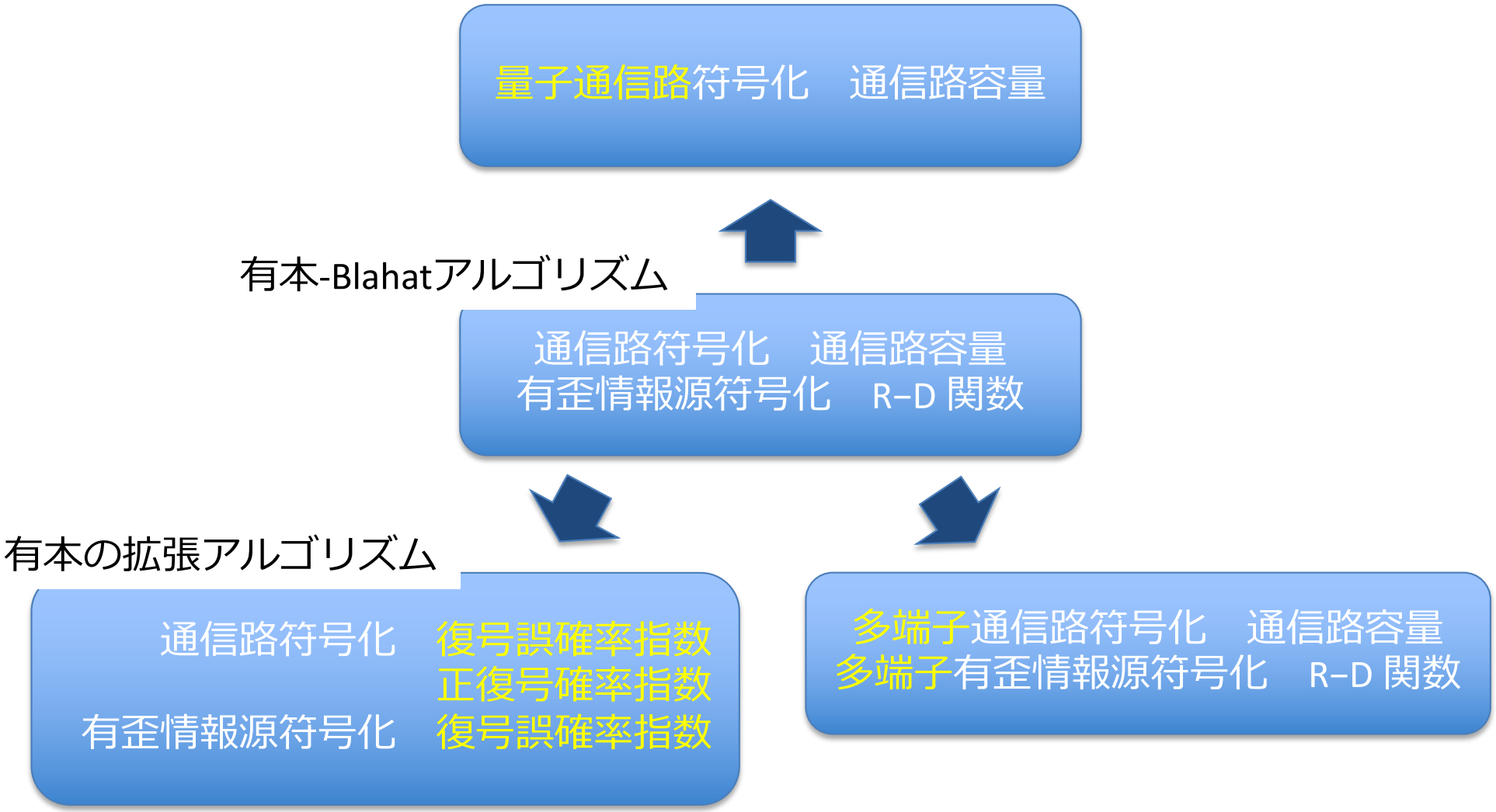
電子情報通信学会2023年総合大会
チュートリアルセッション

Arimoto-Blahutアルゴリズムの50年

有本-Blahutアルゴリズムの多端子モデルへの拡張とその収束性について

早稲田大学　松嶋敏泰

有本–Blahutアルゴリズムの拡張



本チュートリアルの内容

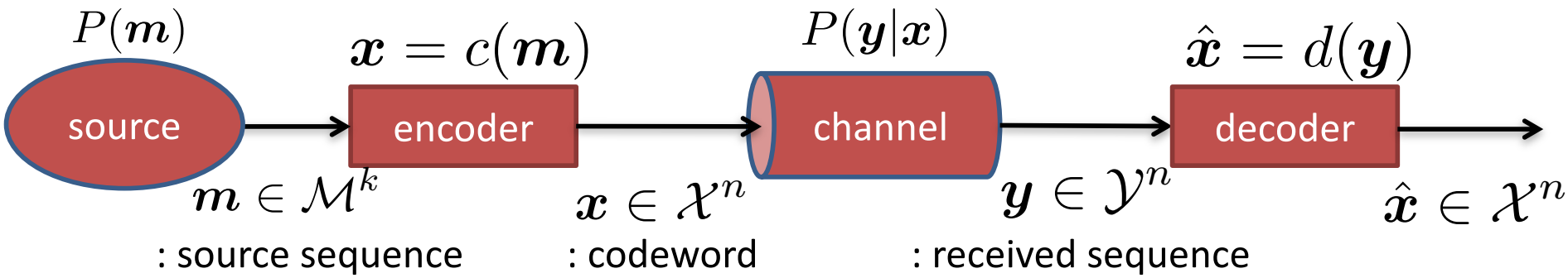
有本-Blahatアルゴリズム

通信路符号化　通信路容量
有歪情報源符号化　R–D 関数

多端子通信路符号化　通信路容量
多端子有歪情報源符号化　R–D 関数

- 多端子モデル上の情報理論的問題の一般表記
- 多端子モデルに適用可能なABアルゴリズムの一般化
- その大域的収束性について
- 適用例
  - CsiszarらのBCの秘密保持容量
  - Kaspiの有歪み情報源符号化多端子モデル

Objective of Channel Coding: Efficiency & Reliability



Efficiency:

$$\text{Coding Rate} = \frac{k}{n}$$

Reliability:

$$\text{Error Rate} = Pr\{\boldsymbol{x} \neq \hat{\boldsymbol{x}}\}$$

Objective of Channel coding:

$$Pr\{\boldsymbol{x} \neq \hat{\boldsymbol{x}}\} \to 0 \qquad \frac{k}{n} \to \max$$

Theoretical bound by Shannon

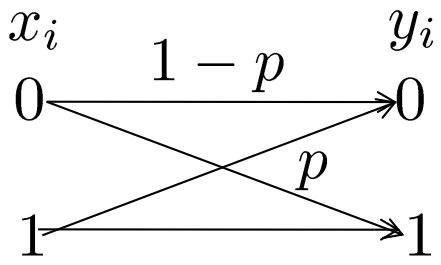
Shannon's channel coding theorem[1948]:

Let Channel Capacity C as the following equation. There exists a coding and decoding system with $\frac{k}{n} < C$, with that system we can transmit information with negligible error rate. If $\frac{k}{n} > C$, then no such system exists.

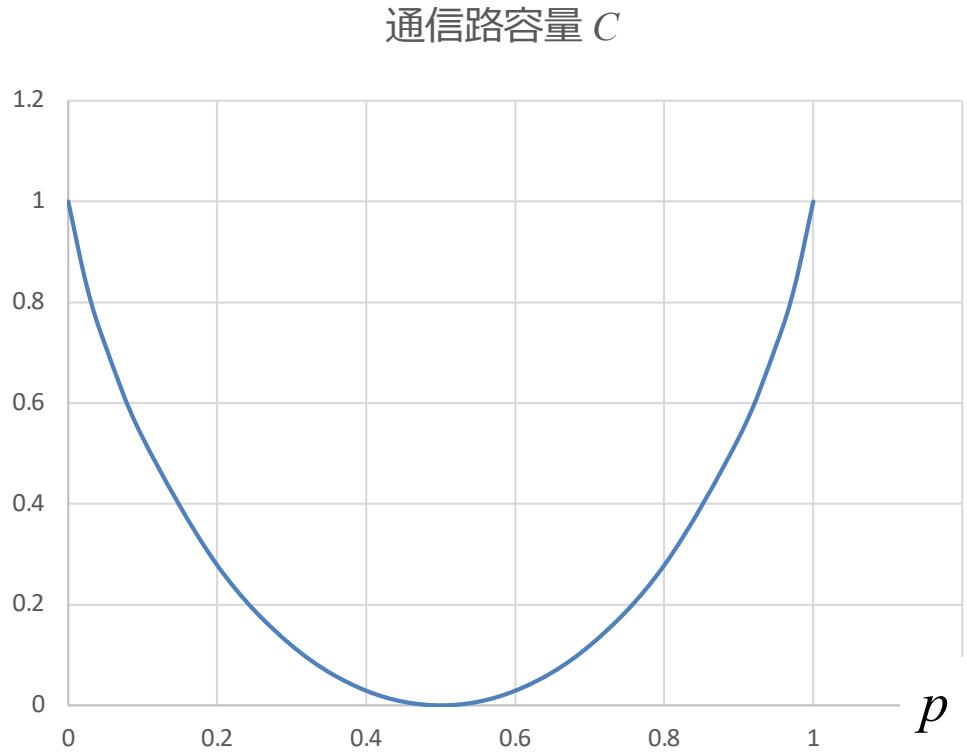
$$C = \max_{q(x) \in \mathcal{Q}} \sum_x \sum_y q(x) P(y|x) \log \frac{P(y|x)}{\sum_x q(x) P(y|x)}.$$

Capacity（通信路容量）の例

e.g.) The capacity C of a Binary Symmetric Channel is as follows:



$$C = 1 + p\log p + (1-p)\log(1-p)$$



最適化問題として考えると

Shannon's channel coding theorem[1948]:

通信路の遷移確率 $P(y|x)$ が与えられた下で，入力（符号）の分布 $q(x) \in \mathcal{Q}$ を操作することにより，相互情報量 $I(X;Y)$ を最大化する

$$C = \max_{q(x)\in\mathcal{Q}} \sum_x \sum_y q(x)P(y|x) \log \frac{P(y|x)}{\sum_x q(x)P(y|x)}.$$

制約付き最適化問題

凸計画問題（凸制約領域上の凸関数の最大化）

$$q(x) \in \mathcal{Q} \qquad I(X;Y)$$

有歪の情報源符号化問題　R(D)関数

レート歪み関数 $R(D)$ は，情報源分布 $P(s)$ が与えられた下で，歪み D で制限された試験通信路の遷移確率 $q(x|s)$ を操作することにより，相互情報量 $I(S;X)$ を最小化

$$R(D) = \min_{q(x|s)\in\mathcal{Q}_D} \sum_s \sum_x P(s)q(x|s) \log \frac{q(x|s)}{\sum_s P(s)q(x|s)}.$$

確率分布だけでなく歪の制約も加わる

$$q(x|s) \in \mathcal{Q}_D = \{q(x|s) | \sum_s \sum_x P(s)q(x|s)d(s,x) \le D\}$$

有歪情報源符号化　R(D)関数のパラメトリック表現

$$R(D) = \min_{q(x|s)\in\mathcal{Q}_{\mathcal{D}}} \sum_s \sum_x P(s)q(x|s) \log \frac{q(x|s)}{\sum_s P(s)q(x|s)}.$$

確率分布だけでなく歪の制約も加わる

$$q(x|s) \in \mathcal{Q}_D = \{q(x|s) | \sum_s \sum_x P(s)q(x|s)d(s,x) \leq D\}$$

歪み制約についてのラグランジュ未定乗数 μ を固定したパラメトリックな表現と呼ばれるレート歪み関数 $R(D_\mu)$ の形式を用いることで，歪み制約がない関数として計算

有本–Blahutアルゴリズム

有本-Blahut アルゴリズムは，上記の通信路容量 C とレート歪み関数 $R(D_\mu)$ を繰り返し計算により効率的に求める方法として知られている

その革新的 Key Points は

その Key Points を継承したアルゴリズムの拡張を行いたい

Key Point 1　二重最適化（通信路容量を例に）

新しいnotationの導入

$$Q[p(x)](x|y) = \frac{p(x)P(y|x)}{\sum_x p(x)P(y|x)}$$

逆条件付き確率を汎関数的に表現

$$C = \max_{q(x)\in\mathcal{Q}} \sum_x \sum_y q(x)P(y|x) \log \frac{P(y|x)}{\sum_x q(x)P(y|x)}.$$

二重最適化

$$C = \max_{q(x)\in\mathcal{Q}} \max_{Q[p(x)](x|y)} f(q(x), Q[p(x)](x|y)),$$

$$f(q(x), Q[p(x)](x|y)) = \sum_x \sum_y q(x)P(y|x) \log \frac{Q[p(x)](x|y)}{q(x)}.$$

Key Point 2　交互最適化（通信路容量を例に）

Step 1

n 回目のステップにおいては，一方の $q^{(n)}(x)$ を固定した下で，$Q[p(x)](x|y)$ により目的関数 $f(q(x), Q[p(x)](x|y))$ の最適化（最大化）をおこなう．

実質動かすのは　$p(x)$

$$f(q(x), Q[p(x)](x|y)) = \sum_x \sum_y q(x)P(y|x) \log \frac{Q[p(x)](x|y)}{q(x)}.$$

Step 2

次にはその $Q^{(n)}[p(x)](x|y)$ を固定した下で，$q(x)$ により $f(q(x), Q[p(x)](x|y))$ の最適化（最大化）をおこなう．

$$f(q(x), Q[p(x)](x|y)) = \sum_x \sum_y q(x)P(y|x) \log \frac{Q[p(x)](x|y)}{q(x)}.$$

Key Point 3　個別最適化計算が容易

Step 1

Shannon の補題から明らかなように $p(x) = q(x)^{(n)}$ とおき $Q[q(x)^{(n)}](x|y)$ とすることで簡単に求めることができる.

$$C = \max_{q(x)\in\mathcal{Q}} \max_{Q[p(x)](x|y)} f(q(x), Q[p(x)](x|y)),$$

$$p(x) = q(x)^{(n)}$$

Key Point 3　個別最適化計算が容易

Step 2

$q(x)$ が確率分布である制約 $q(x) \in \mathcal{Q}$ を条件とする制約付き最適化問題を，ラグランジュ未定乗数法で解くことで得られる．それは $Q^{(n)}[q(x)^{(n)}](x|y)$ を用いた簡単な比率の計算となっている．

$$C = \max_{q(x) \in \mathcal{Q}} \max_{Q[p(x)](x|y)} f(q(x), Q[p(x)](x|y)),$$

$$q(x)^{(n+1)} = \frac{\gamma(x)^{(n)}}{\sum_x \gamma(x)^{(n)}}$$

$$\gamma(x)^{(n)} = \exp(\sum_y P(y|x) \log Q[p(x)](x|y)^{(n)})$$

Key Point 4　単調に最適解に収束

この有本-Blahutアルゴルズムの重要な特徴は，求めたい最適解つまり通信路容量やレート歪み関数に単調に収束することである．

さらに，適切な条件が揃えば繰り返し回数の指数関数で最適解に収束することも示されている．

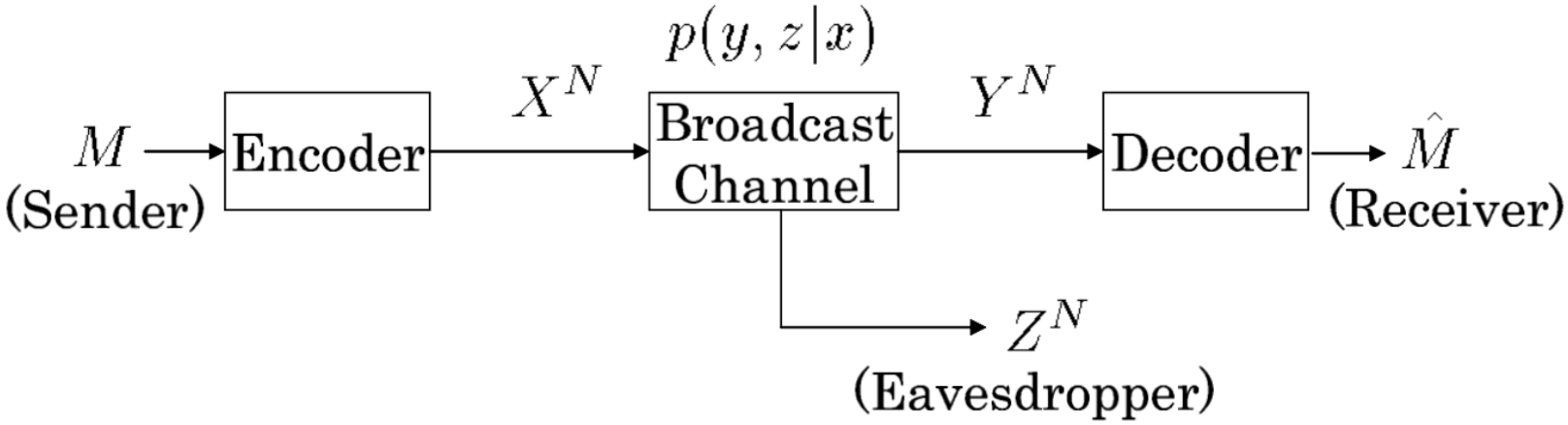
凸計画問題

多端子モデルへの拡張

多端子モデル問題の例 1

Çiszár らにより，Broadcast Channel において受信者の一方が盗聴者となる問題設定が提案.

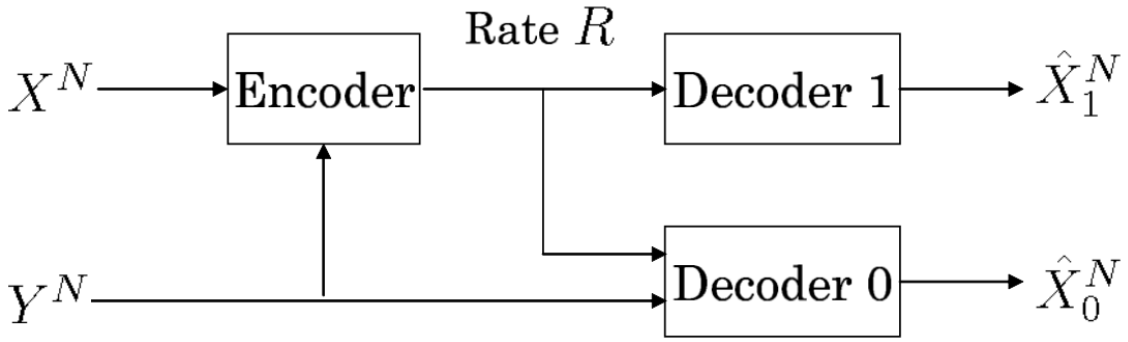
メッセージ M の情報を盗聴者に一切漏らさない条件で，伝送可能な符号化レートの最大値を秘密保持容量 C_s と定義した．通信路 $P(y,z|x)$ を周辺化して得られる $P_1(y|x)$ と $P_2(z|x)$ をそれぞれ主通信路と盗聴通信路と定義し，主通信路が盗聴通信路に比べて less noisy な場合の秘密保持容量を以下のように導出.



$$C_s = \max_{q(x)\in\mathcal{Q}} \left(I(X;Y) - I(X;Z)\right).$$

多端子モデル問題の例２

Kaspi により提案された，復号器が２つあり一方のみで補助情報が利用できる多端子モデルにおけるレート歪み関数



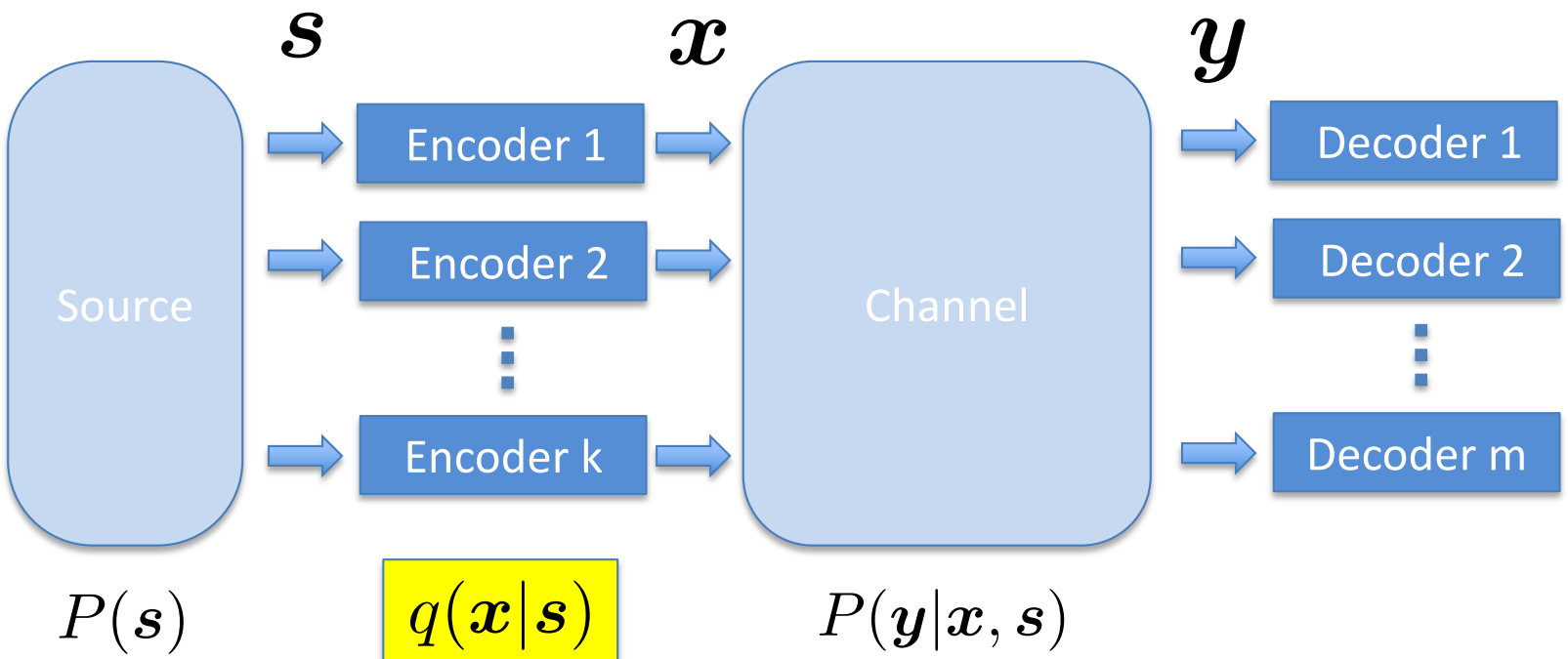
$$R(D_1, D_0) = \min_{q \in \mathcal{Q}(D_1, D_0)} (I(X, Y; \hat{X}_1) - I(X; \hat{X}_0 | Y, \hat{X}_1)).$$

$$\begin{aligned} \mathcal{Q}((D_1, D_0) \quad = \quad & \{q : \sum_{\hat{x}_1, \hat{x}_0} q(\hat{x}_1, \hat{x}_0 | x, y) = 1, q(\hat{x}_1, \hat{x}_0 | x, y) \geq 0, \\ & \sum_{x, y, \hat{x}_1, \hat{x}_0} p(x, y) q(\hat{x}_1, \hat{x}_0 | x, y) d_1(x, \hat{x}_1) \leq D_1 \\ & \sum_{x, y, \hat{x}_1, \hat{x}_0} p(x, y) q(\hat{x}_1, \hat{x}_0 | x, y) d_1(x, \hat{x}_0) \leq D_0\}. \end{aligned}$$

多端子モデルの確率表現

ベクトルです

$$P(\boldsymbol{s})q(\boldsymbol{x}|\boldsymbol{s})P(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s})$$



正確には$\boldsymbol{S}$の一部の情報を使って独立に符号化を行うので
いくつかの条件付き確率に分かれるが簡略化して表現する

多端子の情報理論的問題の一般的表現

多端子情報理論の通信路容量やレート歪み関数を求める多くの問題

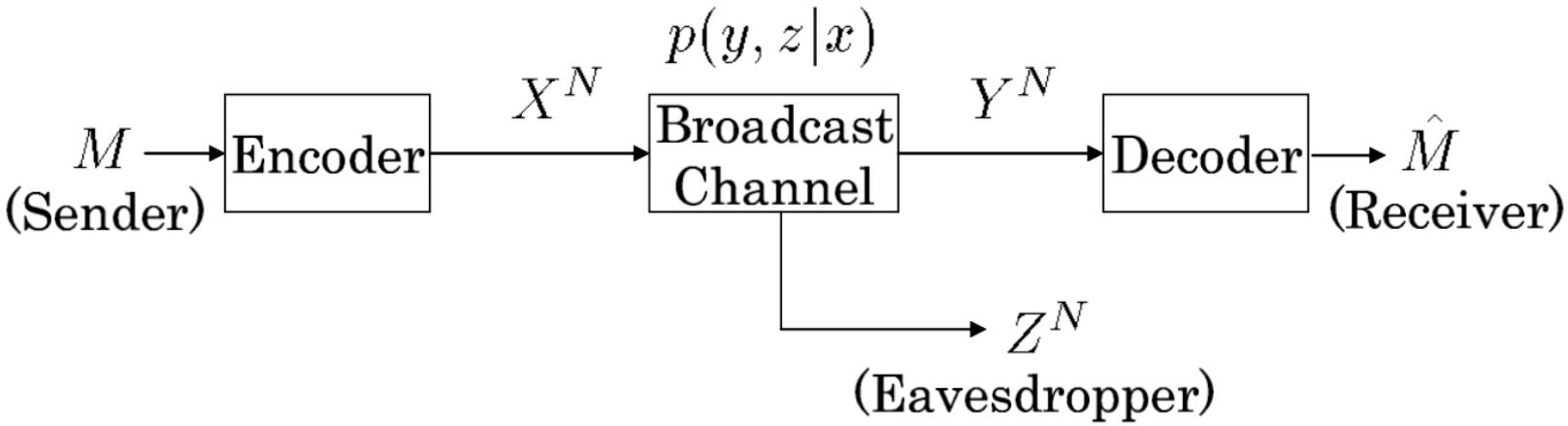
$P(\boldsymbol{s}), P(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s})$ を固定した下で,
$q(\boldsymbol{x}|\boldsymbol{s})$ を操作して,
以下のような情報理論的量を最適化する問題として定義.

P_l は $P(\boldsymbol{s})$ と $P(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s})$ のみを用いた積等の関数.
この関数によって問題設定において固定される量を表している.

$$R = \min_{q(\boldsymbol{x}|\boldsymbol{s})\in\mathcal{Q}} \sum_{\boldsymbol{s}}\sum_{\boldsymbol{x}}\sum_{\boldsymbol{y}} P(\boldsymbol{s})q(\boldsymbol{x}|\boldsymbol{s})P(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s}) \log \frac{q(\boldsymbol{x}|\boldsymbol{s})\prod_l P_l}{\prod_k Q_k[p(\boldsymbol{x}|\boldsymbol{s})]}.$$

$Q_k[p(\boldsymbol{x}|\boldsymbol{s})]$ は, 固定された分布 $P(\boldsymbol{s}), P(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s})$ と
任意の分布 $p(\boldsymbol{x}|\boldsymbol{s})$ を用いて積や周辺化等で計算される関数.

一般的表現の例（例１の秘密保持容量）



$$C_s = \max_{q(x)\in\mathcal{Q}} (I(X;Y) - I(X;Z)).$$

一般的表現の例（例１の秘密保持容量）

$$C_s = \max_{q(x)\in\mathcal{Q}} (I(X;Y) - I(X;Z)).$$

$$C_s = - \min_{q(x)\in\mathcal{Q}} \sum_{x,y,z} q(x)P(y,z|x) \log \frac{q(x)P_2(z|x)}{Q_1[p(x)]Q_2[p(x)]},$$

$$\begin{aligned} Q_1[p(x)] &= \frac{p(x)P_1(y|x)}{\sum_x p(x)P_1(y|x)}, \\ Q_2[p(x)] &= \sum_x p(x)P_2(z|x). \end{aligned}$$

ABアルゴリズムの多端子モデルへの拡張

Key Point 1　二重最適化

$$R = \min_{q(\boldsymbol{x}|\boldsymbol{s})\in\mathcal{Q}} \sum_{\boldsymbol{s}}\sum_{\boldsymbol{x}}\sum_{\boldsymbol{y}} P(\boldsymbol{s})q(\boldsymbol{x}|\boldsymbol{s})P(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s}) \log \frac{q(\boldsymbol{x}|\boldsymbol{s})\prod_l P_l}{\prod_k Q_k[p(\boldsymbol{x}|\boldsymbol{s})]}.$$

$$R = \min_{q(\boldsymbol{x}|\boldsymbol{s})\in\mathcal{Q}} \min_{Q_1,\cdots Q_K} f(q, Q_1, \cdots Q_K)$$

$$f(q, Q_1, \cdots Q_K) = \sum_{\boldsymbol{s}}\sum_{\boldsymbol{x}}\sum_{\boldsymbol{y}} P(\boldsymbol{s})q(\boldsymbol{x}|\boldsymbol{s})P(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{s}) \log \frac{q(\boldsymbol{x}|\boldsymbol{s})\prod_l P_l}{\prod_k Q_k[p(x|s)]}.$$

Key Point 2　交互最適化

$$R = \min_{q(\boldsymbol{x}|\boldsymbol{s}) \in \mathcal{Q}} \min_{Q_1, \cdots Q_K} f(q, Q_1, \cdots Q_K)$$

n 回目のステップでは，一方の $q^{(n)}(\boldsymbol{x}|\boldsymbol{s})$ を固定した下で，
目的関数 $f(q, Q_1, \cdots Q_K)$ を $Q_1, \cdots Q_K$ により最小化

その $Q_1^{(n)}, \cdots Q_K^{(n)}$ を固定した下で，
$f(q, Q_1, \cdots Q_K)$ を $q(\boldsymbol{x}|\boldsymbol{s})$ により最小化

Key Point 3　個別最適化計算が容易

$q^{(n)}(\boldsymbol{x}|\boldsymbol{s})$ を固定した下で目的関数 $f(q, Q_1, \cdots Q_K)$ を最小化する $Q_k[p(\boldsymbol{x}|\boldsymbol{s})]$ は，やはり Shannon の補題から明らかなように任意の $p(\boldsymbol{x}|\boldsymbol{s})$ の関数として表現されている $Q_k[p(\boldsymbol{x}|\boldsymbol{s})]$ のそれぞれで $p(\boldsymbol{x}|\boldsymbol{s}) = q^{(n)}(\boldsymbol{x}|\boldsymbol{s})$ とおき，$Q_k[q^{(n)}(\boldsymbol{x}|\boldsymbol{s})]$ とすることで簡単に求まる

$$R = \min_{q(\boldsymbol{x}|\boldsymbol{s})\in\mathcal{Q}} \min_{Q_1,\cdots Q_K} f(q(\boldsymbol{x}|\boldsymbol{s}), Q_1, \cdots Q_K)$$

$$Q_k[p(\boldsymbol{x}|\boldsymbol{s})]$$

$$p(\boldsymbol{x}|\boldsymbol{s}) = q^{(n)}(\boldsymbol{x}|\boldsymbol{s})$$

Key Point 3　個別最適化計算が容易

$q(\boldsymbol{x}|\boldsymbol{s})$ は，$q(\boldsymbol{x}|\boldsymbol{s})$ が確率分布である制約 $q(\boldsymbol{x}|\boldsymbol{s}) \in \mathcal{Q}$ を条件とする制約付き最適化問題をラグランジュ未定乗数法で解くことで得られる．それは $Q_1^{(n)}, \cdots Q_K^{(n)}$ を用いた簡単な比率の計算で求まる

$$R = \min_{q(\boldsymbol{x}|\boldsymbol{s}) \in \mathcal{Q}} \min_{Q_1, \cdots Q_K} f(q(\boldsymbol{x}|\boldsymbol{s}), Q_1, \cdots Q_K)$$

$$q(\boldsymbol{x}|\boldsymbol{s})^{(n+1)} = \frac{\gamma(\boldsymbol{x}, \boldsymbol{s})^{(n)}}{\sum_x \gamma(\boldsymbol{x}, \boldsymbol{s})^{(n)}}$$

$$\gamma(\boldsymbol{x}, \boldsymbol{s})^{(n)} = \exp\left(\sum_{\boldsymbol{y}} P(\boldsymbol{y}|\boldsymbol{x}, \boldsymbol{s}) \log \frac{\prod_k Q_k^{(n)}[p(x|s)]}{\prod_l P_l}\right)$$

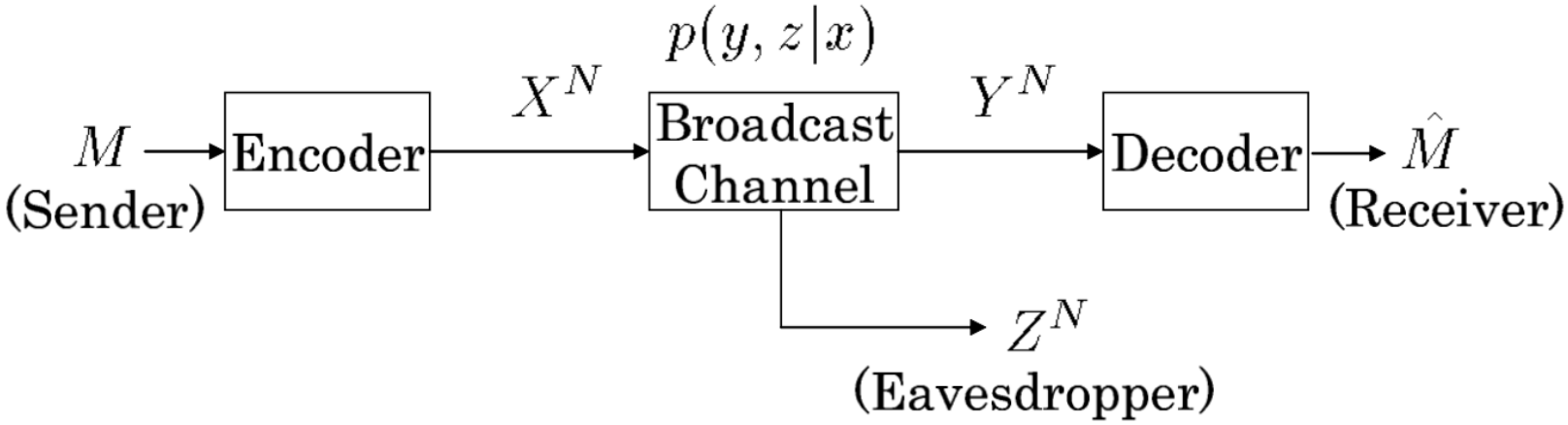
Key Point 4　単調に最適解に収束

この拡張有本-Blahut アルゴルズムもオリジナルのアルゴリズムと同様に，目的関数 $f(q, Q_1, \cdots Q_K)$ が $q^{(n)}(\boldsymbol{x}|\boldsymbol{s})$ に関して下に凸な関数の場合は，求めたい最適解 R^* に単調に収束することが示せる．この大域的収束性はこの問題が凸計画問題であることから KKT 条件などを用いて証明が可能となる．

拡張ABアルゴリズムの適用例（例１）

Çiszár らにより，Broadcast Channel において受信者の一方が盗聴者となる問題設定が提案.

メッセージ M の情報を盗聴者に一切漏らさない条件で，伝送可能な符号化レートの最大値を秘密保持容量 C_s と定義した．通信路 $P(y,z|x)$ を周辺化して得られる $P_1(y|x)$ と $P_2(z|x)$ をそれぞれ主通信路と盗聴通信路と定義し，主通信路が盗聴通信路に比べて less noisy な場合の秘密保持容量を以下のように導出.

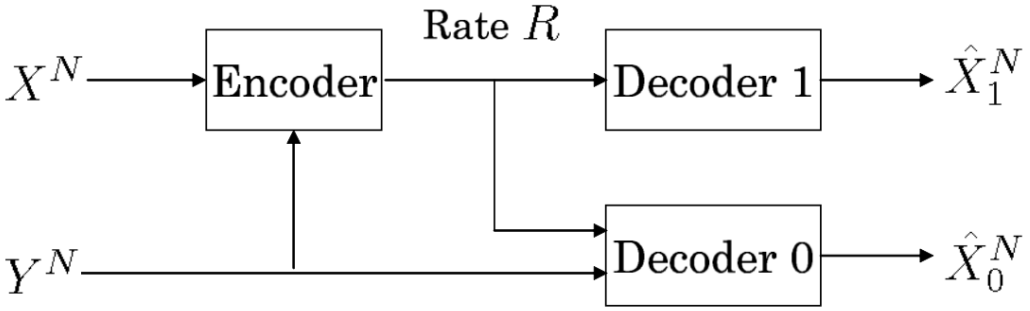


$$C_s = \max_{q(x)\in\mathcal{Q}} (I(X;Y) - I(X;Z)).$$

Less noisyの場合，凸性が示されている[van Dijk 1997}

拡張ABアルゴリズムの適用例（例２）

Kaspi により提案された，復号器が２つあり一方のみで補助情報が利用できる多端子モデルにおけるレート歪み関数



$$R(D_1, D_0) = \min_{q \in \mathcal{Q}(D_1, D_0)} (I(X, Y; \hat{X}_1) - I(X; \hat{X}_0 | Y, \hat{X}_1)).$$

$$\begin{aligned}\mathcal{Q}((D_1, D_0) \quad = \quad & \{q : \sum_{\hat{x}_1, \hat{x}_0} q(\hat{x}_1, \hat{x}_0 | x, y) = 1, q(\hat{x}_1, \hat{x}_0 | x, y) \geq 0, \\ & \sum_{x,y,\hat{x}_1,\hat{x}_0} p(x, y) q(\hat{x}_1, \hat{x}_0 | x, y) d_1(x, \hat{x}_1) \leq D_1 \\ & \sum_{x,y,\hat{x}_1,\hat{x}_0} p(x, y) q(\hat{x}_1, \hat{x}_0 | x, y) d_1(x, \hat{x}_0) \leq D_0\}.\end{aligned}$$

凸性が示されている
[Yasui,Matsushima 2007}

拡張ABアルゴリズムの数値実験例（例１）

$$C_s = -\min_{q(x)\in\mathcal{Q}} \sum_{x,y,z} q(x)P(y,z|x)\log\frac{q(x)P_2(z|x)}{Q_1[p(x)]Q_2[p(x)]},$$

$$\begin{aligned} Q_1[p(x)] &= \frac{p(x)P_1(y|x)}{\sum_x p(x)P_1(y|x)}, \\ Q_2[p(x)] &= \sum_x p(x)P_2(z|x). \end{aligned}$$

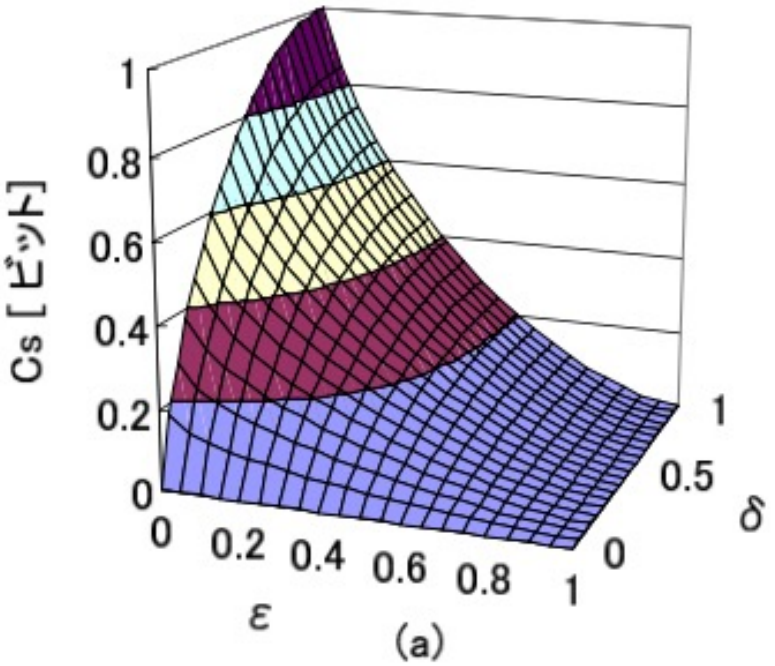
実験条件として，次のような通信路を仮定する．

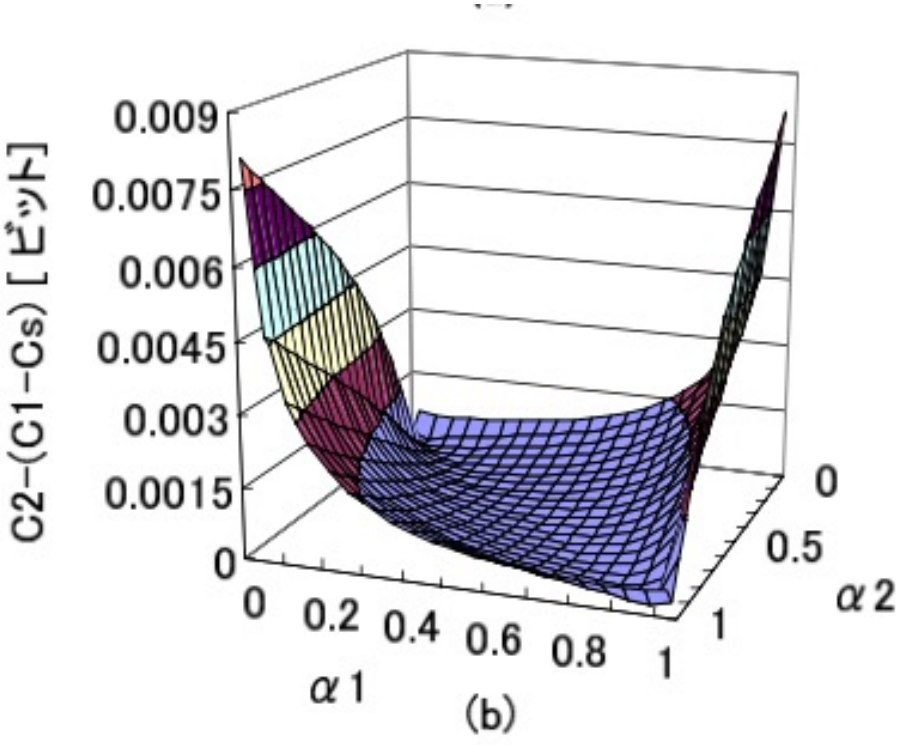
$$\boldsymbol{P}_1 = \begin{pmatrix} 1-\alpha_1\epsilon & \alpha_1\epsilon \\ (1-\alpha_1)\epsilon & 1-(1-\alpha_1)\epsilon \end{pmatrix},$$

$$\boldsymbol{P}_d = \begin{pmatrix} 1-\alpha_2\delta & \alpha_2\delta \\ (1-\alpha_2)\delta & 1-(1-\alpha_2)\delta \end{pmatrix},$$

但し，$\boldsymbol{P}_1$ を主通信路 $p_1(y|x)$ の遷移確率行列，$\boldsymbol{P}_d$ を $p_d(z|y)$ の遷移確率行列とし，α_i $(0\leqq\alpha_i\leqq 1,\ i=1,2)$ は各々の通信路の非対称性を決定するパラメータ，

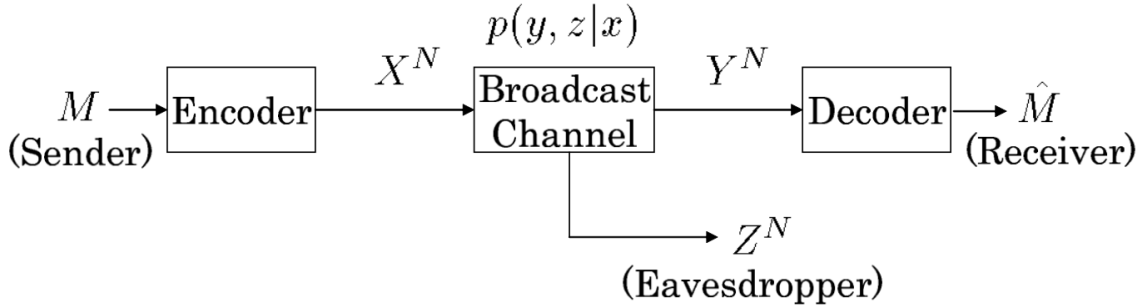
拡張ABアルゴリズムの数値実験例（例１）





$$C_2 - (C_1 - C_s)$$

目的関数が凸関数でない場合への拡張



$$C_s = \max_{q(x)\in\mathcal{Q}} (I(X;Y) - I(X;Z)).$$

例１は秘密保持容量の式は主通信路が盗聴通信路に比べて less noisyの場合だけでなく，more-capableな場合にも成り立つが，一般的には凸関数の最適化の問題にならない.

Definition 1 (more capable): The legitimate user's channel $X \to Y$ is said to be more-capable than the eavesdropper's channel $X \to Z$ if for any distribution $q(x)$, $I(X;Y) \geq I(X;Z)$.

Definition 2 (less noisy): The legitimate user's channel $X \to Y$ is said to be less-noisy than the eavesdropper's channel $X \to Z$ if for any Markov chain $V \to X \to YZ$, $I(V;Y) \geq I(V;Z)$.

目的関数が凸関数でない場合への拡張

例１は秘密保持容量の式は主通信路が盗聴通信路に比べて less noisyの場合だけでなく，more-capableな場合にも成り立つが，一般的には凸関数の最適化の問題にならない.

Degraded Broadcast Channelの場合の通信路容量領域についても一般的には凸関数の最適化の問題にならない.

これらの問題についても，この拡張ABアルゴルズムは適用可能であるが，上記の理由から大域的収束性は一般には保証されない.

ただし，初期値に関するある仮定をおくことで，最適解への収束を保証する研究もおこなわれている.

まとめ

通信路符号化における通信路容量と
有歪み情報源符号化におけるレート歪み関数の
効率良い繰り返し計算法である

有本-Blahutアルゴリズムの優れた性質を生かした

多端子モデルの問題に向けた拡張アルゴリズムについて解説をおこなった.