Wire-Tap Channel II

L. H. Ozarow
A. D. Wyner

AT&T Bell Laboratories
Murray Hill, New Jersey 07974

ABSTRACT

Consider the following situation. K data bits are to be encoded into $N > K$ bits and transmitted over a noiseless channel. An intruder can observe a subset of his choice of size $\mu < N$. The encoder is to be designed to maximize the intruder's uncertainty about the data given his N intercepted channel bits, subject to the condition that the intended receiver can recover the K data bits perfectly from the N channel bits. The optimal tradoffs between the parameters K, N, μ and the intruder's uncertainty H (H is the "conditional entropy" of the data given the μ intercepted channel bits) were found. In particular, it was shown that for $\mu = N - K$, a system exists with $H \approx K - 1$. Thus, for example, when $N = 2K$ and $\mu = K$, it is possible to encode the K data bits into $2K$ channel bits, so that by looking at any K channel bits, the intruder obtains essentially no information about the data.

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 33-50, 1985.

Wire-Tap Channel II

L. H. Ozarow
A. D. Wyner

AT&T Bell Laboratories
Murray Hill, New Jersey 07974

1. Introduction

In this paper we study a communication system in which an unauthorized intruder is able to intercept a subset of the transmitted symbols, and it is desired to maximize the intruder's uncertainty about the data without the use of an encryption key (either "public" or "private").

Specifically, the encoder associates with the K-bit binary data sequence $\mathbf{S}^K$ an N-bit binary "transmitted" sequence $\mathbf{X}^N$, where $N > K$. It is required that a decoder can correctly obtain $\mathbf{S}^K$ with high probability by examining $\mathbf{X}^N$. The intruder can examine a subset of his choice of size μ of the N positions in $\mathbf{X}^N$, and the system designer's task is to make the intruder's equivocation (uncertainty) about the data as large as possible. The encoder is allowed to introduce randomness into the transformation $\mathbf{S}^K \rightarrow \mathbf{X}^N$, but we make the assumption that the decoder and the intruder must share any information about the encoding and the randomness. This assumption precludes the use of "key" cryptography, where the decoder has the exclusive posession of certain information.

As an example, suppose that $K = 1$, $N = 2$, $\mu = 1$. Let the data bit be S, and let ξ be a uniform binary random variable which is independent of S. Let $\mathbf{X}^2 = (\xi, \xi \oplus S)$, where "$\oplus$" denotes modulo 2 addition. If the intruder looks at either coordinate of $\mathbf{X}^2$ he gains no information about S, so that the system has perfect secrecy. The decoder, however, can obtain S by adding (modulo two) the two components of $\mathbf{X}^2$.

Our problem is to replicate this type of performance with large K, N, μ. In fact we assume that $K \approx RN$, $\mu \approx \alpha N$, where R, α are held fixed and N becomes large. Roughly speaking, we show that perfect secrecy is attainable provided that μ is not too large, specifically $\mu \leq N - K$ or $\alpha \leq 1 - R$. In Section 2 we give a precise statement and discussion of our problem and results, leaving the proofs for Sections 3-5.

This problem is similar to the wire-tap channel problem studied in Reference 1. A special case

of the problem studied there allows an intruder to examine a subset of the encoder symbols which is chosen at random by nature. In the present problem, the system designer must make his system secure against a more powerful intruder who can select which subset to examine.

2. Formal Statement of the Problem and Results

In this section we give a precise statement of our problem and state the results.

First a word about notation. Let U be an arbitrary finite set. Denote its cardinality by $|U|$. Consider U^N, the set of N-vectors with components in U. The members of U^N will be written as

$$\mathbf{u}^N = (u_1, u_2, \ldots, u_N) ,$$

where subscripted letters denote components and boldface superscripted letters denote vectors. A similar convention applies to random vectors which are denoted by upper-case letters. When the dimension of a vector is clear from the context, we omit the superscript. Finally, for random variables X, Y, Z etc., the notation $H(X)$, $H(X|Y)$, $I(X;Y)$, etc. denotes the standard information theoretic quantities as defined, for example, in Gallager [2].

We now turn to the description of the communication system.

(i) The *source* output is a sequence $\{S_t\}_1^\infty$, where the S_t are independent, identically distributed binary random variables.

(ii) The *encoder* with parameters (K, N) is a channel with input alphabet $\{0,1\}^K$ and output alphabet $\{0,1\}^N$ and transition probability $q_E(\mathbf{x}^N|\mathbf{s}^K)$. Let $\mathbf{S}^K$ and $\mathbf{X}^N$ be the input and output respectively of the encoder.

(iii) The *decoder* is a mapping

$$f_D: \{0,1\}^N \to \{0,1\}^K .$$

Let $\hat{\mathbf{S}} = (\hat{S}_1, \hat{S}_2, \ldots \hat{S}_K) = f_D(\mathbf{X}^N)$. The *error-rate* is

$$P_e = \frac{1}{K} \sum_{t=1}^{N} Pr\{S_t \neq \hat{S}_t\} .$$

(iv) An intruder with parameter $\mu \leq N$ picks a subset $S \subseteq \{1, 2, ..., N\}$, such that $|S| = \mu$, and is allowed to observe $X_n, n \in S$. Let $\mathbf{Z}^N = (Z_1, ..., Z_N)$, defined by

$$Z_n = \begin{cases} X_n, & n \in S, \\ ?, & n \notin S, \end{cases}$$

denote the intruder's information. The system designer seeks to maximize the equivocation

$$\Delta \triangleq \min_{S:\,|S|=\mu} H(\mathbf{S}^K | \mathbf{Z}^N).$$

Thus, the designer is assured that no matter what subset S the intruder chooses, the intruder's remaining uncertainty about the source vector is at least Δ. When $\Delta = K$, the intruder obtains no information about the source, and the system has attained perfect secrecy.

In this paper we study the tradeoffs between K, N, Δ, and P_e. As we shall see, it will be useful to consider the normalized qualities $K/N, \mu/N, \Delta/K$. Thus K/N is the "rate" of the encoder = the number of data bits per encoded bit, μ/N is the fraction of the encoded bits which the intruder is able to observe, and Δ/K is the normalized entropy.

Let us remark that the intruder which observes $\mathbf{Z}^N$ can reconstruct the data sequence $\mathbf{S}^K$ with a per bit error probability of say P_e'. It follows from Fano's inequality that $h(P_e') \geq \Delta/K$, where $h(\cdot)$ is the binary entropy function defined below Eq. (2.2). Thus $\Delta/K \approx 1$ implies that $P_e' \approx 1/2$ which is essentially perfect secrecy.

We will say that the triple (R, α, δ) is *achievable* if for all $\epsilon > 0$ and all integers $N_0 > 0$, there exists an encoder/decoder with parameters $N \geq N_0$, $K \geq (R-\epsilon)N$, $\mu \geq (\alpha-\epsilon)N$, $\Delta \geq (\delta-\epsilon)N$, and $P_e \leq \epsilon$. We will show in the sequel that (R, α, δ) is achievable for $0 \leq R, \alpha, \delta \leq 1$, and

$$\delta \leq \begin{cases} 1, & 0 \leq \alpha \leq 1-R, \\ \dfrac{(1-\alpha)}{R}, & 1-R \leq \alpha \leq 1. \end{cases} \tag{2.1}$$

A graph of the achievable (α, δ) pairs for fixed R is given in Figure 1.

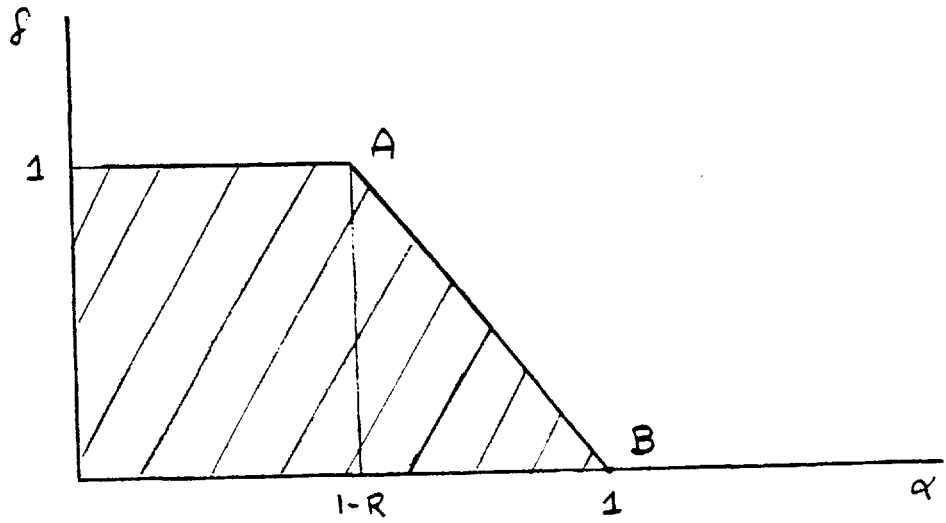

Figure 1. Achievable (α, δ) for fixed R.

The following theorem, a proof of which is given in Section 3, is a "converse" result which gives a necessary condition on achievable (K, N, Δ, P_e).

Theorem 2.1: If (K, N, Δ, P_e) is achievable, then

$$\Delta \leq \begin{cases} K, & 0 \leq \mu \leq N-K, \\ N-\mu+Kh(P_e), & N-K \leq \mu \leq N. \end{cases} \tag{2.2}$$

where $h(\lambda) = -\lambda \log \lambda - (1-\lambda) \log (1-\lambda)$ is the binary entropy function.

Now if (R, α, δ) is achievable, for arbitrary $\epsilon > 0$, there must be an encoder/decoder with parameters $N, K \geq (R-\epsilon)N$, $\mu \geq (\alpha-\epsilon)N$, $\Delta \geq (\delta-\epsilon)N$, $P_e \leq \epsilon$. Applying Theorem 2.1 to this code yields

$$\delta \leq \begin{cases} 1, \\ \dfrac{(1-\alpha)}{R} + O(\epsilon) + h(\epsilon), & 1-R \leq \alpha + O(\epsilon) \leq 1, \end{cases}$$

which is (2.1) as $\epsilon \to 0$. Thus conditions (2.1) are necessary for a triple to be achievable. Theorem 2.2, which is also proved in Section 3, implies that (R, α, δ) is achievable if (2.1) is satisfied.

Theorem 2.2: Let $1-R < \alpha < 1$. Then, for all $\epsilon > 0$, $N_0 \geq 1$, there exists an $N \geq N_0$ and an encoder/decoder with parameters $K = RN$, $\mu = \alpha N$, $\Delta/K \geq [(1-\alpha)/R] - \epsilon$, and $P_e = 0$.

The idea behind the proof of Theorem 2.2 is the following. Partition the set $\{0,1\}^N$ into 2^K subsets $\{A_m\}_1^{2^K}$ with equal cardinality — i.e. $|A_m| = 2^{N-K}$. The 2^K possible values of S^K can be put in 1-1 correspondence with these subsets. When S^K corresponds to A_m $(1 \le m \le 2^K)$, the encoder output is uniformly distributed on A_m. Since the $\{A_m\}$ are disjoint, the decoder can recover S^K perfectly and $P_e = 0$. We show (by random coding) that there exists a partition satisfying Theorem 2.2.

A convenient way to partition $\{0,1\}^N$, is to let the sets $\{A_m\}$ be the cosets of a group code G with $N-K$ information symbols (so that G has 2^K cosets). Theorem 2.3, which is proved in Section 4, asserts that in fact we can do quite well with codes of this type.

Theorem 2.3: If the triple (R, α, δ) satisfies (2.1), then it is achievable using an encoder/decoder derived from a group code.

The following simple lemma allows us to establish the achievability of all triples on the straight line of Figure 1 connecting points A and B by proving only the achievability of point A.

Lemma 2.4: Suppose that we are given an encoder/decoder f_E, f_D with parameters N, K, P_e. Suppose there are two intruders which have parameters $\mu = \mu_1, \mu_2$ and $\Delta = \Delta_1, \Delta_2$, respectively. Then, if $\mu_2 \ge \mu_1$

$$\Delta_2 \ge \Delta_1 - (\mu_2 - \mu_1) . \tag{2.3}$$

Remark: Inequality (2.3) can be rewritten as

$$(\Delta_2/K) \ge (\Delta_1/K) - \left(\frac{\mu_2/N - \mu_1/N}{K/N} \right),$$

from which we conclude that (R, α_1, δ_1) achievable implies that (R, α_2, δ_2) is achievable where $\alpha_2 \ge \alpha_1$, and

$$\delta_2 = \delta_1 - \left(\frac{\alpha_2 - \alpha_1}{R} \right).$$

In particular, if $\alpha_1 = 1-R$, $\delta_1 = 1$, then

$$\delta_2 = (1-\alpha_2)/R \ .$$

Proof of Lemma 2.4: Let $S_1 \subseteq S_2 \subseteq \{1,2,...,N\}$, where $|S_1| = \mu_1$, $|S_2| = \mu_2$. Let $\mathbf{Z}_i^N$ correspond to S_i $(i = 1, 2)$, i.e. $\mathbf{Z}_i = (Z_{i1},..., Z_{iN})$ and

$$Z_{ij} = \begin{cases} X_j, & j \in S_i, \\ ?, & j \notin S_i . \end{cases}$$

Then

$$H(\mathbf{S}^K|\mathbf{Z}_2) - H(\mathbf{S}^K|\mathbf{Z}_1) = H(\mathbf{S}^K|\mathbf{Z}_2, \mathbf{Z}_1) - H(\mathbf{S}^K|\mathbf{Z}_1)$$
$$= -I(\mathbf{S}^K; \mathbf{Z}_2|\mathbf{Z}_1) \geq -H(\mathbf{Z}_2|\mathbf{Z}_1) \geq -(\mu_2-\mu_1) ,$$

where the first equality follows from $S_1 \subseteq S_2$. Thus

$$\begin{aligned} H(\mathbf{S}^K|\mathbf{Z}_2) &\geq H(\mathbf{S}^K|\mathbf{Z}_1) - (\mu_2-\mu_1) \\ &\geq \Delta_1 - (\mu_2-\mu_1) . \end{aligned} \tag{2.4}$$

from the definition of Δ. Minimizing (2.4) over all S_2, with $|S_2| = \mu_2$ yields (2.5) and the lemma.

Finally, we state a theorem which is a rather surprising strengthening of Theorem 2.2. Its proof is given in the full version of this paper.[3]

Theorem 2.5. For arbitrary K, N $(1 \leq K \leq N)$, and $\mu = N-K$, there exists an encoder-decoder with $P_e = 0$ and

$$\Delta \geq K - 1 - \frac{2.23}{\sqrt[4]{N}} .$$

3. Proof of Theorems 2.1 and 2.2

Assume that $\mathbf{S}^K$, $\mathbf{X}^N$, $\mathbf{Z}^N$, $\hat{\mathbf{S}}$ correspond to a source/encoder/decoder as defined in Section 2, with parameters K, N, Δ, P_e. Then, making repeated use of the identity $H(U,V) = H(U) + H(V|U)$, we obtain

$$\begin{aligned}\Delta = H(\mathbf{S}^K|\mathbf{Z}^N) &= H(\mathbf{S},\mathbf{Z}) - H(\mathbf{Z}) \\ &= H(\mathbf{S},\mathbf{X},\mathbf{Z}) - H(\mathbf{X}|\mathbf{S},\mathbf{Z}) - H(\mathbf{Z}) \\ &= H(\mathbf{S}|\mathbf{X},\mathbf{Z}) + H(\mathbf{X},\mathbf{Z}) - H(\mathbf{X}|\mathbf{S},\mathbf{Z}) - H(\mathbf{Z}) \\ &= H(\mathbf{S}|\mathbf{X},\mathbf{Z}) + H(\mathbf{X}|\mathbf{Z}) - H(\mathbf{X}|\mathbf{S},\mathbf{Z}) . \end{aligned} \tag{3.1}$$

Now

$$\begin{aligned} H(\mathbf{S}|\mathbf{X},\mathbf{Z}) &= H(\mathbf{S}|\mathbf{X},\mathbf{Z},\hat{\mathbf{S}}) \le H(\mathbf{S}|\hat{\mathbf{S}}) \\ &\le Kh(P_e) , \end{aligned}$$

where the last inequality follows from Fano's inequality (see [2]). Also, since $H(\mathbf{X}|\mathbf{Z})$ is the entropy of those $N-\mu$ coordinates of $\mathbf{X}$ not specified by $\mathbf{Z}$, we have $H(\mathbf{X}|\mathbf{Z}) \le N-\mu$. Finally, noting that $H(\mathbf{X}|\mathbf{S},\mathbf{Z}) \ge 0$, we have from (3.1)

$$\Delta \le N-\mu + Kh(P_e) ,$$

which is Theorem 2.1.

We now give a proof of Theorem 2.2 which proceeds along the lines suggested in Section 2. Let K, N be given, and let $\{A_m\}$, $1 \le m \le 2^K$, be a partition of $\{0,1\}^N$ into subsets $A_m \subseteq \{0,1\}^N$ such that $|A_m| = 2^{N-K}$. As in Section 2, the partition defines a code: to encode message m $(1 \le m \le 2^K)$, we let $\mathbf{X}^N$ be a randomly chosen vector in A_m. Since the A_m are disjoint, $P_e = 0$ and $H(\mathbf{S}|\mathbf{X},\mathbf{Z}) = 0$. Further, since the 2^K messages are equally likely and $|A_m| = 2^{N-K}$, $\mathbf{X}$ is uniformly distributed on $\{0,1\}^N$, so that its coordinates are independent identically distributed uniform binary random variables. Thus $H(\mathbf{X}^N|\mathbf{Z}^N) = N-\mu$. We conclude from (3.1) that for this encoder

$$\Delta = N-\mu - H(\mathbf{X}^N|\mathbf{S}^K,\mathbf{Z}^N) . \tag{3.2}$$

Now let $\mathbf{z} \in \{0,1,?\}^N$ be a possible value for the intruder's information, and let $\mathbf{x} \in \{0,1\}^N$. We say that $\mathbf{z}$ is "consistent" with $\mathbf{x}$, if $\mathbf{z}$ can be obtained from $\mathbf{x}$ by changing a subset of the coordinates of $\mathbf{x}$ to ?'s. Next, let $L \ge 1$ be an integer to be chosen later. We say that a partition $\{A_m\}$ is "good" if for all m $(1 \le m \le 2^K)$ and all $\mathbf{z} \in \{0,1,?\}^N$ with exactly $N-\mu$ '?'s,

$$\text{card}\,\{\mathbf{x} \in A_m : \mathbf{z} \text{ is consistent with } \mathbf{x}\} < L \ .$$

If our encoder corresponds to a "good" partition for some L, then

$$H(\mathbf{X}^N | \mathbf{S}^K, \mathbf{Z}^N) < \log L \ ,$$

and (3.2) yields

$$\Delta \geq N - \mu - \log L \ . \tag{3.3}$$

At the conclusion of this section we will prove the following proposition about the existence of "good" partitions. This will lead us directly to Theorem 2.2.

Lemma 3.1: Let K, N, μ be such that

$$N - \mu - K < 0 \ . \tag{3.4}$$

Then, there exists a "good" partition (with parameters K, N, μ) provided

$$L > \frac{2N + K + 2 \log e}{K + \mu - N} \ . \tag{3.5}$$

Now let R, α, ϵ, N_0 be given as in the hypothesis of Theorem 2.2. Then, using $2 \log e \leq 3$, we write for $N \geq 1$,

$$\frac{N + K + 2 \log e}{K + \mu - N} \leq \frac{1 + R + 3}{\alpha - (1 - R)} \triangleq B < \infty \ .$$

Thus there exists a "good" partition with $L \leq B + 1$, and we conclude from (3.3) that there exists a code with $\Delta/K \geq (1-\alpha)/R - \frac{\log(B+1)}{RN}$. If we choose $N \geq N_0, \epsilon R / \log(B+1)$, the existence of this code establishes Theorem 2.2. It remains to prove Lemma 3.1.

Proof of Lemma 3.1: Let $\{A_m\}$, $1 \leq m \leq 2^K$, be a partition of $\{0, 1\}^N$, where $|A_m| = 2^{N-K}$. Let $\Psi(A_1, \ldots, A_{2^K}) = 0$ or 1 according as $\{A_m\}$ is "good" or not. We write

$$\Psi(A_1, \ldots, A_{2^K}) \leq \sum_{m=1}^{2^K} \sum_{\mathbf{z}} \phi(A_m, \mathbf{z}) \ , \tag{3.6}$$

where the inner sum is taken over all $\mathbf{z} \in \{0, 1, ?\}^N$ with exactly $N - \mu$ '?'s, and $\phi(A_m, \mathbf{z}) = 1$ if

$$\text{card}\,\{\mathbf{x} \in A_m : \mathbf{z} \text{ is consistent with } \mathbf{x}\} \geq L\ ,$$

and $\Phi(A_m, \mathbf{z}) = 0$ otherwise.

We now choose the partition at random with uniform distribution on the set of partitions of $\{0,1\}^N$ into 2^K classes of equal size. The expectation $E\Psi$, satisfies

$$E\Psi \leq \sum_m \sum_{\mathbf{z}} E\Phi(A_m, \mathbf{z})\ . \tag{3.7}$$

The expectation in the right member of (3.7) is taken, as indicated, with $\mathbf{z}$ held fixed. Let us define the following quantities.

$$\begin{aligned} Q(\mathbf{z}) &= \{\mathbf{x} \subseteq \{0,1\}^N : \mathbf{x} \text{ is consistent with } \mathbf{z}\}\ , \\ n_1 &= |Q(\mathbf{z})| = 2^{N-K}\ , \\ n &= |\{0,1\}^N| = 2^N\ , \\ r &= |A_m| = 2^{N-K}\ . \end{aligned} \tag{3.8}$$

We now compute $E\Phi(A_m, \mathbf{z})$. The r members of A_m are chosen at random from $\{0,1\}^N$ (without replacement). The probability that exactly ℓ members of A_m belong to $Q(\mathbf{z})$ is

$$\frac{\binom{n_1}{\ell}\binom{n-n_1}{r-\ell}}{\binom{n}{r}} \triangleq \pi_\ell\ .$$

To see this, observe that there are $\binom{n}{r}$ ways of choosing the set A_m. The ℓ members of A_m which belong to $Q(\mathbf{z})$ can be chosen in $\binom{n_1}{\ell}$ ways, and the remaining $(r-\ell)$ members of A_m can be chosen from the complement of $Q(\mathbf{z})$ in $\binom{n-n_1}{r-\ell}$ ways.

Now

$$\pi_\ell = \frac{\binom{n_1}{\ell}\binom{n-n_1}{r-\ell}}{\binom{n}{r}} \leq \frac{\binom{n_1}{\ell}\binom{n}{r-\ell}}{\binom{n}{r}}\ .$$

Also, using $\binom{n_1}{\ell} \leq n_1^\ell/\ell!$, and

$$\frac{\binom{n}{r-\ell}}{\binom{n}{r}} = \frac{n!}{(n-r+\ell)!(r-\ell)!} \cdot \frac{r!(n-r)!}{n!}$$

$$= \frac{r(r-1)(r-2)\ldots(r-\ell+1)}{(n+\ell-r)(n+\ell-r-1)\ldots(n-r+1)} \le \frac{r^\ell}{(n-r)^\ell} = \frac{(r/n)^\ell}{(1-r/n)^\ell},$$

we have

$$\pi_\ell \le \frac{(n_1 r/n)^\ell}{\ell!(1-r/n)^\ell},$$

Thus

$$E\,\Phi(A_m, z) = \sum_{\ell=L}^{2^{N-K}} \pi_\ell \le \sum_{\ell=L}^{\infty} \frac{(n_1 r/n)^\ell}{\ell!(1-r/n)^\ell}.$$

Using (3.8), we have $(n_1 r/n) = 2^{N-\mu-K}$, $(1-r/n) \ge 1/2$, so that

$$E\,\Phi(A_m, z) \le \sum_{\ell=L}^{\infty} 2^{(N-\mu-K)\ell} \frac{2^\ell}{\ell!}$$

$$\le 2^{(N-\mu-K)L} \sum_{\ell=0}^{\infty} \frac{2^\ell}{\ell!} = 2^{(N-\mu-K)L} e^2.$$

Substituting into (3.7) we have

$$E\,\Psi \le \sum_m \sum_z 2^{(N-\mu-K)L+2\log e}$$

$$\le 2^{(N-\mu-K)L+2\log e+K+2N}.$$

If L satisfies (3.5), then $E\,\Psi < 1$. Since Ψ is integer valued, there must exist a particular partition, say $\{A_m^*\}$ such that $\Psi(A_1^*, \ldots, A_{2^K}^*) = 0$. This is our "good" partition.

4. Group Codes and Theorem 2.3

In Sections 2 and 3, we discussed how to construct encoder/decoders based on a partition $\{A_m\}$ of $\{0,1\}^N$. In this section we consider the special case where the partition $\{A_m\}$ is defined by a group code and its cosets.

Let H be a $K \times N$ parity-check matrix, which we assume has rank K. Let the partition $\{A_m\}$, $1 \le m \le 2^K$, be the code defined by H and its cosets. Thus $|A_m| = 2^{N-K}$, for $1 \le m \le 2^K$. To encode message $\mathbf{s} = (s_1, \ldots, s_K)$, the encoder makes a random selection of one of the 2^{N-K} members of the A_m corresponding to $\mathbf{s}$. This is equivalent to letting $\mathbf{X}^N$ be a random choice from the 2^{N-K} solutions of

$$H\mathbf{X}^\dagger = \mathbf{s}^\dagger , \tag{4.1}$$

where $\dagger$ denotes matrix transpose. Note that, since $\mathbf{S}$ is uniformly distributed on $\{0,1\}^K$, $\mathbf{X}^N$ is uniformly distributed on $\{0,1\}^N$, and its coordinates $X_1, X_2, \ldots, X_N$ are i.i.d. uniform binary random variables.

The decoder observes $\mathbf{X}^N$ and computes $H\mathbf{X}^\dagger$, which is the message. Thus $P_e = 0$. We now show how to compute Δ in terms of certain distance-like properties of the parity check matrix.

Definition: Let $\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_N$ be the columns of H ($\mathbf{C}_n$ is a K-vector). Let $S \subseteq \{1, 2, \ldots, N\}$ and define $D(S)$ to be the dimension of the subspace spanned by $\{\mathbf{C}_n\}, n \in S$. For a given $K \times N$ parity check matrix H, define for $0 \le \mu \le N$,

$$D^*(\mu) = \min_{|S| = N-\mu} D(S) . \tag{4.2}$$

We now state

Lemma 4.1: Let $D^*(\mu)$ correspond to the $K \times N$ parity-check matrix H. Let w, w' be the minimum weight of the code and dual code, respectively defined by H. Then (1) for $N-w+1 \le \mu \le N$, $D^*(\mu) = N-\mu$; (2) for $0 \le \mu \le w'-1$, $D^*(\mu) = K$.

Proof: Assertion (1) follows immediately on observing that all sets of $w-1$ columns of H are linearly independent. Thus $D(S) = |S|$, for $|S| \le w-1$. If $N-w+1 \le \mu \le N$, then $N-\mu \le w-1$, so that

$$D^*(\mu) = \min_{|S| = N-\mu} D(S) = N-\mu ,$$

which is assertion (1).

Now assertion (2) states that all submatrices $\hat{H} = (C_{i_1} C_{i_2} \ldots, C_{i_q})$ of H have rank K when $q \geq N - w' + 1$. To establish this assertion assume that rank $\hat{H} < K$. Then there exists a set of linear row manipulations which transform $\hat{H}$ into a matrix with a row of 0's. These identical row manipulations will transform H into a matrix for which a row as weight $\leq N - q$. Since the dual code is the row space of H, $N - q \geq w'$ or $q \leq N - w'$, establishing assertion (2).

We now give

Lemma 4.2: When an encoder/decoder is constructed to correspond to the parity check matrix H, then

$$\Delta = D^*(\mu) . \tag{4.3}$$

Proof: Let S, X, Z correspond to an encoder/decoder with parameters K, N, Δ ($P_e = 0$), derived as discussed above, from a parity-check matrix $H = (C_1, \ldots, C_N)$. Since $P_e = 0$, and $\mathbf{X}^N$ is uniformly distributed on $\{0, 1\}^N$, Eq. (3.2) applies. Thus Lemma 4.2 will be established when we show that

$$H(\mathbf{X}^N | \mathbf{S}^K, \mathbf{Z}^N) = N - \mu - D^*(\mu) . \tag{4.4}$$

Now suppose that $\mathbf{S}^K = \mathbf{s}$ and $\mathbf{Z}^N = \mathbf{z}$. Without loss of generality, assume that the last μ coordinates of $\mathbf{z}$ are copies of the corresponding coordinates of $\mathbf{X}$. Thus, given $\mathbf{S}^K = \mathbf{s}, \mathbf{Z}^N = \mathbf{z}$, the remaining unknown coordinates of $\mathbf{X}$ are precisely the solutions for $x_1, \ldots, x_{N-\mu}$ of

$$\sum_{n=1}^{N-\mu} C_n x_n = \mathbf{s}^t + \sum_{n=N-\mu+1}^{N} C_n \mathbf{z}_n \triangleq \alpha . \tag{4.5}$$

Since the number of solutions is $N - \mu - \text{rank}\,(C_1, \ldots, C_{N-\mu})$, and given $\mathbf{S} = \mathbf{s}, \mathbf{Z} = \mathbf{z}$ all these solutions are equally likely, (4.4) follows. Hence the lemma.

Before continuing with the proof of Theorem 2.3, we digress to apply Lemma 4.2 in an example. Let $K = 4, N = 8$, and construct an encoder/decoder using the self-dual Hamming code with block

length 8 and 4 information and 4 check digits. Then $w = w' = 4$, so that

$$\Delta = D^*(\mu) = \begin{cases} 4 = K, & 0 \le \mu \le 3, \\ 3, & \mu = 4, \\ N - \mu, & 5 \le \mu \le 8. \end{cases}$$

Thus the encoder/ decoder is optimal for all μ except $\mu = 4$, when Δ is but one bit less than ideal.

We will establish Theorem 2.3 via a random code argument. Towards this end, we establish the following lemmas.

Lemma 4.3: Let $1 \le m \le n$ and let the $m \times n$ matrix A over $GF(2)$ be chosen at random with uniform distribution on the set of 2^{mn} binary $m \times n$ matrices. Then, for $1 \le L \le m$,

$$Pr\{\text{rank } A < m - L\} \le 2^{-(L+1)(n-m)+n}$$

Proof: Let us choose the n columns of A sequentially and independently. Let $d(j)$ be the dimension of the linear space spanned by the first j columns. Suppose that $d(j) = k \le m$. With probability 2^{k-m}, $d(j+1) = k$; and with probability $(1-2^{k-m})$, $d(j+1) = k+1$. This sequential choice of the columns is modelled by the Markov chain of Figure 2.

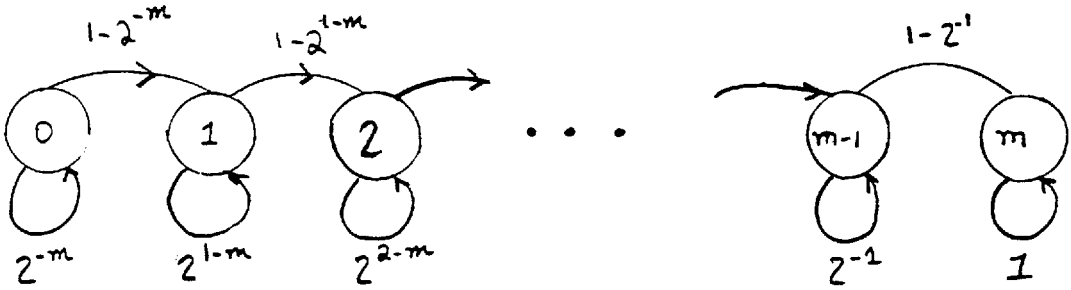

Figure 2

Begin at state 0. With each choice of a column, advance one state if and only if this choice increases the dimension of the space spanned by the columns chosen so far. The rank of the matrix A is $d(n)$, and is equal to the state at which we find ourselves after all n columns are chosen. Let $\Gamma(k)$ denote the set of paths π which start at state 0 and terminate at state k $(0 \le k \le m)$. Then

$$Pr\{\text{rank } A < m-L\} = \sum_{k=0}^{m-L-1} \sum_{\pi \in \Gamma(k)} Pr\{\pi\} . \tag{4.6}$$

Now let the path $\pi \in \Gamma(k)$. This path contains exactly $n-k$ self-loops, each of which has probability $\leq 2^{-m+k}$. Thus, for $\pi \in \Gamma(k)$,

$$Pr\{\pi\} \leq 2^{(-m+k)(n-k)} .$$

Also since $|\Gamma(k)| = \binom{n}{k}$, eq. (4.6) yields

$$Pr\{\text{rank } A < m-L\} \leq \sum_{k=0}^{m-L-1} \binom{n}{k} 2^{-(m-k)(n-k)} .$$

Since the exponent is non-decreasing in k ($k \leq m \leq n$), we have

$$Pr\{\text{rank } A < m-L\} \leq \sum_{k=0}^{m-L-1} \binom{n}{k} 2^{-(L+1)(n-m+L+1)}$$

$$\leq 2^n 2^{-(L+1)(n-m)} ,$$

which is Lemma 4.3.

Lemma 4.4: Let $1 \leq m \leq n$, and let the $m \times n$ matrix A over $GF(2)$ be chosen at random with uniform distribution on the set of 2^{mn} binary $m \times n$ matrices. Then

$$Pr\{\text{rank } A = m\} = \prod_{j=0}^{m-1} (1 - 2^{j-n})$$

$$\geq \exp\left\{\frac{-m\,2^{m-1-n}}{1-2^{m-1-n}}\right\} \geq (1 - \frac{m\,2^{m-1-n}}{1-2^{m-1-n}}).$$

Proof: Choose the *rows* of A sequentially. As in the proof of Lemma 4.3, the probability that the dimension of the space spanned by the first j rows is equal to j is

$$(1-2^{-n})(1-2^{-n+1})...(1-2^{-n+j-1}) .$$

The rest of the lemma follows from $\ln(1-u) \geq -u/(1-u)$ and $e^{-u} \geq 1-u$.

We now turn to Theorem 2.3. Let $R > 0$ be given and held fixed. We will show that $\delta = 1$, $\alpha = 1-R$ is achievable, and the remainder of the theorem will follow from Theorem 2.4. Let $\epsilon > 0$

be arbitrary. We will show that there exists an encoder/decoder with parameters N, $K = RN$, $\mu = (1-R-\epsilon)N$, $\Delta \geq K-L$, provided that

$$L \geq 3/\epsilon . \tag{4.7}$$

We proceed as follows. Let H be a $K \times N$ parity-check matrix, and let L satisfy (4.7). Let $D^*(\mu)$ correspond to H, and define

$$\Psi(H) = \begin{cases} 1, & D^*(\mu) < K-L \text{ or } \operatorname{rank}(H) < K , \\ 0, & \text{otherwise} . \end{cases} \tag{4.8}$$

We must show that there exists an H with $\Psi(H) = 0$. We can write

$$\Psi(H) \leq \sum_{\substack{S \subseteq \{1,\ldots,N\} \\ |S| = \mu}} \Phi(H, S) + \Phi_0(H) , \tag{4.9a}$$

where

$$\Phi_0(H) = \begin{cases} 1, & \operatorname{rank}(H) < K , \\ 0, & \text{otherwise} . \end{cases} \tag{4.9b}$$

and

$$\Phi(H, S) = \begin{cases} 1, & D(S) < K-L , \\ 0, & \text{otherwise} . \end{cases} \tag{4.9c}$$

If we choose $H = (\mathbf{C}_1, \ldots, \mathbf{C}_N)$ at random with uniform distribution on the set of $2^{K \cdot N}$ binary $K \times N$ matrices, (4.9) yields

$$E\Psi(H) \leq \sum_{|S| = \mu} E\Phi(H, S) + E\Phi_0(H) . \tag{4.10}$$

Let S, with $|S| = \mu$, be arbitrary, and let $A = (\mathbf{C}_1 \mathbf{C}_2 \ldots \mathbf{C}_{N-\mu})$, where $S = \{i_1, \ldots, i_{N-\mu}\}$. Then $\Phi(H, S) = 1$ if and only if $\operatorname{rank} A < K-L$, and $E\Phi(H, S) = Pr\{\operatorname{rank} A < K-L\}$. We can apply Lemma 4.3 with $n = N-\mu$, $m = K$, to obtain

$$E\Phi(H, S) \leq 2^{-(L+1)(N-\mu-K)+(N-\mu)} . \tag{4.11}$$

Similarly we can apply Lemma 4.4 with $A = H$, $n = N$, $m = K$, to obtain

$$E\,\Phi_0(H) \le \frac{K2^{K-N-1}}{1-2^{K-N-1}} \le \frac{K2^{K-N}}{1-2^{K-N}} . \tag{4.12}$$

Since there are no more than 2^N subsets S, (4.10)-(4.12) yields (using $N-\mu-K = \epsilon N, K = RN$)

$$E\,\Psi(H) \le 2^{-(L+1)(N-\mu-K)+(N-\mu)+N} + \frac{K2^{K-N}}{1-2^{K-N}}$$

$$\le 2^{-L\epsilon N+2N} + \frac{RN2^{-(1-R)N}}{1-2^{-(1-R)N}} . \tag{4.13}$$

Since L satisfies (4.7), the first term in the right member of (4.13) $< 1/2$. Furthermore, for N sufficiently large, the second term in (4.13) is also $< 1/2$. Thus

$$E\,\Psi(H) < 1 .$$

Since $\Psi(\cdot)$ is an integer valued function, there must exist a $K \times N$ matrix H_0 such that $\Psi(H_0) = 0$; so that rank $H_0 = K$ and for the corresponding encoder/decoder, $\Delta = D^*(\mu) \ge K-L$, which is what we set out to prove. Thus we have shown that for arbitrary $R > 0$, the triples (R, α, δ) where $\alpha \le 1-R$, $\delta \le 1$, are achievable, completing the proof of Theorem 2.4.

REFERENCES

[1] Wyner, A. D., "The Wire-Tap Channel," *BSTJ*, **54**, pp. 1355-1387, October 1975.

[2] Gallager, R. G., *Information Theory and Reliable Communication*, Wiley, New York, 1968.

[3] Ozarow, L. H., and A. D. Wyner, "Wire-Tap Channel II", to appear in AT&T Bell Laboratories Technical Journal.