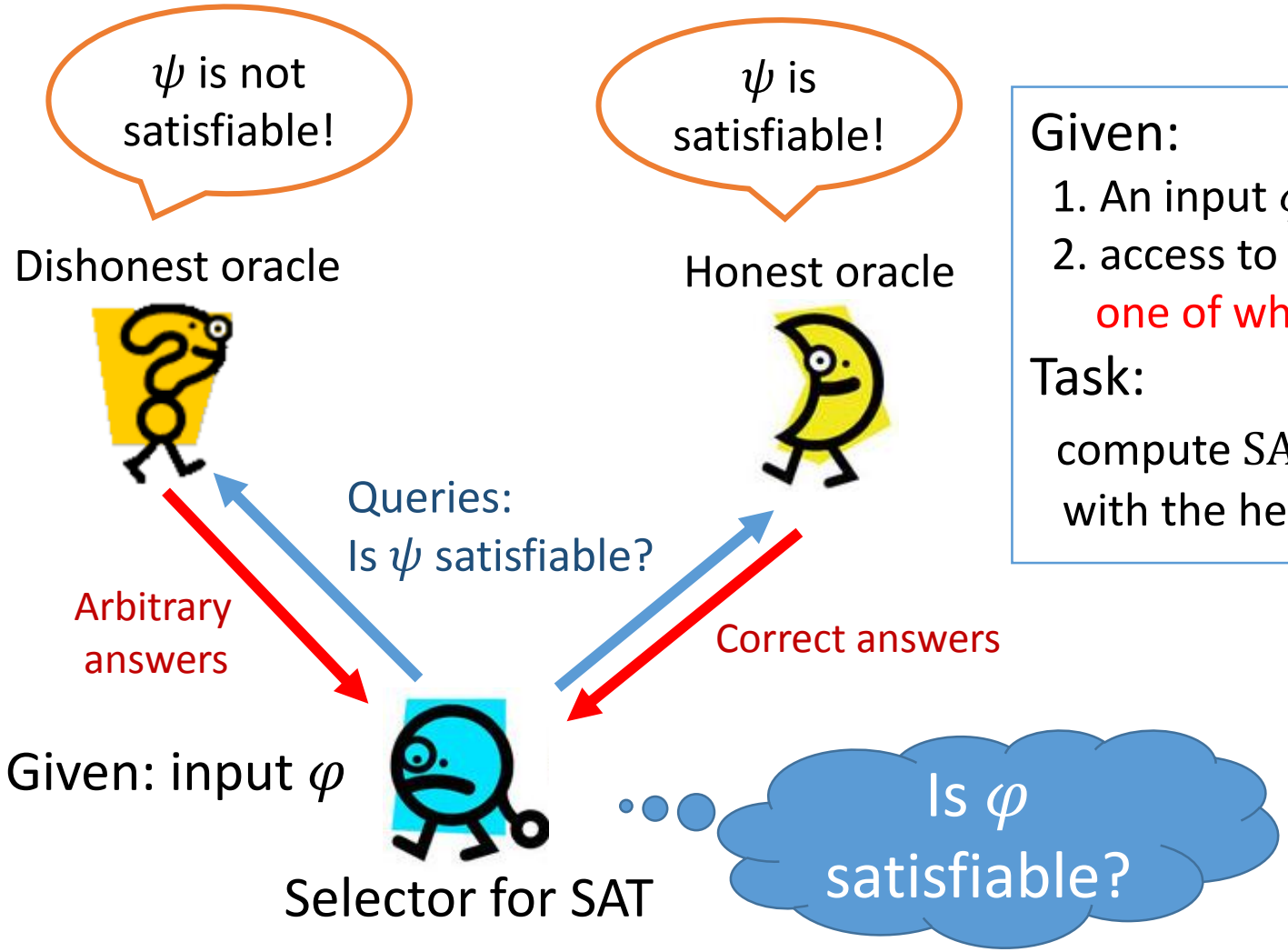
Given:

1. An input φ, and
2. access to two oracles
   one of which is honest.

Task:

compute $\mathrm{SAT}(\varphi)$
with the help of the oracles

(Probabilistic) Selector for SAT



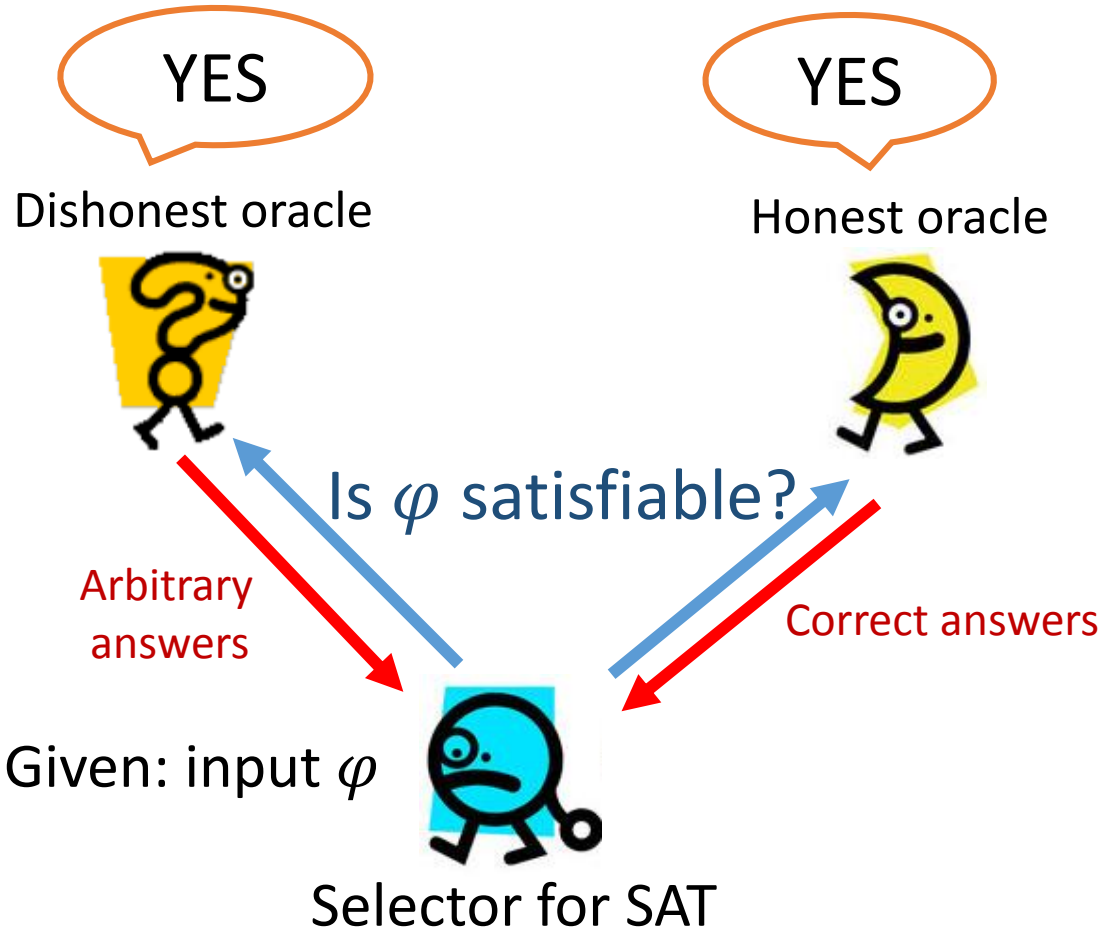
Given:

1. An input φ, and
2. access to two oracles
   one of which is honest.

Task:

compute $\mathrm{SAT}(\varphi)$
with the help of the oracles

Why is it called “selector”?

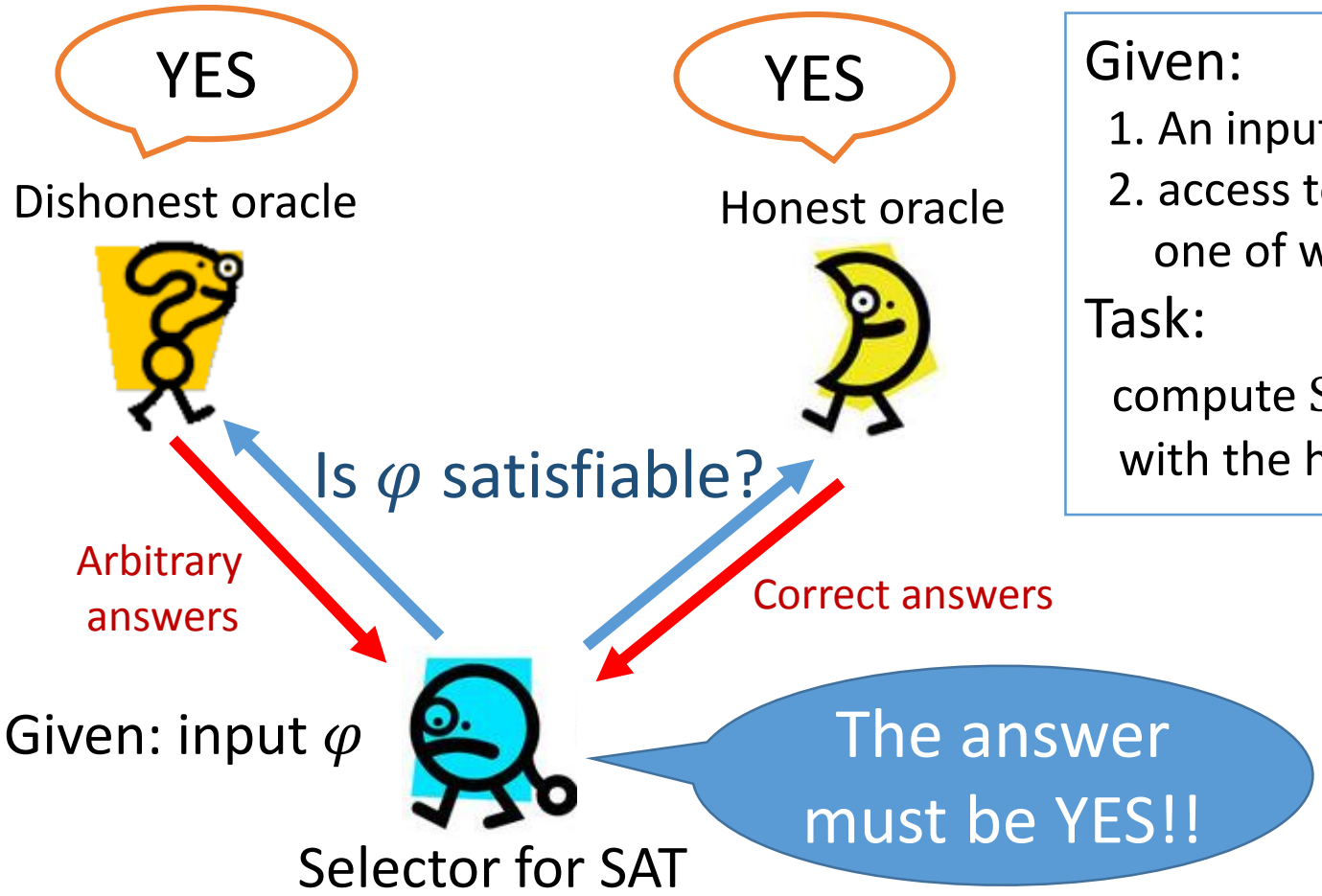


Given:
1. An input φ, and
2. access to two oracles
   one of which is honest.

Task:

compute $\mathrm{SAT}(\varphi)$
with the help of the oracles

Why is it called “selector”?

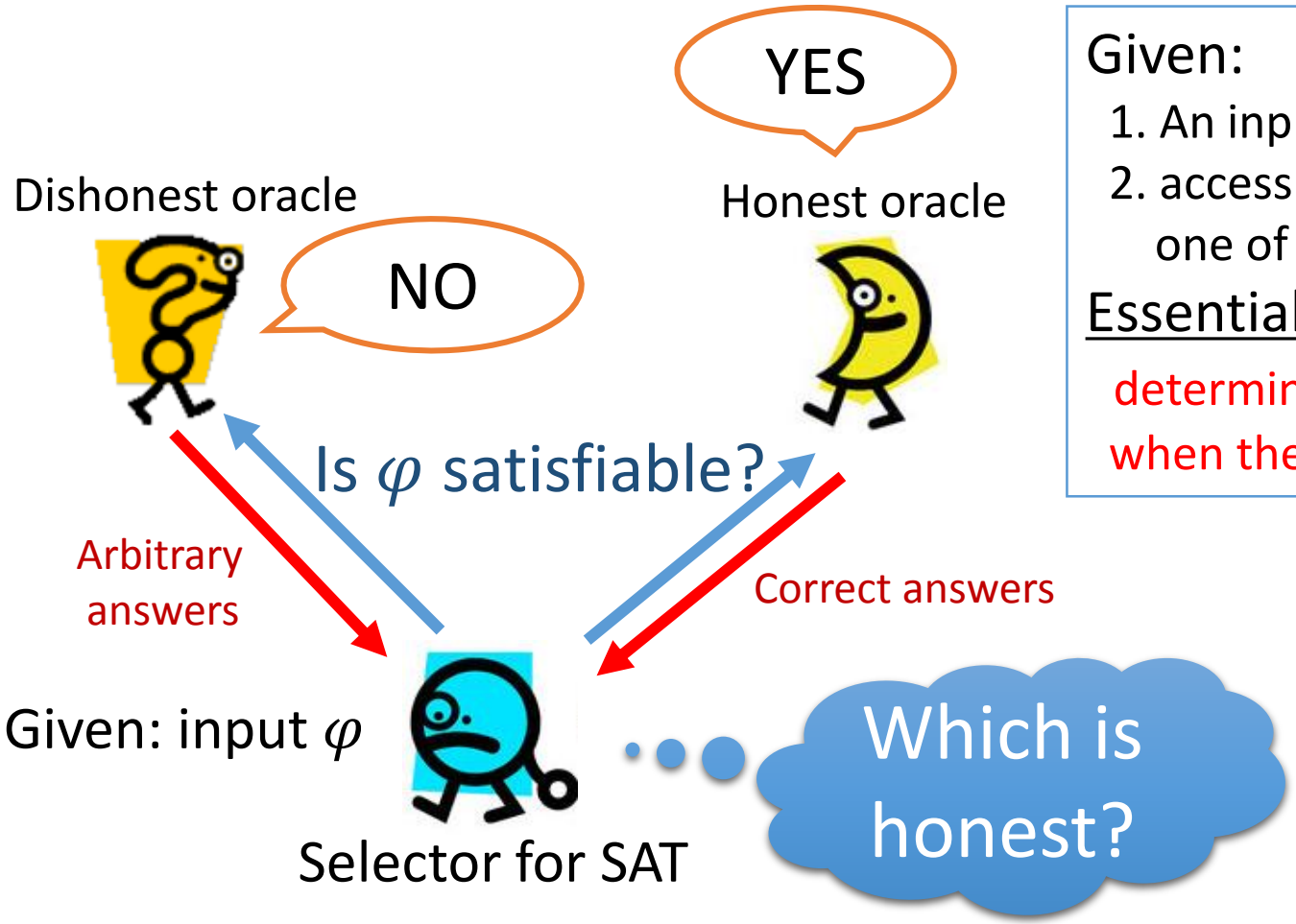


Given:
1. An input φ, and
2. access to two oracles
   one of which is honest.

Task:

compute $\mathrm{SAT}(\varphi)$
with the help of the oracles

Why is it called “selector”?



Given:
1. An input φ, and
2. access to two oracles one of which is honest.

Essential Task:

determine which is honest when they disagree on φ.

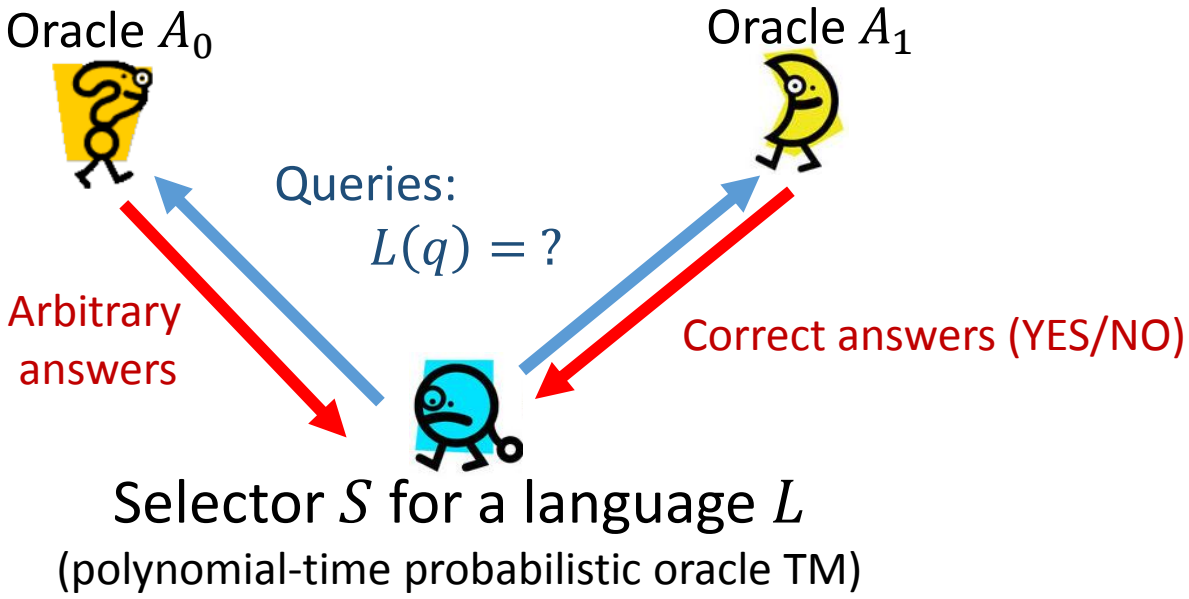
選択者の定義

定義 (選択者)

問題Lに対する選択者Sとは、多項式時間乱択チューリングマシンであって、以下の条件を満たすものをいう。

$$A_0 = L \text{ or } A_1 = L \implies \Pr[S^{A_0,A_1}(x) = L(x)] \geq 0.99$$

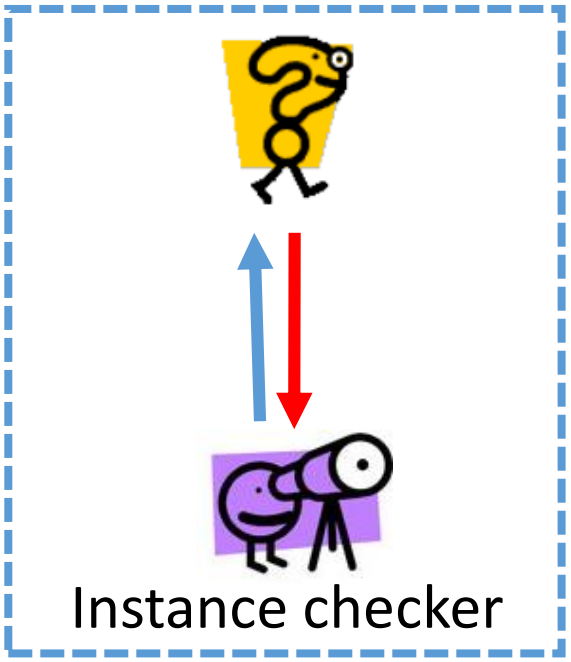
(for any $A_0, A_1 \subseteq \{0,1\}^*, x \in \{0,1\}^*$)

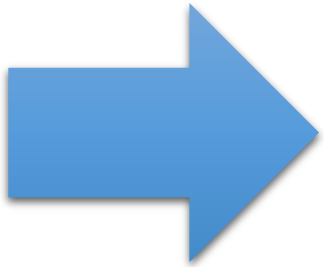


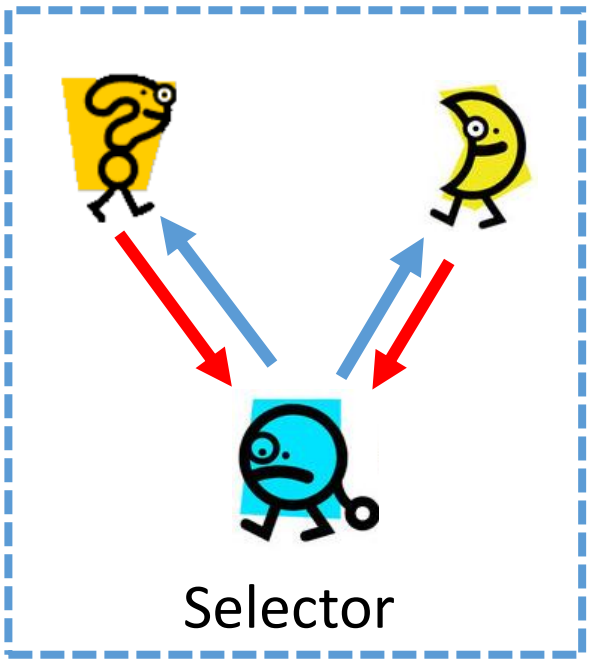
Instance Checker vs. Selector


が存在すれば、

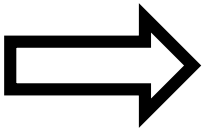
も存在する。







ひとつのオラクルを見て
正直かどうか判定する



二つのオラクルのうち
正直な方を選択する

例: P^{NP}完全問題に対する選択者

定義（P^{NP}完全問題: 辞書順最大の充足割当て）

入力: 充足可能なn変数論理式 φ と 自然数 $k \in \{1, \ldots, n\}$
出力: φの辞書順最大の充足割当てのk番目の変数の割り当てが真かどうか。

主張: この問題に対して選択者を構成できる。

✓ 入力(φ, k)と二つのオラクル  が与えられる。

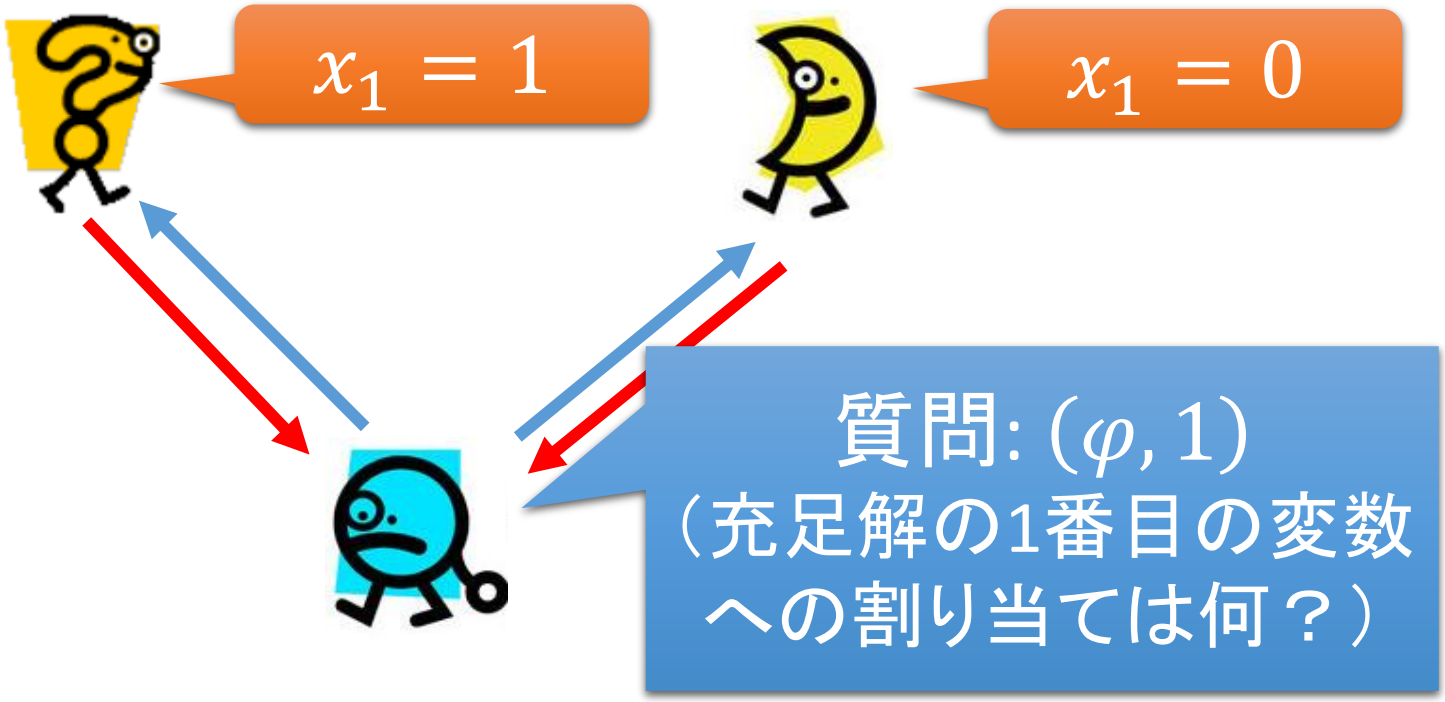
Step 1. それぞれのオラクルの主張する割当てを得る。

辞書順最大の充足割当ては… a_0 a_1

例: P^{NP}完全問題に対する選択者

定義（P^{NP}完全問題: 辞書順最大の充足割当て）

入力: 充足可能なn変数論理式 φ と 自然数 $k \in \{1, \ldots, n\}$
出力: φの辞書順最大の充足割当てのk番目の変数の割り当てが真かどうか。



例: P^{NP}完全問題に対する選択者

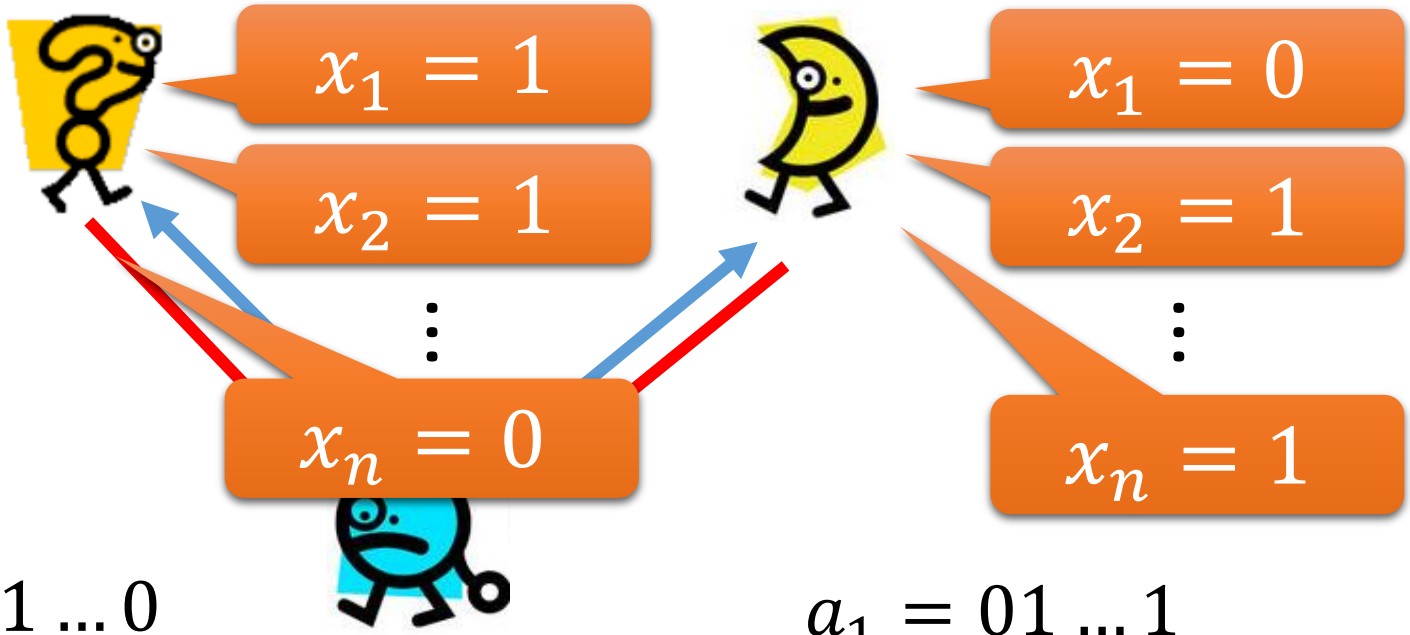
定義（P^{NP}完全問題: 辞書順最大の充足割当て）

入力: 充足可能なn変数論理式 φ と 自然数 $k \in \{1, \ldots, n\}$
出力: φの辞書順最大の充足割当てのk番目の変数の割り当てが真かどうか。

例: P^{NP}完全問題に対する選択者

定義（P^{NP}完全問題: 辞書順最大の充足割当て）

入力: 充足可能なn変数論理式 φ と 自然数 $k \in \{1, \dots, n\}$
出力: φの辞書順最大の充足割当てのk番目の変数の割り当てが真かどうか。



$a_0 = 11 \dots 0$

$a_1 = 01 \dots 1$

例: P^{NP}完全問題に対する選択者

定義（P^{NP}完全問題: 辞書順最大の充足割当て）

入力: 充足可能なn変数論理式 φ と 自然数 $k \in \{1, \dots, n\}$
出力: φの辞書順最大の充足割当てのk番目の変数の割り当てが真かどうか。

✓ **Step 1.** それぞれのオラクルの主張する割当てを得る。

$a_0 = 11 \dots 0$   $a_1 = 01 \dots 1$

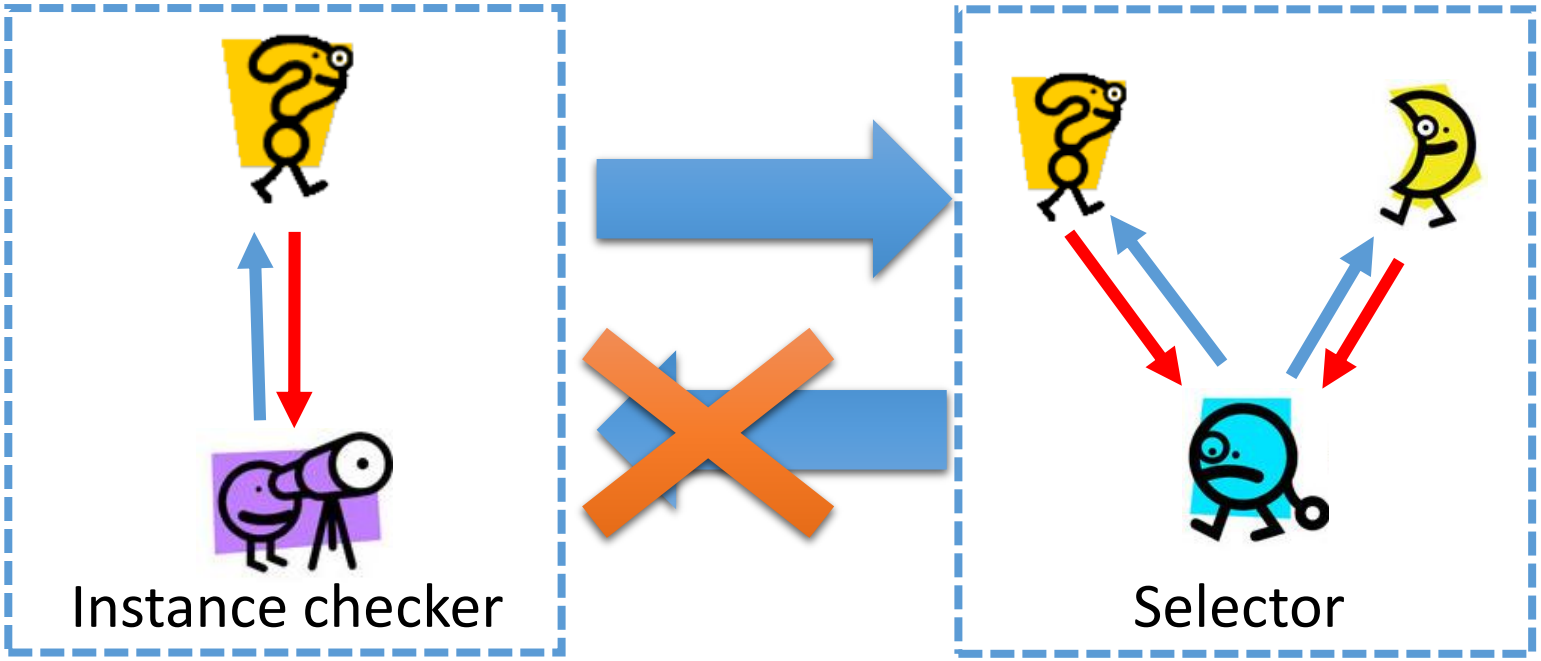
✓ **Step 2.** 大きい方の割当てが充足解か調べる。

 : $a_0 > a_1$なので$\varphi(a_0)$を評価する。

a_0が充足解であれば$(\varphi(a_0) = \mathrm{true})$、  を信じる。
そうでなければ  を信じる。

（構成終わり）

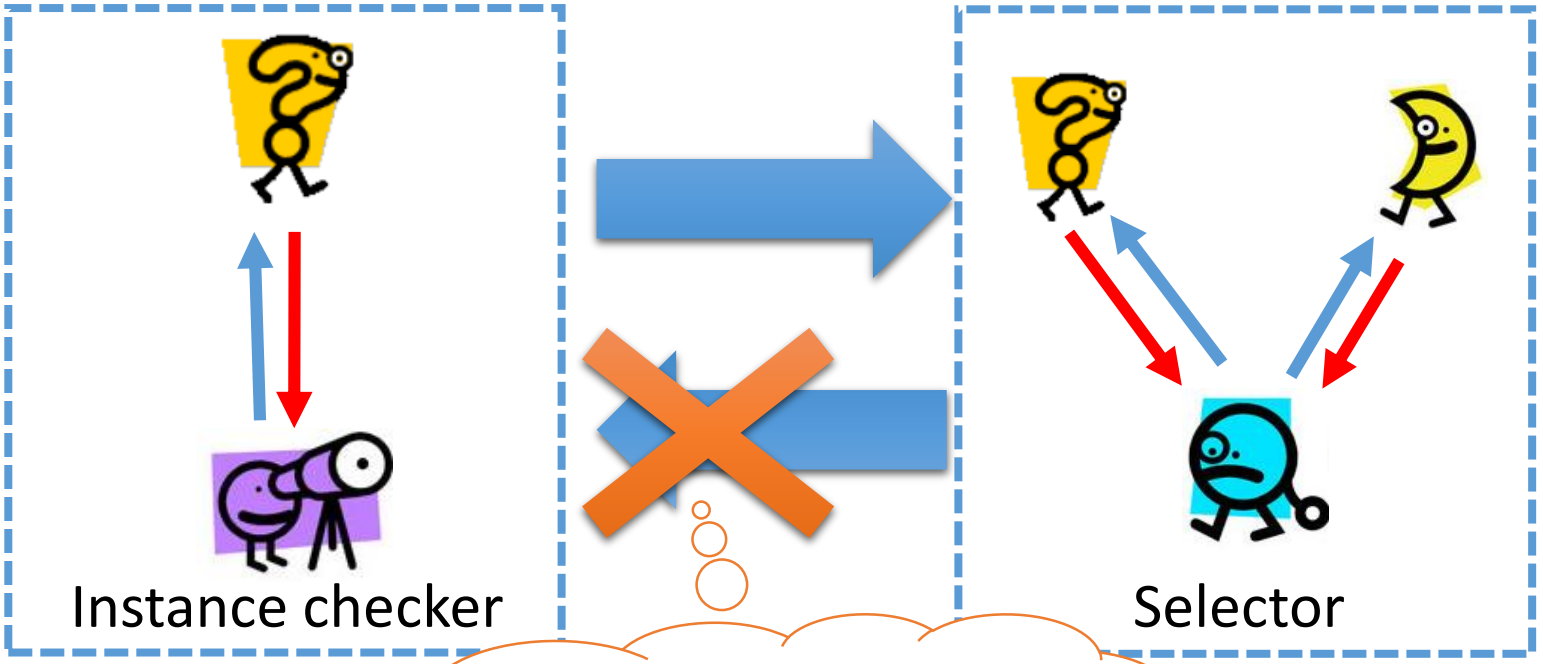
Instance Checker vs. Selector



ひとつのオラクルを見て
正直かどうか判定する

二つのオラクルのうち
正直な方を選択する

Instance Checker vs. Selector



ひとつのオラ
正直かどうか

オラクルのうち
な方を選択する

反例:
$\mathrm{EXP}^{\mathrm{NP}}$完全問題

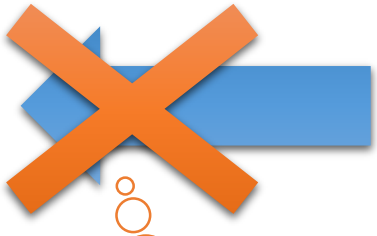
（$\mathrm{NEXP} = \mathrm{EXP}^{\mathrm{NP}}$でない限り）

Instance Checker vs. Selector

主定理

$\mathrm{EXP}^{\mathrm{NP}}$完全問題に対する選択者が存在する。

Instance checker



Selector

ひとつのオラ
正直かどうか

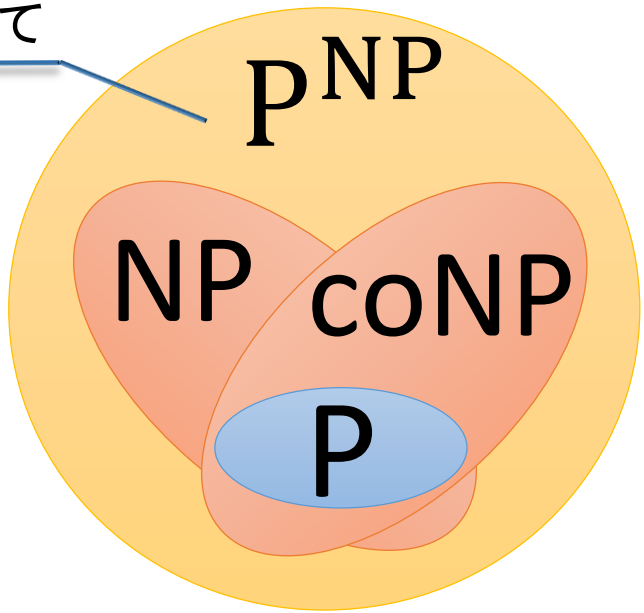
反例:
$\mathrm{EXP}^{\mathrm{NP}}$完全問題

オラクルのうち
な方を選択する

（$\mathrm{NEXP} = \mathrm{EXP}^{\mathrm{NP}}$でない限り）

P^{NP}とは

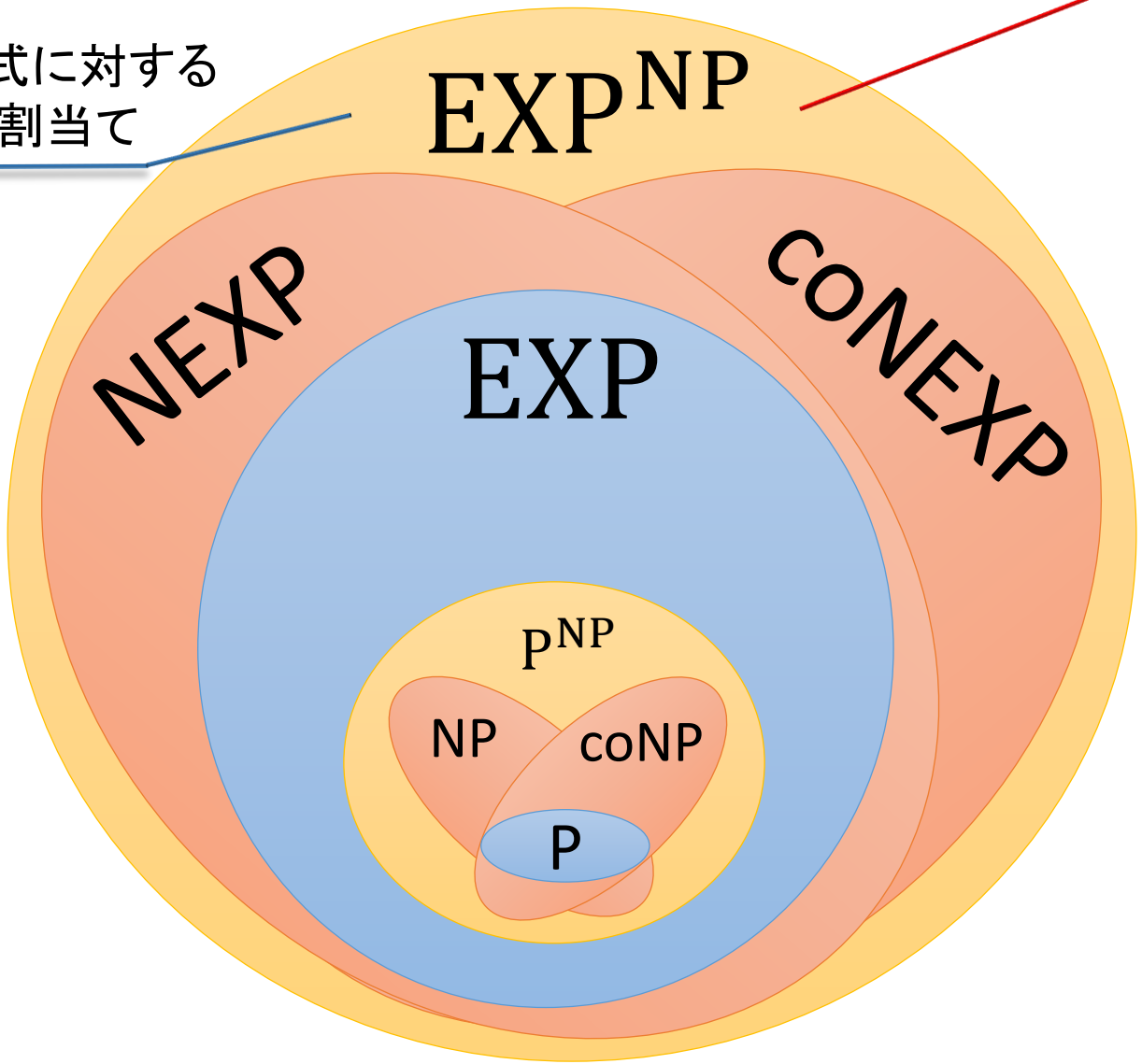
例:辞書順最大の充足割当て



EXP^{NP}とは

例:指数サイズの論理式に対する
辞書順最大の充足割当て

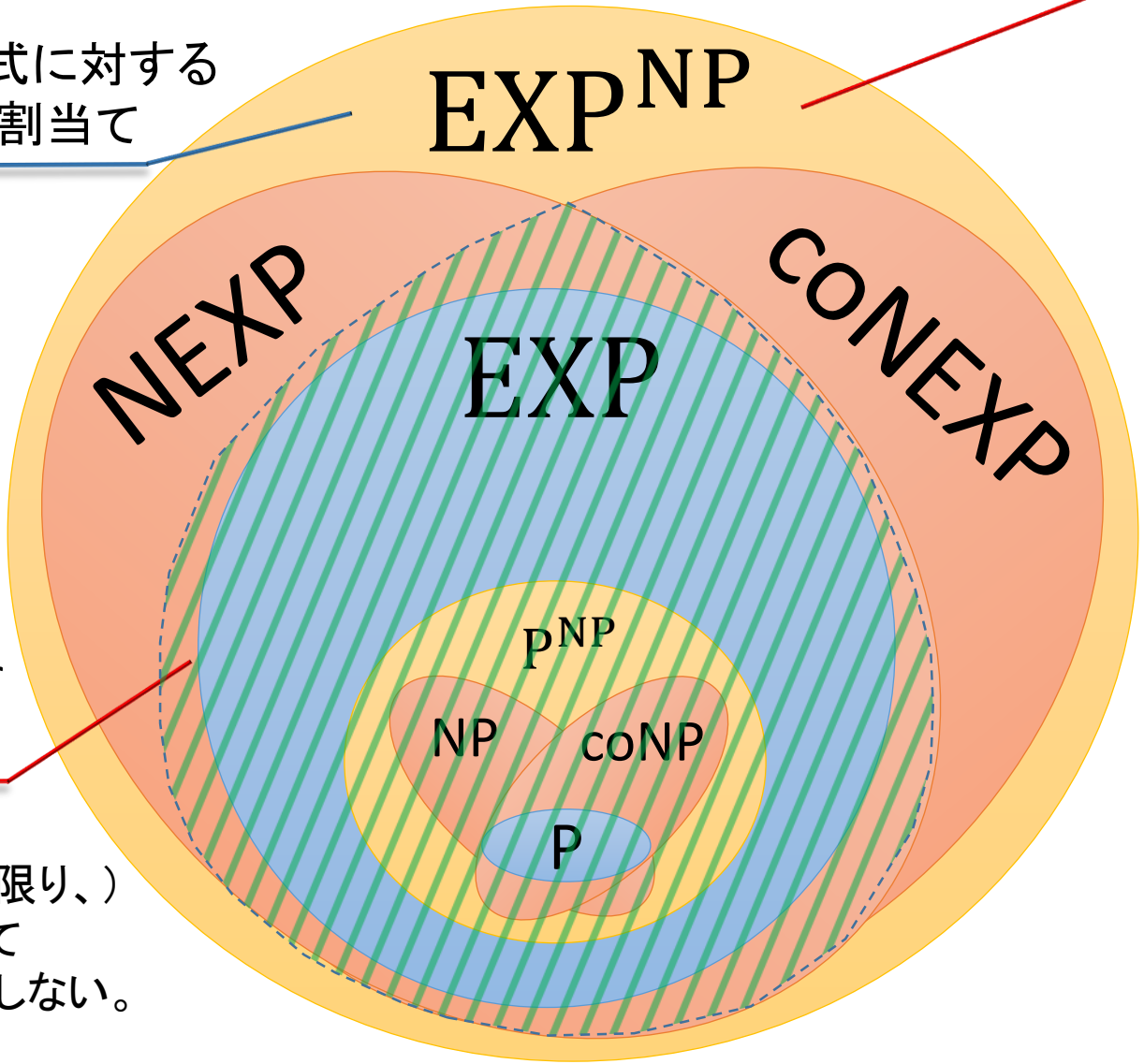
主結果: 完全問題についてヨ選択者



$\mathrm{EXP}^{\mathrm{NP}}$とは

主結果: 完全問題についてヨ選択者

例:指数サイズの論理式に対する
辞書順最大の充足割当て



Instance checker
の存在範囲

（$\mathrm{EXP}^{\mathrm{NP}} = \mathrm{NEXP}$でない限り、）
$\mathrm{EXP}^{\mathrm{NP}}$完全問題に対して
instance checkerは存在しない。

ここまで

Instance checker

✓「オラクルが正直か確認する」ことより「正直なオラクルを選ぶ」方が真に簡単。

selector

ここから

➢選択者が「短いアドバイスの消去」という条件を特徴付けることについて。

アドバイスとは

- 入力の長さnのみに依存する、計算を補助するデータ$\alpha_n \in \{0,1\}^*$のこと。

定義 (対数長のアドバイスで解ける問題全体)

問題Lに対し、$L \in \mathbf{P/log}$とは、

1. 各nについて 長さ$O(\log n)$のアドバイスα_nが存在し、
2. 多項式時間チューリングマシンM  が存在して、

長さnの任意の入力xに対し $M(x, \alpha_n) = L(x)$ となること。

（アドバイスは入力xには依存せず、入力の長さnにのみ依存する。）

動機: 短いアドバイスの消去

[Karp & Lipton (1980)]

$$\mathrm{SAT} \in \mathbf{P/log} \Longrightarrow \mathrm{SAT} \in \mathbf{P}$$

✓ SATを解くためには対数長のアドバイスは不要

[Trevisan & Vadhan (2002)]

$$\mathrm{EXP} \subseteq \mathbf{BPP/log} \Longrightarrow \mathrm{EXP} \subseteq \mathbf{BPP}$$

➢ EXP完全問題に対するinstance checkerが存在することから従う。

Q. 一般に, アドバイスを消去できる条件は？

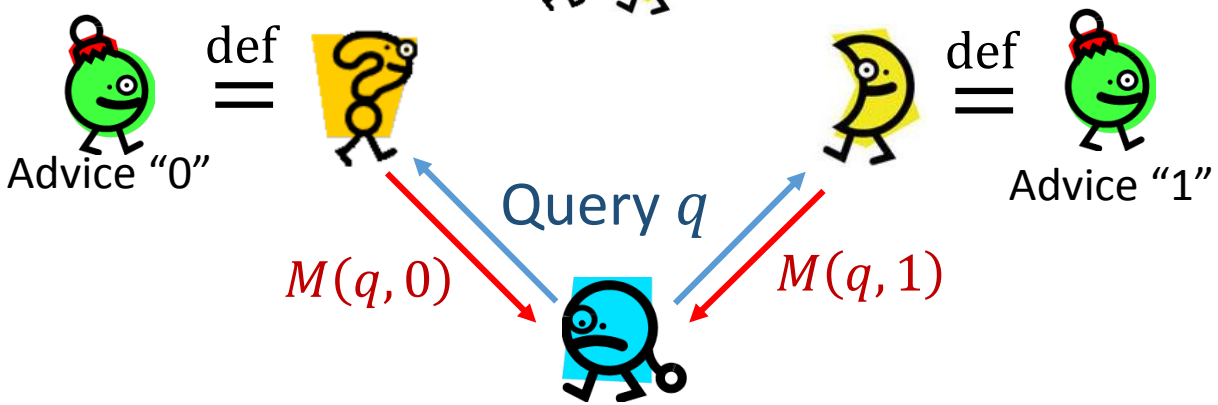
答え: 選択者が存在すること(必要十分条件)

ヨ選択者 $\Longrightarrow$ 1bitのアドバイスの消去

1. 問題 L が1bitのアドバイスで計算できるとする。

   i.e. ある機械M が存在し、アドバイス"0"か"1"を与えると問題Lを正しく計算する。

2. 二つのオラクル を以下のように定める:

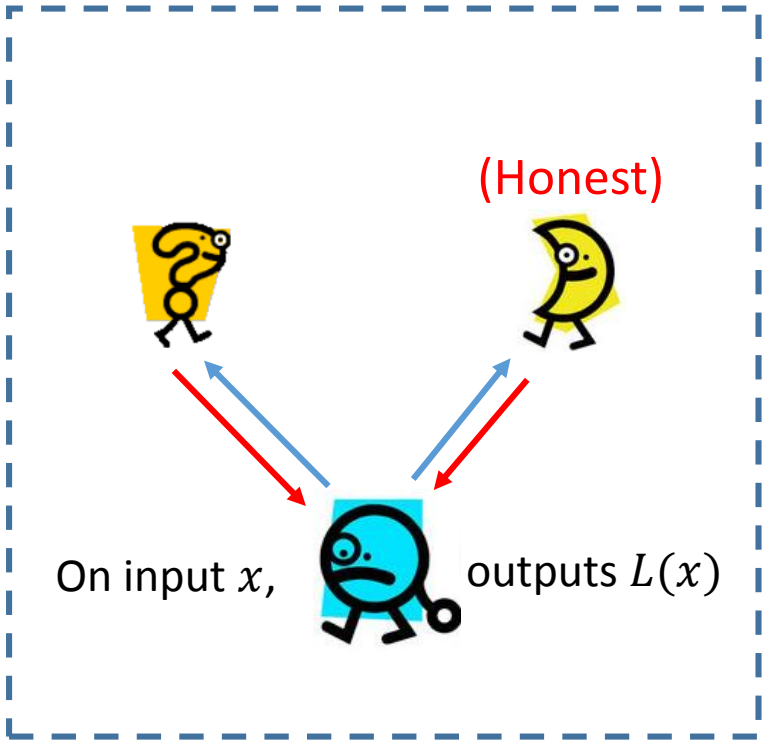


どちらか一方は正直なオラクルになる！

$\Longrightarrow$ 選択者は(アドバイスなしで)Lを正しく計算する。

Key Lemma: "Among Many"

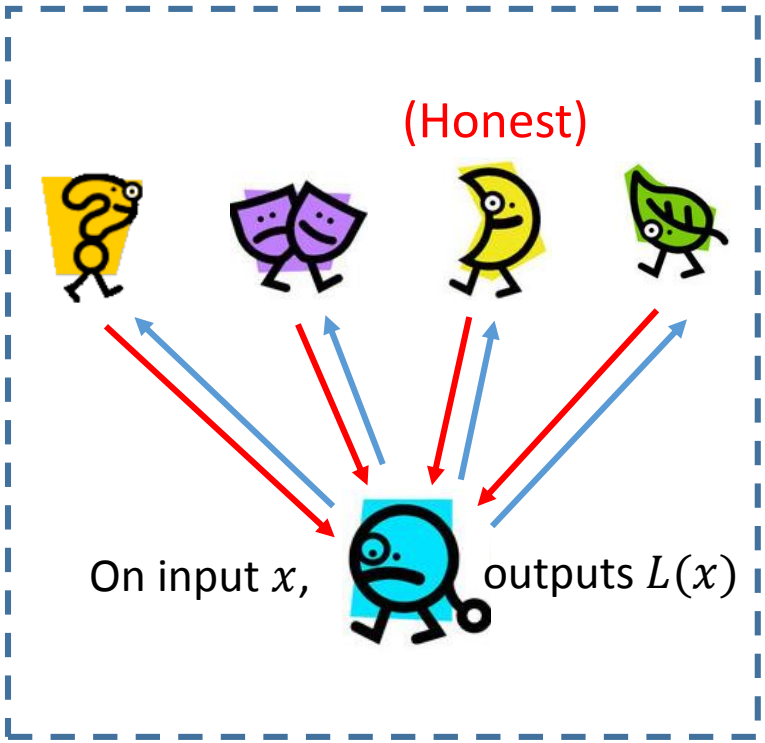
Identifying an honest oracle among two



✓ Able to remove advice of 1 bit

=

Identifying an honest oracle among polynomially many



✓ Able to remove advice of $O(\log n)$ bits

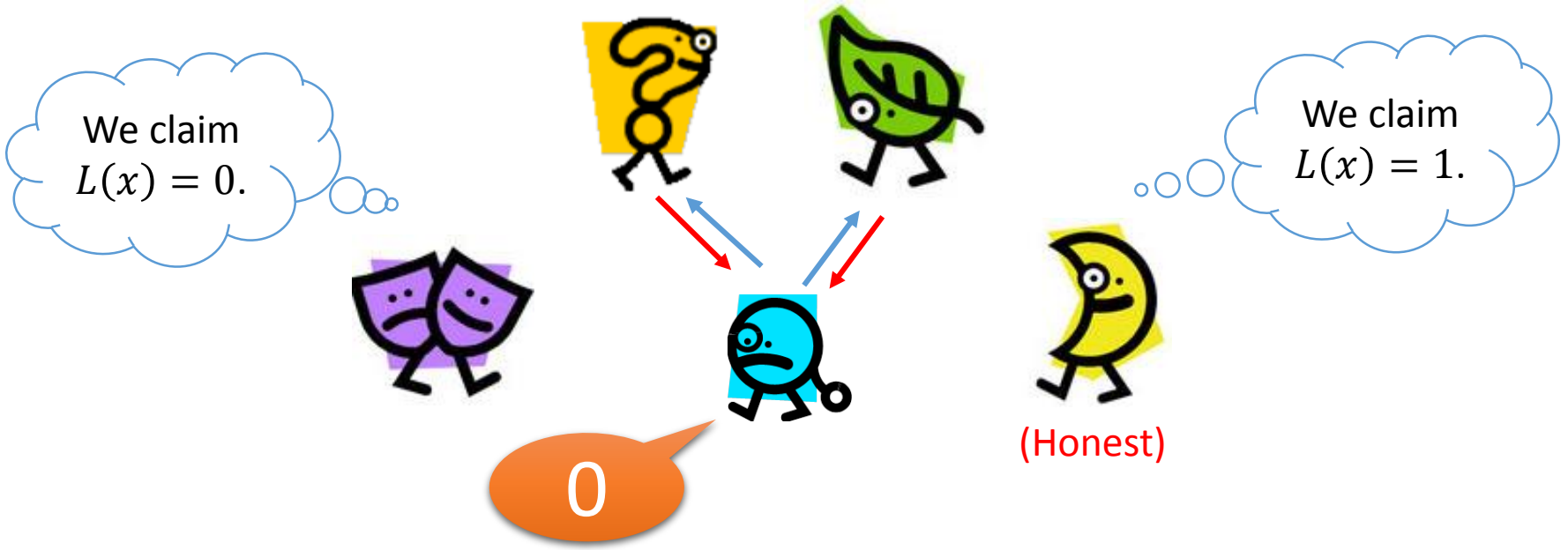
Proof of the Key Lemma (1/2)

- We have a selector  that identifies an honest oracle among two.
- Given input x and many oracles
- Ask them about x: $L(x)$ is
- Divide them into two teams:

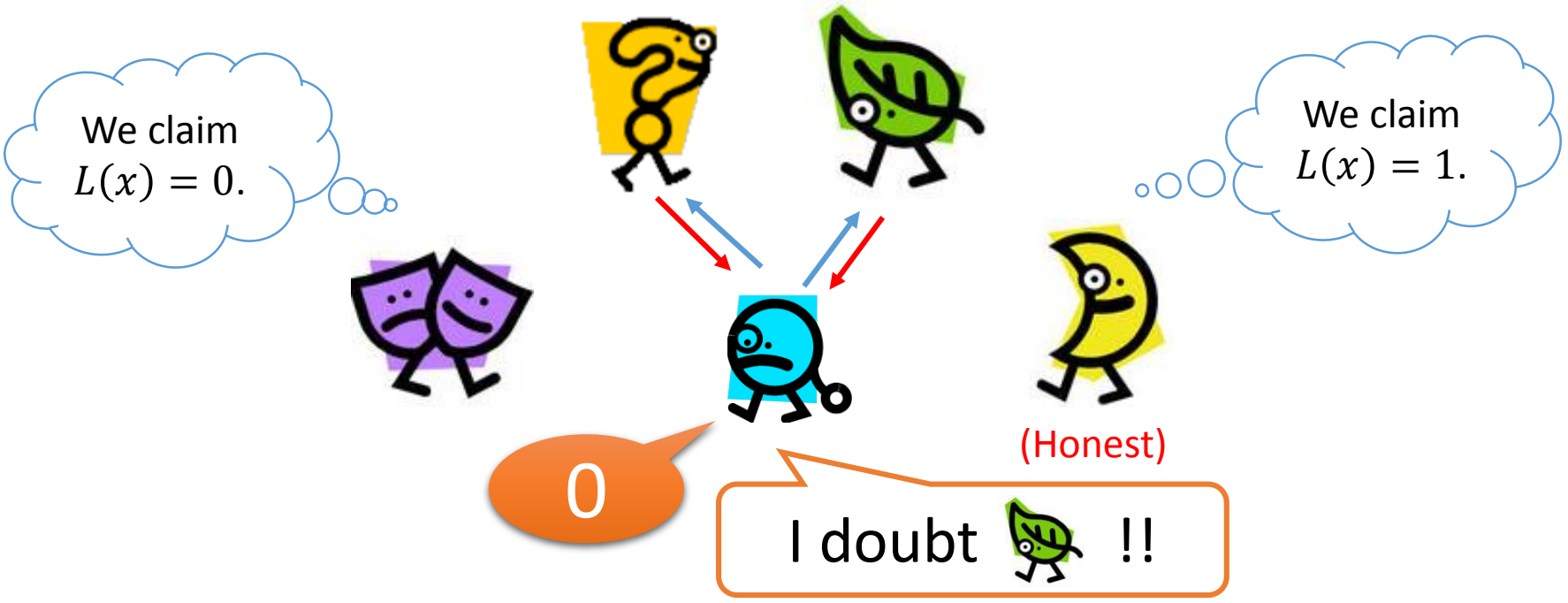
Idea: "Tournament"

Proof of the Key Lemma (2/2)

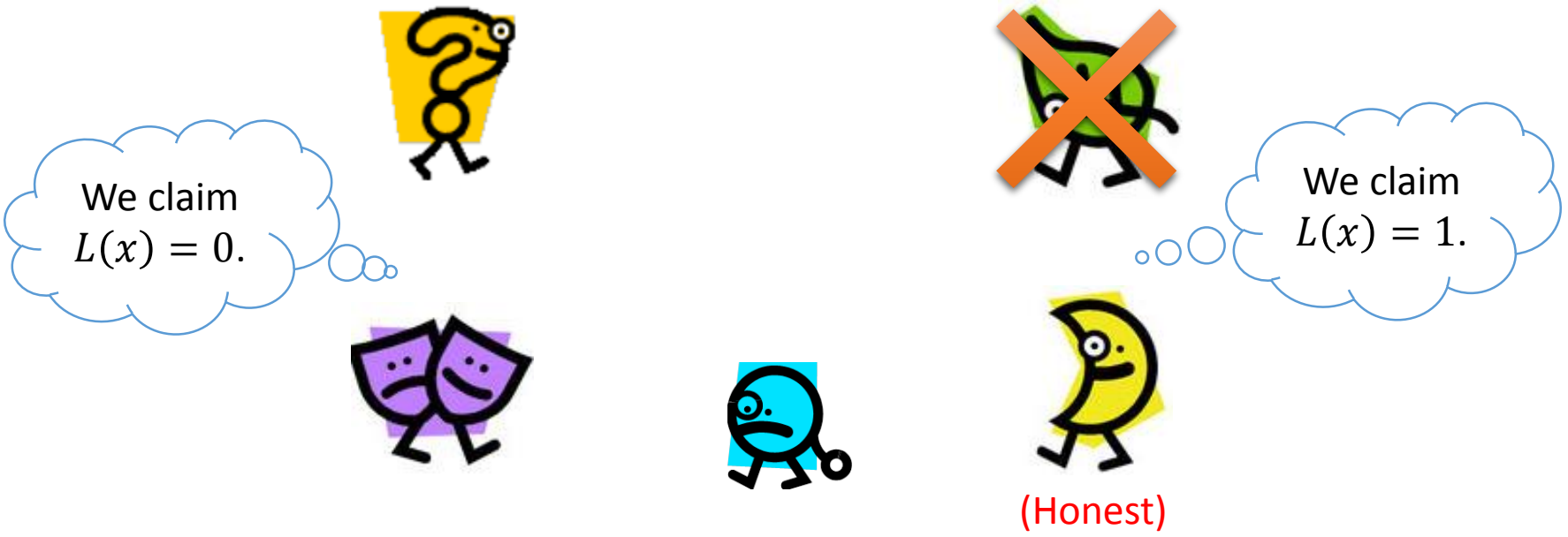
Proof of the Key Lemma (2/2)



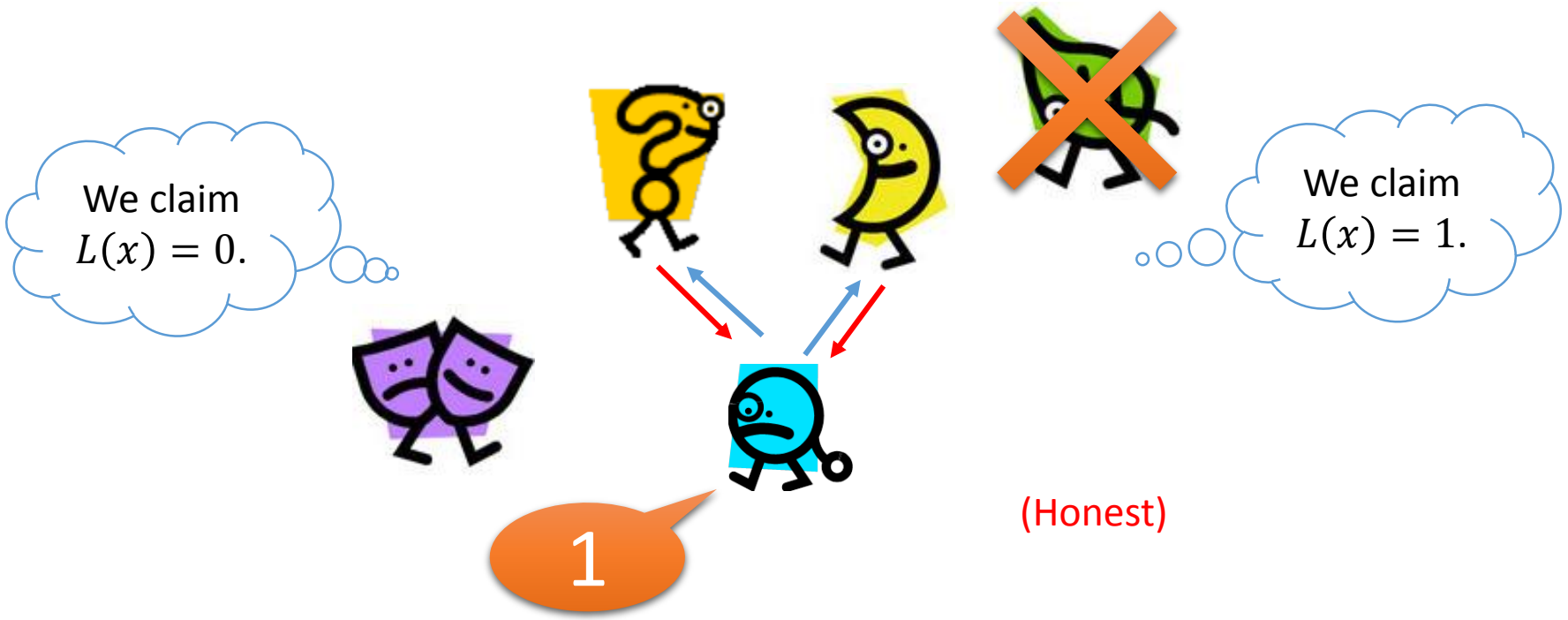
Proof of the Key Lemma (2/2)



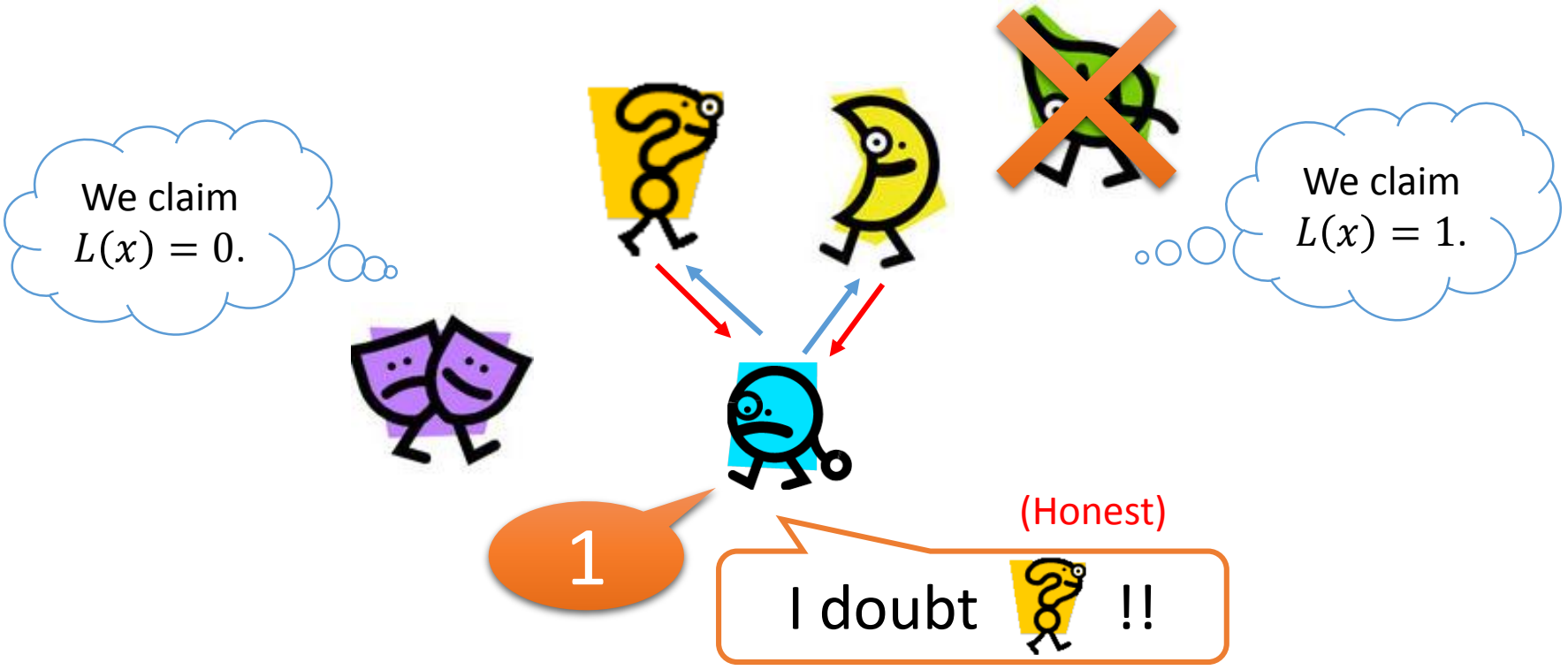
Proof of the Key Lemma (2/2)



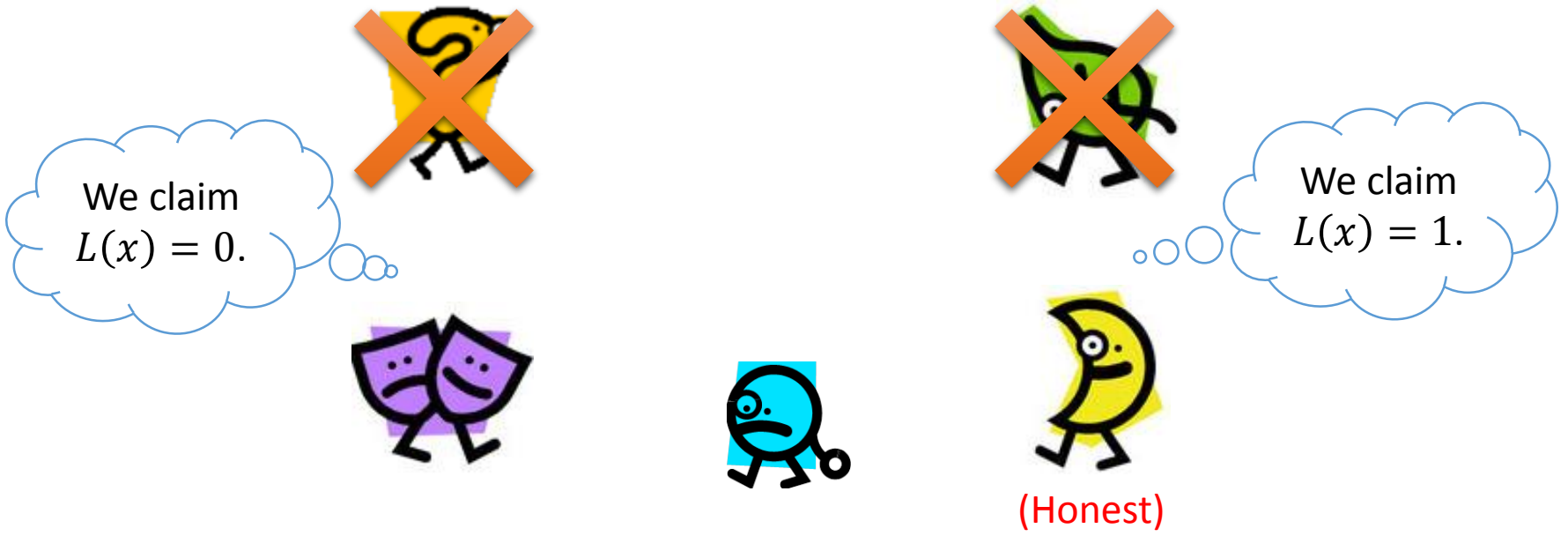
Proof of the Key Lemma (2/2)



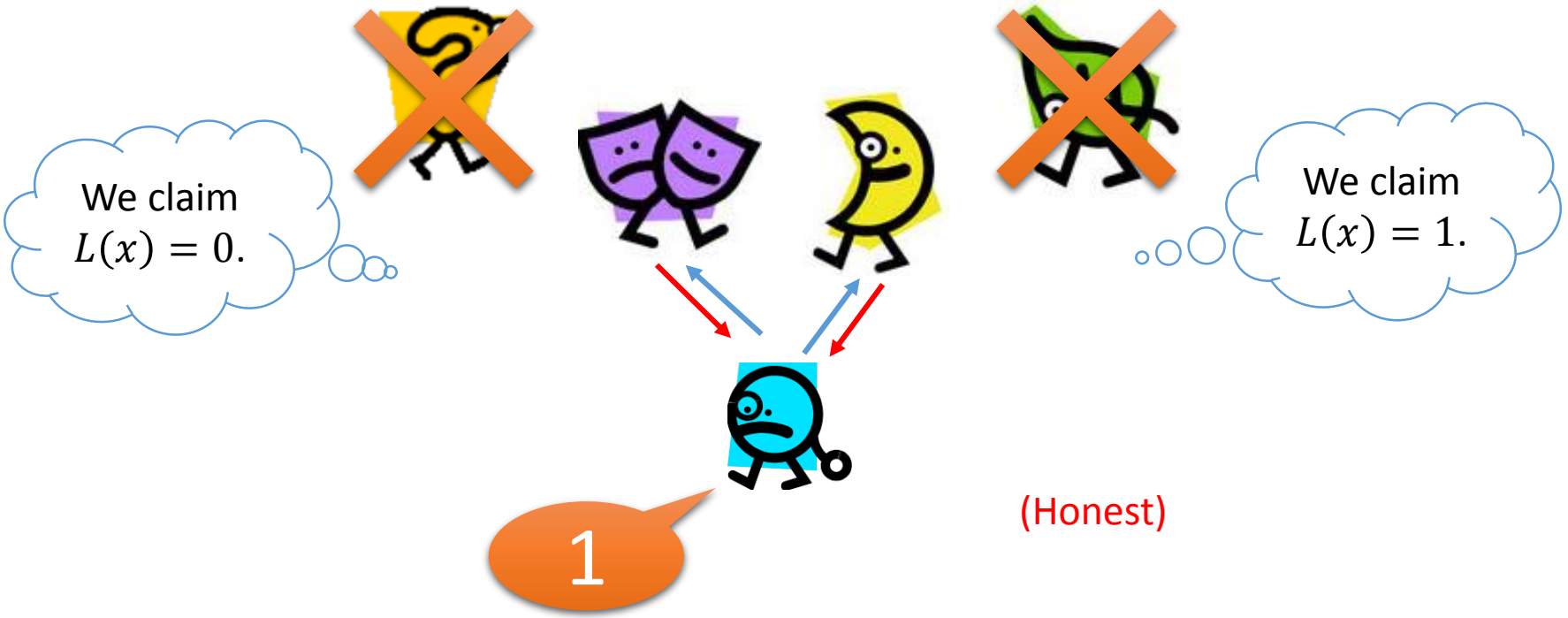
Proof of the Key Lemma (2/2)



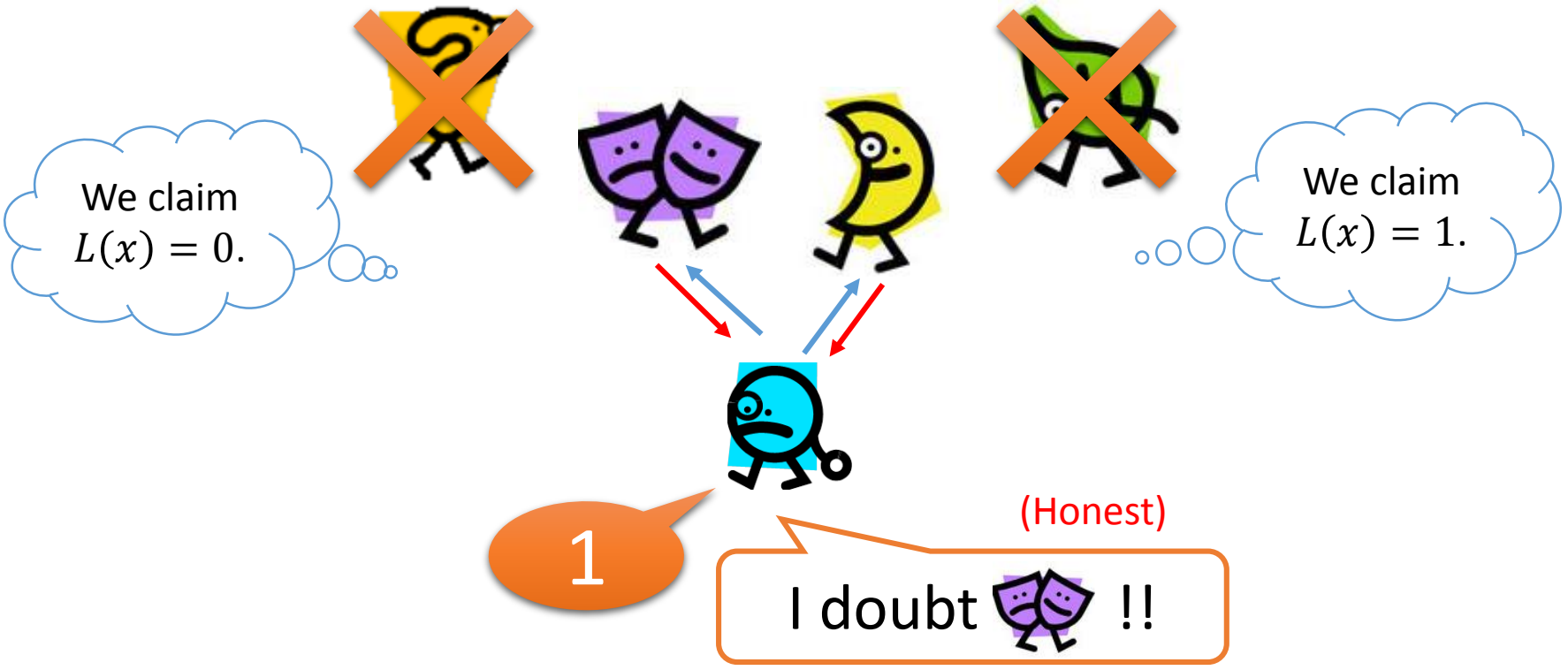
Proof of the Key Lemma (2/2)



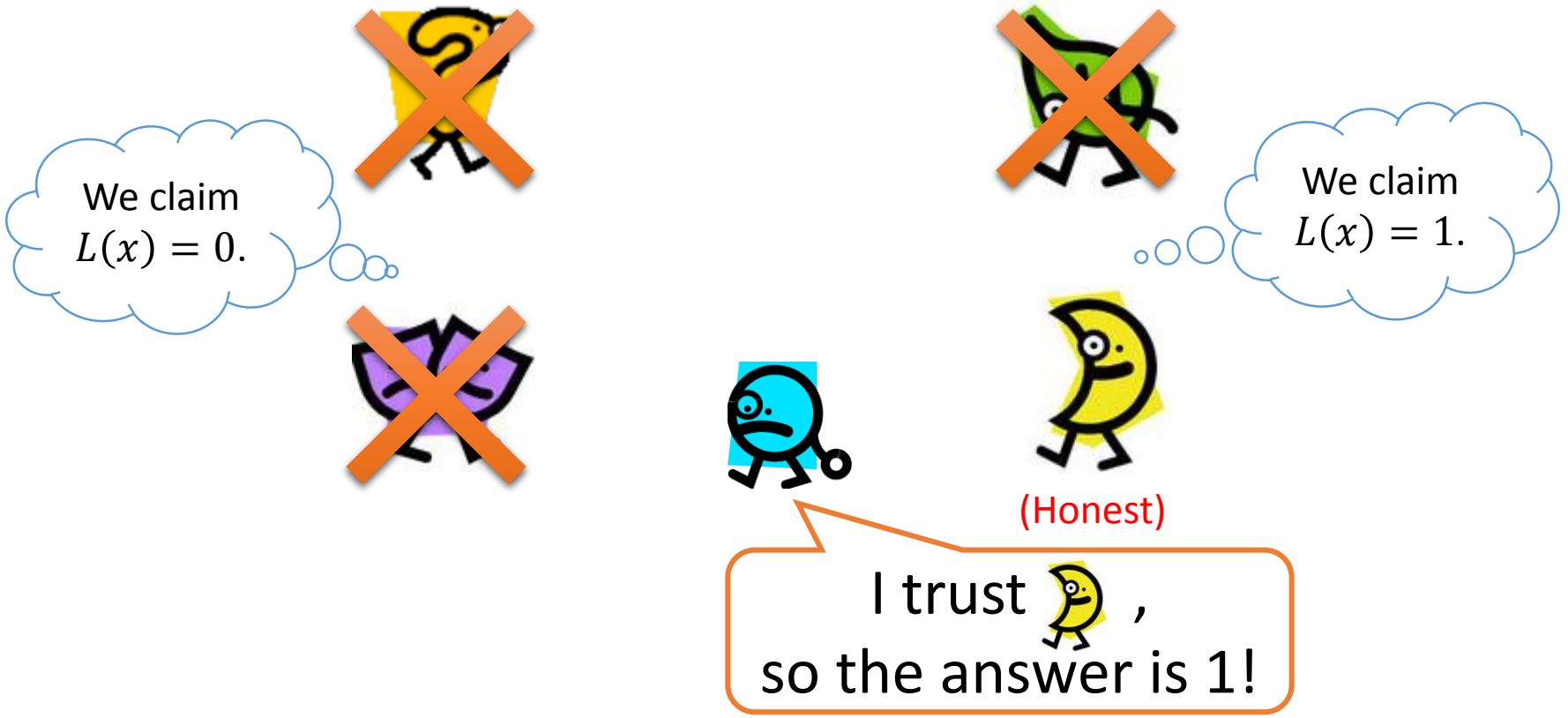
Proof of the Key Lemma (2/2)



Proof of the Key Lemma (2/2)

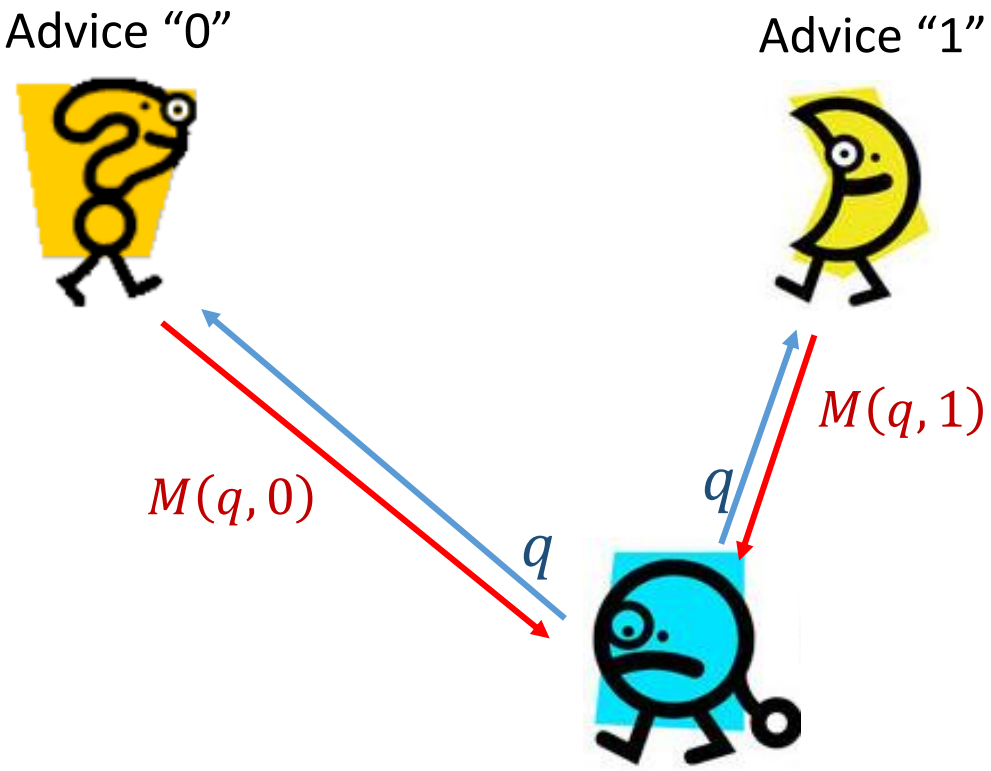


Proof of the Key Lemma (2/2)

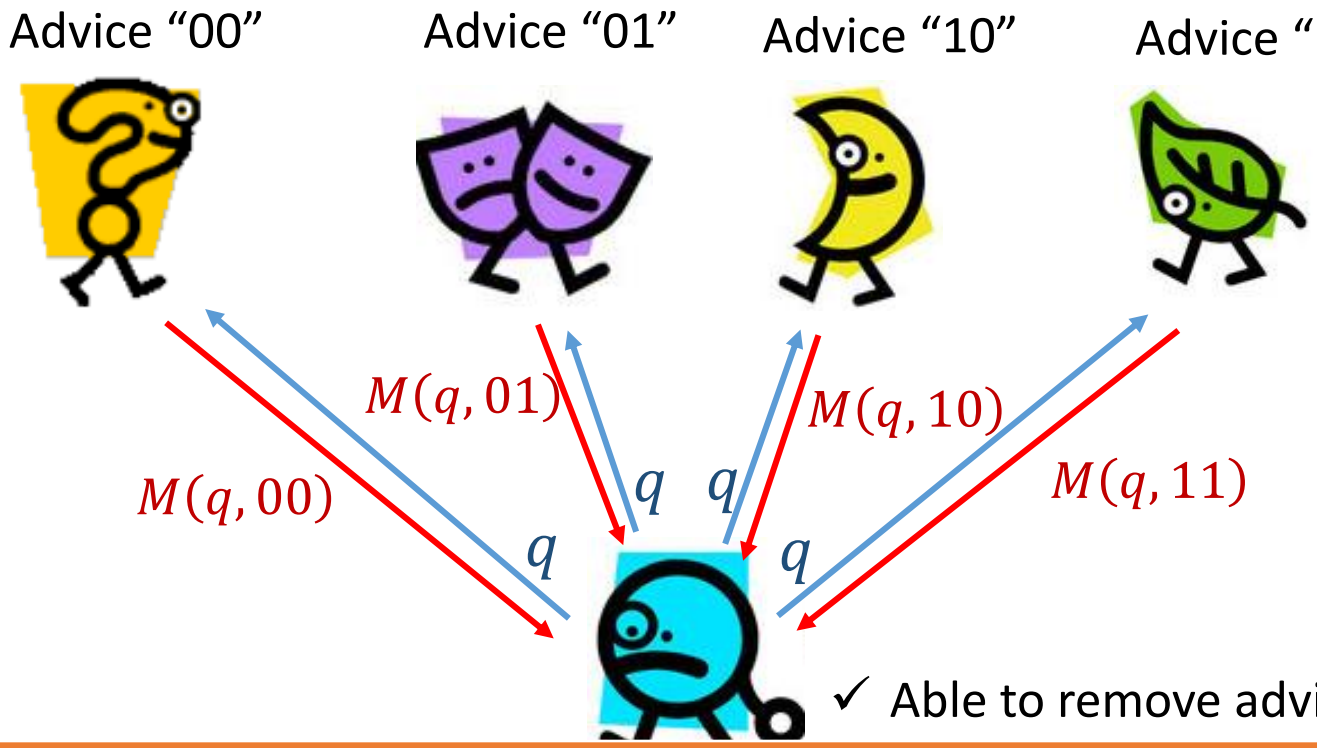


✓The honest oracle always wins!

Removing advice of size $O(\log n)$



Removing advice of size $O(\log n)$



✓ Able to remove advice of 2 bits

Corollary (Selector ⇒ Removing short advice)

Suppose that there exists a selector for a paddable language L. Then, $L \in \mathbf{BPP/log}$ implies $L \in \mathbf{BPP}$.

まとめ

- ✓選択者という概念を導入した。
  - ➢二つのオラクルのうちから正直なオラクルを選ぶ。
  - ➢多項式個のオラクルのうちから正直なオラクルを選ぶ、といっても同じ。
- ✓Instance checkerの仕事よりも選択者の仕事の方が真に簡単。($\mathrm{EXP}^{\mathrm{NP}}$完全問題)
- ✓短いアドバイスの消去について、今まではinstance checkerが使われてきたが、実は選択者が必要十分条件を与える。