
奢り・割勘プロトコル

吉村 優 (YOSHIMURA Hikaru)

hikaru_yoshimura@r.recruit.co.jp

株式会社リクルート (Recruit Co., Ltd)

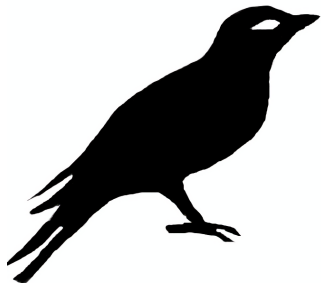
January 25, 2023 @ 社会人語学プロ開 2023 年 3 月期 4Q 部会

<https://github.com/y-yu/fair-or-all-slide> (88215f8)

目次

- ① はじめに
- ② 奢り・割勘問題
- ③ 従来手法
- ④ 提案手法
- ⑤ まとめ

自己紹介



Twitter @_yyu_

Qiita yyu

GitHub y-yu

- 筑波大学 情報学群 情報科学類卒 (2011-15, 学士)
 - プログラム論理研究室、WORD 編集部
- ドワンゴ ニコニコ動画 アカウントチーム
- 未踏ターゲット 2018 (ゲート式量子コンピュータ)
- CTF (<https://urandom.team/>)
 - SECCON CTF 2022 で世界 57 位 (国内 20 位)
- プログラミング
 - Scala, \LaTeX , Rust, Go, Swift

奢り・割勘問題



夜星

@Y_N_Hoshi · [Follow](#)



年収1500万円の男と付き合って7万の温泉で2万出させられて、昼のカフェ代や夜ご飯もたまに出させられることに不満を感じている女性を見かけたが.....それは正しいです。全然余裕で出せるところなので付き合っているレベルでその程度を奢らないのなら男として終わりです。

11:28 PM · Dec 15, 2022



[Read the full conversation on Twitter](#)



22.2K



Reply



Copy link

[Read 999 replies](#)

[1]

奢り・割勘問題

“

アリスとボブの飲食費について下記のいずれにするか決定する問題

- ① ボブが全額を奢る
- ② 割勘とする

”

アリス (Alice)



ボブ (Bob)



従来手法① – コイントス

従来手法① – コイントス

- ① 2人でコイントスを行う

従来手法① – コイントス

- ① 2人でコイントスを行う
- ② 表1に基づいて決定する

表 1: コインの意味

コインの結果	意味
表	ボブの奢り
裏	割勘

従来手法① – コイントス

- ① 2人でコイントスを行う
- ② 表1に基づいて決定する

表 1: コインの意味

コインの結果	意味
表	ボブの奢り
裏	割勘

2人の意見が何も反映されないため
プライバシーは完全🙊



従来手法① – コイントス

- ① 2人でコイントスを行う
- ② 表1に基づいて決定する

表 1: コインの意味

コインの結果	意味
表	ボブの奢り
裏	割勘

2人の意見が何も反映されないため
プライバシーは完全👤



しかしゲーム性は全くない



従来手法① – コイントス

そもそもこのゲームはアリスが有利👹



従来手法① – コイントス

そもそもこのゲームはアリスが有利👹



そもそも不公平なゲームなので、
50:50 ではおもしろくない



- ボブが支払うのは安目で 50% 高目で 100%だが、一方でアリスは安目 0%高目でも 50%

従来手法② – 公平な第三者を用いた AND 計算

従来手法② – 公平な第三者を用いた AND 計算

- ① アリスとボブは公平な第三者チャーリーに **希望** $\in \{\text{奢り}, \text{割勘}\}$ を渡す

従来手法② – 公平な第三者を用いた AND 計算

- ① アリスとボブは公平な第三者チャーリーに **希望** $\in \{\text{奢り}, \text{割勘}\}$ を渡す
- ② チャーリーはアリス・ボブの希望を次の表 2 に基づいて AND 演算する

表 2: 奢り・割勘 AND 演算

アリス	ボブ	結果
割勘	割勘	割勘
割勘	奢り	割勘
奢り	割勘	割勘
奢り	奢り	奢り

従来手法② – 公平な第三者を用いた AND 計算

- ① アリスとボブは公平な第三者チャーリーに **希望** $\in \{\text{奢り}, \text{割勘}\}$ を渡す
- ② チャーリーはアリス・ボブの希望を次の表 2 に基づいて AND 演算する
- ③ チャーリーが結果を 2 人に通知する

表 2: 奢り・割勘 AND 演算

アリス	ボブ	結果
割勘	割勘	割勘
割勘	奢り	割勘
奢り	割勘	割勘
奢り	奢り	奢り

従来手法② – 公平な第三者を用いた AND 計算

- ① アリスとボブは公平な第三者チャーリーに **希望** $\in \{\text{奢り}, \text{割勘}\}$ を渡す
- ② チャーリーはアリス・ボブの希望を次の表 2 に基づいて AND 演算する
- ③ チャーリーが結果を 2 人に通知する

表 2: 奢り・割勘 AND 演算

アリス	ボブ	結果
割勘	割勘	割勘
割勘	奢り	割勘
奢り	割勘	割勘
奢り	奢り	奢り

- ボブは期待値は $\frac{5}{8}$ (62.5%) の支払い、アリスは期待値 $\frac{3}{8}$ (37.5%) の支払い

従来手法② – 公平な第三者を用いた AND 計算

そもそもチャーリーが信頼できるのか？



従来手法② – 公平な第三者を用いた AND 計算

そもそもチャーリーが信頼できるのか？



次のケース👉で**情報リーク**が生じる！

- ① アリスが奢り、ボブは割勘を希望
- ② アリスが割勘、ボブは奢りを希望
- ③ アリスが奢り、ボブは奢りを希望



- AND 計算なので片方の入力
と結果から、残りの入力を逆
算できる場合がある

従来手法② – 公平な第三者を用いた AND 計算

希望が場合によっては流出するのは
ゲーム性とみなすことができそう！ 😈



従来手法② – 公平な第三者を用いた AND 計算

希望が場合によっては流出するのは
ゲーム性とみなすことができそう！ 😈



しかしこの方法では
アリスの希望は絶対にリークしない 😡



- たとえば「アリスが奢り・ボブは割勘を希望」のとき、結果は割勘となる
- アリスは奢ってもらえないが、ボブのケチさを知ることができる
- しかしアリスのがめつさ情報がリークすることはない

従来手法② – 公平な第三者を用いた AND 計算

希望が場合によっては流出するのは
ゲーム性とみなすことができそう！ 😈



しかしこの方法では
アリスの希望は絶対にリークしない 😡



- たとえば「アリスが奢り・ボブは割勘を希望」のとき、結果は割勘となる
- アリスは奢ってもらえないが、ボブのケチさを知ることができる
- しかしアリスのがめつさ情報がリークすることはない
- なぜなら**衝突**したときに“奢り”になるケースがないから

2人の希望の衝突

2人の希望の衝突

2人の希望が一致したケースなら
AND 計算で問題ない



表 3: 現状のコンセンサス

アリス	ボブ	
割勘	割勘	} 🧑
奢り	奢り	
割勘	奢り	} 🧑
奢り	割勘	

2人の希望の衝突

2人の希望が一致したケースなら
AND 計算で問題ない



一方で衝突 (*conflict*) した
ケースは考える必要がある



表 3: 現状のコンセンサス

アリス	ボブ	
割勘	割勘	}
奢り	奢り	
割勘	奢り	}
奢り	割勘	

① はじめに

② 奢り・割勘問題

③ 従来手法

④ 提案手法

⑤ まとめ

コイントス

AND計算



ハイブリッドプロトコル

コイントスとAND計算のハイブリッドプロトコル

表 4: 奢り・割勘と情報リーク

表 4 のようにランダム[§]を導入したうえで、
不本意な結果を強いられた側だけが
相手の希望を得るといえるのはどうか？



アリス	ボブ	結果	情報
割勘	割勘	割勘	†
割勘	奢り	ランダム	‡
奢り	割勘	ランダム	‡
奢り	奢り	奢り	†

[§]コイントス同様に奢り・割勘それぞれ $\frac{1}{2}$ の確率

†お互いの希望はいずれもリークしない

‡結果が奢りの場合はアリスの希望がボブへ、
結果が割勘の場合はボブの希望がアリスへリーク
する

このプロトコルはチャーリー (*trusted third party*) **なし**で達成できる

手順

このプロトコルはチャリー (trusted third party) なしで達成できる

- ① アリス・ボブに2枚のカード \heartsuit , \clubsuit を配る[†]
- ② アリス・ボブは表5に従って希望を裏向き $\boxed{?}$ にして提出する
- ③ ②で提出されたカードをシャッフルする
- ④ どちらか1枚をドローして表向きにする
- ④のカードを表5に対応させてプロトコルの結果とする

表 5: カードの意味

カード	意味
\heartsuit	ボブの奢り
\clubsuit	割勘

[†]これらのカードはトランプのようにいずれも裏が $\boxed{?}$ となっており、裏向きになった状態でどちらのカードなのか特定することができない

ケーススタディ①－2人の希望が一致

ケーススタディ① – 2人の希望が一致


- 2人の希望が一致しているので次のようなケース



ケーススタディ① – 2人の希望が一致

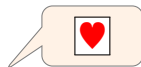
- 2人の希望が一致しているので次のようなケース



- これらをシャッフルして1枚選んだときは必ずとなる

ケーススタディ① – 2人の希望が一致

- 2人の希望が一致しているので次のようなケース



- これらをシャッフルして1枚選んだときは必ず♥となる
 - そしてこのときアリス・ボブは相手のカードについて
 - 両方とも♥だったのか
 - 相手は♣だったがランダムで♥が選ばれたのか
- 👉 のどちらなのか分からず、情報リークはない

ケーススタディ②－2人の希望が衝突

- 2人の希望が衝突しているので次のようなケース



ケーススタディ②－2人の希望が衝突

- 2人の希望が衝突しているので次のようなケース



- これらをシャッフルしてランダムに選べば、結果は♥,♣それぞれ $\frac{1}{2}$ の確率になる

ケーススタディ②－2人の希望が衝突

- 2人の希望が衝突しているので次のようなケース



- これらをシャッフルしてランダムに選べば、結果は♥,♣それぞれ $\frac{1}{2}$ の確率になる

結果が♥

- アリスの希望通りとなるが、結果がボブの希望通りかランダムか不明
- ボブは衝突してアリスの希望♥になったと特定

ケーススタディ②－2人の希望が衝突

- 2人の希望が衝突しているので次のようなケース



- これらをシャッフルしてランダムに選べば、結果は♥,♣それぞれ $\frac{1}{2}$ の確率になる

結果が♥

- アリスの希望通りとなるが、結果がボブの希望通りかランダムか不明
- ボブは衝突してアリスの希望♥になったと特定

結果が♣ 同様

コイントスと AND 計算のハイブリッドプロトコル

期待值的にはボブが不公平なままだが、
もし不本意に奢った場合はアリスのがめつさが分かる



コイントスと AND 計算のハイブリッドプロトコル

期待值的にはボブが不公平なままだが、
もし不本意に奢った場合はアリスのがめつさが分かる



このときアリスはボブの奢りが本意か
不本意か分からないが、奢られを得る



コイントスとAND計算のハイブリッドプロトコル

逆にアリスが不本意に
割勘となってしまった場合、
ボブの希望は割勘だと特定する



- アリスが不本意に割勘となった場合、アリスは奢りを希望していたがボブは割勘を希望しており、ランダムで割勘となった

コイントスとAND計算のハイブリッドプロトコル

逆にアリスが不本意に
割勘となってしまった場合、
ボブの希望は割勘だと特定する



しかしこのときボブは
アリスの希望が分からない



- アリスが不本意に割勘となった場合、アリスは奢りを希望していたがボブは割勘を希望しており、ランダムで割勘となった
- このように希望通りになった側は相手の希望が分からず、希望通りにならなかった側は相手の希望を知ることができる

まとめ

まとめ

- 簡単なプロトコルで奢り・割勘問題に決着をつけられるかもしれない
 - 2人の参加者は安目・高目と情報を賭博する

まとめ

- 簡単なプロトコルで奢り・割勘問題に決着をつけられるかもしれない
 - 2人の参加者は安目・高目と情報を賭博する
- 今回紹介した技術は“Covert Lottery[2]”という名前が付いている
 - Covert Lottery を量子コンピュータでやるという記事 [3] を過去に書いた

まとめ

- 簡単なプロトコルで奢り・割勘問題に決着をつけられるかもしれない
 - 2人の参加者は安目・高目と情報を賭博する
- 今回紹介した技術は“Covert Lottery[2]”という名前が付いている
 - Covert Lottery を量子コンピュータでやるという記事 [3] を過去に書いた
- 今回は2人だったが、これを多人数拡張すると別のゲームに使えるかも

参考文献

- [1] @Y_N_Hoshi tweet.
https://twitter.com/Y_N_Hoshi/status/1603396700453871618.
Accessed: 2023-01-25.
- [2] Yuto Shinoda, Daiki Miyahara, Kazumasa Shinagawa, Takaaki Mizuki, and Hideaki Sone.
Card-Based Covert Lottery.
In Diana Maimut, Andrei-George Oprina, and Damien Sauveron, editors, *Innovative Security Solutions for Information Technology and Communications*, pp. 257–270, Cham, 2021. Springer International Publishing.
- [3] 量子コンピュータで2人の“Covert”！？ ガチャ.
<https://zenn.dev/yyu/articles/79c6c48226166aa0e875>.
Accessed: 2023-01-25.

Thank you for the attention!