IBISML2010

秘密の忠告からのオンライン予測

筑波大学 コンピュータサイエンス専攻
科学技術振興機構 さきがけ
佐久間 淳

シナリオ

- 株価予測
  - N人の株価予測エキスパートがいる
  - 各エキスパートは自分の予測関数や予測を他のエキスパートに明かしたくない
  - しかし全員の知恵を集めればよりよい予測ができるかもしれないと思っている

シナリオ

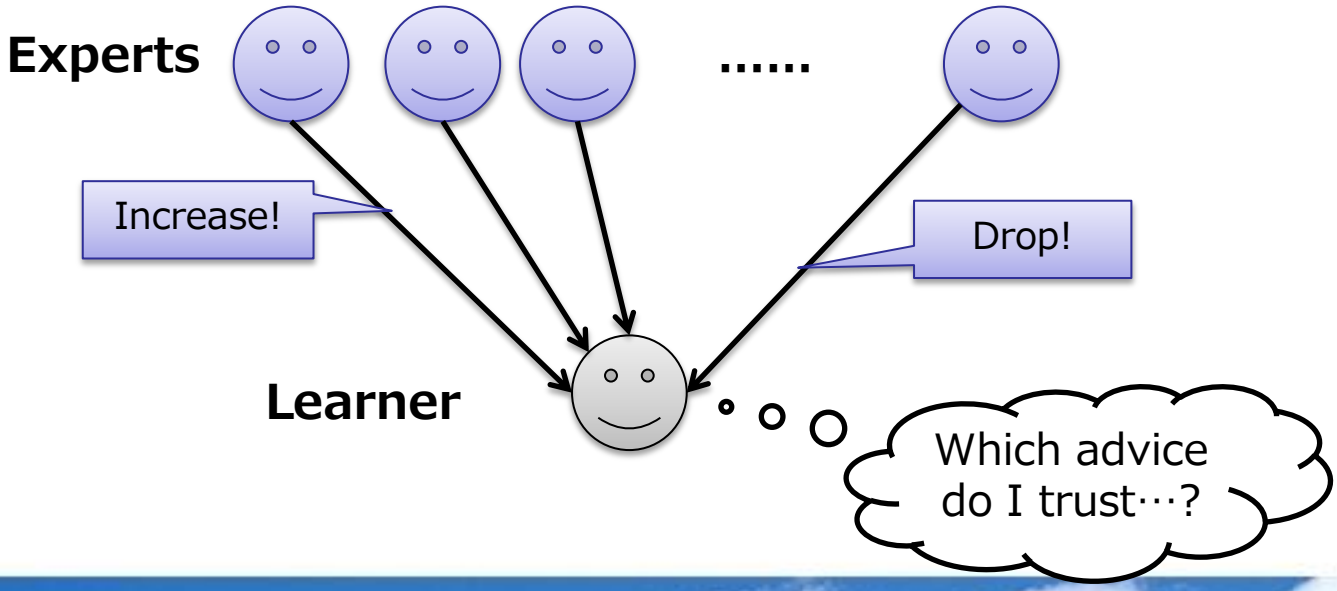
- 株価予測
  - N人の株価予測エキスパートがいる
  - 各エキスパートは自分の予測関数や予測を他のエキスパートに明かしたくない
  - しかし全員の知恵を集めればよりよい予測ができるかもしれないと思っている
- 感染病流行予測
  - 感染病の流行を予測しようとしているN個の病院がある
  - 個々の病院のカルテやその分析結果は、患者のプライバシーを考慮すると開示できない
  - しかし全病院の予測結果を集約できれば、感染病の流行を正確に予測できるかもしれない

シナリオ

- 株価予測
  - N人の株価予測エキスパートがいる
  - 各エキスパートは自分の予測関数や予測を他のエキスパートに明かしたくない
  - しかし全員の知恵を集めればよりよい予測ができるかもしれないと思っている
- 感染病流行予測
  - 感染病の流行を予測しようとしているN個の病院がある
  - 個々の病院のカルテやその分析結果は、患者のプライバシーを考慮すると開示できない
  - しかし全病院の予測結果を集約できれば、感染病の流行を正確に予測できるかもしれない
- **それぞれの予測を他に開示せずによりよい予測は可能か？**

オンライン予測:株価予測を例に

- For t=1,2,…,T:
  1. エキスパート: 忠告「株価は “騰がる ($y_{i,t}$=1)” or “下がる($y_{i,t}$=0)”」を開示
  2. 学習者: エキスパートの忠告を基に予測$y_{H,t}$ を生成
  3. 環境(マーケット): 株価y_t を開示
  4. エキスパート: 自身の予測に対する損失 l (y_t, $y_{i,t}$)を受ける
  5. 学習者: 自身の予測に対する損失 l (y_t, $y_{H,t}$) を受ける



Regret minimization

- 評価基準：regret
  - 期間Tにおいて、結果的に最も少ない損失を被ったエキスパートに対して、学習者はどの程度損失が多かったか

$$R_{\mathrm{H},\mathrm{T}} = \underbrace{L_{\mathrm{H},T}}_{\text{学習者Hの損失和}} - \underbrace{\min_i L_{i,T}}_{\text{最も少ない損失和を被ったエキスパートの損失和}}$$

Regret minimization

- 評価基準：regret
  - 期間Tにおいて、結果的に最も少ない損失を被ったエキスパートに対して、学習者はどの程度損失が多かったか

$$R_{\mathrm{H},\mathrm{T}} = \underbrace{L_{\mathrm{H},T}}_{\text{学習者Hの損失和}} - \underbrace{\min_i L_{i,T}}_{\text{最も少ない損失和を被ったエキスパートの損失和}}$$

- 目標:　$R_{H,T} < O(T)$
  - $T \to \infty$ の極限において$R_{H,T}$ は消失 (a.k.a. **Hannan consistency**)
  - 期間が十分長ければ、最良のエキスパートと同等程度の損失ですむ
- この目標を達成するために、学習者はどのような戦略をとればよいか？

Exponential Weighting Scheme

- 戦略
  - よい予測をしているエキスパートは選ばれやすいように
  - 悪い予測をしているエキスパートは選ばれにくいように

Exponential Weighting Scheme

- 戦略
  - よい予測をしているエキスパートは選ばれやすいように
  - 悪い予測をしているエキスパートは選ばれにくいように

1. 各エキスパートついて重みw_{it}を毎ステップ更新

$$w_{i,t} = \exp\left(-\eta \underbrace{\sum_{s=1}^{t-1} \ell(y_{i,s}, y_s)}_{\text{i番目のエキスパートの累積損失}}\right)$$

Exponential Weighting Scheme

- 戦略
  - よい予測をしているエキスパートは選ばれやすいように
  - 悪い予測をしているエキスパートは選ばれにくいように

1. 各エキスパートついて重みw_{it}を毎ステップ更新

$$w_{i,t} = \exp\left(-\eta \underbrace{\sum_{s=1}^{t-1} \ell(y_{i,s}, y_s)}_{\text{i番目のエキスパートの累積損失}}\right)$$

2. 重みw_{it}を正規化

$$p_{i,t} = \frac{w_{i,t}}{\sum_{j=1}^{N} w_{j,t}}$$

Exponential Weighting Scheme

- 戦略
  - よい予測をしているエキスパートは選ばれやすいように
  - 悪い予測をしているエキスパートは選ばれにくいように

1. 各エキスパートついて重みw_{it}を毎ステップ更新

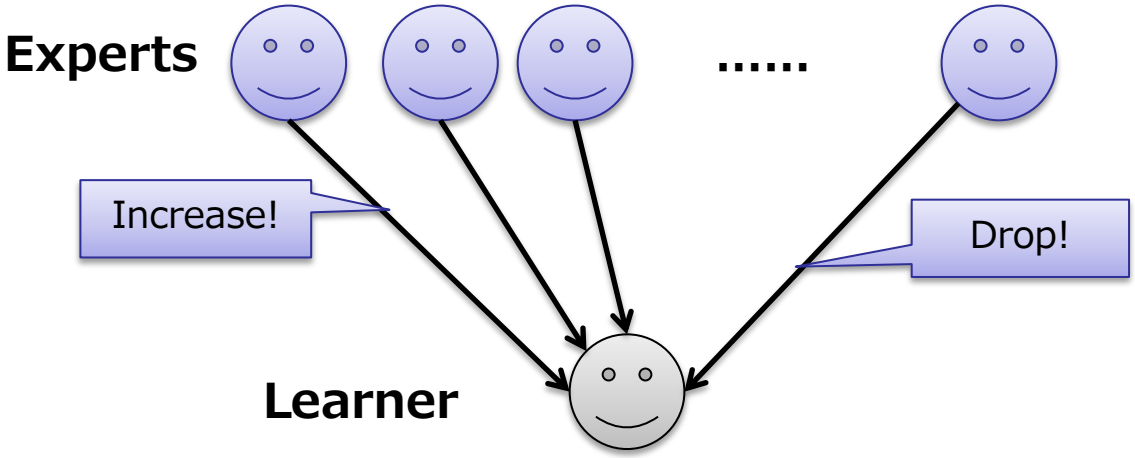
$$w_{i,t} = \exp\left(-\eta \underbrace{\sum_{s=1}^{t-1} \ell(y_{i,s}, y_s)}_{\text{i番目のエキスパートの累積損失}}\right)$$

2. 重みw_{it}を正規化

$$p_{i,t} = \frac{w_{i,t}}{\sum_{j=1}^{N} w_{j,t}}$$

3. p_{it}による予測の決定
   1. p_{it}に比例する確率でエキスパートを一つ選択 (jとする)
   2. y_{jt}を時刻tの学習者の予測とする

完全情報モデル

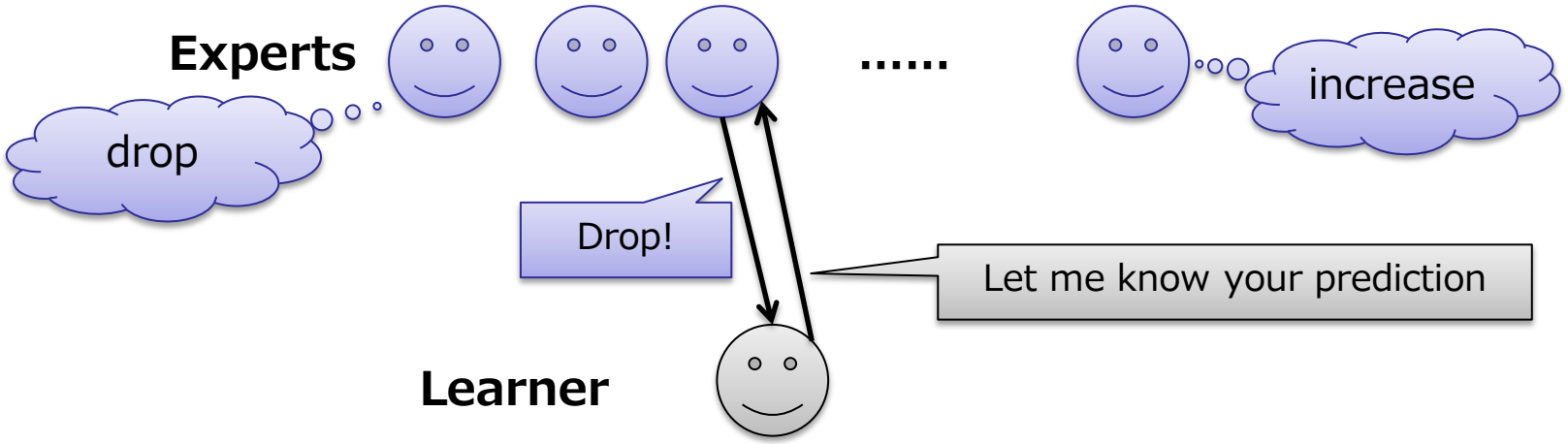


- 完全情報モデル (eg. Exponential weighting)
  - 学習者はすべてのエキスパートの忠告と損失を観測可能
  - Exponential weighting LearnerのRegret bound[Vovk90]

$$R_{\mathrm{EW},T} \leq \sqrt{2T \ln N}$$ Hannan cosistent!

T:ラウンド数、N: エキスパート数

部分情報モデル



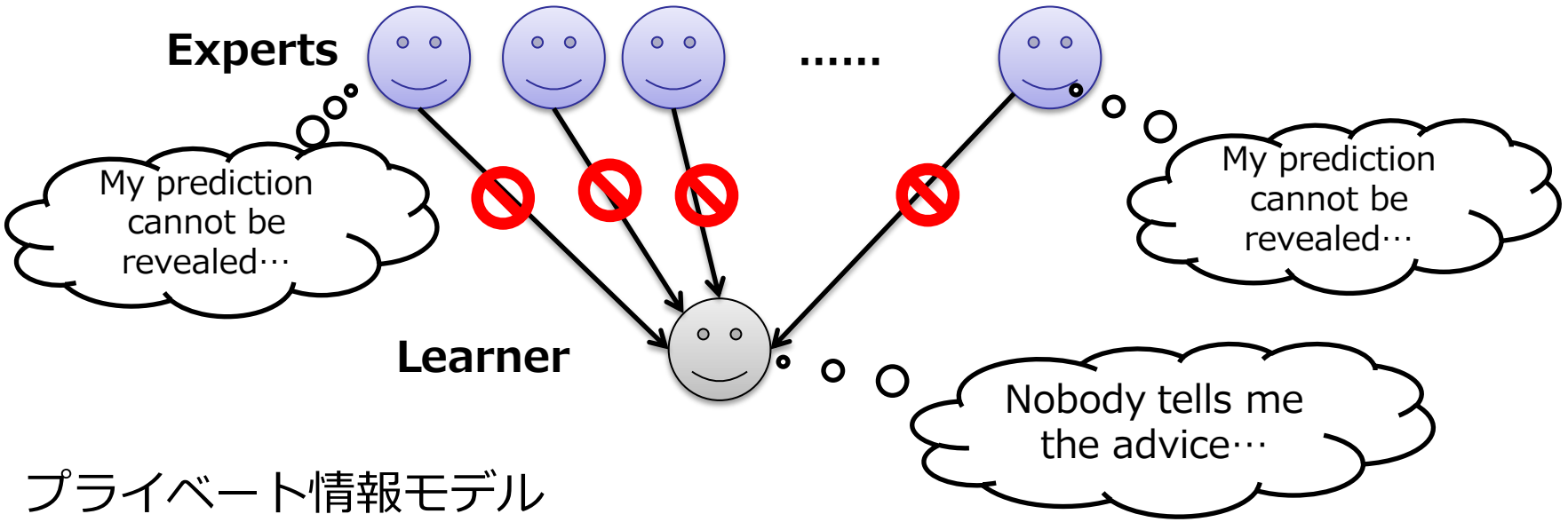
- 部分情報モデル (eg. Exp3 [Auer et. al. 2003])
  - あらかじめ決めたエキスパートからのみ忠告と損失を観測
  - Exp3 learnerのRegret bound

Hannan cosistent!

$$R_{\mathrm{Exp3},T} \leq 2\sqrt{e-1}\sqrt{NT\ln N}$$

- エキスパートからの秘密の忠告を扱うにはまだ不足
- 実現したいシナリオはもっと制限の厳しい情報モデル

プライベート情報モデル



- プライベート情報モデル
  - エキスパートも学習者も互いに予測と損失を一切開示したくない
  - Hannnan consistentなオンライン予測はほとんど不可能に見えるが？

プライベート情報モデルにおけるExponential Weighting

1. 各エキスパートついて重みw_{it}を毎ステップ更新

$$w_{i,t} = \exp\left(-\eta \underbrace{\sum_{s=1}^{t-1} \ell(y_{i,s}, y_s)}_{\text{i番目のエキスパートの累積損失}}\right)$$

各エキスパートがローカルで計算可能

このルーレット選択を解決するoblivious rouletteを考える

2. 重みw_{it}を正規化

$$p_{i,t} = \frac{w_{i,t}}{\sum_{j=1}^{N} w_{j,t}}$$

ローカルで計算できない

3. p_{it}による予測の決定
   1. p_{it}に比例する確率でエキスパートを一つ選択(jとする)
   2. y_{jt}を時刻tの学習者の予測とする

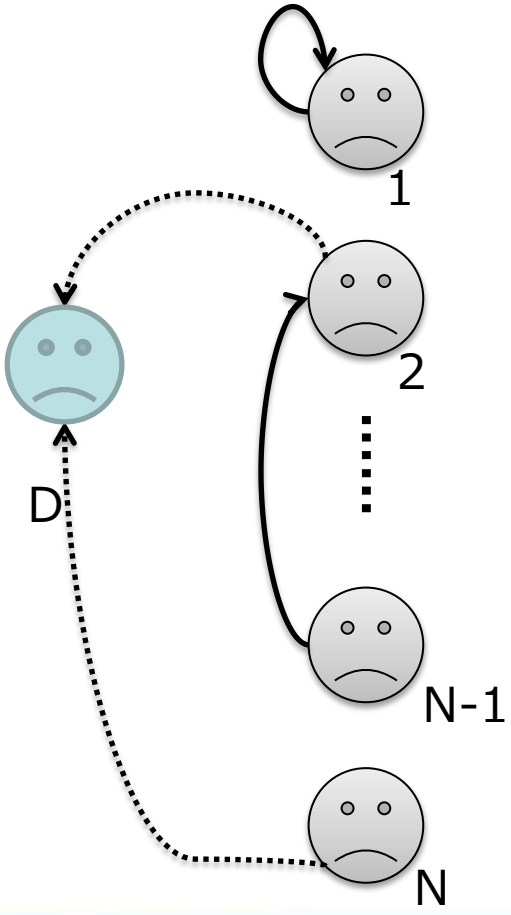
ローカルで計算できない

Oblivious rouletteの直感的な理解

エキスパート

学習者

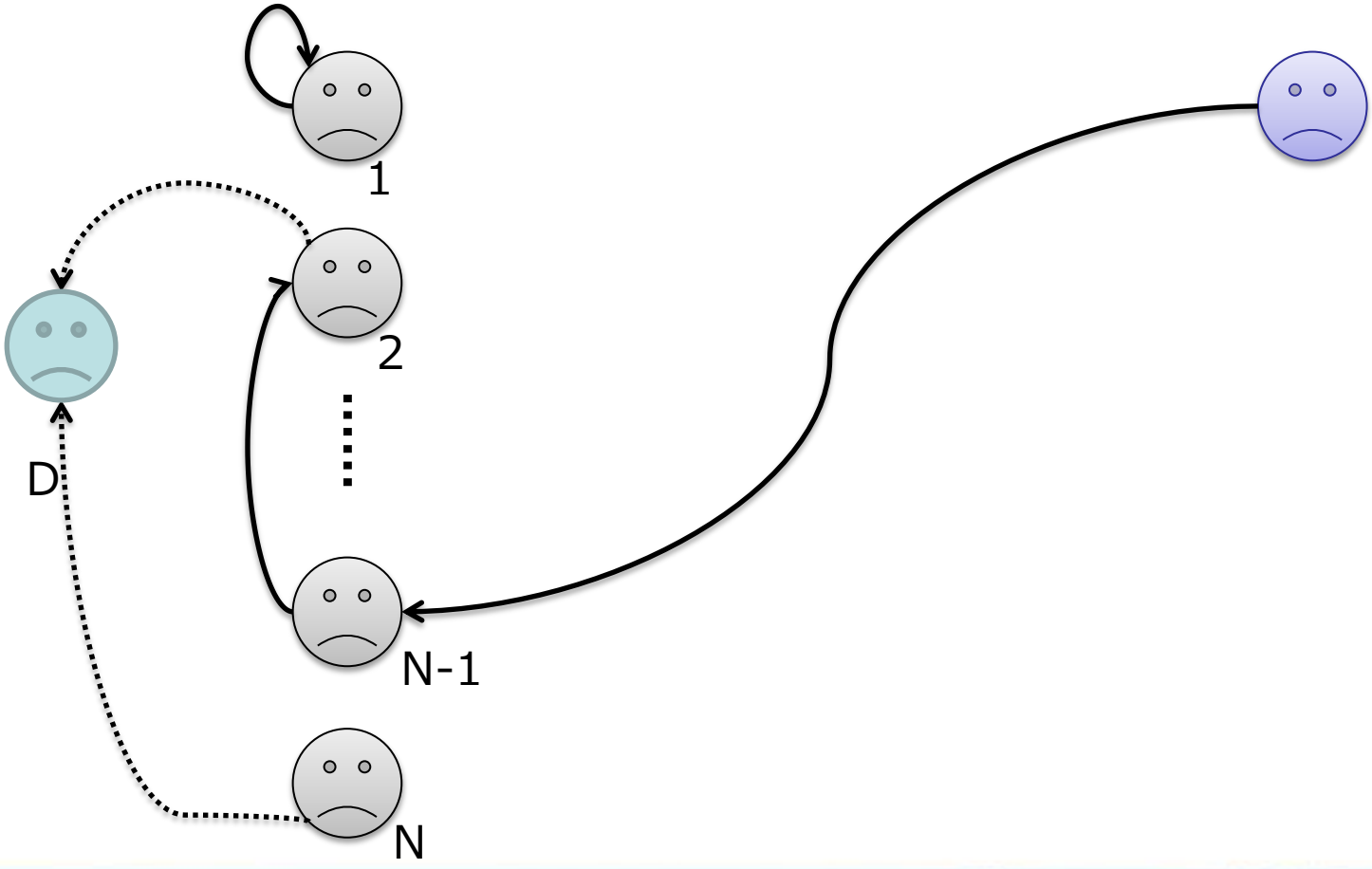
1．エキスパートを確率w_iでランダムに一人指名
それ以外の場合は存在しないエキスパートを指名



Oblivious rouletteの直感的な理解

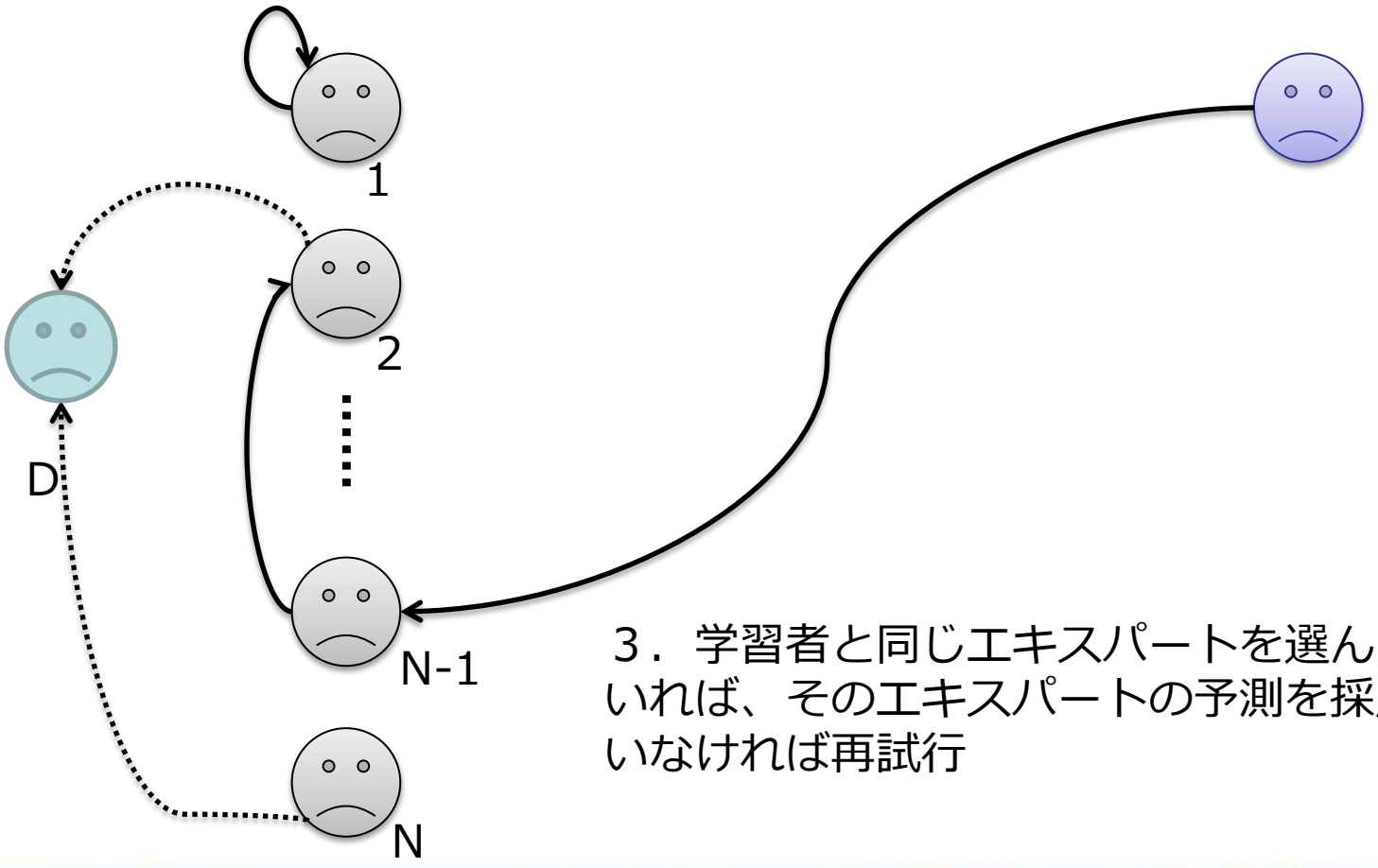
エキスパート　　**学習者**

2．エキスパートをランダムに一人指名



Oblivious rouletteの直感的な理解

エキスパート　　学習者



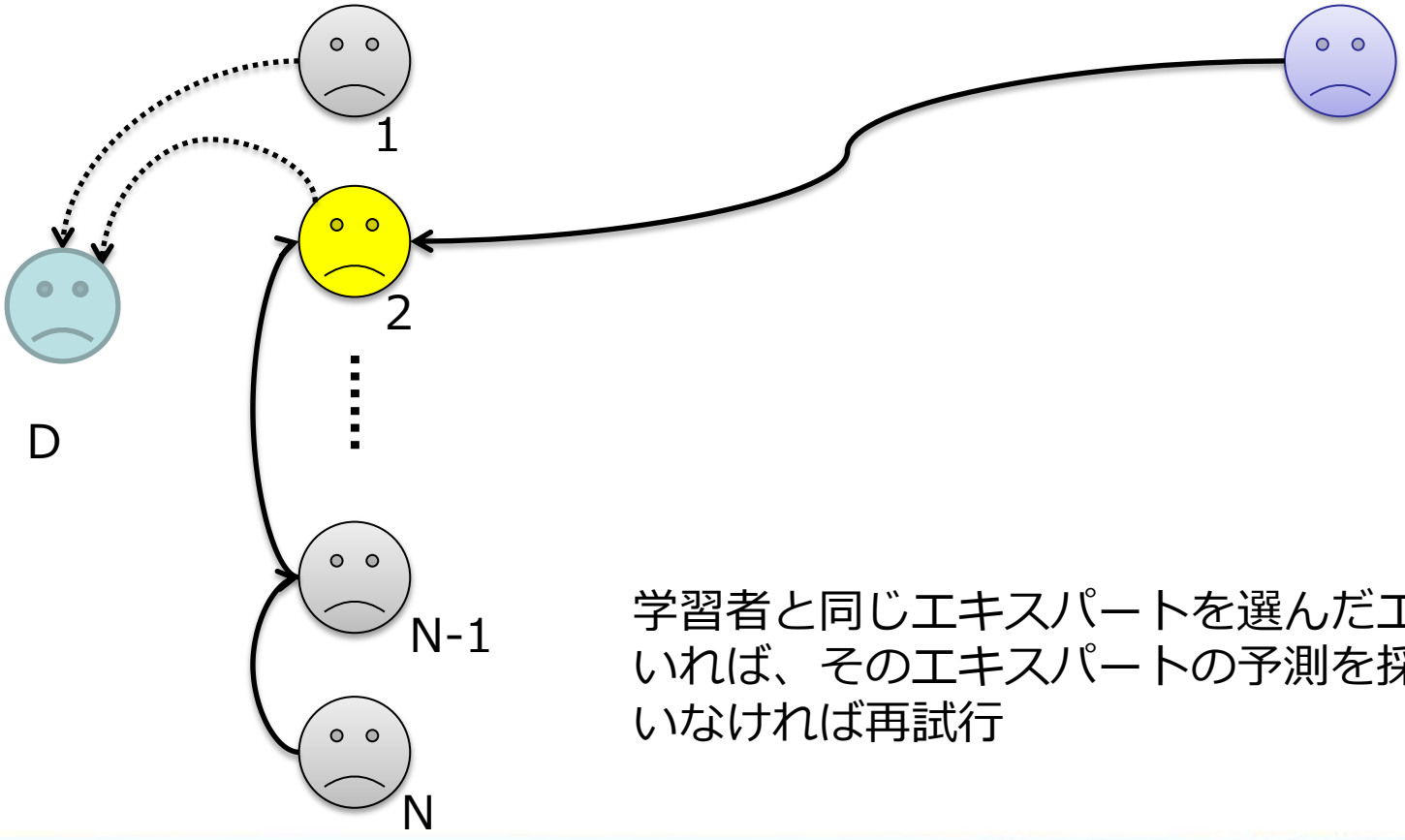
３．学習者と同じエキスパートを選んだエキスパートがいれば、そのエキスパートの予測を採用、
いなければ再試行

Oblivious rouletteの直感的な理解

エキスパート

学習者

エキスパートをランダムに一人指名



学習者と同じエキスパートを選んだエキスパートがいれば、そのエキスパートの予測を採用
いなければ再試行

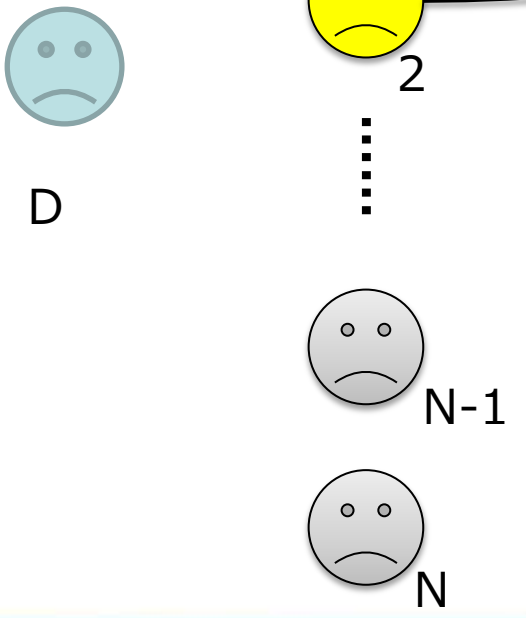
Oblivious rouletteの直感的な理解

エキスパート

学習者

エキスパートをランダムに一人指名

エキスパート2の予測を採用



こうすることで…

$$p_{i,t} = \frac{w_{i,t}}{\sum_{j=1}^{N} w_{j,t}}$$ に従うルーレット選択が実現

ただし、誰がどんな予測をしたか、学習者はどんな予測を得たか、などは知られてしまう

準同形性公開鍵暗号によるoblivious rouletteの構築

- m ∈ Z_N をメッセージ, r ∈ Z_N を乱数とする
- (pk, sk): 公開鍵と秘密鍵のペア
  - 暗号化: $c \leftarrow \mathrm{Enc}_{p_k}(m_0; r_0)$
  - 複号化: $m_0 \leftarrow \mathrm{Dec}_{s_k}(c)$
- m0,m1, r1,r2 ∈ Z_N
- 暗号系が(加法的)準同型性を持つとき:
  - 暗号文の和

$$\mathrm{Enc}_{p_k}(m_0; r_0) \cdot \mathrm{Enc}_{p_k}(m_1; r_1) = \mathrm{Enc}_{p_k}(m_0 + m_1; r_1 \cdot r_2)$$

  - 暗号文と平文の積

$$\mathrm{Enc}_{p_k}(m_0; r_0)^{m_1} = \mathrm{Enc}_{p_k}(m_0 m_1; r')$$

- これを使ってルーレット選択の結果のみが学習者に伝わるような計算法を開発

Oblivious roulette protocol

各エキスパート

1. エキスパートをランダムに一人指名 (j_k'とする)し、以下を評価

$$a_{i,k} \leftarrow \begin{cases} j'_k, & \text{with prob. } m_i, \\ Y+1, & \text{otherwise} \end{cases}$$

2. エキスパートは以下を評価し学習者へ送信

$$c_{i,k} \leftarrow \left(\mathrm{Enc}_{\mathrm{pk}}(a_{i,k}) \cdot \mathrm{Enc}_{\mathrm{pk}}(-j_k)\right)^{r_{i,k}} \cdot \mathrm{Enc}_{\mathrm{pk}}(y_i)$$

学習者

1. エキスパートをランダムに一人指名 (j_kとする)

3. プレイヤは(c_{1k},…,c_{Nk})を解読：

$$u_i \leftarrow \mathrm{Dec}_{\mathrm{sk}}(c_{i,k})$$

$u \in_r Y$ ならuを出力、そうでなければ1へ

プロトコルの性質

- **プロトコルの肝**

$$c_{i,k} = \mathrm{Enc}_{\mathrm{pk}}(\underbrace{(a_{i,k} - j_k)r_{i,k}}_{\text{エキスパートの指名jkと学習者の指名が一致すれば0、そうでなければランダムな値をとる}} + \underbrace{y_i}_{\text{エキスパートiの予測}} \bmod N)$$

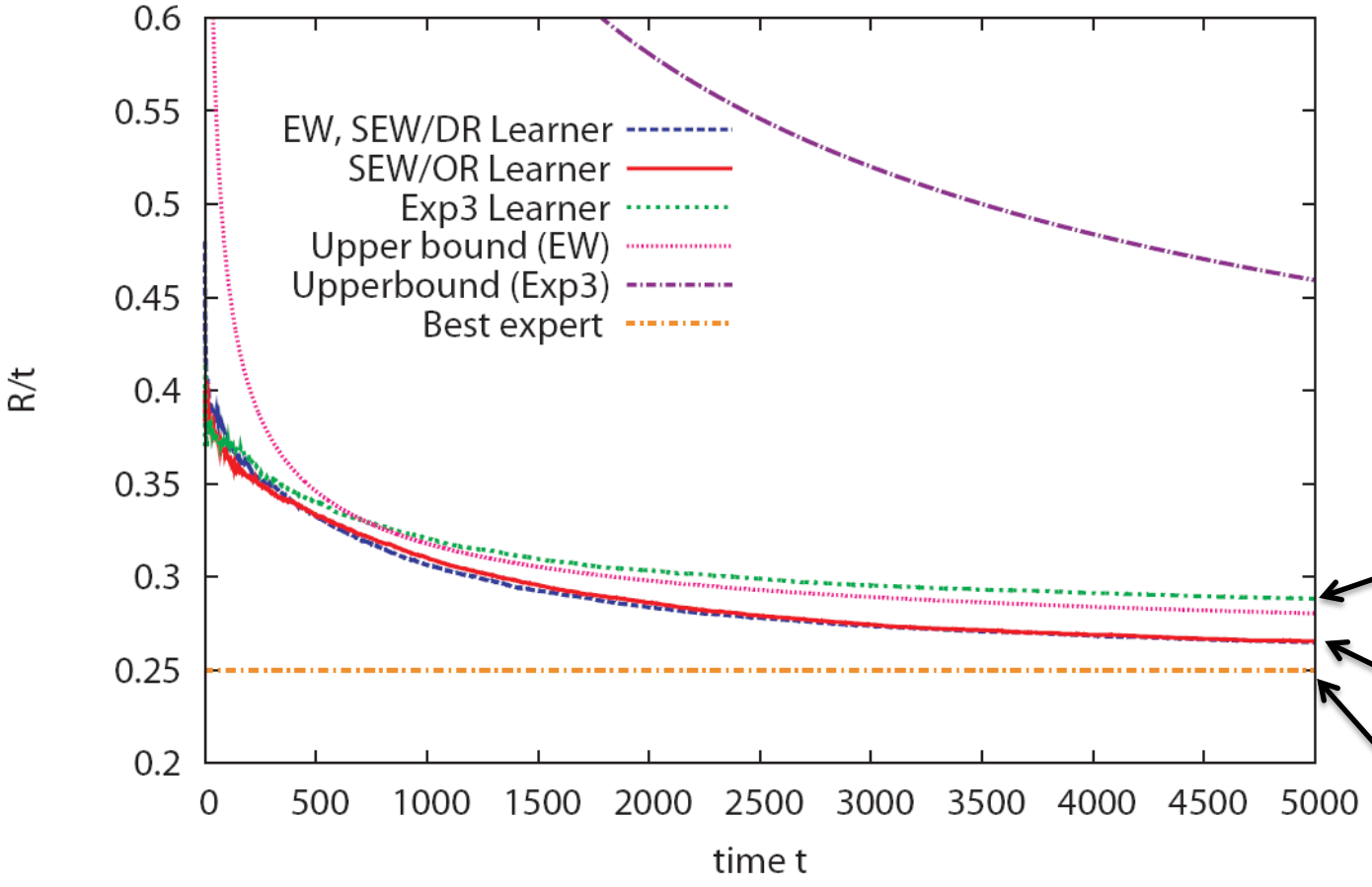
- **Oblivious roulette protocol**
  - ルーレット盤を見ない(見せない)ルーレットを実現
  - エキスパートは互いの予測や重みを他人に見られない
  - 学習者はだれから予測をもらったか、どんな予測を採用したかエキスパートに知られない
  - これをつかうとexponential weightingをプライベート情報モデルで実行できる

この研究の成果

情報モデル	観測可能な情報	Regret bound
完全情報モデル	全エキスパートの損失,予測	$R_{\mathrm{EW},T} \leq \sqrt{2T \ln N}$
部分情報モデル	指名したエキスパートの損失,予測	$R_{\mathrm{Exp3},T} \leq 2\sqrt{e-1}\sqrt{NT \ln N}$
プライベート情報モデル	**他エキスパートの損失,予測は観測できない**	$R_{\mathrm{EW},T} \leq \sqrt{2T \ln N}$

- プライベート情報モデルにおいても…
  - Hannan consistencyを達成できました
  - しかもregret boundは完全情報モデルと同じオーダーです
- 結論：情報を他のエキスパートと共有しなくとも、学習者は完全情報モデルにおけるexponential weightingと同等の予測ができます

Experiments: Regret



Exp3
(partial. info. mdl)

SEW/OR, SEW/DR
(private. info. mdl)

Regret lower
bound

まとめ

- 完全情報モデルと同等の性能を達成。しかも、
  - エキスパートは予測と損失を開示しなくてもよい
  - 学習者も予測と損失を開示しなくともよい
- 拡張
  - いろんなオンライン学習がこれによりプライベート化できるはず…
  - 繰り返しゲームにおけるminmax戦略とregret最小化は等価
    - ペイオフ行列を秘密にたままのminmax均衡の実現
  - Boosting…シナリオ募集中