技術解說

情報理論概說

趙 成 晧*

1940년대 shannon에 依해서 體系를 이룬 情報理論은 비단 現代 通信系統에 哲學을 이룰뿐아니라 그것의 應用 範圍는 藝術 言語學등에서 硏究가 行하여 졌으며, 독자적인 學問으로서도 계속 成長하고 있다. 따라서 그 應用 範圍도 擴大될 것으로 보여진다.

이글에서는 情報理論의 간략한 起源과 그것의 基本的인 理論을 槪說코저 한다.

I. 情報理論의 起源

現代文明은 무엇보다도 신속하고 거대한 量의 通信을 취급할 수 있는 通信수단에 依存함이 크다고 할 수 있다. 地球上 어느 地域에서 發生한 事件이나 달에서 作業하는 宇宙人의 모습을 그순간 순간을 편안히 거실에서 TV를 通해서 보고 들을 수 있는 것을 당연히 여긴다는 것은 매우 놀라운 사실이 아닐 수 없다. 때는 大西洋航海時代로 1832年 Morse가 實用性있는 電信장치가 電氣的인 通信수단의 총아로 등장한 以來 通信에 關한 여러 가지 문제가 제기 되었다. 通信의 目的과 性格에 따라 惹起되는 문제가 多樣하지만 대체로 共通되는 點은 同時에 많은 通信量을 신속히 여러가지 방해를 받고 있는 매개체를 通해서 目的地에 보내어 이곳서 될 수 있는한 정보의 손실이 없이 受信하려는 것이다. 이것을 위해서 通信方式을 연구 개선 하든가 또는 裝置를 고안하게 된다. Morse가 전신장치를 고안 하였을 시 當面한 문제는 符號를 定하는 것이었다. 初期에 符號는 現在 使用하는 Morse부호가 아니고 一連의 長短의 線으로 數를 表示하고 이 番號로서 부호책에서 해당하는 말(Word)을 찾아 내었다. 이 방법이 오늘날 效率的인 것으로는 알려졌으나 當時에는 複雜하고 조잡한 作業이 되었다. 오늘날 볼수 있는 Morse부호는 1838년에 完成되었다. 이부호는 Dot, Dash 및 Space로 되어 Dot와 Dash의 조합으로 글자(Letter)를 表示하게 된다. 이 부호는 매우 잘 짜여져서 使用頻度가 큰자는 짧은 부호가 되도록 하였고 빈도가 크지 않은 글자는 비교적 긴 부호가 되도록 하였다. 오늘날 이것을 다시 改良한다 해도 15%程度 밖에 개선치 못한다고 하니 當時 Morse로서는 오늘날 情報理論의 核心을 이루는 Message의 符號化(Encode)를 즉감적으로 잘 理解하였던것 같다. 그러나 곧 이어서 1875년 Bell이 電話를 고안하여 내고난 뒤는 이러한 오늘날 情報理論의 실마리를 주는 Encoding 문제는 오랜동안 關心 밖으로 되었다. 20세기 初에 Nyquist 및 Hartley가 電信速度에 關하여 단편적인 연구를 수행 하였을 뿐 세계제2차대전까지도 通信에 대한 根本的인 폭넓은 振學的 原理는 이루어지지 않았다. 特히 세계제 2 차대전중 通信工學에 놀라운 發展을 보게되어 매우 精巧한 기구를 通信에 使用하게 되었고 새로운 通信方式도 發展을 보게되었다. 特히 이 期間동안 레이더를 위한 Filter 問題가 Kolmogoroff 및 Wiener에 依해서 각각 독자적으로 들어 내어져서 연합군의 전쟁승리에 보이지 않는 要因이 되었다. 2차대전 末쯤 Shannon은 그때껏 이루어 놓은 여러가지 통신방식을 비교 검토 하려고 試圖하였다. 그리고 이들 통신 방식의 長短을 비교 할수 있는 根本的인 方法을 求하려 하였다. 따라서 通信 信號를 解析 하는데에도 어느 單一 通信信號를 취급 하려 하지 않고 信號群 또는 可能한 모든 形態의 信號들에서 선택된 어느 信號도 적절히 취급하는 問題를 다루었다. 그의 이러한 思

* 미네소타 대학교

想은 1948년 Bell 기술잡지에 "通信의 數學的 原理"라는 論文에 發表되었으며 오늘날 情報理論의 基幹을 이루게 되었다. 그후 이 分野에 많은 사람에 의해서 체계적인 발전이 이루어졌으며 오늘날에는 實用的인 면도 점차 커가고 있다. 또한 이 情報理論은 必然的으로 符號理論(Coding Theory)을 개척하게 하였다. Coding Theory는 이를 뒷받침 하는 現代의 代數學을 써서 새로운 通信工學의 分野로 출현 하였다.

Ⅱ. 情報理論 序言

情報理論은 通信系統(Communication System)의 基本的인 問題를 취급하는 數學的인 原理(Mathematical Theory)이다. 다른 모든 數學的理論에서 그렇듯 취급하는 相對(object)를 數學的인 model로 하여 이 Model의 特性과 다른 model과의 關係를 數學的으로 관계 지운다. 一般的인 通信系統을 그림 1과 같이 表示할 수 있다.

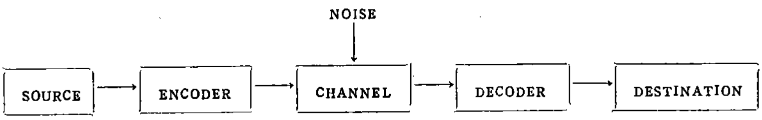

그림 1 一般的 通信系統

그림 1에서 보는 바와같이 情報理論에서는 Source의 情報測定(Information Measurement), Channel의 容量(Capacity) 그리고 Encoding, decoding이 主要 Topic이 되고 이들을 說明하는데 特히 確率理論을 主要한 도구로 使用한다.

Ⅲ. 情報源, 情報의 測定 및 符號化 (Information Source, Information Measurement and Source Encoding)

現象界에는 정확히 예측이 되는것 (Deterministic System)과 그렇지 못한것 (Undeterministic System)이 있다. 天體의 運行은 좋은 Deterministic System의 一例이다. 天文學者들은 100년뒤의 천체의 위치(물론 상대적인 위치이지만)를 정확히 예측 할수 있다. 그러나 주사위를 던졌을 경우 점수, 인간의 언어 행위, 공기중 작은 粒子의 위치는 앞서 말한 Deterministic System의 法則으로는 說明할 수 없다. 이러한 System은 Random 또는 Statical Model로 다루어 지게된다. 情報源도 Undeterministic system에 속한다. 따라서 Information Source는 통계적인 방법으로 설명한다. 엄밀히 평형된 주사위를 情報源으로 하였다면 각 점수는 확율 1/6로서 나타나게 된다. 가장 간단한 情報源은 동전이다. 동전을 던지면 앞면과 뒷면은 확율 1/2로 출현한다. 7個의 文字(또는 event)를 갖고 있는 情報源에서 文字의 확율이 $P(a_i)$이라 할시 이 情報源으로 부터 文字 a_i를 받았을시 情報 I를 $I \triangle \log \frac{1}{P(a_i)}$로 한다. 특히 對數의 Base가 2일시 I의 단위는 bit라고 한다. 동전을 던져서 앞 또는 뒷면이 나왔을 때 주는 정보는 1bit이다. 어느 지역의 기후가 개이는 확율이 $\frac{1}{2}$, 흐리는 확율이 $\frac{1}{4}$, 비가오는 확율이 $\frac{1}{8}$, 안개가낄 확율이 $\frac{1}{8}$, 이라 한다. 이경우 각 event의 自己情報(Self information)는 개임은 1bit, 흐림 2bit, 비 3bit, 안개 3bit이 된다. 즉 가장 적은 기대의 event의 情報가 크다는 것은 우리의 경험적인 개념과 잘 일치한다. 하지만 아무리 출현 가능성이 없는 event일지라도 우리의 흥미가 없다면 그러한 event의 출현은 아무 정보의 가치가 없다고 볼 수 있다. 즉 理論的인 정보의 측정은 주관적인 흥미 라든가 별다른 뜻은 생각지 않는다. 理論的인 情報測定에 실제적인 느낌을 갖기 위해서 TV의 한 영상과 Radio 아나운서를 예를 들어 보기로 하자. TV의 영상은 밝기의 정도가 틀리는 많은 점으로 되어있다. 대략 이러한 점은 500개의 횡선과 600개의 종선으로 $500 \times 600 = 300,000$점으로 되어 있고 각점의 밝기의 정도는 10레벨이라면 가능한 영상면의 수는 10^{300000}개의 각기 다른 영상면이 된다. 만일 이들의 출현 확율이 모두 같다면 그 확율은 $1/10^{300000}$이고 한영상면의 自己情報 I는 $I = 300000 \log 10 = 10^6$ bits가 된다. 이제 Radio 아나운서가 10,000개의

단어를 구사해서 한번 보도 하는데 1,000단어를 취하여 쓴다면 가능한 보도의 수는 $10,000^{1,000}$이고 그중 한보도의 확율은 $1/(10,000)^{1,000}$이다. 따라서 한보도의 自己情報는 $I = 1,000\log 10,000 = 1.3\times10^4$ bits 이다. 여기서 보면 한순간 TV 의 한영상은 Radio 아나운서 1,000마디 말보다 더많은 情報를 제보한다고 볼수 있다.

情報測定으로 중요성을 갖는것은 이 自己情報보다 이것에 대한 情報源, 전체의 평균치인 Entrophy 이다. Entrophy H는 다음과 같이 정의된다.

$$H = \sum_{k=1}^{K} P(a_k)\log\frac{1}{P(a_k)}$$

따라서 Entrophy H는 情報源에서 한개의 文字를 받았을 시 얻을 수 있는 평균 情報인 것이다. Entrophy H의 단위도 또한 대수의 Base가 2일시 bits로 표시되고 특별히 情報源에서 秒마다 한개의 文字를 내놓을 때 단위 시간당 Entrophy 는 H bits/t_s이다. 위에 예를 들은 날씨의 情報源의 Entrophy 는 1.75 bits 이다.

情報源에 대해 더 생각하여 보면 앞서 말한 情報源으로서 주사위라든가 동전과 날씨와는 좀 다른성질이 있다. 즉 주사위의 점수 또는 동전의 앞뒷면의 출현은 개개의 출현이 먼저 출현한 것과 독립되어서 출현 한다. 그러나 날씨에서 각 event 의 출현은 앞서 있었든 event 에 관계를 갖고(통례적 의미에서) 출현한다. 情報源에서 각 文字가 독립된 확율로 출현할시 이 情報源을 Memoryless Source 라고 한다. 실제의 Information Source 는 Zeromemory Source 가 아니고 각 文字의 출현이 앞서 출현한 m 개의 文字와 관계가 주어져 출현하는 Markov Source 이다. 인간의 언어 행위로 보는 情報源은 이러한 Markov Source 에 속한다.

이상에드는 情報源은 Discrete Source 이었다. Nondiscrete Source 로서는 Source 의 out put 가 연속적인 것을 들수 있다. 그러나 이러한 Source 도 단위시간에 유한한 수 만큼 Sampling 하여서 Discrete Source 로 고칠 수가 있다. 하지만 실제적인 면에서 Distortion 이 따르게 된다.

情報源의 out put 를 Channel 로 보내기 위해서 부호화하지 않으면 안된다. 실제적인 편리한 점에서 情報源은 二進부호(Binary Code)로서 符號化되고 다시 이것이 Channel 에 맞도록 다시 符號化된다. 전자를 Source encode, 후자를 channel encode 라고 한다. Source encoder 에서는 문제가 단위시간에 주어진 Source 를 부호화 하기 위해서 얼마나 많은 Binary digit 가 필요한가 가 주요 관심사다.

符號化하는데 일반적인 조건으로서는 符號는 유일하게 decode 되어야 한다. 또한 符號는 일연의 Code word 에서 다른 부호를 기준하지 않고 순간순간 decode 될 수 있어야 한다. 다음 code 에서 이점을 검토하면

Source letter	확율	Code 1	Code 2	Code 3	Code 4
S_1	$\frac{1}{2}$	0	0	00	0
S_2	$\frac{1}{4}$	1	01	01	10
S^3	$\frac{1}{8}$	10	011	10	110
S_4	$\frac{1}{8}$	11	0111	11	111

Code 1은 情報源의 文字에 二進數로서 번호를 붙인것인데 이것은 유일하게 decode 도 안되고 순간순간 decode 되지도 못한다. Code 2는 Uniquely decodable 이지만 instantaneous Code 는 못된다. Code 3, 4는 Uniquely decodable and instantaneous Code 이다. 다시 Code 3과 Code 4의 평균길이가 얼마인가 계산 하여보면 Code 3는 2 Bits Code 4는 $1\frac{3}{4}$bit 로 Code 4가 Code 3보다 12.5% 더 효율이 높음을 알수 있다. 그러면 우리는 평균길이가 가장 짧은 符號의 한계가 어느정도 일가가 문제가 된다. 여기에 대해 Shannon 의 첫정리는

$$H(s) \leq L \leq H(s)+1$$

임을 보인다.

여기서 L은 Code 의 평균길이 이고 H(s)는 情報源의 Entrophy 이다. 따라서 각각의 情報源의 文字 a_i를 $-\log p(a_i) \leq l_i < -\log p(a_i)+1$ 되게끔 선택하면 된다. Shannon 의 정리는 Code 길이의 Bound 를 정해주지만 如何히 이러한 instantaneous Code 를 구성하느냐는 제시하지 않는다. Compact Code 를 구성하는 것은 Huffman 의 방법으로 구성할 수 있다. 앞서 例를든 Code 중 Code 4는 Huffman 의 方法으로 求한 Compact Code 이다. 이경우 Entrophy 는 $H(s) = 1\frac{3}{4}$bits 이고 특히 Lav

=H(s)가 되었다. Channel encoding 은 다음절에서 설명 하기로 한다.

IV. Information Channel 과 Channel encoding

實際의 通信의 전송매개체는 送信과 受信을 연결하여 주면서 또한 그것 자체의 作用으로 通信의 전송을 방해 한다. 즉 전송하는 과정에 통신내용에 착오를 가져 오게 된다.

Information Channel 의 特性도 情報源에서 처럼 統計的인 方法으로 나터내는 것은 극히 자연스럽고 합리적이다. Information Channel 은 가능한 모든 入力 文字와 이에 의한 모든 出力文字, 그리고 각 入力 文字에 對한 出力文字의 조건확율 $P(b_j/a_i)$로서 표시된다.

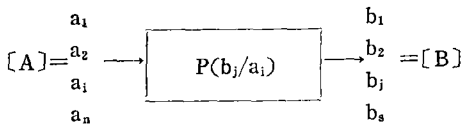

그림 2 Information Channel

특히 이러한 類의 Channel 을 Discrete memoryless Channel 이라고 한다.

이제 Channel 의 統計的인 관계를 알기 위해서 다음과 같이 入力文字 A와 出力文字 B의 관계를 생각한다.

$$I(A,B)=\sum_{A,B} P(a_i.b_j)\ log\ \frac{P(a_i,\ b_j)}{P(a_i)\ P(b_j)}$$

여기서 $I(A,B)$를 相互情報(mutual Information)라고 한다. $P(a,b)=P(a)P(b/a)$ 인고로 $I(A,B)$는 고쳐 쓰면

$$I(A,B)=\sum_{A,B} P(b_j/a_i)\ P(a_i)\ log\frac{P(b_j/a_i)}{P(b_j)}$$

$$=\sum_{A} P(a_i)\ log\frac{1}{P(a_i)}-\sum_{B} P(b_j)$$

$$\sum_{A} P(a_j/b_j)\ log\ \frac{1}{(a_i/b_j)}$$

따라서 $I(A,B)=H(A)-H(A/B)$

여기서 $H(A)=\sum_{A} P(a_i)\ log\frac{1}{P(a_i)}$ 즉 Source 의 Entrophy 이고

$$H(A/B)=\sum_{B} P(b_j)\ P(a_j/b_j)\ log\frac{1}{P(a_i/b_j)}$$

$H(A/B)$는 A의 B에 대한 Equivocation 이라고 한다. $I(A,B)$는 또한 다음과 같이 나타낼 수도 있다.

$$I(A,\ B)=H(B)-H(B/A)$$

相互情報는 Channel 의 出力에서 文字당 얻을 수 있는 평균 情報이고 이 정보는 이 Channel 을 지나 오는 동안 $H(A/B)\geq 0$ 만큼 감소 된것이다. 두개의 극단적인 경우를 생각하여 보기로 하자. 入力文字와 出力文字 AB가 통계적으로 獨立이라 한다면 $P(b/a)=P(b)$이다.

따라서 $H(A/B)=\sum_{A} P(a_i/b_j)\ log\frac{1}{P(a_i/b_j)}$

$$=\sum_{A} P(a_i)\ log\frac{1}{P(a_i)}=H(A)$$

그리고 $I(A,B)=H(A)-H(A/B)=0$

즉 이 Channel 의 出力文字를 받아도 아무 정보도 받지 못한다. 반대로 완전무결 한 Channel 즉 Noiseless Channel 의 경우는 $P(a/b)=1$일시 $M(A/B)=0$이고 $I(A,B)=H(A)$가 되어서 이 Channel 은 入力情報를 完全히 전달 한다.

相互情報 $I(A,B)$는 Channel 자체의 統計에도 관계 하지만 또한 入力 文字群의 統計에도 관계된다. 즉 $I(A,B)$는 入力文字群의 分布의 함수이다

$I(A,B)$의 최대값을 이 Channel 의 容量(Capacity)이라고 한다. 實際로 일반적인 Channel 의 容量을 계산하는 것은 용이 하지는 않다. 그리고 이 容量은 Channel 자체만의 統計로서 定하여진다. 특별히 Symmetric Discrete memoryless Channel 에서의 容量은 入力文字群의 각 文字가 同一한 確率을 갖을시 相互情報를 計算함으로써 容量을 求할 수 있다.

Discrete memoryless Channel 로 형태가 가장 간단 하면서 理論的으로나 實際的으로도 중요한 Binary Symmetrical Channel 에 對하여 생각 하기로 한다.

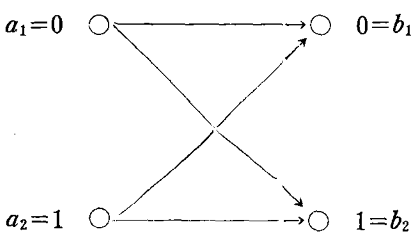

그림 3 Binary Symmetrical Channel

그림 3에서 보는 바와 같이 $P(b_1/a_1)=P(b_2/a_2)=\bar{P}$, $P(b_2/a_1)=P(b_1/a_2)=P$ 로서 P는 오차가 생길 확율이다. $I(A,B)$를 알기 위해서

$$H(B)=\sum_{j=1}^{n} P(b_j)\ log\frac{1}{P(b_j)}$$

$$H(A/B)=\sum_{i=1}^{2} P(a_i) \sum_{j=i}^{2} P(b_j/a_i)\ log\frac{1}{P(b_j/a_i)}$$

특히 $P(a_1)=w_1$, $P(a_2)=w_2$ 그리고 $w_1+w_2=1$이면

$$H(B)=(w_1\bar{p}+w_2p)\ log\frac{1}{w_1\bar{p}+w_2p}+(w_1p+w_2\bar{p})\ log\frac{1}{w_1p+w_2\bar{p}}$$

$$H(B/A)=P\ log\frac{1}{p}+\bar{P}\ log\frac{1}{\bar{p}}$$

위에서 求한 $H(B)$ 및 $H(A/B)$에 의해서

$$I(A,B)=(a_1\bar{p}+w_2p)\ log\frac{1}{w_1\bar{p}+w_2p}+(w_1p+w_2\bar{p})\ log\frac{1}{w_1p+w_2\bar{p}}-\left(p\ log\frac{1}{p}+\bar{p}\ log\frac{1}{\bar{p}}\right)$$

특별히 $w_1=w_2=\frac{1}{2}$이면

$I(A,B)\ \max=1-(p log\frac{1}{p}+\bar{p} log\frac{1}{\bar{p}})$되어

BSC의 容量은 대수의 Base가 2일시 $C=1-(p log\frac{1}{p}+\bar{p} log\frac{1}{\bar{p}})$ bits/binit가 된다. 그리고 $P+\bar{p}=1$이고 이들의 분포에 의한 容量 C의 變化는 그림 4와 같다.

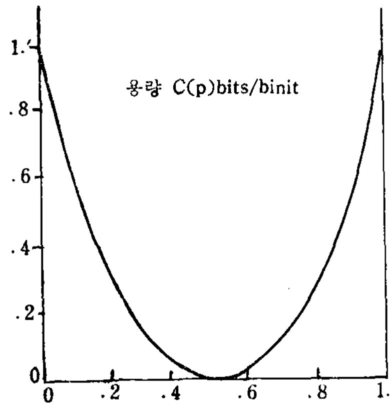

그림 4 BSC의 容量

위에서 보다 바와 같이 情報는 Channel을 通하여 가는 過程에서 손실을 가져온다. 그리하여 문제는 이러한 信頼性 없는 Information Channel을 통해서 어느 程度信頼性 있게 情報를 보낼 수 있느냐 하는 것과 그 방법인 것이다. 앞서든 동전의 例서 처럼 동일 확율의 단지 두개의 文字만 있는 情報源을 二進符號로 하여서 BSC를通해서 가는 過程을 생각 하기로 한다. 이제 情報源의 文字 a_1을 0으로 a_2를 1 로 하여 BSC를 通할시 Channel 出力에서 한 文字를 받았을 경우 誤差의 確率은 $P_E=P$이다. 다음 $a_1=0$ $a_2=1$로 하는 대신 $a_1=000$, $a_2=111$ 이라 하자, 즉 한 Binits를 使用하는 대신 文字當 3Binits를 使用한다. 이때 Channel의 出力 측에 可能한 모든 符號는 000, 001, 010, 100, 011, 101, 110, 및 111이다. 그리고 多數의 원측을 써서 000, 001, 010, 100은 000로서 011, 101, 110, 111은 111로서 받아 드릴때 誤差의 確率은 $P_E=P^3+3P^2\ P$로서 만일 $P=.01$이라면 $P_E\approx3\times10^{-4}$가 된다. 한개 Digit를 쓸때의 誤차의 3%程度로 減少시켰다. 5개의 Digit를 써서 할때의 오차확율은 $P_E=P^5+5P^4P+10P^3P^2\sim10^{-5}$되어서 .1%程度로 誤差를 감소 시킬 수 있다. 이렇게 符號에 Digit를 증가시키면 증가 시킬수록 오차의 확율은 감소되어 간다. 이렇게 해서 얻는 利點은 단위 시간당 보낼 수 있는 情報를 감소 시켜서 얻는 것이다. 오차의 확율을 무한소로 하기 위해서 단위 시간당의 情報도 무한소로 하지 않으면 안된다. 오차의 확율과 Message Rate의 관계가 그림 5에 도시 되었다.

그림 5에 도시 된것과 같이 단순히 Digit를 반복하여서 符號化하는 방법외에 다른 더 효율적인 符號化方法의 존재 여부를 묻는다면 이물음에 대해서 Shannon의 정리는 긍정적인 대답을 하였다. 즉 Message Rate를 一定히 하고 符號의 길이를 길게 하면 오차의 確率을 任意로 작게 할수 있다. 위에서 例든 BSC의 경우 오차의 확율 P_E는

$$P_E\leq\delta(n)+M2^{-nC} \qquad 이다.$$

위식에서 M은 文字의 數, C는 BSC의 容量 함수 $\delta(n)$은 符號의 길이 n이 크면 임의로 작게 할 수 있다. 위식에서 Message Rate $R=\frac{\log M}{n}$

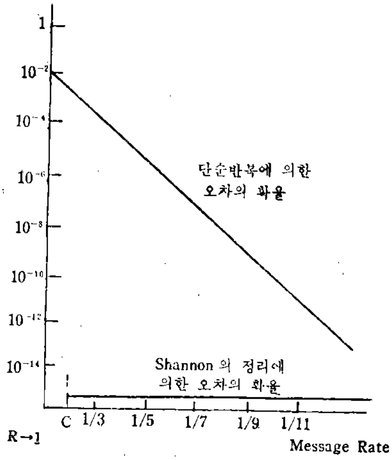

그림 5 Message Rate 와 오차의 확율관계

$\leq C$ 이며는 P_E는 n을 증가 시켜서 원하는 만큼 작게 할수가 있다. 그러나 여기에서 주의 할점은 길이가 n Binary Digits 인 부호 중에서 선택한 모든 M개 부호組들이 동일한 오차의 확율을 갖은 것은 아니다. Shannon 의 정리는 $M \leq 2^{nC}$ 일시, n이 매우 크면 2^n 개의 모든 可能한 부호중에서 선택한 M개의 부호組들중 오차확율을 任意로 작게하는 M개 부호組를 선택 할수 있다는 것이다. 하지만 如何히 이 부호조를 찾아 내느냐 하는 것은 또 다른 문제이다. 따라서 情報源을 위한 符號化(Source encoding)와 Channel 을 위한 符號化(Channel encoding)은 문제의 방향이 다르게 된다. 즉 전자는 단위시간에 情報源의 出力을 符號化하기 위해서 얼마나 많은 Digit 가 필요한가가 주요문제 이고 후자의 경우는 주어진 Binary Data 를 Channel 의 출력측에서 如何히 原來의 Data로서 再生할 수 있도록 하느냐 하는 것이 주요 문제가 된다.

Shannon 의 정리 2 의 근거는 Random Coding 에 의한것이 었다. M개의 부호를 2^n개의 부호중에서 랜덤으로 끄집어 내는 것이다. 이렇게 해서 가능한 모든 M개의 부호조는 2^{nM}개가 되고 그중 적어도 한組는 우리가 원하는 부호組인 것이다. 그러나 Random Coding 의 方式은 실제적이 못된다. 현재로는 이러한 Random Coding 을 실현 할만한 기구를 제작 한다는 것은 거의 불가능 한것이다. 例로서 n=25인 부호를 제작한다면 모든가능한 부호의 수는 $2^{25} \approx 3.4 \times 10^7$이며 이중 $M=2^{20} \approx 10^6$개의 부호를 선택한다면 선택하는 방법은 $2^{45} \approx 4.0 \times 10^{13}$가 되어 이것 자체가 어려운 일이고 어느 부호군을 정한다 하여도 이것이 원하는 최선의 것인지의 여부를 판단키 어려운 점이다. 어떻게 좋은 부호를 제작하느냐 하는데 있어서 Random Coding 은 공학적인 見地에서는 결코 良策이 못 된다는 사실은 정보이론의 학자를 다소 섭섭하게 하는 점이기도 하다. 그러나 이러한 점에서 다시方 向을 돌려서 부호를 제작하는데 Deterministic Methods 를 시도 하는 것은 당연한 처사일 것이다.

V. 結 言

以上 情報理論의 起源과 Shannon 의 정리를 중심으로 그 理論을 概述하였다. 情報理論은 앞서 말한바와 같이 現代 Data 通信에 基本的인 길잡이가 된다. 通信工學의 모든 理論的인 문제를 情報理論에 依據하여서 說明하는 것이 타당 하다는 것은 아니나 Shannon 이 理論的 체계를 세운 以來 情報論은 많은 점이 발전되었으며 實際응용면이 커가는 것도 사실이다. 情報理論으로 인해서 발전을 보게된 符號理論에 依한 여러가지 부호는 Data 通信의 一種의 Carrier 役을 하고 있으며 디지털 계산기 내에서도 부호는 중요한 役을 하고 있다. 情報理論이 通信工學외에 다른 분야에서 얼마나 더 應用될지는 아직 未知에 속하나 앞서 말한바와 같이 몇몇 분야에 연구가 수행된것으로 보아서 더 확장될것으로 보인다. 이분야에 관심이 있는 사람을 위해서 情報理論에 중요한 참고문헌을 붙였다.

참 고 문 헌

1. Abramson, N. (1963) Information Theory and Coding, McGraw-Hill, New York.
2. Ash, R. B. (1965) Information Theory, Interscience Publisher, New York
3. Bell, D. A. (1953) Information Theory and Its Engineering Applications. Sir Isaac Pitman & Sons, Ltd., London
4. Blackwell, D. (1957) "The Entrophy of

Functions of Finite-State Markov Chains, " Transaction of the First Prague Conference on Information Theory, Statistical Decision Functions, and Random Processes, Publishing House of the Czechosolvak Academy of Sciences, Prague, 13—20

5. Bose, R.C., and D.K. Ray-Chaudhuri (1960), "On a Class of Error Corecting Binary Group Coder," Infor; and Control, 3, 68—79
6. Dobrushin, R.L. (1959), "General Formulation of Shannons Main Theorem in Information Theory," Usp. Math. Nauk, 14, No.6(90), 3—104, translated in Am. math Soc. Translations, 33, Series 2, 323—438
7. Eisenberg, E.(1963) "On Channel Capacity," Techncal Memorandum M-35, Electronic Research Lab. Univ. of California, Berkelely. Calif
8. Elias, P.(1955) „Coding for Noisy Channels," IRE Convention Record
9. Fano, R.M.(1961) Transmission of Information, MIT Press, Cambridge, Mass. and Wiley, New York
10. Feinstein, A(1954), "A New Basic Theorem of Information Theory "IRE Trans. Inform. Theory, PGIT-4,
11. (1959) Foundation of Information Theory, McGraw Hill, New York.
12. Gallager, R. G.(1968) Information Theory and Reliable Communication, Wiley, New York
13. Huffman, D.A.(1962), "A Method for the Construction of Minimum Redundancy Codes," Proc. IRE, 40, 1098—1101
14. Kolmogorov, A.N.(1956), "On the Shannon Theory of Infomation in the Case of Continuous Signals," IRE Trans. Inform. Theory, IT-2, 102-108
15. McMillan, B.(1953). "The Basic Theorems of Information Theory" Ann. Math. stat., 24, 196-219
16. Peterson, W.W., and J.L. Massey(1963)," Report on Progress on Infamation Theory in the U.S.A., 1960—1963, Coding Theory," IEEE Trans. Inform. Theory IT-9, 223-229
17. Shannon, C.E. (1948) "A Mathematical Theory of Communicaion." Bell System Tech. J, 27, 379-423 (Part I)
18. Shannon, C.E.(1949). "Communication in the Presence of Noise," Proc. IRE. 37,
19. Wozencraft, J.M., and M. Jacobs(1965), Principles of Communication Engineering. Wiley, New York.