Digital Communication Systems ECS 452

Asst. Prof. Dr. Prapun Suksompong

prapun@siit.tu.ac.th

4. Mutual Information and Channel Capacity





Office Hours:

Check Google Calendar on the course website. Dr.Prapun's Office: 6th floor of Sirindhralai building, BKD

Reference for this chapter

- Elements of Information Theory
- By Thomas M. Cover and Joy A. Thomas
- 2nd Edition (Wiley)
- Chapters 2, 7, and 8
- 1st Edition available at SIIT library: Q360 C68 1991





JOY A. THOMAS

Recall: Entropy

4.29. Reminder:

- (a) Some definitions involving entropy
 - (i) Binary entropy function: $h(p) = -p \log_2 p (1-p) \log_2 (1-p)$

(ii)
$$H(X) = -\sum_{x} p(x) \log_2 p(x)$$

(iii)
$$H(\underline{\mathbf{p}}) = -\sum_{i} p_i \log_2(p_i)$$

(b) A key entropy property that will be used frequently in this section is that for any random variable X,

 $H(X) \leq \log_2 |\mathcal{X}|$ with equality iff X is uniform.

[Page 70]

Recall: Entropy

- **Entropy** measures the amount of uncertainty (randomness) in a RV.
- Three formulas for calculating entropy:
 - [Defn 2.41] Given a pmf $p_X(x)$ of a RV X,
 - $H(X) \equiv -\sum_{x} p_X(x) \log_2 p_X(x)$. Set $0 \log_2 0 = 0$.
 - [2.44] Given a probability vector **p**,

•
$$H(\underline{\mathbf{p}}) \equiv -\sum_i p_i \log_2 p_i.$$

• [Defn 2.47] Given a number $p \in [0,1]$, binary entropy function
• $H(p) \equiv h_b(p) = -p \log_2 p - (1-p) \log_2 (1-p)^{(1-p)}$

• [2.56] Operational meaning: Entropy of a random variable is the average length of its shortest description.

Recall: Entropy

• Important Bounds

$$\begin{array}{c} 0 \\ \text{deterministic} \leq H(X) \leq \log_2 |S_X| \\ \text{uniform} \end{array}$$

- The entropy of a uniform (discrete) random variable: $H(X) = \log_2 |S_X|$
- The entropy of a Bernoulli random variable: $H(p) \equiv h_b(p) = -p \log_2 p - (1-p) \log_2 (1-p)$

• binary entropy function



Digital Communication Systems ECS 452

Asst. Prof. Dr. Prapun Suksompong prapun@siit.tu.ac.th Information-Theoretic Quantities



Entropy and Joint Entropy

• Entropy

- $H(X) = -\sum_{x} p(x) \log_2 p(x)$
 - Amount of randomness in *X*
- $H(Y) = -\sum_{y} q(y) \log_2 q(y)$
 - Amount of randomness in *Y*
- Joint Entropy
 - $H(X,Y) = -\sum_{(x,y)} p(x,y) \log_2 p(x,y)$
 - Amount of (combined) randomness in (X, Y) pair
 - In general, $H(X, Y) \neq H(X) + H(Y)$

• There might be some shared randomness between X and Y.

H(X)

H(X

Conditional Entropies

Amount of randomness in Y

$$H(Y) \equiv -\sum_{y \in \mathcal{Y}} q(y) \log_2 q(y) \equiv H\left(\underline{\mathbf{q}}\right)$$

Amount of randomness still remained in *Y* when we know that X = x.

given a particular value
$$x$$

 $H(Y|X = x) \equiv H(Y|x) \equiv -\sum_{y \in \mathcal{Y}} Q(y|x) \log_2 Q(y|x)$
Apply the entropy calculation to a row from the **Q** matrix

X

= 0

average of H(Y|x)

The **average** amount of randomness still remained in *Y* when we know *X*

$$H(Y|X) \equiv \sum_{x \in \mathcal{X}} p(x) H(Y|x)$$

= H(X,Y) - H(X)

Conditional Entropies

Amount of randomness in Y

$$H(Y) \equiv -\sum_{y \in \mathcal{Y}} q(y) \log_2 q(y) \equiv H\left(\underline{\mathbf{q}}\right)$$

Amount of randomness still remained in *Y* when we know that X = x.

given a particular value
$$x$$

 $H(Y|X = x) \equiv H(Y|x) \equiv -\sum_{y \in \mathcal{Y}} Q(y|x) \log_2 Q(y|x)$
Apply the entropy calculation to a row from the \mathbf{Q} matrix
 $x \begin{bmatrix} x \end{bmatrix} = \mathbf{Q}$
 $Average of H(Y|x)$
 $H(Y|X) \equiv \sum_{x \in \mathcal{X}} p(x)H(Y|x)$

The **average** amount of randomness still remained in *Y* when we know *X*

= H(Y) - I(X;Y)

= H(X,Y) - H(X)







Digital Communication Systems ECS 452

Asst. Prof. Dr. Prapun Suksompong prapun@siit.tu.ac.th Operational Channel Capacity



Shannon [1948] shows that these two quantities are actually the same.



Some results from Section 3.3-3.4

Example 3.66.

- (1) MAP decoder is optimal. (It minimizes $P(\mathcal{E})$).
- (2) ML decoder is suboptimal. However, it can be optimal (same $P(\mathcal{E})$ as the MAP decoder) when the <u>codewords are equally-likely</u>.
- (3) ML decoder is the same as the minimum distance decoder when the crossover probability of the BSC p is < 0.5 (which is usually the case).

17

Under appropriate assumptions, minimum distance decoder is optimal.









Review **Repetition Code** Example 3.63. Find the codebook and code rate for the encoder which uses repetition code with n = 5. codeword code book: info-block 0100000 D info - bit 2) xrows = 2k = 2 = 2







- Use repetition code with n = 5 at the transmitter
- Use majority vote at the receiver
- New BSC with $\tilde{p} = {5 \choose 3} p^3 (1-p)^2 + {5 \choose 4} p^4 (1-p)^1 + {5 \choose 5} p^5 (1-p)^0 \approx 10^{-5}$



A simple error-correcting code is the *repetition code*. Example of such code is described below:

Two ways to calculate the probability of error:

(a) (transmission) error occurs if and only if the number of bits

in error are ≥ 3 . expective s error bits = 4 $\beta = P(E) = {5 \choose 3} p^3 (1-p)^2 + {5 \choose 7} p^7 (1-p) + {5 \choose 5} p^5 (1-p)^5$ with p=0.01 $P(E) \approx 10^{-5}$

(b) (transmission) error occurs if and only if the number of bits <u>not in error are ≤ 2 </u>. $\rightarrow 0$, 1 , 2

 $P(E) = {\binom{5}{0}} (1-p)^{\circ} p^{5} + {\binom{5}{1}} (1-p)^{1} p^{4} + {\binom{5}{2}} (1-p)^{2} p^{3}$





MATLAB

```
function PE = PE minDist(C,p)
% Function PE minDist 3 computes the error probability P(E) when code C
% is used for transmission over BSC with crossover probability p.
% Code C is defined by putting all its (valid) codewords as its rows.
M = size(C,1);
k = loq2(M);
n = size(C,2);
% Generate all possible received vectors
Y = dec2bin(0:2^n-1) - '0';
% Normally, we need to construct an extended Q matrix. However, because
% each conditional probability in there is a decreasing function of the
% Hamming distance, we can work with the distances instead of the
% conditional probability. In particular, instead of selecting the max in
% each column of the O matrix, we consider min distance in each column.
dmin = zeros(1, 2^n);
for i = 1:(2^n)
    % for each received vector y,
    y = Y(j,:);
   % find the minimum distance (the distance from y to the closest
    % codeword)
    d = sum(mod(bsxfun(@plus,y,C),2),2);
    dmin(j) = min(d);
end
% From the distances, calculate the conditional probabilities.
% Note that we compute only the values that are to be selected (instead of
% calculating the whole Q first).
n1 = dmin; n0 = n-dmin;
Qmax = (p.^n1).*((1-p).^n0);
% Scale the conditional probabilities by the input probabilities and add
% the values. Note that we assume equally likely input.
PC = sum((1/M)*Omax);
PE = 1 - PCi
end
```

MATLAB

- Annotated version [Posted @ 3PM on Feb 21; Updated @ 5PM on Feb 28]
- Slides [Posted @ 9PM on Feb 8; Updated @ 4:30PM on Feb 14, @ 3PM on Feb 21, and @ 5PM on Feb 28]
- Exercise 5 Solution [Posted @ 10AM on Feb 25]
- Exercise 6 Solution [Posted @ 10AM on Feb 25]
- Exercise 7 Solution [Posted @ 10AM on Feb 25]
- MATLAB: BSC_demo.m, BAC_demo.m, DMC_demo.m, DMC_Analysis_demo.m, DMC_Channel_sim.m, BSC_decoder_ALL_demo.m, DMC_decoder_DIY_demo.m, DMC_decoder_ALL_demo.m, DMC_decoder_MAP_demo.m, DMC_decoder_ML_demo.m
- MATLAB: PE_minDist.m, PE_minDist_demo1 .m, PE_minDist_demo2.m
- Chapter 4: Mutual Information and Channel Capacity [Posted @ 11AM on Feb 20]
 - Annotated version [Posted @ 5PM on Feb 28; Updated @ 5PM on Mar 7 and @ 3PM on Mar 8]
 - MATLAB: capacity_blahut.m
 - Exercise 8 Solution [Posted @ 9AM on Mar 6]
 - Exercise 9 Solution [Posted @ 5PM on Mar 7]
 - Exercise 10 Solution [Posted @ 3PM on Mar 19]
 - Slides [Posted @ 5PM on Mar 7; Updated @ 3PM on Mar 8]
- Chapter 5: Channel Coding

Example: Repetition Code

• Original Equivalent Channel:

• BSC with crossover probability *p*

• New (and Better) Equivalent Channel:



- Use repetition code at the transmitter
- Use majority vote at the receiver
- New BSC with new crossover probability $ilde{p}$



Searching for the best encoder

- Now that we have MATLAB function PE_minDist, for specific values of n, k, we can try to search for the encoder that minimizes the error probability.
- Recall that, from Example 3.64, there are $\binom{2^n}{M} = \binom{2^n}{2^k}$ reasonable encoders.
- Even for small *n* and *k*, this is a large space to look at every possible cases.

Example: Repetition Code



n	\widetilde{p}
1	p = 0.1
3	$\binom{3}{2}p^{2}(1-p) + \binom{3}{3}p^{3} \approx 0.0280$
5	$\binom{5}{3}p^3(1-p)^2 + \binom{5}{4}p^4(1-p)^1 + \binom{5}{5}p^5 \approx 0.0086$
7	≈ 0.0027
9	$\approx 8.9092 \times 10^{-4}$
11	$\approx 2.9571 \times 10^{-4}$



Shannon [1948] shows that these two quantities are actually the same.

Digital Communication Systems ECS 452

Asst. Prof. Dr. Prapun Suksompong prapun@siit.tu.ac.th Information Channel Capacity



Shannon [1948] shows that these two quantities are actually the same.

MATLAB

```
function H = entropy2s(p)
% ENTROPY2 accepts probability mass function
% as a row vector, calculate the corresponding
% entropy in bits.
p=p(find(abs(sort(p)-1)>1e-8)); % Eliminate 1
p=p(find(abs(p)>1e-8)); % Eliminate 0
if length(p)==0
    H = 0;
else
    H = simplify(-sum(p.*log(p))/log(sym(2)));
end
```

```
function I = informations(p,Q)
X = length(p);
q = p*Q;
HY = entropy2s(q);
temp = [];
for i = 1:X
    temp = [temp entropy2s(Q(i,:))];
end
HYgX = sum(p.*temp);
I = HY-HYgX;
```



Capacity of 0.0918 bits is achieved by p = [0.5380, 0.4620]

Capacity calculation for BAC



Same procedure applied to BSC

$$p(0) = p_0 \qquad 0 \qquad 0.6 \qquad 0 \\ X \qquad p(1) = 1 - p_0 \qquad 0.4 \qquad 0.6 \qquad 0 \\ 0.4 \qquad 0.6 \qquad 1 \qquad \longrightarrow Y \qquad Q = \begin{bmatrix} 0.6 & 0.4 \\ 0.4 & 0.6 \end{bmatrix}$$



Blahut–Arimoto algorithm

```
function [ps C] = capacity_blahut(Q)
% Input: 0 = channel transition probability matrix
% Output: C = channel capacity
      ps = row vector containing pmf that achieves capacity
%
tl = 1e-8; % tolerance (for the stopping condition)
n = 1000; % max number of iterations (in case the stopping condition
          % is "never" reached")
nx = size(Q,1); pT = ones(1,nx)/nx; % First, guess uniform X.
for k = 1:n
    ;0*Tq = Tp
    % Eliminate the case with 0
    % Column-division by qT
    temp = Q.*(ones(nx,1)*(1./qT));
    %Eliminate the case of 0/0
    12 = log2(temp);
    l2(find(isnan(l2) | (l2==-inf) | (l2==inf)))=0;
    logc = (sum(Q.*(12),2))';
   CT = 2.^{(logc)};
    A = log2(sum(pT.*CT)); B = log2(max(CT));
    if((B-A)<tl)
       break
    end
    % For the next loop
    pT = pT.*CT; % un-normalized
    pT = pT/sum(pT); % normalized
    if(k == n)
        fprintf('\nNot converge within n loops\n')
    end
end
ps = pT;
                                                [capacity_blahut.m]
C = (A+B)/2;
```


$$\begin{array}{c} x \\ p(1) = 1 - p_0 \\ p(1) = 1 - p_0 \\ 1 \\ \hline 0.6 \\ 0.6 \\ 1 \end{array} \xrightarrow{q \ 0} Y \qquad Q = \begin{bmatrix} 0.1 & 0.9 \\ 0.4 & 0.6 \end{bmatrix}$$



Richard Blahut

- Former chair of the Electrical and Computer Engineering Department at the University of Illinois at Urbana-Champaign
- Best known for
 Blahut–Arimoto
 algorithm
 (Iterative
 Calculation of C)







Claude E. Shannon Award

Claude E. Shannon (1972) David S. Slepian (1974) Robert M. Fano (1976) Peter Elias (1977) Mark S. Pinsker (1978) Jacob Wolfowitz (1979) W. Wesley Peterson (1981) Irving S. Reed (1982) Robert G. Gallager (1983) Solomon W. Golomb (1985) William L. Root (1986) James L. Massey (1988) Thomas M. Cover (1990) Andrew J. Viterbi (1991)

Elwyn R. Berlekamp (1993) Aaron D. Wyner (1994) G. David Forney, Jr. (1995) Imre Csiszár (1996) Jacob Ziv (1997) Neil J. A. Sloane (1998) Tadao Kasami (1999) Thomas Kailath (2000) Jack Keil Wolf (2001) Toby **Berger** (2002) Lloyd R. Welch (2003) Robert J. McEliece (2004) Richard Blahut (2005) Rudolf Ahlswede (2006)

Sergio Verdu (2007) Robert M. Gray (2008) Jorma Rissanen (2009) Te Sun Han (2010) Shlomo Shamai (Shitz) (2011) Abbas El Gamal (2012) Katalin Marton (2013) János Körner (2014) Arthur Robert Calderbank (2015) Alexander S. Holevo (2016) David Tse (2017)

Berger plaque



ទៅមាន ទេខ័រ Raymond Yeung

 BS, MEng and PhD degrees in electrical engineering from Cornell University in 1984, 1985, and 1988, respectively.







Raymond Yeung

- Introduce, for the first time in a textbook,
 - analytical theory of I-Measure and
 - geometrically intuitive information diagrams
 - Establish a one-to-one correspondence between Shannon's information measures and set theory.
- Rooted in works by G. D. Hu, by H. Dyckman, and by R. Yeung et al.



Chapter 6 THE *I*-MEASURE

In Chapter 2, we have shown the relationship between Shannon's information measures for two random variables by the diagram in Figure 2.2. For convenience, Figure 2.2 is reproduced in Figure 6.1 with the random variables X and Y replaced by X_1 and X_2 , respectively. This diagram suggests that Shannon's information measures for any $n \ge 2$ random variables may have a set-theoretic structure.

In this chapter, we develop a theory which establishes a one-to-one correspondence between Shannon's information measures and set theory in full generality. With this correspondence, manipulations of Shannon's information measures can be viewed as set operations, thus allowing 'he rich suite of tools in set theory to be used in information theory. Moreover, the structure of Shannon's information measures can easily be visualized by means of an



Figure 6.1. Relationship between entropies and mutual information for two random variables.

⁹⁵ R. W. Yeung, A First Course in Information Theory © Springer Science+Business Media New York 2002

Toby Berger with Berger plaque



Douglas Chan and 802.11n

Contributions to this amendment was received from the follo

Bill Abbott Santosh Abraham Tomoko Adachi Dmitry Akhmetov Carlos Aldana Dave Andrus Micha Anholt Tsuguhide Aoki Yusuke Asai Geert Awater David Bagby Raja Banerjea Kaberi Banerjee Amit Bansal Gal Basson Anuj Batra John Benko Mathilde Benveniste Bjorn Bjerke Yufei Blakenship Daniel Borges Douglas Chan Jerry Chang

Vinko Erceg Mustafa Eroz Stefan Fechtel Paul Feinberg Matthew Fischer Guido Frederiks Takashi Fukagawa Patrick Fung Edoardo Gallizio



Yuh-Ren Jauh

IEEE

 \geq

IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

Amendment 5: Enhancements for Higher Throughput

IEEE Computer Society

Sponsored by the LAN/MAN Standards Committee

IEEE 3 Park Avenue New York, NY 10016-5997, USA 29 October 2009 IEEE Std 802.11n[™]-2009 (Arnendment to IEEE Std 802.11[™]-2007 as amended by IEEE Std 802.11[™]-2008, IEEE Std 802.11[™]-2008, IEEE Std 802.11[™]-2008, and IEEE Std 802.11[™]-2008,

Hui-Ling Lou Adina Matache Laurent Mazet

Douglas Chan and 802.11n

September 2005

doc.: IEEE 802.11-05/0946r0

Improving IEEE 802.11 Performance with Cross-Layer Design and Multipacket Reception via Multiuser Iterative Decoding

Date: 2005-09-20

Authors:

Name	Company	Address	Phone	email
Douglas S. Chan	Cornell	School of Electrical	607-254-8818	dsc29@cornell.edu
Prapun	University	Engineering, Cornell University, Ithaca, NY 14853		ps92@cornell.edu
Jun Chen				jc353@cornell.edu
Toby Berger			607-255-1447	berger@ece.cornell.edu

Digital Communication Systems ECS 452

Asst. Prof. Dr. Prapun Suksompong

prapun@siit.tu.ac.th

Special Cases for Calculation of Channel Capacity

Channel Capacity: Special Cases

- Channel with Nonoverlapping Outputs (NO²)
 - There is only one non-zero element in each column of its **Q** matrix.
 - $C = \log_2 |\mathcal{X}|$ is achieved by uniform input probabilities. [4.30]
 - Ex. Noiseless Binary Channel: C = 1 [bpcu] [Ex. 4.27]
- Weakly Symmetric Channel
 - (1) all the rows of **Q** are permutations of each other and [Defn 4.36]
 (2) all the column sums are equal.
 - $C = \log_2 |\mathcal{Y}| H(\underline{\mathbf{r}})$ where $\underline{\mathbf{r}}$ is any row from the \mathbf{Q} matrix. [4.37] is achieved by uniform input probabilities.

• Ex. Binary Symmetric Channel: C = 1 - H(p) [bpcu]