量子ネットワーク符号

西村治道（大阪府立大学理学系研究科）

2010年11月6日

IBIS2010，東京大学　生産技術研究所

ネットワーク上での効率的通信

- ネットワーク符号 [Ahlswede-Cai-Li-Yeung. 2000]
  - 通信理論とネットワーク上での配送理論の融合分野
  - 情報理論，通信理論の研究者が研究の中心

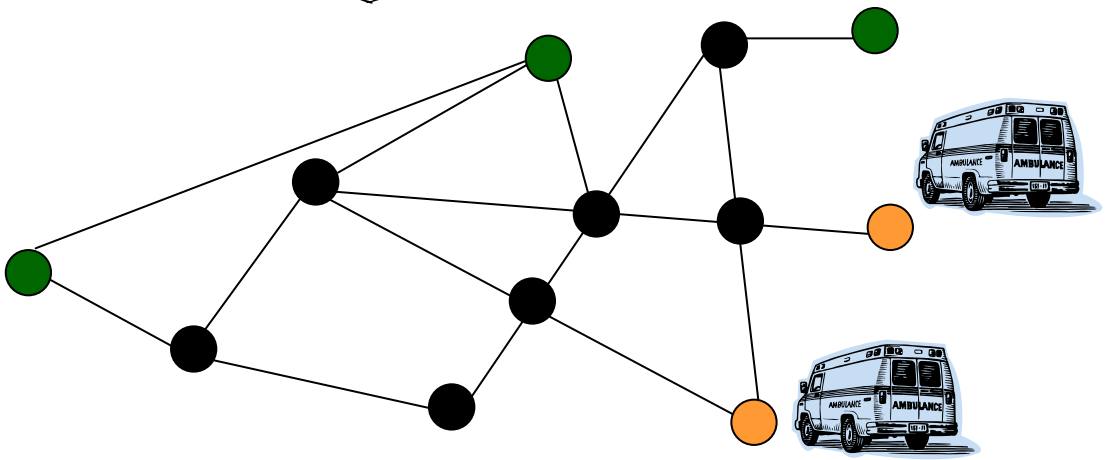
通信理論　　主に1対1の（ノイズを含む通信路における）通信に関する理論

データ圧縮

エラー訂正

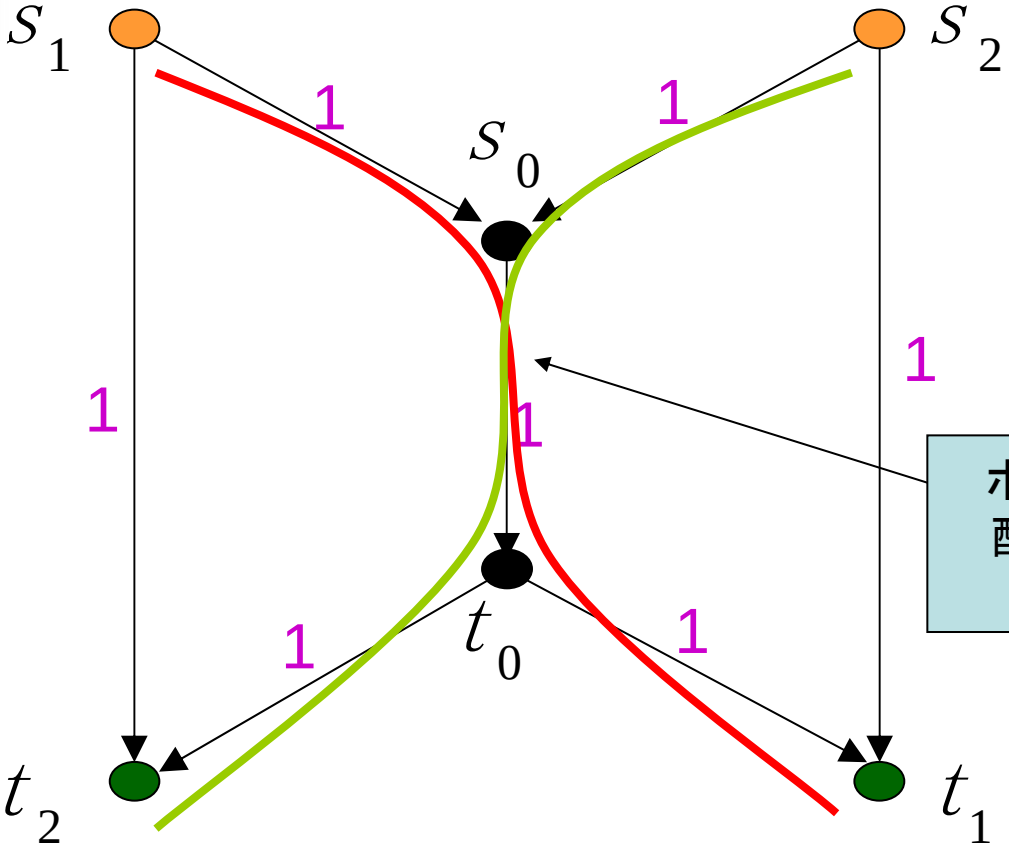
セキュリティ

ネットワーク上での配送問題



複雑なネットワーク上での効率的配送に関する理論

液体フロー (Liquid Flow)

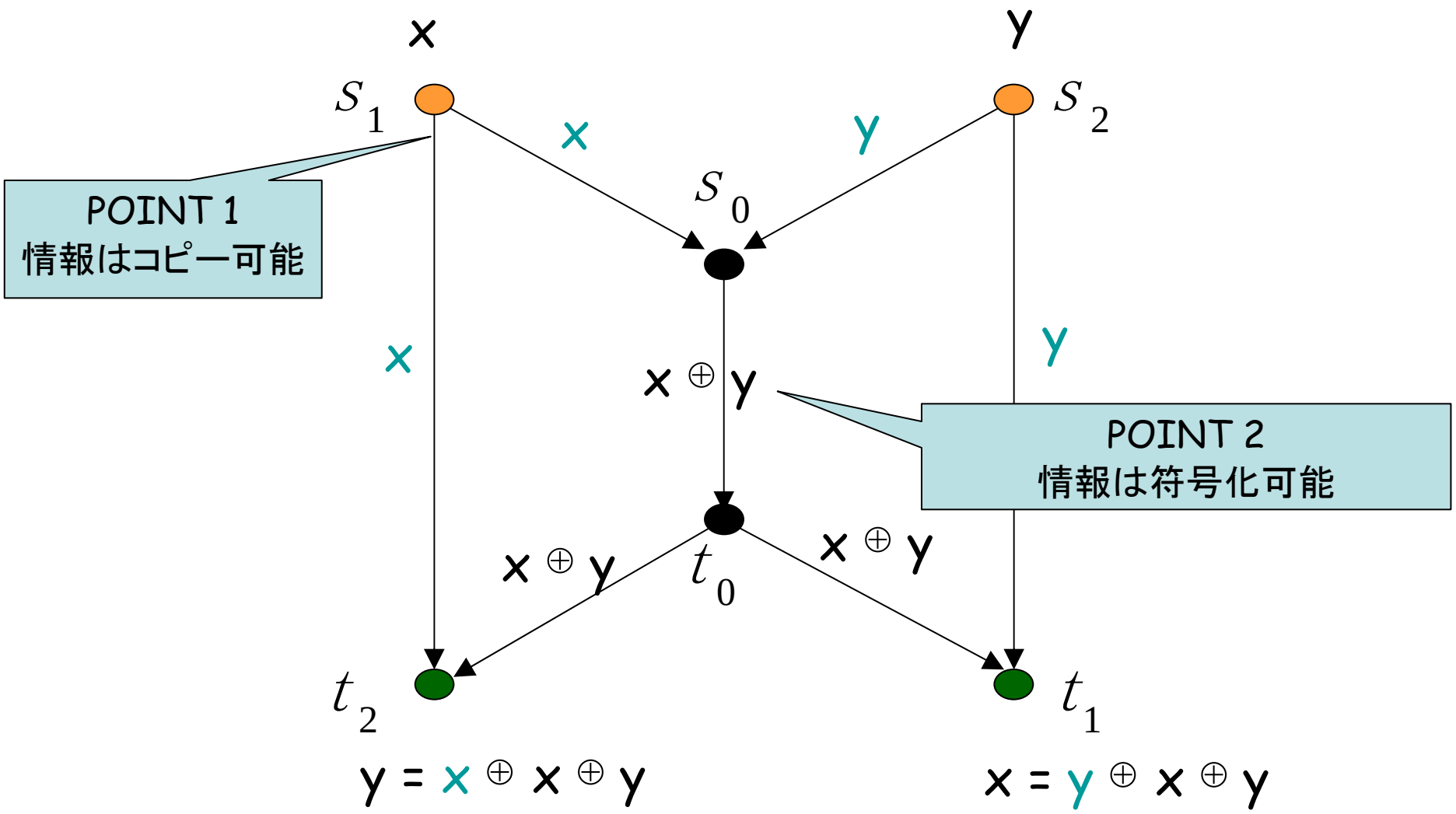


ボトルネックにより
配送問題としては
解なし

Butterfly Network

情報フロー (Information Flow)

[Ahlswede et al. 2000]

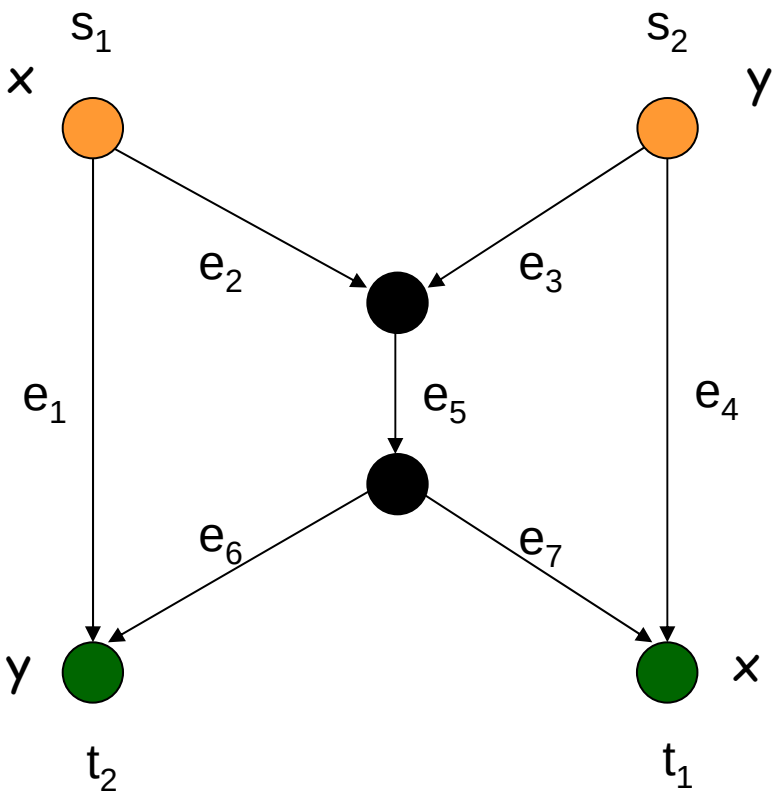


ネットワーク符号問題

[A. Lehman PhD, 2005 より]

- **入力例**
  - （有向かつ非環式）グラフ G=(V, E)
  - Capacity c(e) for 各辺 e
  - k 個の品種(commodity)からなる集合 I
  - 各品種 $i \in I$ に対するソースの集合 S(i)とシンクの集合 T(i)
- Network code
  - Alphabet Σ
  - 各辺 e に対しての関数　f[e]: $\Sigma^{(e\text{の出発点の入次数})} \rightarrow \Sigma^{c(e)}$
- Network codeの解
  - f[e] は e=(u,v) へ入ってくる辺上の関数及び uがソースの場合のメッセージから計算可能な関数
  - 各品種 i の各シンク $v \in T(i)$に対し，vへの辺上の関数から S(i)に与えられるメッセージ $M(i) \in \Sigma$が復号可能

解が存在するネットワーク符号問題の例



Butterfly network

全ての辺のcapacityは 1

2つの品種 X, Yがあって

$S(X)=\{s_1\}$, $S(Y)=\{s_2\}$,

$T(X)=\{t_1\}$, $T(Y)=\{t_2\}$

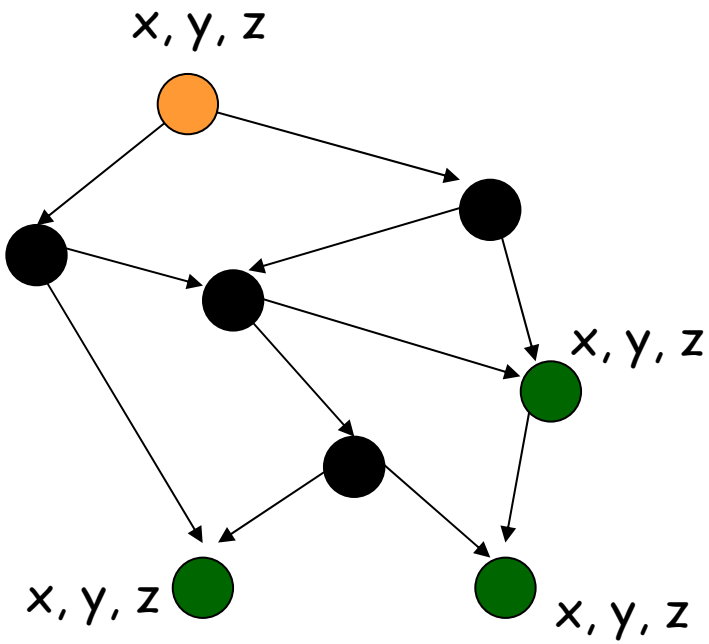
解（の1つ）はアルファベットとして {0,1} を取り，各辺に対する関数として

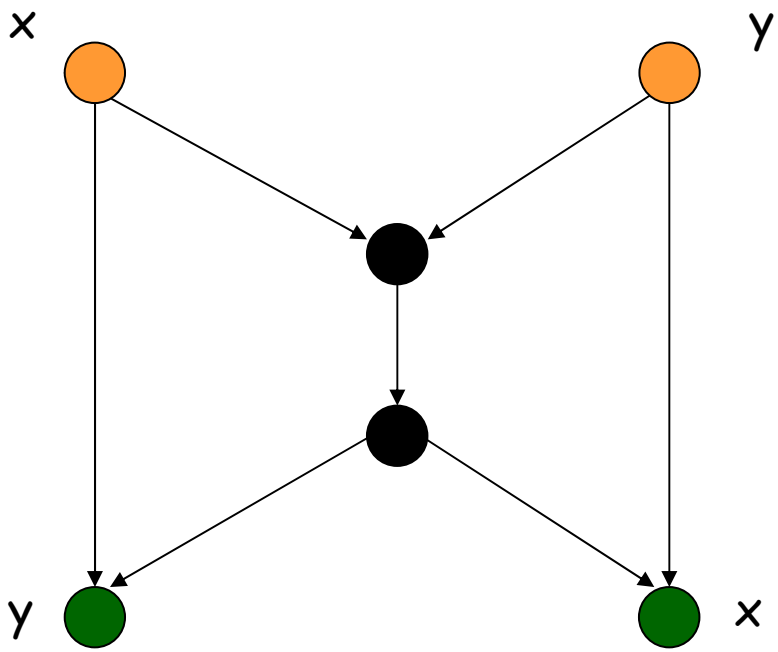
$f[e_1](z)=z$（$f[e_2]$, $f[e_3]$, $f[e_4]$, $f[e_6]$, $f[e_7]$ も同様）

$f[e_5](w,z)=w+z$

である.

ネットワーク符号問題の例





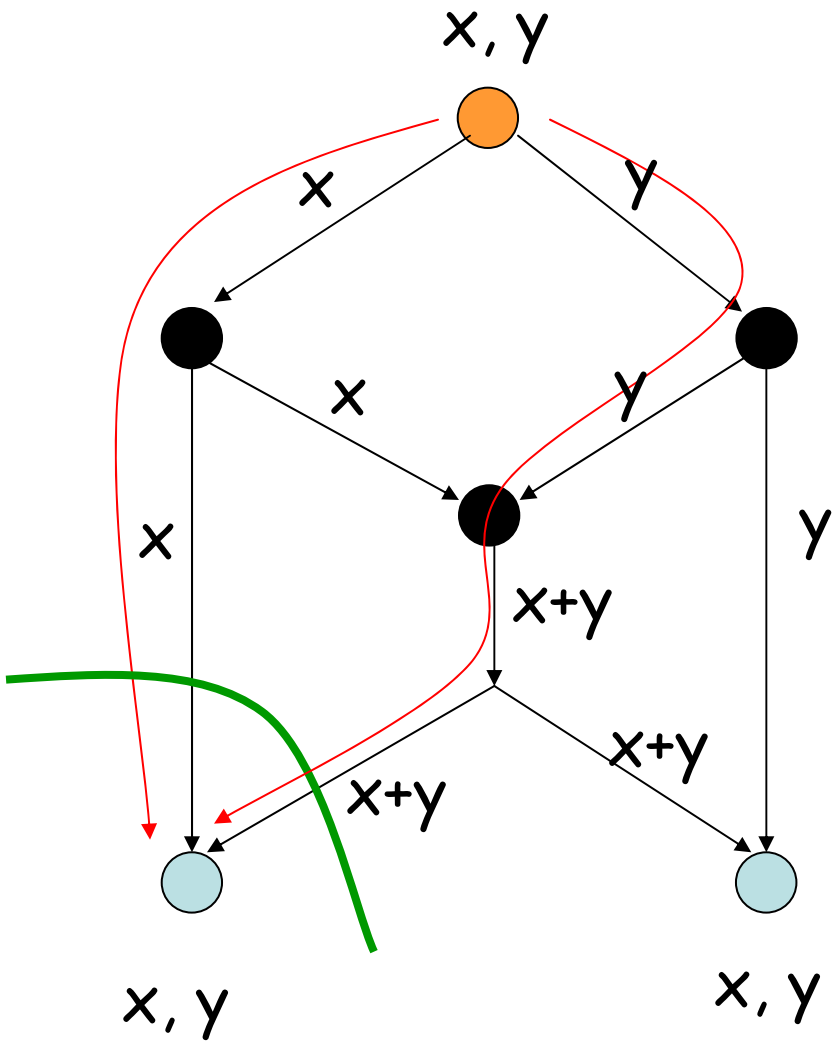
Multicast 問題:

ソースが持つメッセージ全てを全てのシンクが要求する

k-ペア通信問題 (Multiple Unicast):

k品種のそれぞれが1つのソースと1つのシンクを持つ．Butterfly networkは2-通信問題の一種

Multicast問題の例



Max-flow Min-cut 定理
ソースとシンクが各1個の場合，Min-cutを達成するような（ルーティングによる）Max-flowが存在する

Max-flow=2

Min-cut=2

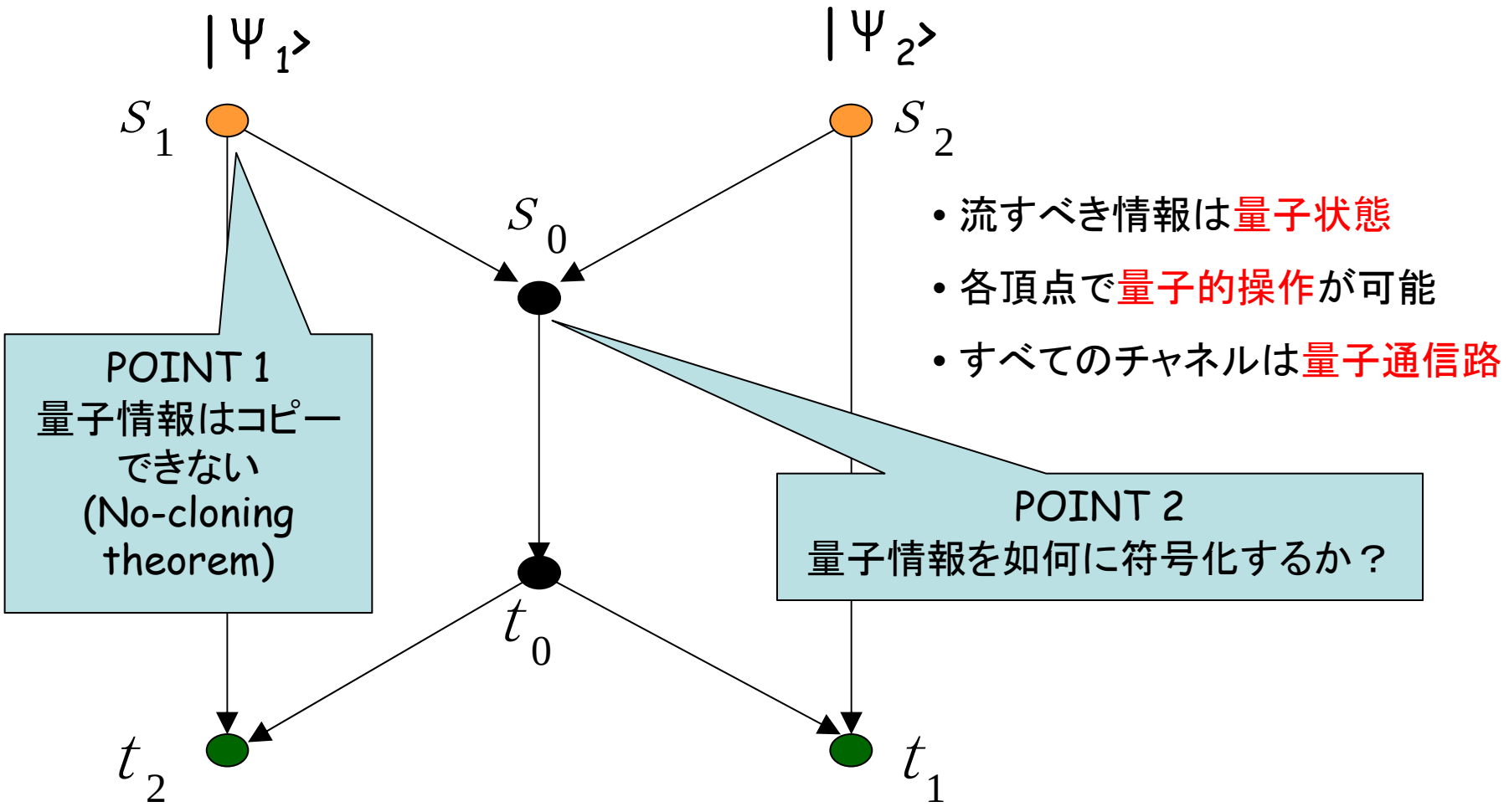
Multicast問題の場合，**符号化**を（しかも線形符号を）使ってMin-cutを達成するようなMax-flowが存在する [Ahlswede et al. 2000, Li et al. 2003]

※しかも多項式時間アルゴリズム存在 [Jaggi et al. 2005]

kペア通信問題

- kがグラフサイズに依存する場合，可解性は計算可能か否かさえ未解決
- 線形符号に限ってもNP完全 [Lehman-Lehman 2004]
- k=2の場合，多項式時間アルゴリズム存在 [Wang-Shorff 2007]
- kが3以上の定数の場合未解決
  - 体のサイズ有限の線形符号に限ると，多項式時間アルゴリズム存在 [Iwama et al. 2008]

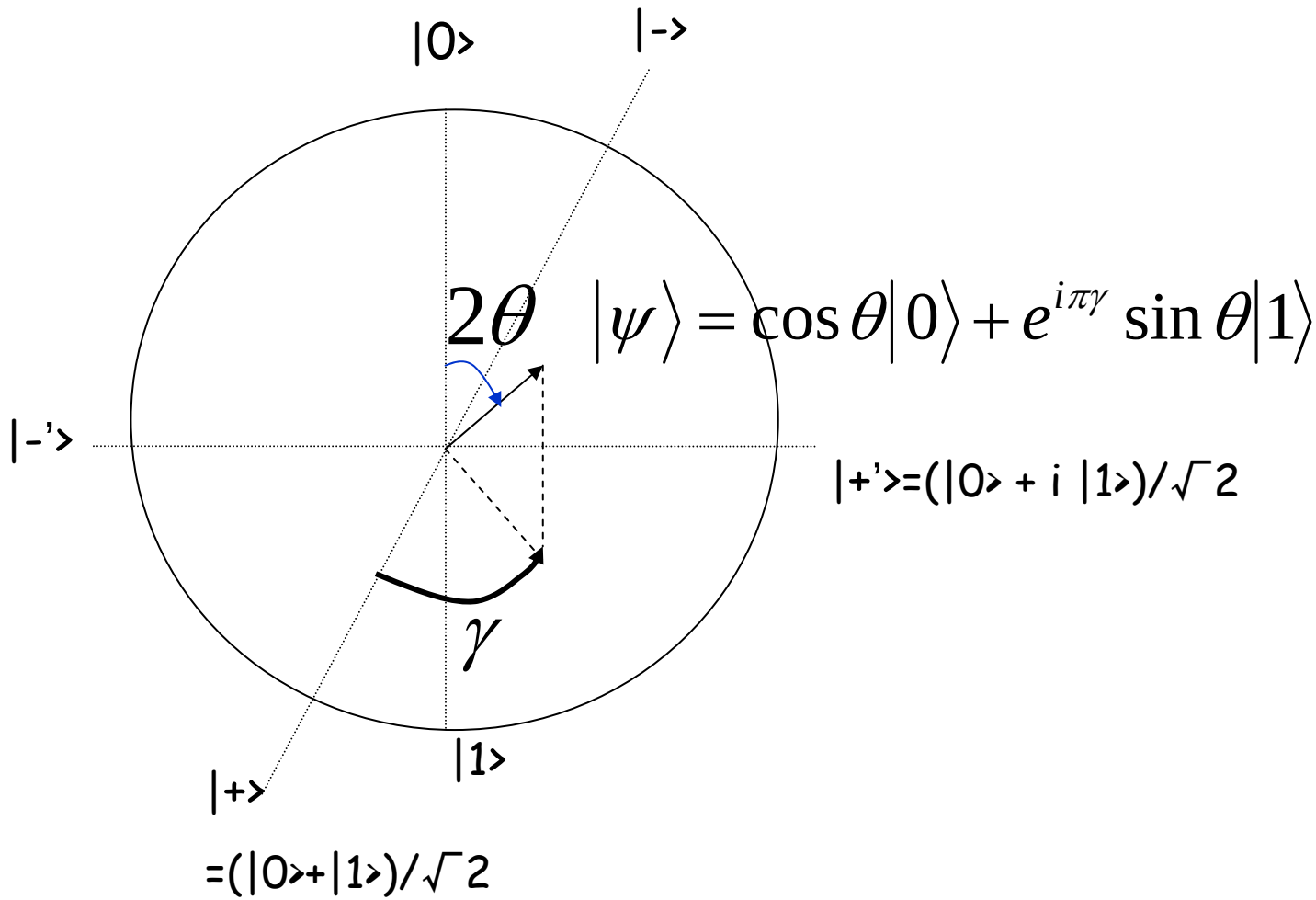
情報フローの量子化（量子ネットワーク符号）



Q. 古典で可解なネットワーク符号問題は量子でも可解か？

量子ビット

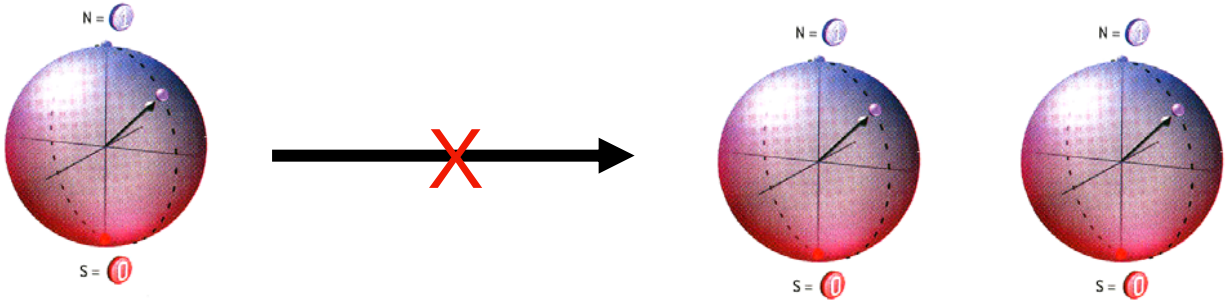
- 量子ビットはBloch球と呼ばれる単位球の表面上（及び内部の）点として表現可能



どうやってコピーするか？

- ユニタリ変換を使ってコピーできればよいが，しかし・・

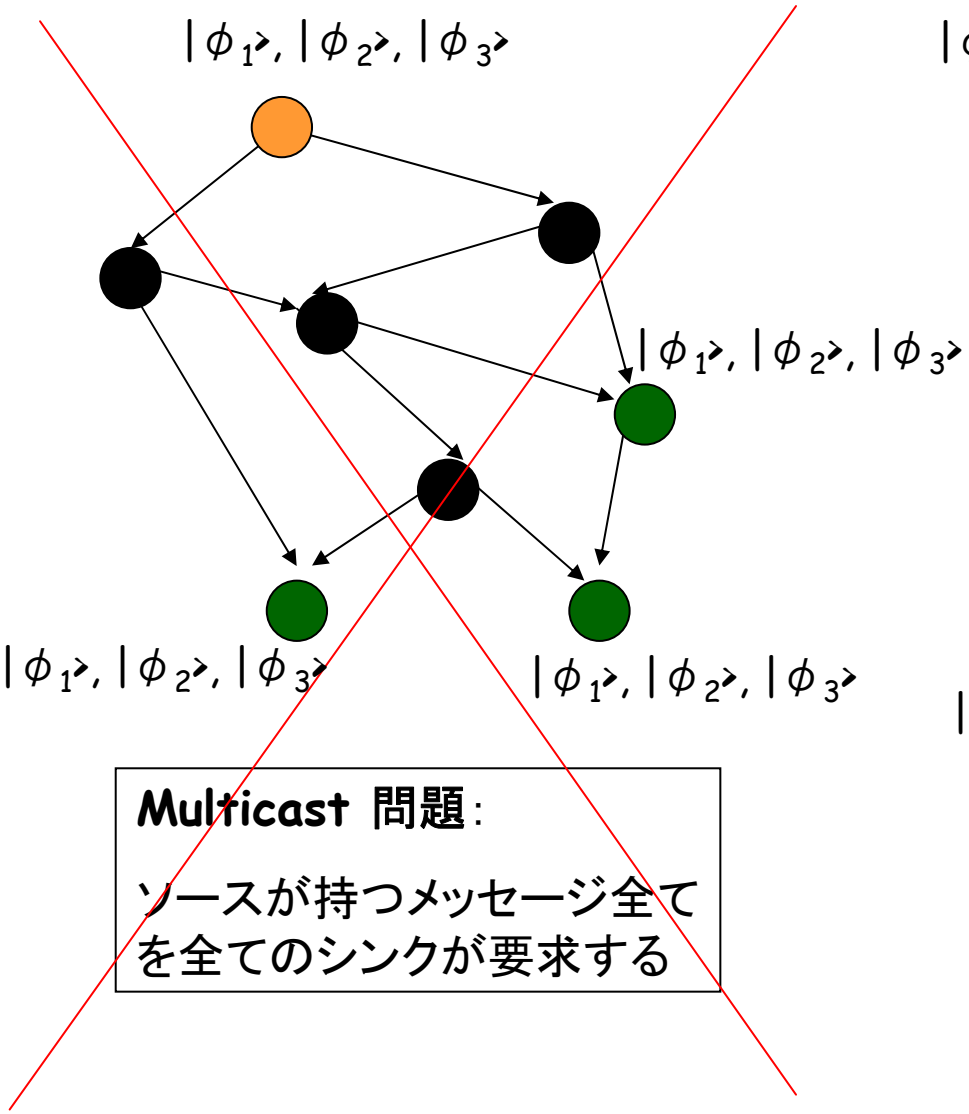
(No-cloning theorem: Wootters-Zurek) 未知の量子状態は，正確にコピーすることは不可能.



$$|0\rangle|a\rangle \xrightarrow{U} |00\rangle|\varphi\rangle,$$
$$|1\rangle|a\rangle \xrightarrow{U} |11\rangle|\phi\rangle$$

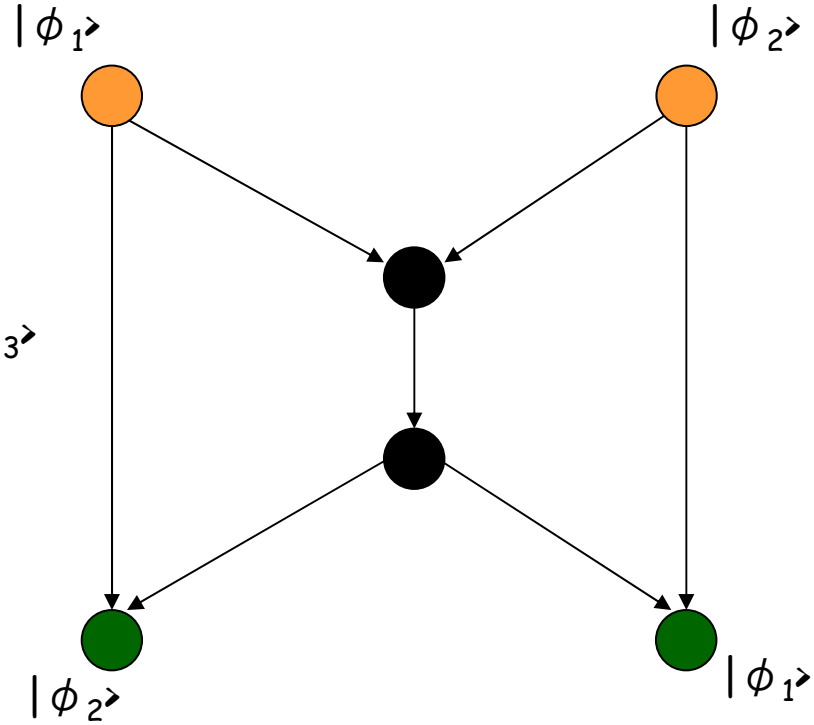
$$(\alpha|0\rangle+\beta|1\rangle)|a\rangle \xrightarrow{U}$$
$$\alpha|00\rangle|\varphi\rangle+\beta|11\rangle|\phi\rangle$$
$$\neq (\alpha|0\rangle+\beta|1\rangle)(\alpha|0\rangle+\beta|1\rangle)|\chi\rangle$$

ネットワーク符号問題の例



Multicast 問題:

ソースが持つメッセージ全てを全てのシンクが要求する

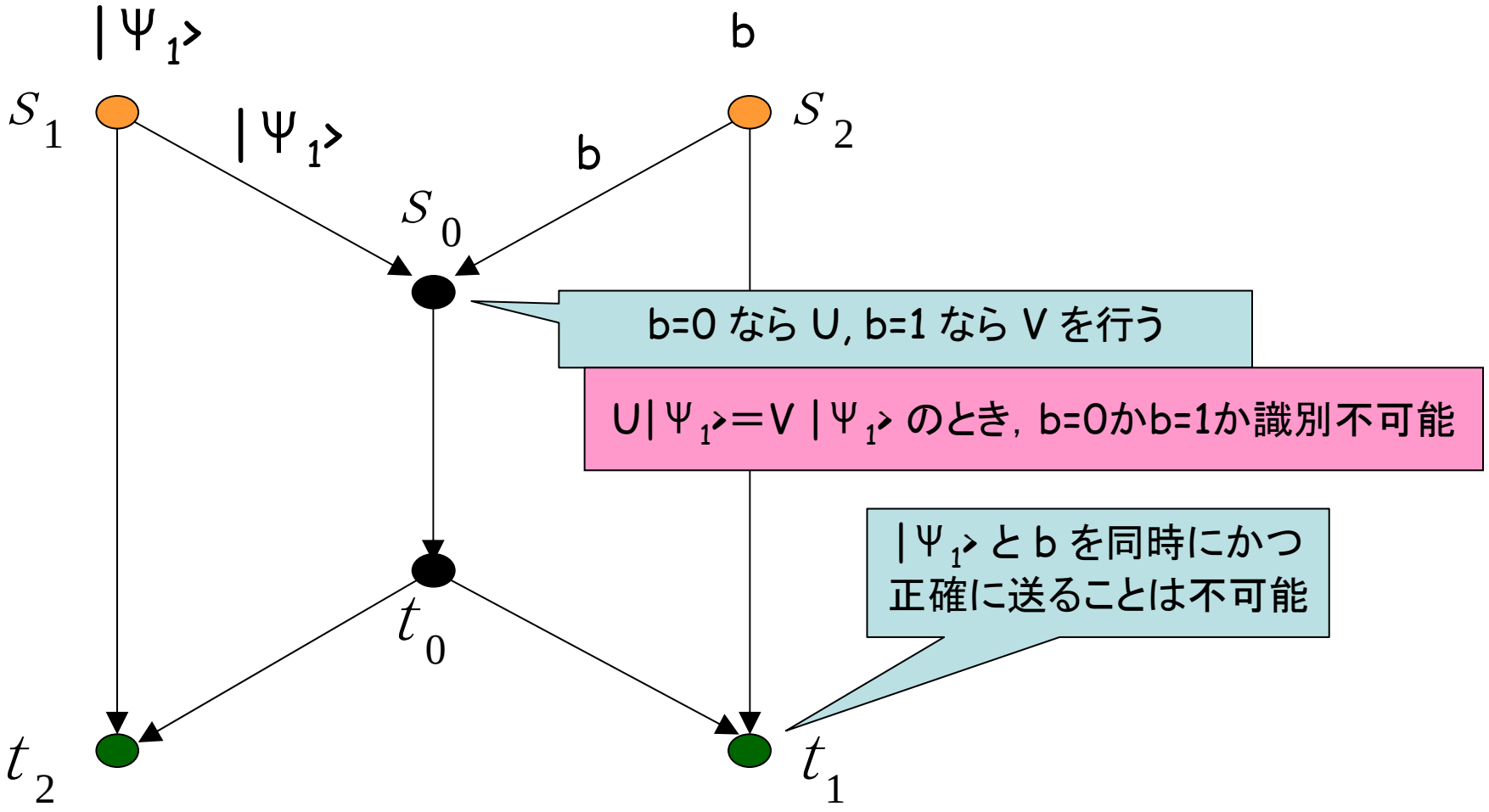


k-ペア通信問題 (Multiple Unicast):

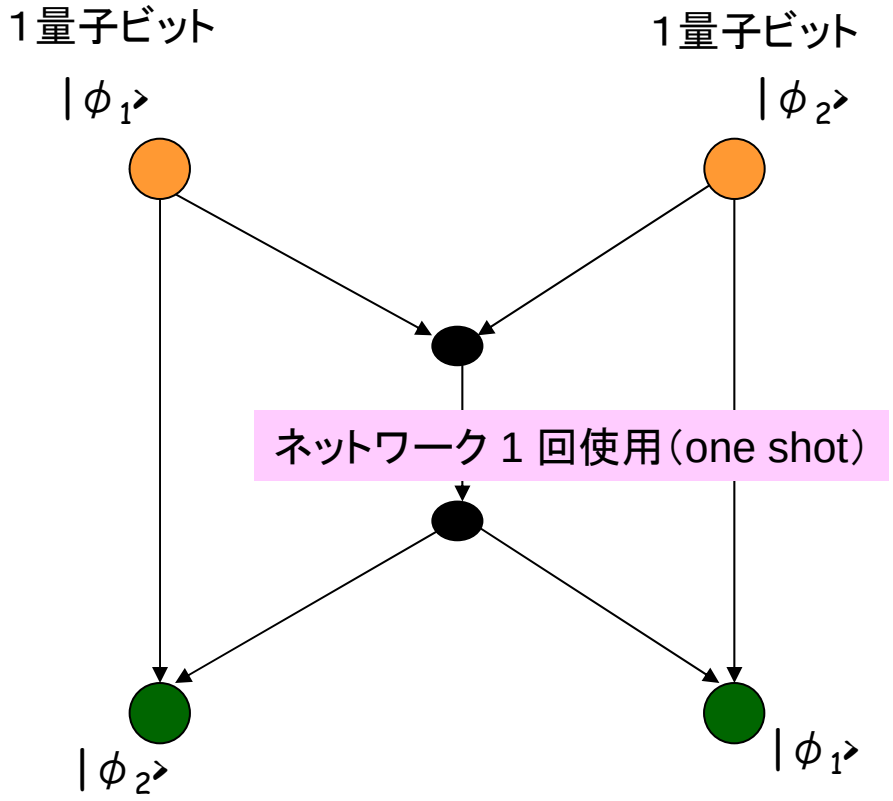
k品種のそれぞれが1つのソースと1つのシンクを持つ

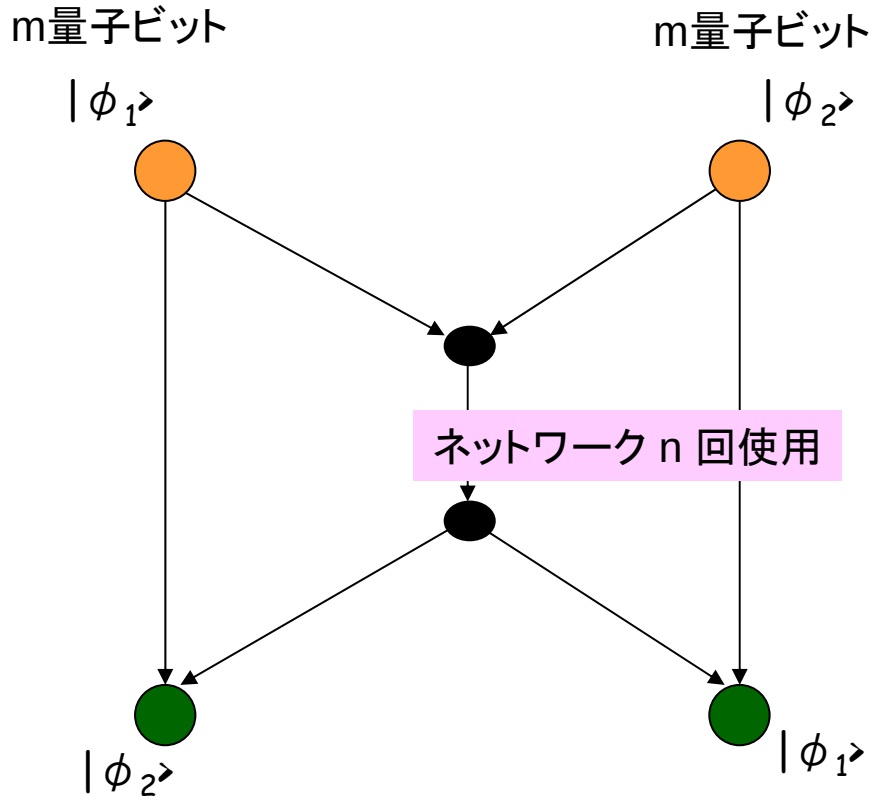
c.f. Shi-Soljanin 2006, Kobayashi et al. 2010

どうやって量子情報を符号化するか？



不可能性に関する結果





ネットワークの1回の使用のもと，

1量子ビットを忠実に送ることは不可能

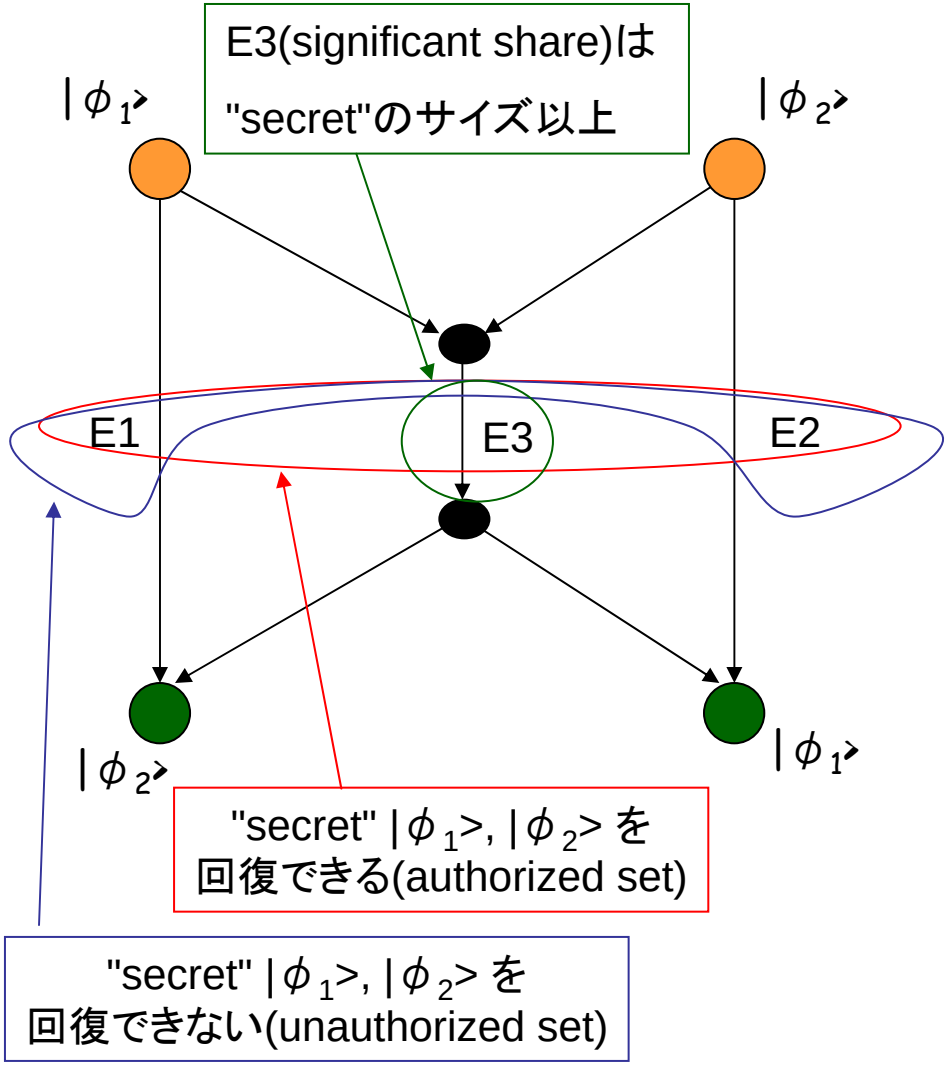
[Hayashi et al. 2007]

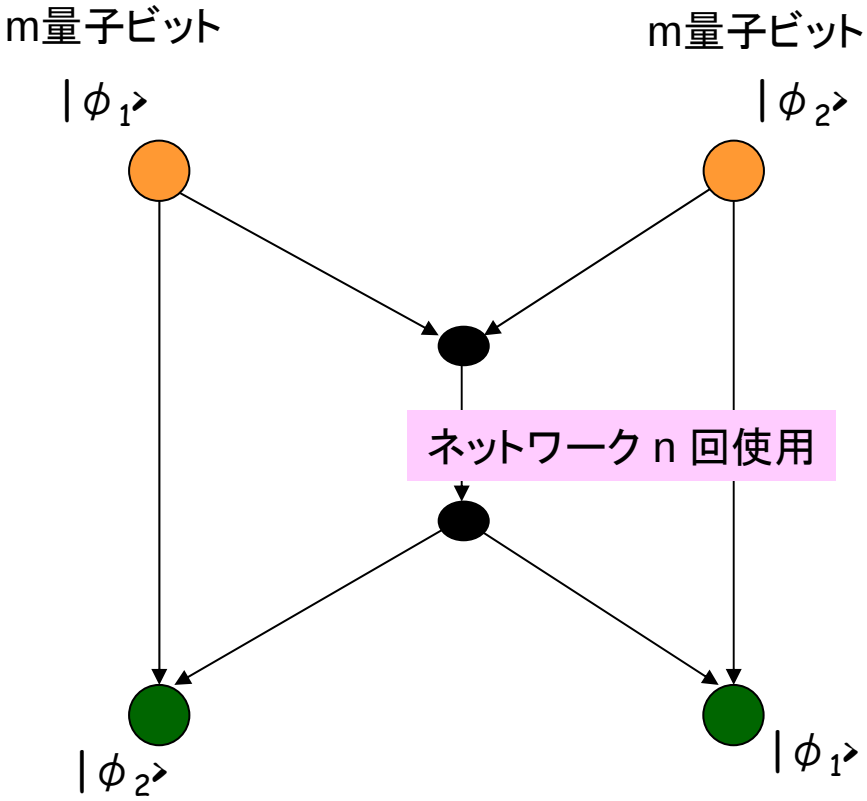
1量子ビットを忠実に送ることは

漸近的にも（つまりm/nが漸近的に1に近づく）

不可能 [Hayashi 2007, Leung et al. 2010]

不可能性に関する結果



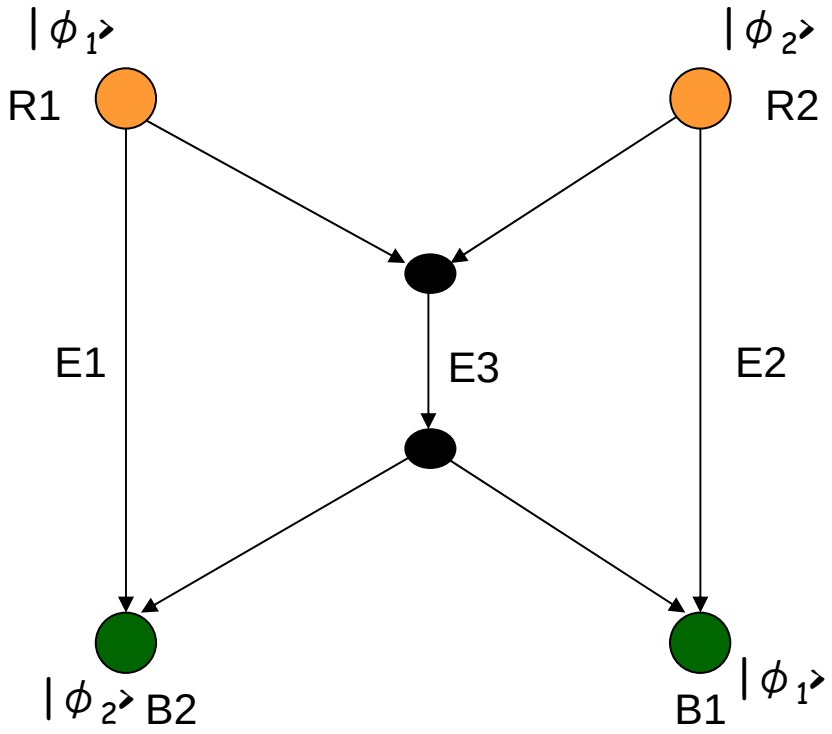


1量子ビットを忠実に送ることは

漸近的にも（つまりm/nが漸近的に1に近づく）

不可能 [Hayashi 2007, Leung et al. 2010]

不可能性に関する結果

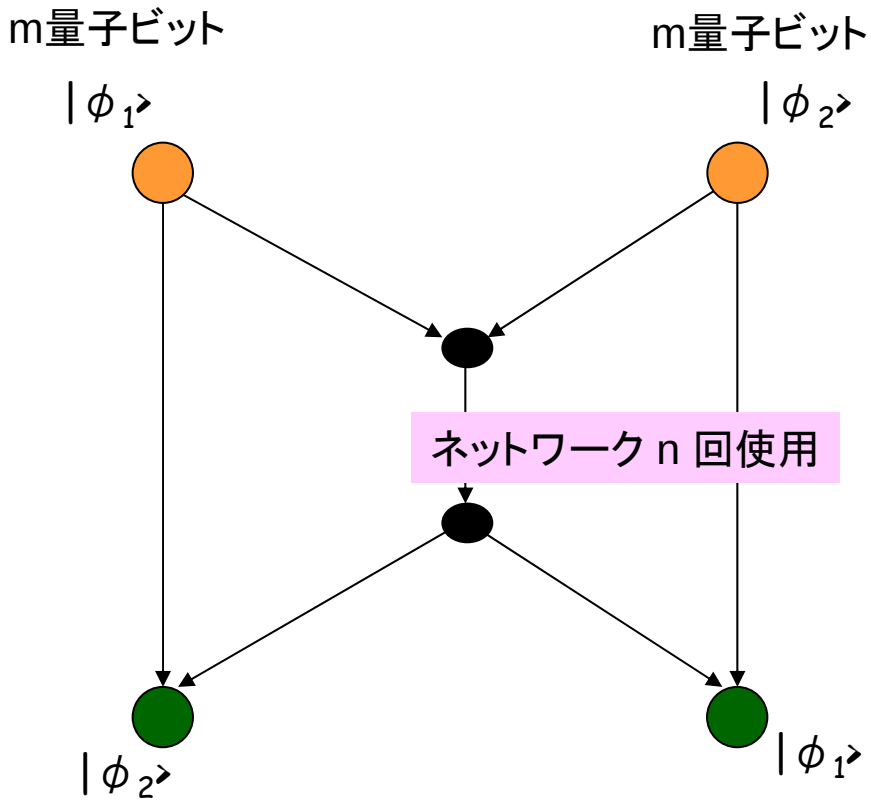


$I(R1R2:B1B2) \le I(R1R2:E1E2E3)$ (単調性)

$= I(R1R2:E3|E1E2)+I(R1R2:E1E2)$ (Chain Rule)

$\le 2H(E3) + I(R1:E1)+I(R2:E2)$

$\le 2n + 2H(R1) - I(R1:B1)+2H(R2) - I(R2:B2)$

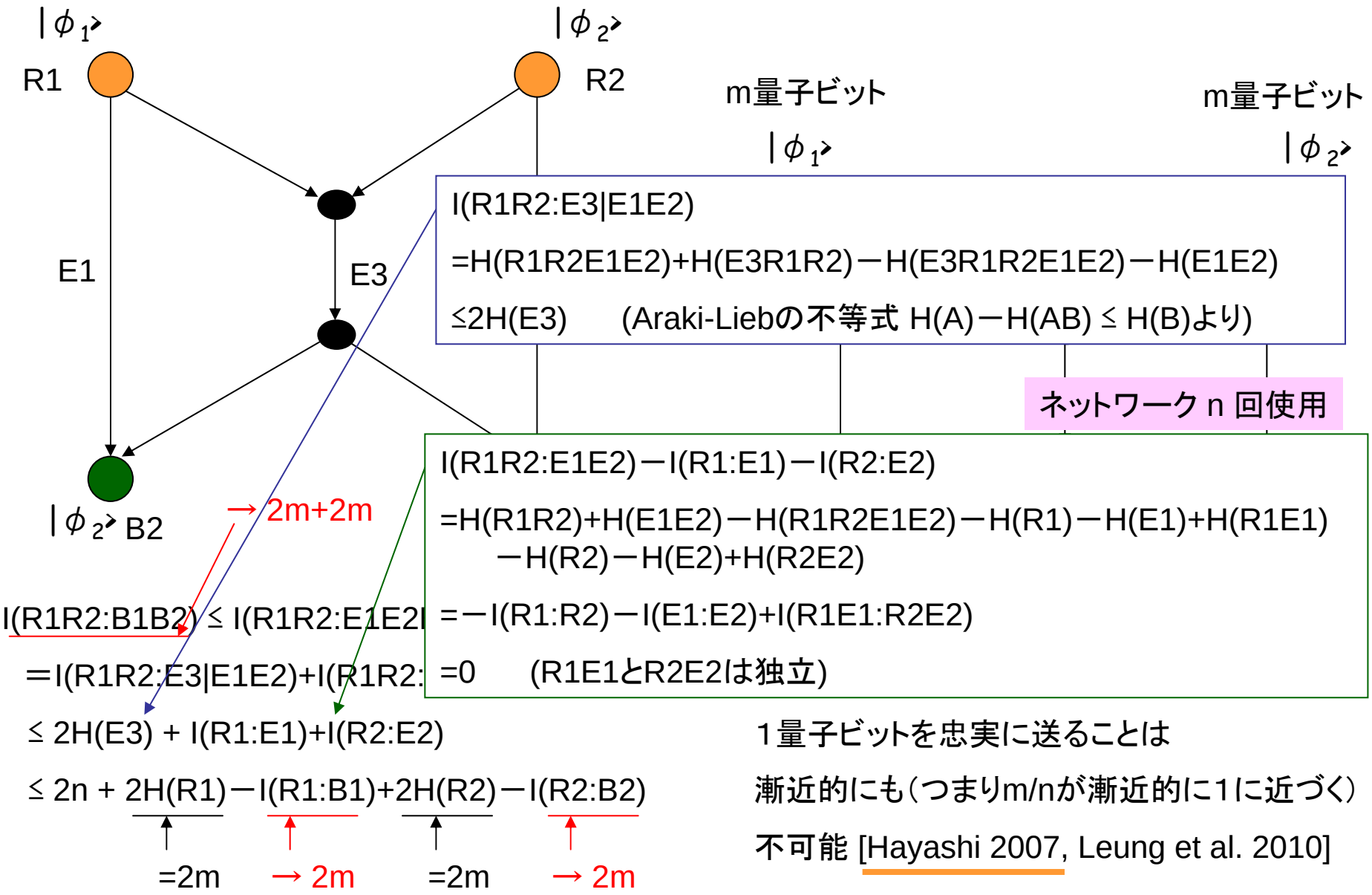


1量子ビットを忠実に送ることは

漸近的にも（つまりm/nが漸近的に1に近づく）

不可能 [Hayashi 2007, Leung et al. 2010]

不可能性に関する結果



1量子ビットを忠実に送ることは

漸近的にも（つまりm/nが漸近的に1に近づく）

不可能 [Hayashi 2007, Leung et al. 2010]

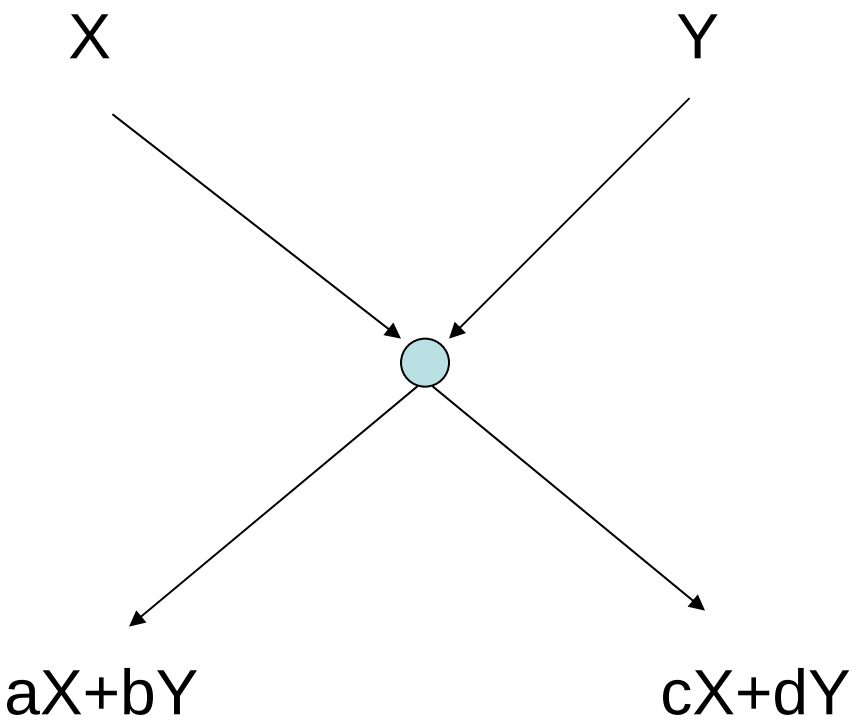
補助的なリソースを認めると・・・

- エンタングルメント
  - ソース間 [Hayashi 2007]
  - 各辺の間 [Leung-Oppenheim-Winter 2010]
- 古典通信路 [Leung et al. 2010, Kobayashi et al., 2009, 2010]
  - 量子通信路より安価 『 LOCC(Local Operation & Classical Communication)は量子通信より易しい（？）』
  - 古典通信を自由に認めることで，量子通信路の使用回数を減らせるなら・・・

Q. 古典で可解なネットワーク符号問題は，古典通信を自由に許すことで量子でも可解となるか？

A. 古典のネットワーク符号問題の解が線形符号化で実現されているなら，量子でも可解 [Kobayashi et al. 2009]

線形符号によるネットワーク符号

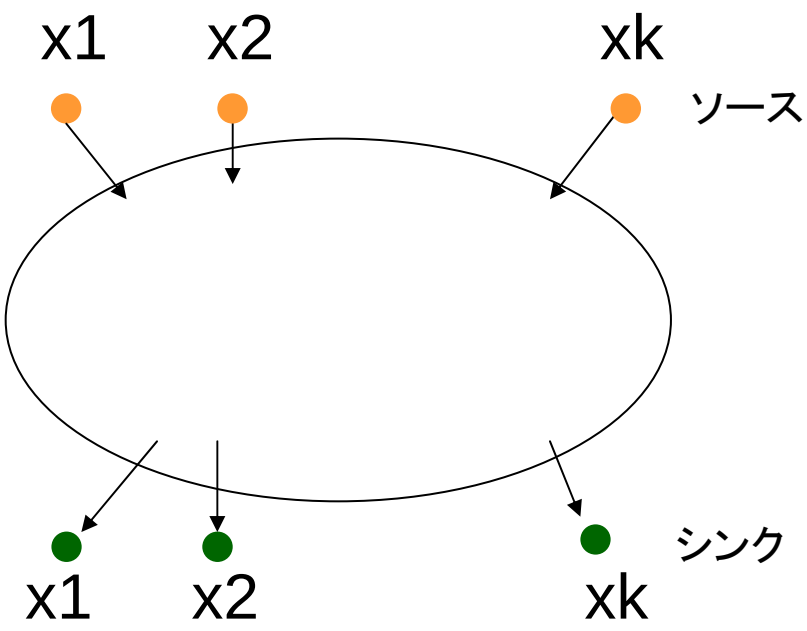


各頂点での出力が入力の線形結合であるとき，線形という

プロトコル

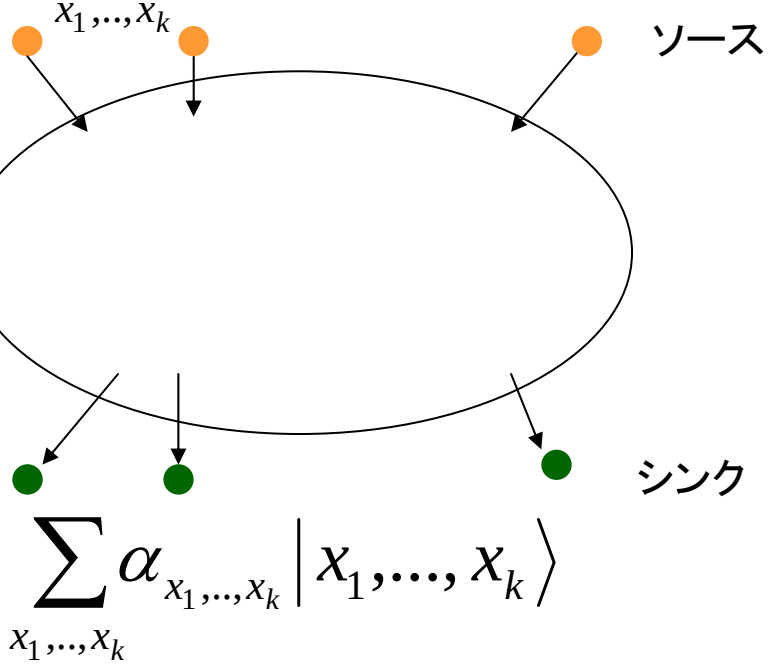
- 基本アイデア
  - 各ノードごとに古典の操作を模倣
  - フーリエ基底による測定
  - 測定により生じた位相エラーをシンクで修正

古典



量子

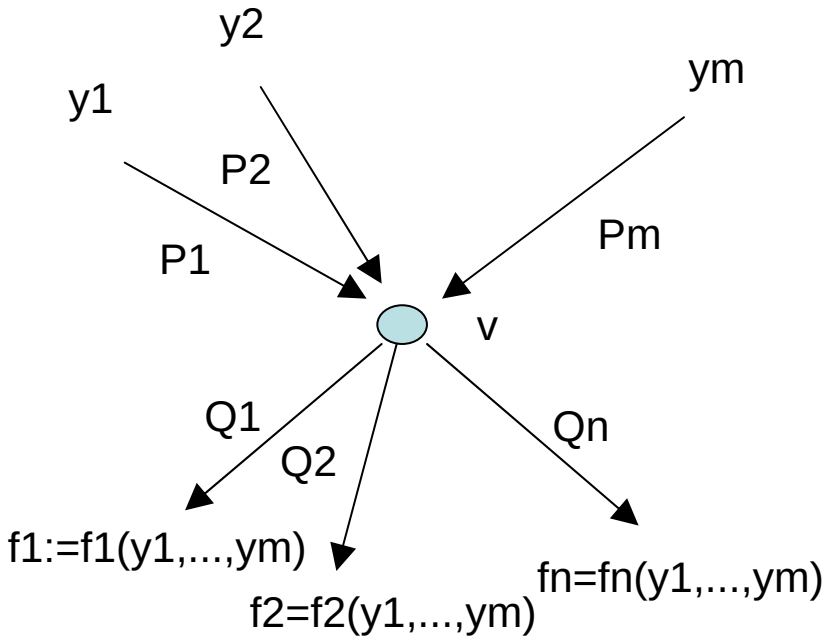
$$\sum_{x_1,..,x_k} \alpha_{x_1,..,x_k} \left| x_1,\ldots, x_k \right\rangle$$



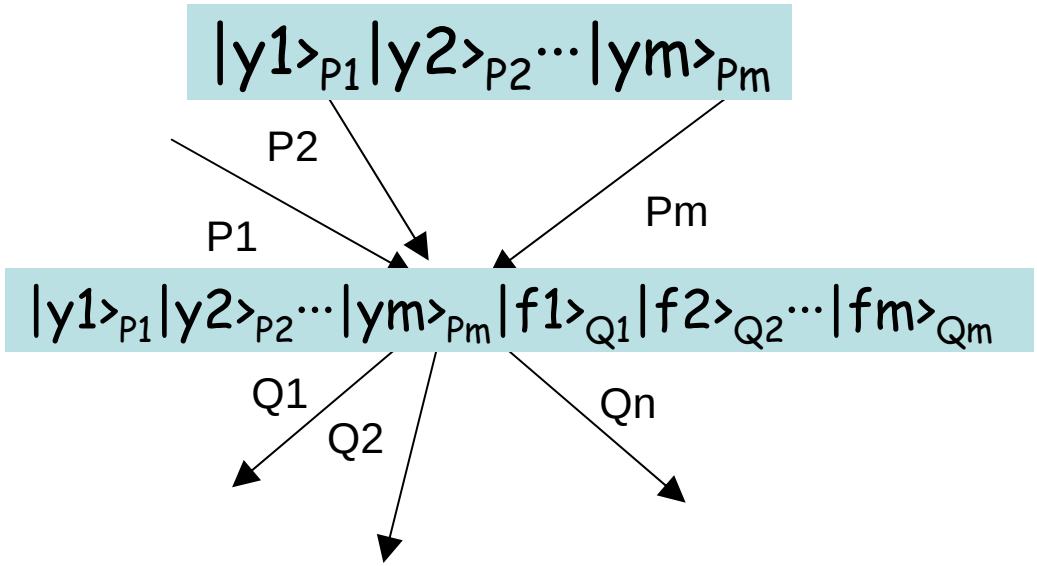
各中間ノードでの操作①

古典

解が体 F_p 上での線形符号で実現されていると仮定



量子



① ユニタリ変換

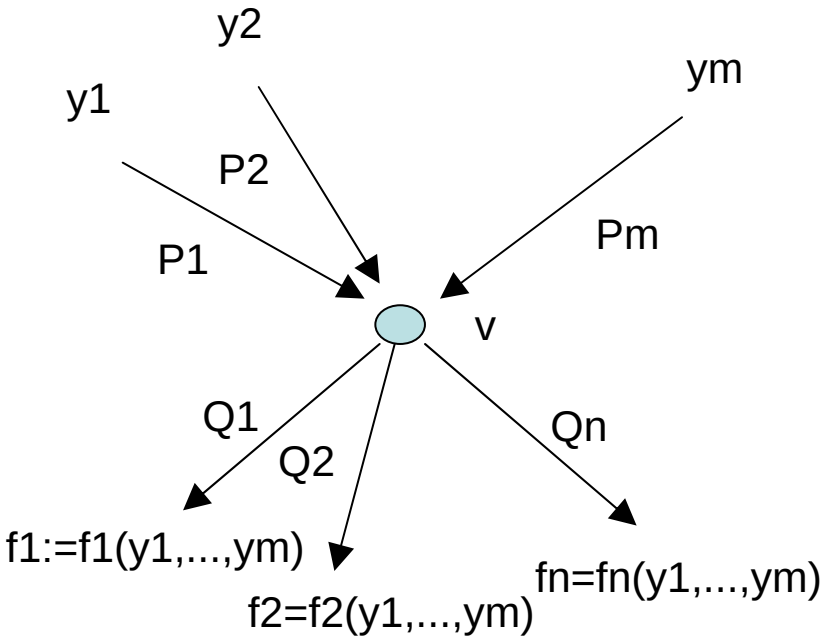
$$U_{f1,..,fm}\left|y1,...,ym\right\rangle\left|0,...,0\right\rangle := \left|y1,...,ym\right\rangle\left|f1,...,fm\right\rangle$$

を施す

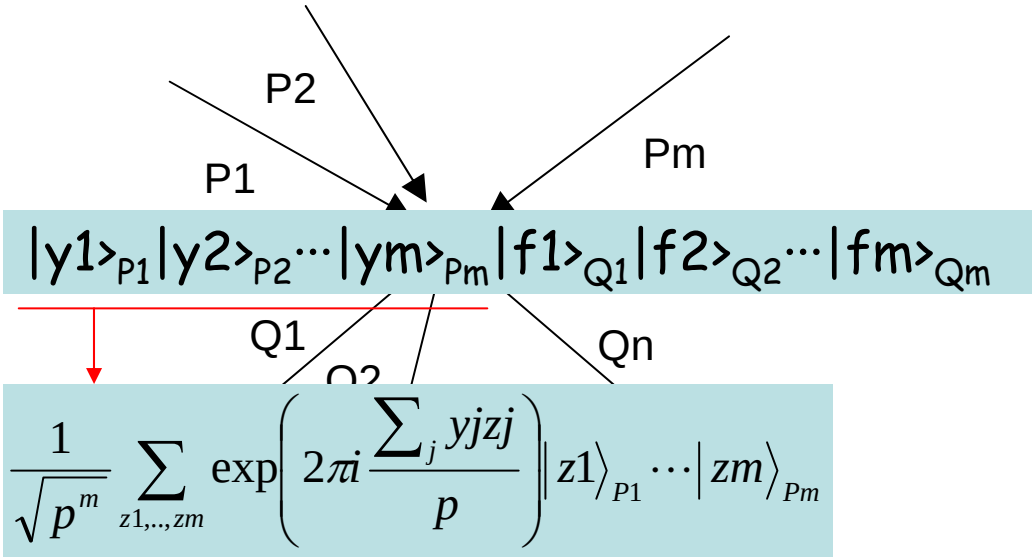
各中間ノードでの操作②

古典

解が体 F_p 上での線形符号で実現されていると仮定



量子



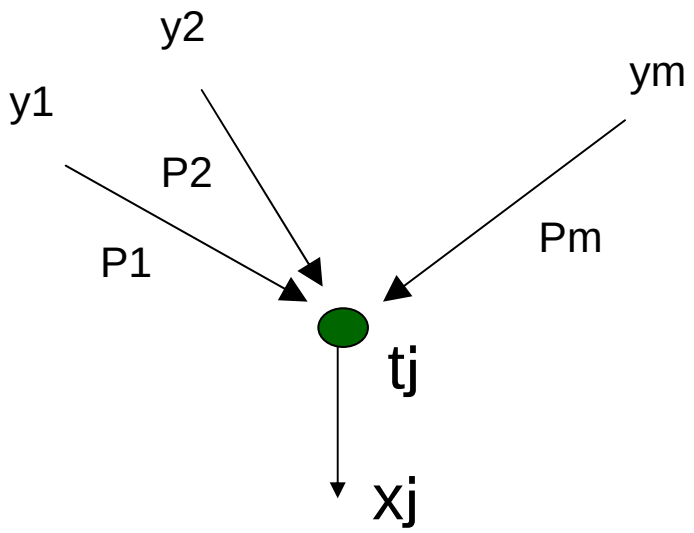
② P1,P2,...,Pmにフーリエ変換

$$F|y\rangle := \frac{1}{\sqrt{p}}\sum_z \exp\left(2\pi i\frac{yz}{p}\right)|z\rangle$$

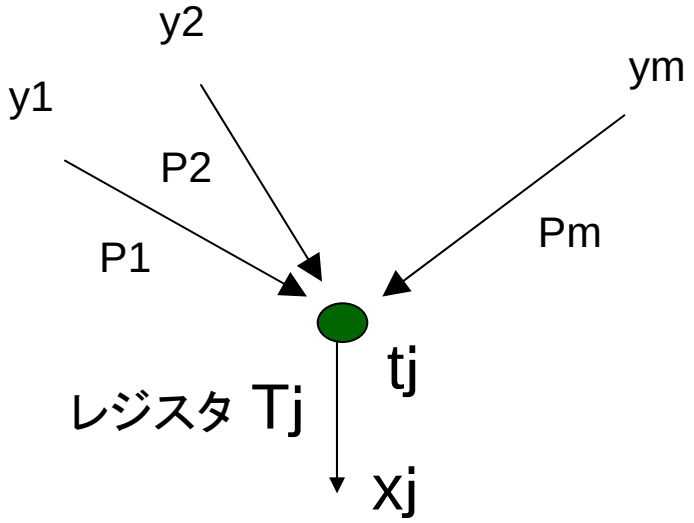
を施した後測定し，測定値 z1,..,zm をシンクに送る

各シンクでの操作

古典



量子



位相訂正前

$$\exp\left(2\pi i \sum_v h_v(x_1,\ldots,x_k)\right) \left| x_1,\ldots,x_k \right\rangle_{T_1,\ldots,T_k}$$

$$h_v(x_1,\ldots,x_k) = h_{v,1}(x_1) + \ldots + h_{v,k}(x_k)$$

中間ノード同様の操作に加えて，

各中間ノードからの測定値情報をもとに

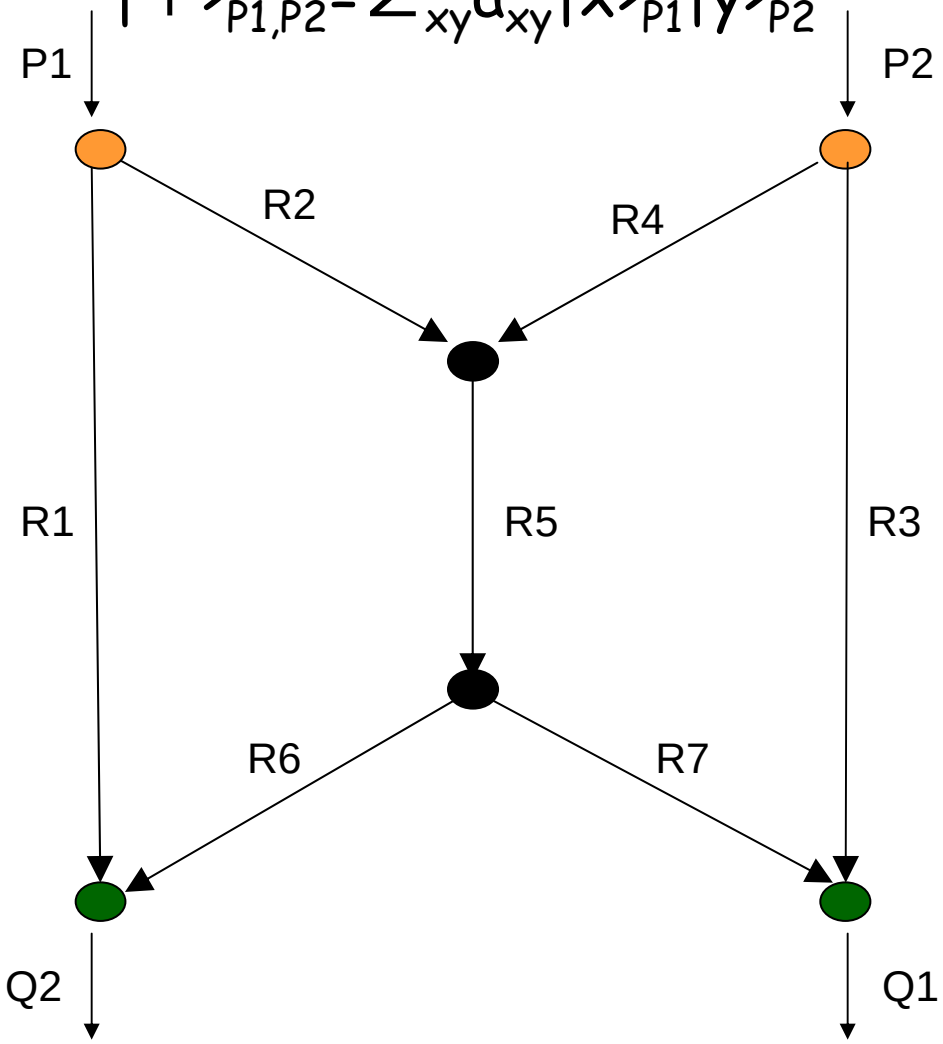
位相エラーの訂正を行う

$$\left| x \right\rangle \mapsto \exp\left(-2\pi i h_t(x)\right) \left| x \right\rangle$$

位相エラー

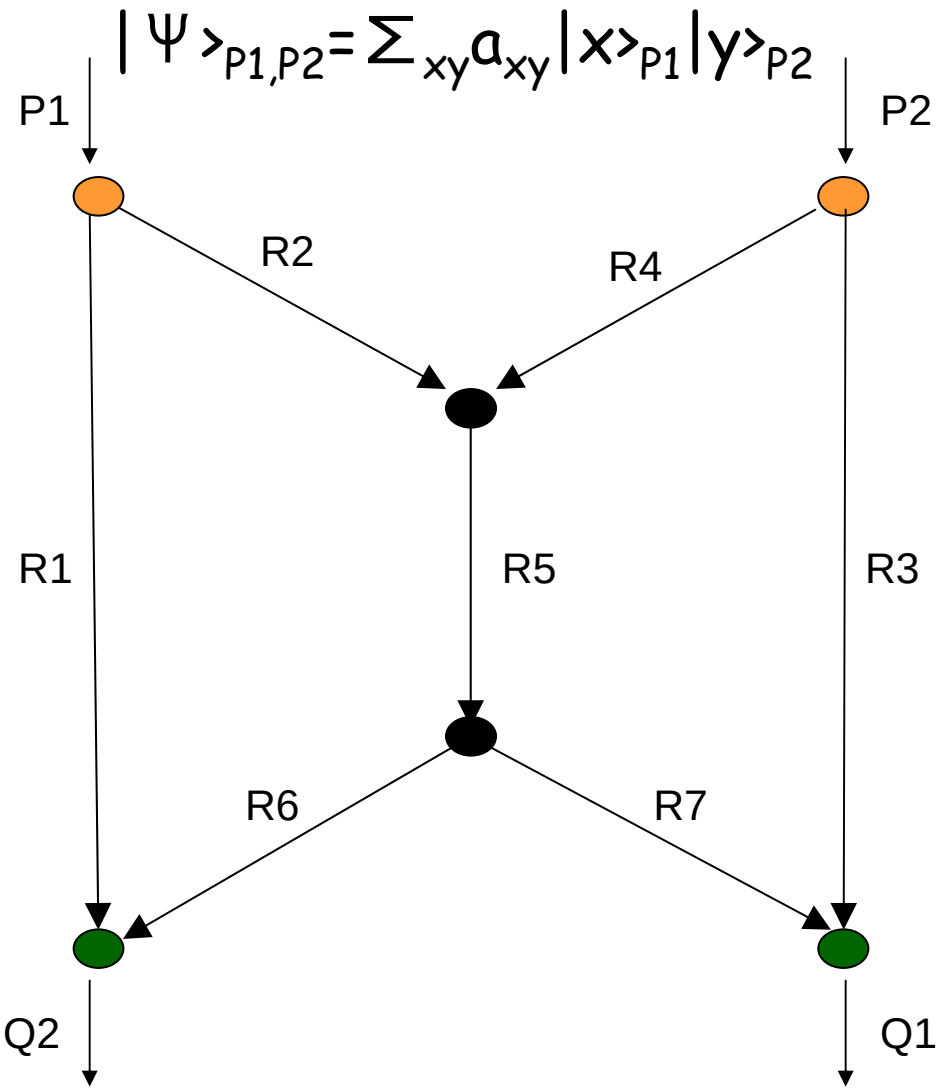
具体例

$$|\Psi\rangle_{P1,P2} = \Sigma_{xy} a_{xy} |x\rangle_{P1} |y\rangle_{P2}$$



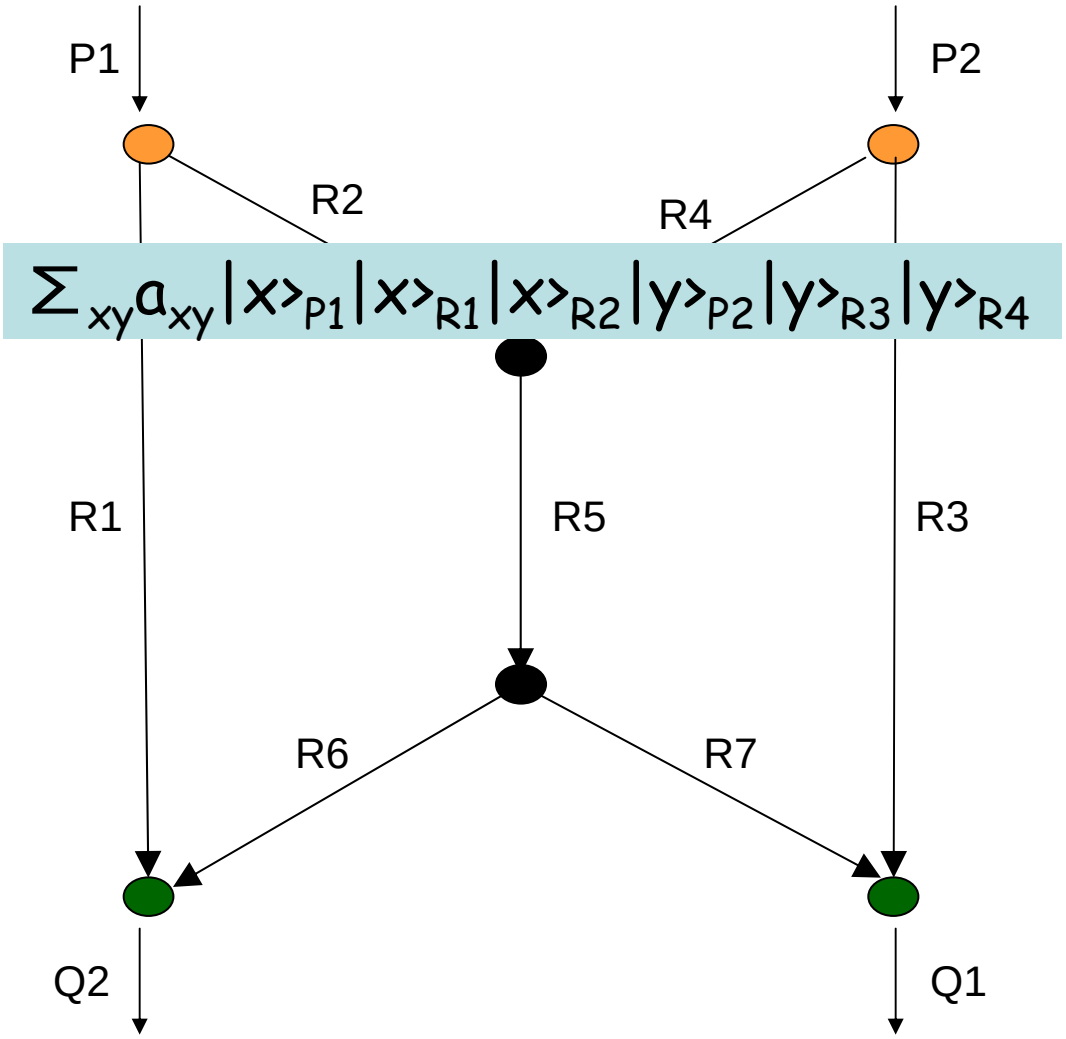
P1をR1,R2に「コピー」
P2をR3,R4に「コピー」

具体例



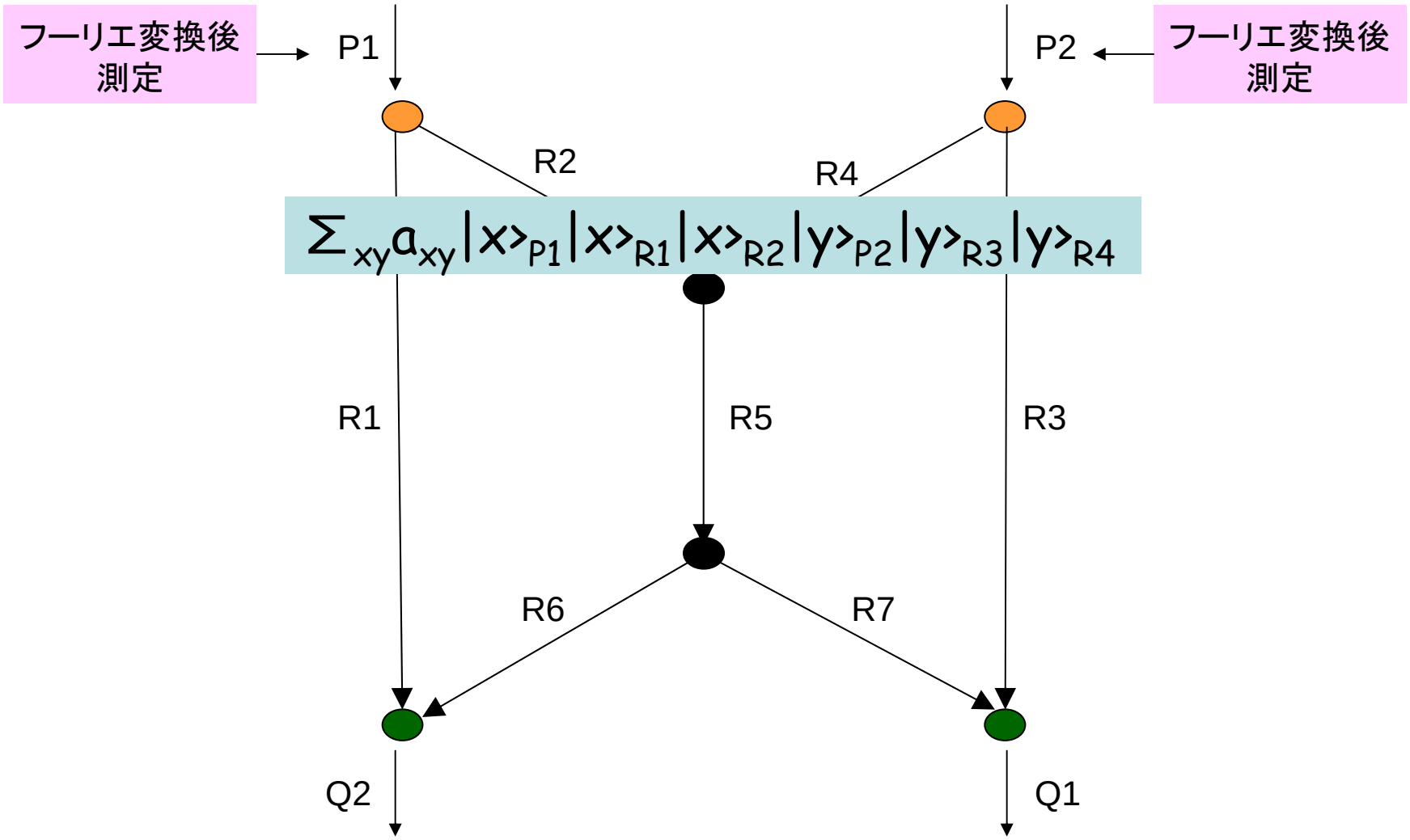
P1をR1,R2に「コピー」
P2をR3,R4に「コピー」

具体例

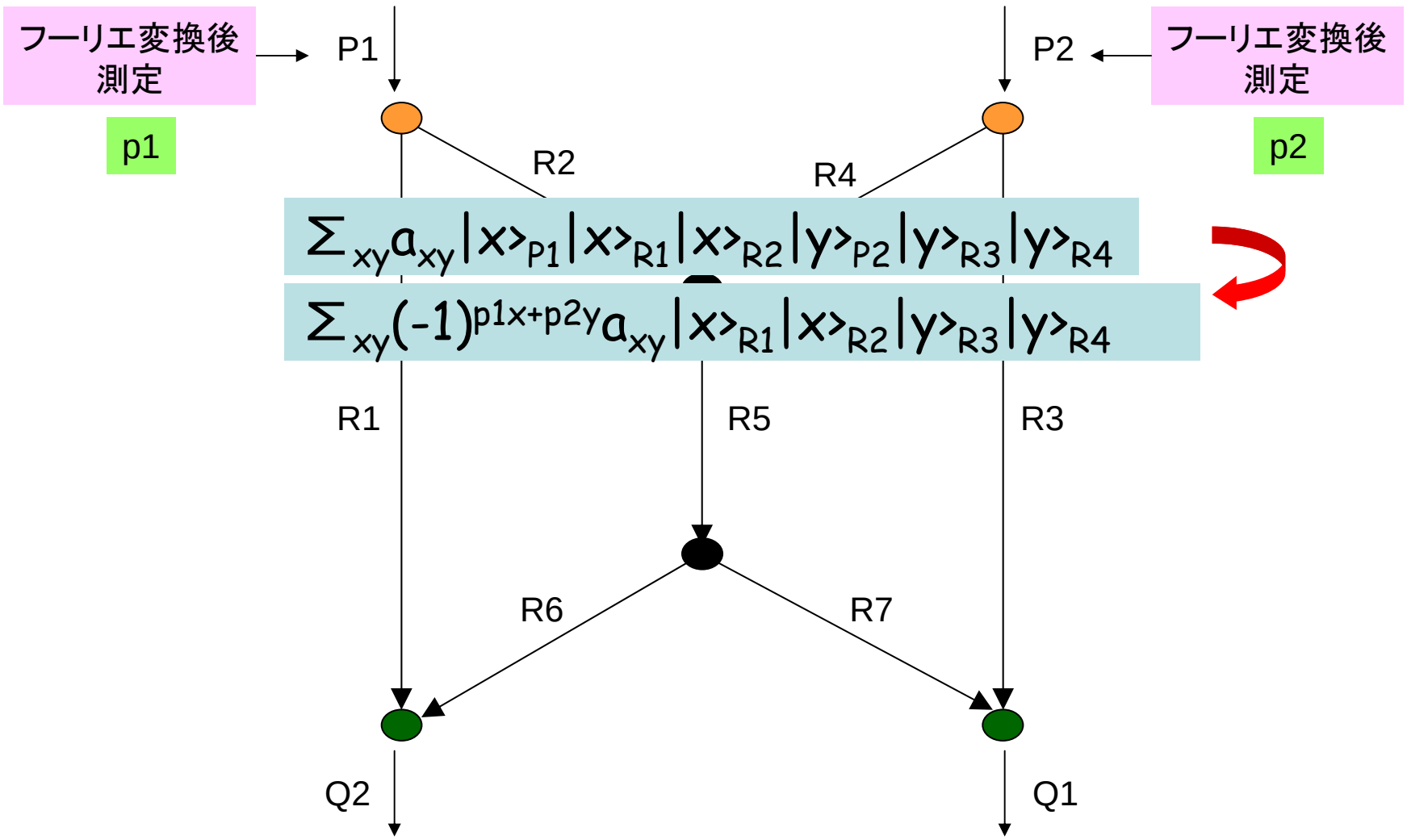


P1をR1,R2に「コピー」
P2をR3,R4に「コピー」

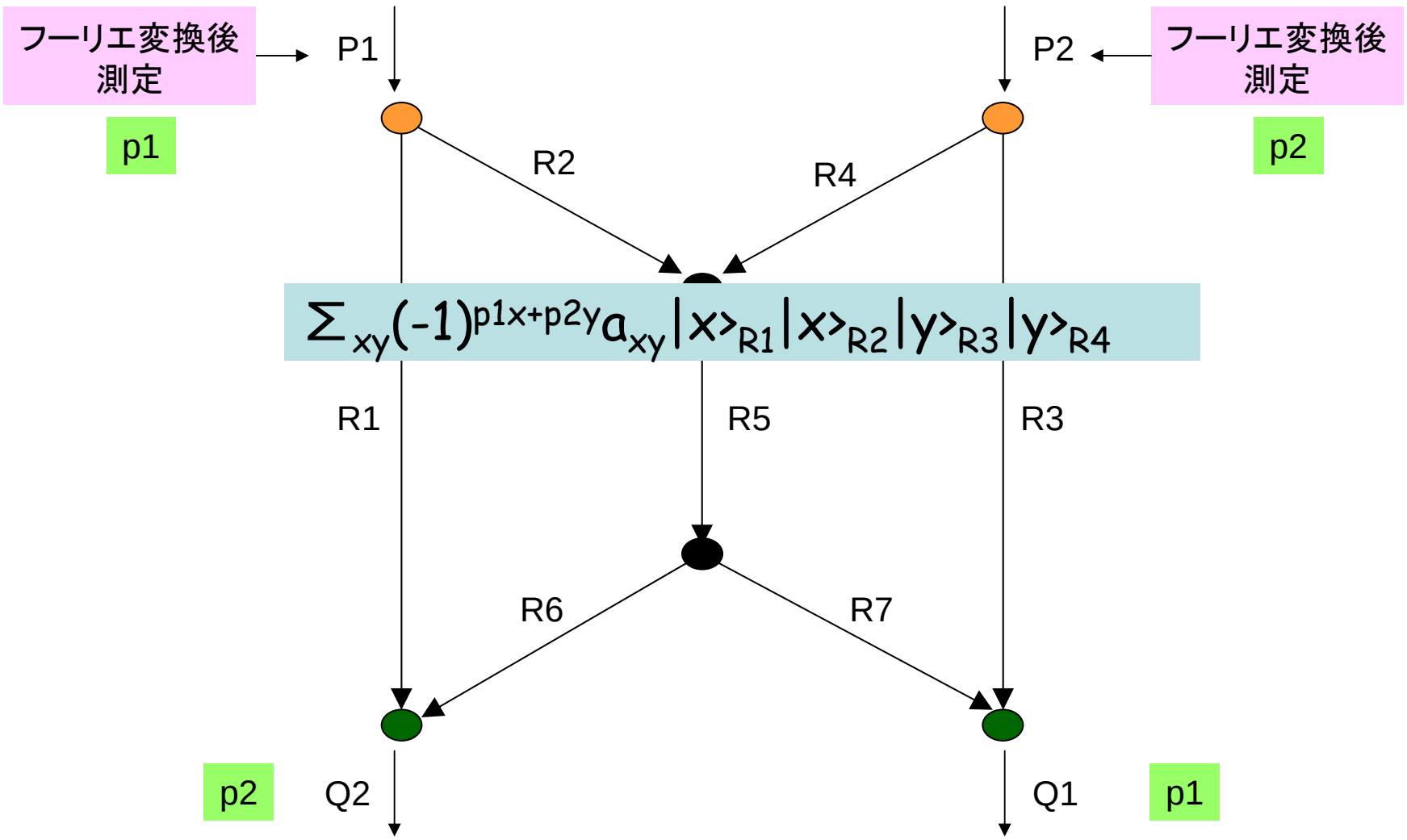
具体例



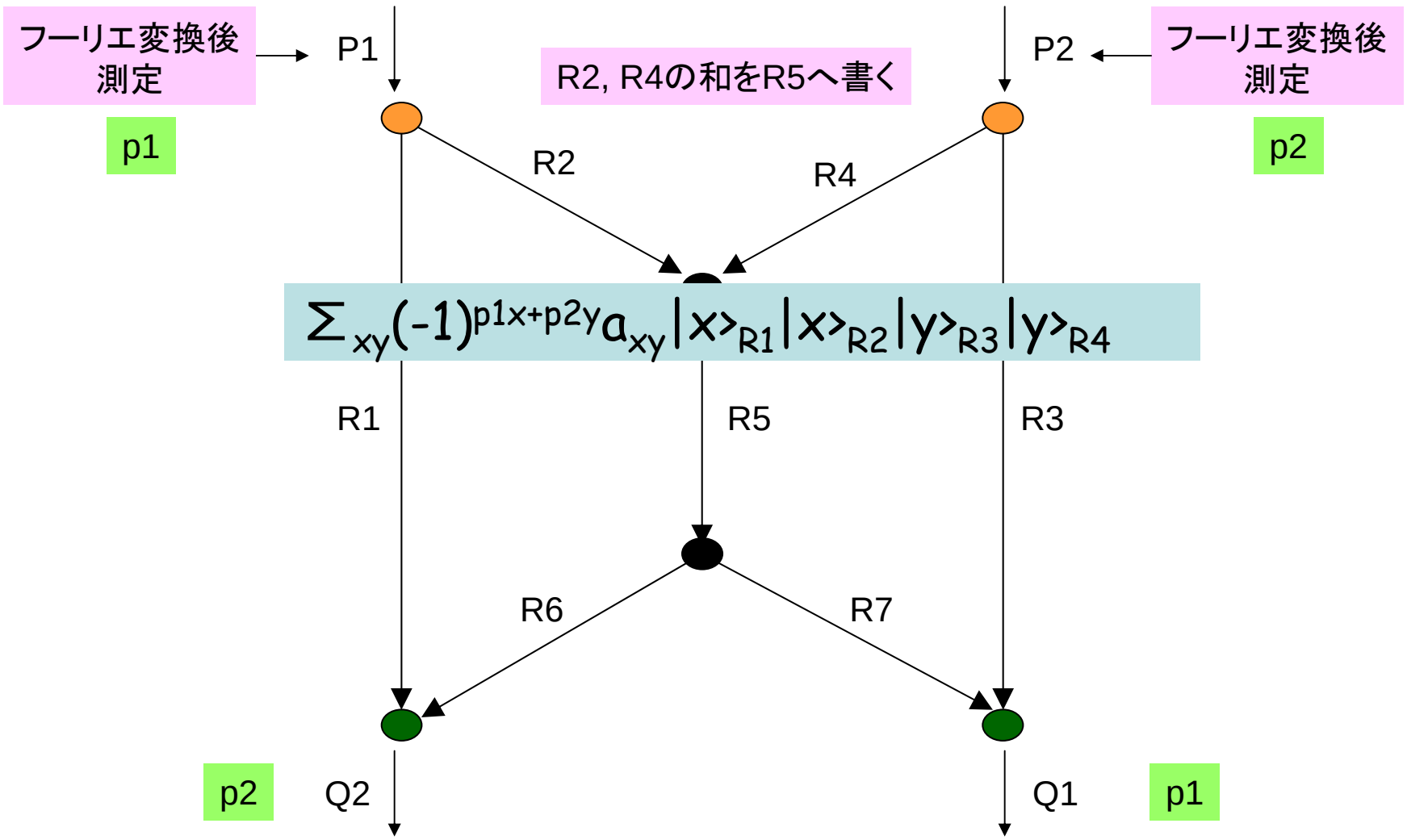
具体例


フーリエ変換後
測定
p1
P1
P2
フーリエ変換後
測定
p2
R2
R4
$\Sigma_{xy} a_{xy} |x\rangle_{P1} |x\rangle_{R1} |x\rangle_{R2} |y\rangle_{P2} |y\rangle_{R3} |y\rangle_{R4}$
$\Sigma_{xy} (-1)^{p1x+p2y} a_{xy} |x\rangle_{R1} |x\rangle_{R2} |y\rangle_{R3} |y\rangle_{R4}$
R1
R5
R3
R6
R7
Q2
Q1

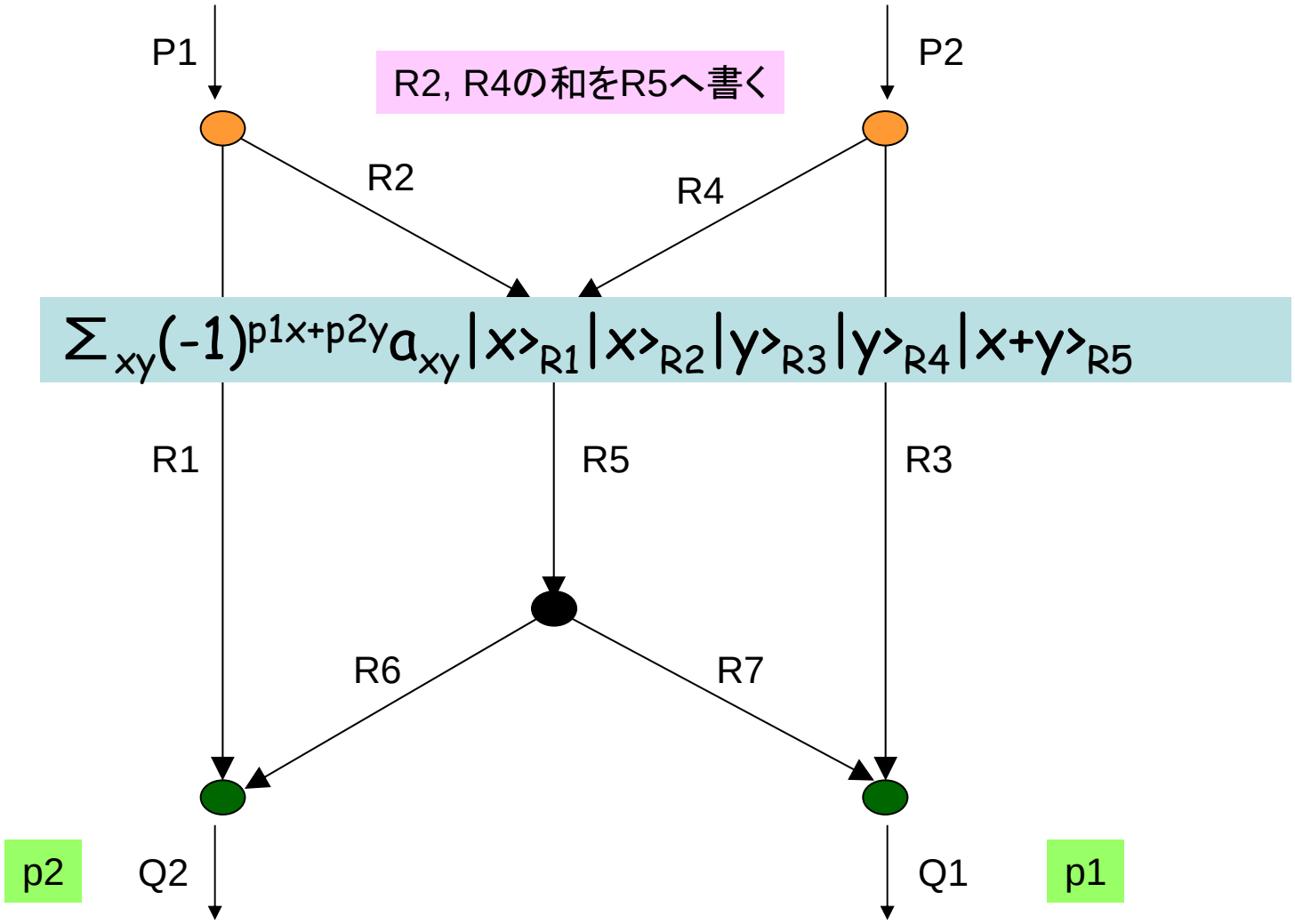
具体例


フーリエ変換後
測定
p1
P1
P2
フーリエ変換後
測定
p2
R2
R4
$\Sigma_{xy}(-1)^{p1x+p2y}a_{xy}|x\rangle_{R1}|x\rangle_{R2}|y\rangle_{R3}|y\rangle_{R4}$
R1
R5
R3
R6
R7
p2
Q2
Q1
p1

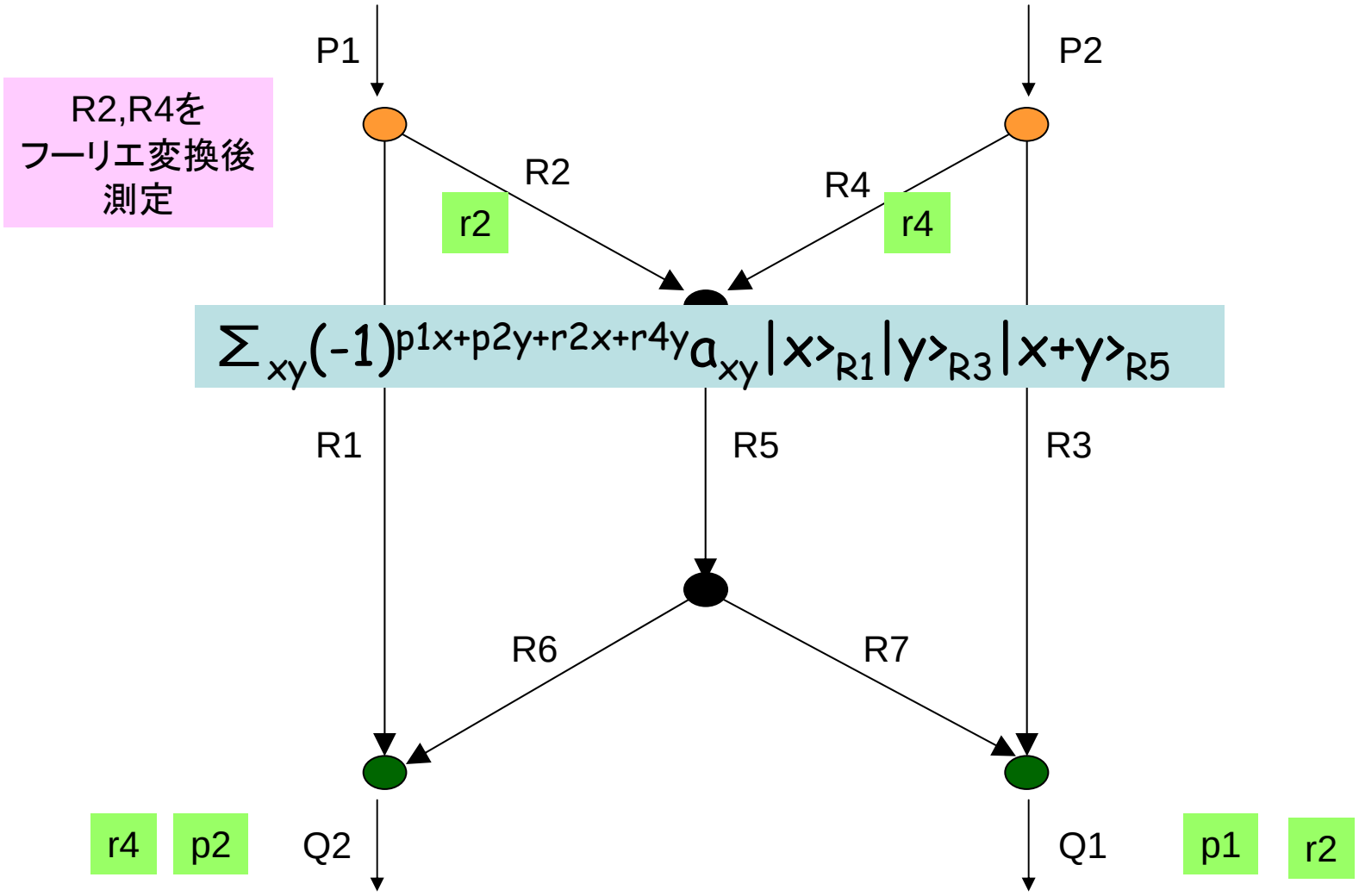
具体例


フーリエ変換後
測定
p1
P1
R2, R4の和をR5へ書く
P2
フーリエ変換後
測定
p2
R2
R4
$\Sigma_{xy}(-1)^{p1x+p2y}a_{xy}|x\rangle_{R1}|x\rangle_{R2}|y\rangle_{R3}|y\rangle_{R4}$
R1
R5
R3
R6
R7
p2
Q2
Q1
p1

具体例

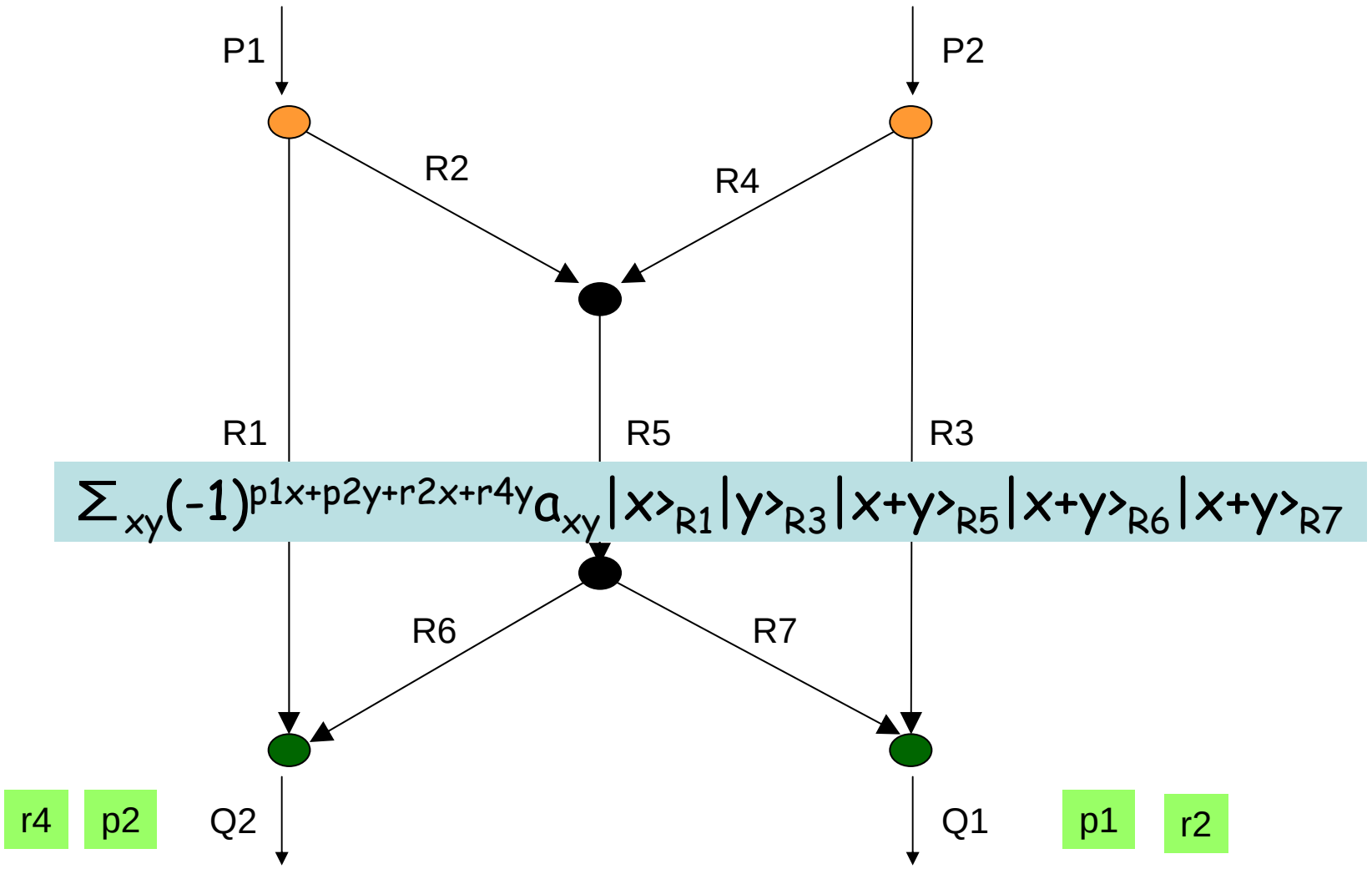

P1
P2
R2, R4の和をR5へ書く
R2
R4
$\Sigma_{xy}(-1)^{p1x+p2y}a_{xy}|x\rangle_{R1}|x\rangle_{R2}|y\rangle_{R3}|y\rangle_{R4}|x+y\rangle_{R5}$
R1
R5
R3
R6
R7
p2
Q2
Q1
p1

具体例


R2,R4を
フーリエ変換後
測定
P1
P2
R2
r2
R4
r4
$\Sigma_{xy}(-1)^{p1x+p2y+r2x+r4y}a_{xy}|x\rangle_{R1}|y\rangle_{R3}|x+y\rangle_{R5}$
R1
R5
R3
R6
R7
r4
p2
Q2
Q1
p1
r2

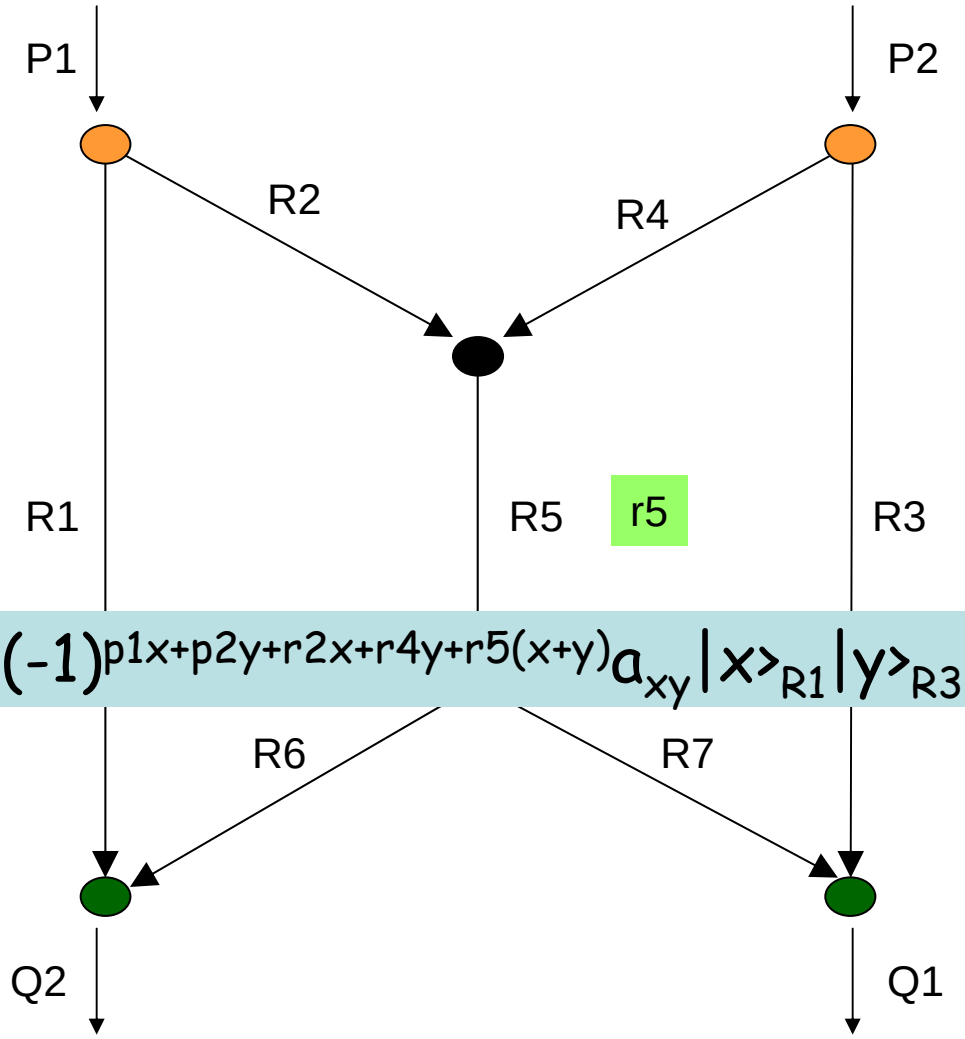
具体例

R5をR6,R7に「コピー」



具体例

R5を
フーリエ変換後
測定



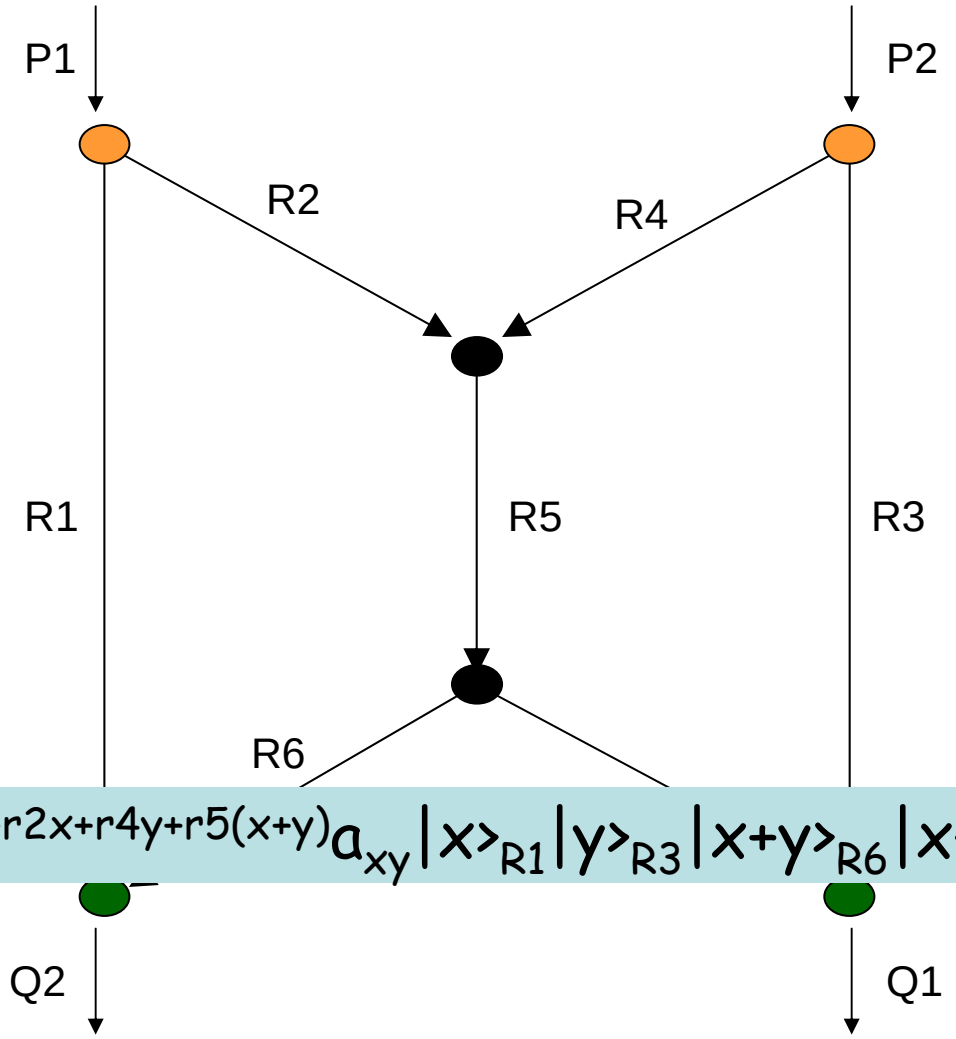
$$\Sigma_{xy}(-1)^{p1x+p2y+r2x+r4y+r5(x+y)}a_{xy}|x\rangle_{R1}|y\rangle_{R3}|x+y\rangle_{R6}|x+y\rangle_{R7}$$

r5 r4 p2

p1 r2 r5

R7, R3の和をQ1へ書く
R1, R6の和をQ2へ書く

具体例



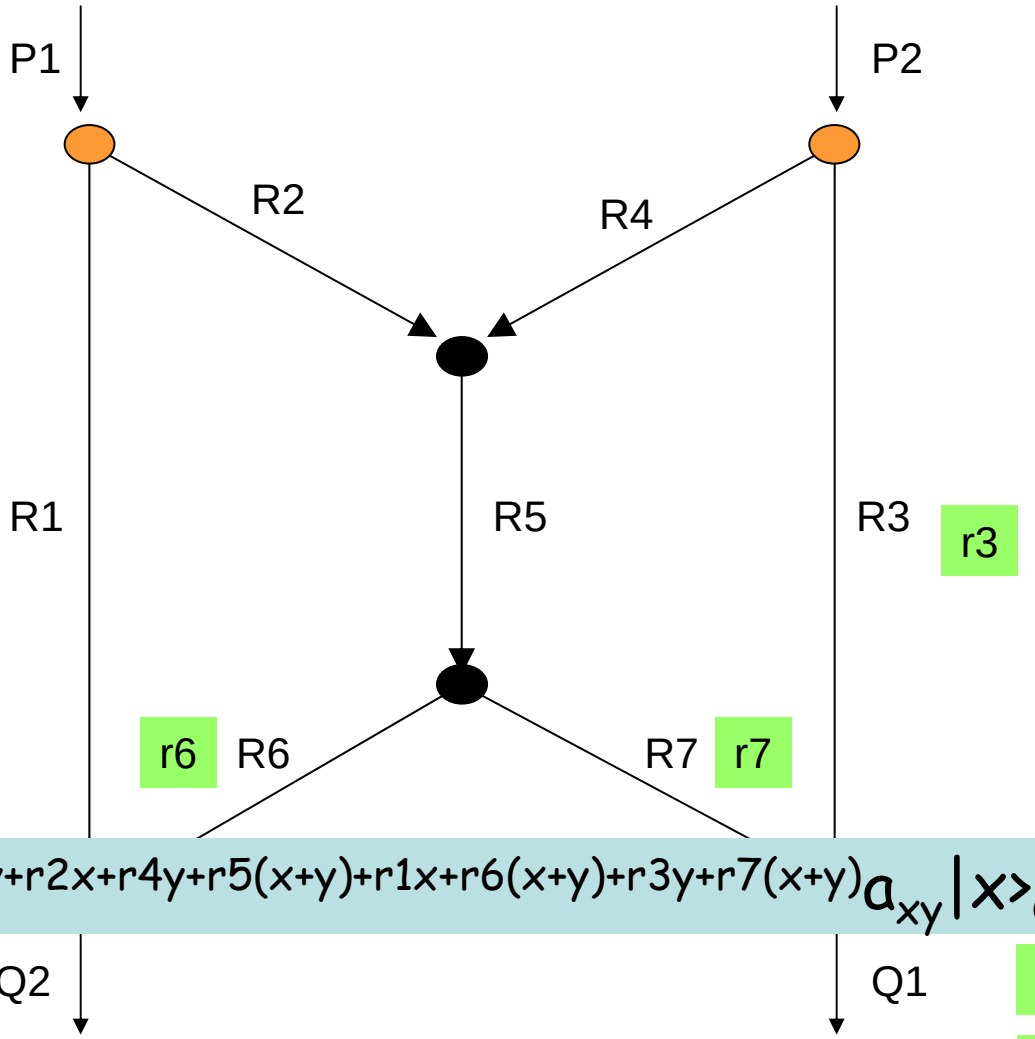
$$\Sigma_{xy}(-1)^{p1x+p2y+r2x+r4y+r5(x+y)}a_{xy}|x\rangle_{R1}|y\rangle_{R3}|x+y\rangle_{R6}|x+y\rangle_{R7}|x\rangle_{Q1}|y\rangle_{Q2}$$

r5 r4 p2

p1 r2 r5

具体例

R1,R6,R7,R3を
フーリエ変換後
測定



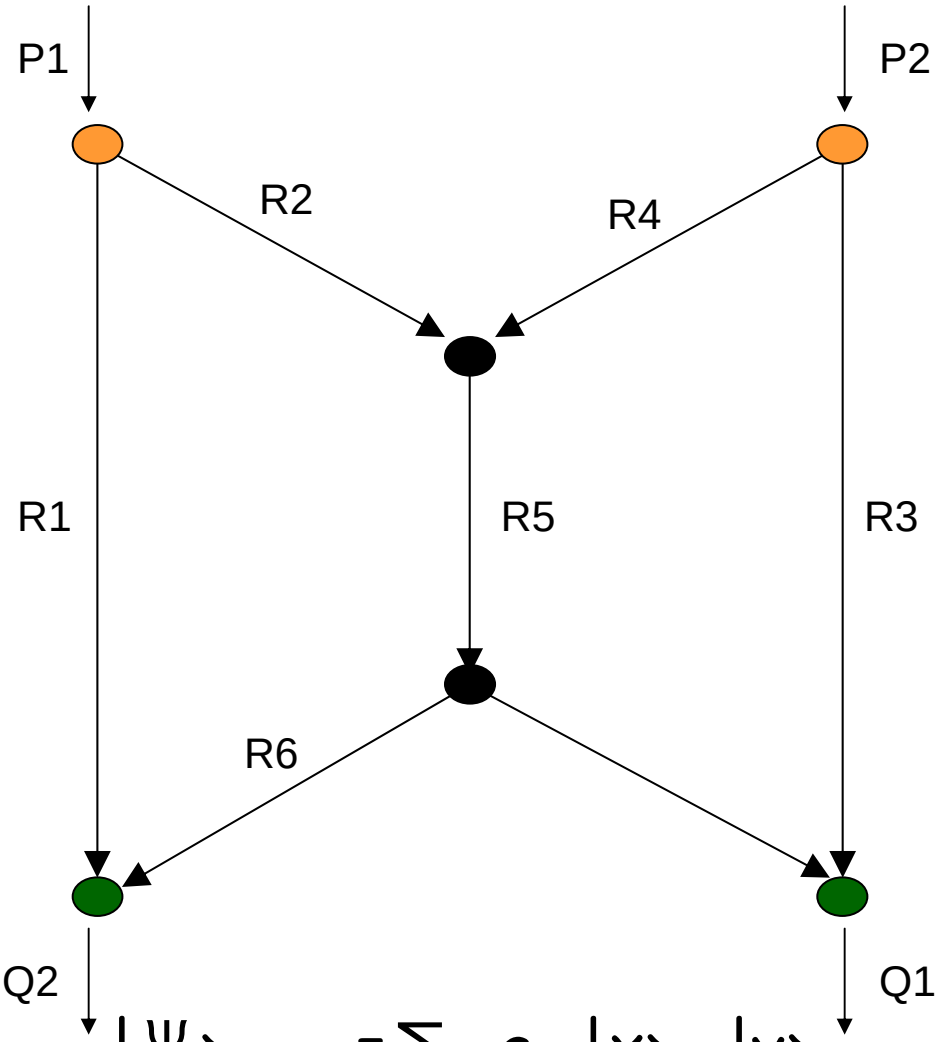
r1 r3 r6 r7

$$\Sigma_{xy}(-1)^{p1x+p2y+r2x+r4y+r5(x+y)+r1x+r6(x+y)+r3y+r7(x+y)}a_{xy}|x\rangle_{Q1}|y\rangle_{Q2}$$

r5 r4 p2 r3 r6 r7

p1 r2 r5 r1 r6 r7

具体例



Q1,Q2で
位相エラーを訂正

r5 r4 p2
r3 r6 r7

p1 r2 r5
r1 r6 r7

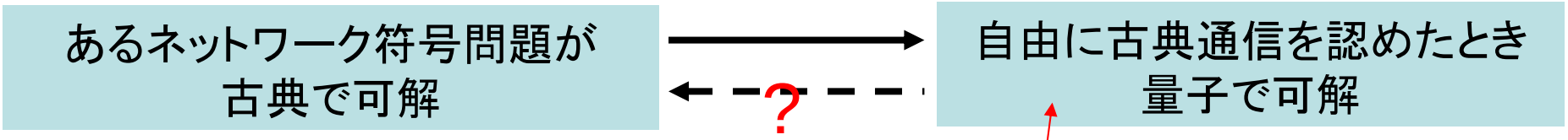
今後の課題（狭い意味で）

[補助的リソースが何も利用できない場合]

あるネットワーク符号問題が量子で可解ならば，その解はルーティングで達成可能？ ←ある非常に限られたクラスのネットワークのみ肯定的に証明

[Leung et al. 2010]

[補助的に古典通信が利用できる場合]



実は･･･古典の未解決問題と関連するかも？

無向グラフにおけるkペア通信問題が可解ならば，かならずルーティングによる解が存在する？

量子テレポーテーションを使うことで，
有向辺の逆向きに量子情報を送ることが
可能になるので，実質無向グラフ

今後の課題

- 一般のグラフにおける達成可能なレート
- 応用（古典のワイヤレス通信のような）
- セキュリティや計算量的側面における優位性
- 損失のある量子チャネル

などなど・・・

参考文献（古典のネットワーク符号関連）

- R. Alhswede, N. Cai, S.-Y. R. Li, R. Yeung. Network information flow. IEEE Transactions on Information Theory 46(4), pp.1204-1216, 2000.
- K. Iwama, H. Nishimura, M. Paterson, R. Raymond, S. Yamashita. Polynomial-time construction of linear network coding. Proc. ICALP2008 (Lecture Notes in Computer Science 5125), pp.271-282, 2008.
- S. Jaggi, P. Sanders, P.A. Chou, M. Effros, S. Egner, K. Jain, L. Tolhuizen. Polynomial time algorithms for multicast network coding construction. IEEE Transactions on Information Theory 51(6), pp.1973-1982, 2005.
- A. R. Lehman. Network Coding. Ph.D. dissertation, MIT, 2005.
- A. Lehman, E. Lehman. Complexity classification of network information flow problems. Proc. SODA2004, pp.142-150, 2004
- S.-Y. R. Li, R. Yeung, N. Cai. Linear network coding. IEEE Transactions on Information Theory 49(2), pp.371-381, 2003.
- C.-C. Wang, N. B. Shroff. Beyond the butterfly – a graph-theoretic characterization of the feasibility of network coding with two simple unicast sessions. Proc. ISIT2007, pp. 121-125, 2007.

参考文献（量子ネットワーク符号関連）

- M. Hayashi. Prior entanglement between senders enables perfect quantum network coding with modification. Physical Review A76(4), 040301(R), 2007.
- M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, S. Yamashita. Quantum network coding. Proc. STACS2007 (Lecture Notes in Computer Science 4393), pp.610-621, 2007. quant-ph/0601088.
- H. Kobayashi, F. Le Gall, H. Nishimura, M. Roetteler. Perfect quantum network communication protocol based on classical network coding. Proc. ISIT2010, pp.2686-2690, 2010. arXiv:0902.1299.
- H. Kobayashi, F. Le Gall, H. Nishimura, M. Roetteler. General scheme for perfect quantum network coding with free classical communication. Proc. ICALP2009 (Lecture Notes in Computer Science 5555), pp.622-633, 2009. arXiv:0908.1457.
- D. Leung, J. Oppenheim, A. Winter. Quantum network communication –the butterfly and the beyond. IEEE Transactions on Information Theory 56(7), pp.3478-3490, 2010. quant-ph/0608223.
- Y. Shi, E. Soljanin. On multicast in quantum networks. Proc. CISS2006, pp.871-876, 2006.