Mental Jinro

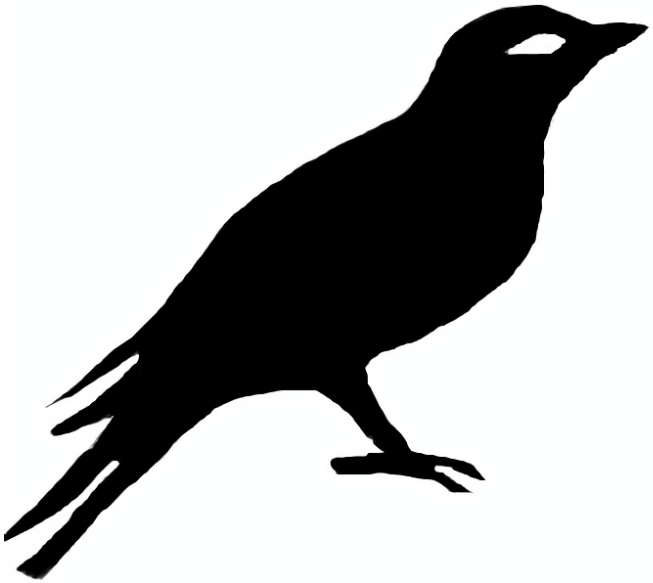
tsukuba.pm #3

吉村 優

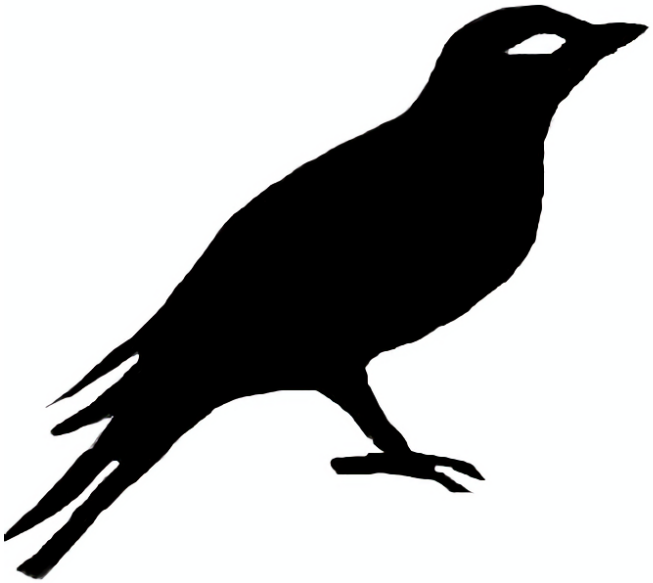
https://twitter.com/_yyu_
http://qiita.com/yyu
https://github.com/y-yu

May 14, 2016

自己紹介

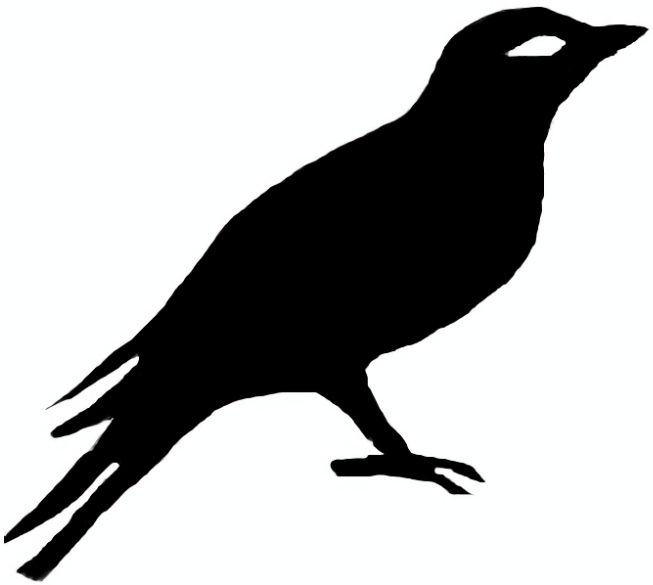


自己紹介



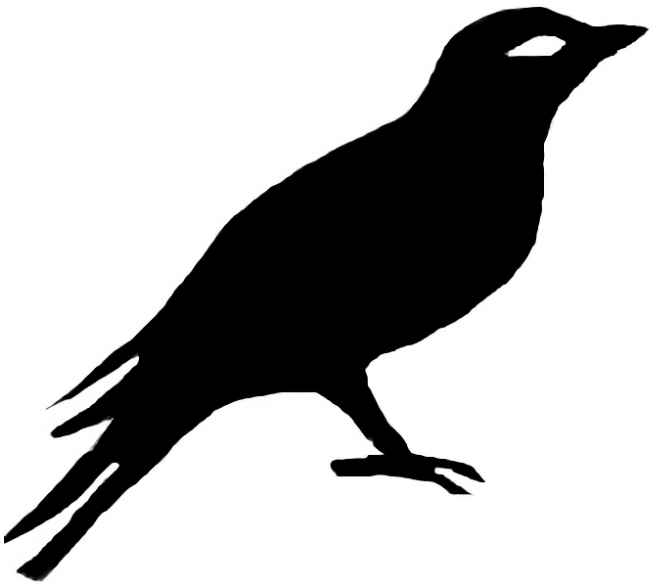
- 筑波大学 情報科学類 学士（COINS11）

自己紹介



- 筑波大学 情報科学類 学士（COINS11）
- WORD 編集部 OB

自己紹介



- 筑波大学 情報科学類 学士（COINS11）
- WORD 編集部 OB
- プログラム論理研究室 OB

“Mental Jinro” とは？

“Mental Jinro” とは？

> “ ***Mental Jinro*** は人狼からゲームマスターを排除したゲームである。 ”

“Mental Jinro” とは？

> “ ***Mental Jinro*** は人狼からゲームマスターを排除したゲームである。 ”

ゲームマスターとは何か？

“Mental Jinro” とは？

> “ ***Mental Jinro*** は人狼からゲームマスターを排除したゲームである。 ”

ゲームマスターとは何か？

そもそも人狼とは何か？

人狼とは？

人狼*

“

”

Wikipedia —— 汝は人狼なりや？

*人狼には様々なルールがあるが、このスライドではこのルールを用いる

人狼とは？

人狼*

“

- プレイヤーはそれぞれが**村人**と村人に化けた**人狼**となり、自分自身の正体がばれないように他のプレイヤーと交渉して正体を探る

”

Wikipedia —— 汝は人狼なりや？

*人狼には様々なルールがあるが、このスライドではこのルールを用いる

人狼とは？

人狼*

“

- プレイヤーはそれぞれが**村人**と村人に化けた**人狼**となり、自分自身の正体がばれないように他のプレイヤーと交渉して正体を探る
- ゲームは半日単位で進行し、昼には全プレイヤーの投票により決まった人狼容疑者の**処刑**が、夜には人狼による村人の**襲撃**が行われる

”

Wikipedia —— 汝は人狼なりや？

*人狼には様々なルールがあるが、このスライドではこのルールを用いる

人狼とは？

人狼*

“

- プレイヤーはそれぞれが**村人**と村人に化けた**人狼**となり、自分自身の正体がばれないように他のプレイヤーと交渉して正体を探る
- ゲームは半日単位で進行し、昼には全プレイヤーの投票により決まった人狼容疑者の**処刑**が、夜には人狼による村人の**襲撃**が行われる
-
  - 全ての人狼を処刑することができれば村人チームの勝ち

”

Wikipedia —— 汝は人狼なりや？

*人狼には様々なルールがあるが、このスライドではこのルールを用いる

人狼とは？

人狼 *

“

- プレイヤーはそれぞれが**村人**と村人に化けた**人狼**となり、自分自身の正体がばれないように他のプレイヤーと交渉して正体を探る
- ゲームは半日単位で進行し、昼には全プレイヤーの投票により決まった人狼容疑者の**処刑**が、夜には人狼による村人の**襲撃**が行われる
-
  - 全ての人狼を処刑することができれば村人チームの勝ち
  - 人狼と同じ数まで村人を減らすことができれば人狼チームの勝ち

”

Wikipedia —— 汝は人狼なりや？

*人狼には様々なルールがあるが、このスライドではこのルールを用いる

人狼の役職

人狼に必要な役職

参加者を次の役職に分ける必要がある

人狼の役職

人狼に必要な役職

参加者を次の役職に分ける必要がある

- 村人

人狼の役職

人狼に必要な役職

参加者を次の役職に分ける必要がある

- 村人
- 人狼

人狼の役職

人狼に必要な役職

参加者を次の役職に分ける必要がある

- 村人
- 人狼
- ゲームマスター

人狼の役職

人狼に必要な役職

参加者を次の役職に分ける必要がある

- 村人
- 人狼
- ゲームマスター

ゲームマスターとは何か？

ゲームマスターと公平性

ゲームマスターの役割

ゲームマスターと公平性

ゲームマスターの役割

- 人狼と村人のチーム分けをする

ゲームマスターと公平性

ゲームマスターの役割

- 人狼と村人のチーム分けをする
- 人狼に襲撃された村人を村人チームに宣告する

ゲームマスターと公平性

ゲームマスターの役割

- 人狼と村人のチーム分けをする
- 人狼に襲撃された村人を村人チームに宣告する
- 人狼と村人の数を管理し、どちらかのチームが勝利した時それを宣言する

ゲームマスターと公平性

ゲームマスターの役割

- 人狼と村人のチーム分けをする
- 人狼に襲撃された村人を村人チームに宣告する
- 人狼と村人の数を管理し、どちらかのチームが勝利した時それを宣言する

ゲームマスターとは審判

ゲームマスターと公平性

ゲームマスターの役割

- 人狼と村人のチーム分けをする
- 人狼に襲撃された村人を村人チームに宣告する
- 人狼と村人の数を管理し、どちらかのチームが勝利した時それを宣言する

ゲームマスターとは審判

ゲームマスターが不公平だったら？

ゲームマスターと公平性

ゲームマスターの役割

- 人狼と村人のチーム分けをする
- 人狼に襲撃された村人を村人チームに宣告する
- 人狼と村人の数を管理し、どちらかのチームが勝利した時それを宣言する

ゲームマスターとは審判

ゲームマスターが不公平だったら？

大問題！

Mental Jinro

ゲームマスターを消そう！

Mental Jinro

ゲームマスターを消そう！

ゲームマスターが消えると……

Mental Jinro

ゲームマスターを消そう！

ゲームマスターが消えると……

- チーム分けはどうする？

Mental Jinro

ゲームマスターを消そう！

ゲームマスターが消えると……

- チーム分けはどうする？
- 襲撃された村人の情報をどう伝える？

Mental Jinro

ゲームマスターを消そう！

ゲームマスターが消えると……

- チーム分けはどうする？
- 襲撃された村人の情報をどう伝える？
- 勝敗は誰が判断する？

Mental Jinroを支える技術

Mental Jinroを支える技術
コミットメント

コイントスゲーム

アリスとボブの二人がいるとする

コイントスゲーム

アリスとボブの二人がいるとする

1. アリスがコインの “表” または “裏” を紙に書き、紙を封筒に入れる

コイントスゲーム

アリスとボブの二人がいるとする

1. アリスがコインの “表” または “裏” を紙に書き、紙を封筒に入れる
2. ボブはコインを投げる

コイントスゲーム

アリスとボブの二人がいるとする

1. アリスがコインの “表” または “裏” を紙に書き、紙を封筒に入れる
2. ボブはコインを投げる
3. 封筒から紙を取り出し、
   - アリスの予想とコインの結果が同じなら、アリスの勝利
   - アリスの予想とコインの結果が違えば、ボブの勝利

コイントスゲーム

アリスとボブの二人がいるとする

1. アリスがコインの “表” または “裏” を紙に書き、紙を封筒に入れる
2. ボブはコインを投げる
3. 封筒から紙を取り出し、
   - アリスの予想とコインの結果が同じなら、アリスの勝利
   - アリスの予想とコインの結果が違えば、ボブの勝利
4. このゲームは電話上で行う

コイントスゲーム

アリスとボブの二人がいるとする

1. アリスがコインの“表”または“裏”を紙に書き、紙を封筒に入れる
2. ボブはコインを投げる
3. 封筒から紙を取り出し、
   - アリスの予想とコインの結果が同じなら、アリスの勝利
   - アリスの予想とコインの結果が違えば、ボブの勝利
4. このゲームは電話上で行う

アリスが予想を反故にする？

コイントスゲーム

アリスとボブの二人がいるとする

1. アリスがコインの“表”または“裏”を紙に書き、紙を封筒に入れる
2. ボブはコインを投げる
3. 封筒から紙を取り出し、
   - アリスの予想とコインの結果が同じなら、アリスの勝利
   - アリスの予想とコインの結果が違えば、ボブの勝利
4. このゲームは電話上で行う

アリスが予想を反故にする？

ボブがアリスの主張を信じない？

コイントスゲーム

プロトコル

[†]整数 $x \bmod p$ かつ $xy \equiv 1 \pmod{p}$ となる逆元 y が存在する x の集合である

コイントスゲーム

プロトコル

1. ボブは $p = 2q + 1$ となる大きな素数 p, q をランダムに生成して、$\mathbb{Z}_p^{*\dagger}$ の位数 q の部分群 G から生成元 g, v をランダムに選択して p, q, g, v をアリスへ送信する

---

†整数 $x \bmod p$ かつ $xy \equiv 1 \pmod{p}$ となる逆元 y が存在する x の集合である

コイントスゲーム

プロトコル

1. ボブは $p = 2q + 1$ となる大きな素数 p, q をランダムに生成して、$\mathbb{Z}_p^{*\dagger}$ の位数 q の部分群 G から生成元 g, v をランダムに選択して p, q, g, v をアリスへ送信する
2. アリスは p, q, g, v を検証し、表と予想するなら $m := 1$ を選択し、裏と予想するなら $m := q - 1$ を選択し、乱数 $r \in \{1, \ldots, q-1\}$ を用いて $c := g^r v^m \bmod p$ 計算し c をボブへ送信する

---

†整数 $x \bmod p$ かつ $xy \equiv 1 \pmod{p}$ となる逆元 y が存在する x の集合である

コイントスゲーム

プロトコル

1. ボブは $p = 2q + 1$ となる大きな素数 p, q をランダムに生成して、$\mathbb{Z}_p^{*\dagger}$ の位数 q の部分群 G から生成元 g, v をランダムに選択して p, q, g, v をアリスへ送信する
2. アリスは p, q, g, v を検証し、表と予想するなら $m := 1$ を選択し、裏と予想するなら $m := q - 1$ を選択し、乱数 $r \in \{1, \ldots, q-1\}$ を用いて $c := g^r v^m \bmod p$ 計算し c をボブへ送信する
3. ボブはコイントスをして、結果をアリスへ送信する

---

†整数 $x \bmod p$ かつ $xy \equiv 1 \pmod{p}$ となる逆元 y が存在する x の集合である

コイントスゲーム

プロトコル

1. ボブは $p = 2q + 1$ となる大きな素数 p, q をランダムに生成して、$\mathbb{Z}_p^{*\dagger}$ の位数 q の部分群 G から生成元 g, v をランダムに選択して p, q, g, v をアリスへ送信する
2. アリスは p, q, g, v を検証し、表と予想するなら $m := 1$ を選択し、裏と予想するなら $m := q - 1$ を選択し、乱数 $r \in \{1, \ldots, q-1\}$ を用いて $c := g^r v^m \bmod p$ 計算し c をボブへ送信する
3. ボブはコイントスをして、結果をアリスへ送信する
4. アリスは r, m を公開する

---

†整数 $x \bmod p$ かつ $xy \equiv 1 \pmod{p}$ となる逆元 y が存在する x の集合である

コイントスゲーム

プロトコル

1. ボブは $p = 2q + 1$ となる大きな素数 p, q をランダムに生成して、$\mathbb{Z}_p^{*\dagger}$ の位数 q の部分群 G から生成元 g, v をランダムに選択して p, q, g, v をアリスへ送信する
2. アリスは p, q, g, v を検証し、表と予想するなら $m := 1$ を選択し、裏と予想するなら $m := q - 1$ を選択し、乱数 $r \in \{1, \ldots, q-1\}$ を用いて $c := g^r v^m \bmod p$ 計算し c をボブへ送信する
3. ボブはコイントスをして、結果をアリスへ送信する
4. アリスは r, m を公開する
5. ボブは $c \equiv g^r v^m \pmod{n}$ を検証する

---

†整数 $x \bmod p$ かつ $xy \equiv 1 \pmod{p}$ となる逆元 y が存在する x の集合である

目次