KYBERNETIKA — VOLUME 22 (1986), NUMBER 5

ON A GENERALIZATION OF SHANNON'S RANDOM CIPHER RESULT

PRASANNA K. SAHOO

In this paper, Shannon's random cipher result was generalized using the entropy of degree α. This generalization leads to new definitions, like redundancy of degree α and key rate of degree α.

1. INTRODUCTION

Shannon's random cipher result [13] states that a good secrecy system can be built if the key rate of the crypto system is greater than the message redundancy. This random cipher result was obtained by Shannon considering the equivocation of the key over a random cipher. Hellman [6] proved the same result by counting the average number of spurious decipherments over a restricted class of random ciphers. Lu [11] obtained a general result by considering average probability of correct decryptment for the cryptanalyst.

Havrda and Charvát [5], and Daróczy [2] have proposed a generalization of Shannon entropy. This generalized entropy is called the entropy of degree α. For various characterizations and other properties regarding this entropy see [1, 2, 7, 8, 10]. A coding theorem for entropy of degree α can be obtained from a general theorem proved in [9]. A generalized Fano bound was given by El-Sayed [4] by considering entropy of degree α. In this paper, Shannon's random cipher result will be generalized using entropy of degree α. A similar generalization of random cipher result was given by the author [12] considering the Renyi's entropy of order α. The present generalization leads to new definitions, like redundancy of degree α and key rate of degree α.

2. MATHEMATICAL MODEL

A message is a stationary random sequence from a finite set called the set of alphabets. A key is a bijective mapping which is used for enciphering the message. A cryptogram is a message which is being enciphered by the use of a key. To encipher

means to transfer the message by using a key into a cryptogram. To decipher means to solve the cryptogram with the aid of the key used in the original enciphering, whereas to decrypt means to solve the cryptogram without knowing the particular key used. An encipherer writes the message into a cryptogram by using some randomly selected key. A decipherer decodes the cryptogram using the particular key that has been used in generating the cryptogram. An instantaneous block encipherer is an encipherer which instantaneously groups the incoming message sequence into words of fixed block length. An instantaneous block decipherer groups the cryptograms sequence into cryptogram words and deciphers them into the original messages. The set of messages, together with their probability, is called the message space. A cipher is a pair consisting of the set of keys and their probability distribution.

Consider the simple block diagram in Figure 1 that represents a crypto system. The output $\{M_i\}$ of the message source is a stationary random sequence. Each component M_i takes the value from a finite set A_M. The instantaneous block encipherer groups the incoming message sequence $\{M_i\}$ into message words of length n. Let us denote a message word of length n by $M = (M_1, M_2, \ldots, M_n)$.

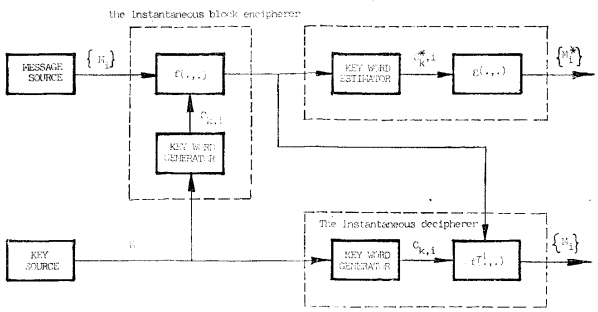

Fig. 1. Block diagram of a Crypto system.

For a fixed key K, the key word generator outputs a key word of length n. Let $C_K = (C_{K,1}, C_{K,2}, \ldots, C_{K,n})$ denote the key word of length n, where each $C_{K,i} \in A_C$, a finite set of key alphabets.

For each digit i, the instantaneous block encipherer produces the ith digit of the cryptogram word X using the following relation

$$X_i = f(M_i, C_{K,i}), \quad i = 1, 2, \ldots, n, \tag{1}$$

where f is a bijective function from $A_M \times A_C$ into A_K; the set of the cryptogram letters. The instantaneous decipherer uses the key to generate the key word and applies the inverse of f to each letter X_i of the cryptogram word X to recover the message

word M. That is

$$M_i = f^{-1}(f(M_i, C_{K,i}), C_{K,i}) . \tag{2}$$

The cryptanalyst intercepts the cryptogram words and attempts to decrypt the words by using his/her knowledge of the a priori message and key probabilities, the combiner f, the block length n, the key rate r, and the cipher. That is for the actual key K the cryptanalyst estimates a key K^* and decrypts the message as $M_i^* = (M_1^*, M_2^*, \ldots, M_n^*)$ where

$$M_i^* = g(X_i, C_{K^*,i}) , \quad i = 1, 2, \ldots, n . \tag{3}$$

The decrypted message word M^* is only one of the possible message words, given the cryptogram word X and the cipher.

3. DEFINITIONS

Let $\Gamma_n = \{P = (p_1, p_2, \ldots, p_n) \mid p_k \geqq 0, \sum_{k=1}^{n} p_k = 1\}$ denote the set of all n-components complete probability distributions. Havrda and Charvát [5] have defined entropy of degree α as

$$H_n^\alpha(P) = \mu^{-1}(\sum_{k=1}^{n} p_k^\alpha - 1) , \quad \alpha \neq 1 \tag{4}$$

where $\mu = (2^{1-\alpha} - 1)$, $\alpha \neq 1$ and $P \in \Gamma_n$. This entropy of degree α is a generalization of Shannon's entropy in the sense that

$$\lim_{\alpha \to 1} H_n^\alpha(P) = H_n^1(P) , \tag{5}$$

where

$$H_n^1(P) = -\sum_{k=1}^{n} p_k \log p_k . \tag{6}$$

Throughout this paper $0 \log 0$ and 0^α are assumed to be zero and logarithm is taken with respect to base 2.

Let X and Y be two ensembles, and $X \times Y$ be the cartesian product of X and Y called the joint ensemble of X and Y. Let $x_1, x_2, \ldots, x_n$ be the events in X with probabilities $p(x_1), p(x_2), \ldots, p(x_n)$, respectively. Similarly, let $y_1, y_2, \ldots, y_m$ be the events in Y with probabilities $p(y_1), p(y_2), \ldots, p(y_m)$. The outcomes of $X \times Y$ are $(x_1, y_1), (x_1, y_2), \ldots, (x_n, y_m)$ with probabilities $p(x_1, y_1), p(x_1, y_2), \ldots, p(x_n, y_m)$, respectively. Using Bayes rule, one can write

$$p(x_i \mid y_j) = \frac{p(x_i, y_j)}{p(y_j)} , \quad p(y_j) > 0 . \tag{7}$$

The joint entropy of degree α is defined as

$$H_{nm}^\alpha(X, Y) = \mu^{-1}(\sum_{i=1}^{n} \sum_{j=1}^{m} p^\alpha(x_i, y_j) - 1) \tag{8}$$

and the equivocation of degree α is defined as (see [2] and [4])

$$H^{\alpha}_{nm}(X \mid Y) = \mu^{-1}\Big(\sum_{i=1}^{n}\sum_{j=1}^{m} p^{\alpha}(x_i, y_j) - \sum_{j=1}^{m} p^{\alpha}(y_j)\Big)\,. \tag{9}$$

From (9) it is easy to see that

$$H^{\alpha}_{nm}(X, Y) = H^{\alpha}_{m}(Y) + H^{\alpha}_{nm}(X \mid Y)\,. \tag{10}$$

If X and Y are stochastically independent, then from (7) and (8), the following is obtained

$$H^{\alpha}_{nm}(X, Y) = H^{\alpha}_{n}(X) + H^{\alpha}_{m}(Y) + \mu H^{\alpha}_{n}(X)\, H^{\alpha}_{m}(Y)\,. \tag{11}$$

The suffix from H^{α}_{n} will be dropped henceforth and will be used only in the case of possible confusion.

Let $m \in A_M^n$ be a message word of length n, and m^* be the decrypted word for the message word m. Let the probability of an error in correct decryptment of the ith digit be

$$p_e(i, n) = \sum_{m \in A_M{}^n} \sum_{\substack{m^* \in A_M{}^n \\ m^* \neq m}} p(m, m^*)\,. \tag{12}$$

The expected number of errors on decryptment of a message words is

$$p_e(n) = \sum_{i=1}^{n} p_e(i, n)\,. \tag{13}$$

and the average probability of error per letter for a message words of length n is defined as

$$\bar{p}_e(n) = \frac{1}{n}\, p_e(n)\,. \tag{14}$$

It is assumed that the sets A_M, A_C, and A_K are of finite cardinality and the combiner f is one-to-one in each variable. Based on this assumption, it follows that

$$p_e(i, n) = pr\{C_{K,i} \neq C_{K^*,i}\}\,. \tag{15}$$

The redundancy of degree α in message words corresponding to a given crypto system is defined as

$$d_n(\alpha) = \frac{|A_M|^{n-n\alpha} - 1}{n\mu} - \frac{H^{\alpha}_{n}(M)}{n}\,(|A_K|^{1-\alpha})\,. \tag{16}$$

By l'Hopital rule, it can be proven that

$$\lim_{\alpha \to 1} d_n(\alpha) = \log |A_M| - \frac{H^{1}_{n}(M)}{n}\,. \tag{17}$$

The right hand side of (17) is the redundancy d of the message words as defined

by Lu [11]. Similarly, the key rate of degree α is defined as

$$r_n(\alpha) = \frac{|A_K|^{1-\alpha} - 1}{n\mu}. \tag{18}$$

and in the limiting case it is equal to the key rate r (see [11]), that is

$$\lim_{\alpha \to 1} r_n(\alpha) = \frac{\log |A_K|}{n}. \tag{19}$$

4. THE MAIN RESULT

The following two results on the entropy of degree α are due to El-Sayed [4].

Result 1 (cf. [4]). *Let $\alpha > 1$ and (X, Y) be a joint ensemble, such that each of the sample spaces X and Y contains the same N elements, and let $p_e(n)$ be the probability of error. Then the equivocation of degree α satisfies the inequality*

$$H^\alpha(X \mid Y) \leqq H_2^\alpha(p_e(n)) + p_e^\alpha(n) \frac{1 - (N-1)^{1-\alpha}}{1 - 2^{1-\alpha}}. \tag{20}$$

Result 2 (cf. [4]). *Let $\alpha > 1$ and (X^n, Y^n) be a joint ensemble of sequences $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ of length n, such that each of the sample spaces X_i and Y_i $(i = 1, 2, \ldots, n)$ of x_i and y_i respectively contain the same N elements. If $\bar{p}_e(n)$ is the average probability of error, then the (n-ary) equivocation of degree α satisfies the following inequality*

$$\frac{1}{n} H^\alpha(X^n \mid Y^n) \leqq H_2^\alpha(\bar{p}_e(n)) + \bar{p}_e^\alpha(n) \frac{1 - (N-1)^{1-\alpha}}{1 - 2^{1-\alpha}}. \tag{21}$$

Now, to prove the main theorem, consider a stationary discrete message source with redundancy of degree α and alphabet size $|A_M|$, and a cipher with the key rate of degree α. Let M denote the random variable representing the message and K denote the random variable representing the key. Since M and K are stochastically independent,

$$H^\alpha(M, K) = H^\alpha(M) + H^\alpha(K) + \mu H^\alpha(M) H^\alpha(K). \tag{22}$$

Using f as one-to-one in each variable and

$$X = f(M, C_K), \tag{23}$$

the following is obtained

$$H^\alpha(M, K) = H^\alpha(X, K), \tag{24}$$

where X is the cryptogram. However, by (10)

$$H^\alpha(X, K) = H^\alpha(X) + H^\alpha(K \mid X) \tag{25}$$

is obtained. From (22), (24) and (25), one can get

$$H^{\alpha}(K \mid X) = H^{\alpha}(M) + H^{\alpha}(K) + \mu H^{\alpha}(M)\, H^{\alpha}(K) - H^{\alpha}(X)\,. \tag{26}$$

Since the total number of cryptograms is equal to $|A_M|^n$, $H^{\alpha}(X)$ can be bounded by

$$H^{\alpha}(X) \leqq \mu^{-1}(|A_M|^{n-n\alpha} - 1)\,. \tag{27}$$

The use of (27) in (26) yields

$$H^{\alpha}(K \mid X) \geqq H^{\alpha}(K) - \left[\frac{|A_M|^{n-n\alpha} - 1}{n\mu} - \frac{H^{\alpha}(M)}{n}\,(1 + \mu H^{\alpha}(K))\right] n\,. \tag{28}$$

Since the keys are chosen randomly, each key is equiprobable, hence

$$H^{\alpha}(K) = \frac{|A_K|^{1-\alpha} - 1}{\mu}\,. \tag{29}$$

Replacing $H^{\alpha}(K)$ in (28) by (29) and using the definitions (16) and (18), it follows that

$$H^{\alpha}(K \mid X) \geqq n(r_n(\alpha) - d_n(\alpha))\,. \tag{30}$$

Notice that K^* is a function of only X (i.e. the cryptanalyst gets the estimate K^* from the intercepted cryptogram X), therefore,

$$H^{\alpha}(K \mid K^*) \geqq H^{\alpha}(K \mid X)\,. \tag{31}$$

Hence (30) with (31) yield

$$H^{\alpha}(K \mid K^*) \geqq n(r_n(\alpha) - d_n(\alpha))\,. \tag{32}$$

Since there is a key words C_K, associated with each key K, and since key words are distinct

$$H^{\alpha}(C_K \mid C_{K^*}) = H^{\alpha}(K \mid K^*)\,, \tag{33}$$

where $C_K = (C_{K,1}, C_{K,2}, \ldots, C_{K,n})$ and $C_{K^*} = (C_{K^*,1}, C_{K^*,2}, \ldots, C_{K^*,n})$. Using a result from El-Sayed [3]

$$\begin{aligned} H^{\alpha}(C_K \mid C_{K^*}) = {} & H^{\alpha}(C_{K,1} \mid C_{K^*}) + H^{\alpha}(C_{K,2} \mid C_{K,1}, C_{K^*}) + \ldots \\ & \ldots + H^{\alpha}(C_{K,n} \mid C_{K,1}, \ldots, C_{K,n-1}, C_{K^*})\,. \end{aligned} \tag{34}$$

It has been shown (see [3]) that for $\alpha > 1$,

$$H^{\alpha}(X \mid Y, Z) \leqq H^{\alpha}(X \mid Y)\,, \tag{35}$$

where X, Y and Z are any three random variables. Using the inequality (35) in (34),

$$\sum_{i=1}^{n} H^{\alpha}(C_{K,i} \mid C_{K^*,i}) \geqq H^{\alpha}(C_K \mid C_{K^*})\,. \tag{36}$$

and from (33), (36) and (32),

$$\frac{1}{n} \sum_{i=1}^{n} H^{\alpha}(C_{K,i} \mid C_{K^*,i}) \geqq r_n(\alpha) - d_n(\alpha)\,, \tag{37}$$

is obtained. Applying Result 1, one can get

$$p_e^{\alpha}(i, n)\frac{1-(|A_M|-1)^{1-\alpha}}{1-2^{1-\alpha}} + H_2^{\alpha}(p_e(i, n)) \geqq H^{\alpha}(C_{K,i} \mid C_{K^*,i}) . \tag{38}$$

By mimicking the proof of Result 2 (see [4]) and using (37) and (38) the following

$$H_2^{\alpha}(\bar{p}_e(n)) + \bar{p}_e(n)\frac{1-(|A_M|-1)^{1-\alpha}}{1-2^{1-\alpha}} \geqq r_n(\alpha) - d_n(\alpha) \tag{39}$$

is obtained. Thus the following theorem is proved.

Theorem. *Consider a stationary random discrete source with alphabet size* $|A_M|$. *For* $\alpha > 1$, *let* $d_n(\alpha)$ *be the redundancy of degree* α, $r_n(\alpha)$ *be the key rate of degree* α, *and* $\bar{p}_e(n)$ *be the average probability of error of correct decryptment, then*

$$H_2^{\alpha}(\bar{p}_e(n)) + \bar{p}_e(n)\frac{1-(|A_M|-1)^{1-\alpha}}{1-2^{1-\alpha}} \geqq r_n(\alpha) - d_n(\alpha) .$$

Remark. For a limiting case (i.e. when $\alpha \to 1^-$), the inequality (39) tends to the following inequality

$$H_2^1(\bar{p}_e(n)) + \bar{p}_e(n)\log(|A_M| - 1) \geqq r - d .$$

This inequality was proven by Lu [11].

ACKNOWLEDGEMENT

The author is thankful to H. Brown and the referee for the comments and help in improving the readability and presentation of this paper.

(Received June 12, 1985.)

REFERENCES

[1] J. Aczél and Z. Daróczy: On Measures of Information and Their Characterizations. Academic Press, New York 1975.

[2] Z. Daróczy: Generalized information functions. Inform. and Control *16* (1970), 36—51.

[3] A. El-Sayed: On Different Information Measures and Communication Channels. Ph. D. Thesis University of Waterloo, Waterloo, Ontario 1975.

[4] A. El-Sayed: A generalized entropy form of the Fano inequality. Utilitas Math. *12* (1977), 289—298.

[5] J. Havrda and F. Charvát: Quantification method of classification process, concept of structural *a*-entropy. Kybernetika *3* (1967), 30—35.

[6] M. Hellman: An extension of the Shannon theory approach to cryptography. IEEE Trans. Inform. Theory *IT-23* (1977), 289—294.

[7] Pl. Kannappan: On some functional equations from additive and nonadditive measures I. Proc. Edinburgh Math. Soc. *23* (1980), 145—150.

[8] Pl. Kannappan and P. K. Sahoo: On a functional equation connected to sum form non-additive information measures on an open domain — I. Kybernetika *22* (1986), 268—275.

[9] A. B. Khan, R. Autar and H. Ahmad: Noiseless coding theorems for generalized non-additive entropy. Tamkang J. Math. *12* (1981), 15—20.
[10] L. Losonczi: A characterization of entropies of degree α. Metrika *28* (1981), 237—244.
[11] S. C. Lu: The existence of good cryptosystems for key rates greater than the message redundancy. IEEE Trans. Inform. Theory *IT-25* (1979), 475—477.
[12] P. K. Sahoo: Renyi's entropy of order α and Shannon's random cipher result. J. Combin. Inform. System Sci. *8* (1983), 263—270.
[13] C. E. Shannon: Communication theory of secrecy system. Bell System Tech. J. *28* (1949), 656—715.

Dr. Prasanna K. Sahoo, Department of Applied Mathematics, Waterloo, Ontario, NSL 3G1, Canada.