Coding Theory

Paramate Horkaew

School of Computer Engineering
Institute of Engineering, Suranaree University of Technology

Lecture Outline

- The Coded Reality
- **Coding Concept**
  - Information
  - Entropy
  - Multivariable Formulation
- Transmission Channels
  - Transmission Matrix
  - Binary Channel and BSC
- Mutual Information
- Capacity of a Noisy Channel
  - Capacity of a BSC

The Coded Reality

การส่งคลื่นวิทยุผ่านอวกาศมายังโลก เป็นระยะทางหลายล้านกิโลเมตร ต้องผ่านสิ่งแวดล้อมที่ไม่พึงประสงค์หลายประการ เช่น สัญญาณรบกวน การลดทอนความแปรปรวน ฯลฯ แต่คลื่นวิทยุต้นทางมีกำลังส่งเพียงแค่ไม่กี่วัตต์ เท่านั้น

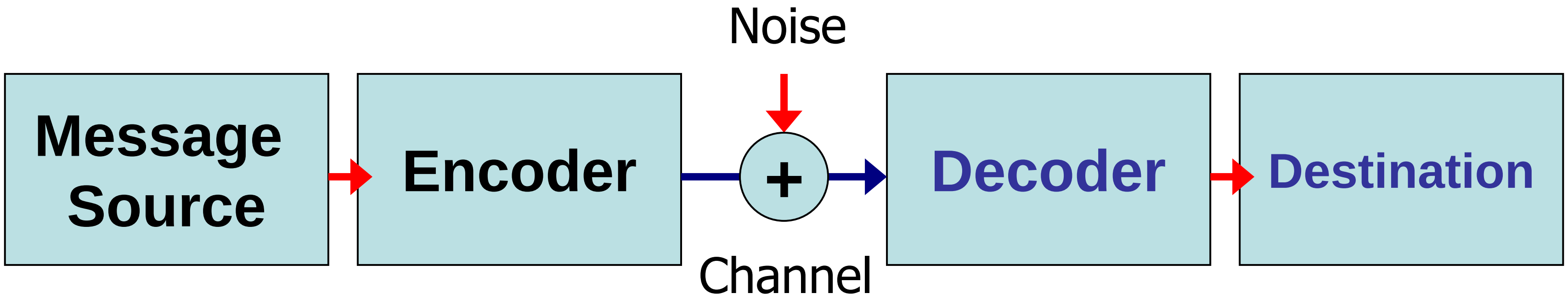
Coding Theory ว่าด้วยการส่งข้อมูลผ่านช่องสัญญาณ ที่มีสัญญาณรบกวน และการกู้คืนข้อมูลข่าวสารที่ด้านรับ, กระบวนการที่ทำให้ข่าวสารสามารถอ่านได้ง่าย

Richard Pinch, Coding Theory: The First 50 Years, **Plus Magazine**, 1997.

Coding Concept

กำหนดให้

- ข้อมูลอยู่ในรูปของ**เลขฐานสอง** (Binary Digits หรือ Bits)
- ข้อมูลส่งไปตามสายสัญญาณ ที่มีสัญญาณรบกวนแบบสุ่ม (Random Noise)
- ผู้ส่งไม่สามารถ ทำนายค่าของสัญญาณรบกวน ณ เวลาใดๆ ได้ แต่รู้**อัตรา**ของสัญญาณรบกวน (เช่น เป็น dB เทียบกับสัญญาณ)
- **การเข้ารหัสที่มี ภูมิต้านทาน ต่อสัญญาณรบกวน รหัสต้องมีความยาว** (จำนวน Bits) **มากกว่าข้อมูลต้นฉบับ**



Richard Pinch, Coding Theory: The First 50 Years, **Plus Magazine**, 1997.

The Concept of Information

Information คือ **ความรู้ใหม่**

Information สัมพันธ์กับ Uncertainty

พิจารณากล่องบรรจุลูกบอลดังต่อไปนี้

1. ลูกบอลสีดำ 1 ลูก ลูกบอลสีดำ 1 ลูก
2. ลูกบอลสีดำ 9 ลูก ลูกบอลสีขาว 1 ลูก
3. ลูกบอลสีดำ 999 000 ลูก ลูกบอลสีขาว 1 000 ลูก

จากทฤษฎีของความน่าจะเป็น พบว่า โอกาสที่จะทำนาย (*a priori*) ว่าลูกบอลที่จะหยิบออกมาในกรณีที่ 1 (ความน่าจะเป็นพอๆ กัน) ยากกว่า กรณีที่ 2 และ 3 (บอลน่าจะเป็นสีดำมากกว่า)

เมื่อเราหยิบลูกบอลออกจากกล่องแล้ว (*a posteriori*)

กรณีที่ 1 ไม่ว่าได้สีอะไร เราจะได้ ความรู้ใหม่ เสมอ (**คาดเดาไม่ได้**)

กรณีที่ 2 ถ้าหยิบได้สีดำ เราไม่ได้ความรู้ใหม่ (**คาดว่าน่าจะเป็นสีดำอยู่แล้ว**)

ถ้าหยิบได้สีขาว เราได้ความรู้ใหม่มากมาย (**คาดไม่ถึงมาก่อน**)

The Concept of Entropy

สมมติการทดลอง **E** ที่มี ผลลัพธ์ *m* กรณี ได้แก่ X = $\{x_1, x_2, \ldots, x_m\}$
และให้ผลลัพธ์แต่ละตัว x_i มีค่าความน่าจะเป็นที่จะเกิดขึ้น p_i
โดยที่ ผลรวมของ p_i สำหรับทุกๆ กรณี ($\Sigma_i\ p_i$) มีค่าเท่ากับ **1**

ความไม่แน่นอน ของการทดลอง E สามารถวัดได้ด้วย Entropy ซึ่งนิยามดังต่อไปนี้

$$H_b(X) = -\sum_{i=1}^{m} p_i \log_b p_i$$

เมื่อ	b = 2	หน่วยของ Entropy จะมีค่าเป็น *bit*
	b = e	หน่วยของ Entropy จะมีค่าเป็น *nat*
	b = 10	หน่วยของ Entropy จะมีค่าเป็น *decit*

ตัวอย่าง

The Information

สมมติการทดลอง **E** ที่มี ผลลัพธ์ *m* กรณี ได้แก่ X = $\{x_1, x_2, \ldots, x_m\}$
และให้ผลลัพธ์แต่ละตัว x_i มีค่าความน่าจะเป็นที่จะเกิดขึ้น p_i
โดยที่ ผลรวมของ p_i สำหรับทุกๆ กรณี ($\Sigma_i\ p_i$) มีค่าเท่ากับ **1**

ปริมาณของข่าวสารของการทดลอง E เมื่อกำหนด X = $\{ x_i \}$ นิยามโดย

$$I_b(x_i) = -\log_b p_i$$

จากนิยามข้างต้นอาจสรุปได้ว่า Entropy คือ Expected Value ของ Information (mean)

$$H_b(X) = E[I(x_i)]$$

$$= -\sum_{i=1}^{m} p_i \log_b p_i$$

Multivariate Information

สมมติตัวแปรสุ่ม (Discrete) X = $\{x_1, x_2, \ldots, x_m\}$
และให้ผลลัพธ์แต่ละตัว x_i มีค่าความน่าจะเป็นที่จะเกิดขึ้น p_i
โดยที่ ผลรวมของ p_i สำหรับทุกๆ กรณี ($\Sigma_i\ p_i$) มีค่าเท่ากับ **1**

สมมติตัวแปรสุ่ม (Discrete) Y = $\{y_1, y_2, \ldots, y_n\}$
และให้ผลลัพธ์แต่ละตัว y_k มีค่าความน่าจะเป็นที่จะเกิดขึ้น q_i
โดยที่ ผลรวมของ q_k สำหรับทุกๆ กรณี ($\Sigma_k\ q_k$) มีค่าเท่ากับ **1**

ดังนั้นสำหรับตัวแปรสุ่ม (X, Y) = { (x_i, y_k) } มีความน่าจะเป็น p_{ik} = P { X=x_i, Y=y_k }

Entropy ของตัวแปรสุ่ม (X, Y) นิยามด้วยสมการ

$$H(X,Y) = -\sum_{i=1}^{m}\sum_{k=1}^{n} p_{ik} \log p_{ik}$$

Useful Formulae

สำหรับระบบที่ประกอบด้วยตัวแปรสุ่ม 2 ตัว (X, Y) Entropy ของตัวแปรสุ่ม Y เมื่อกำหนดตัวแปรสุ่ม X (Conditional Entropy) นิยามได้ดังนี้

$$H(Y|X = x_i) = -\sum_{k=1}^{n} p_{k|i} \log p_{k|i}$$

$$H(Y|X) = \sum_{i=1}^{m} p_i H(Y|X = x_i)$$

ความสัมพันธ์ของค่า Entropy ในรูปแบบต่างๆ จึงเขียนได้ดังนี้

$$H(X,Y) = H(X) + H(Y|X)$$

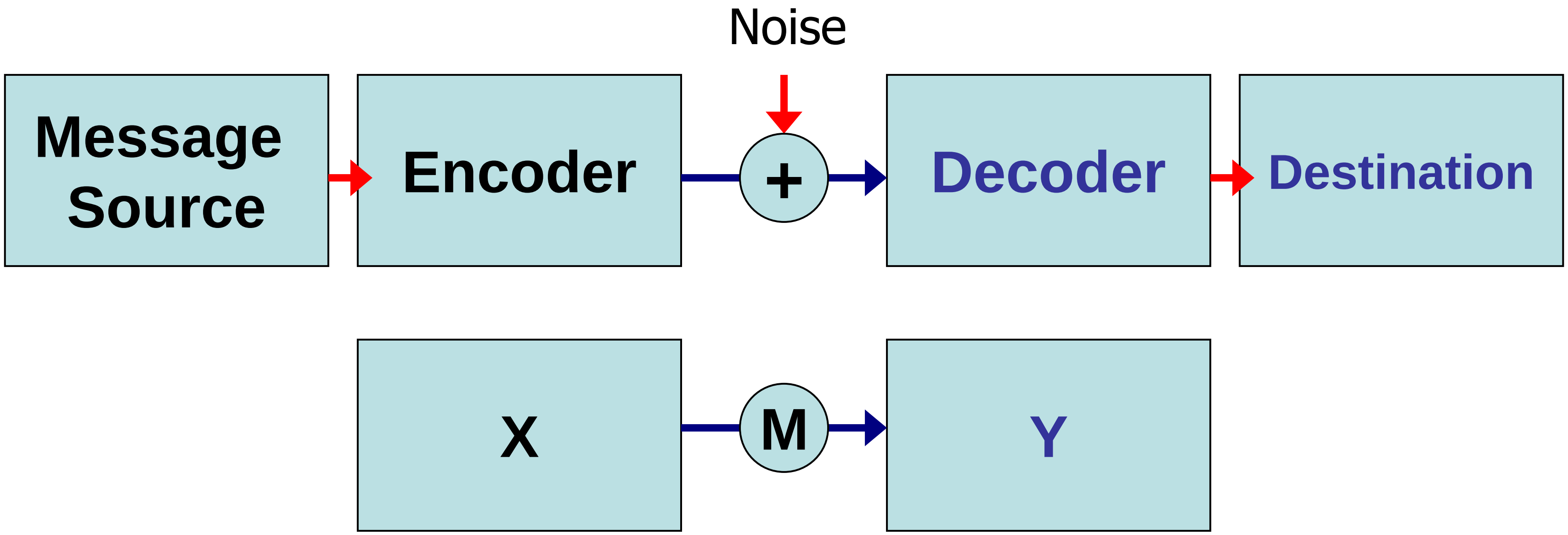
$$H(X,Y) \le H(X) + H(Y)$$

$$H(X,Y) = H(X) + H(Y)$$

X และ Y เป็นอิสระต่อกัน

Transmission Channel

การสื่อสารสามารถแสดงในรูปของแบบจำลองทางคณิตศาสตร์ของช่องสัญญาณ ได้ดังนี้



- Input ได้แก่ X ให้กำเนิดสัญลักษณ์จากภาษา A = $\{x_1, x_2, \ldots, x_m\}$
- Output ได้แก่ Y ให้กำเนิดสัญลักษณ์จากภาษา B = $\{y_1, y_2, \ldots, y_n\}$
- ช่องสัญญาณ Transmission Matrix [T] นิยามด้วย $t_{ik} = p_{k/i}$

Suranaree University of Technology

Transmission Matrix

- Input ได้แก่ X ให้กำเนิดสัญลักษณ์จากภาษา A = $\{x_1, x_2, \ldots, x_m\}$
- Output ได้แก่ Y ให้กำเนิดสัญลักษณ์จากภาษา B = $\{y_1, y_2, \ldots, y_n\}$
- ช่องสัญญาณ Transmission Matrix [T] นิยามด้วย $t_{ik} = p_{k/i}$

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} p_{1|1} & p_{1|2} & \cdots & p_{1|m} \\ p_{2|1} & p_{2|2} & \cdots & p_{2|m} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n|1} & p_{n|2} & \cdots & p_{n|m} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix}$$

ความน่าจะเป็นของการเกิด y_1 มีค่าเท่ากับผลรวมของ ความน่าจะเป็นของการเกิด y_1 ถ้าทราบว่าเกิด x_i คูณกับความน่าจะเป็นของการเกิด x_i

Binary Channel

- Input ได้แก่ X ให้กำเนิดสัญลักษณ์จากภาษา A = {*0*, *1*}
- Output ได้แก่ Y ให้กำเนิดสัญลักษณ์จากภาษา B = {*0*, *1*}

$$\begin{bmatrix} p(Y=0) \\ p(Y=1) \end{bmatrix} = \begin{bmatrix} p_{y=0|x=0} & p_{y=0|x=1} \\ p_{y=1|x=0} & p_{y=1|x=1} \end{bmatrix} \begin{bmatrix} p(X=0) \\ p(X=1) \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} p(X=0) \\ p(X=1) \end{bmatrix} \Rightarrow Y = X$$

ถ้าช่องสัญญาณถูกรบกวน ซึ่งมีความน่าจะเป็นในการเกิดความผิดพลาด = q

$$\begin{bmatrix} p(Y=0) \\ p(Y=1) \end{bmatrix} = \begin{bmatrix} 1-q & q \\ q & 1-q \end{bmatrix} \begin{bmatrix} p(X=0) \\ p(X=1) \end{bmatrix}$$

Binary Symmetric Channel

Mutual Information

Mutual Information I ของการส่งข้อมูล X ผ่าน M ไปยังด้านรับ Y นิยามโดย

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

ความหมายของสมการ – *ช่องสัญญาณทำให้เราแปลกใจได้แค่ไหน?*

ปริมาณข่าวสาร (ความรู้ใหม่ I) หาได้จากความแตกต่างระหว่าง ความไม่แน่นอนของสัญญลักษณ์ที่ **output** เมื่อเราไม่ทราบอะไรเลย กับ ความไม่แน่นอนเมื่อเราทราบข้อมูลเกี่ยวกับสัญลักษณ์ **ที่ส่งมา**

ปริมาณข่าวสาร (ความรู้ใหม่ I) หาได้จากความแตกต่างระหว่าง ความไม่แน่นอนของสัญญลักษณ์ที่ **input** เมื่อเราไม่ทราบอะไรเลย กับ ความไม่แน่นอนเมื่อเราทราบข้อมูลเกี่ยวกับสัญลักษณ์ **ที่รับได้**

Capacity of a Channel

ความจุของช่องสัญญาณหาได้จากสมการ

$$C = \max_{p(X)} I\left(X;Y\right)$$

ความหมายของสมการ – *ช่องสัญญาณต้องรองรับข้อมูลได้มากแค่ไหน?*
เมื่อกำหนดสิ่งต่อไปนี้
- ความน่าจะเป็นของสัญญลักษณ์แต่ละตัวที่ input p (X)
- คุณสมบัติเชิงสัญญาณรบกวนของช่องสัญญาณ (Transmission Matrix)

สามารถคำนวณค่าต่อไปนี้ได้
- H (X), H (Y), H (X, Y), H (Y | X) และ I (X, Y)
- C คือค่า I (X, Y) ที่มากที่สุด สำหรับค่า p (X) ที่เป็นไปได้ค่าหนึ่ง

Capacity of a BSC

จงหาปริมาณข่าวสารของช่องสัญญาณแบบ Binary Symmetric Channel

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

เมื่อกำหนดให้ช่องสัญญาณมีคุณสมบัติดังต่อไปนี้

$$\begin{bmatrix} p(Y=0) \\ p(Y=1) \end{bmatrix} = \begin{bmatrix} 1-q & q \\ q & 1-q \end{bmatrix} \begin{bmatrix} p(X=0) \\ p(X=1) \end{bmatrix}$$

จงหาความจุของช่องสัญญาณ

$$C = \max_{p(X)} I(X;Y)$$

และค่า p (X) ที่ช่องสัญญาณมีปริมาณข่าวสารมากที่สุด (ที่ C)

Conclusion

- The Coded Reality
- **Coding Concept**
  - Information
  - Entropy
  - Multivariable Formulation

- Transmission Channels
  - Transmission Matrix
  - Binary Channel and BSC
- Mutual Information
- Capacity of a Noisy Channel
  - Capacity of a BSC