Practical Codes for Photon Communication

ROBERT J. McELIECE, MEMBER, IEEE

Abstract— **In a recent paper, Pierce studied the problems of communicating at optical frequencies using photon-counting techniques, and concluded that "at low temperatures we encounter insuperable problems of encoding long before we approach [channel capacity]." In this paper it is shown that even assuming a noiseless model for photon communication for which capacity (measured in nats/photon) is infinite, it is unlikely that a signaling efficiency of even 10 nats/photon could be achieved practically. On the positive side, it is shown that pulse-position modulation plus Reed–Solomon coding yields practical results in the range of 2 to 3 nats/photon.**

I. Introduction

In [14], Pierce argued that if one uses photon-counting techniques for communication at optical frequencies, channel capacity is hf/kT nats/photon[1] where f is the photon center frequency and T is the noise temperature (h is Planck's constant, k is Boltzmann's constant). Later Pierce, Posner, and Rodemich [15] derived the same result more rigorously. In [14] Pierce also observed that the techniques of linear amplification (which are used successfully at microwave frequencies) yield a capacity of 1 nat/photon. If one has deep-space applications in mind, these results strongly favor photon-counting techniques. For example, if $f = 6 \times 10^{14}$ Hz (green light) and if $T = 400°$ K (an average temperature of space at optical frequencies [5]), we find $hf/kT = 72$ nats/photon. However, channel capacity is an *absolute* limit on performance and only tells us what is possible using arbitrarily complex encoding and decoding strategies. This paper is a study of the "practical" limits of photon communication.

Of course it is a general rule that the closer one approaches channel capacity, the more complex and costly the needed coding strategies become. In the case of photon communication, however, coding problems seem to become serious much sooner than usual, and for an unexpected reason. We shall see below that it is not the noise temperature, but the nature of the photon-counting process itself, that causes the most serious problems; so that even in the limiting case $T = 0$, when capacity is in principle infinite, it seems unlikely that a signalling efficiency of even 10 nats/photon could be achieved practically. This is because, as we will show, when the signalling rate increases beyond 1 nat/photon one encounters an explosive increase in the required bandwidth expansion. This negative result was predicted by Pierce [14] who wrote "at low temperatures we [will] encounter insuperable problems of encoding long before we approach the theoretical limit of [hf/kT nats/photon]".

On the positive side, however, we will show that with pulse position modulation combined with Reed–Solomon coding, it is possible to design a practical photon-counting system which operates at about 3 nats/photon. Since channel *capacity* for linear amplification is only 1 nat/photon, we can conclude from this that photon counting is in fact significantly superior to linear amplification.

In Section II we present a channel model appropriate for the study of noiseless photon communication which we call the photon channel. In Section III we study the use of q-ary pulse position modulation (q-PPM) on the photon channel. There we show that q-PPM channel capacity is $\log q$ nats/photon, and we give performance curves (error probability versus signalling efficiency) for coded and uncoded q-PPM. We conclude by showing that if ρ denotes the signalling rate in nats/photon, and if β denotes the minimum required bandwidth expansion, then $\beta \geq e^{\rho}/\rho$ for PPM. In Section IV we show that this exponential growth of β as a function of ρ is not due to some inherent weakness of PPM by proving that $\beta > (e^{\rho-1} - 1)/\rho$ no matter what modulation scheme is used. Finally in Section V, we discuss the R_0-parameters involved in photon communication. We show that for q-PPM, $R_0 = 1 - 1/q$ nats/photon, whereas for the unrestricted photon channel $R_0 = 1$. If one believes that R_0 is the rate above which reliable communication becomes extremely difficult, our claim that $\rho = 10$ is a "practical" limit even though channel capacity is infinite, is perhaps less baffling.

II. The Photon Channel Model

We assume that any photon communication system works as follows. The time interval during which communication takes place is divided into many subintervals ("slots"), each of duration t_0 seconds. The transmitter is a laser which is pulsed during each time slot; it may be pulsed with a different intensity in each slot. At the receiver is a photon counter which accurately counts the number of photons received during each time slot. We denote by x_i the expected number of photons received

Manuscript received April 28, 1980; revised September 1, 1980. This work was supported by the National Aeronautics and Space Administration under Contract NAS7-100.

The author was with the Jet Propulsion Laboratory, California Institute of Technology, Pasadena. He is now with the Department of Mathematics, and the Coordinated Science Laboratory, University of Illinois, Urbana, IL 61801.

[1]The unit *nats/photon* is somewhat unorthodox, but in the present context seems very natural. Its main advantage is that it is independent of time, which allows us to avoid questions of absolute bandwidth and power and to focus on more fundamental physical limitations.

0018-9448/81/0700-0393$00.75

during the ith time slot; x_i will be called the *intensity* of the ith pulse.

It may be that "noise photons" are present in such a system, but in many cases of practical interest, noise photons are extremely rare. (For example, in a careful analysis of a potentially practical system, Katz [6] estimated the rate of arrival of noise photons to be around 10^{-3} per second.) In any event we shall make the assumption that no noise photons exist.[2] In this case, because of the Poisson nature of photon arrivals, the probability that exactly k photons will be received during a slot in which the laser was pulsed with intensity x is $e^{-x}x^k/k!$.

Thus we have a discrete memoryless channel with an input alphabet equal to the set of nonnegative real numbers (the possible values for the intensities x_i), and output alphabet equal to the set of nonnegative integers (the possible outputs of the photon counter). If a real number x is transmitted, the probability that the integer k will be received is given by

$$p(k|x) = e^{-x}\frac{x^k}{k!}. \tag{2.1}$$

We call the channel described by (2.1) the *photon channel.*

A code for this channel is a set of vectors $\boldsymbol{x}_i = (x_{i1},\cdots,x_{in})$, $i = 1,\cdots,M$, of length n. Each component x_{ij} is a nonnegative real number, and represents an intensity of the transmitting laser. Assuming that each component of a codeword requires one time slot for transmission, the rate of such a code is

$$R = \log M/n \text{ nats/slot.}^3 \tag{2.2}$$

On the other hand, each component x_{ij} represents an average number of (received) photons, and so the code's rate in nats/photon is

$$\rho = R/\mu \text{ nats/photon, where} \tag{2.3}$$

$$\mu = \left(\sum_{i,j} x_{ij}\right)/nM, \text{ photons/slot (average).} \tag{2.4}$$

The reciprocal of the rate R in (2.2) is a measure of "bandwidth expansion". If we are transmitting at a rate of say A nats/s, using a code of rate R nats/slot, it follows that we require A/R slots/second. Thus the slot rate is equal to the nat rate multiplied by the factor $1/R$. We thus define

$$\beta = 1/R = n/\log M \text{ slots/nat,} \tag{2.5}$$

and call β the *bandwidth expansion factor.*

In the following sections, we will make various information-theoretic calculations using this model. The reader should bear in mind that since our chief aim is to show what is not possible, more elaborate models incorporating external noise sources could only strengthen our conclusions.

[2]A careful information-theoretic analysis of the photon channel when noise photons are present is given in [15].

[3]Throughout the paper all logarithms are natural.

III. Pulse Position Modulation

In [14], Pierce suggested the use of pulse position modulation (PPM) for optical communication. In PPM, a fixed integer $q \geq 2$ is selected, and the transmission interval is divided into consecutive blocks of q slots each. In each such block the laser is pulsed in exactly one of the q slots at a fixed intensity λ. We regard each of these q patterns as a letter in the sender's alphabet. For example with $q = 4$, if we denote "no pulse" by 0 and "pulse" by 1, the letters are 1000, 0100, 0010, 0001. There are, however, $q + 1$ possibilities for the received letter, because of the possibility that no photons may be received in a slot in which the laser was pulsed. This erasure symbol (e.g. 0000 if $q = 4$), is by (2.1) received with probability $P_E = e^{-\lambda}$. On the other hand, if each of the q letters is sent with probability q^{-1}, each will carry $\log q$ nats of information, using an average of λ photons, so the rate of this primitive signalling strategy is $\rho = (\log q)/\lambda$ nats/photon. Hence for uncoded PPM, the relation between the error probability P_E and the rate ρ is

$$P_E = q^{-(1/\rho)}. \tag{3.1}$$

It follows from (3.1) that for any fixed $\rho > 0$, and $\epsilon > 0$, there exists a q such that the corresponding PPM system has rate exceeding ρ nats/photon and error probability less than ϵ. This shows that the capacity of the photon channel (measured in nats/photon) is infinite; indeed, this is essentially the argument given by Pierce in [14].

As a practical system, uncoded PPM leaves much to be desired, however. In Fig. 1 we have plotted P_E versus ρ for PPM and $q = 2^5, 2^{10}, 2^{20}$. With $q = 2^{20}$ for example, we can achieve $P_E = 10^{-6}$ and $\rho = 1.0$, but only at the cost of an enormous bandwidth expansion factor (cf. (2.5)) of $\beta = 2^{20}/20\log 2 = 75639$. But we can do much better using *coded* PPM.

In coded PPM, the idea is to regard the q letter transmission alphabet as the input alphabet of a discrete memoryless channel with $q + 1$ output letters. The $(q + 1)$st letter (symbolically 00000) is regarded as an erasure symbol; thus the photon channel of Section II, combined with q-ary PPM becomes a q-ary erasure channel with erasure probability $e^{-\lambda}$. The capacity of this channel, which is achieved by a uniform probability distribution on the input alphabet, is $(1 - e^{-\lambda})\log q$ nats/letter. Since each letter requires an average of λ photons, the channel capacity measured in nats/photon is

$$C(q, \lambda) = \frac{1 - e^{-\lambda}}{\lambda}\log q \text{ nats/photon.} \tag{3.2}$$

If q is fixed, the supremum of $C(q, \lambda)$ over $\lambda > 0$ occurs as $\lambda \to 0$, and is

$$C(q) = \log q \text{ nats/photon.} \tag{3.3}$$

What (3.3) says is that if q-PPM is used, then for small error probability the largest possible value of ρ (cf. (2.3)), in the limit of arbitrarily complex coding, is $\log q$ nats/photon.

But what can be achieved practically? We have found that if q is a power of two, *Reed–Solomon (RS) codes,*

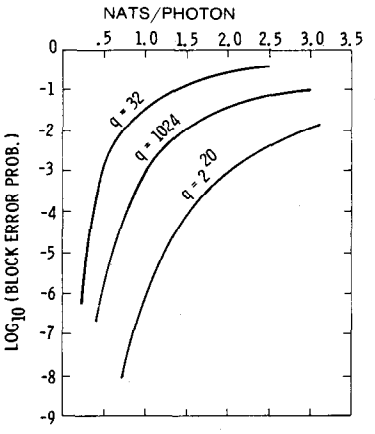

Fig. 1. Performance of uncoded PPM.

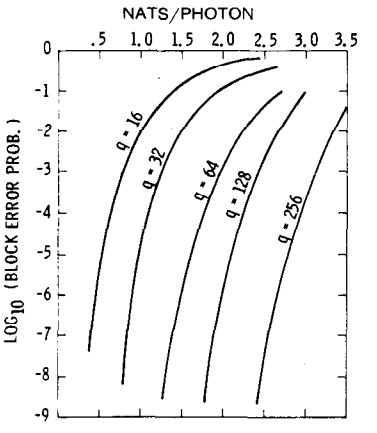

Fig. 2. Performance of Reed–Solomon coded PPM.

which are extremely efficient at correcting erasures, give good performance. An (n, k) Reed–Solomon code with symbol alphabet GF(q), and $n = q - 1$, can correct any pattern of up to $n - k$ erasures. Furthermore, when q is a power of two, very efficient encoding and decoding procedures exist; indeed Berlekamp [2] has described a hardware implementation of a $q = 256$ RS decoder which operates at 40 Mbits/s.

If we use an (n, k) RS code for the present application, each of the q^k codewords carries $k \log q$ nats of information, and each codeword requires n pulses. Thus if we are transmitting ρ nats/photon, the average number of photons/pulse is

$$\lambda = \rho^{-1} \frac{k \log q}{n} \text{ photons/pulse.} \tag{3.4}$$

It follows that the erasure probability for the corresponding q-ary erasure channel is

$$\epsilon = e^{-\lambda} = q^{-R/\rho}, \tag{3.5}$$

where $R = k/n$ is the rate of the RS code. Since the RS code can correct all patterns of up to $n - k$ erasures, the decoding error probability P_E satisfies

$$P_E \leq \sum_{j=n-k+1}^{n} \binom{n}{j} \epsilon^j (1-\epsilon)^{n-j}, \tag{3.6}$$

where ϵ is given in (3.5). In Fig. 2 we have plotted this bound on P_E versus ρ for five typical RS codes. The curve labelled $q = 16$ is for a (15, 8) RS code with $q = 16$. The others are (31, 16), $q = 32$; (63, 32), $q = 64$; (127, 64), $q = 128$; and (255, 128), $q = 256$. (Recall that as codes for the photon channel, the length is actually $n = 16 \cdot 15 = 240$ for the $q = 16$ code; $n = 31 \cdot 32 = 992$ for $q = 32$; $n = 4032$ for $q = 64$; $n = 16256$ for $q = 128$; and $n = 65280$ for $q = 256$.) Each of these codes is the best RS code of its length, at least in the limit as $\rho \to 0$, and so no significant improvement is possible merely by altering the code rate k/n.

We see by comparing Figs. 1 and 2 that, for example, at $P_E = 10^{-6}$ coded PPM with $q = 32$ works as well as uncoded PPM with $q = 2^{20}$. This represents an enormous reduction in bandwidth expansion (from $2^{20}/\log(2^{20}) = 75639$ down to $(32/\log(32)) \times (31/16) = 18$) at only a modest increase in receiver complexity.

On the other hand, by extrapolation we can see from Fig. 2 that even using coded PPM, one needs a very large q to obtain say $P_E = 10^{-6}$ at $\rho = 5$. More generally, if q-ary PPM is used, each of the q input letters carries at most $\log q$ nats of information, so the bandwidth expansion β must be $\geq q/\log q$. However, from (3.3), $\rho < \log q$, and so for $\rho > 1$, we must have

$$\beta \geq \frac{e^\rho}{\rho}. \tag{3.7}$$

Thus if PPM is used, the bandwidth occupancy must grow exponentially with ρ. In the next section we will see that any communication strategy for the photon channel will encounter similar difficulties.

IV. A Negative Result

In the last section we saw that PPM forces an exponential increase in bandwidth expansion as a function of ρ. We now show that any reliable coded communication system for the photon channel must encounter similar difficulties, viz.:

$$\beta > \frac{e^{\rho-1} - 1}{\rho}. \tag{4.1}$$

To prove (4.1), we return to the photon channel model of Section II, and consider the mutual information $I(X; K)$, where X is a nonnegative random variable and K is a nonnegative integer-valued random variable related to X by the conditional probabilities (2.1). We now define

$$C(\mu) = \sup\{I(X; K) : E(X) = \mu\}. \tag{4.2}$$

According to Shannon's noisy-channel coding theorem (see [4, ch. 7]), $C(\mu)$ represents the maximum possible rate (in nats per slot) of a reliable communication system which is restricted to operate at an average of μ photons per slot. By a well-known inequality (see e.g. [9, ch. 1]),

$$I(X; K) \leq H(K), \tag{4.3}$$

where $H(K)$ denotes the entropy $\Sigma p_k \log p_k$ of the random variable K. Since for the photon channel $E(K \mid X) = X$, it

follows that $E(K) = E(E(K|X)) = E(X)$, and so K has the same mean as X, viz., μ.

The problem of maximizing the entropy of a nonnegative integer-valued random variable with given mean was solved by Stern [17], indeed in essentially this context. (Stern's problem was that of finding the maximum-entropy photon source, given an average-power constraint.) The result is

$$H(K) \leq \log(1+\mu) + \mu \log\left(1 + \frac{1}{\mu}\right),$$

with equality if and only if $\Pr\{K = k\} = (1-p)p^k$, $p = \mu/(1+\mu)$. Thus from (4.2) we have the estimate

$$C(\mu) \leq \log(1+\mu) + \mu \log\left(1 + \frac{1}{\mu}\right). \tag{4.4}$$

It follows then from (4.4) and the converse to the noisy-channel coding theorem, [4, th. 7.3.1], that the rate R of a reliable communication system which operates at an average of μ photons per slot is bounded by the right side of (4.4). Using the inequality $\log(1+\mu) \leq \mu$, we have

$$R < \mu(1 + \log(1 + 1/\mu)). \tag{4.5}$$

The rate R in (4.5) is in nats per slot. The rate measured in nats/photon is by (2.3) R/μ, and so

$$\rho < 1 + \log(1 + 1/\mu). \tag{4.6}$$

For $\rho > 1$ a simple manipulation of (4.6) yields

$$\mu < (e^{\rho - 1} - 1)^{-1}. \tag{4.7}$$

Now since the bound on the right side of (4.5) is an increasing function of μ, it follows from (4.5) and (4.7) that

$$R < \frac{\rho}{e^{\rho-1} - 1},$$

which proves (4.1) since $R = \beta^{-1}$.

Equation (4.1) implies that one encounters an explosive increase in the required bandwidth expansion beyond $\rho = 1$. In the next section we will show that the R_0-parameter for the photon channel is $\rho_0 = 1$ nat/photon.

Thus for the photon channel, (4.1) gives rigorous mathematical substantiation to the widely believed "R_0-conjecture", which is that for any channel R_0 is the rate above which the implementation of reliable communication becomes very difficult. Conversely, if one believes the R_0-conjecture, our claim that $\rho = 10$ is perhaps the ultimate limit of a practical photon communication system, even when channel capacity is infinite, may appear less baffling.

IV. The R_0-Parameters

In this section we will show that the R_0-parameter for the photon channel of Section II is 1 nat/photon. We will also show that if q-PPM is being used, R_0 is $(q-1)/q$ nats/photon. Thus although the capacity of q-PPM is infinitely far removed from the capacity of the unrestricted photon channel, R_0 for PPM is very close to the unrestricted R_0 for even small values of q. This result perhaps justifies our feeling that there is no essential loss of performance involved when PPM is used. (This feeling is reinforced by the results of Snyder and Rhodes [16] which imply that among all modulation schemes using q letters, q-PPM gives the largest possible value for R_0.)

Recall the definition of R_0 for a time-discrete memoryless channel. Let A denote the input alphabet and B the output alphabet, which we assume to be finite or countable. For $x \in A$, $y \in B$, denote by $p(y|x)$ the probability that y will be received given that x is transmitted. For each pair of input letters x_1, x_2, define the Bhattacharyya distance between them as

$$d_B(x_1, x_2) = -\log \sum_{y \in B} \sqrt{p(y|x_1)p(y|x_2)}. \tag{5.1}$$

If X is a random variable taking values in the set A, and if X_1, X_2 are independent random variables with the same distribution as X, define

$$R_0(X) = -\log E(\exp - d_B(X_1, X_2)). \tag{5.2}$$

Finally, the quantity R_0 is defined as

$$R_0 = \sup_X R_0(X), \tag{5.3}$$

the supremum in (5.3) being taken over all possible random variables X taking values in the set A.

Since the function $f(t) = e^{-t}$ is convex upwards, it follows from Jensen's inequality [9, appendix B] that $E(\exp - d) \geq \exp - E(d)$, and hence from (5.2) that

$$R_0(x) \leq E(d_B(X_1, X_2)), \tag{5.4}$$

$$R_0 \leq \sup_X E(d_B(X_1, X_2)). \tag{5.5}$$

These two inequalities prove to be very useful in estimating R_0 in specific cases, as we will see below.

We consider the photon channel with q-PPM first. Here $|A| = q$, $B = A \cup \{?\}$, where "?" is the erasure symbol, and the channel transition probabilities are given by

$$p(y|x) = \begin{cases} 1 - e^{-\lambda}, & \text{if } y = x, \\ e^{-\lambda}, & \text{if } y = ?, \\ 0, & \text{otherwise.} \end{cases}$$

From this we easily compute that the Bhattacharyya distances are given by

$$d_B(x_1, x_2) = \begin{cases} 0, & \text{if } x_1 = x_2, \\ \lambda, & \text{if } x_1 \neq x_2. \end{cases} \tag{5.6}$$

Hence by (5.4) we have, for any random variable X,

$$R_0(X) \leq \lambda \cdot \Pr\{X_1 \neq X_2\}, \tag{5.7}$$

the units in (5.7) being nats/letter. If we denote the probability $\Pr\{X = x\}$ by $p(x)$, then

$$P\{X_1 \neq X_2\} = 1 - \sum_{x \in A} p(x)^2 \leq 1 - \frac{1}{q},$$

since by Schwarz's inequality $(\Sigma p(x) \cdot 1)^2 \leq \Sigma p(x)^2 \cdot \Sigma 1^2 =$

$q \cdot \Sigma p(x)^2$. Thus from (5.7)

$$R_0(X) \leq \lambda\left(1 - \frac{1}{q}\right) \text{ nats/letter}, \tag{5.8}$$

or since each transmitted letter requires λ photons on the average,

$$R_0 \leq 1 - \frac{1}{q} \text{ nats/photon}. \tag{5.9}$$

On the other hand, if X is uniformly distributed on the input alphabet, a simple calculation gives

$$R_0(X) = -\frac{1}{\lambda} \log\left(e^{-\lambda} + (1 - e^{-\lambda})/q\right) \text{ nats/photon}. \tag{5.10}$$

The limit of (5.10) as $\lambda \to 0$ is easily seen to be $(q-1)/q$, and so we conclude that $R_0 \geq (q-1)/q$. This, combined with (5.9) shows that for q-PPM,

$$R_0(q) = (q-1)/q \text{ nats/photon}. \tag{5.11}$$

We turn now to the unrestricted photon channel. Here the input alphabet A is the set of nonnegative real numbers, and the output alphabet B is the set of nonnegative integers, with the transition probability given by (2.1). The first step in computing R_0 for this channel is the computation of the Bhattacharyya distances. According to (5.1) and (2.1),

$$\begin{aligned} \exp - d_B(x_1, x_2) &= \sum_{k=0}^{\infty} \sqrt{p(k|x_1)p(k|x_2)} \\ &= e^{-(x_1+x_2)/2} \sum_{k=0}^{\infty} \frac{1}{k!} \sqrt{x_1 x_2}^k \\ &= e^{-(x_1+x_2)/2} e^{\sqrt{x_1 x_2}} \\ &= \exp - \left(\sqrt{x_1} - \sqrt{x_2}\right)^2/2. \end{aligned} \tag{5.12}$$

Hence

$$d_B(x_1, x_2) = \left(\sqrt{x_1} - \sqrt{x_2}\right)^2/2. \tag{5.13}$$

Note also that if we only take the term $k = 0$ in the sum in (5.12) we get the estimate

$$d_B(x_1, x_2) \leq (x_1 + x_2)/2. \tag{5.14}$$

It thus follows immediately from (5.14) and the bound (5.4) that

$$R_0(X) \leq E(X) \text{ nats per slot}. \tag{5.15}$$

In words, (5.15) says that if the average laser intensity is $E(X) = \mu$ photons per slot, then the R_0-parameter is at most μ nats per slot. In units of nats/photon then, it follows from (5.15) that

$$R_0 \leq 1 \text{ nat/photon}. \tag{5.16}$$

But we have seen in (5.11) that $R_0(q) = 1 - 1/q$. Thus by taking q sufficiently large, R_0 can be made as close to one as desired. This fact combined with (5.16) shows that $R_0 = 1$, as claimed.

Acknowledgment

The results in this paper have been considerably influenced by the work of several other researchers at the Jet Propulsion Laboratory, including most especially Joseph Katz, Richard Lipes, Eugene Rodemich, Arthur Rubin, and Lloyd Welch. Indeed, many of the results in this paper have already appeared in [10]–[13]. I would also like to point out that in [12], it is shown that as ρ increases above one the needed ratio of peak-to-average signal power also increases exponentially.

References

[1] L. D. Baumert, R. J. McEliece, and M. Rumsey, Jr., "Coding for optical channels," Jet Propulsion Laboratory Deep Space Network Progress Reports, Pasadena, CA 91103, vol. 42–49, pp. 70–77, 1978.

[2] E. R. Berlekamp, "The technology of error-correcting codes," *Proc. IEEE*, vol. 68, pp. 564–593, 1980.

[3] S. Butman, J. Katz, and J. R. Lesh, "Practical limitations on noiseless optical channel capacity," Jet Propulsion Laboratory Deep Space Network Progress Reports, Pasadena, CA 91103, vol. 42–55, pp. 12–14, 1979.

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

[5] S. Gulkis, private communication. Excerpt: "By definition, the sky brightness temperature is that temperature T which when used in the Planck blackbody radiation law yields the observed sky brightness $\cdots$(Using Fig. 1 in the paper by Longair and Sunyaev, Soviet Physics, vol. 14, no. 5, March–April, 1972) the optical radiation of normal galaxies in the 1μ to 10μ range is estimated to be 10^{-23} Wm^{-2} Hz^{-1} sr^{-1}. Taking [this figure for I_ν and] $\nu = 3 \times 10^{14}$ Hz $\cdots$we obtain $T = 377\mathrm{K} \cdots$."

[6] J. Katz, "Comments on the photon channel," privately circulated Jet Propulsion Laboratory memo.

[7] R. Lipes, "Pulse position modulation coding as near optimum utilization of photon-counting channel with bandwidth and power constraints," Jet Propulsion Laboratory Deep Space Network Progress Reports, Pasadena, CA 91103, vol. 42–56, pp. 108–113.

[8] J. L. Massey, "Coding and modulation in digital communications," in *Proc. Int. Zurich Seminar on Digital Communications*, 1974.

[9] R. J. McEliece, *The Theory of Information and Coding*. Reading, MA: Addison–Wesley, 1977.

[10] R. J. McEliece, "The R_0-parameter for optical communication using photon-counting," Jet Propulsion Laboratory Deep Space Network Progress Reports, Pasadena, CA 91103, vol. 42–53, pp. 62–64, 1979.

[11] R. J. McEliece, "Coding for the photon channel," in *Proc. 1979 Nat. Telecommun. Conf.*, pp. 23.3.1–23.3.3.

[12] R. McEliece, E. Rodemich, and A. Rubin, "Practical limits of photon communication," Jet Propulsion Laboratory Deep Space Network Progress Reports, Pasadena, CA 91103, vol. 42–55, pp. 63–67, 1979.

[13] R. McEliece and L. Welch, "Coding for optical channels with photon counting," Jet Propulsion Laboratory Deep Space Network Progress Reports, Pasadena, CA 91103, vol. 42–52, pp. 61–66, 1979.
[14] J. R. Pierce, "Optical channels: practical limits with photon counting," *IEEE Trans. Commun.*, vol. COM-26, pp. 1819–1821, 1978.
[15] J. R. Pierce, E. C. Posner, and E. R. Rodemich, "The capacity of the photon counting channel," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 61–77, Jan. 1981.
[16] D. L. Snyder and I. B. Rhodes, "Some implications of the cutoff-rate criterion for coded direct-detection optical communication systems," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 327–338, May 1980.
[17] T. E. Stern, "Some quantum effects in information channels," *IEEE Trans. Inform. Theory*, vol. IT-6, pp. 435–440, 1960.

To Get a Bit of Information May Be As Hard As to Get Full Information

RUDOLF AHLSWEDE AND IMRE CSISZÁR

Abstract—**The following coding problem for correlated discrete memoryless sources is considered. The two sources can be separately block encoded, and the values of the encoding functions are available to a decoder who wants to answer a certain question concerning the source outputs. Typically, this question has only a few possible answers (even as few as two). The rates of the encoding functions must be found that enable the decoder to answer this question correctly with high probability. It is proven that these rates are often as large as those needed for a full reproduction of the outputs of both sources. Furthermore, if one source is completely known at the decoder, this phenomenon already occurs when what is asked for is the joint type (joint composition) of the two source output blocks, or some function thereof such as the Hamming distance of the two blocks or (for alphabet size at least three) just the parity of this Hamming distance.**

I. Introduction

We are given a discrete memoryless double source (DMDS) with alphabets $\mathcal{X}$, $\mathcal{Y}$, and generic variables X, Y, i.e., a sequence of independent replicas (X_i, Y_i), $i = 1, 2, \cdots$, of the pair of random variables (X, Y) taking values in the finite sets $\mathcal{X}$ and $\mathcal{Y}$, respectively. Slepian and Wolf [9] considered the problem of encoding the source output blocks $X^n \triangleq X_1 \cdots X_n$ resp. $Y^n \triangleq Y_1 \cdots Y_n$ by two separate encoders in such a way that a common decoder could reproduce both blocks with small probability of error. They proved that such an encoding is possible with rates (R_1, R_2) if and only if

$$R_1 \geq H(X|Y), \quad R_2 \geq H(Y|X), \quad R_1 + R_2 \geq H(X, Y). \tag{1.1}$$

Manuscript received March 19, 1980.

R. Ahlswede is with the Department of Mathematics at the University of Bielefeld, 4800 Bielefeld, West Germany.

I. Csiszár was with the University of Bielefeld, on leave from the Mathematical Institute of the Hungarian Academy of Sciences, 1053 Budapest, Hungary.

It may happen, however, that what is actually required at the decoder is to answer a certain question concerning (X^n, Y^n). Such a question can of course be described by a function F of (X^n, Y^n). We are interested in those functions for which the number k_n of possible values of $F(X^n, Y^n)$ satisfies

$$\lim_{n\to\infty} \frac{1}{n} \log k_n = 0. \tag{1.2}$$

This means that the questions asked have only "a few" possible answers. For example, X_i and Y_i may be the results of two different quality control tests performed on the ith item of a lot. Then for certain purposes, e.g., for determining the price of the lot, one may be interested only in the frequencies of the various possible pairs (x, y) among the results, their order, i.e., the knowledge of the individual pairs (X_i, Y_i), being irrelevant. In this case $k_n \leq (n+1)^{|\mathcal{X}||\mathcal{Y}|}$, and (1.2) holds. A natural first question is whether or not it is always true in this case that, for large n, arbitrarily small encoding rates permit the decoder to determine $F(X^n, Y^n)$. To our knowledge, even this seemingly simple question had not been answered prior to this paper, except for the particular case of independent binary X and Y, where one of them takes the values 0, 1 with equal probabilities. In this particular case, Körner [6] showed the necessity of positive rates if both entropies are positive.

We also consider here other choices of F and first obtain the following result. For every DMDS with

$$H(X|Y) > 0, \quad H(Y|X) > 0$$

there exists a binary question (function F with only two possible values) such that in order to answer this question

0018-9448/81/0700-0398$00.75