量子通信複雑性理論

西村治道（名古屋大学）

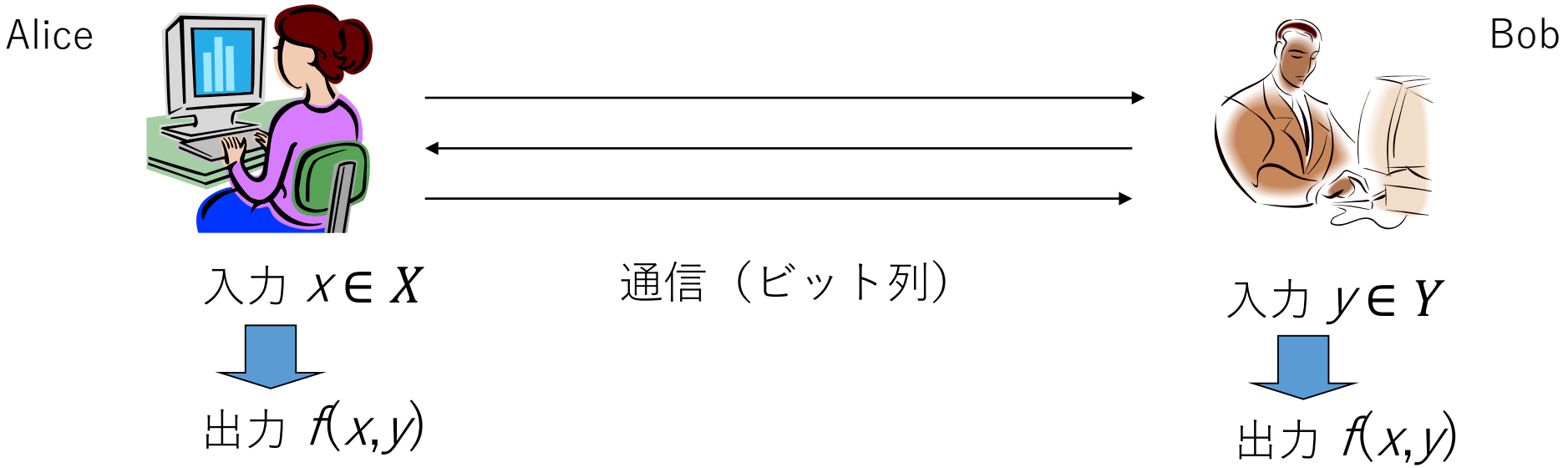
2020年7月2日

京大量子情報ユニット・基研 量子情報スクール

今回のはなし

- 古典通信複雑性
  - 決定性
  - 乱択
- 量子通信複雑性
- 応用

通信複雑性(通信計算量)モデル



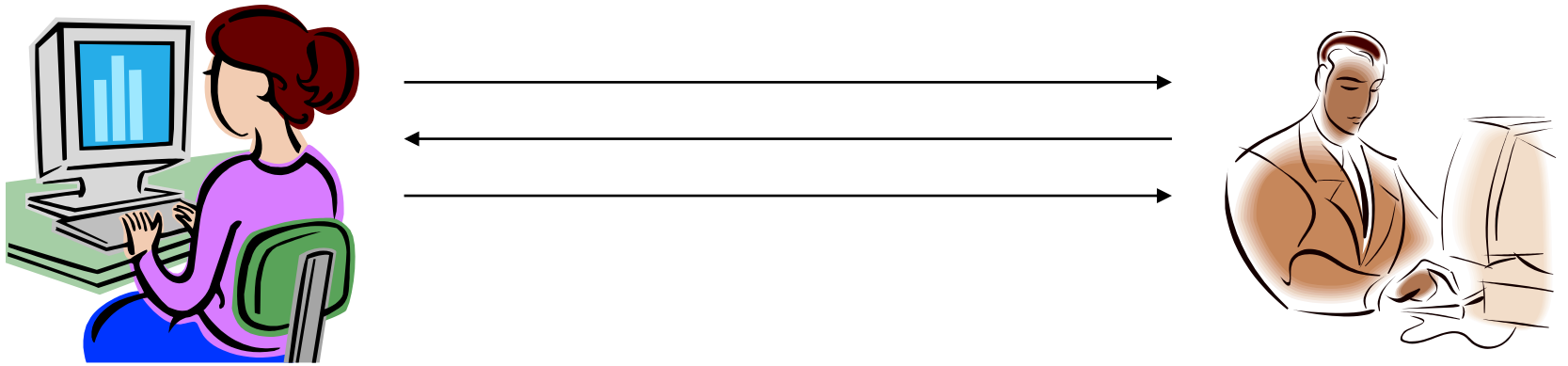
fの通信計算量:= $f(x,y)$を計算するために必要な通信量
（ビット列の長さ）

- Andrew C.-C. Yao が導入したモデル[Yao79]
- 計算を通信プロセスの一種とみなすことで計算限界を示す

問題の例その１：PARITY

入力
$x \in \{0, 1\}^n$

入力
$y \in \{0, 1\}^n$

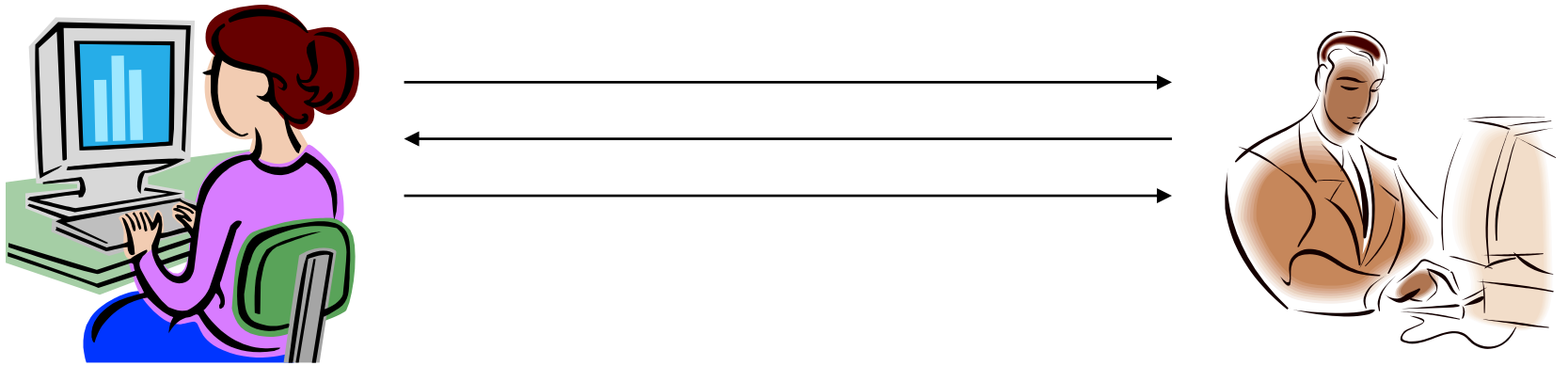


AliceとBobは xと yが含む１の総数の偶奇 を互いにビット列を送りあうことで判定したい．可能な限り送りあうビット列の長さ（通信量）は小さくしたい．

問題の例その１：PARITY

入力
$x \in \{0,1\}^n$

入力
$y \in \{0,1\}^n$



AliceとBobは xと yが含む１の総数の偶奇 を互いにビット列を送りあうことで判定したい．可能な限り送りあうビット列の長さ（通信量）は小さくしたい．

関数として書くなら
PARITY(x,y)=1 if $\sum_i x_i + \sum_i y_i = 1 \bmod 2$
=0 otherwise

問題の例その１：PARITY

入力

$x \in \{0,1\}^n$

入力

$y \in \{0,1\}^n$

$\sum_{i=1}^{n} x_i \mod 2$

PARITY(x,y)

AliceとBobは xとyが含む１の総数の偶奇 を互いにビット列を送りあうことで判定したい．可能な限り送りあうビット列の長さ（通信量）は小さくしたい．

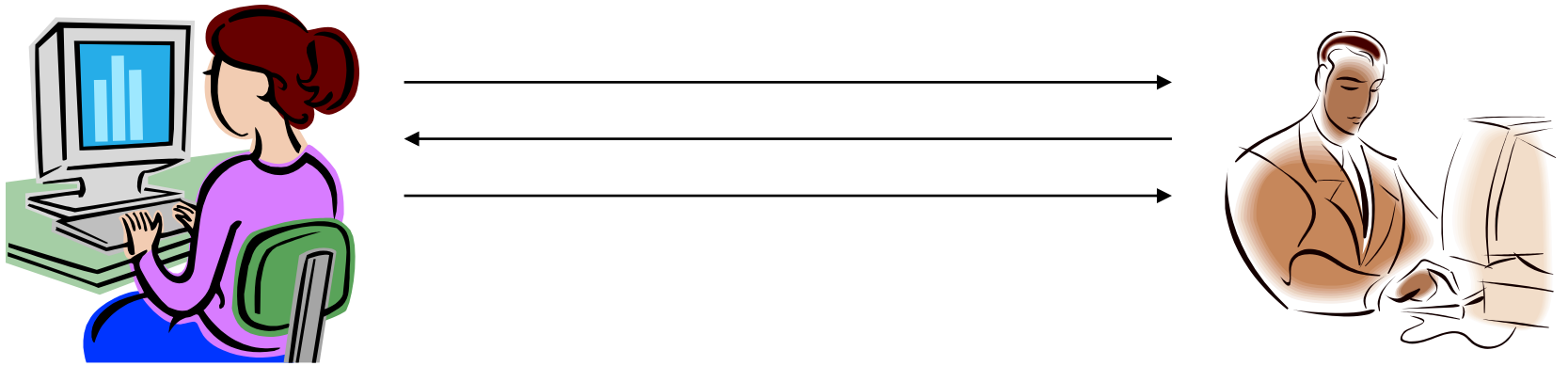
通信計算量は 2

$$\sum_{i=1}^{n} x_i \mod 2 + \sum_{i=1}^{n} y_i \mod 2 = PARITY(x,y)$$

問題の例その２：EQ

入力
$x \in \{0, 1\}^n$

入力
$y \in \{0, 1\}^n$



AliceとBobは $x=y$ かどうかを互いにビット列を送りあうことで判定したい．可能な限り送りあうビット列の長さ（通信量）は小さくしたい．

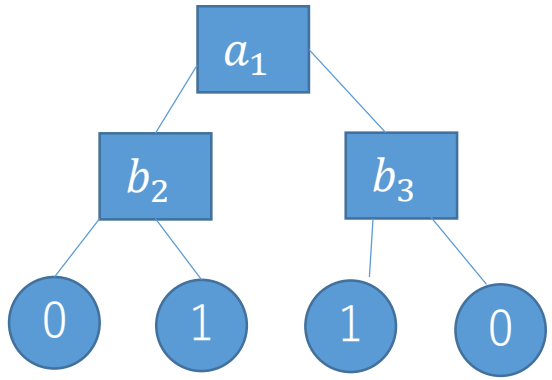
関数として書くなら
EQ(x,y)=1 if x=y
=0 otherwise

Q. EQの通信計算量は？

プロトコル木，通信複雑性

- $X \times Y \to Z$を計算するプロトコルP を表現する木（プロトコル木）
  ラベル付き２分木で:
  - 根からプロトコルはスタート
  - 葉でない頂点vはアリスの通信を表す関数 $a_v: X \to \{0,1\}$かボブの通信を表す関数 $b_v: Y \to \{0,1\}$でラベリング
  - vがa_v（b_vのときも同様）でラベリングされているとき，
    $a_v(x) = 0$なら左の子頂点へ，$a_v(x) = 1$なら右の子頂点へ
  - 各葉は$z \in Z$でラベリングされ，入力(x, y)のときに，上記のルールでたどり着いた葉の値がPの(x, y)上での出力
  - Pのコスト$c(P)$：＝Pのプロトコル木の高さ
- $D(f) := \min_P \{c(P) | P$は$f$を計算する$\}$

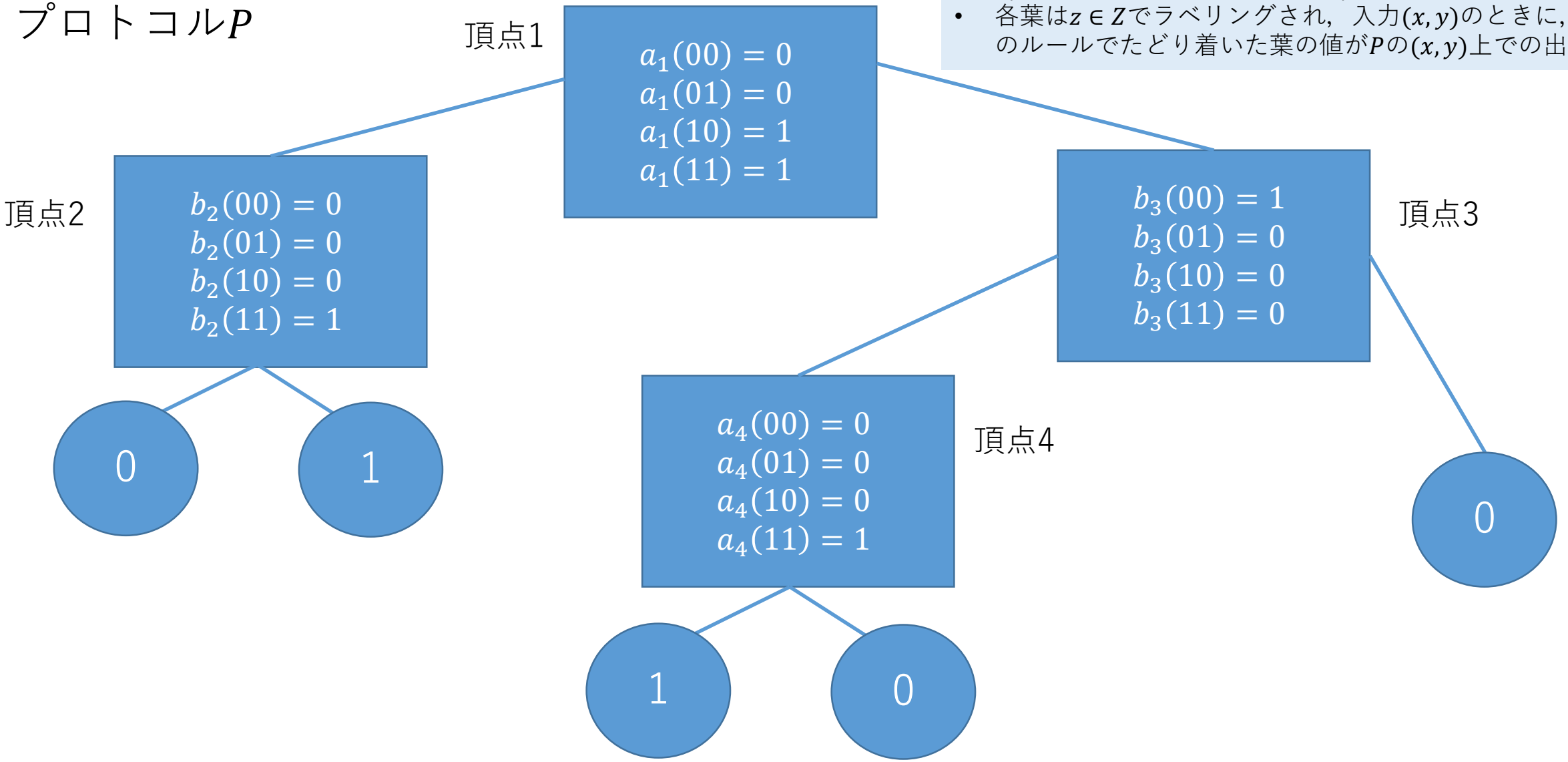
  （fの決定性通信計算量）



プロトコル木の例

プロトコル木はラベル付き２分木で：
- 根からプロトコルはスタート
- 葉でない頂点vはアリスの通信を表す関数 $a_v: X \to \{0,1\}$かボブの通信を表す関数 $b_v: Y \to \{0,1\}$でラベリング
- vがa_v（b_vのときも同様）でラベリングされているとき，$a_v(x) = 0$なら左の子頂点へ，$a_v(x) = 1$なら右の子頂点へ
- 各葉は$z \in Z$でラベリングされ，入力(x, y)のときに，上記のルールでたどり着いた葉の値がPの(x, y)上での出力

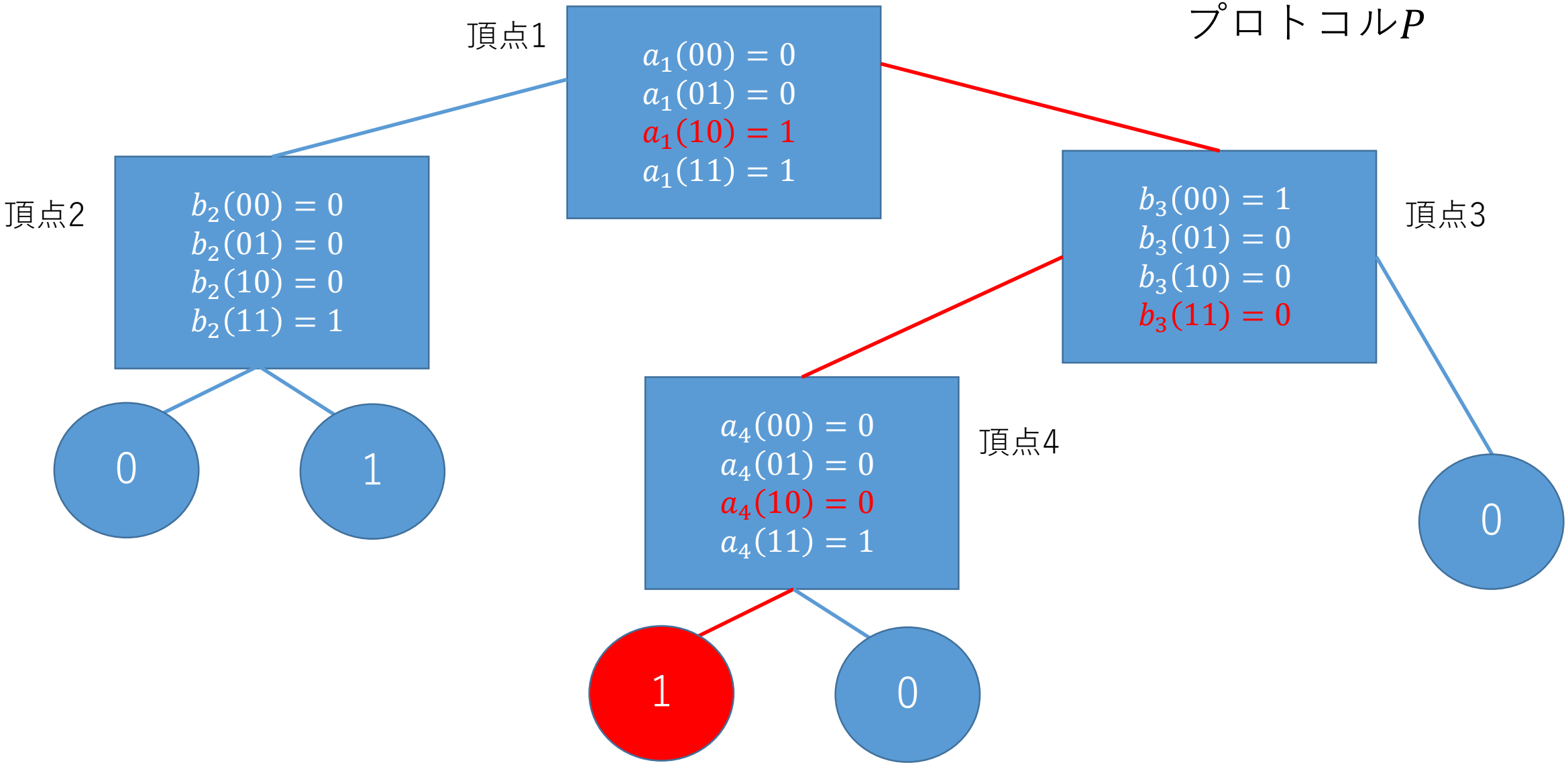
プロトコルP



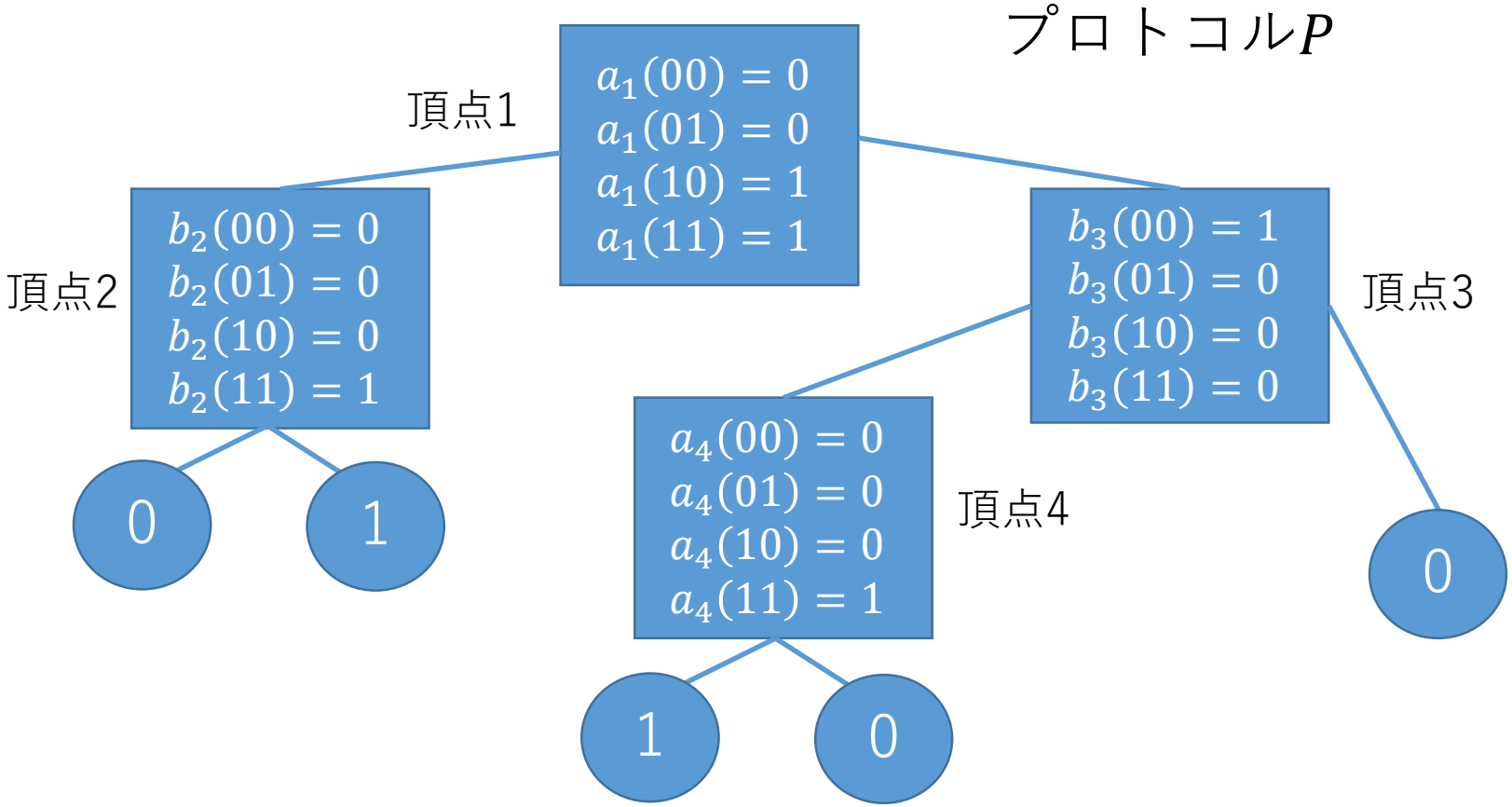
プロトコル木の例

入力 $(x, y) = (10,11)$

プロトコルP



プロトコル木が計算する関数

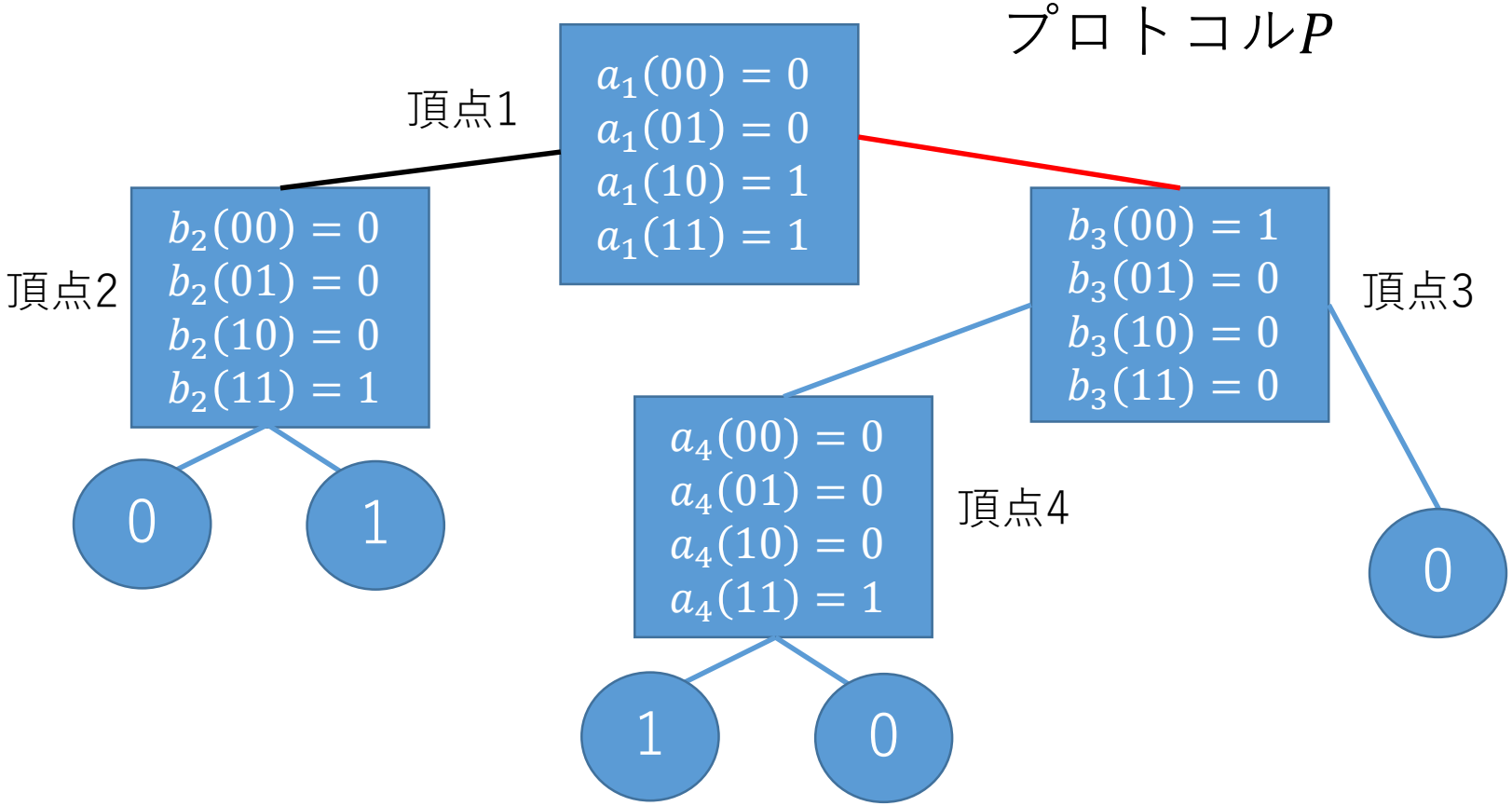


x/y	00	01	10	11
00	0	0	0	1
01	0	0	0	1
10	0	1	1	1
11	0	0	0	0

Pが計算する関数を表す
行列（通信行列）

プロトコルと矩形(rectangle)

- すべてのプロトコルは通信行列を矩形に分割する

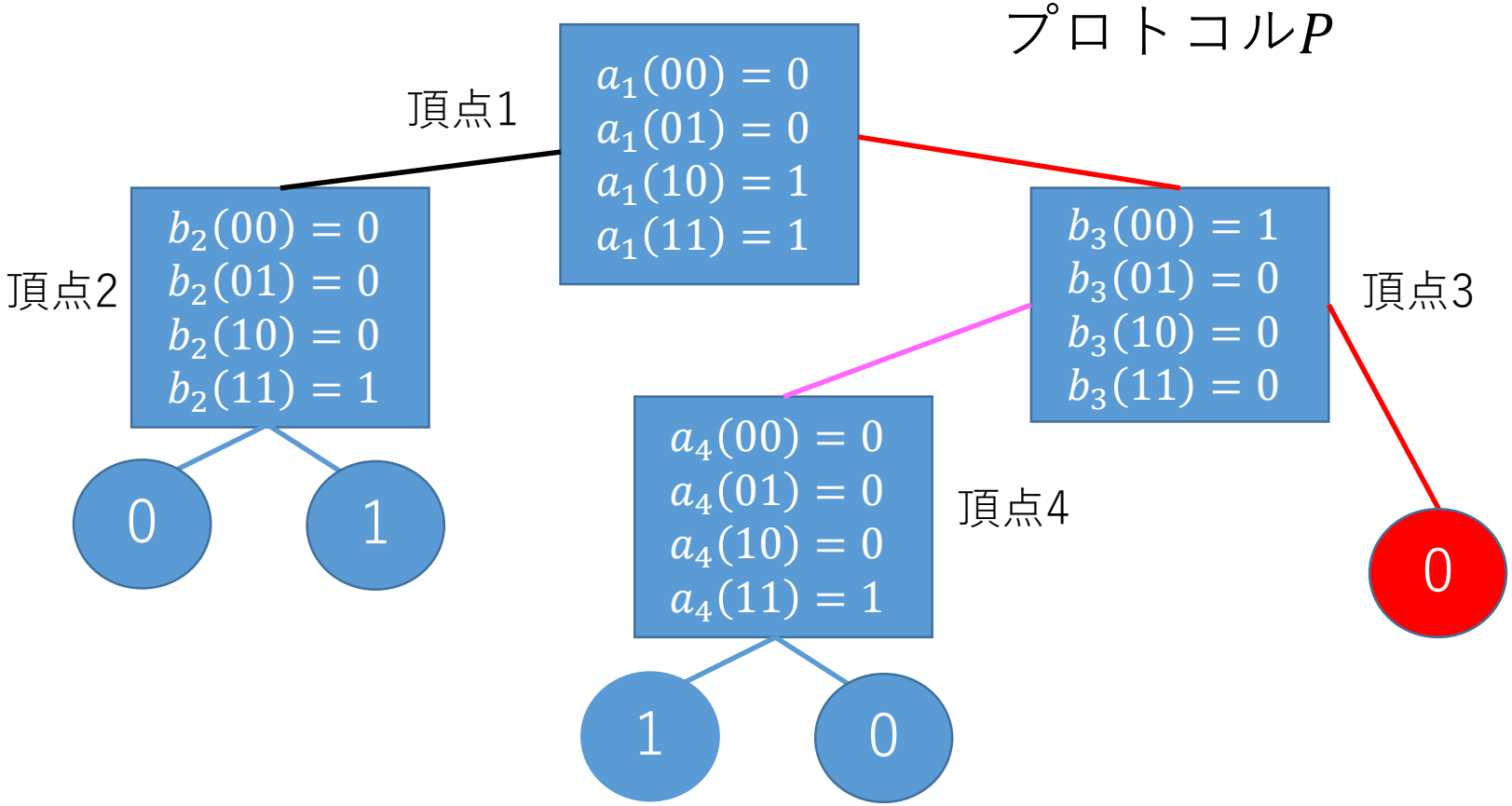


x/y	00	01	10	11
00	0	0	0	1
01	0	0	0	1
10	0	1	1	1
11	0	0	0	0

Pが計算する関数を表す行列（通信行列）

プロトコルと矩形(rectangle)

- すべてのプロトコルは通信行列を矩形に分割する

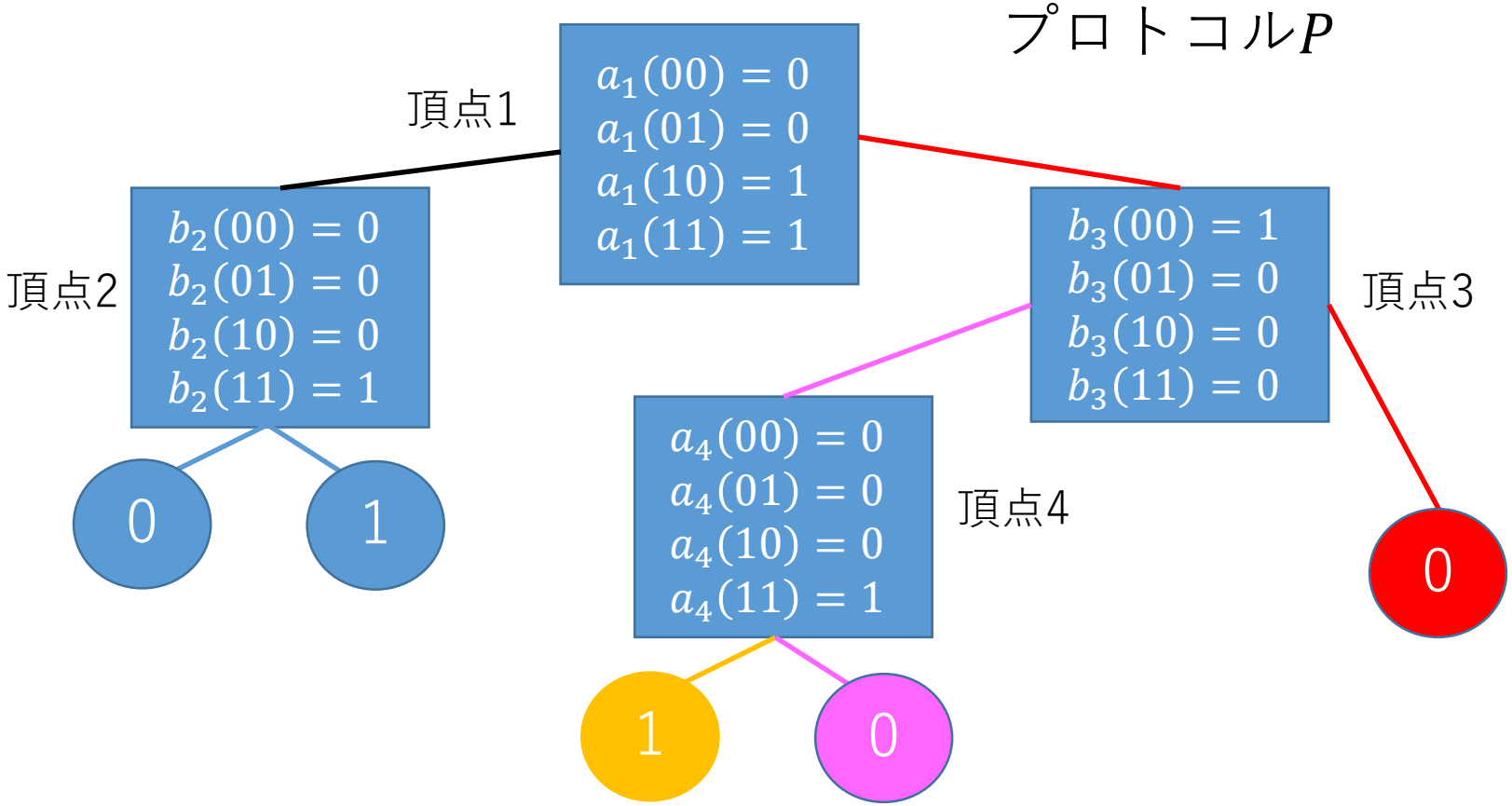


x/y	00	01	10	11
00	0	0	0	1
01	0	0	0	1
10	0	1	1	1
11	0	0	0	0

Pが計算する関数を表す行列（通信行列）

プロトコルと矩形(rectangle)

- すべてのプロトコルは通信行列を矩形に分割する

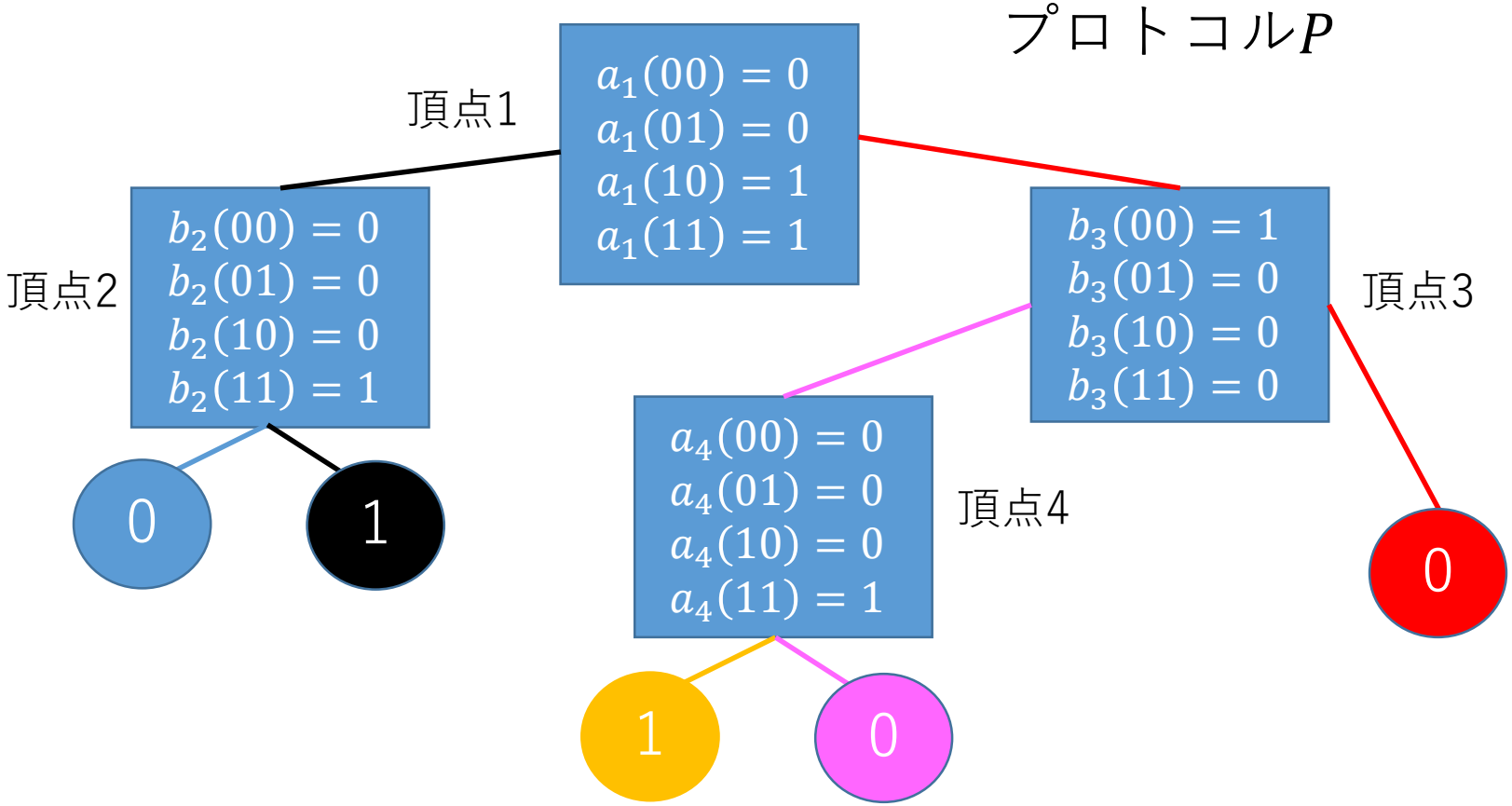


x/y	00	01	10	11
00	0	0	0	1
01	0	0	0	1
10	0	1	1	1
11	0	0	0	0

Pが計算する関数を表す行列（通信行列）

プロトコルと矩形(rectangle)

- すべてのプロトコルは通信行列を矩形に分割する

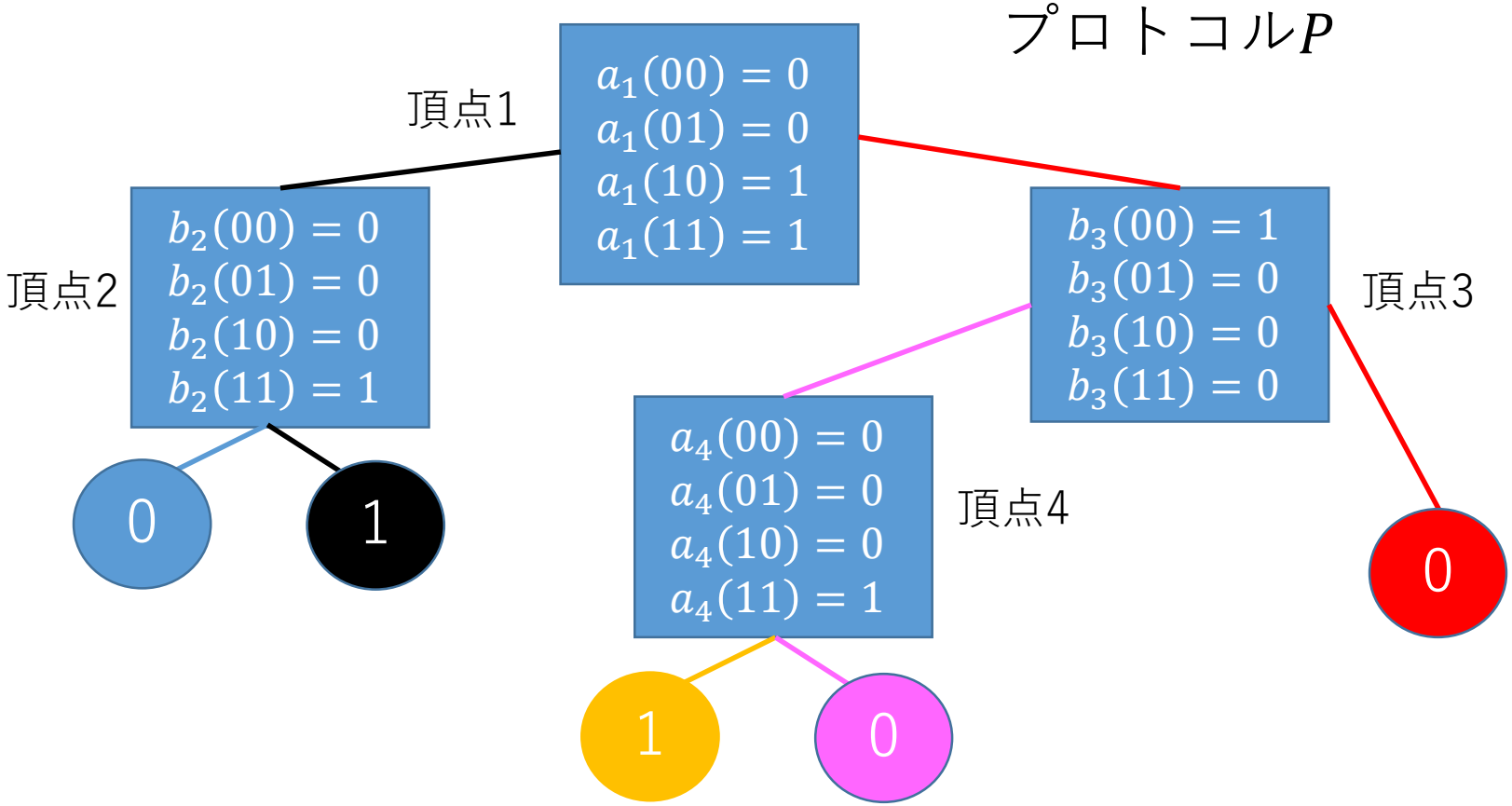


x/y	00	01	10	11
00	0	0	0	1
01	0	0	0	1
10	0	1	1	1
11	0	0	0	0

Pが計算する関数を表す行列（通信行列）

プロトコルと矩形(rectangle)

- すべてのプロトコルは通信行列を矩形に分割する



x/y	00	01	10	11
00	0	0	0	1
01	0	0	0	1
10	0	1	1	1
11	0	0	0	0

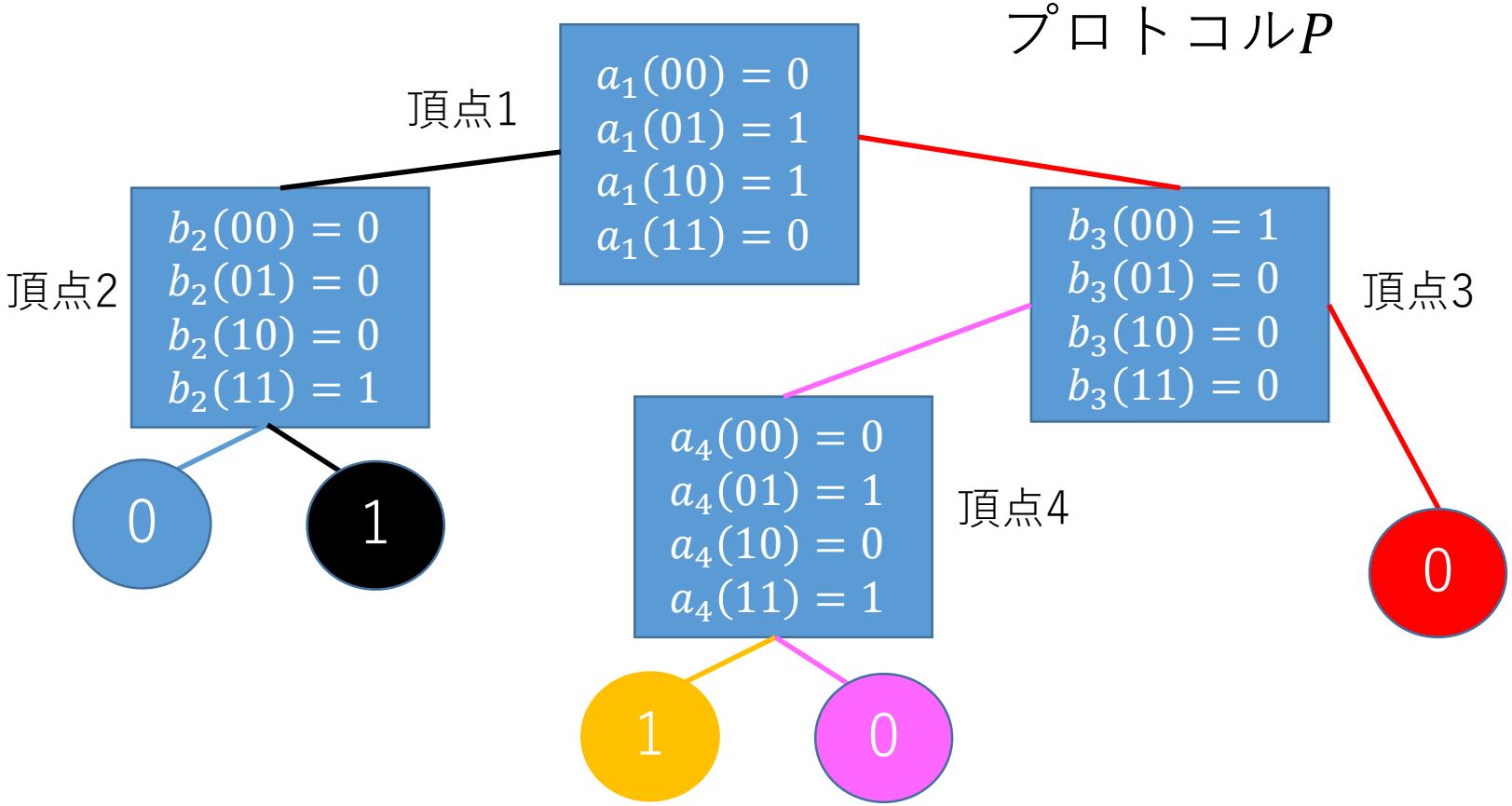
Pが計算する関数を表す行列（通信行列）

・各矩形は各葉に対応
・各矩形においてその成分はすべて同じ値（単色矩形）

プロトコルと矩形(rectangle)

行や列が飛ばし飛ばしでもOK

- すべてのプロトコルは通信行列を矩形に分割する



x/y	00	01	10	11
00	0	0	0	1
01	0	0	0	0
10	0	1	1	1
11	0	0	0	1

Pが計算する関数を表す行列（通信行列）

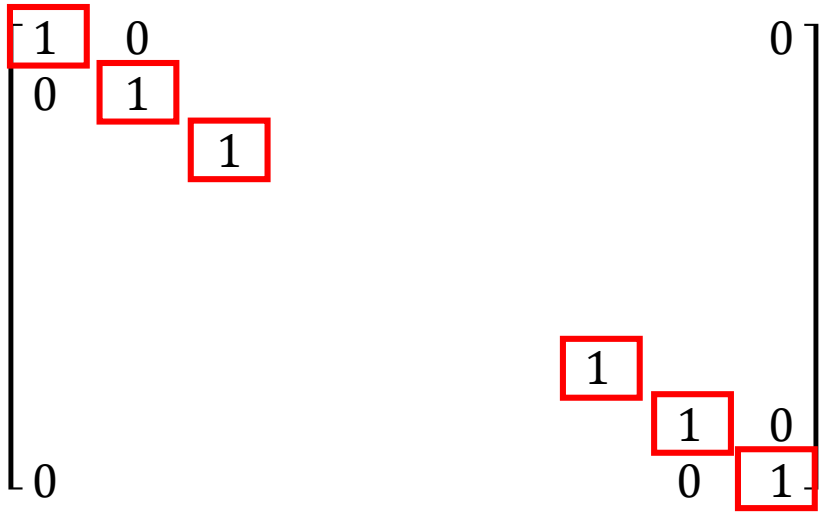
・各矩形は各葉に対応
・各矩形においてその成分はすべて同じ値（単色矩形）

単色矩形の個数と通信複雑性

関数$f: X \times Y \to Z$の通信行列を単色矩形に分割するのに
t個以上の単色矩形が必要ならば，$D(f) \geq \log_2 t$

例：$EQ_n: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}: EQ_n(x,y) = \delta_{xy}$

$EQ_n =$



- 単色矩形で分割するには
  2^n個の単色矩形が必要
- $D(EQ_n) \geq \log_2(2^n) = n$

代表的な下界導出法

- 関数の通信行列の情報から導出できる以下の方法が代表的
  - Fooling set method
  - Rank method

Fooling set

- 関数$f: X \times Y \to \{0,1\}$に対して，集合$S \subseteq X \times Y$が$f$に対するfooling setであるとは，ある$z \in \{0,1\}$が存在して
  - すべての$(x, y) \in S$について$f(x, y) = z$
  - すべての異なる２組$(x_1, y_1), (x_2, y_2) \in S$について，
    $f(x_1, y_2) \neq z$または$f(x_2, y_1) \neq z$

$$M_f = \begin{matrix} \\ y_1 \\ y_2 \\ \\ \end{matrix} \begin{matrix} \left[\right. \\ \\ \\ \left. \right] \end{matrix} \begin{matrix} \\ x_1 & x_2 \\ \\ \\ \end{matrix} \quad \begin{matrix} \\ 1 & ? \\ \\ 0 & 1 \\ \\ \end{matrix}$$

Fooling setと通信複雑性

関数$f: X \times Y \to \{0,1\}$がサイズ$t$のfooling setをもつならば,
$D(f) \geq \log_2 t$

例：$EQ_n: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}: EQ_n(x,y) = \delta_{xy}$

$$EQ_n = \begin{bmatrix} \boxed{1} & 0 & & 0 \\ 0 & \boxed{1} & 0 & \\ & 0 & \boxed{1} & \\ & & & \\ & & & \\ 0 & 0 & 0 & \boxed{1} \end{bmatrix}$$

- $\{(x,x) | x \in \{0,1\}^n\}$は
  EQ_nのサイズ2^n個のfooling set
- $D(EQ_n) \geq \log_2(2^n) = n$

Rank method

- 関数$f: X \times Y \to \{0,1\}$について,
  rank(f):= fの通信行列M_fの（実数体上での）ランク

$$D(f) \geq \log_2 \operatorname{rank}(f)$$

Rank method

- 関数$f: X \times Y \to \{0,1\}$について,
  rank(f):= fの通信行列M_fの（実数体上での）ランク

$$D(f) \geq \log_2 \operatorname{rank}(f)$$

$$EQ_n = \begin{bmatrix} 1 & 0 & & & & & 0 \\ 0 & 1 & 0 & & & & \\ & 0 & 1 & & & & \\ & & & & & & \\ & & & & & & \\ & & & & & & \\ & & & & 1 & 0 & \\ & & & & 0 & 1 & 0 \\ 0 & & & & & 0 & 1 \end{bmatrix}$$

- rank(EQ_n)=2^n
- $D(EQ_n) \geq \log_2(2^n) = n$

Rank method

- 関数$f: X \times Y \to \{0,1\}$について,
  rank(f):= fの通信行列M_fの（実数体上での）ランク

$$D(f) \geq \log_2 \operatorname{rank}(f)$$

(証明)

M_fを分割する矩形のうち出力が１のものを$R_1, R_2, \ldots, R_l$ とすると（lは葉の数）

$$M_f = R_1 + R_2 + \cdots + R_l$$

なので,

$$rank(M_f) \leq \sum_{i=1}^{l} rank(R_i) = l$$

DISJ: 通信複雑性理論での最重要関数

- $DISJ_n: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$

$$DISJ_n(x,y) = \begin{cases} 1 & (\forall j\ [x_j = 0 \text{ または } y_j = 0]) \\ 0 & (\text{そうでない場合}) \end{cases}$$

例：$DISJ_4(0101,1010) = 1,\ DISJ_4(0101,1001) = 0$

- 多くの通信複雑性理論の応用で利用される

- $\mathrm{rank}(DISJ_n) = 2^n$
- $D(DISJ_n) \geq n$

$$M_{DISJ_2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \qquad M_{DISJ_3} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

乱択プロトコル

Alice

Bob

乱択アルゴリズム

入力 $x \in X$

通信（ビット列）

入力 $y \in Y$

乱択アルゴリズム

出力 $out = f(x,y)$ with prob.$\geq 1-\varepsilon$

- fの乱択通信計算量 $R_\varepsilon(f)$:= $f(x,y)$を確率$1-\varepsilon$以上で正しく計算するために必要な通信量（ビット列の長さ）
- $R_\varepsilon^{pub}(f)$:=AliceとBobが共有乱数を事前共有する場合
- $R(f) := R_{1/3}(f)$

乱択プロトコルの例：EQ

$x \in \{0,1\}^n$

$y \in \{0,1\}^n$

$(z, p_x(z))$ 但し，$p_x(z)=x_1+x_2z+\ldots+x_nz^{n-1}$

ビット長　2log(10000n)

$R(EQ_n) = O(\log n)$

z ∈Fをランダムに選択

F: サイズ 10000n 以上の有限体

1 if $p_x(z)=p_y(z)$

0 otherwise

解析：

x=yなら，ボブは確率 1 で 1 を出力

x≠yなら，多項式$p_x(z) - p_y(z)$の零点の個数はせいぜいn-1なので，確率(n-1)/10000n<1/10000で 1 を出力

乱択プロトコルの例：EQ

入力
$x \in \{0,1\}^n$

通信量 $O(\log n)$，成功率0.99
$R(EQ_n) = O(\log n)$

$(i, C(x)_i)$

C(x)の第 i ビット

入力
$y \in \{0,1\}^n$

ランダムに
$i \in \{1,2,..,m\}$
を選択

$C(x)_i = C(y)_i$ なら 1
そうでないなら 0
$\approx EQ(x,y)$

符号長 m=O(n)

∃誤り訂正符号 C: $\{0,1\}^n \to \{0,1\}^m$; 任意の異なる n bits x, yに対して
$\mathrm{Ham}(C(x), C(y)) \geq 0.99m$

xとyは99パーセントのビットで食い違う

さらに共有乱数を許せば

入力
$x \in \{0,1\}^n$

通信量 $O(1)$, 成功率0.99
$R^{pub}(EQ_n) = O(1)$

$C(x)_i$

$C(x)$の第 i ビット

入力
$y \in \{0,1\}^n$

共有乱数として

$i \in \{1,2,..,m\}$

を選択

$C(x)_i = C(y)_i$ なら 1

そうでないなら 0

$\approx EQ(x,y)$

符号長 m=O(n)

∃誤り訂正符号C: $\{0,1\}^n \to \{0,1\}^m$; 任意の異なる n bits x, yに対して
$\mathrm{Ham}(C(x), C(y)) \geq 0.99m$

共有乱数あり vs 共有乱数なし

- 通信複雑さが$\Omega(\log n)$のとき，共有乱数ありプロトコルは共有乱数なしプロトコルと差はなし

[Newman91] $f: X \times Y \to \{0,1\}$について，

$$R_{\varepsilon+\delta}(f) \leq R_{\varepsilon}^{pub}(f) + O(\log\log|X||Y| + \log(1/\delta))$$

$X = Y = \{0,1\}^n$のとき $\log n$

乱択通信複雑性の下界導出法

- Yaoのmin-max定理によるdistributional complexityへの帰着
  - discrepancy method
- 情報理論的手法
  - 情報複雑性（Information complexity）

Distributional Complexity

（Distributinal complexity）μを$X \times Y$上の確率分布とするとき,

$$D_{\varepsilon}^{\mu}(f) := \min_{P:\text{決定性プロトコル}} \{c(P) | P \text{は} \mu \text{のもと} 1-\varepsilon \text{以上の割合の入力を正しく解く}\}$$

例: $GT(x,y) = 1 \Leftrightarrow x \geq y$ (辞書式順序)のとき, $D_{\frac{1}{4}}^{unif}(GT) \leq 2$

$$M_{GT_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Distributional Complexity

（Distributinal complexity）μを$X \times Y$上の確率分布とするとき，

$$D_{\varepsilon}^{\mu}(f) := \min_{P:\text{決定性プロトコル}} \{c(P) | P \text{は} \mu \text{のもと} 1-\varepsilon \text{以上の割合の入力を正しく解く}\}$$

例: $GT(x,y) = 1 \Leftrightarrow x \geq y$ (辞書式順序)のとき，$D_{\frac{1}{4}}^{unif}(GT) \leq 2$

$$M_{GT_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Alice: xの最初のビットx_1送る
Bob: yの最初のビットy_1送る
$x_1 = 1 \,\&\, y_1 = 0 \rightarrow$ 1を出力
$x_1 = 0 \,\&\, y_1 = 1 \rightarrow$ 0を出力
それ以外は1を出力

Yaoのmin-max定理

[Yao's min-max theorem]

任意の$f: X \times Y \to \{0,1\}$および$\varepsilon > 0$について

$$R_{\varepsilon}^{pub}(f) = \max_{\mu} D_{\varepsilon}^{\mu}(f)$$

- 誤り確率εの乱択プロトコルの下界は$1-\varepsilon$以上の割合で正しく答えるような決定性プロトコルの解析に帰着
- 決定性プロトコルにとって平均的に難しい入力の分布を選べばよい

$R^{pub}(DISJ_n) = \Omega(n)$

① 以下をみたす$A \subseteq DISJ_n^{-1}(1), B \subseteq DISJ_n^{-1}(0)$と確率分布$\mu$を与える

1. $\mu(A) = \frac{3}{4}$
2. すべての矩形Rについて$\mu(R \cap B) \geq \alpha\mu(R \cap A) - 2^{-\delta n}$ (α, δは正定数)

② 十分小さい定数$\varepsilon > 0$について$D_\varepsilon^\mu(DISJ_n) \geq \delta n - O(1)$

- $D_\varepsilon^\mu(DISJ_n) = k$とするとそれを達成する決定性プロトコル$P$は入力を$2^k$個の矩形に分割：$R_1, R_2, \ldots, R_t$を出力が 1 となる矩形とする
- Pは$1-\varepsilon$の割合の入力で正しいので$\mu\left(\cup_{i=1}^t (R_i \cap A)\right) \geq \frac{3}{4} - \varepsilon$
- $R_i \cap B$に対応する入力ではPは間違っている
- Pの誤り確率$\geq \mu\left(\cup_{i=1}^t (R_i \cap B)\right) \geq \mu\left(\alpha\mu(R \cap A) - 2^{-\delta n}\right) \geq \alpha\left(\frac{3}{4} - \varepsilon\right) - 2^{k-\delta n}$
- Pの誤り確率$\leq \varepsilon$より十分小さい$\varepsilon > 0$に対して $k \geq \delta n - O(1)$

①みたす分布μとA, B

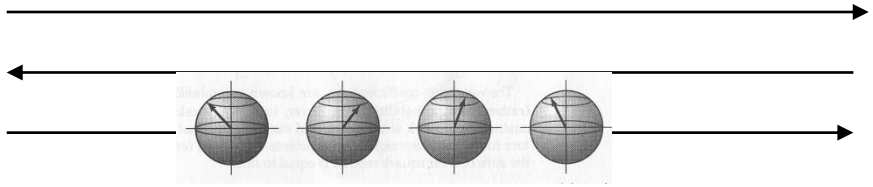
- μ: $n = 4l - 1$として以下を行う
  - $\{1,2, \dots, n\}$を$|T_1| = |T_2| = 2l - 1$, $|T_3| = 1$なる３つの集合T_1, T_2, T_3にランダムに分割
  - $|S_x| = l$なる集合S_xを$T_1 \cup T_3$からランダムに選ぶ
  - $|S_y| = l$なる集合S_yを$T_2 \cup T_3$からランダムに選ぶ
  - S_xの元に対応するビットを1，それ以外を0としたビット列をxとする
  - S_yの元に対応するビットを1，それ以外を0としたビット列をyとする
- A, B:
  - $A = \{(x, y): \mu(x, y) > 0 \ \& \ S_x \cap S_y = \emptyset\}$
  - $B = \{(x, y): \mu(x, y) > 0 \ \& \ S_x \cap S_y \neq \emptyset\}$

今回のはなし

- 古典通信複雑性
  - 決定性
  - 乱択
- 量子通信複雑性
  - 量子・古典ギャップ
  - 下界
- 応用

量子通信複雑性

入力 x



通信（**量子**ビット）

入力 y

量子アルゴリズム

量子アルゴリズム

fの量子通信複雑さ:= $f(x,y)$を計算するために必要な通信量（量子ビット列の長さ）

出力 $f(x,y)$

- 再びAndrew C.-C. Yao が導入[Yao93]
- $Q_\varepsilon(f) :=$ fを確率$1-\varepsilon$以上で正しく計算する最良の量子プロトコルで送られる総量子ビット数
- $Q(f) := Q_{1/3}(f)$

量子と古典（乱択）のギャップ

[BCW98] $Q(DISJ_n) = O(\sqrt{n}\log n)$ （cf. $R(DISJ_n) = \Omega(n)$）

- $\neg DISJ_n(x,y) = \bigvee_{j=1}^{n}(x_j \wedge y_j)$ と書けることから，Groverのアルゴリズムを利用（$x_j = y_j = 1$なるjを探索）
- より一般にあるタイプの関数に対する量子質問アルゴリズムを量子通信プトロトコルに変換

[AA03] $Q(DISJ_n) = O(\sqrt{n})$

[BCW98] H. Buhrman, R. Cleve, A. Wigderson, STOC'98, pp.63-68.
[AA03] A. Aaronson, A. Ambainis, FOCS'03, pp.200-209.

量子と古典（乱択）のギャップ

[BCW98] $Q(DISJ_n) = O(\sqrt{n}\log n)$ （cf. $R(DISJ_n) = \Omega(n)$）

- $\neg DISJ_n(x,y) = \bigvee_{j=1}^{n}(x_j \wedge y_j)$ と書けることから，Groverのアルゴリズムを利用（$x_j = y_j = 1$なるjを探索）

入力 $x \in \{0,1\}^n$

$$|\psi\rangle := \frac{1}{\sqrt{n}}\sum_{j=1}^{n}|j\rangle|0\rangle|0\rangle$$

入力 $y \in \{0,1\}^n$

量子と古典（乱択）のギャップ

[BCW98] $Q(DISJ_n) = O(\sqrt{n}\log n)$ （cf. $R(DISJ_n) = \Omega(n)$）

- $\neg DISJ_n(x,y) = \bigvee_{j=1}^{n}(x_j \wedge y_j)$ と書けることから，Groverのアルゴリズムを利用（$x_j = y_j = 1$なるjを探索）

入力 $x \in \{0,1\}^n$

$$\frac{1}{\sqrt{n}}\sum_{j=1}^{n}|j\rangle|x_j\rangle|0\rangle$$

入力 $y \in \{0,1\}^n$

量子と古典（乱択）のギャップ

[BCW98] $Q(DISJ_n) = O(\sqrt{n}\log n)$ （cf. $R(DISJ_n) = \Omega(n)$）

- $\neg DISJ_n(x,y) = \bigvee_{j=1}^{n}(x_j \wedge y_j)$ と書けることから，Groverのアルゴリズムを利用（$x_j = y_j = 1$なるjを探索）

入力 $x \in \{0,1\}^n$

$$\frac{1}{\sqrt{n}}\sum_{j=1}^{n}|j\rangle|x_j\rangle|x_j \wedge y_j\rangle$$

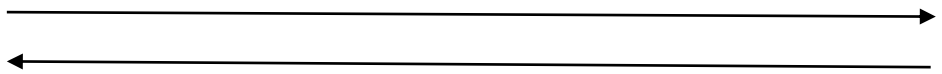
入力 $y \in \{0,1\}^n$

量子と古典（乱択）のギャップ

[BCW98] $Q(DISJ_n) = O(\sqrt{n}\log n)$ （cf. $R(DISJ_n) = \Omega(n)$）

- $\neg DISJ_n(x,y) = \bigvee_{j=1}^{n}(x_j \wedge y_j)$ と書けることから，Groverのアルゴリズムを利用（$x_j = y_j = 1$なるjを探索）

入力 $x \in \{0,1\}^n$



入力 $y \in \{0,1\}^n$

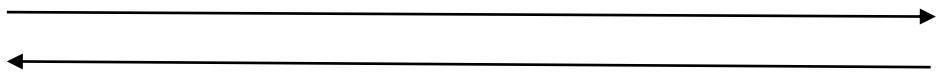
$$\frac{1}{\sqrt{n}}\sum_{j=1}^{n}|j\rangle|0\rangle|x_j \wedge y_j\rangle$$

量子と古典（乱択）のギャップ

[BCW98] $Q(DISJ_n) = O(\sqrt{n}\log n)$ （cf. $R(DISJ_n) = \Omega(n)$）

- $\neg DISJ_n(x,y) = \bigvee_{j=1}^{n}(x_j \wedge y_j)$ と書けることから，Groverのアルゴリズムを利用（$x_j = y_j = 1$なるjを探索）

入力 $x \in \{0,1\}^n$



入力 $y \in \{0,1\}^n$

$$\frac{1}{\sqrt{n}}\sum_{j=1}^{n}(-1)^{x_j \wedge y_j}|j\rangle|0\rangle|x_j \wedge y_j\rangle$$

量子と古典（乱択）のギャップ

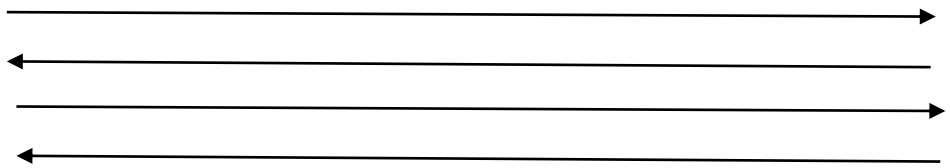
[BCW98] $Q(DISJ_n) = O(\sqrt{n}\log n)$ （cf. $R(DISJ_n) = \Omega(n)$）

- $\neg DISJ_n(x,y) = \bigvee_{j=1}^{n}(x_j \wedge y_j)$ と書けることから，Groverのアルゴリズムを利用

平均に関する折り返し$I - 2|\psi\rangle\langle\psi|$ とともに繰り返す

$$|\psi\rangle := \frac{1}{\sqrt{n}}\sum_{j=1}^{n}|j\rangle|0\rangle|0\rangle$$

入力 $x \in \{0,1\}^n$



入力 $y \in \{0,1\}^n$

$$\frac{1}{\sqrt{n}}\sum_{j=1}^{n}(-1)^{x_j \wedge y_j}|j\rangle|0\rangle|0\rangle$$

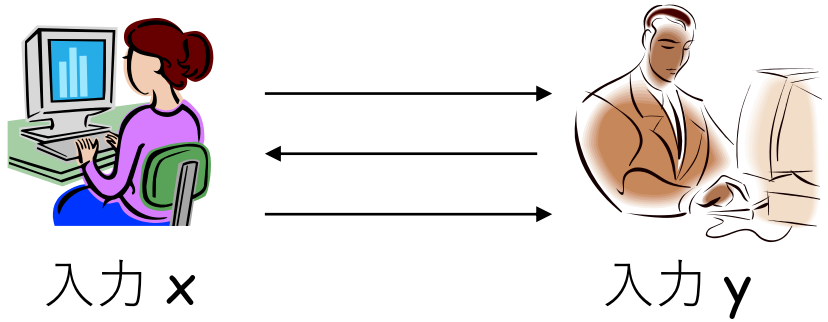
データベースへの質問完了

EQの量子通信複雑性

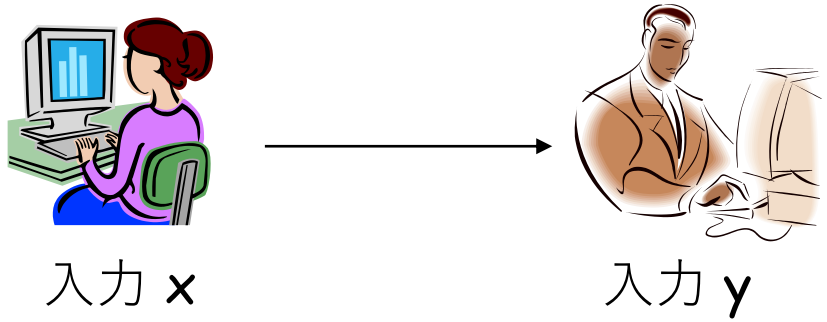
- 古典の乱択プロトコルで十分効率的
  - $R(EQ_n) = O(\log n)$
  - $R^{pub}(EQ_n) = O(1)$
- プロトコルの通信形態をもっと制約したらどうか？
  - 双方向通信（制限なし）
  - ラウンド数制限
  - 一方向通信（１ラウンド）
  - 同時通信型モデル（SMP: Simultaneous Message Passing）
- 通信形態を制限されたモデルは応用上も重要

EQの古典通信複雑性（通信形態制限）

制限なし（双方向）



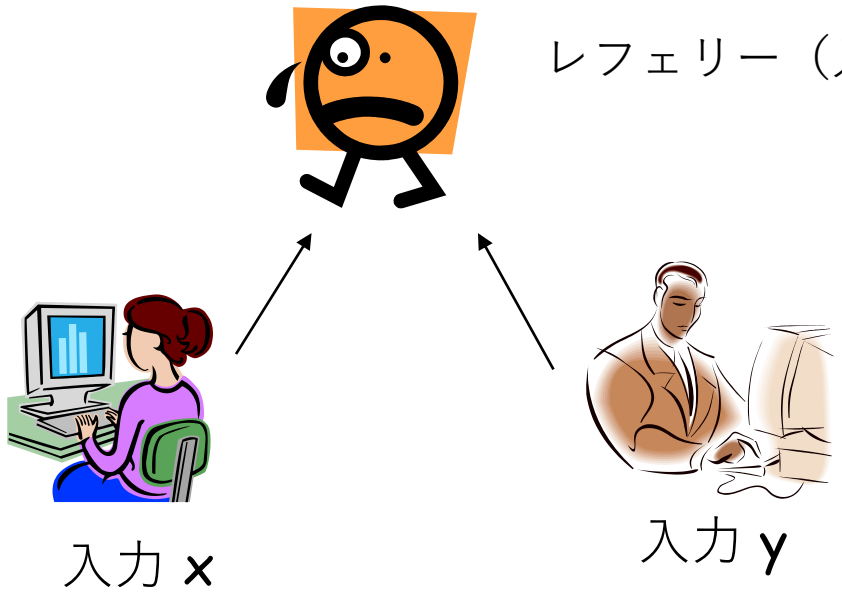
一方向



共有乱数なし O(log n)　共有乱数あり O(1)

SMP（同時通信型）

共有乱数あり O(1)



共有乱数なし Θ(√n)　[Ambainis96, Nisan-Szegedy96, Babai-Kimmel97]

プロトコルの強さ

SMP ≤ 一方向 ≤ 双方向

弱 ⟷ 強

共有乱数ありの古典SMPプロトコル

c.f. 共有乱数なし Θ(√n)
[Amb96, NS96, BK97]

レフェリー
（入力なし）

$C(x)_i = C(y)_i$ なら $x=y$
さもなければ $x \neq y$
と判定

$C(x)_i$

$C(y)_i$

x の符号（符号長
m=O(n) ）の第 i ビット

入力
$x \in \{0,1\}^n$

共有ランダムビット列 $i \in \{1,2,\ldots,m\}$

入力
$y \in \{0,1\}^n$

∃誤り訂正符号 C: $\{0,1\}^n \to \{0,1\}^m$; 任意の異なる n bits x, yに対して
$\mathrm{Ham}(C(x), C(y)) \geq 0.99m$

通信量O(1)，成功率0.99

EQに対する量子プロトコル

[Buhrman-Cleve-Watrous-de Wolf 01]

Referee はAliceとBobから送られた状態に対して量子的操作 （C-SWAP）

Referee: 入力なし

ポイント：

$x=y$：2つの状態は同じ

$x \neq y$：2つの状態はほぼ直交

O(log n)量子ビットで高確率で $x=y$かを判定可能

$$|\phi_x\rangle = \sum_i |i\rangle |C(x)_i\rangle$$

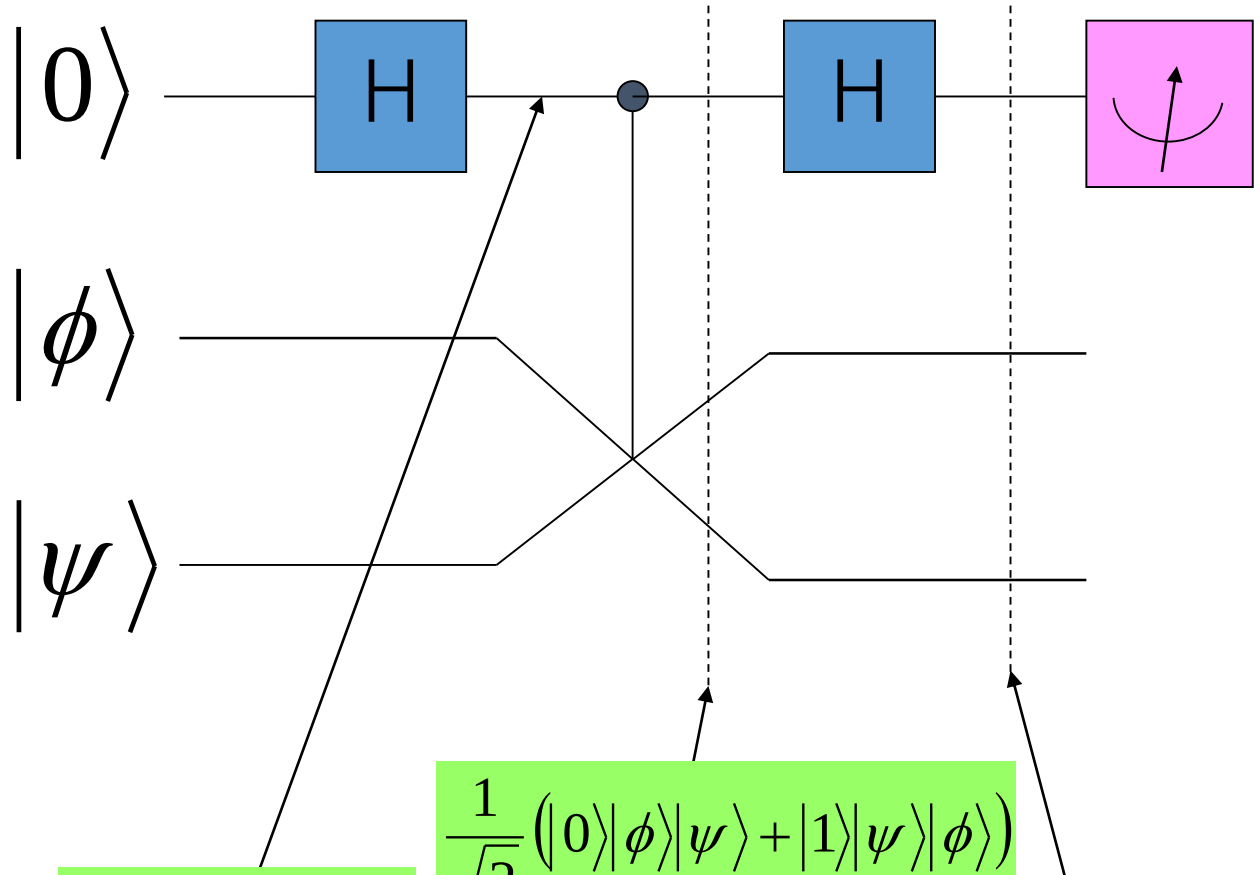
$$|\phi_y\rangle = \sum_i |i\rangle |C(y)_i\rangle$$

x の符号（符号長 O(n)）の第 i ビット

Alice： 入力　x（長さ n）

Bob： 入力 y（長さ n）

(Controlled)　Swap Test



Pr[測定値=0]=

$$\frac{1}{2}\left(1+\left|\langle\psi|\phi\rangle\right|^2\right)$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle|\phi\rangle|\psi\rangle+|1\rangle|\psi\rangle|\phi\rangle\right)$$

$$\frac{1}{2}\left(|0\rangle\left(|\phi\rangle|\psi\rangle+|\psi\rangle|\phi\rangle\right)+|1\rangle\left(|\phi\rangle|\psi\rangle-|\psi\rangle|\phi\rangle\right)\right)$$

EQに対する量子プロトコル

[Buhrman-Cleve-Watrous-de Wolf 01]

$Q^{\|}(EQ_n) = O(\log n)$

ポイント：

$x=y$：2つの状態は同じ

$x \neq y$：2つの状態はほぼ直交

O(log n)量子ビットで高確率で $x=y$かを判定可能

Referee はAliceとBobから送られた状態に対して量子的操作 （C-SWAP）

Referee: 入力なし

$|\phi_x\rangle = \sum_i |i\rangle |C(x)_i\rangle$

$|\phi_y\rangle = \sum_i |i\rangle |C(y)_i\rangle$

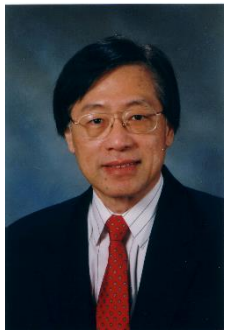
x の符号（符号長 O(n)）の第 i ビット

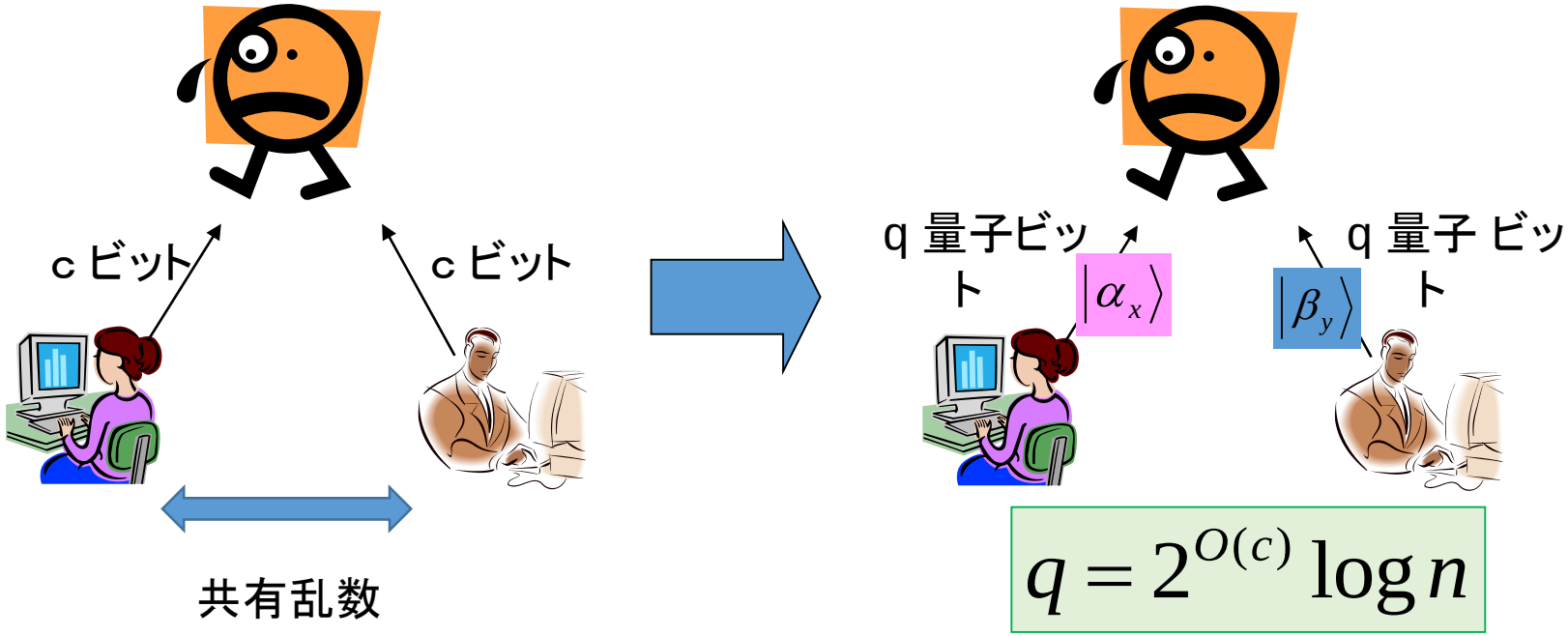
Alice： 入力　x（長さ n）

Bob： 入力 y（長さ n）

共有乱数古典プロトコルの量子指紋による模倣

[Yao03]





とくに，$R^{||,pub}(f) = O(1)$ なら $Q^{||}(f) = O(\log n)$:
共有乱数古典プロトコルがO(1)プロトコルなら
O(log n)量子指紋プロトコルに変換できる.（EQはその典型例）

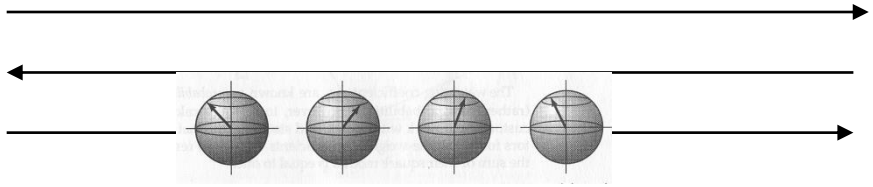
量子・古典間ギャップ

- 最初の量子古典間ギャップ [Buhrman-Cleve-Wigderson98]
  - 関数DISJ(x,y)（x_i=y_i=1となる i が存在するか否か）のO(√n log n)量子プロトコル（古典はΩ(n)なので２乗のギャップ）
- 最初の指数的ギャップ [Raz99]
  - 問題：（Aliceの入力）ベクトル$\boldsymbol{v}$ 直交する２つの部分空間 H_0, H_1（Bobの入力） ユニタリ U,（出力） $U\boldsymbol{v}$が H_0に近いかH_1に近いか？
  - 量子O(log n) vs. 古典Ω($n^{1/4}$/log n)
- SMPモデルにおける指数的ギャップ[Buhrman-Cleve-Watrous-de Wolf01]
  - 関数EQに対するO(log n)量子プロトコル（古典はΩ(√n)）
  - 量子指紋（quantum fingerprinting）のアイデア
- 一方向通信モデルにおける指数的ギャップ[Bar-Yossef, Jayram, Kerenidis04]
  - 量子O(log n) vs. 古典Ω(√n)
  - 共有乱数ありSMPでの指数的ギャップも示す（Hidden Matching Problem）
  - ブール関数で同様のギャップ [Gavinsky-Kempe-Kerenidis-Raz-de Wolf 2008]
- 量子SMPの古典双方向モデルに対する指数的優位性 [Gavinsky 1911.01381]

量子通信複雑性(共有エンタングルメント有)

入力 x

量子アルゴリズム



通信（**量子**ビット）

共有エンタングルメント

入力 y

量子アルゴリズム

出力 $f(x,y)$

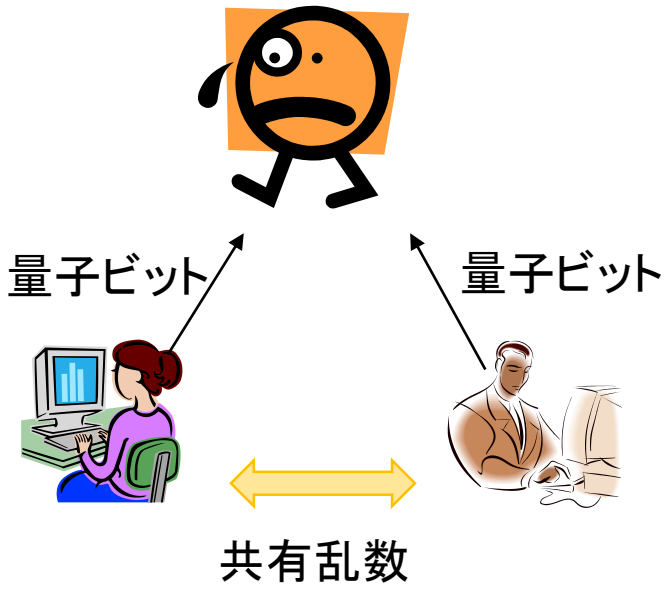
fの量子通信複雑さ $Q^{ent}(f) := f(x,y)$を計算するために必要な通信量（量子ビット列の長さ）

Q. $Q^{ent}(f)$は$Q(f)$と複雑さに差はないのか？

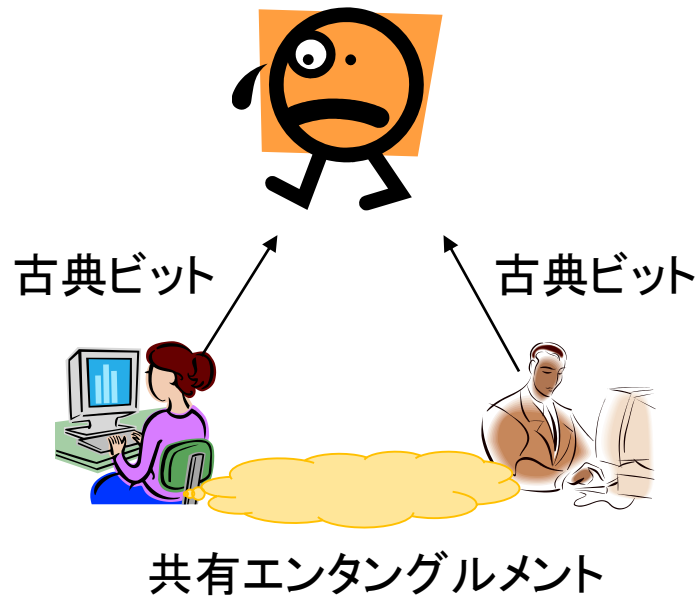
Cf. [Newman91] $R_{\varepsilon+\delta}(f) \leq R_{\varepsilon}^{pub}(f) + O(\log\log|X||Y| + \log(1/\delta))$

共有エンタングルメントの有用性

[Gavinsky-Kempe-Regev-de Wolf 08]



通信量＝$\Omega(n^{1/3}/\log n)$



通信量＝$O(\log n)$

問題 [Modified Hidden Matching Problem]

Aliceの入力：$x\in\{0,1\}^n$；Bobの入力：perfect matching $M=\{(i_1,j_1),(i_2,j_2),\ldots,(i_{n/2},j_{n/2})\}$，$y\in\{0,1\}^{n/2}$

出力：$(i, j, y_{L(i,j)}, x_i\oplus x_j)$ s.t. $(i, j)\in M$，ただし，$L(i,j)$は(i,j)のM内の順位

量子通信複雑性の下界

- 古典より難しい
  - Yaoのmin-max定理使って決定性の場合に帰着できない
- 主な手法
  - 多項式による近似
  - 行列解析
  - 量子情報理論的手法
    - 量子情報複雑性（quantum information complexity）

$DISJ_n$の量子通信複雑性の下界

[Razborov03] $Q(DISJ_n) = \Omega(\sqrt{n})$

- 上界とオーダ的に一致
- 受理確率を多項式で表現して，多項式による近似理論を利用
- AliceとBobがエンタングルメントを共有していてもOK

[ラウンド数が制限された場合]

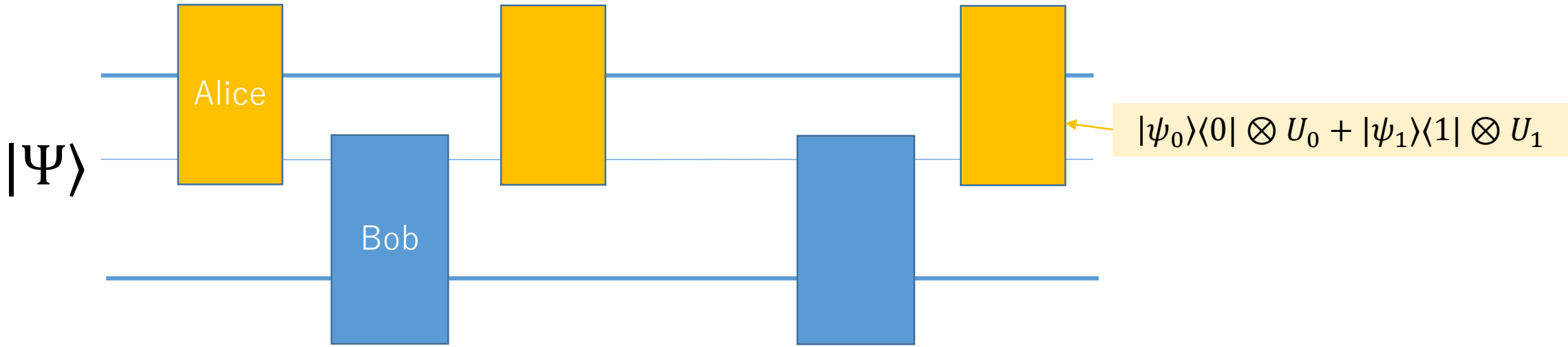
- mラウンドで$DISJ_n$を解くには$\widetilde{\Omega}(\frac{n}{m} + m)$個の量子ビットの通信が必要 [BGKMT18]
- 量子情報複雑性の議論を利用

$Q(DISJ_n) = \Omega(\sqrt{n})$

[Lemma(Kremer-Yao)] $|\Psi\rangle$をプロトコルの初期状態とすると，プロトコルの受理確率（最後は通信ビットを計算基底で測るとする）は

$$P(x,y) = \left\| \sum_{h\in\{0,1\}^q} \left(A_h(x) \otimes B_h(y)\right)|\Psi\rangle \right\|^2$$

と書ける．ただし，qはプロトコルの通信ビット数で$||A||, ||B|| \leq 1$



Kremer-Yao Lemma

[Lemma(Kremer-Yao)] $|\Psi\rangle$をプロトコルの初期状態とすると，プロトコルの受理確率（最後は通信ビットを計算基底で測るとする）は

$$P(x,y) = \left\| \sum_{h\in\{0,1\}^q} \left(A_h(x) \otimes B_h(y)\right)|\Psi\rangle \right\|^2$$

と書ける．ただし，qはプロトコルの通信ビット数で$||A||, ||B|| \leq 1$

とくに，$|\Psi\rangle = |\Psi_A\rangle \otimes |\Psi_B\rangle$(共有エンタングルメントなし)なら

$$P(x,y) = \sum_{h,k\in\{0,1\}^q} \underbrace{\langle\Psi_A|A_h(x)^* A_k(x)|\Psi_A\rangle}_{=2^q\text{次行ベクトル}a(x)\text{の(h,k)成分}} \underbrace{\langle\Psi_B|B_h(y)^* B_k(y)|\Psi_B\rangle}_{=2^q\text{次列ベクトル}b(y)\text{の(h,k)成分}}$$
$$= a(x)b(y)$$

[Corollary] Pは$P = AB$と分解可能．ただし，Aは$|X| \times 2^q$行列，Bは$2^q \times |Y|$行列で各成分の絶対値は１以下

プロトコル→多項式

[多項式近似補題]

$$P(i) = E_{(x,y):|x|=|y|=\frac{n}{4},|x\wedge y|=i}[P(x,y)]$$

とすると，すべての$d \leq \frac{n}{4}$に対して，

$$|P(j) - \tilde{p}(j)| \leq 2^{2q-\frac{d}{4}} \ (j = 0,1,\cdots,\frac{n}{8})$$

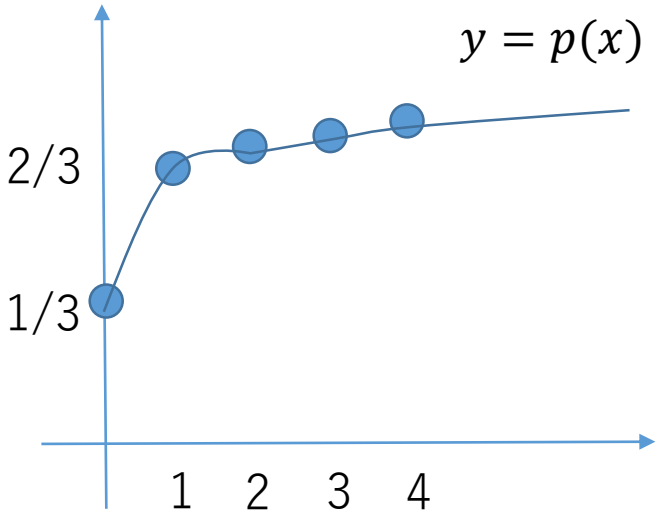
となる次数dの多項式$\tilde{p}$が存在する．

（証明の流れ）ハミング重み$\frac{n}{4}$のx,yについて行列$P = P(x,y)$を考えたとき，
すべてのjで$P(j) = p(j)$となる次数$\frac{n}{4}$の多項式$p(i)$が（組み合わせ行列の理論から）得られる．

$p(i)$を次数dで切った近似多項式$\tilde{p}(i)$の差は$\frac{2^{-\frac{d}{4}}}{N}\|P\|_{tr}$（ただし，$N = \binom{n}{n/4}$）でおさえられ，
Kremer-Yao（Corollary）を使うと，$\|P\|_{tr} \leq \|A\|_F\|B\|_F \leq N2^{2q}$がいえる．

$Q(\neg DISJ_n) = \Omega(\sqrt{n})$

- $P(i) = E_{(x,y):|x|=|y|=\frac{n}{4},|x\wedge y|=i}[P(x,y)]$は以下をみたす
  - $P(0) \in [0,1/3]$
  - $P(i) \in [2/3,1]$ $(i = 1,2,\dots,n/8)$
- 多項式近似補題で$d = 8q + [4\log_2 1/\varepsilon]$とすると，
  - $\tilde{p}(0) \in [-\varepsilon, \frac{1}{3} + \varepsilon]$
  - $\tilde{p}(i) \in [\frac{2}{3} - \varepsilon, 1 + \varepsilon]$ $(i = 1,2,\dots,n/8)$



- 狭い値域で急激に上がる（微分係数が高くなる）多項式$\tilde{p}$の次数dは高くなる

[EZ64,RC66] $b_1 \le p(i) \le b_2$が全ての整数$i \in \{0,1,\dots,N\}$で成立し，$|p'(x)| \ge c$があるx ∈ [0, N]で成り立つなら，$\deg(p) \ge \sqrt{cN/(c + b_2 - b_1)}$

- $\exists c \ge \frac{1}{3} - 2\varepsilon$（平均値の定理），$b_1 = 0, b_2 = n/8$とすれば $d = \Omega(\sqrt{n})$ゆえ，
  $q = \Omega(\sqrt{n})$

近似ランク

- 行列Mがfの通信行列M_fを近似するとは，すべてのx, yについて $\left|M(x,y) - M_f(x,y)\right| \leq 1/3$ をみたす
- $\widetilde{rank}(f) = \min_M \{rank(M) | M$は$M_f$を近似する$\}$

[Buhrman-de Wolf01]

$$Q(f) = \Omega(\log_2 \widetilde{rank}(f))$$

(証明) Kremer-Yaoよりプロトコルの受理確率行列を$P = (P(x,y))$（PはM_fを近似する），qを通信ビット数とすると

$$\widetilde{rank}(f) \leq rank(P) = rank(AB) \leq 2^q$$

(Aは$|X| \times 2^q$行列，Bは$2^q \times |Y|$行列だった)

Cf. $D(f) = \Omega(\log_2 rank(f))$

Log-rank Conjecture

[log-rank conjecture [Lovasz-Saks88]] 任意のブール関数$f:\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$に対して，$D(f) = O(\log^c rank(f))$ (cは定数)

⇒未解決

- $\forall f\ [D(f) = \tilde{O}(\sqrt{rank(f)})]$ [Lov16]
- $\exists f\ [D(f) = \tilde{\Omega}(\log^2 rank(f))]$ [GPW18]

[(quantum) log-approximate-rank conjecture [LS09]]

任意のブール関数$f:\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$に対して，$R(f) = O(\log^c rank(f))$ (cは定数)あるいは$Q(f) = O(\log^c rank(f))$ (cは定数)

⇒否定的に解決！

- $\exists f\ [R(f) = \Omega(\sqrt{n})\ \&\ \log rank(f) = O(\log n)]$ [CMS19]
- $\exists f\ [Q(f) = \Omega(n^{1/6})\ \&\ \log rank(f) = O(\log n)]$ [ABT19,SW19]

今回のはなし

- 古典通信複雑性
  - 決定性
  - 乱択
- 量子通信複雑性
  - 量子・古典ギャップ
  - 下界
- 応用

通信複雑さの応用例

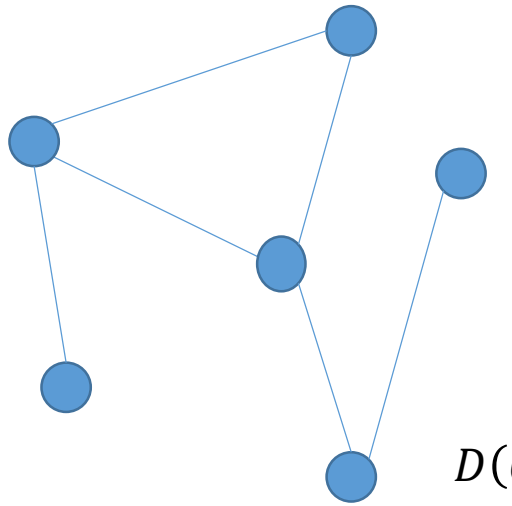
- VLSI
- 決定木，データ構造
- 回路計算量
- Turing機械，分岐プログラム
- ストリーミングアルゴリズム
- 性質検査（property testing）
- 分散計算

…

- 量子力学の非局所性
- 量子ランダムアクセス符号(INDEX関数)

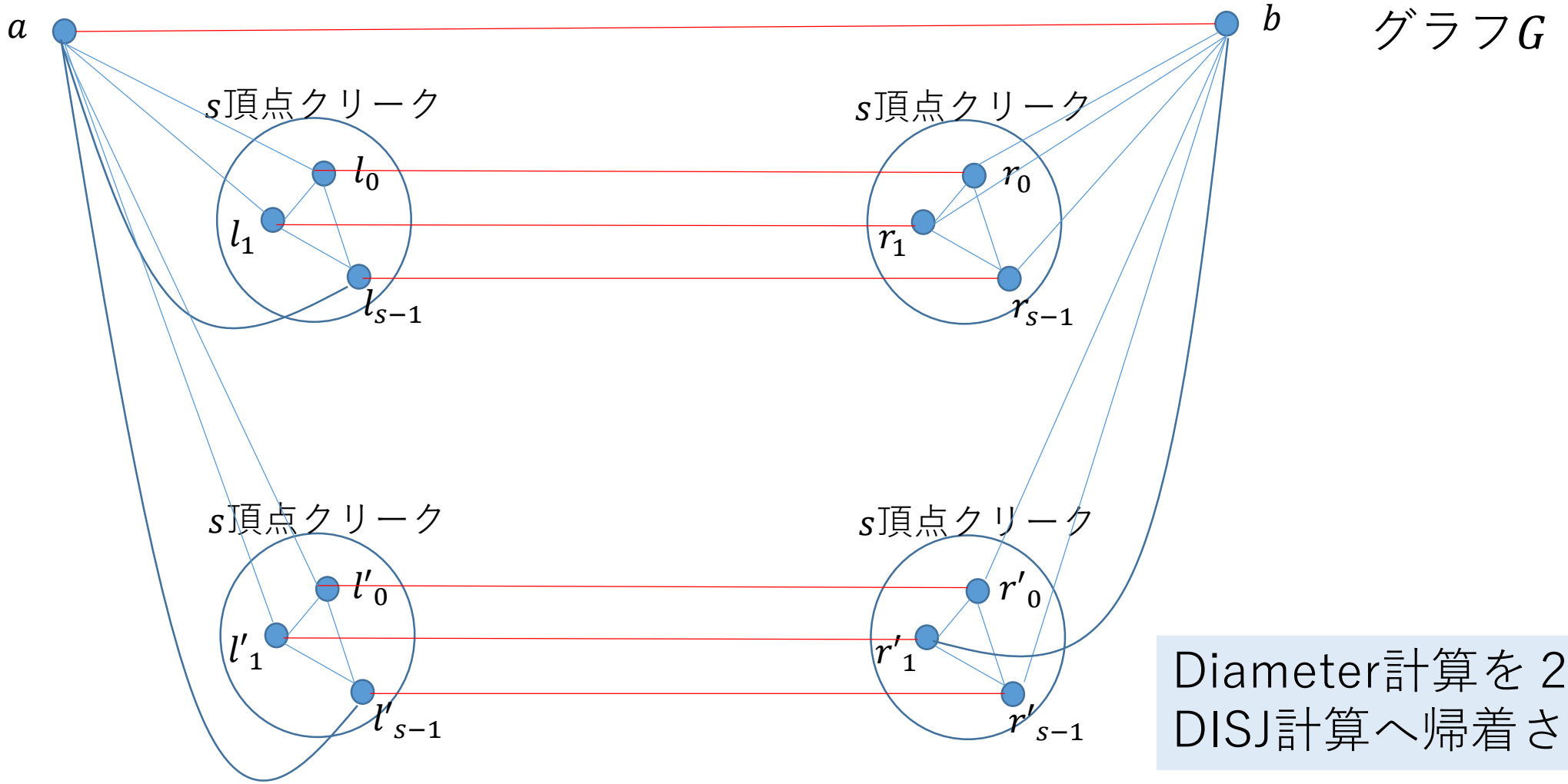
分散計算における直径(Diameter)の計算

- 分散計算:=グラフ上の各頂点は局所的な情報しか知らず，通信により，計算を行う
  - Congest model:=グラフ上の各頂点は１ラウンドあたり各隣接辺に O(log n)(量子)ビットしか送れない（n：グラフの頂点数）
- グラフGの直径 $D(G)$:=G上で最も離れている２頂点間の距離
- 直径を計算するのに必要なラウンド数
  - 古典：$\Theta(n)$ [HW12,PRT12,FHW12]
  - 量子：
    - 上界 $\tilde{O}(\sqrt{nD})$ [LM18]
    - 下界 $\tilde{\Omega}(\sqrt{n}+D)$ [LM18]
      $\tilde{\Omega}(\sqrt[3]{nD^2}+\sqrt{n}+D)$ [MN20]



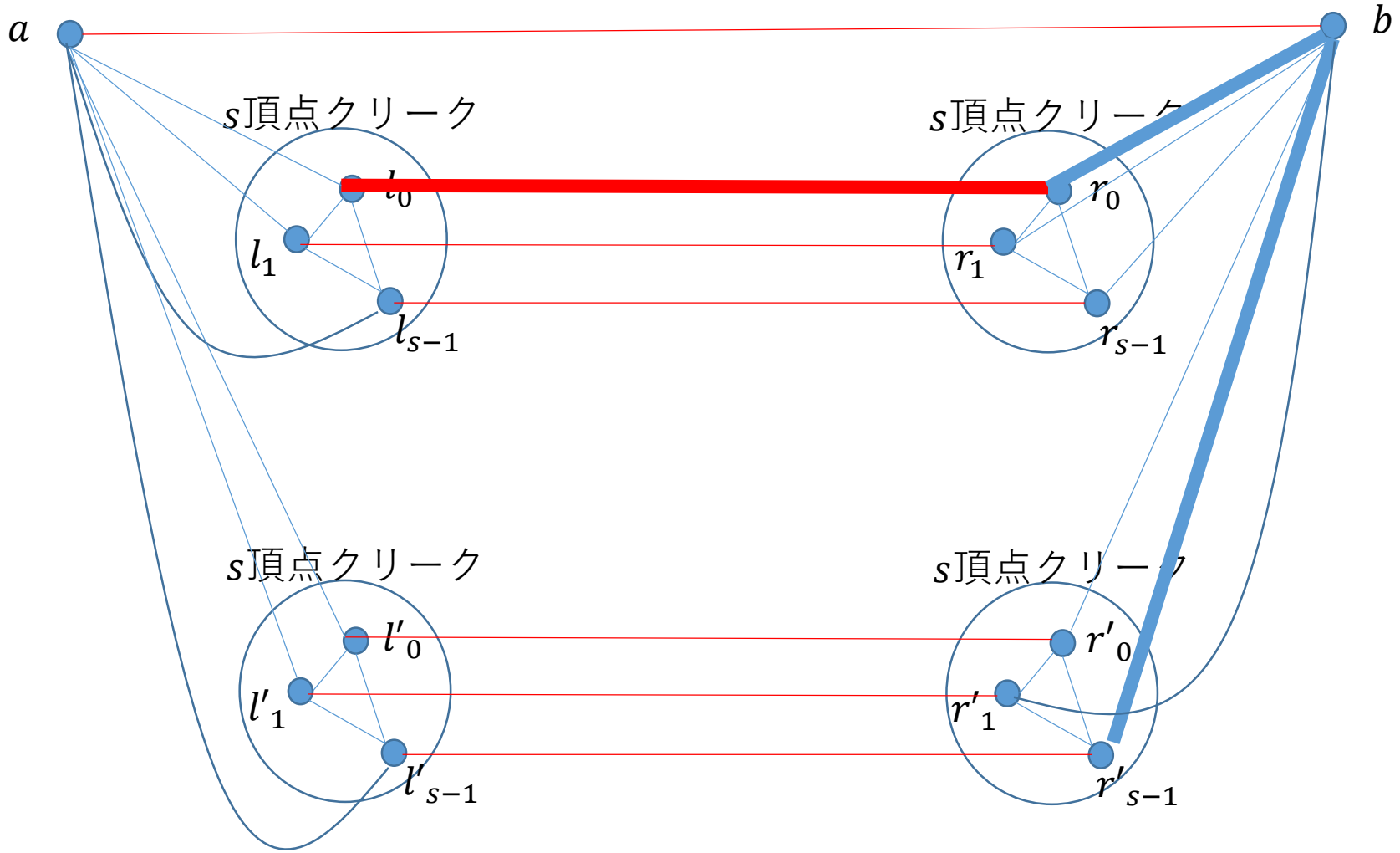
$D(G)=4$

Diameterのラウンド数下界



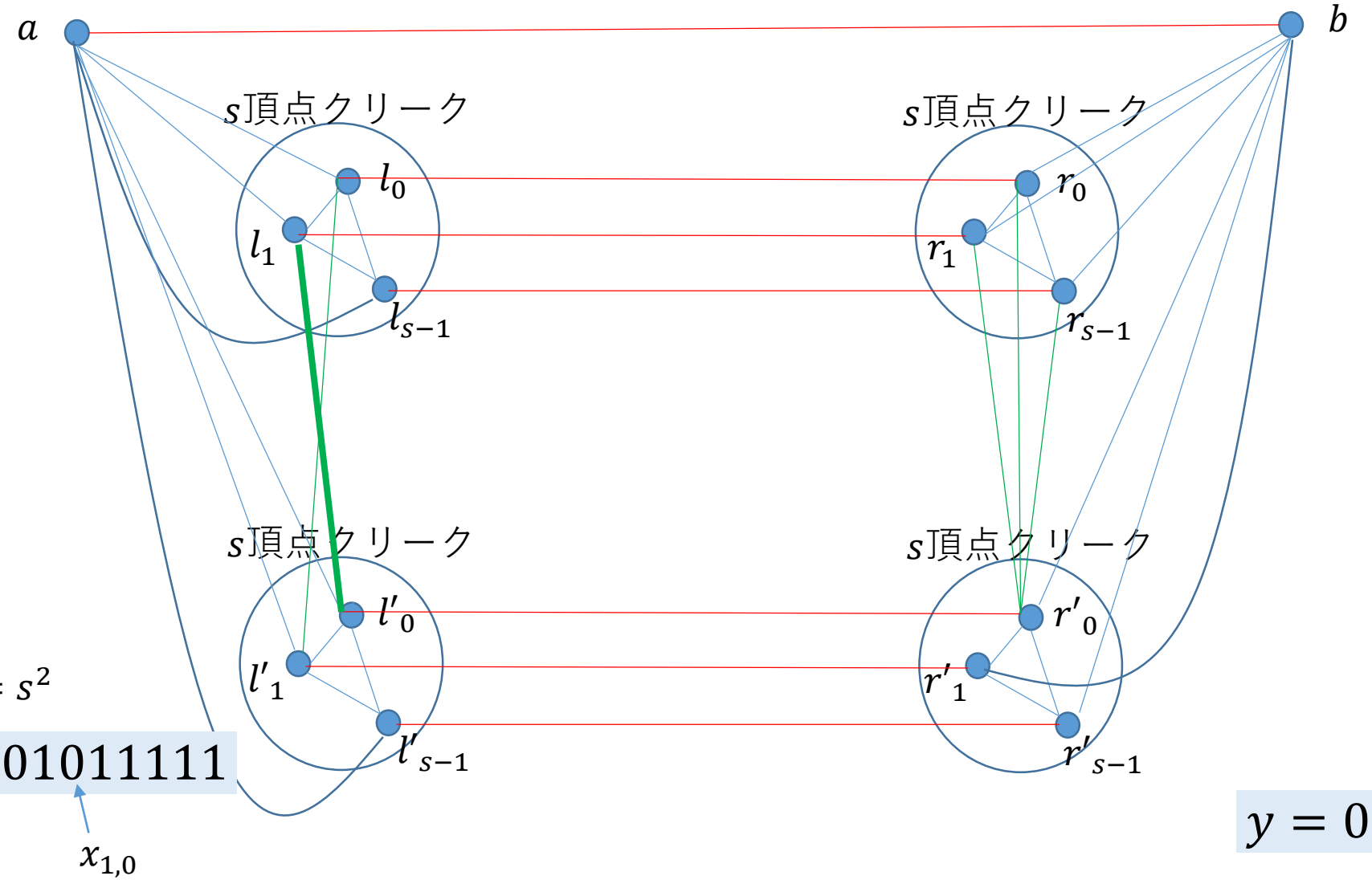
Diameter計算を 2 者間の
DISJ計算へ帰着させる

DiameterからDISJ



グラフG
直径は３

DiameterからDISJ



グラフG'

- $x_{i,j} = 0$ のときl_iとl'_jを辺で結ぶ
- $y_{i,j} = 0$ のときr_iとr'_jを辺で結ぶ

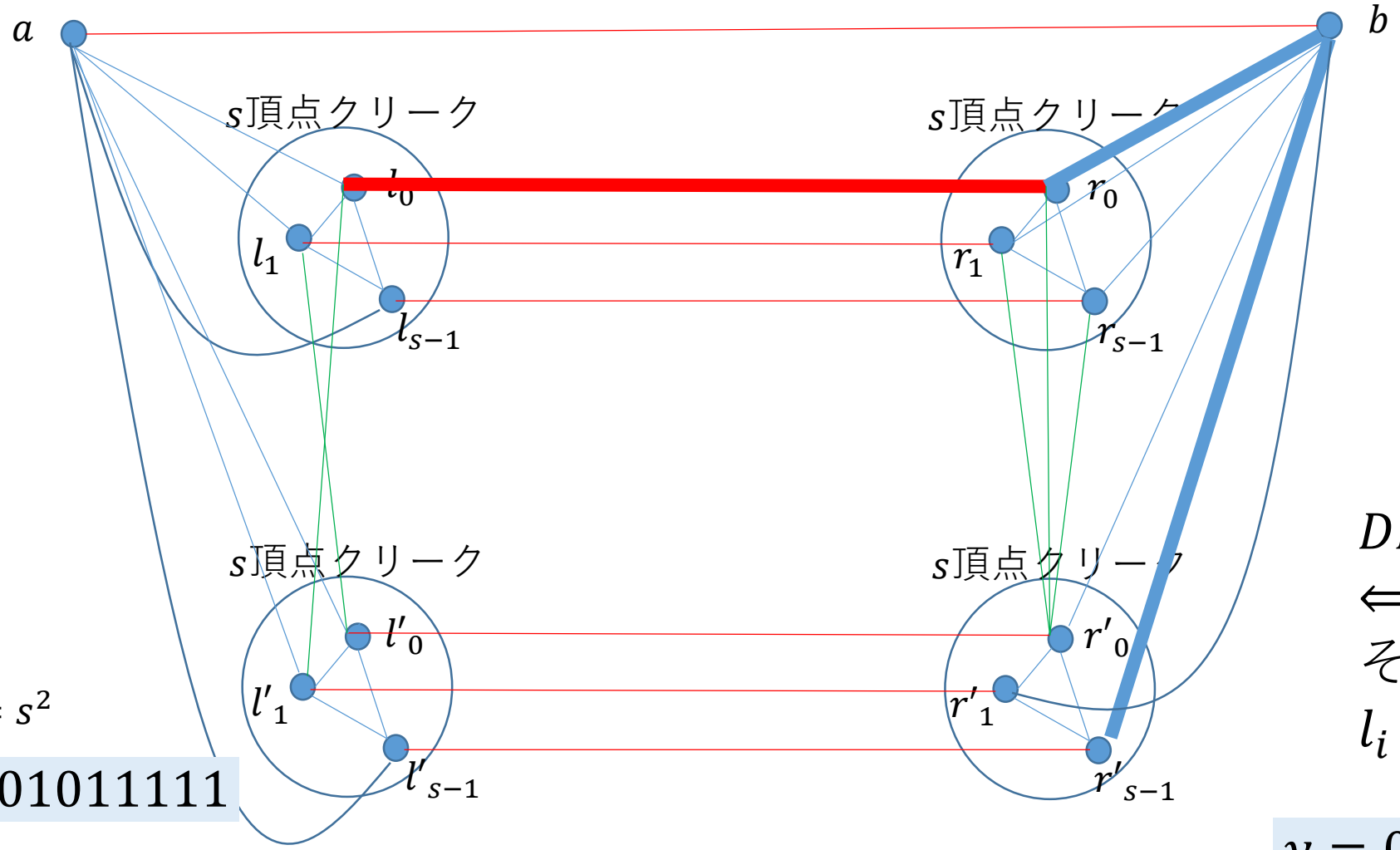
長さ$k = s^2$

$x = 101011111$

$x_{1,0}$

$y = 011011011$

DiameterからDISJ



長さ$k = s^2$

$x = 101011111$

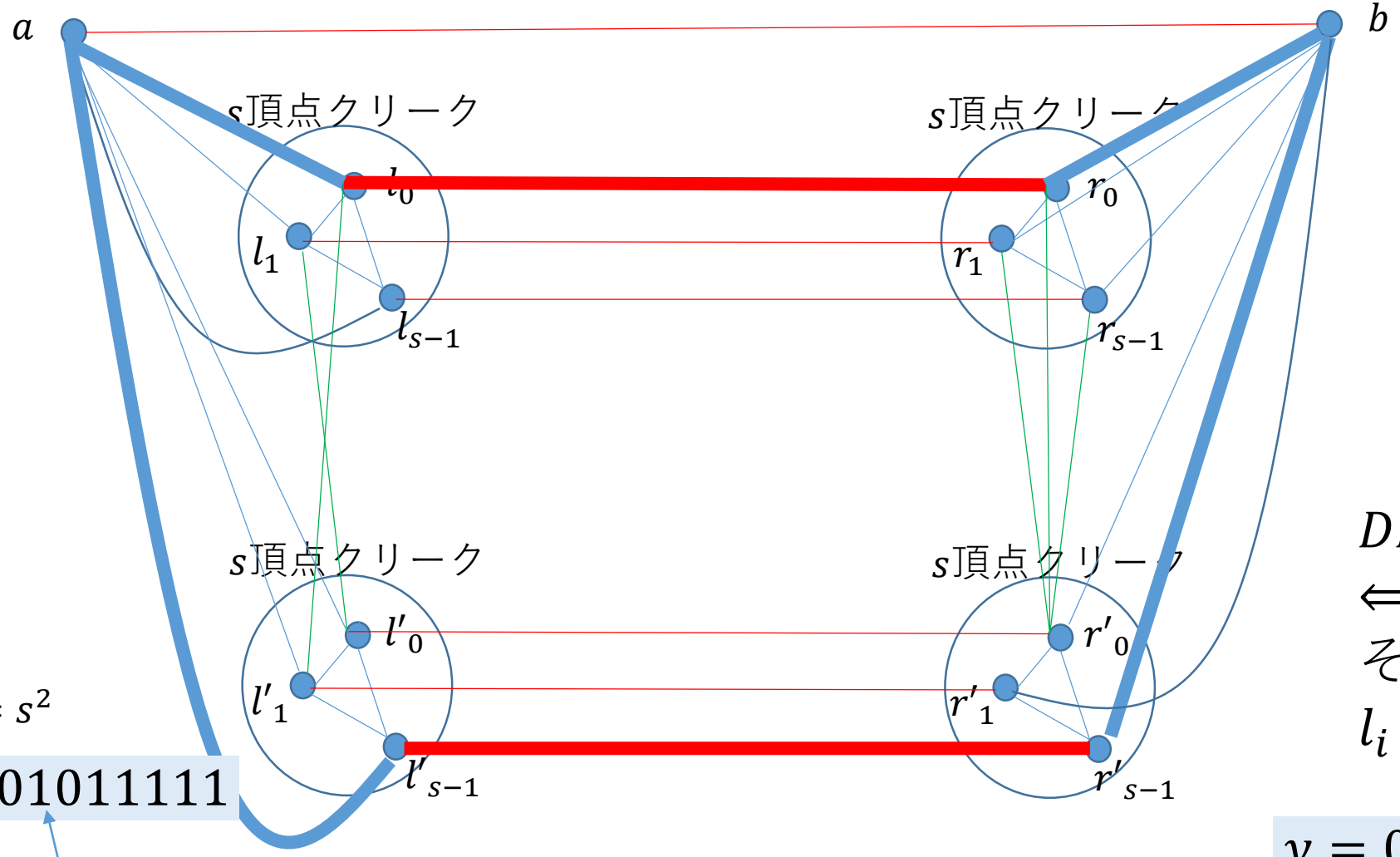
グラフG'

- $x_{i,j} = 0$ のときl_iとl'_jを辺で結ぶ
- $y_{i,j} = 0$ のときr_iとr'_jを辺で結ぶ

$DISJ_k(x, y) = 1$
$\Leftrightarrow \exists i, j : x_{i,j} = y_{i,j} = 1$
そのようなi, jについて
l_iとr'_jの距離は3

$y = 011011011$

DiameterからDISJ



長さ$k = s^2$

$x = 101011111$

$x_{0,s-1}$

グラフG'

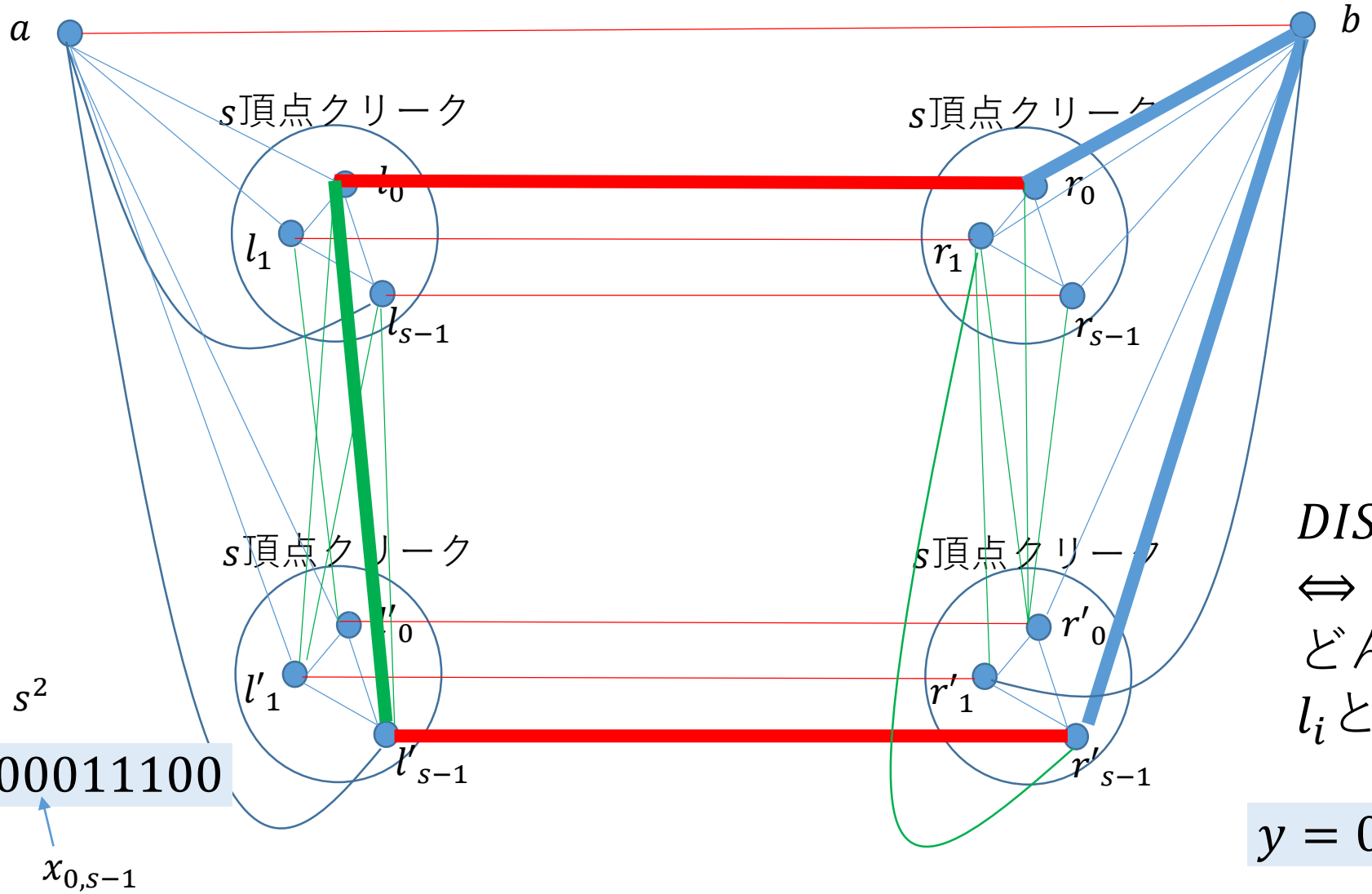
- $x_{i,j} = 0$ のときl_iとl'_jを辺で結ぶ
- $y_{i,j} = 0$ のときr_iとr'_jを辺で結ぶ

$DISJ_k(x, y) = 1$
$\Leftrightarrow \exists i, j : x_{i,j} = y_{i,j} = 1$
そのようなi, jについて
l_iとr'_jの距離は3

$y = 011011011$

DiameterからDISJ

- $DISJ_k(x,y) = 1 \rightarrow D(G') = 3$
- $DISJ_k(x,y) = 0 \rightarrow D(G') = 2$



グラフG'

- $x_{i,j} = 0$ のとき l_iとl'_jを辺で結ぶ
- $y_{i,j} = 0$ のとき r_iとr'_jを辺で結ぶ

$DISJ_k(x,y) = 0$
$\Leftrightarrow \forall i,j: x_{i,j} = 0 \; or \; y_{i,j} = 0$
どんなi,jについても
l_iとr'_jの距離は2

長さ$k = s^2$

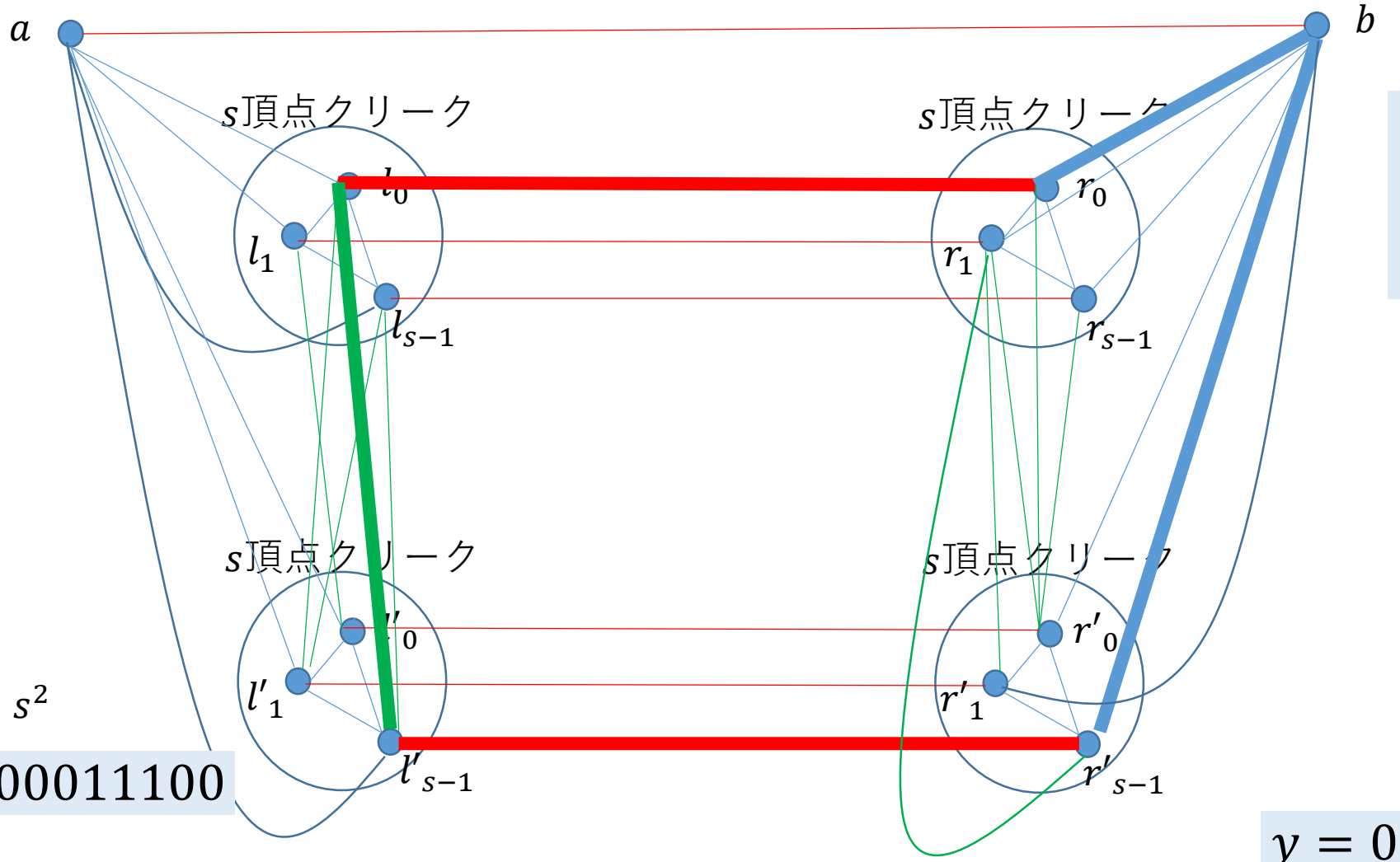
$x = 100011100$

$x_{0,s-1}$

$y = 011000011$

DiameterからDISJ

- $DISJ_k(x,y) = 1 \rightarrow D(G') = 3$
- $DISJ_k(x,y) = 0 \rightarrow D(G') = 2$



$D(G') = 3$か$= 2$かmラウンドで判定できるとすると：

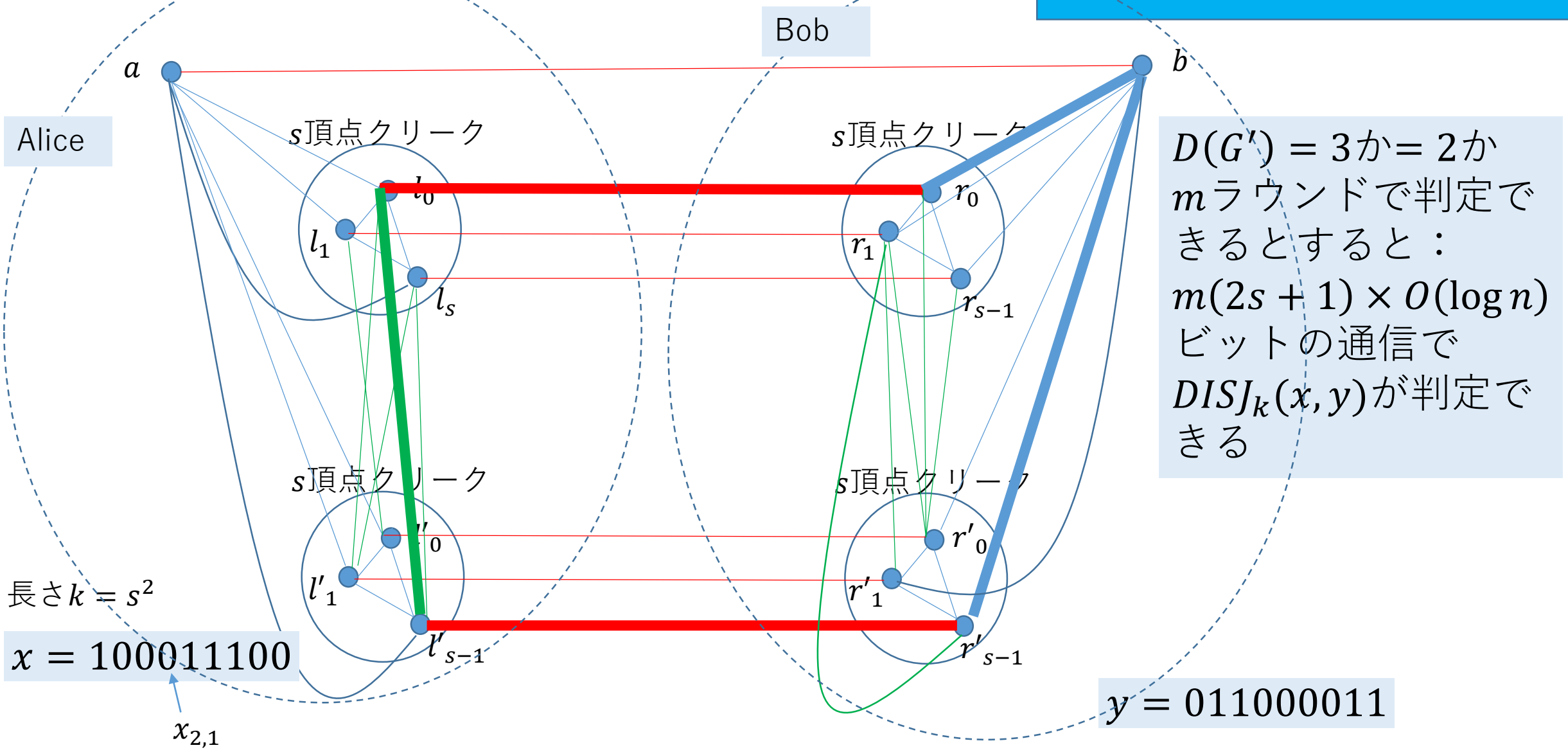
長さ$k = s^2$

$x = 100011100$

$y = 011000011$

DiameterからDISJ

- $DISJ_k(x,y) = 1 \rightarrow D(G') = 3$
- $DISJ_k(x,y) = 0 \rightarrow D(G') = 2$



$D(G') = 3$か$= 2$かmラウンドで判定できるとすると：
$m(2s+1) \times O(\log n)$ビットの通信で$DISJ_k(x,y)$が判定できる

分散計算(congest model)におけるDiameterの下界

[LM18]

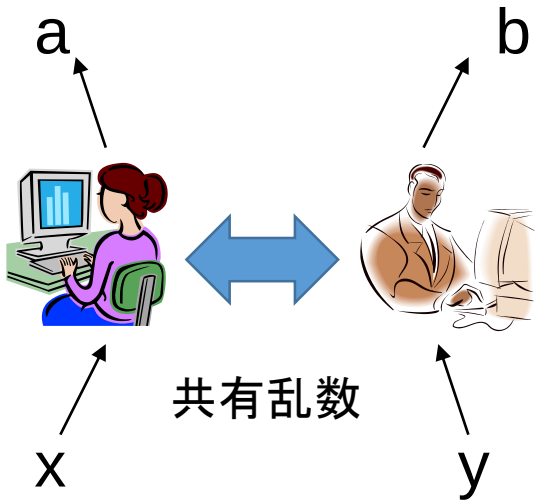
- $D(G') = 3$か$= 2$かmラウンドで判定できるとすると：

$$m(2s+1) \times O(\log n)$$

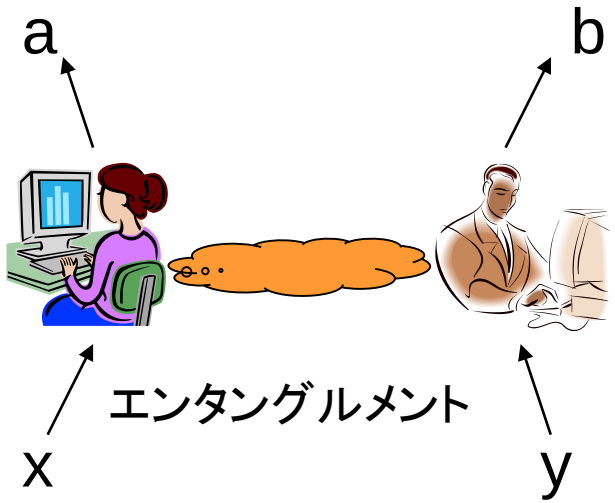
ビットの通信で$DISJ_k(x, y)$が判定できる

- $DISJ_k$のmラウンド量子通信計算量$=\Omega(\frac{k}{m} + m)$ [BGKMT18]
- $m \geq \tilde{\Omega}\left(\sqrt{\frac{k}{s}}\right) = \tilde{\Omega}(s) = \tilde{\Omega}(\sqrt{n})$
- $\Omega(D)$は自明なので下界$\tilde{\Omega}(\sqrt{n} + D)$を得る

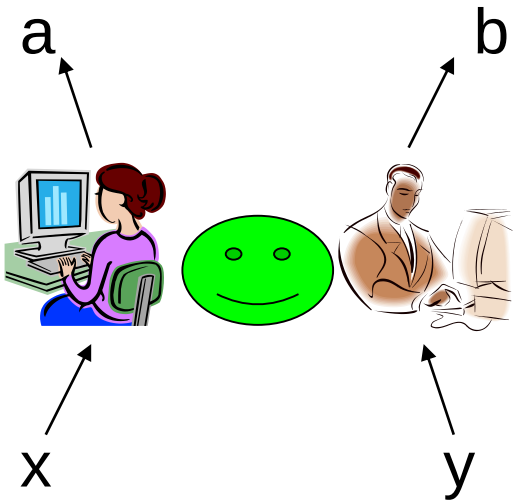
NL boxの存在と通信複雑性



Pr[xy=a⊕b]≤0.75



Pr[xy=a⊕b]≤0.85



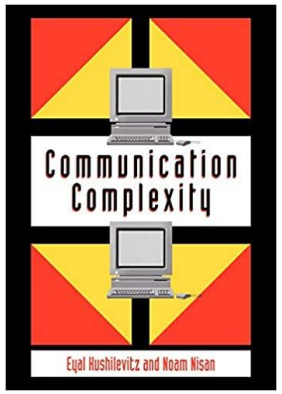
Pr[xy=a⊕b]=1

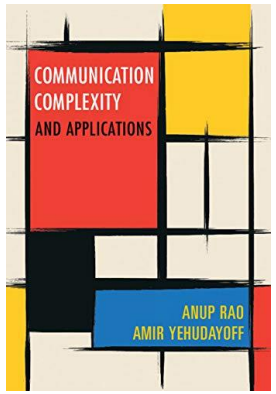
[van Dam 05] AliceとBobがNL boxを使えるなら，
すべてのブール関数の通信複雑さは1になる
[BBLMTU06] NL boxの成功率が1でなくても
1/2+1/√6≒90.8%以上なら，やはりすべてのブール関数
の通信複雑さは１になる

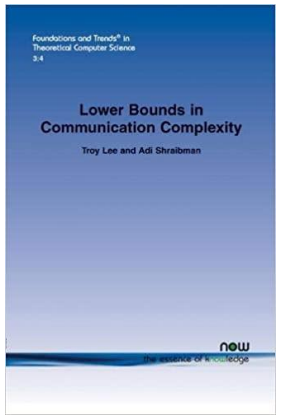
NL (Non-Local) box (またはPR box)
[Popescu-Rohrlich 94]

[BBLMTU06] G. Brassard, H. Buhrman, N. Linden, A. Methot, A. Tapp, PRL96, 250401

参考文献







- 古典

[KN97] Eyal Kushilevitz, Noam Nisan, Communication Complexity, Cambridge University Press, 1997

[RY20] Anup Rao, Amir Yehudayoff, Communication Complexity and Applications, Cambridge University Press, 2020

[Izu16] 泉泰介，通信複雑性理論入門ー基礎と情報理論からのアプローチ，IEICE Fundamantals Review 10(1), pp. 46-56, 2016

- 量子

[BCMW10] Harry Buhrman, Richard Cleve, Serge Massar, Ronald de Wolf, Non-locality and communication complexity, Review of Modern Physics 82(1), pp. 665-698, 2010

[LS09] Troy Lee and Adi Shraibman, Lower bounds in communication complexity, Foundations and Trends in Theoretical Computer Science 3(4), Now publishers, 2009

参考文献

(2010年以前は[KN97]か[BCMW10]の参考文献を参照せよ)

- DISJの量子下界

[BGKMT18] Mark Braverman, Ankit Garg, Young Kun Ko, Jieming Mao, Dave Touchette, Near-optimal bounds on the bounded-round quantum communication complexity of disjointness, SIAM Journal on Computing 47(6): 2277-2314, 2018.

- Log-rank conjecture

[Lov16] Shachar Lovett, Communication is bounded by root of rank, Journal of the ACM, 63(1):1:1–1:9, 2016.

[GPW18] Mika Göös, Toniann Pitassi, and Thomas Watson. Deterministic communication vs. partition number, SIAM Journal on Computing 47(6): 2435-2450, 2018.

[CMS19] Arkadev Chattopadhyay, Nikhil S. Mande, Suhail Sherif, The log-approximate-rank conjecture is false, STOC'19, pp. 42-53.

[ABT19] Anurag Anshu, Naresh Goud Boddu, Dave Touchette, Quantum log-approximate-rank conjecture is also false, 1811.10525, FOCS'19, pp. 982-994.

[SW19] Makrand Sinha, Ronald de Wolf, Exponential separation between quantum communication and logarithm of approximate rank, 1811.10090, FOCS'19, pp. 966-981.

- 分散計算

[LM18] Francois Le Gall, Frederic Magniez, Sublinear-time quantum computation of the diameter in

CONGEST networks, 1804.02917, PODC'18, pp. 337-346. ([HW12,PRT12,FHW12]は[LM18]の参考文献参照せよ)

[MN20] Frederic Magniez, Ashwin Nayak, Quantum Distributed Complexity of Set Disjointness on a Line, 2002.11795, ICALP'20, pp. 82:1-82:18.