通信複雑性入門

2015/11/24

泉　泰介（名古屋工業大学）
電子情報通信学会IT研究会(若手研究者のための講演会)

(2者間)通信複雑性

- Alice と Bobが nビットデータ列$x \in X, y \in Y$を保有

  - 問題：関数$f: X \times Y \to Z$が与えられたとき，$f(x, y)$の計算に**最悪何ビットの通信が必要か？**
  - AliceとBobの計算能力は無限
  - 複数ラウンド使っても良い

通信複雑性：背景

- Andrew Chi-Chiu Yao により創始[Yao79]
  - ‘00 Turing award winner

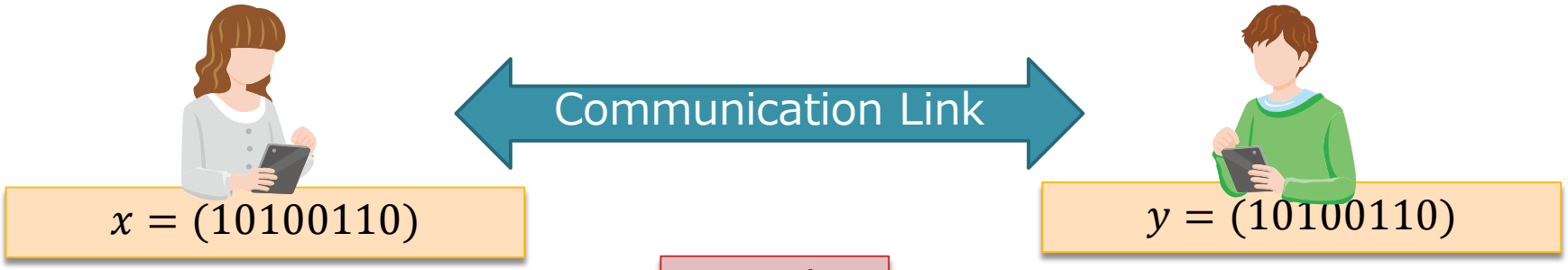
> “In recognition of his fundamental contributions to the theory of computation, including the complexity-based theory of pseudorandom number generation, cryptography, and communication complexity”

  - 計算複雑性の理論における最重要ツールの一つ
    - さまざまな計算モデルでの限界導出に現れる
      - データ構造，オートマトン，論理回路，ストリーム計算
        分散並列計算，学習理論，アルゴリズム的ゲーム理論...

[Yao79]Some Complexity Questions Related to Distributive Computing, In Proc. of STOC, pp.209-213, 1979.

代表的な問題

- 等価性判定（equality）



- 交叉判定（set-disjointness）

x,yともにビット1が立っている位置はないか？($x \cdot y = 0$か？)

決定性プロトコルの動作

- プロトコルはラウンドに従って動作
  - 1ラウンドでAliceかBobのいずれかが自身の状態に従って1ビットメッセージを決定・送信
  - 必ずしも交互に送るわけではない
    - が，漸近的な議論をするならば交互の送信を仮定してOK
  - メッセージは同時に送信されるかもしれない
    - が，ラウンド数に関して議論しない(or漸近的に議論する)ならば逐次的に送信されているとみなす
  - 最終的にAliceとBobは$f(\boldsymbol{x}, \boldsymbol{y})$の値を出力して停止

決定性プロトコル：形式的な定義

- プロトコルPは決定木Tとその頂点/辺への
  ラベル付けにより定義される
- 全ての内部頂点vはある関数$a_v: X \to \{0,1\}$あるいは
  $b_v: Y \to \{0,1\}$でラベル付け
  - 次に送信される(1ビット)メッセージを決める関数
- 全ての葉頂点はZ(fの値域)中の要素でラベル付け
- 左の子への辺には0,右の子への辺には1が
  ラベル付け(これは冗長であるが，わかりやすさのため)

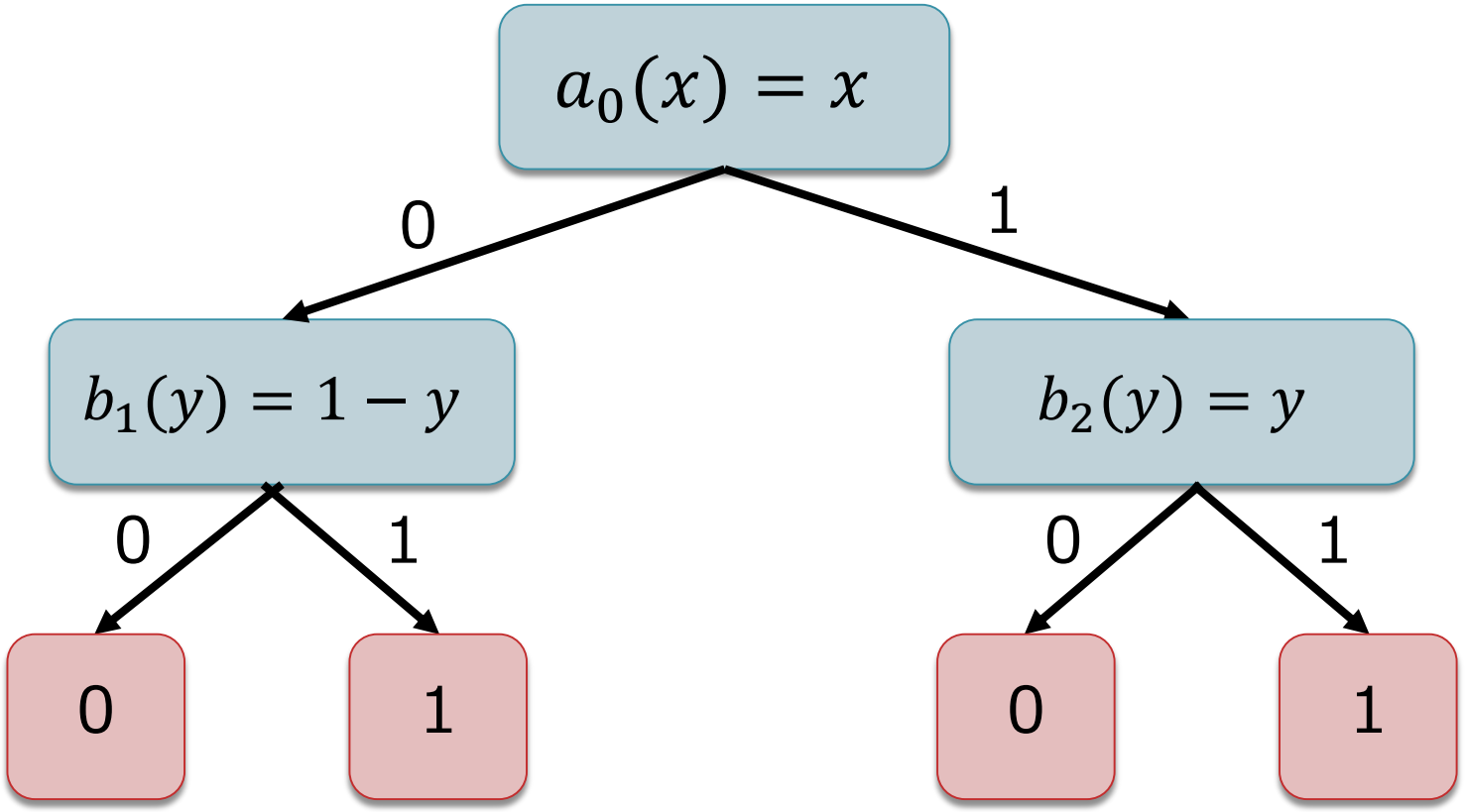
決定性プロトコルの例

- 1ビット等価性判定問題を考える

$$f(x,y)=\begin{cases}0 & \text{if } x\neq y\\ 1 & \text{if } x=y\end{cases}\qquad (x,y)\in\{0,1\})$$

- この問題に対するプロトコルP
  - Aliceはxを送信
    - Bobは受信したら$x=y$かどうか判定する
    - 判定結果をビット値として返信

Pの決定木



決定性プロトコルの通信量

- 決定性プロトコルの通信量$D(f,P)$
  - 最悪時入力におけるPの通信ビット数
- 明らかに

$$D(f,P) = \text{Pの決定木の高さ}$$

(注) 木の高さ＝葉へのパスの長さの最大値

- fの決定性通信複雑性$D(f)$

$$D(f) = \min_{P \in \mathcal{P}_f} D(f,P)$$

ケーススタディ：等価性判定問題の複雑性

- 等価性判定問題の決定性通信複雑性

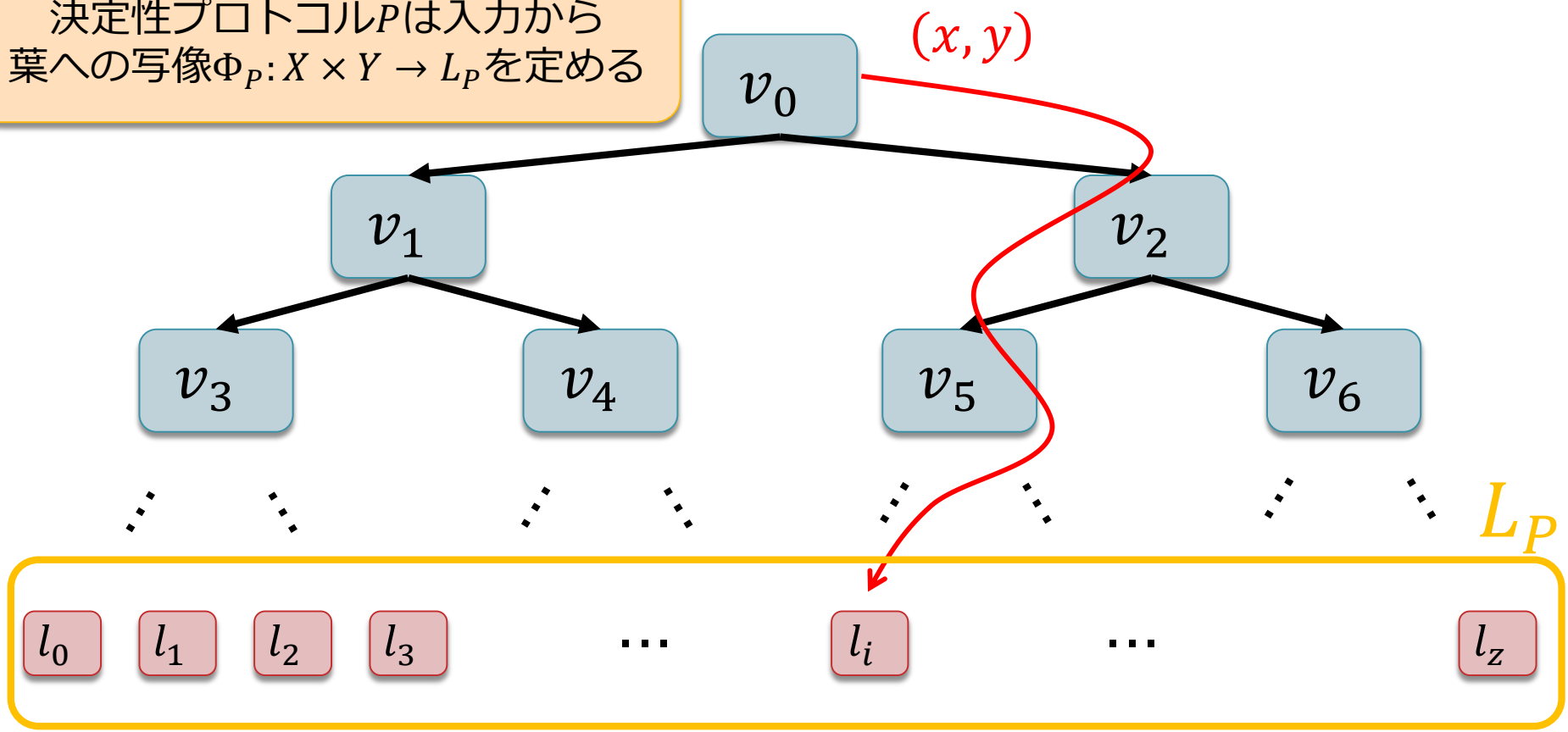
$$D(equal) = \Theta(n)$$

- 上界は明らか
  - Aliceが全情報を送信し，Bobがチェックして答えを送信(通信量$n+1$ビット)
- 下界は自明ではない

決定性プロトコルの動作

- 入力(x, y)を決めると，決定木のパス(=葉)が一つ決まる

決定性プロトコルPは入力から
葉への写像$\Phi_P: X \times Y \to L_P$を定める



真理値表への葉頂点の割り当て

- 関数Φ_Pは真理値表の各セルへの葉頂点の割り当てを決める

Alice \ Bob

x \ y	0000	0001	0010	0011	…	1111
0000	1	0	0	0		0
0001	0	1	0	0		0
0010	0	0	1	0		0
0011	0	0	0	1		0
⋮						
1111	0	0	0	0		1

Alice \ Bob

x \ y	0000	0001	0010	0011	…	1111
0000	l_0	l_1	l_1	l_1		l_1
0001	l_0	l_2	l_4	l_4		l_4
0010	l_0	l_3	l_5	l_7		l_7
0011	l_0	l_3	l_6	l_8		l_{10}
⋮						
1111	l_0	l_3	l_6	l_9		l_{44}

矩形

- $R = C \times D$ $(C \subseteq X, D \subseteq Y)$を関数$f: X \times Y \to Z$の真理値表における矩形(rectangle)と呼ぶ

Bob

Alice

x \ y	0000	0001	0010	0011	…	1111
0000	1	0	0	0		0
0001	0	1	0	0		0
0010	0	0	1	0		0
0011	0	0	0	1		0
⋮						
1111	0	0	0	0		1

$C = \{0000,0001\}$, $D = \{0000,0001\}$によって決まる矩形

$C = \{0000,0010,0011\}$, $D = \{0001,1111\}$によって決まる矩形

矩形でない例

単色矩形

- $\forall (x_1, y_1), (x_2, y_2) \in R: f(x_1, y_1) = f(x_2, y_2)$である矩形$R$を$f$-単色矩形($f$-monochromatic rectangle)と呼ぶ

Bob

Alice

x \ y	0000	0001	0001	0011	…	1111
0000	1	0	0	0		0
0001	0	1	0	0		0
0010	0	0	1	0		0
0011	0	0	0	1		0
⋮						
1111	0	0	0	0		1

特に，矩形内のfの値が全てbであるときb-単色(b-monochromatic)と呼ぶ

単色でない矩形

単色な矩形(0-単色)

プロトコルと矩形：補題

補題：fを計算する任意のプロトコルPと，その決定木の葉$l \in L$について，$S_{P,l} = \{(\boldsymbol{x}, \boldsymbol{y}) | \Phi_P(\boldsymbol{x}, \boldsymbol{y}) = l\}$ は単色矩形

Alice

Bob

x \ y	0000	0001	0010	0011	…	1111
0000	1	0	0	0		0
0001	0	1	0	0		0
0010	0	0	1	0		0
0011	0	0	0	1		0
⋮						
1111	0	0	0	0		1

Bob

x \ y	0000	0001	0010	0011	…	1111
0000	l_0	l_1	l_1	l_1		l_1
0001	l_0	l_2	l_4	l_4		l_4
0010	l_0	l_3	l_5	l_7		l_7
0011	l_0	l_3	l_6	l_8		l_{10}
⋮			S_{P,l_3}			
1111	l_0	l_3	l_6	l_9		l_{44}

S_{P,l_1}

補題から分かること

- 真理値表のf-単色矩形による分割数の下限を求めることで通信複雑性の下界が得られる！

Bob

Alice

x \ y	0000	0001	0010	0011	…	1111
0000	1	0	0	0		0
0001	0	1	0	0		0
0010	0	0	1	0		0
0011	0	0	0	1		0
⋮						
1111	0	0	0	0		1

分割の例

補題から分かること

- 真理値表のf-単色矩形に
  で通信複雑性の下界が得

Bob

Alice

x \ y	0000	0001	0010	0011	…	1111
0000	1	0	0	0		0
0001	0	1	0	0		0
0010	0	0	1	0		0
0011	0	0	0	1		0
⋮						
1111	0	0	0	0		1

fの表をf-単色矩形で分割するには
少なくともr個の矩形が必要

↓

任意のPについて，Φ_Pによって
定まる分割の矩形数はr以上

↓

任意のPの決定木は葉数r個以上

↓

任意のPの決定木は高さ$\lceil \log r \rceil$以上

↓

fの通信複雑性は$\lceil \log r \rceil$以上

矩形の数の下限：錯誤集合による導出

- $F \subseteq X \times Y$に対して，以下の2条件を満たす$b \in Z$が存在するとき，Fを錯誤集合(fooling set)と呼ぶ
  1. $\forall (\boldsymbol{x}, \boldsymbol{y}) \in F : f(\boldsymbol{x}, \boldsymbol{y}) = b$
  2. $\forall (\boldsymbol{x_1}, \boldsymbol{y_1}), (\boldsymbol{x_2}, \boldsymbol{y_2}) \in F : f(\boldsymbol{x_1}, \boldsymbol{y_2}) \neq b$ or $f(\boldsymbol{x_2}, \boldsymbol{y_1}) \neq b$

錯誤集合 F中の全ての要素は
異なるf-単色矩形に必ず属する

□ はサイズ３の錯誤集合

Bob

Alice: x \ y	00	01	01	11
00	1	0	0	0
01	0	1	~~0~~	~~0~~
10	0	~~0~~	1	~~0~~
11	0	~~0~~	~~0~~	1

関数Equalの錯誤集合

- サイズ2^nの錯誤集合 $F = \{(x, y) | x = y\}$

Bob

Alice

x \ y	0000	0001	0010	0011	…	1111
0000	1	0	0	0		0
0001	0	1	0	0		0
0010	0	0	1	0		0
0011	0	0	0	1		0
⋮						
1111	0	0	0	0		1

これより以下の定理を得る

$$D(equal) = \log 2^n = \Theta(n)$$

Rank bound

- 矩形の分割数は真理値表の行列ランクと関係する
- ある1-単色矩形一つからなる真理値表行列→ランク1

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- 真理値表行列がk個の単色矩形に分割できる

  ⇔真理値表行列がk個のランク1行列の和で書ける

Rank bound

- 行列のランクは劣加法性を持つ
  - $A = A_1 + A_2 + \cdots + A_k$のとき

$$rank(A) \leq rank(A_1) + rank\,(A_2) + \cdots + rank(A_k)$$

- A_fを関数fの真理値表行列，A_1~A_kを1-単色矩形に対応する行列として$A_f = A_1 + A_2 + \cdots + A_k$と分解すると

$$rank(A_f) \leq \text{1-単色矩形の個数}$$

- よって，

$$\log rank(A_f) \leq D(f)$$

対数ランク予想

- 真理値表の行列ランクと通信複雑性についての上界側の関係の予想

予想(log rank conjecture)[LS88]
ある定数$c \geq 1$が存在し，任意の関数$X \times Y \to \{0,1\}$に対して

$$D(f) \leq \left(\log rank\left(A_f\right)\right)^c$$

- 通信複雑性理論における大きな未解決問題のひとつ
  - $c = 1$に関しては否定的に解決されている[RS95]

[LS88] L. Lovasz and M. Saks. Lattices, Mobius Functions and Communication Complexity, In Proc. of FOCS, pp. 81–90, 1988
[RS95] R. Raz, and B. Spieker, On the “log rank”-conjecture in communication complexity, Combinatorica, Vol. 15, No. 4, pp. 567-588, 1995.

乱択プロトコルの場合

- プロトコルはターンに従って動作
  - 1ターンでAliceかBobのいずれかが自身の状態**+ランダムビット**に従って(1ビット)メッセージを決定し，送信
  - 必ずしも交互に送るわけではない
    - が，漸近的な議論をするならば交互の送信を仮定してOK
  - メッセージは同時に送信されるかもしれない
    - が，ラウンド数に関して議論しない(or漸近的に議論する)ならば逐次的に送信されているとみなす
  - 最終的にAliceとBobは$f(x,y)$の値を出力して停止

乱択プロトコルの種類

- 関数fに対するゼロエラー乱択プロトコルP

任意の入力$(x, y) \in X \times Y$に対して

$$\Pr[P(x, y) = f(x, y)] = 1$$

- 関数fに対するϵ-誤り乱択プロトコルP

任意の入力$(x, y) \in X \times Y$に対して

$$\Pr[P(x, y) = f(x, y)] \geq 1 - \epsilon$$

これ以外にも片側誤り版の定義が存在するが，今回は触れない

乱択通信複雑性

- 乱択プロトコルPは，ランダムビット列$\boldsymbol{r}$を引数に取る決定性プロトコル$P: X \times Y \times \{0,1\}^* \to Z$と見なせる
- 関数fに対するϵ-誤り乱択プロトコルの(平均)通信量
  - 最悪時入力における(平均)通信量 ← 最悪通信量で定義することもある(漸近的にはあまり差なし)

$$R_P^{AVG}(f) = \max_{(x,y)\in X\times Y} E_r[C_P(x,y)]$$

  - 関数fに対するϵ-誤り乱択通信複雑性

Errata m(_ _)m

$$R_\epsilon(f) = \min_{P\in\mathcal{P}_{f,\epsilon}} R_P^{AVG}(f)$$

等価性判定問題の乱択プロトコル

- n-ビット等価性判定問題の通信複雑性の上界

$$R_{o(1)}(equal) = \Theta(\log n)$$

  - すなわち，乱択を用いることで全データの送信を避けることができる！

プロトコルP_{EQ}

1. Aliceは区間$[2, n^2]$中の素数pを一様乱択する
2. Aliceは組$(Num(\boldsymbol{x}) \bmod p, p)$をBobに送信($O(\log n)$ビット)
   ($Num(\boldsymbol{x})$は$\boldsymbol{x}$を2進数値と見なしたときの値)
3. Bobは(v, p)を受信したら$v = Num(\boldsymbol{y}) \bmod p$?の
   比較結果を答としてAliceに返信
4. 2人とも答を出力

ハッシュ値の比較を用いることで，高確率で等しい値かどうかを検証できる

プロトコルP_{EQ}の正当性

補題：プロトコルP_{EQ}において
1. 入力が$\boldsymbol{x} = \boldsymbol{y}$ならば答えはいつも正しい
2. 入力が$\boldsymbol{x} \neq \boldsymbol{y}$のとき答えが$\boldsymbol{x} = \boldsymbol{y}$となる確率$\leq 2\log n/n$

- 1.はほぼ自明
- 2.の証明
  - 答えが$\boldsymbol{x} = \boldsymbol{y}$のとき，$Num(\boldsymbol{x}) \bmod p = Num(\boldsymbol{y}) \bmod p$
    $\Rightarrow h = |Num(\boldsymbol{x}) - Num(\boldsymbol{y})|$は$p$で割り切れる
  - すなわち，pはhの素因数

プロトコルP_{EQ}の正当性

補題：プロトコルP_{EQ}において
1. 入力が$\boldsymbol{x} = \boldsymbol{y}$ならば答えはいつも正しい
2. 入力が$\boldsymbol{x} \neq \boldsymbol{y}$のとき答えが$\boldsymbol{x} = \boldsymbol{y}$となる確率$\leq 2\log n/n$

- 2.の証明(続き)
  - $h < 2^n$なので，hの素因数は高々n個
  - 素数定理より，$[0, n^2]$の間には少なくとも$\frac{n^2}{\log n^2}$個の素数が存在
  - 誤り確率(偶然hの素数を引き当てる確率)は高々

$$\frac{n}{n^2/\log n^2} = \frac{2\log n}{n}$$

(終)

分布つき複雑性 (Distributional Complexity)

- 入力に関する確率分布$\mu \sim X \times Y$を仮定したもとでの関数fの複雑性を考える
- 以下の条件を満たすプロトコルPをμのもとでのϵ-誤り決定性プロトコルと呼ぶ

入力$(x,y)\sim\mu$に対して $\Pr[P(x,y) = f(x,y)] \geq 1-\epsilon$

- fの分布つき複雑性$D_\epsilon^\mu(f)$

$$D_\epsilon^\mu(f) = \min_{P \in \mathcal{P}^{det}_{f,\mu,\epsilon}} \max_{(x,y)\in X\times Y} C_P(x,y)$$

($\mathcal{P}^{det}_{f,\mu,\epsilon}$は$\mu$のもとでの$f$に対する$\epsilon$-誤り決定性プロトコル全ての集合)

Yaoのミニマックス原理

任意のf，ϵ，μについて以下が成立

$$R_\epsilon(f) \geq D_\epsilon^\mu(f)$$

また，以下を満たす分布μ'が存在する

$$R_\epsilon(f) = D_\epsilon^{\mu'}(f)$$

- 入力分布を仮定した決定性プロトコルの複雑性を議論することで，乱択プロトコルの通信量下界を得られる

乱択プロトコルの下界導出

- 単色矩形でなく「ほとんど単色」矩形の分割を考える

Bob

Alice

x \ y	0000	0001	0010	0011	…	1111
0000	1	0	0	0		0
0001	0	1	0	1		1
0010	0	0	1	1		1
0011	0	1	1	1		1
⋮						
1111	0	1	1	1		1

分布μの下で成功確率が$1-\epsilon$以上であればよい（例えば，1がプロトコルの出力であれば，入力値が [ ] の0である確率がϵ以下）

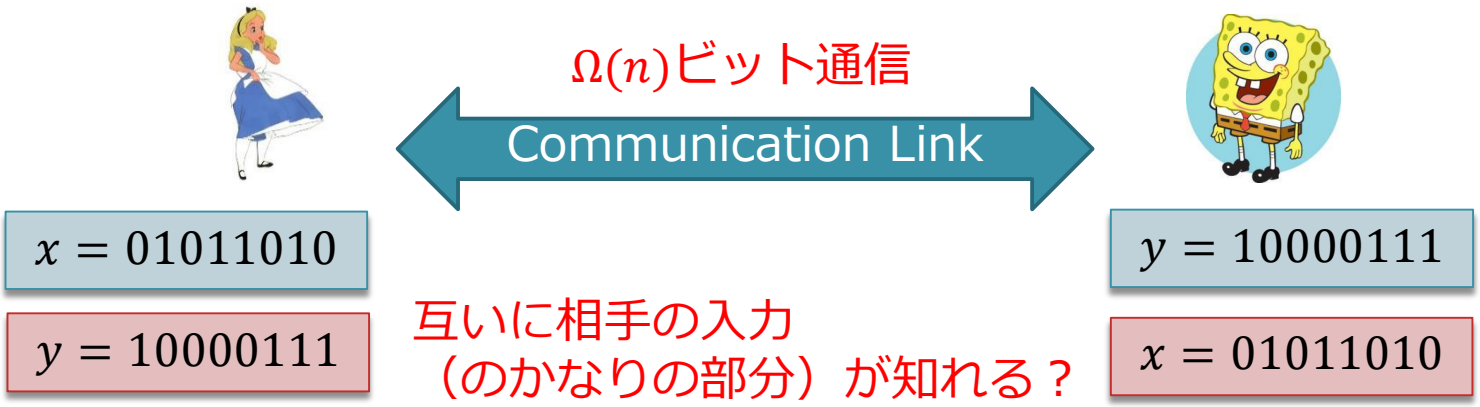
ほとんど単色な矩形の分割数の下界から以下の定理が得られる

$$R_{O(1)}(disj) = \Theta(n)$$
[Raz92]

[Raz92] A. A. Razborov, On the distributional complexity of disjointness, Theoretical Computer Science, Vol. 106, pp. 385-390, 1992.

プロトコルの情報量についての観察

- 関数fの通信複雑性が$\Omega(n)$であるとはどういうことか？



- 直感的に納得のできる解釈だが，（全く)自明ではない
  - (x, y)との依存性が小さい(が，fの計算には必要な)情報が$\Omega(n)$ビット流れるかもしれない

情報複雑性(Information Complexity)

- プロトコルのコストを通信ビット数基準でなく情報量基準で図る
- 何らかの入力分布$\mu\sim(x,y)$を仮定する
  - プロトコルの分布μに関する知識は様々
- プロトコルPの入力(x,y)に対するtranscript $P(x,y)$
  - プロトコルが使う通信ビット列(と乱数列)の連接
    - 各プレイヤにプロトコルの実行が与える(外部からの)情報
  - transcriptは(μに依存する)確率変数

情報複雑性(Information Complexity)

- プロトコルの(μ に関する) (内部)情報コスト

$$IC^{\mu}(P) = I(y; P(x,y)|x) + I(x; P(x,y)|y)$$

PがBobに与えるxについての情報量

PがAliceに与えるyについての情報量

- 関数fのϵ-誤り情報複雑性

$$IC_{\epsilon}(f) = \inf_{P \in \mathcal{P}_{f,\epsilon}} \max_{\mu} IC^{\mu}(P)$$

ICを用いた下界導出

定理[BR10]

$$R_\epsilon(x,y) \geq IC_\epsilon\left(P(x,y)\right)$$

この路線での上下界の探求が近年盛ん
(今年のISITの話もその一部)

[BR10]M. Braverman, A. Rao, Information equals Amortized Communication, IEEE 52nd Annual Symposium on Foundations of Computer Science(FOCS), pp.748-757, 2011.

まとめ・参考文献

- 通信複雑性の入り口について概説
  - 決定性プロトコルと乱択プロトコルの差
  - 矩形分割を用いた限界の導出
- 参考文献
  - [KN95] 古典的な教科書．古いが依然有用
  - [CP10] 交差判定を中心にした同理論の進展が良くまとめられている
  - [Wei15] 近年の情報理論的手法の発展についてまとめられている

[KN95] E. Kushilevitz, N. Nisan, Communication Complexity, Cambridge University Press, 1997.
[CP10] A. Chattopadhyay, T. Pitassi, The story of set-disjointness, SIGACT news, Vol.41, Issue 3, 2010.
[Wei15] O. Weinstein, Information Complexity and the Quest for Interactive Compression, SIGACT news, Vol.46, Issue 2, 2015