情報理論研究の広がりと面白さ

山本博資

東京大学　新領域創成科学研究科
早稲田大学　基幹理工学研究科
中央大学　研究開発機構
明治大学　研究・知財戦略機構

2021年度功績賞

作 品 の 意 図

青 柳 均 衛

人間の明日への夢をゆだねられて
飛翔する
電子「通信」と人間の関係を心の核
として
無限の旗手ともいうべき女児を流
動的に宇宙に浮遊させ
無意識な洋風追随におちいらぬよ
う 風土から生れた表現にそって人
間が叡智と愛の花冠を永遠に見失う
ことなくあれかしとの想いを底に爽
やかな作風をとりました

今までに行った研究を通じて，情報理論の広がりとその面白さを紹介する.

共同研究者およびサポートを頂いた全ての方に
深く感謝致します.

今までに行った情報理論の研究テーマ

誤り訂正符号・誤り制御方式

フィードバック通信方式および理論（無雑音フィードバック，有雑音フィードバック）

その他（TCM，LDPC符号，Polar符号など）

データ圧縮符号

ユニバーサル符号，正整数のユニバーサル符号，競合最適符号化

準瞬時符号，有歪み圧縮符号化

シャノン理論

マルチユーザ情報理論（セキュリティ問題無し）

マルチユーザ情報理論（セキュリティ問題有り，シャノン暗号システム，盗聴通信路符号化など）

その他（符号化定理，情報スペクトル理論，同定符号など）

情報セキュリティ

秘密分散法，視覚暗号，量子秘密分散法

複雑さ理論・乱数検定，その他

その他

機械学習，
ネットワーク符号化など

今までに行った情報理論の研究テーマ

誤り訂正符号・誤り制御方式

フィードバック通信方式および理論（無雑音フィードバック，有雑音フィードバック）

その他（TCM，LDPC符号，Polar符号など）

データ圧縮符号

ユニバーサル符号，正整数のユニバーサル符号

準瞬時符号，有歪み圧縮符号化

シャノン理論

マルチユーザ情報理論（セキュリティ問題無し）

マルチユーザ情報理論（セキュリティ問題有り，シャノン暗号システム，盗聴通信路符号化など）

その他（符号化定理，情報スペクトル理論，同定符号など）

SITA2018特別講演

秘密情報の符号化

情報セキュリティ

秘密分散法，視覚暗号，量子秘密分散法

複雑さ理論・乱数検定，その他

その他

機械学習，
ネットワーク符号化など

今までに行った情報理論の研究テーマ

誤り訂正符号・誤り制御方式

フィードバック通信方式および理論（無雑音フィードバック，有雑音フィードバック）

その他（TCM，LDPC符号，Polar符号な

データ圧縮符号

ユニバーサル符号，正整数のユニバ

準瞬時符号，有歪み圧縮符号化

シャノン理論

マルチユーザ情報理論（セキュリティ

マルチユーザ情報理論（セキュリティ
盗聴通信路

その他（符号化定理，情報スペクトル

情報セキュリティ

秘密分散法，視覚暗号，量子秘密分散法

複雑さ理論・乱数検定，その他

ISITA2014 Plenary Talk

Topics in FV and VF source coding

2017年11月情報理論研究会
若手研究者のための講演会

準瞬時FV符号とその拡張符号

電子情報通信学会誌 解説
（vol.104, no.1, pp.35−42, 2021年1月）

準瞬時FV符号
−ハフマン符号に勝る圧縮率を達成する符号−

機械学習，
ネットワーク符号化など

今までに行った情報理論の研究テーマ　本講演出取り扱う内容

誤り訂正符号・誤り制御方式

フィードバック通信方式および理論（無雑音フィードバック，有雑音フィードバック）

その他（TCM，LDPC符号，Polar符号など）

データ圧縮符号

ユニバーサル符号，正整数のユニバーサル符号，競合最適符号化

準瞬時符号，有歪み圧縮符号化

シャノン理論

マルチユーザ情報理論（セキュリティ問題無し）

マルチユーザ情報理論（セキュリティ問題有り，シャノン暗号システム，盗聴通信路符号化など）

その他（符号化定理，情報スペクトル理論，同定符号など）

情報セキュリティ

秘密分散法，視覚暗号，量子秘密分散法

複雑さ理論・乱数検定，その他

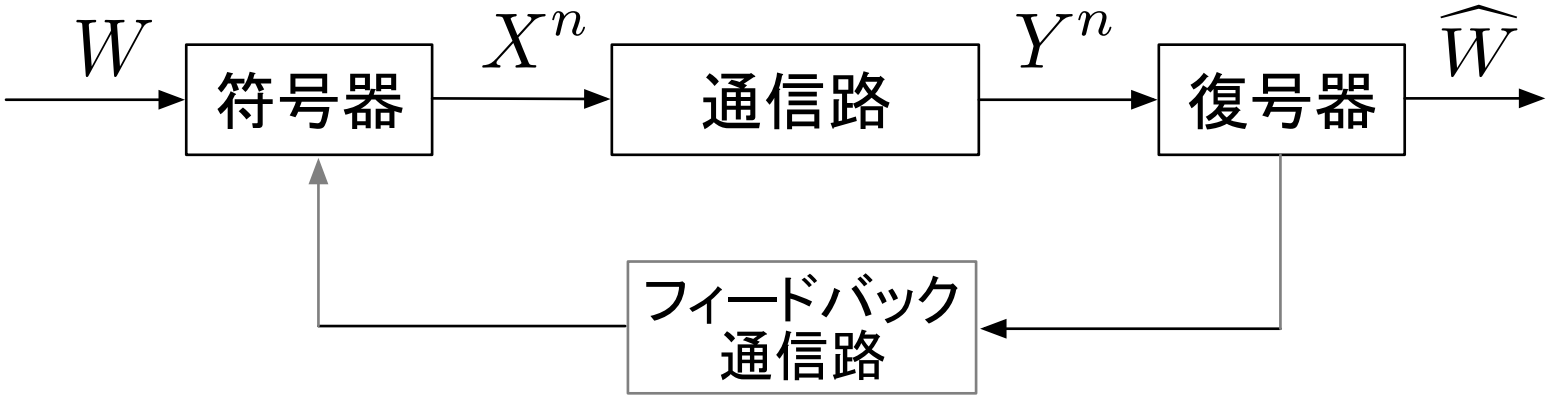
その他

機械学習，
ネットワーク符号化など

フィードバック通信方式

$W \in I_M = \{0, 1, \cdots, M-1\}$

情報の伝送は一方向のみ



符号化レート:

$$R = \frac{1}{n} \log_2 M$$

前向き通信路の通信路容量 C は増加しない. （C.E.Shannon, 1961）

信頼性関数（誤り指数）（Reliability function (Error exponent)）$E(R)$を大きく改善できる.

復号誤り率: $P_e = \Pr\{\widehat{W} \neq W\}$

$$E(R) = \lim_{n \to \infty} \frac{-\log_2 P_e}{n}$$

$$P_e \approx 2^{-nE(R)}$$

無雑音フィードバック通信方式

1960年代，1970年代

宇宙開発

1957年：初の人工衛星(スプートニク1号)

1958年：初の通信衛星(スコアー計画)

1959年：初の気象衛星(ヴァンガード2号)
初の月の裏側撮影(ルナ3号)

1960年：初の偵察衛星(GRAB-1)

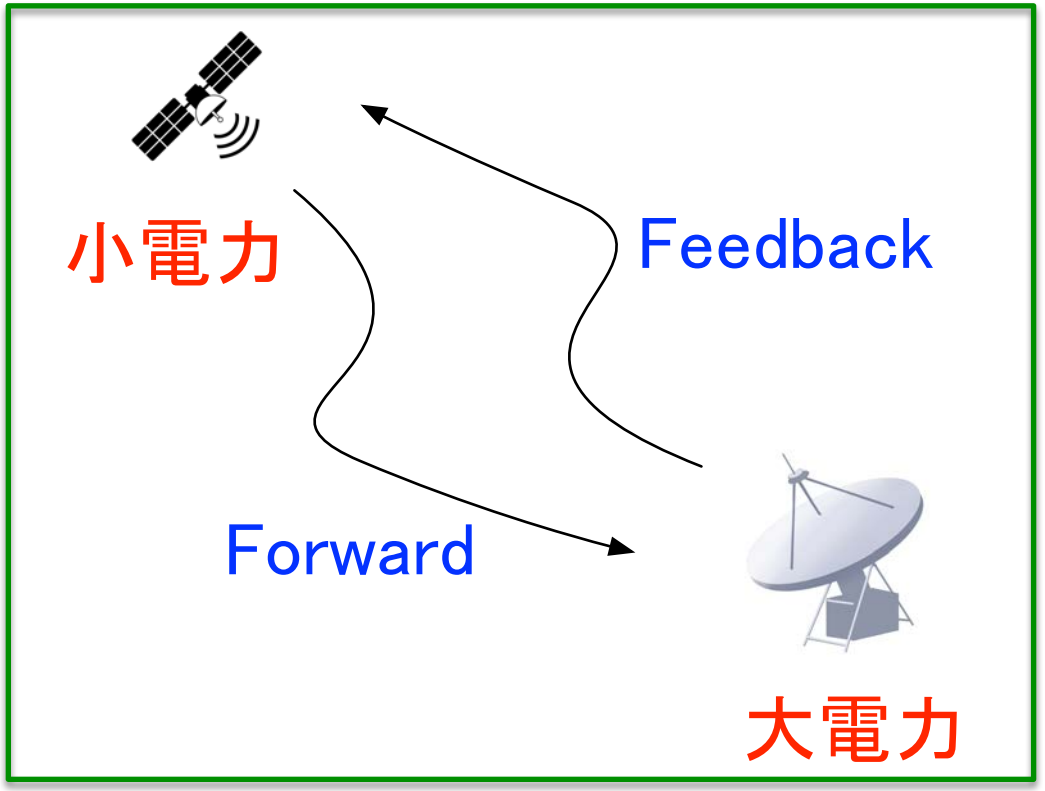
1962年：初の金星近傍通過(マリーナ2号)

1964年：初の静止通信衛星(シンコム3号)

1961年～1972年：アポロ計画

1966年：月面軟着陸（サーベイヤー1号）

1969年：人類の月面軟着陸帰還（アポロ11号）



無雑音フィードバック仮定の正当性

前向き通信路に比べてフィードバック通信路のSNRが非常に大きい

無雑音フィードバック通信方式

1960年代

IEEE Information Theory Society Paper Award

1967年受賞

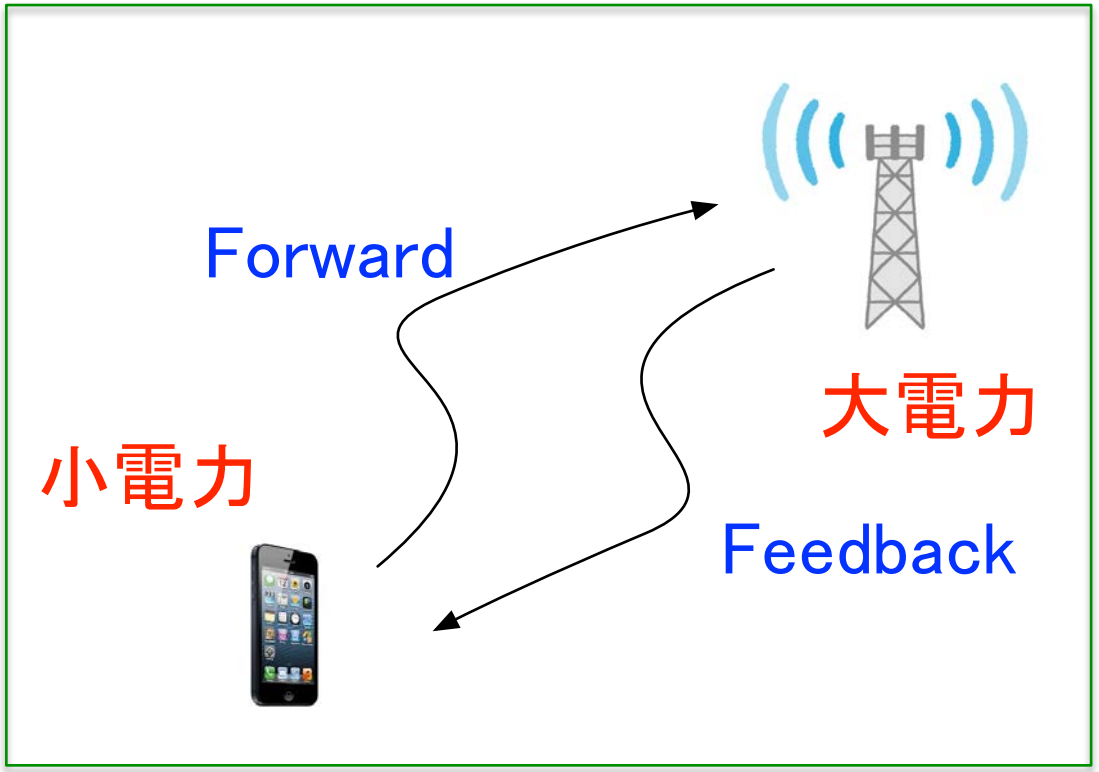
J.P.M.Schalkwijk and T.Kailath,
“A coding scheme for additive noise channels with feedback -I: No bandwidth constraint,” IEEE Trans. on Information Theory, April 1966

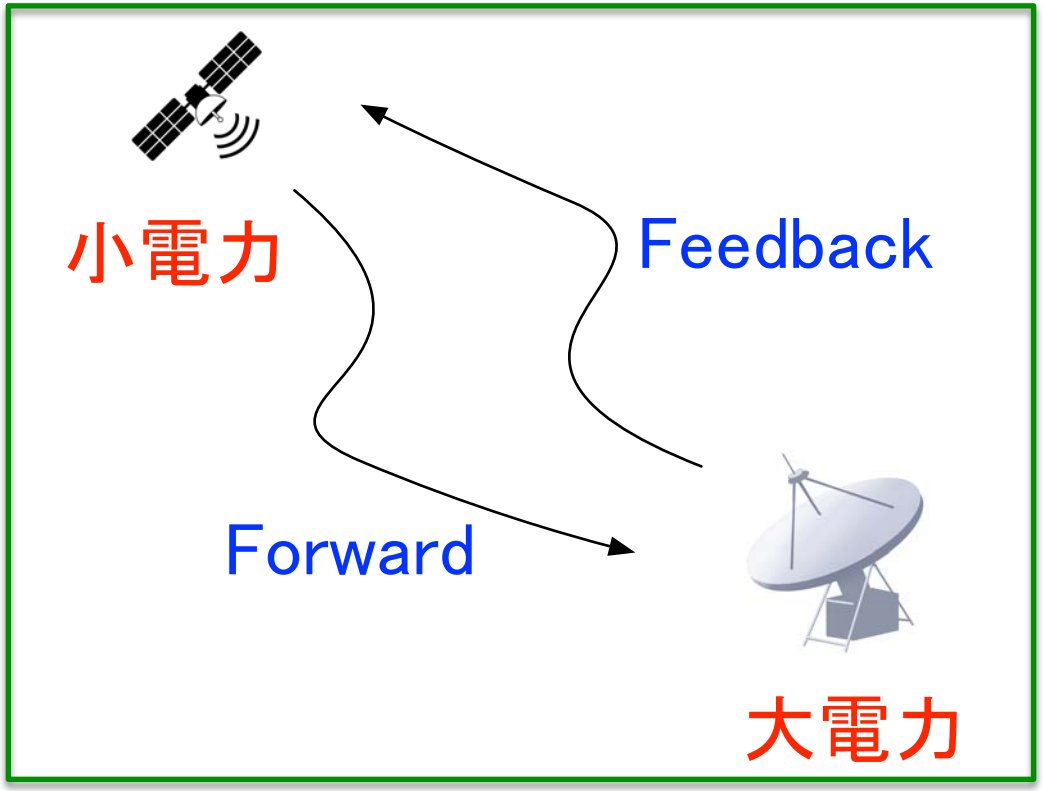
1970年受賞

G. D. Forney,
“Exponential error bounds for erasure, list, and decision feedback schemes,” IEEE Trans. on Information Theory, March 1968

無雑音フィードバック通信方式

1990年代以降：携帯電話によるデジタル通信





無雑音フィードバック仮定の正当性

前向き通信路に比べてフィードバック通信路のSNRが非常に大きい

無雑音フィードバック通信方式

H.Yamamoto and K.Itoh,
“Asymptotic performance of a modified Schalkwijk-Barron scheme for channels with noiseless feedback,” IEEE Trans. on Information Theory, Nov. 1979

Yamamoto-Itoh scheme

H.Yamamoto and K.Itoh,
“Viterbi decoding algorithm for convolutional codes with repeat request,”
IEEE Trans. on Information Theory, Sep. 1980

Yamamoto-Itoh algorithm

無雑音フィードバック通信方式

AWGNC（加法的白色雑音通信路，帯域制限無し）

S：平均電力，N：雑音電力密度，T：送信時間，C：通信路容量，R：符号化レート

$$C = \frac{S}{N} \qquad R = \frac{\ln M}{T} \qquad \text{(nats/秒)}$$

Schalkwijk-Kailath (1966)

復号誤り率：$P_e = \exp\left\{-\frac{3C}{2R}\exp[2(C-R)T] + o(T)\right\}$

Kramer (1969)

復号誤り率：$P_e = \exp\left\{-\underbrace{\exp\left[\cdots\exp}_{N-1\text{回}}\left[T\left(\frac{C}{2}-R\right)\right]\cdots\right] + RT + o(T)\right\}$

欠点：ピークパワーも指数的に大きくなる．フィードバックする情報が実数値

Schalkwijk-Barron (1971)

復号誤り率：$P_e = \exp\left\{-T\left(\sqrt{\alpha C - R} + \sqrt{C-R}\right)^2 + o(T)\right\}$ $\qquad \alpha = \dfrac{\text{Peak power}}{\text{Average power}}$

ピークパワー制限の下で最も大きな誤り指数

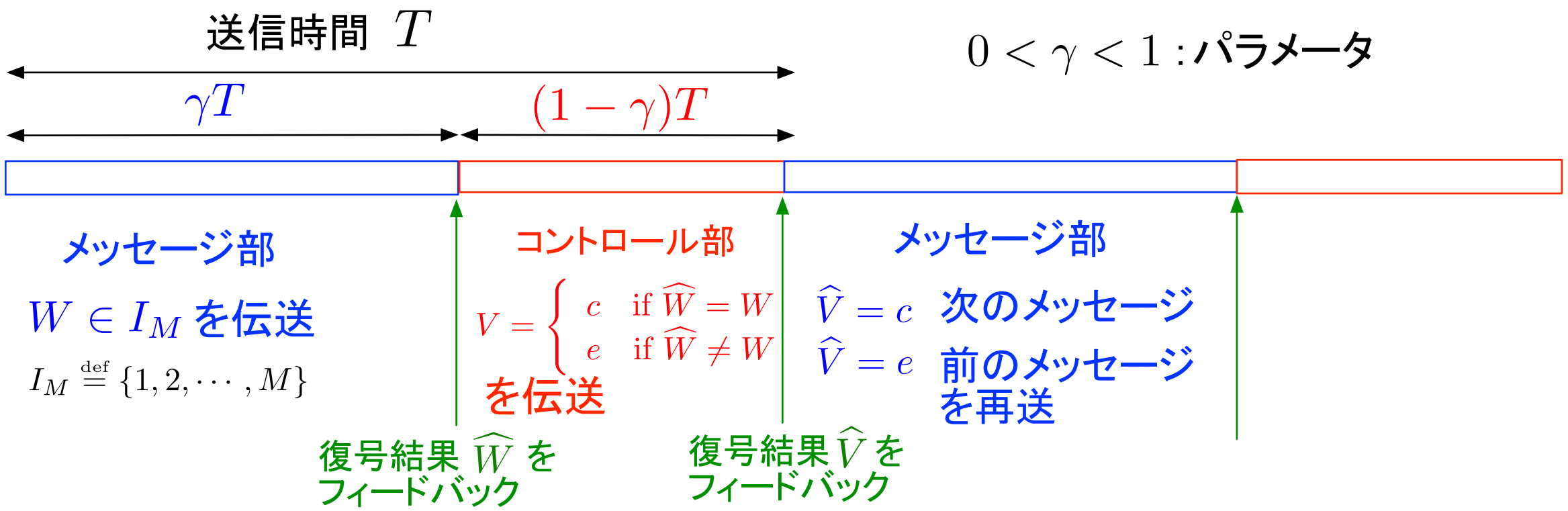
Schalkwijk-Barron (1971)

復号誤り率: $P_e = \exp\left\{-T\left(\sqrt{\alpha C - R} + \sqrt{C-R}\right)^2 + o(T)\right\}$

$$\alpha = \frac{\text{Peak power}}{\text{Average power}}$$

送信時間 T

$0 < \gamma < 1$: パラメータ



Sequential decision feedback

$\pm s(t)$ を送信

復号器: $\log \frac{P_+}{P_-}$ がスレショールドを超えたところで,

c or e をフィードバック

欠点:

コントロール部が可変長

フィードバック情報は2値と言えない

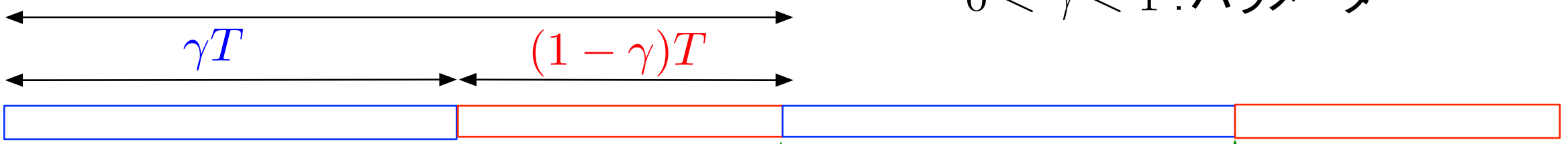
Yamamoto-Itoh (1979)

復号誤り率: $P_e = \exp\left\{-T\left(\sqrt{\alpha C - R} + \sqrt{C - R}\right)^2 + o(T)\right\}$

$$\alpha = \frac{\text{Peak power}}{\text{Average power}}$$

送信時間 T

$0 < \gamma < 1$: パラメータ



メッセージ部

$W \in I_M$ を伝送

$I_M \stackrel{\text{def}}{=} \{1, 2, \cdots, M\}$

コントロール部

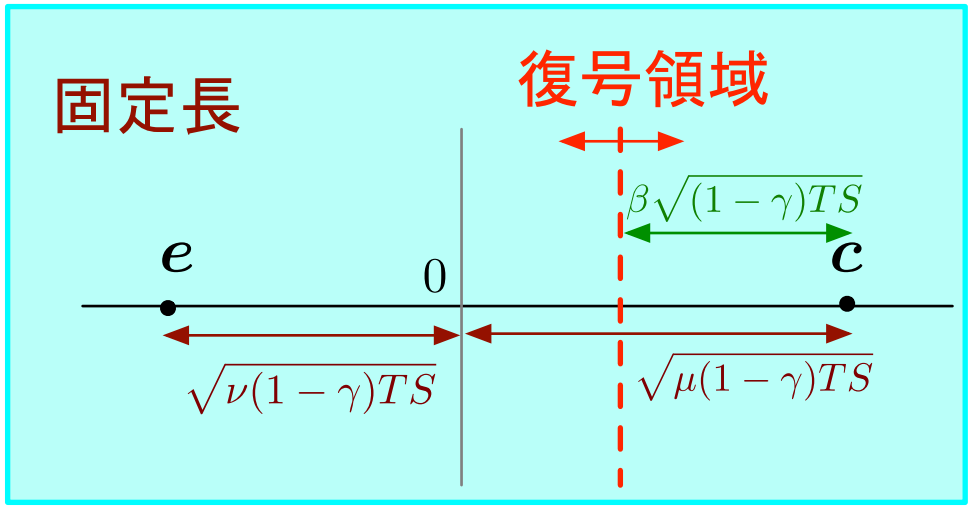
$$V = \begin{cases} c & \text{if } \widehat{W} = W \\ e & \text{if } \widehat{W} \neq W \end{cases}$$

を伝送

メッセージ部

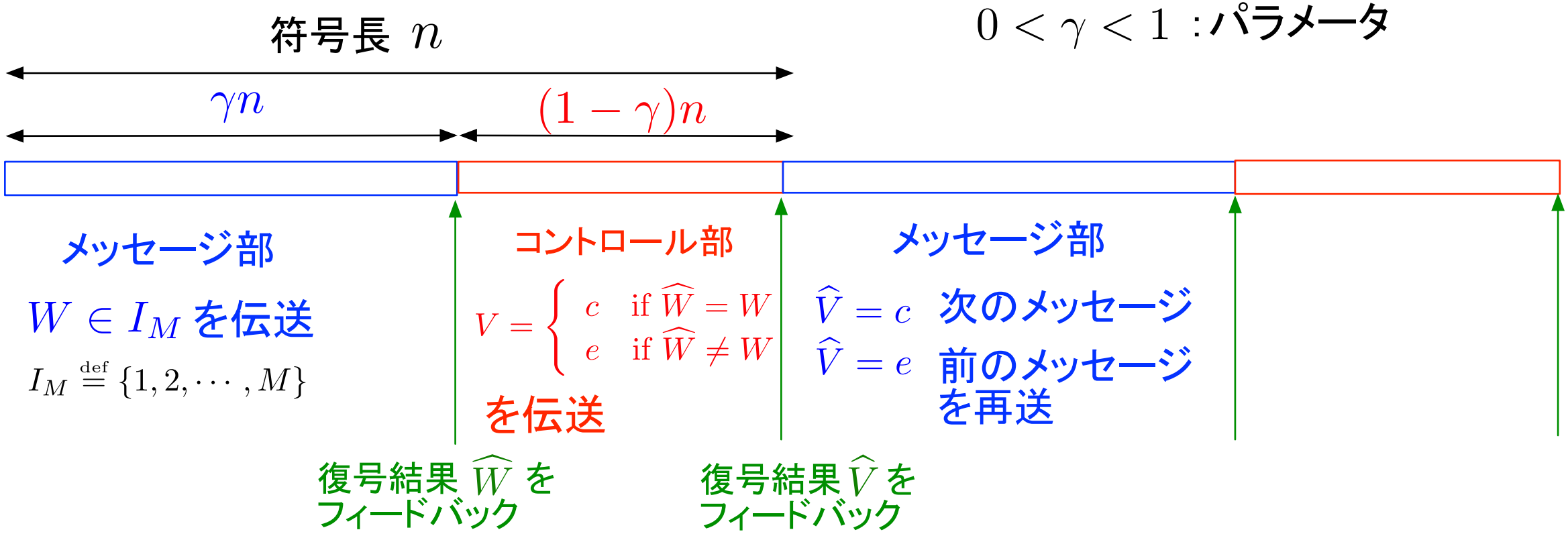
復号結果 $\widehat{W}$ を
フィードバック

復号結果 $\widehat{V}$ を
フィードバック



DMC(離散無記憶通信路)に
容易に拡張可能

Yamamoto-Itoh (1979)　DMCの場合：



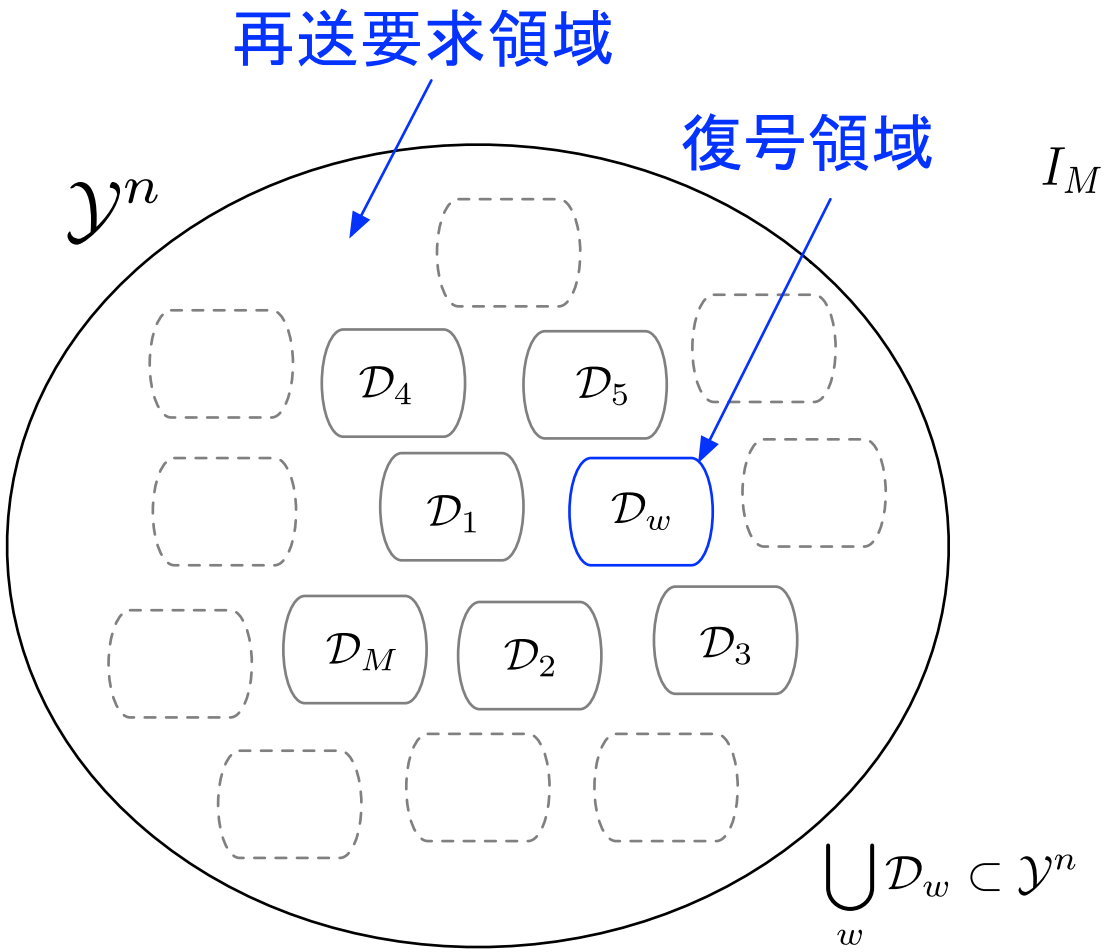
復号誤り率：$P_e = \exp\{-n[E_B(R) + o(n)]\}$

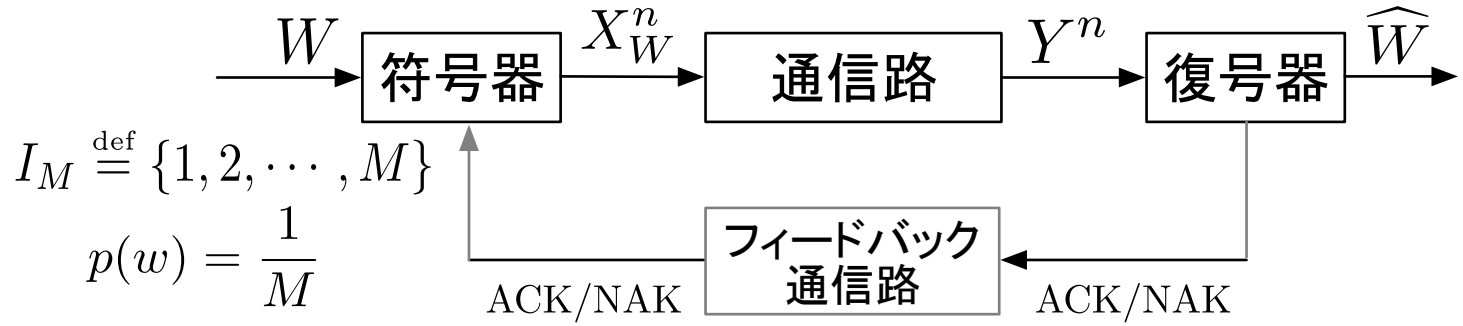
$$E_B(R) = \left(1 - \frac{R}{C}\right) \max_{x,x'} D(p_{Y|x} \| p_{Y|x'})$$　：Burnashevの誤り指数 (1976)

逆定理のsimple proof：　Berlin-Nakiboglu,-Telatar (2009)

無雑音フィードバック通信方式

Forney (1968)　DMC(離散無記憶通信路)に対するブロック符号を用いた Hybrid-ARQ (Auto Repeat Request)方式





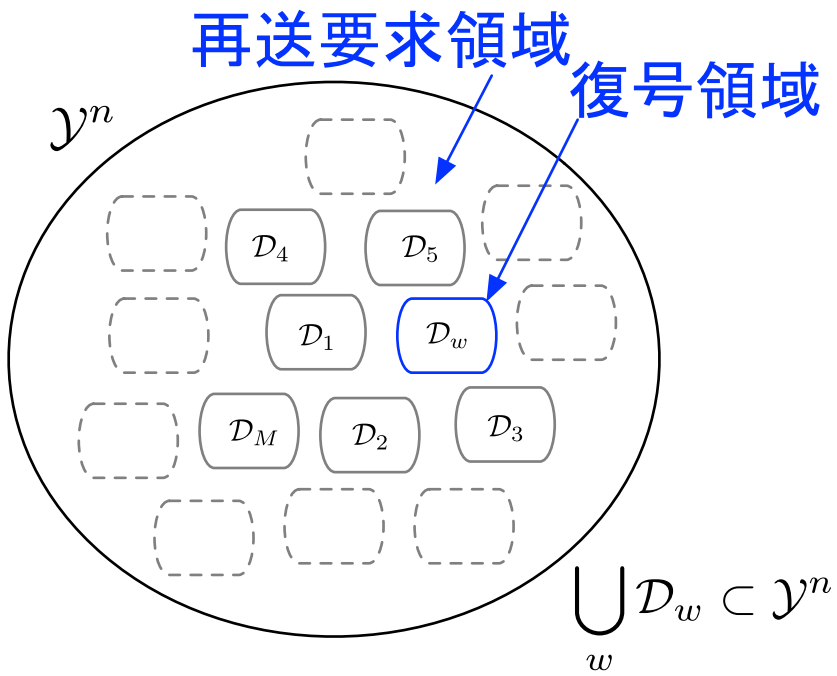
Forneyの復号領域

$$\mathcal{D}_w = \left\{ y^n : \frac{p(y^n|x_w^n)}{\sum_{w' \neq w} p(y^n|x_{w'}^n)} \geq \mathrm{e}^{nT} \right\}$$

T : パラメータ

無雑音フィードバック通信方式

Forney (1968)　DMC(離散無記憶通信路)に対するブロック符号を用いた Hybrid-ARQ (Auto Repeat Request)方式



Forneyの復号領域

$$\mathcal{D}_w = \left\{ y^n : \frac{p(y^n|x_w^n)}{\sum_{w' \neq w} p(y^n|x_{w'}^n)} \geq \mathrm{e}^{nT} \right\}$$

T : パラメータ

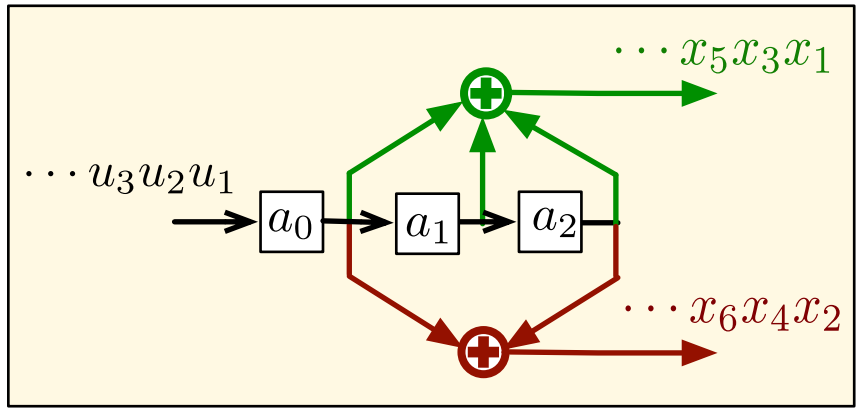
$\mathcal{D}_w$ の境界では，最も近い $x_{w'}^n$ が大きく影響する．

$$\widetilde{\mathcal{D}}_w = \left\{ y^n : \frac{p(y^n|x_w^n)}{\max_{w' \neq w} p(y^n|x_{w'}^n)} \geq \mathrm{e}^{nT} \right\}$$

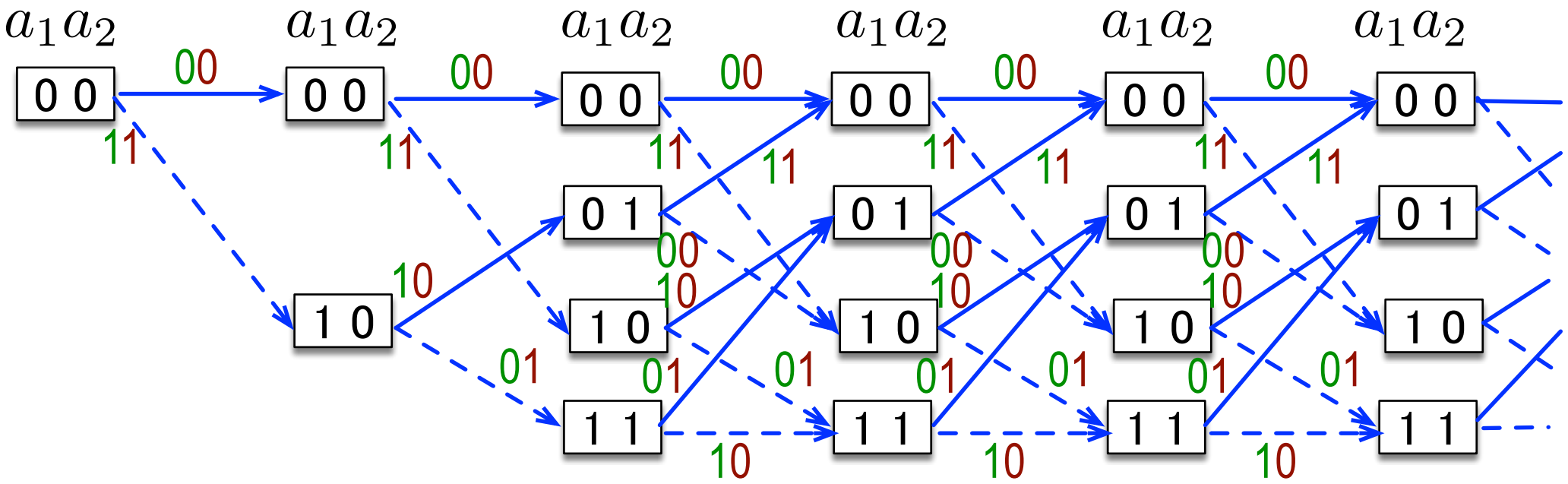
$$= \left\{ y^n : \ln p(y^n|x_w^n) - \max_{w' \neq w} \ln p(y^n|x_{w'}^n) \geq T \right\}$$

無雑音フィードバック通信方式

Yamamoto-Itoh (1980)　DMC(離散無記憶通信路)に対する畳み込み符号を用いた Hybrid-ARQ (Auto Repeat Request)方式



トレリス図

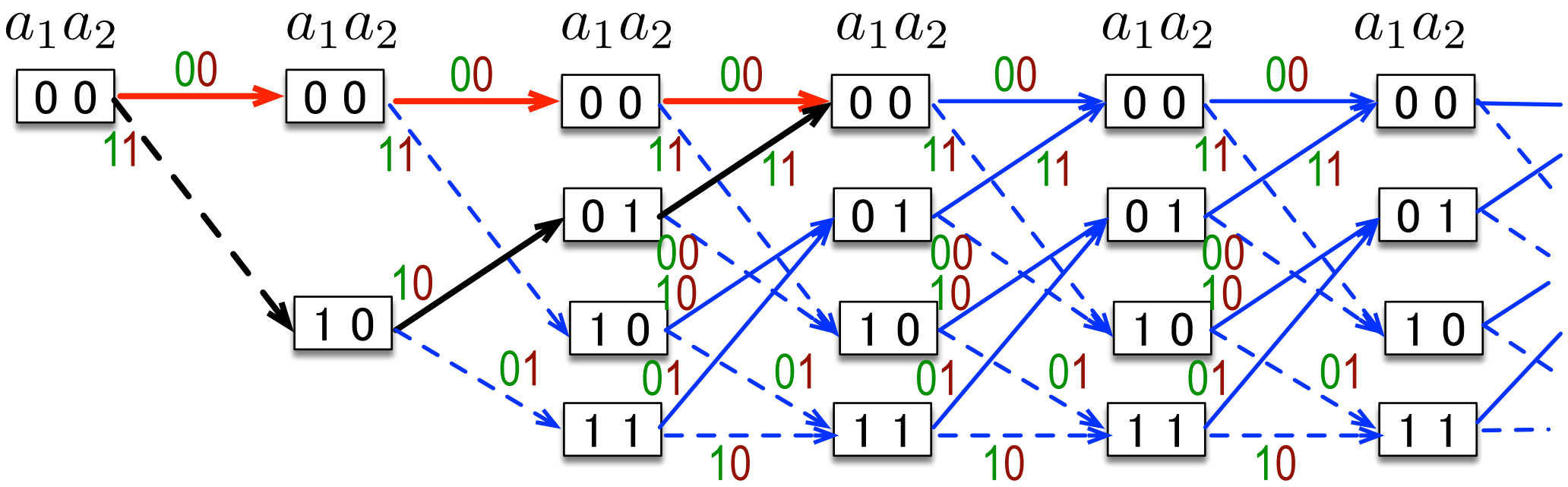


無雑音フィードバック通信方式

Viterbi復号(最尤復号法)

大きい方が生き残る

$$\begin{cases} \ln p(y^n|x^n) \\ \ln p(y^n|\tilde{x}^n) \end{cases}$$



無雑音フィードバック通信方式

YI−Algorithm

大きい方が生き残る

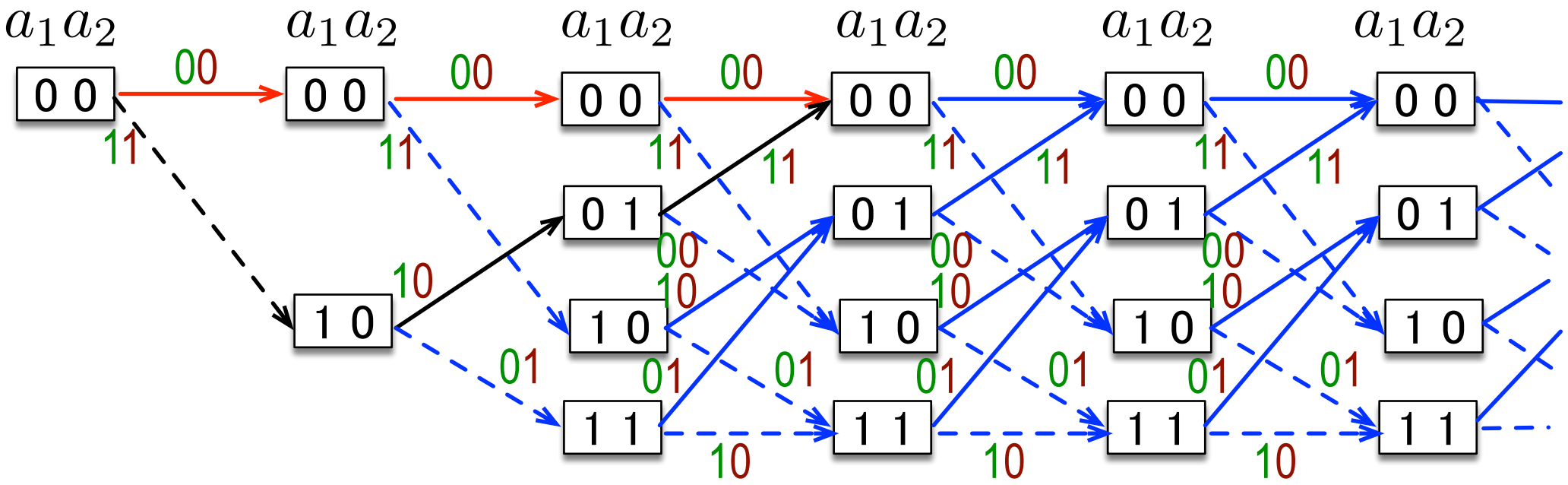
$$\begin{cases} \ln p(y^n|x^n) \\ \ln p(y^n|\tilde{x}^n) \end{cases}$$

Forneyの復号領域の近似

$$\widetilde{\mathcal{D}}_w = \left\{ y^n : \ln p(y^n|x_w^n) - \max_{w' \neq w} \ln p(y^n|x_{w'}^n) \geq T \right\}$$

$\ln p(y^n|x^n) - \ln p(y^n|\tilde{x}^n) < T$ ⟶ ×印生き残りパス

全ての生き残りパスが×印 ⟶ 再送要求



KeyStone Architecture
Viterbi Coprocessor (VCP2)

User Guide

Literature Number: SPRUGV6A
June 2011

Chapter 2

Architecture 2-1

Table 3-5 VCP2 Input Configuration Register 1 (VCPIC1) Field Descriptions

Bit	Field	Value	Description
31-29	Reserved	0	Reserved. The reserved bit location is always read as 0. A value written to this field has no effect.
28	YAMEN		Yamamoto algorithm enable bit. See Section 2.3.
		0	Yamamoto algorithm is disabled.
		1	Yamamoto algorithm is enabled.
27-16	YAMT	0-FFFh	Yamamoto threshold value bits. See Section 2.3.
15-0	Reserved	0	Reserved. These reserved bit locations must be 0. A value written to this field has no effect.
End of Table 3-5			

Table 3-11 VCP2 Output Register 1 (VCPOUT1) Field Descriptions

Bit	Field	Value	Description
31-17	Reserved	0	Reserved. The reserved bit location is always read as 0. A value written to this field has no effect.
16	YAM		Yamamoto bit result. This bit is a quality indicator bit and is only used if the Yamamoto logic is enabled. See Section 2.3.
		0	At least one trellis stage had an absolute difference less than the Yamamoto threshold and the decided frame has poor quality
		1	No trellis stage had an absolute difference less than the Yamamoto threshold and the frame has good quality.
15-8	Reserved	0	Reserved. The reserved bit location is always read as 0. A value written to this field has no effect.
7-0	FMAXI	0-FFFh	State index for the state with the final maximum state metric. There are $2^{(k-1)}$ state metrics for each trellis stage. Valid range for FMAXI is 0 to $2^{(k-1)}$ -1.
End of Table 3-11			

有雑音フィードバック

Burnashev-Yamamoto, Problems of Information Transmission

BSC (2008, 2010), AWGNC (2012, 2014)

Sato-Yamamoto, ISITA2010

Yamamoto-Itoh scheme

Kim-Lapidoth-Weiseman, IEEE Transactions on Information Theory (March 2011)

AWGNC

アイデアを出せば，新しい面白い結果を出せる可能性が残っている.

マルチユーザ情報理論

1970年代

多重アクセス通信路 (Ahlswede, 1971)

中継通信路 (van der Meulen, 1971)

IEEE Information Theory Society Paper Award

放送通信路 (Cover, 1972) ⇐ 1973年受賞

干渉通信路 (Ahlswed, 1974)

Slepian-Wolf System (Slepian-Wolf, 1973) ⇐ 1975年受賞

Wyner—Ziv System (Wyner-Ziv, 1976) ⇐ 1977年受賞

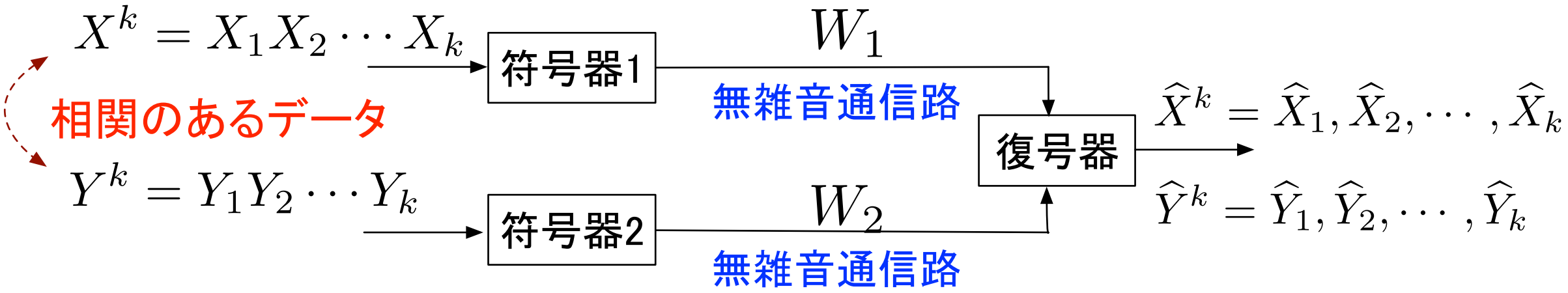
日本：インフォメーション理論研究会：1953年9月～1971年12月

（情報理論研究の暗黒時代：1972年～1977年）

情報理論とその応用シンポジウム(SITA)：1978年～

情報理論研究会：1981年11月～

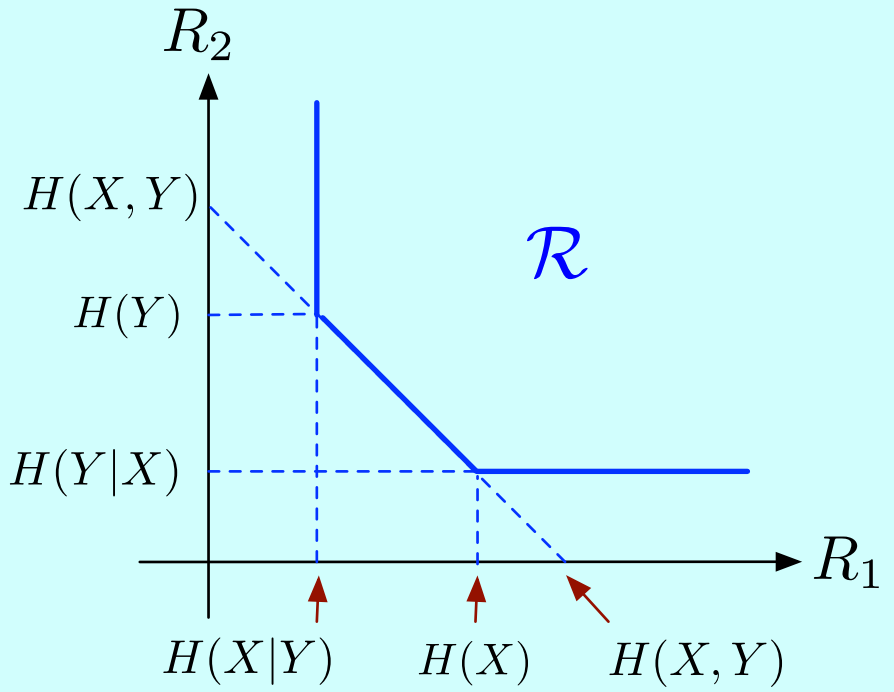
Slepian-Wolf System (Slepian-Wolf, 1973) (Cover, 1975)



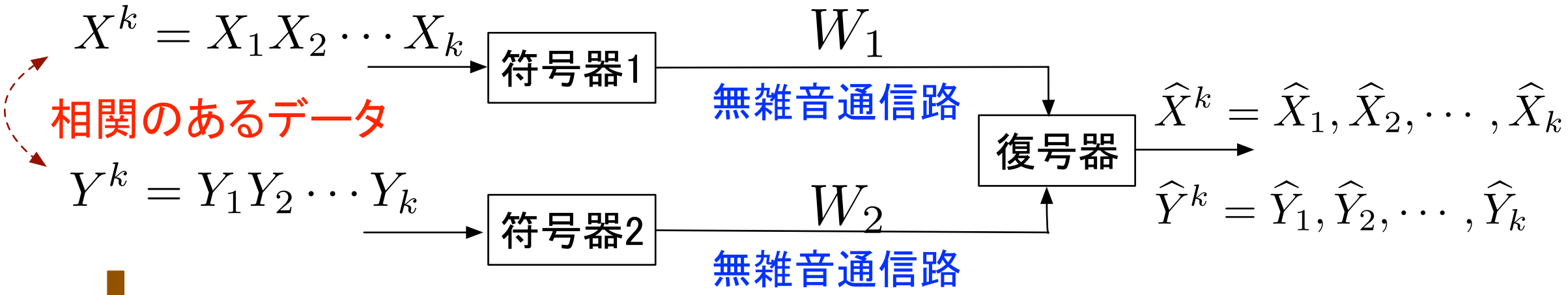
$$W_j \in I_{M_j} = \{1, 2, \cdots, M_j\}$$

符号化レート: $R_j = \dfrac{\log M_j}{n}$

達成可能領域: $\mathcal{R} = \{(R_1, R_2) : R_1 \geq H(X|Y),$
$R_2 \geq H(Y|X),$
$R_1 + R_2 \geq H(X,Y)\}$



Slepian-Wolf System (Slepian-Wolf, 1973) (Cover, 1975)



歪みを許す場合への拡張

Berger-Tung
Housewright-Omura
Wolfowitz

全員共著で
IEEE Transaction on Information Theory
vol.IT-25, no.6, Nov. 1979

山本，電子情報通信学会総合大会（1979年3月）

昭和54年度電子通信学会総合全国大会

1170 相関情報源と2つの独立な符号器を有する通信システムに対する情報源符号化定理

山本博資 （東京大学 宇宙航空研究所）

1. はじめに

元来、情報源符号化に関する理論は単一送信、単一受信の通信システムを対象として発展してきており、多くの成果が得られている。近年、その拡張として、簡単な通信網に対する情報源符号化理論の研究がなされている。[1][2][3] etc. 本稿ではその1つとして 図1のようなシステムにおけるRate-distortion理論の情報源符号化定理が証明できたので報告する。

2. 対象とする通信システムについて

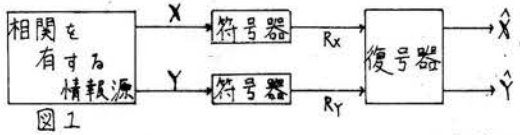


図1

$\hat{X}^n = F_{DX}(F_{EX}(X^n), F_{EY}(Y^n))$, $\hat{Y}^n = F_{DY}(F_{EX}(X^n), F_{EY}(Y^n))$ (10)

である。任意の $\varepsilon > 0$ に対して、n が十分大きな所で、

$$M_X \leq 2^{n(R_X+\varepsilon)} \qquad M_Y \leq 2^{n(R_Y+\varepsilon)} \qquad (11)$$

$$\Delta_X \leq d_X + \varepsilon \qquad \Delta_Y \leq d_Y + \varepsilon \qquad (12)$$

を満たす符号 $(n, M_X, M_Y, \Delta_X, \Delta_Y)$ が存在する時に伝送速度対 (R_X, R_Y) は ひずみ (d_X, d_Y) に対して、達成可能 (achievable) であると言う。(d_X, d_Y)-達成可能な速度対 (R_X, R_Y) の集合を $\mathcal{R}^*(d_X, d_Y)$ で表わすことにする。

3. 情報源符号化定理

この $\mathcal{R}^*(d_X, d_Y)$ の領域を、ある確率分布により定まる確率変数の相互情報量を用いて表わすことを考える。そのためには、まず次のような確率分布 $P(\xi_X, x, y, \xi_Y)$, $\xi_X \in \mathcal{Z}_X$, $x \in \mathcal{X}$, $y \in \mathcal{Y}$, $\xi_Y \in \mathcal{Z}_Y$ ($\mathcal{Z}_X, \mathcal{Z}_Y$ は任意の有限集合) を考え、$P(\xi_X, x, y, \xi_Y)$ が

を満たす関数 $f_X: \mathcal{Z}_X \times \mathcal{Y} \to \mathcal{X}$, $f_Y: \mathcal{Z}_X \times \mathcal{Y} \to \mathcal{Z}_Y$ が存在するような確率分布 $P(\xi_X, x, y, \xi_Y)$ の集合を $\mathcal{P}(d_X, d_Y)$ で表わす。ある1つの確率分布 $P(\xi_X, x, y, \xi_Y)$ に対して、図2のような領域 $R(P)$ を定義し、さらに、$\mathcal{R}(d_X, d_Y)$ を (17) 式で定義する。

$$\mathcal{R}(d_X, d_Y) = \left[\bigcup_{P(\cdot) \in \mathcal{P}(d_X, d_Y)} R(P)\right]^C \qquad (17)$$

ここで C は閉包 (closure) を示す。

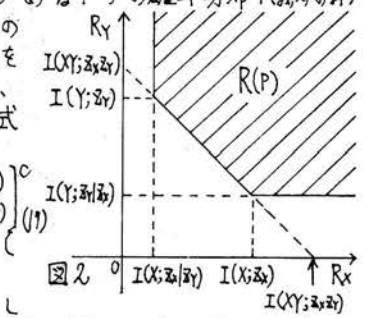


図2

上記で定義した $\mathcal{R}^*(d_X, d_Y)$, $\mathcal{R}(d_X, d_Y)$ に関して次の定理が成りたつことが証明できる。

定理（図1のシステムに対する源符号化定理）
$d_X \geq 0$, $d_Y \geq 0$ に対して、次式が成立する。

$$\mathcal{R}^*(d_X, d_Y) \supseteq \mathcal{R}(d_X, d_Y) \qquad (18)$$

参考文献

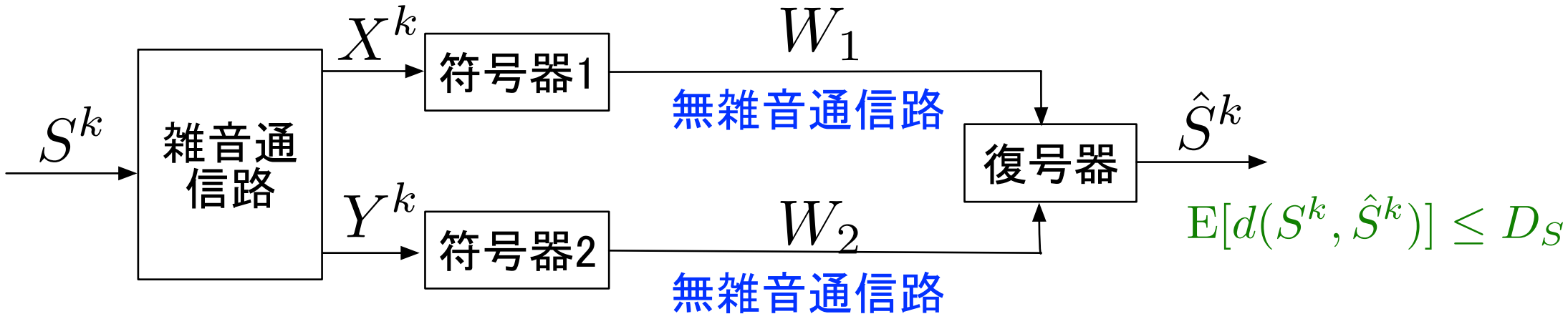
[1] D.Slepian & J.K.Wolf, IEEE Trans., vol.IT-19, pp.471-480 July 1971
[2] A.D.Wyner & J.Ziv, IEEE Trans., vol.IT-22, pp.1-10, Jan.1976
[3] R.M.Gray & A.D.Wyner, B.S.T.J., vol.53, pp.1681-1721, Nov. 1974

山本博資“相関情報源と2つの独立な符号器を有する通信システムに対する情報源符号化定理,”
昭和54年度電子情報通信学会総合大会予稿集, p. S-159, 1979年3月より抜粋

山本, 電子情報通信学会総合大会 (1979年3月)

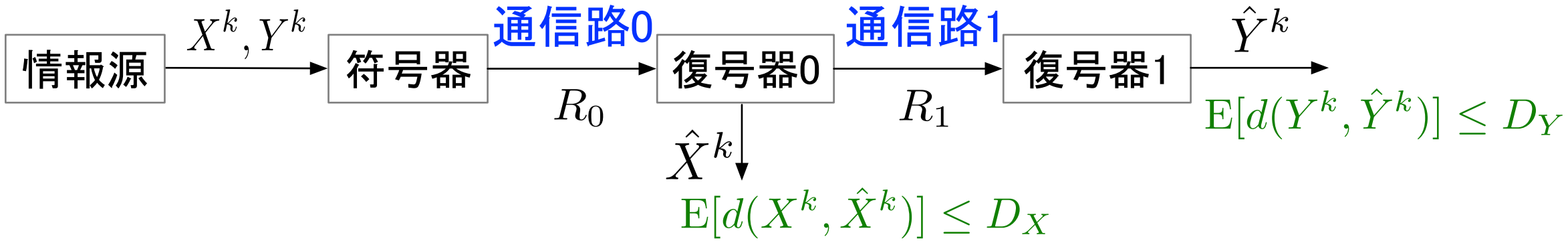
Remote Source, Correlated Observation, CEO Problem

Yamamoto-Itoh (Oct. 1980)

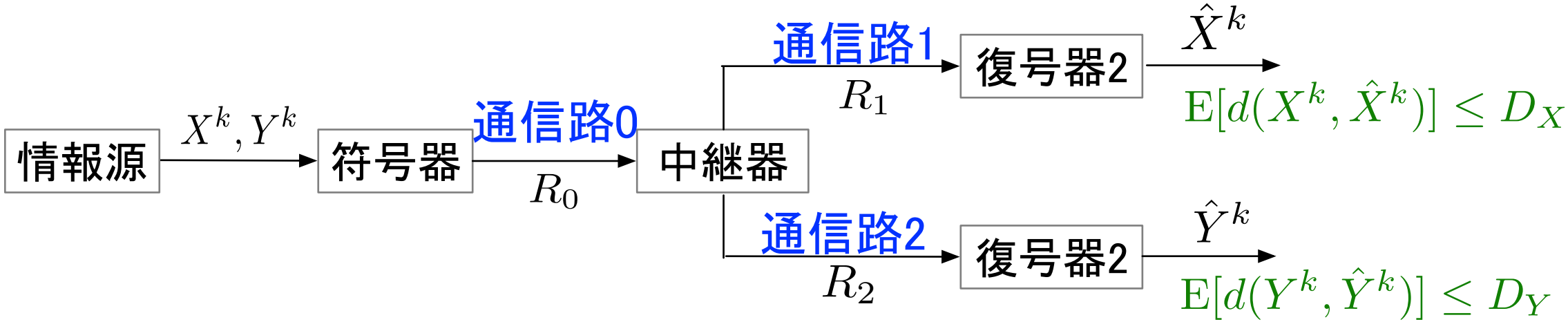


Multihop Communication System

Yamamoto (May 1981)

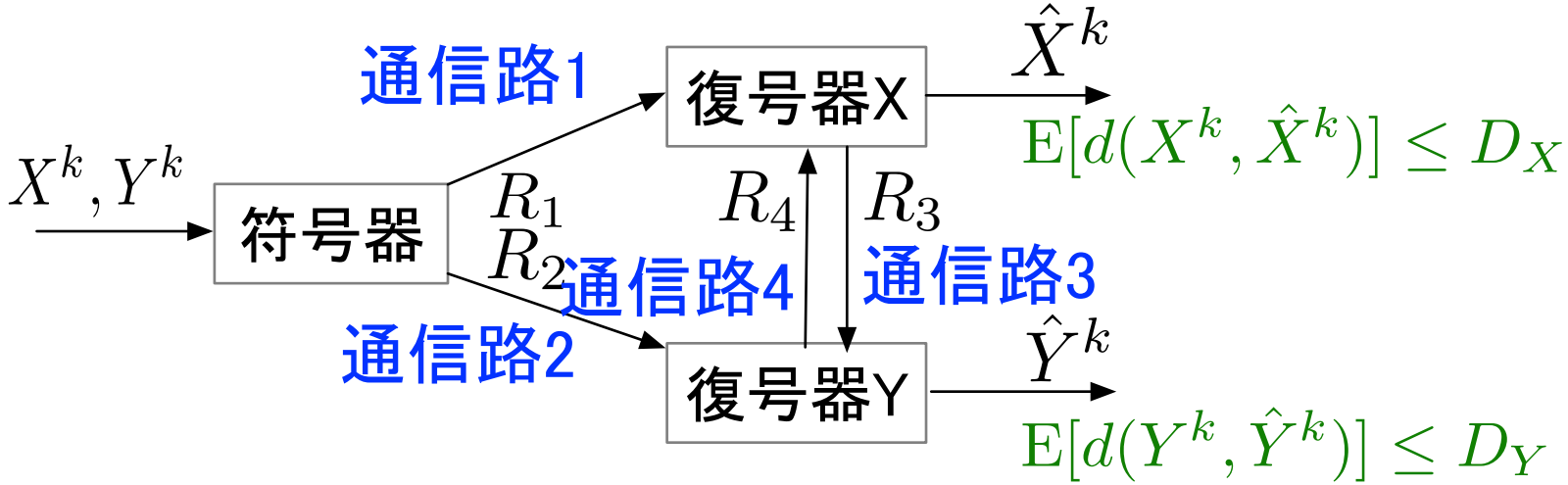


Branching Communication System　Yamamoto (May 1981)

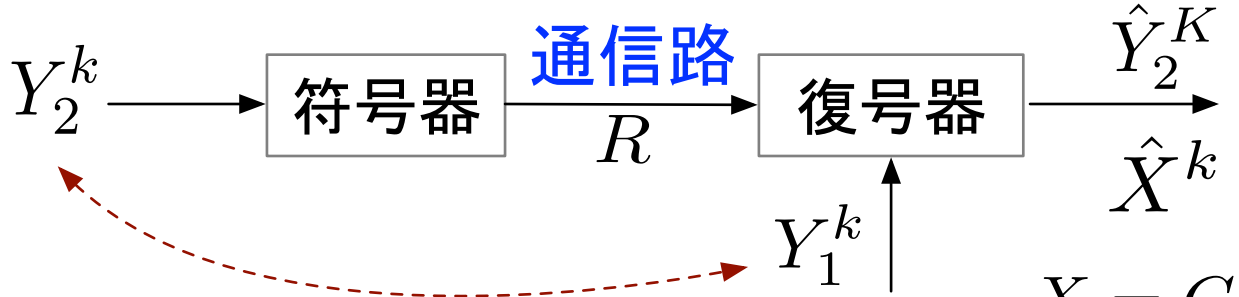


達成可能領域はOpen Problem

Triangular Communication System　Yamamoto (May 1996)



Wyner–Ziv System + 関数値復号

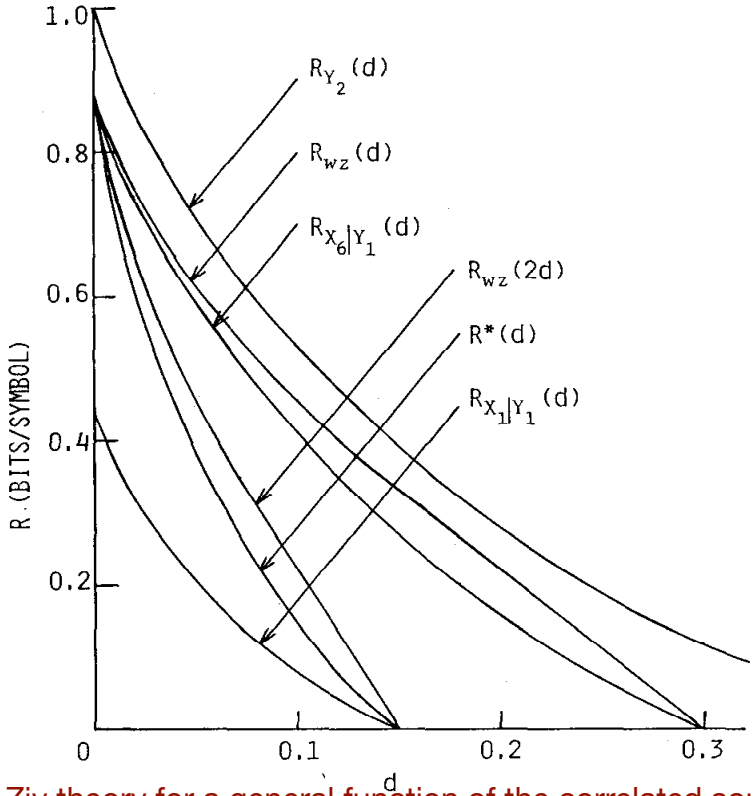


Wyner–Ziv (1976)

Yamamoto (1982)

$$X = G_i(Y_1, Y_2) \qquad \mathrm{E}[d(X^k, \hat{X}^k)] \le D_X$$

i	$X_i=G_i(Y_1,Y_2)$ Y_1Y_2 00	01	10	11	$R_i(d)$	$R_{X_i\|Y_1}(d)$
0	0	0	0	0	0	0
1	0	0	0	1	R*(d)	(h(p)-h(2d))/2
2	0	0	1	0	R*(d)	(h(p)-h(2d))/2
3	0	1	0	0	R*(d)	(h(p)-h(2d))/2
4	1	0	0	0	R*(d)	(h(p)-h(2d))/2
5	0	0	1	1	0	0
6	0	1	0	1	Rwz(d)	h(p)-h(d)
7	0	1	1	0	Rwz(d)	h(p)-h(d)
8	1	0	0	1	Rwz(d)	h(p)-h(d)
9	1	0	1	0	Rwz(d)	h(p)-h(d)
10	1	1	0	0	0	0
11	0	1	1	1	R*(d)	(h(p)-h(2d))/2
12	1	0	1	1	R*(d)	(h(p)-h(2d))/2
13	1	1	0	1	R*(d)	(h(p)-h(2d))/2
14	1	1	1	0	R*(d)	(h(p)-h(2d))/2
15	1	1	1	1	0	0

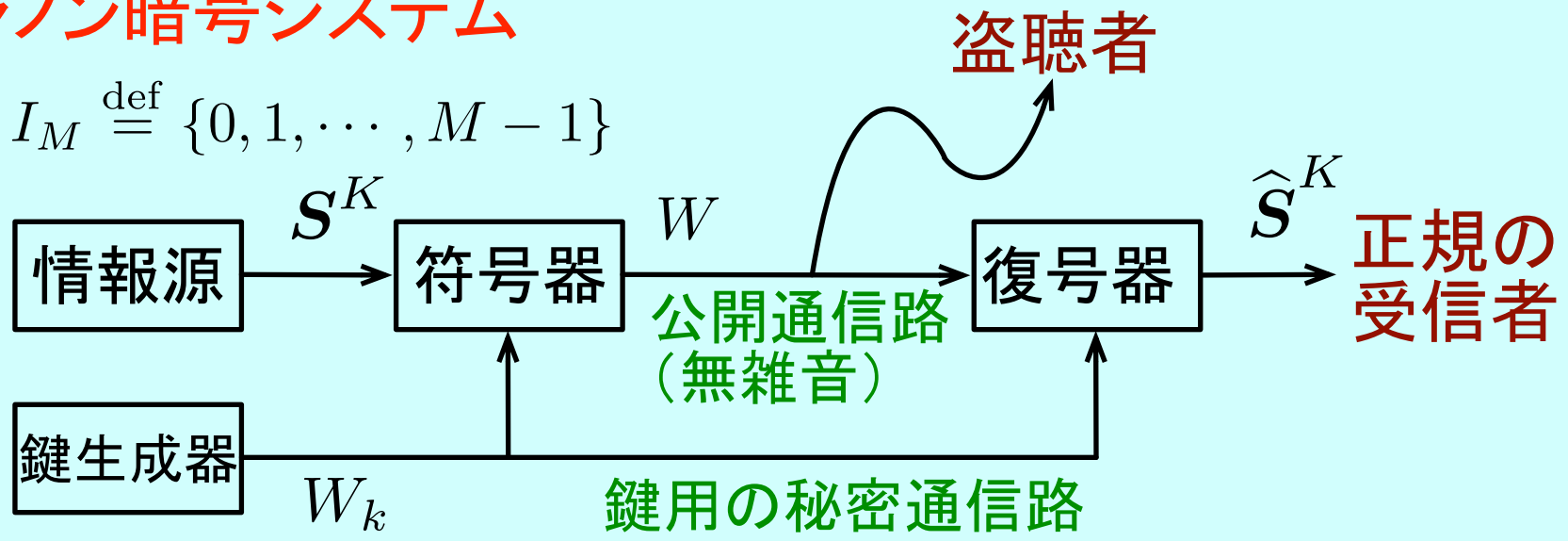


H.Yamamoto, “Wyner-Ziv theory for a general function of the correlated sources,” IEEE Trans. on Information Theory, vol.IT-28, no.5, pp.803-807, Sep. 1982 より抜粋

情報セキュリティ符号化

シャノン暗号システム

$W \in I_M \stackrel{\text{def}}{=} \{0, 1, \cdots, M-1\}$



$W_k \in I_{M_k} \stackrel{\text{def}}{=} \{0, 1, \cdots, M_k - 1\}$

符号化レート：

$$R = \frac{\log M}{K}$$

鍵レート：

$$R_k = \frac{\log M_k}{K}$$

復号誤り率：$P_e = \Pr\left\{S^K \neq \widehat{S}^K\right\}$

セキュリティ測度：$I(S^K; W)$

$\frac{1}{K} I(S^K; W)$

$\left.\begin{array}{l} \\ \\ \\ \end{array}\right\} \begin{array}{l} 0 \text{ or} \\ \leq \varepsilon \end{array}$

完全秘匿

Shannon (1947)　$P(s) = \frac{1}{|\mathcal{S}|}$ の場合

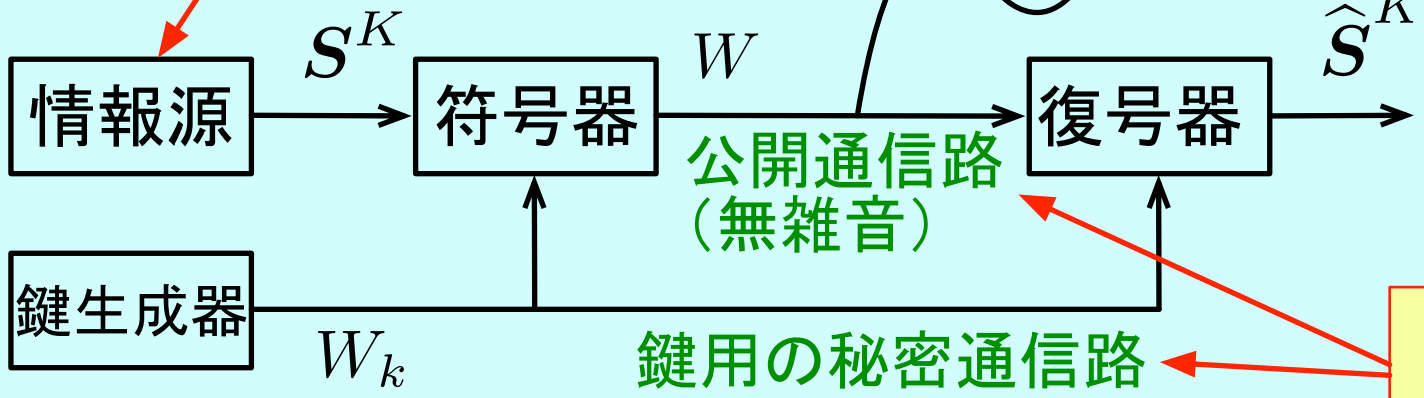
Hellman (1977)　一般の $P(s)$ の場合

情報セキュリティ符号化

相関を持つ情報源の場合

シャノン

$W \in I_M \stackrel{\text{def}}{=} \{0, 1, \cdots, M-1\}$



$W_k \in I_{M_k} \stackrel{\text{def}}{=} \{0, 1, \cdots, M_k - 1\}$

対等な通信路の場合

符号化レート：

$$R = \frac{\log M}{K}$$

鍵レート：

$$R_k = \frac{\log M_k}{K}$$

完全秘匿

完全秘匿でない場合

S $\frac{1}{|\mathcal{S}|}$ の場合

Hellman (1977) 一般の $P(s)$ の場合

歪みを許す場合

他のセキュリティ測度場合

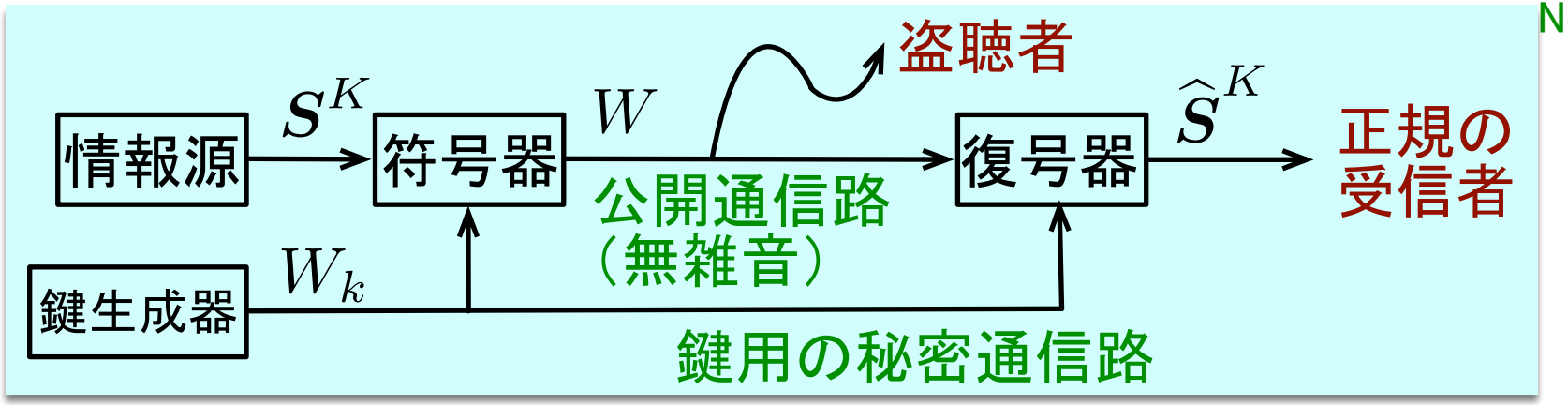
復号誤り率： $P_e = \Pr\left\{S^K \neq \widehat{S}^K\right\}$

セキュリティ測度： $I(S^K; W)$

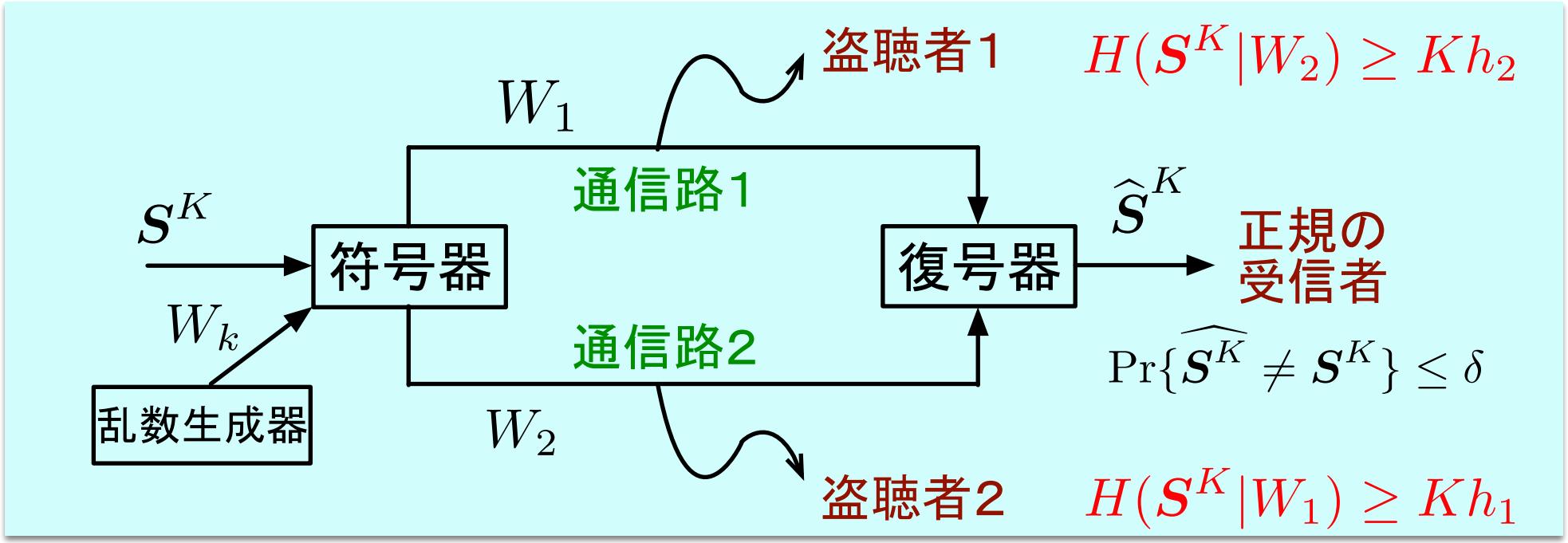
$\frac{1}{K} I(S^K; W)$

$\left.\begin{array}{l} \\ \\ \\ \end{array}\right\} \begin{array}{l} 0 \text{ or} \\ \leq \varepsilon \end{array}$

通信路の対等化



秘密分散通信システム (Secret Sharing Communication System)　Yammaoto (1986)

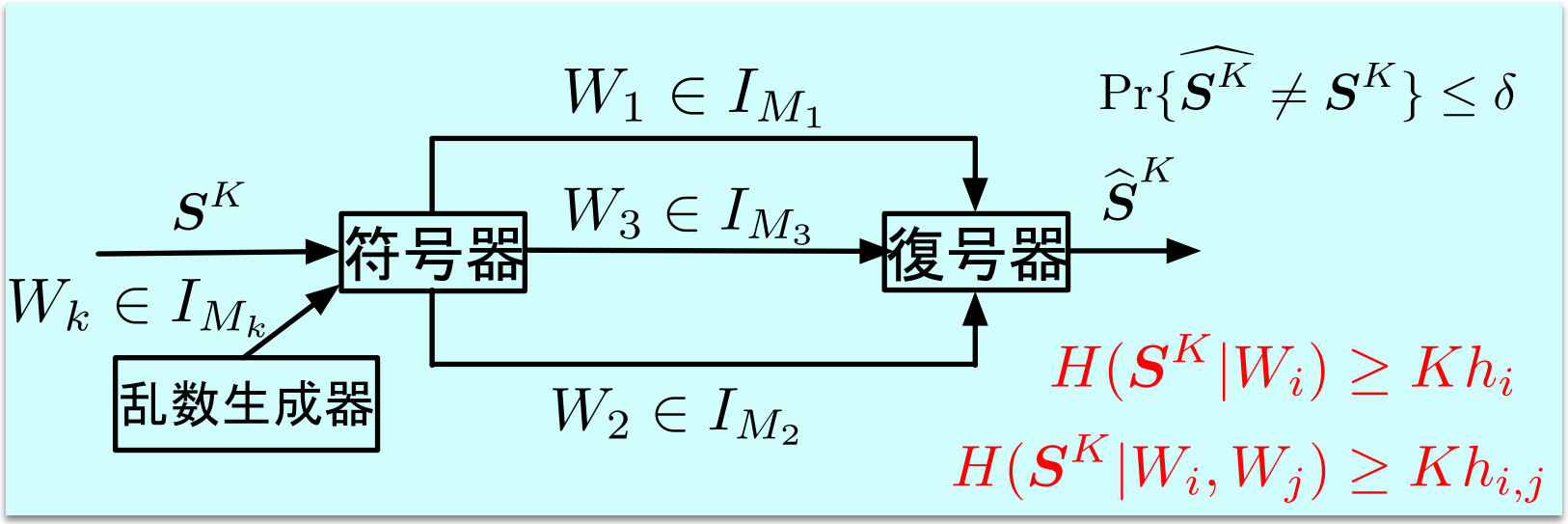


有雑音通信路への拡張
Yammaoto (DMC:1989, AWGNC: 1991)

盗聴通信路符号化　Wyner (1975)
Csiszar Korner (1975)

秘密分散通信システム (Secret Sharing Communication System) Yammaoto (1986)

3通信路の場合



秘密分散法 (Secret Sharing Scheme)

Shamir (1979)

Blakley (1979)

Karnine-Greene-Hellman (1983)

(k, L, n)しきい値ランプ秘密分散法

Blakley-Meadows (1985)

山本博資 (1985)

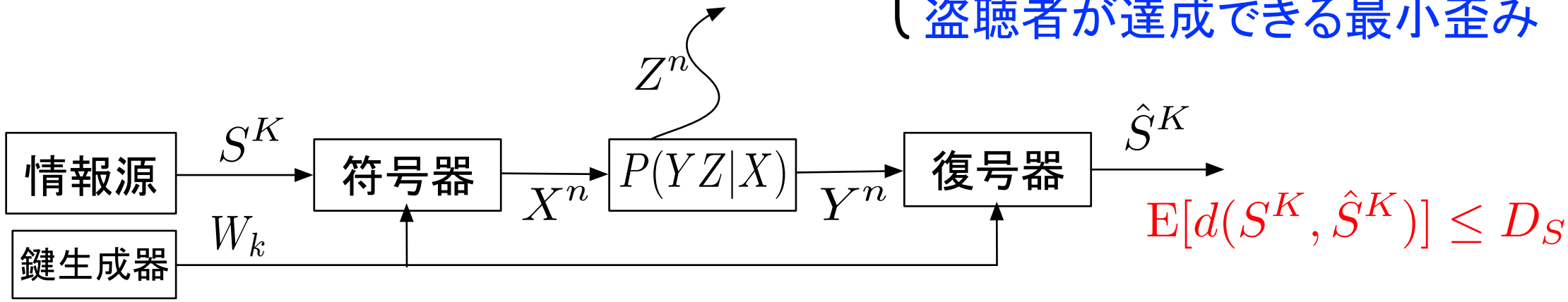
強安全なランプしきい値秘密分散法

シャノン暗号システムの一般化

Yamamoto (1997)

盗聴通信路符号化　Wyner（1975）
Csiszar Korner（1975）

盗聴者
- $H(S^K|Z^n)$
- $H(U^K|Z^n)$　　$I(S;U)>0$
- 盗聴者が達成できる最小歪み

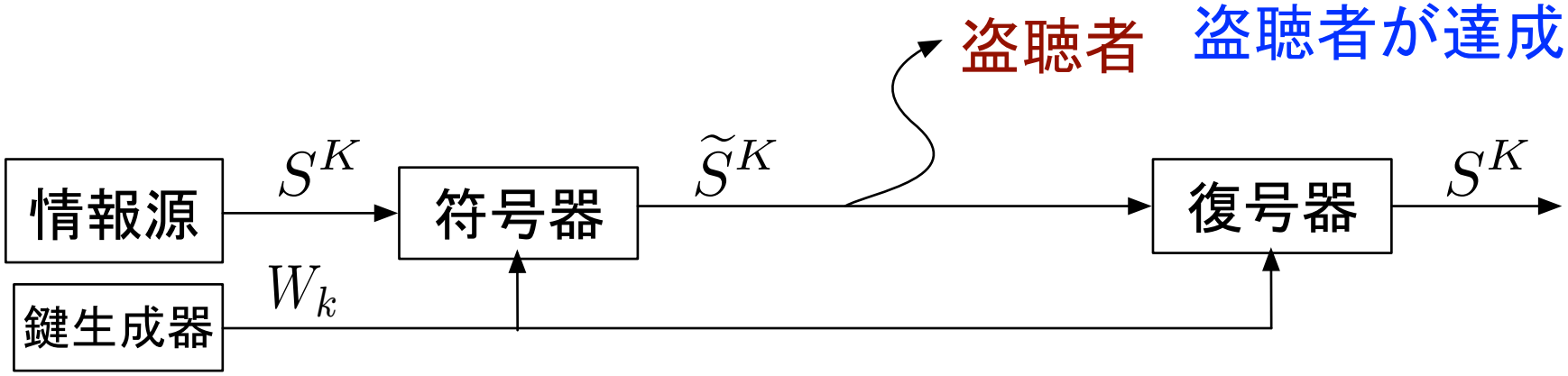


分離符号化定理

- シャノンの暗号符号化
- レート歪み符号化
- 盗聴通信路符号化

独立に符号化したものを組み合わせれば
漸近的に最適

歪みの大きさによる安全性指標の問題点



$$\mathcal{S} = \{0, 1\}$$
$$P_S(0) = P_S(1) = 0.5$$

$$d(S, \hat{S}) = \begin{cases} 0, & \text{If } \hat{S} = S \\ 1, & \text{If } \hat{S} \neq S \end{cases}$$

$$S^K = S_1 S_2 \cdots S_K$$
$$\bar{S}^K = \bar{S}_1 \bar{S}_2 \cdots \bar{S}_K$$
$$\widetilde{S}^K = \begin{cases} S^K, & \text{if } W_k = 0 \\ \bar{S}^K, & \text{if } W_k = 1 \end{cases}$$

$$\mathrm{E}[d(S^K, \tilde{S}^K)] = \frac{1}{K} \sum_i \mathrm{E}[d(S_i, \tilde{S}_i)] = 0.5$$ 最大

歪みの大きさだけでは，安全性として不十分

Shieler–Cuff (2014)

情報の多重符号化

（情報，乱数）を用いた符号化 ➡ （情報1，情報2）を用いた符号化

秘密分散法

Karnine–Greene–Hellman (1983)

(k, n) しきい値法

$$(W_1, W_2, \cdots, W_n) = (S, U_1, U_2, \cdots, U_{k-1})G$$

シェア　秘密情報　乱数

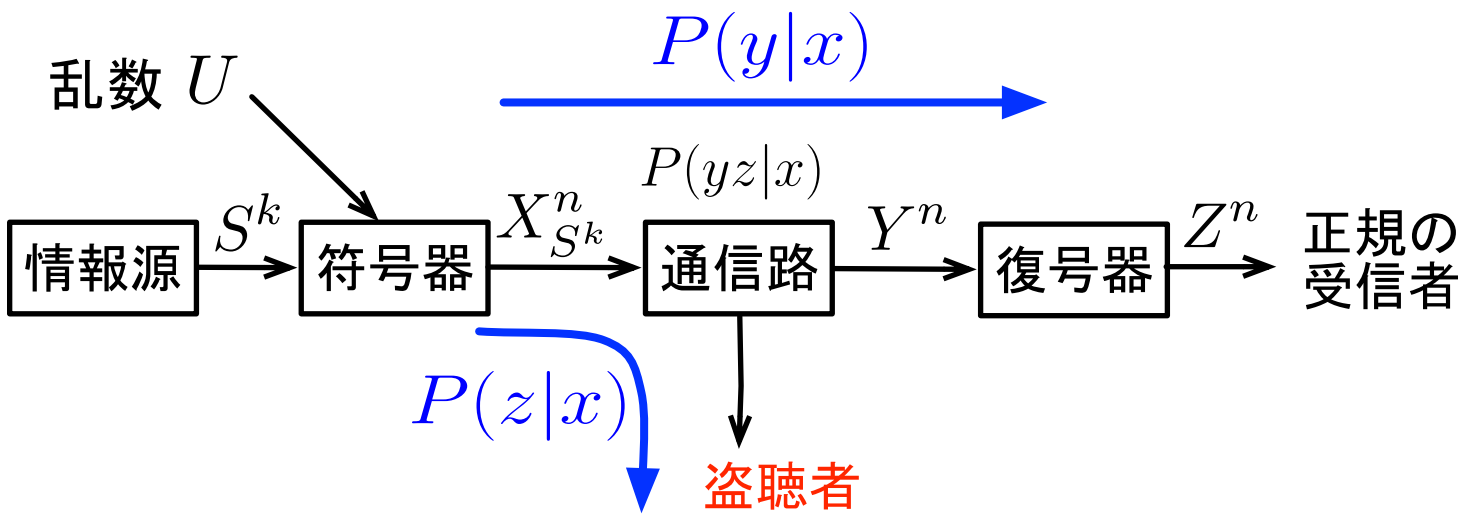
山本博資 (1985)

(k, L, n) ランプしきい値法

$$(W_1, W_2, \cdots, W_n) = (S_1, S_2, \cdots, S_L, U_1, U_2, \cdots, U_{k-L})G$$

シェア　秘密情報　乱数

盗聴通信路符号化　Wyner (1975), Csiszár-Körner (1978)



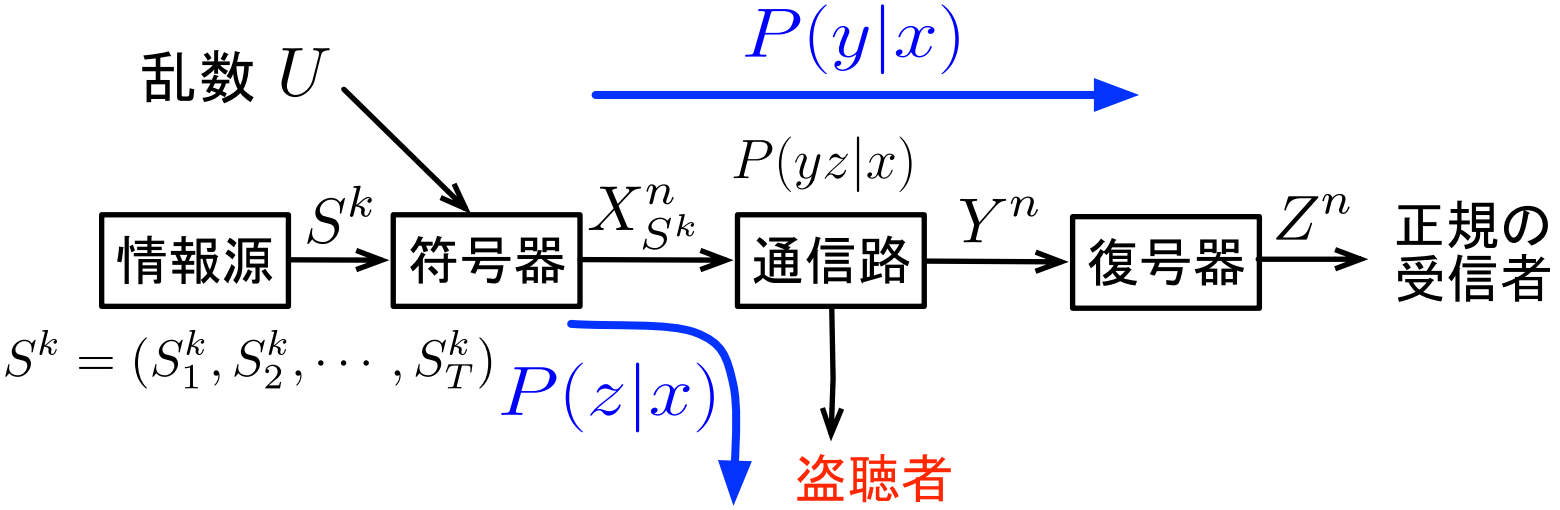
通信路容量: C

秘匿通信路容量: C_S

$R < C_S$ ➡ 完全秘匿

$C_S < C \quad (C_S \ll C)$

盗聴通信路の多重符号化　Kobayashi-Yamamoto-Ogawa (2013)



R_i : S_i の符号化レート

$R_i < C_S$

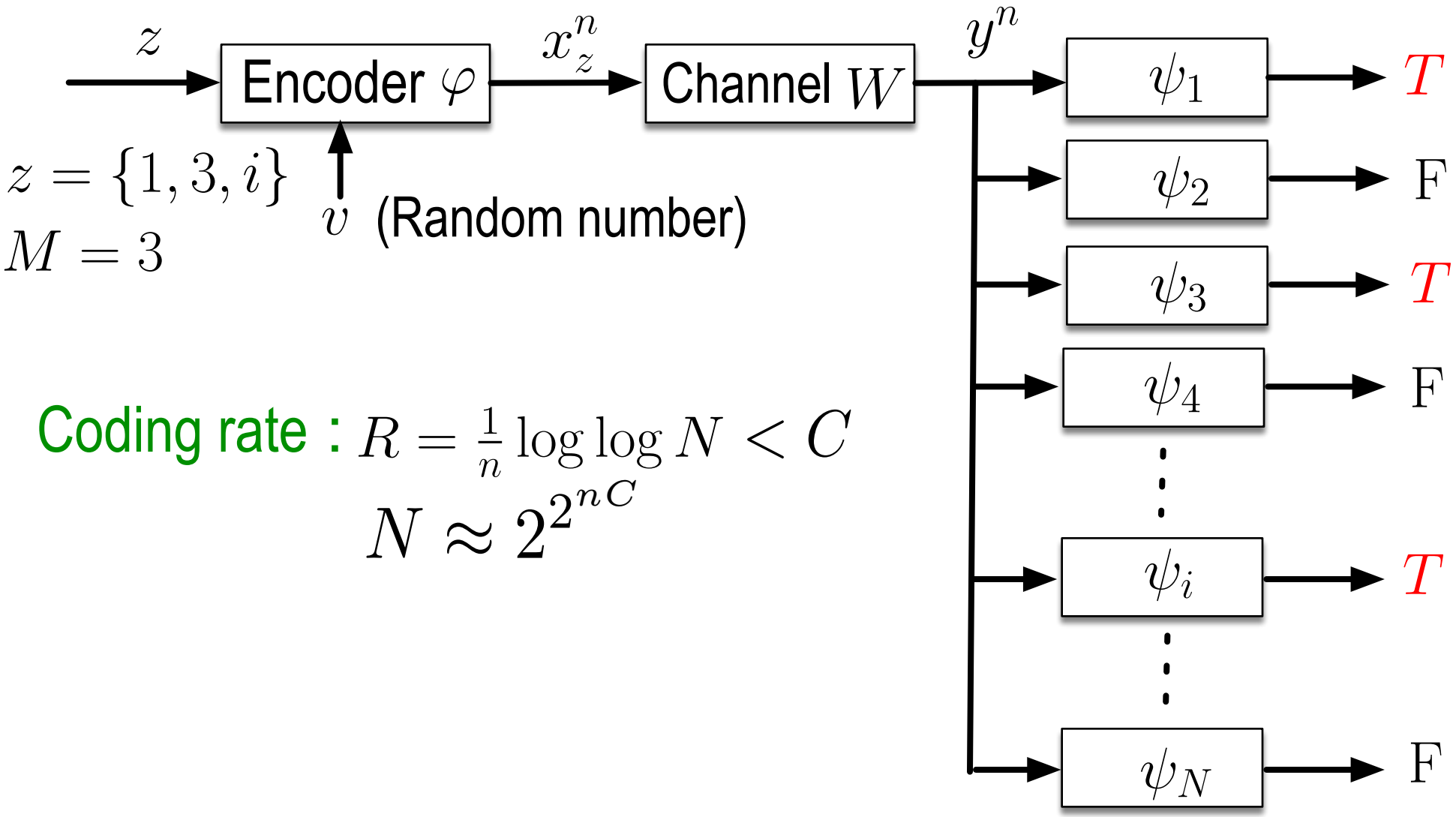
➡ 各 S_i を完全秘匿

$\sum_{i=1}^{T} R_i < C$

➡ トータルの符号化レートを通信路容量まで増やせる

同定符号化　Ahlswede-Dueck (1989)

多重同定符号化　Yamamoto-Ueda (2013)



Coding rate : $R = \frac{1}{n} \log \log N < C$

$$N \approx 2^{2^{nC}}$$

データ圧縮符号

平均最適符号(平均符号長が最小) → 繰り返し使用することが前提

競合最適符号
(competitively optimal code) → 一度だけの使用に対する最適性

Cover (1991)

2つの符号間の優越性

符号Aは符号Bを優越：

$$\Pr\{l_A(X) < l_B(X)\} \geq \Pr\{l_A(X) > l_B(X)\}$$

全ての符号に対して優越

競合最適符号

（必ずしも存在するとは限らない）

Shannon符号： 1ビットハンデで競合最適

$$\Pr\{l_S(X) < l_B(X) + 1\} \geq \Pr\{l_S(X) > l_B(X) + 1\}$$

Cover (1991)

Huffman符号： 1ビットハンデで競合最適

$$\Pr\{l_H(X) < l_B(X) + 1\} \geq \Pr\{l_H(X) > l_B(X) + 1\}$$

Feder (1992)

競合最適符号が存在 ➡ 競合最適符号は平均最適

ゲーム理論との関係

Yamamoto-Itoh (1995)

Elements of Information Theory, 1st Ed. (Cover-Thomas, 1991)

5.11 Competitively Optimality of the Shannon Code

Elements of Information Theory, 2nd Ed. (Cover-Thomas, 2006)

「Competitively Optimality of the Shannon Code」の節は削除

競合最適符号化問題の拡張

Alphabetic code
(Maruyama-Yamamoto, 2000)

コスト付き符号化
(d,k)制約符号化
など
} Open problems

T.Cover and J.Thomas, Elements of Information Theory, 1st ed., John Wiley & Sons, Inc. (1991)より抜粋

データ圧縮符号

正整数のユニバーサル符号化

Elias (1975)　γ-code, δ-code, ω-code

Bentley–Yao (1976)

Even–Rodeh (1978)

$$n \in \{1, 2, 3, \cdots\}, \quad P(n) \geq P(n+1)$$

ユニバーサル: $\dfrac{\mathrm{E}[L_a(n)]}{\max\{1, H(P)\}} \leq \rho_a$ を満たす定数 ρ_a が存在

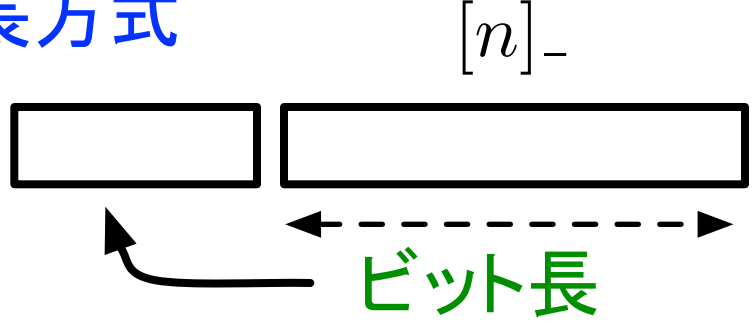
漸近最適: $\dfrac{\mathrm{E}[L_a(n)]}{\max\{1, H(P)\}} \leq g_a(H(P))$　　$\lim_{x\to\infty} g_a(x) = 1$

ほとんど漸近最適: $\dfrac{\mathrm{E}[L_{a(t)}(n)]}{\max\{1, H(P)\}} \leq g_{a(t)}(H(P))$　$\lim_{t\to\infty}\lim_{x\to\infty} g_{a(t)}(x) = 1$

（ t は符号 a のパラメータ）

正整数のユニバーサル符号化

(1) メッセージ長方式



再帰的メッセージ長方式

Elias ω-code (1975)
Bentley–Yao (1976)
Even–Rodeh (1978)
Yamamoto (2000)

(2) Flag方式

数値情報部にFlag系列が
現れないように工夫する

Fibonacci方式

Capocelli (1989,1990)

Bit-Stuffing方式

Yamamoto–Ochi (1991)

(3) グルーピング方式

Amemiya–Yamamoto (1993)

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 .....

グループ番号＋グループ内順位で符号化

正整数のユニバーサル符号化

ユニバーサル: $\dfrac{\mathrm{E}[L_a(n)]}{\max\{1, H(P)\}} \le \rho_a$ を満たす定数 ρ_a が存在

漸近最適: $\dfrac{\mathrm{E}[L_a(n)]}{\max\{1, H(P)\}} \le g_a(H(P))$ $\lim_{x\to\infty} g_a(x) = 1$

ほとんど漸近最適: $\dfrac{\mathrm{E}[L_{a(t)}(n)]}{\max\{1, H(P)\}} \le g_{a(t)}(H(P))$ $\lim_{t\to\infty}\lim_{x\to\infty} g_{a(t)}(x) = 1$

漸近最適で，かつρ_a をどこまで小さくできるか？　Yan-Lin (2021)

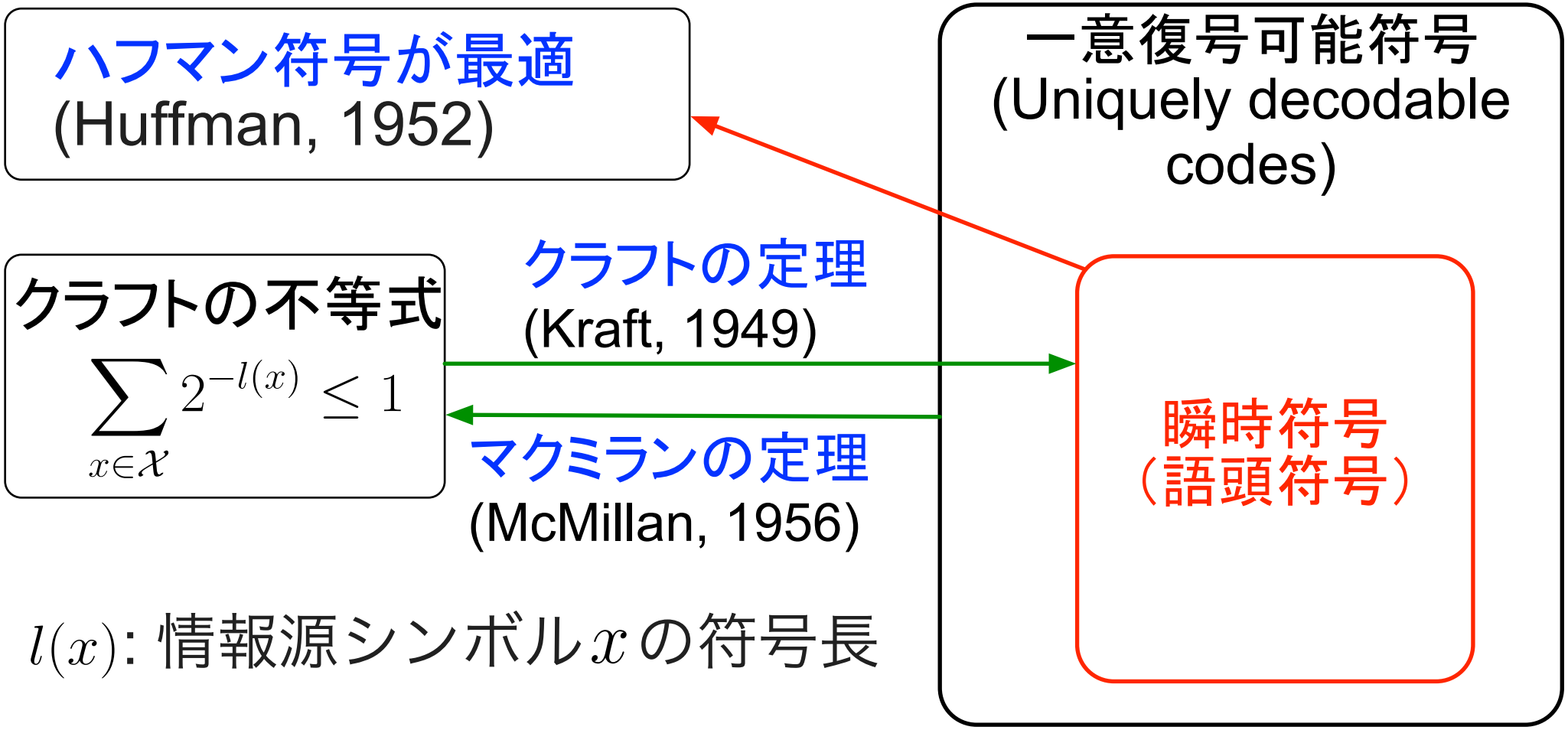
$$\rho = \inf_a \{\rho_a \mid \mathrm{E}[L_a(n)] \le \rho_a H(P) \quad \text{for any } P(n)\}$$

さまざまな問題設定が可能　Open problems

$$\rho(x) = \inf_a \{\rho_a(x) \mid \mathrm{E}[L_a(n)] \le \rho_a(H(P)) \cdot H(P) \quad \text{for any } P(n)\}$$

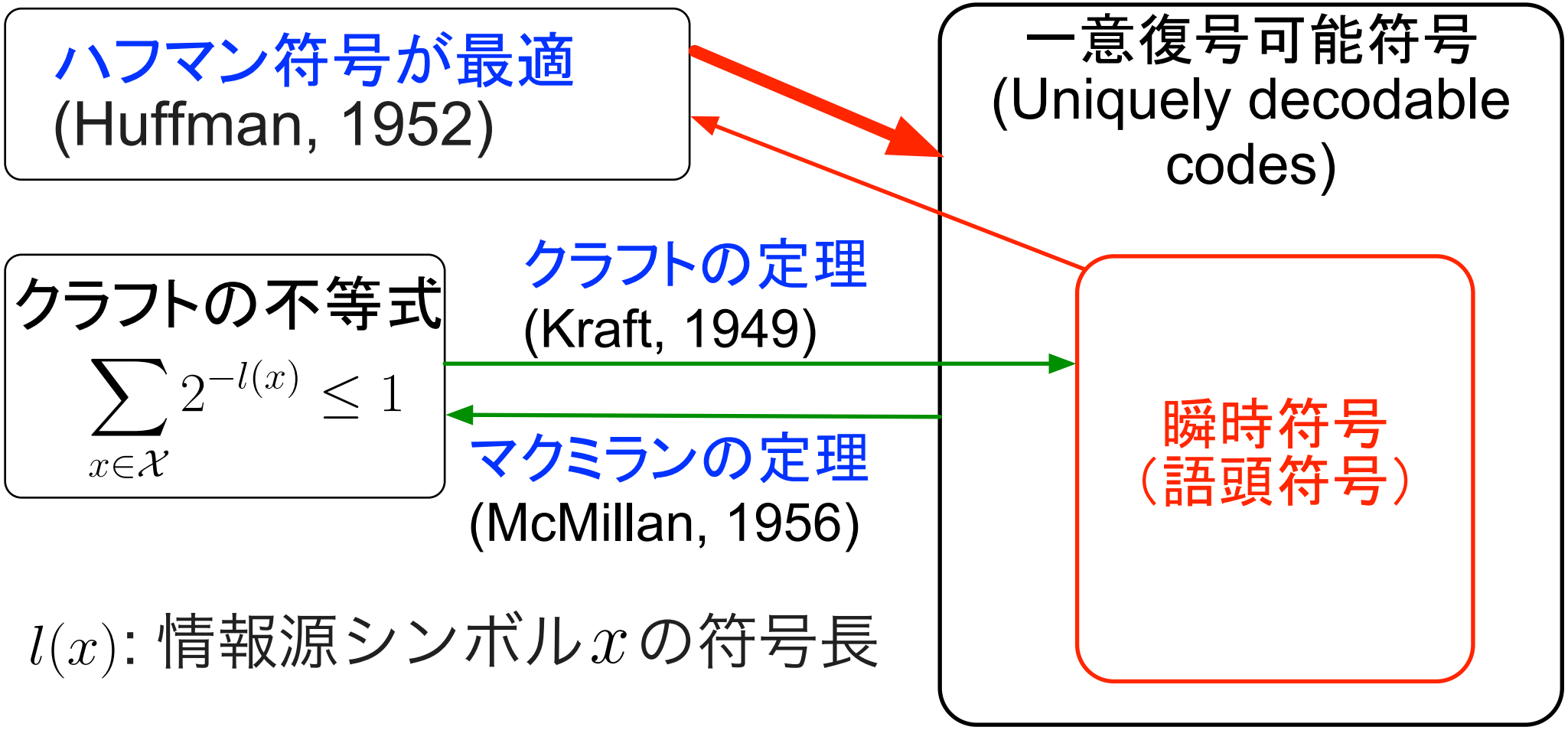
$$\kappa = \min_a \{\kappa \mid \mathrm{E}[L_a(n)] \le H(P) + \kappa_a \log H(P) \quad \text{for any } P(n)\}$$

FV符号 (Fixed-to-Variable length code)



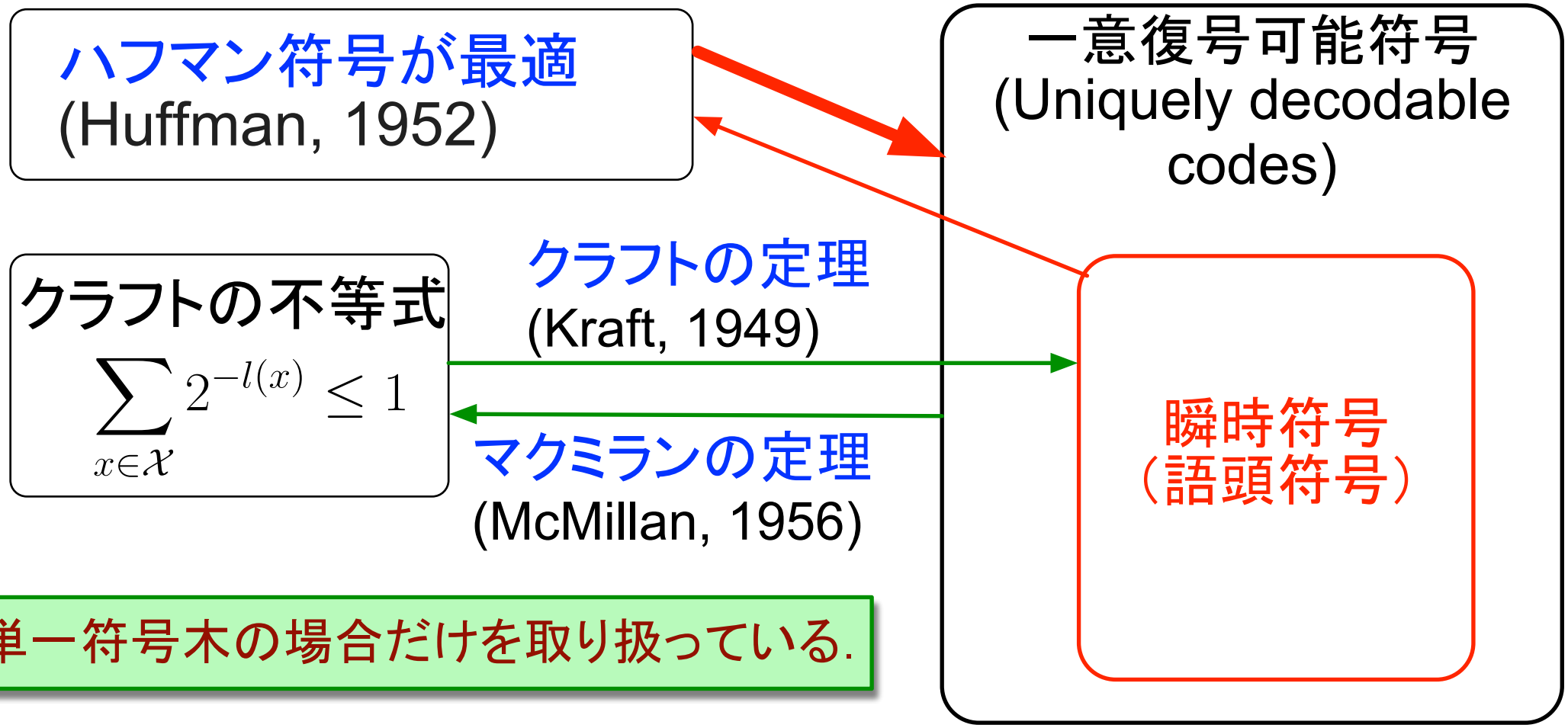
$l(x)$: 情報源シンボルxの符号長

FV符号 (Fixed-to-Variable length code)

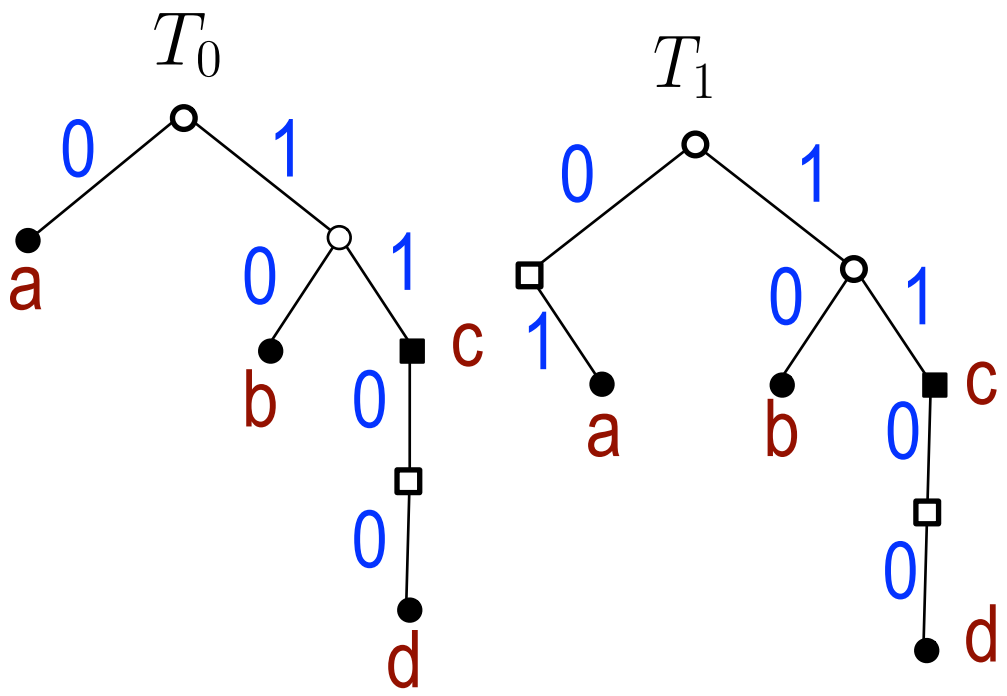


$l(x)$: 情報源シンボルxの符号長

FV符号 (Fixed-to-Variable length code)

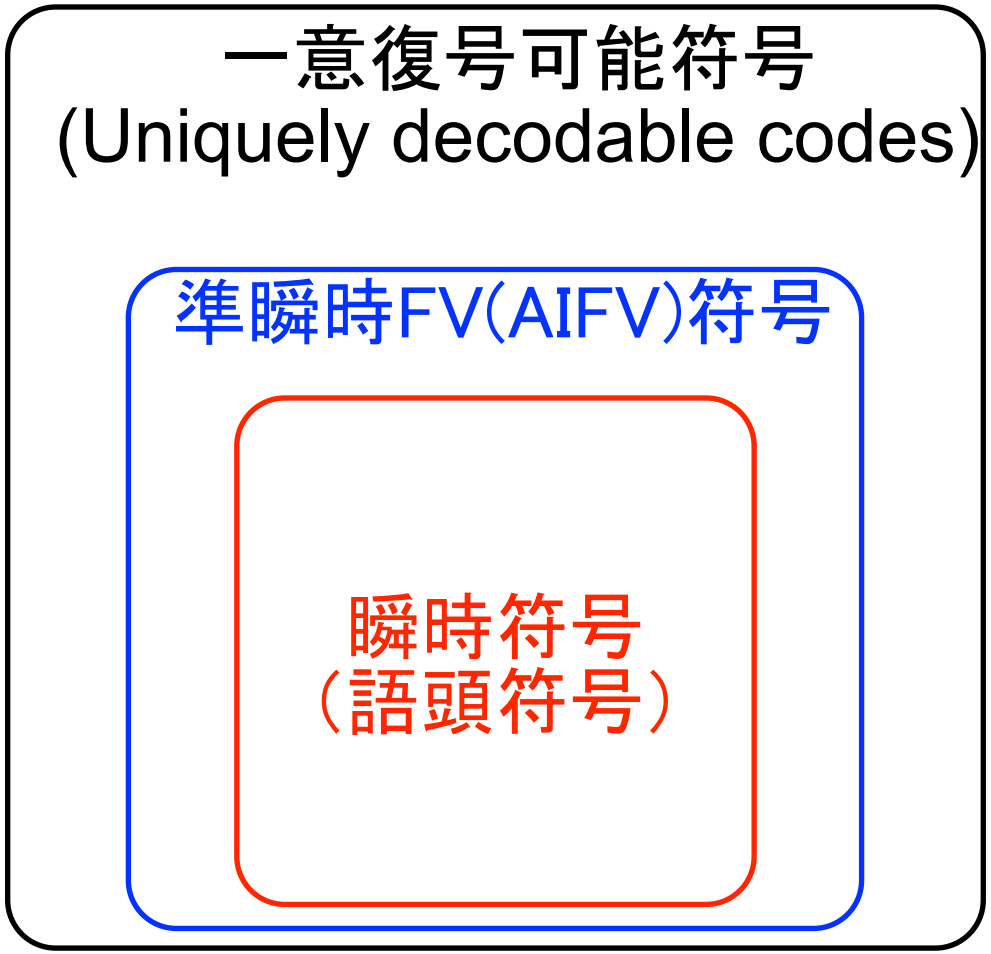


準瞬時FV(AIFV)符号



2本の符号木:
AIFV符号(準瞬時FV符号)

復号遅延:最大2ビット



Yamamoto-Wei (2013)
Yamamoto-Tsuchihasi-Honda (2015)

AIFV符号の最悪冗長度

ハフマン符号： 符号木：1個，復号遅延：0

$$H(P) \leq L < H(P) + 1$$

AIFV符号： 符号木：2個，復号遅延：最大2ビット

$$H(P) \leq L < H(P) + \frac{1}{2}$$

AIFV-m符号： 符号木：m個，復号遅延：最大mビット

$$H(P) \leq L < H(P) + \frac{1}{m}$$

for $2 \leq m \leq 4$ Hu–Yamamoto–Honda (2017)

for $m = 5$ Fujita–Iwata–Yamamoto (2020)

AIFV符号関連研究に関する解説

解 説

準瞬時 FV 符号（AIFV 符号）
――ハフマン符号に勝る圧縮率を達成する符号――

AIFV Code to Achieve Better Compression Rate than the Huffman Code

山本博資

Abstract

ハフマン符号は，定常無記憶なデータ系列を最も効率良く圧縮できる最適なデータ圧縮符号としてよく知られている．しかし，2015 年に Yamamoto, Tsuchihashi, Honda によって提案された準瞬時 FV 符号（AIFV 符号：Almost Instantaneous Fixed-to-Variable length code）を用いると，ハフマン符号より更に良い圧縮率を実現することができる．AIFV 符号は 2 個の符号木から構成されるが，その AIFV 符号の符号木の構造，符号化／復号アルゴリズム，平均符号長，最適な AIFV 符号木の構成法などについて解説する．更に，m 個の符号木を用いる AIFV-m 符号をはじめとする様々な拡張符号や関連する研究について紹介する．

キーワード：AIFV 符号，ハフマン符号，AIFV-m 符号，AIVF 符号，データ圧縮，反復最適化

山本博資，“準瞬時FV符号(AIFV符号) ―ハフマン符号に勝る圧縮率を達成ふる符号―,”
電子情報通信学会誌，vol.104, no.1, pp.35-42, 2021年1月　より抜粋

AIFV符号関連研究に関する解説

最適な符号木の構成法

繰り返し最適化＋IP （Yamamoto-Tsuchihashi-Honda, 2015）

繰り返し最適化＋DP (Iwata-Yamamoto, 2017)

有限状態マルコフ連鎖の平均最適化 (Fujita-Iwata-Yamamoto, 2019)

AIFV-m符号の繰り返し最適化＋DP (Iwata-Yamamoto, 2021)

符号木総数の数え上げ

AIFV符号木総数の数え上げ （Sumigawa-Yamamoto, 2017）

AIFVコンパクト符号木総数の数え上げ (Hashimoto-Iwata-Yamamoto, 2019)

動的AIFV符号 (Hiraoka-Yamamoto, 2018)

Alphabetic AIFV 符号 （Hiraoka-Yamamoto, 2018）

AIVF符号 (Yamamoto-Yokoo, 2001) (Iwata-Yamamoto, 2021)

:

今までに行った情報理論の研究テーマ

面白い研究課題が
まだたくさん残っている

誤り訂正符号・誤り制御方式

フィードバック通信方式および理論（無雑音フィードバック，有雑音フィードバック）

その他（TCM，LDPC符号，Polar符号など）

データ圧縮符号

ユニバーサル符号，正整数のユニバーサル符号，競合最適符号化

準瞬時符号，有歪み圧縮符号化

シャノン理論

マルチユーザ情報理論（セキュリティ問題無し）

マルチユーザ情報理論（セキュリティ問題有り，シャノン暗号システム，
盗聴通信路符号化など）

その他（符号化定理，情報スペクトル理論，同定符号など）

情報セキュリティ

秘密分散法，視覚暗号，量子秘密分散法

複雑さ理論・乱数検定，その他

その他

機械学習，
ネットワーク符号化など