

Capacity of Frequency-Hop Spread-Spectrum Multiple-Access Communication Systems

MANJUNATH V. HEGDE, MEMBER, IEEE, AND WAYNE E. STARK, MEMBER, IEEE

Abstract—The information theoretic capacity of frequency-hop spread-spectrum multiple-access communication is considered. In order to account for independent encoding and decoding and private (to the sender and receiver) hopping patterns an interference channel model is adopted with K sender-receiver pairs with the i th receiver only interested in the message transmitted by the i th sender. Both synchronous and asynchronous hopping patterns are investigated. Although the channel exhibits memory in the latter case, we are able to compute the capacity region. The asymptotic normalized sum capacity is also computed.

I. INTRODUCTION

IN this paper, we consider the multiple-access capability of frequency-hop spread-spectrum communication systems from an information theoretic viewpoint. This capability is calculated by modeling the communication system from the modulator input to the demodulator output as an interference channel and determining the capacity region of this channel. We examine synchronous and asynchronous hopping patterns and consider the cases of side information at the receiver and no side information at the receiver.

There have been several recent studies of multiple-access performance of spread-spectrum communication systems [1], [3]. These have concerned themselves with the probability of error of packets or codewords over such multiple-access channels using specific codes, typically Reed-Solomon codes. For the (much harder to analyze) unslotted channel they have used bounding techniques to approximate the packet or codeword error probability ([4]). In this paper, we address the issue of performance with the best possible codes. Here we examine only the slotted channel with both synchronous and asynchronous hopping each with and without side information and determine the capacity region. In all the cases we use simple "hit" models which are popular in the literature [1], [3], [4] and which approximately describe the symbol error probability in a frequency hopped multiple-access system. Our results indicate that memory does not seem to affect the capacity of such systems significantly and allow us to find the optimal number of users to maximize the sum capacity in all the cases mentioned above. More accurate models taking partial hits into consideration and utilizing error probabilities depending on the number of interferers and, possibly, their data symbols, are possible but this complicates the analysis enormously. We simplify the situations but do so conservatively, i.e., by assuming a partial hit is a hit and by using upper bounds on the error probability when a symbol is hit. Thus, our capacity results may be viewed as inner bounds on the actual capacity regions.

We do not allow cooperation between users either at the encoder or at the decoder. This makes the interference channel model more

Paper approved by the Editor for Spread Spectrum of the IEEE Communications Society. Manuscript received September 15, 1988; revised May 15, 1989. This work was supported by the Office of Naval Research under Contract N0014 85 K0545. This paper was presented in part at the 1989 Conference on Information Sciences and Systems, The Johns Hopkins University, Baltimore, MD.

M. V. Hegde is with the Electrical and Computer Engineering Department, Louisiana State University, Baton Rouge, LA, 70803.

W. E. Stark is with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109-2122.

IEEE Log Number 9036339.

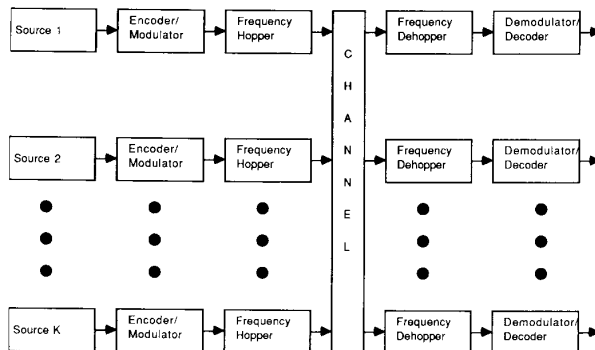


Fig. 1. Multiuser frequency-hop spread-spectrum communication system.

appropriate to our situation rather than the multiple-access channels. Using this model we are able to calculate the capacity region in each of the cases mentioned above. We then focus our attention on the largest possible total rate that can be achieved by all users.

II. CHANNEL MODELS

The model for multiple-access frequency-hop spread-spectrum communication consists of K source-receiver pairs with the i th source desiring to communicate only with its corresponding receiver over a common channel (see Fig. 1). There are K separate encoder devices: one for each source. The i th encoder has as its input only the messages from the i th source and produces a symbol $x^{(i)} \in X$ (the common input alphabet). This symbol is transmitted by modulating and frequency-hopping the desired symbol. The i th receiver examines its assigned hopping pattern, demodulates the received waveform and produces the output symbol $y^{(i)} \in Y$ (the common output alphabet). Decoding is done independently at the i th receiver. The i th source may transmit one of $[2^{nR_i}]$ messages and this is then encoded by the i th encoder, modulated using one of M signals, and then frequency hopped by the i th frequency hopper to one of q frequency slots. The hopping patterns are modeled by independent sequences equiprobable over the q slots. Thus, each component of each of the K input vectors of length n is chosen from the common alphabet $\{1, 2, \dots, M\}$. We assume l encoded symbols are transmitted per hop and this is incorporated into the channel alphabet size M . We assume that the channel is slotted and thus the number of transmissions during a slot is constant.

The hopping patterns we consider are modeled by independent sequences, one for each sender-receiver pair, equiprobable over the q slots. In the case of synchronous hopping, this makes the channel hits (i.e., the event of more than one user transmitting over the same frequency slot) independent. However, in the case of asynchronous hopping patterns, the occurrence of past hits for a particular user affects the conditional distribution of the frequency slots used by the $K - 1$ other users and so the sequence of hits for any particular user exhibits memory. Moreover, it turns out that this sequence is not even Markovian [5]. In this paper, we demonstrate that this sequence is a function of an underlying Markov chain which enables us to treat the marginal channels in the asynchronous case as finite state

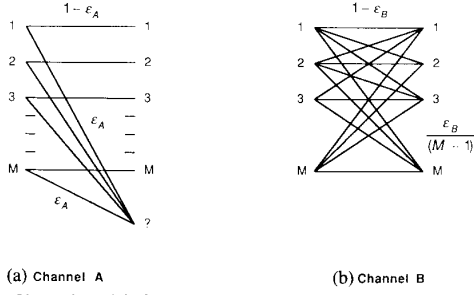


Fig. 2. Channel models for synchronous frequency hopped spread-spectrum communications system (a) with side information, (b) without side information.

channels thereby allowing us to compute the capacity regions of the K -user channel with asynchronous hopping in both the case with side information at the receiver (knowledge about whether each received symbol was hit or not) and the case with no side information at the receiver. We consider only the noise arising from interference due to other users and do not include any other background noise in our analysis (although it would not be difficult to do so).

Case A) Synchronous Hopping-Side Information Available: We first examine the case of synchronous hopping patterns and thus consider a memoryless channel model (since the symbol hits are independent in this case). The side information referred to is the awareness of each of the K decoders about whether or not there was a hit on the corresponding transmission. To allow for the possibility of not detecting hits we use a parameter e_e to denote the conditional probability of a symbol which is hit being erased. This model is shown in Fig. 2(a) where the event of an erasure is defined as “?”. It is easy to see that the symbol erasure probability is

$$\epsilon_A \triangleq P\{\text{erasure}\} = e_e(1 - (1 - p)^{K-1}) \quad (1)$$

where $p = 1/q$.

Case B) Synchronous Hopping-No Side Information Available: Here again synchronous hopping is considered but in this case the decoders do not receive any information about hits on each symbol. Thus, the hits remain undetected and cause a symbol error with probability e_0 [see Fig. 2(b)]. Whenever an error does occur, the affected symbol is equally likely to be decoded as any of the other $M - 1$ symbols. Thus, the crossover probabilities shown in Fig. 2(b) are all equal to $\epsilon_B/(M - 1)$ where

$$\epsilon_B/(M - 1) \triangleq P\{\text{error}\} = (1 - (1 - p)^{K-1})e_0/(M - 1). \quad (2)$$

Note that in our model we do not distinguish one hit from more than one hit in the conditional probability of error e_0 , i.e., e_0 does not depend on the number of other users who “hit.”

Case C) Asynchronous Hopping-Side Information Available: We now address the situation where the hopping is asynchronous and the receivers have side information which enables the demodulator and decoder to determine which symbols have been hit. It is assumed that all symbols that have been hit are erased. We need to introduce some notation which we do with the aid of Fig. 3. Each user employs a hopping pattern with frequencies chosen uniformly from the set $\{1, \dots, q\}$ and independently of the frequencies chosen by the other users. We denote the random hopping pattern for user i as $\{F_{i,j}, j = 0, 1, \dots\}$. (All capital letters will denote random quantities (variables or vectors), and the corresponding lower case letters will denote particular realizations of these random quantities). Observe that two channel symbols of user i overlap in time with the j th channel symbol of user 1. We number the hops as follows (see Fig. 3). For the i th user ($i \neq 1$) we denote the first hop after the j th hop of user 1 as $F_{i,j}$. Thus user i will interfere with the j th symbol of user 1 on the right if and only if $F_{i,j} = F_{1,j}$. Similarly user i will interfere with the j th symbol of user 1 on the left if and only if $F_{i,j-1} = F_{1,j}$. We define the set of frequency slots used by the $K - 1$ other users

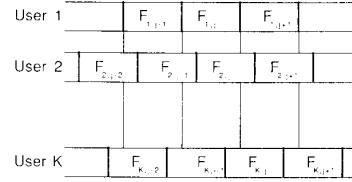


Fig. 3. Timing diagram for frequency-hopped multiple-access.

for transmitting symbol j as $\tilde{F}_j = (F_{2,j}, \dots, F_{K,j})$. Now suppose all K users are transmitting packets and receiver 1 (which desires to receive user 1's messages) locks onto user 1's hopping pattern. We assume that user 1 transmits using frequencies $F_{1,1}, F_{1,2}, \dots, F_{1,n}$. We denote by $H_j, j = 1, \dots, n$, n binary random variables such that $H_j = 1$ if the j th symbol transmitted by user 1 is hit (i.e., if at least one of the other $K - 1$ users uses the same frequency during the slot corresponding to the j th channel symbol) and $H_j = 0$, otherwise. We note that $H_j = 1$ if and only if $F_{1,j} \in \tilde{F}_{j-1} \cup \tilde{F}_j$. We also will need the binary random variables $H_j^L, H_j^R, j = 1, 2, \dots, n$ defined as follows:

$$H_j^L = \begin{cases} 1 & F_{1,j} \in \tilde{F}_{j-1} \\ 0 & \text{otherwise,} \end{cases}$$

$$H_j^R = \begin{cases} 1 & F_{1,j} \in \tilde{F}_j \\ 0 & \text{otherwise} \end{cases}$$

where the superscripts L and R refer to overlapping from the right and left, respectively. Finally, let S_j^i be the number of frequency slots out of time slots $i, i + 1, \dots, j$ of user 1 that have been hit.

Note that in the model we have just described the set $\{F_{i,j}; i = 1, 2, \dots, K, j = 0, 1, \dots, n\}$ is an independent identically distributed (i.i.d.) set of random variables with each $F_{i,j}$ being uniformly distributed on the set $1, 2, \dots, q$ and consequently $\{\tilde{F}_j; j = 0, 1, \dots, n\}$ is an i.i.d. sequence. $H_j = 1$ if and only if $H_j^L = 1$ or $H_j^R = 1$; also $S_j^i = H_i + \dots + H_j$. Now we can state our key lemma.

Lemma 1: The sequence (H_j^L, H_j^R) is a Markov chain.

Proof: See Appendix A.

Note: In the sequence $(\dots, H_{j-1}^L, H_{j-1}^R, H_j^L, H_j^R, \dots)$, H_j^L depends on H_{j-1}^R but is independent of H_{j-1}^L and H_j^R . The reason why H_j is not a Markov chain (for $K > 2$) is that knowledge of H_{j-1}, H_{j-2}, \dots affects our *posteriori* distribution of $\tilde{F}_k, k = j - 1, j - 2, \dots$ and thereby H_{j-1}^L thus making

$$P(H_j | H_{j-1}, H_{j-2}, \dots) \neq P(H_j | H_{j-1}).$$

Since $H_j = 1$ iff $H_j^L = 1$ or $H_j^R = 1$ we recognize that the sequence of symbol hits is really a function of the underlying stationary Markov chain (H_j^L, H_j^R) with four states, viz. $(H_j^L, H_j^R) = (0, 0), (0, 1), (1, 0),$ or $(1, 1)$. For the sake of brevity we use $U_j^{(i)}$ to denote the state of the component channel between the i th sender and the corresponding receiver during the j th symbol transmission, i.e., $U_j^{(i)} = (H_j^L, H_j^R)$ for the i th component channel.

This Markov chain, (H_j^L, H_j^R) is shown in Fig. 4 and the transition probabilities are calculated in Appendix B. In the K -user situation each of the K component channels (between the i th sender and the corresponding receiver) is thus a finite state channel. Corresponding to state $a = (0, 0)$ we have a noiseless channel and corresponding to states $b = (0, 1), c = (1, 0),$ or $d = (1, 1)$ [i.e., a hit on the current symbol] we have a channel which puts out an erasure symbol.

Case D) Asynchronous Hopping-No Side Information Available: Finally, we address the case where the hopping is asynchronous and the decoders receive no information about whether a symbol is hit or not. Hits are thus undetected and cause errors with probability e_0 . The component channel in this case may be modeled as an M -ary input M -ary output channel where the output letters Y_j associated with the input X_j are given by $Y_j = X_j \oplus H_j R_j$ where H_j is the

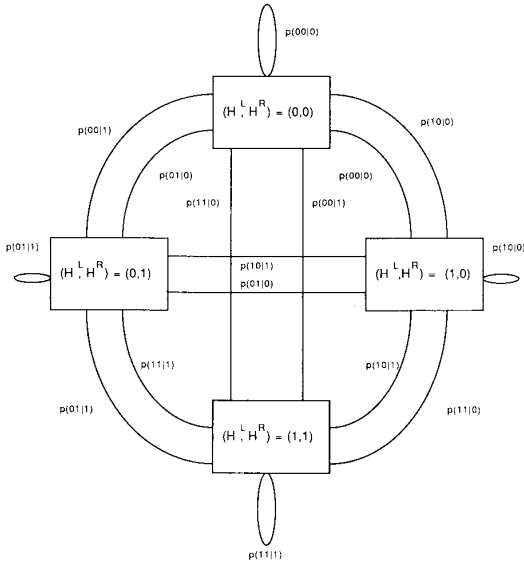


Fig. 4. Markov chain for asynchronous frequency-hopped spread-spectrum multiple-access communications with side-information.

random variable (defined earlier) which is 1 if the j th symbol was hit and is 0 otherwise and R_j is a random variable independent of the input and independent of H_j with a distribution on $\{0, 1, \dots, M-1\}$ such that $P(R_j = 0) = 1 - e_0$ and $P(R_j = l) = e_0/(M-1)$ for $l = 1, 2, \dots, M-1$. Finally, the addition \oplus is modulo M addition.

III. CAPACITY REGIONS

We observe that in both the synchronous cases our models are a simple case of a K -user discrete memoryless interference channel, i.e., a channel characterized by a probability density $p(y^{(1)}, \dots, y^{(K)} | x^{(1)}, \dots, x^{(K)})$ with the i th sender trying to communicate with the i th receiver through independent encoders and decoders. The capacity region for such channel is not known in general but various inner and outer bounds have been developed for it [6]. Our channels fall into a simple class known as separated channels for which the marginal probabilities $p(y^{(i)} | x^{(1)}, \dots, x^{(K)})$ do not depend on $x^{(j)}$, $j \neq i$, i.e.,

$$p(y^{(i)} | x^{(1)}, \dots, x^{(K)}) = p(y^{(i)} | x^{(i)}).$$

This property is obtained on account of the channel models we have adopted. In Case A) all hits cause an erasure with probability e_e and in Case B) all hits cause an error with probability e_0 (irrespective of the actual data symbols transmitted by the users whose symbols "hit" and cause no error with probability $1 - e_0$). Since the capacity region depends only upon the conditional probabilities $p(y^{(i)} | x^{(1)}, \dots, x^{(K)})$ we see from the converse to the coding theorem for the two-user channel that the maximum rate of reliable transmission for the i th sender-receiver pair cannot be more than $\max_{Q_i} I(X_i; Y_i)$ where X_i and Y_i are related by the conditional probability distribution $p(y^{(i)} | x^{(i)})$ and Q_i is the input distribution. Clearly, this rate will be a bound for to the rate of reliable transmission between the i th sender and receiver in the multiple-access case. This rate can actually be simultaneously achieved by maximizing each Q_i individually and hence we see that the capacity region is

$$0 \leq R_i \leq C_i \quad (3)$$

where $C_i = \max_{Q_i} I(X_i; Y_i)$.

In the asynchronous case we similarly see that

$$p(y^{(i)} | x^{(1)}, \dots, x^{(i)}, \dots, x^{(K)}, u^{(1)}, u^{(2)}, \dots, u^{(K)}) \\ = p(y^{(i)} | x^{(i)}, u^{(i)})$$

where the $u^{(i)}$'s are the states of the underlying Markov chain corresponding to the i th sender-receiver pair. Thus again from the converse to the coding theorem for the single user channel [9] the maximum rate of reliable information transmission cannot be more than the capacity of this finite state two user channel. Again, clearly this rate will be a bound to the rate of reliable transmission in the multiple-access case and since we can actually simultaneously achieve this rate for all users by suitable choice of input probabilities (in fact, by i.i.d. inputs) we see that the capacity region of this communication system is

$$0 \leq R_i \leq C_i, \quad 1 \leq i \leq K \quad (4)$$

where C_i is the capacity of the finite state channel corresponding to the i th sender-receiver pair.

We now calculate the interference capacities for the models described above.

Case A) (Synchronous Hopping, Side Information Available):

$$R_i \leq C_i = (1 - \epsilon_A) \log_2 M, \quad i = 1, \dots, K \quad (5)$$

where q is fixed. For $e_e = 1$, the sum of the rates of the individual users, $R_{\text{sum}} = \sum_{i=1}^K R_i$, is maximized by

$$K^* = \frac{-1}{\ln(1-p)}$$

for which the sum rate is

$$R_{\text{sum}} \leq C_{\text{sum}} \triangleq \sum_{i=1}^K C_i = \frac{-1}{\ln(1-p)} \frac{e^{-1}}{1-p} \log_2 M.$$

For large q the optimum number of users approaches q , i.e.,

$$\lim_{q \rightarrow \infty} \frac{K^*}{q} = 1 \quad (6)$$

and

$$\lim_{q \rightarrow \infty} \frac{K^* C_i}{q} = e^{-1} \log_2 M. \quad (7)$$

Case B) (Synchronous Hopping, No Side Information Available):

$$R_i \leq C_i = \log_2 M - h_M(\epsilon_B), \quad i = 1, \dots, K \quad (8)$$

and

$$R_{\text{sum}} \leq C_{\text{sum}} = K(\log_2 M - h_M(\epsilon_B)) \quad (9)$$

where

$$h_M(x) \triangleq -x \log_2(x/(M-1)) - (1-x) \log_2(1-x). \quad (10)$$

The limiting sum capacity for $K = \lambda q$ with λ fixed is

$$\lim_{q \rightarrow \infty} \frac{C_{\text{sum}}}{q} = \lambda(\log_2 M - h_M(e_0(1 - e^{-\lambda}))). \quad (11)$$

With $M = 2$ and $e_0 = 1/2$, optimizing the above over λ gives $\lambda^* = 0.46$ and $\lim_{q \rightarrow \infty} q^{-1} C_{\text{sum}} = 0.143$.

Case C) (Asynchronous Hopping, Side Information Available): The channel model for the i th user is a finite state channel with four states a, b, c , and d . Since the Markov chain $U_j = (H_j^L, H_j^R)$ is ergodic and its state sequence is independent of the input we see that our channel model belongs to the class of indecomposable finite state channels with no intersymbol interference memory. We calculate the capacity C_i of the i th component channel as follows (see [9]):

$$C_i = \lim_{n \rightarrow \infty} \max_{Q_n(x^n)} \min_{u_0} \frac{I_Q(X^n; Y^n | u_0)}{n}$$

where $Q_n(\cdot)$ is some n -dimensional joint density on the input and u_0 is some initial state of the Markov chain (H_j^L, H_j^R) . Since the channel is indecomposable and therefore C_i is independent of the initial state of the Markov chain and may be written as

$$C_i = \lim_{n \rightarrow \infty} \max_{Q_n(x^n)} \frac{I_{Q_n}(X^n; Y^n)}{n}$$

for any initial state u_0 . Now

$$I_{Q_n}(X^n; Y^n) = H(Y^n) - H(Y^n | X^n)$$

and denoting by W_i a random variable which is 1 if the i th symbol is erased and is 0 otherwise, and denoting $p(y_j^{(i)} = ? | x_j^{(i)} = k)$ ($= e_e(1 - (1 - 1/q)^{2(K-1)})$) by ϵ_C , we have (see Appendix C)

$$C_i = (1 - \epsilon_C) \log_2 M.$$

Hence,

$$R_i \leq C_i = \left\{ 1 - e_e \left[1 - \left(1 - \frac{1}{q} \right)^{2(K-1)} \right] \right\} \log_2 M, \quad i = 1, \dots, K \quad (12)$$

is the capacity region of the K -user channel in this case. For $e_e = 1$, asymptotically, as the number of frequency slots q approaches infinity with $K = \lambda q$, (λ some constant) we get

$$\left(1 - \left(1 - \left(1 - \frac{1}{q} \right)^{2(K-1)} \right) \right) \rightarrow 1 - (1 - e^{-2\lambda}) = e^{-2\lambda}. \quad (13)$$

Hence, asymptotically $C_i = e^{-2\lambda} \log_2 M$. Optimizing

$$\lim_{q \rightarrow \infty} C_{\text{sum}}/q = \lim_{q \rightarrow \infty} \sum_i C_i/q = \lambda e^{-2\lambda} \log_2 M$$

over λ gives $\lambda^* = 0.5$ and $\lim_{q \rightarrow \infty} \sum_i C_i/q = 0.5e^{-1} \log_2 M$.

Case D) (Asynchronous Hopping, No Side Information Available): In this case, with asynchronous hopping and no side information available we calculate the capacity C_i of the i th component channel using, as in Case C),

$$C_i = \lim_{n \rightarrow \infty} \max_{Q_n(x^n)} \min_{u_0} \frac{I_{Q_n}(X^n; Y^n | u_0)}{n}.$$

Again since the channel is indecomposable C_i is independent of the initial state of the Markov chain and may be written as

$$C_i = \lim_{n \rightarrow \infty} \max_{Q_n(x^n)} \frac{I_{Q_n}(X^n; Y^n)}{n}$$

for any initial state u_0 . Now (see Appendix D)

$$\begin{aligned} I_{Q_n}(X^n; Y^n) &= H(Y^n) - H(Y^n | X^n) \\ &= H(Y^n) - H(Y^n, V^n | X^n) \\ &= H(Y^n) - \left[H(V^n) + \sum_{i=0}^n i P(T_1^n = i) \log_2 (M-1) \right] \end{aligned}$$

where V_n is 1 if an error occurred on the n th symbol and is 0 otherwise and T_1^n is the number of symbols from 1 to n for which an error is made. Hence, (see Appendix D)

$$\begin{aligned} C_i &= \lim_{n \rightarrow \infty} \max_{Q_n(x^n)} \frac{I_{Q_n}(X^n; Y^n)}{n} \\ &= \log_2 M - H_\infty(V) \\ &\quad - e_0 \left(1 - \left(1 - \frac{1}{q} \right)^{2(K-1)} \right) \log_2 (M-1) \quad (13) \end{aligned}$$

since $H(Y^n) \leq n \log_2 M$ with equality for equally likely outputs which are achieved by equally likely inputs and since $\lim_{n \rightarrow \infty} (H(V^n))/n$ is equal to $H_\infty(V)$, i.e., the entropy of the stationary random (non-Markovian) process $\{V_j\}$ which is a function of the Markov chain, $\{(H_j^L, H_j^R, R_j)\}$.

Computing the entropy of a function of a Markov process has been considered by Blackwell [11]. While a closed-form expression for the capacity is not available in our case, tight upper and lower bounds are available [12]. Let $W_j = (H_j^L, H_j^R, R_j)$ be the state of a Markov chain and V_j the function of the state given by $V_j = 1$ if $H_j^L = H_j^R = 1$ and $R_j \neq 0$ and $V_j = 0$ otherwise. Then the entropy $H_\infty(V)$ of V_j is bounded as follows:

$$\begin{aligned} H(V_n | V_{n-1}, V_{n-2}, \dots, V_1, W_0) &\leq H_\infty(V) \\ &\leq H(V_n | V_{n-1}, V_{n-2}, \dots, V_1). \end{aligned}$$

Furthermore these bounds converge exponentially fast in n to $H_\infty(V)$. From [12] it can be seen that the difference between the upper and lower bounds above is less than $D\rho^{n-1}$ where

$$D = \frac{N_D \log e}{N_1 \min_{i,j} m_{i,j}},$$

N_1 and N_D are the minimum and maximum number of states collapsed, respectively, by the function of the Markov chain (in our case $N_1 = M - 1$, $N_D = 3M + 1$), $m_{i,j}$ is the transition probability of the Markov chain W and

$$0 < \rho = 1 - \min_{i,j,k,m,n} \frac{N_1 m_{i,k} m_{k,n}}{m_{i,j} m_{j,m}} < 1.$$

In our model this convergence is especially rapid since for most parameters of interest the Markovian dependence of W_j on W_{j-1} is very "weak," i.e., the transition probabilities are almost independent of the previous state. In fact our numerical results show that the upper and lower bound are essentially identical for $n = 2$, even for moderate values of q . (For $q = 50$ the upper and lower bounds agree out to more than 8 significant digits). In Appendix C, we show a sample calculation of the entropy used in the upper and lower bounds.

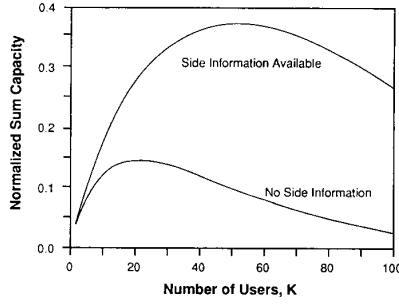
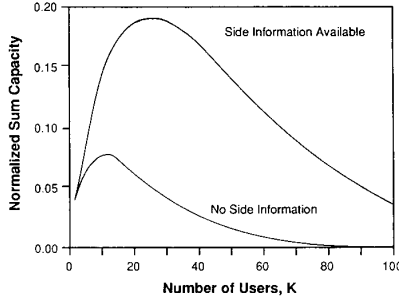
If we let $q \rightarrow \infty$ with $K = \lambda q$ (λ constant) we see that the stationary distribution of the Markov chain $\{U_i\}$ tends to the conditional distribution $P(U_i | U_{i-1})$ with $P(U_j = 00) = 1 - e^{-2\lambda}$, $P(U_j = 01) = P(U_j = 10) = e^{-\lambda}(1 - e^{-\lambda})$ and $P(U_j = 11) = (1 - e^{-\lambda})^2$. Thus, for large q (and $K = \lambda q$) the U_i become independent. Thus for the case of errors occurring with probability $(M-1)/M$ given a hit occurs, (i.e., when there is a hit, any of the M outputs are equally likely making $e_0 = (M-1)/M$) asymptotically as K and q become large with $K/q \rightarrow \lambda$

$$\frac{C_{\text{sum}}}{q} = \lambda (\log_2 M - h_M(e_0(1 - e^{-2\lambda}))). \quad (14)$$

Now it is easy to see that the asymptotic normalized capacity of this asynchronous case is exactly half of the synchronous normalized capacity when optimized over λ .

IV. NUMERICAL RESULTS AND CONCLUSIONS

In Fig. 5 we show the sum capacity for the case of synchronous hopping with $q = 50$ and $M = 2$ while in Fig. 6 we show the sum capacity for the case of asynchronous hopping with $q = 50$ and $M = 2$. When there is no side information the errors are assumed to occur with probability 1/2. In all cases, it is clear that there is an optimal number of users to maximize the sum capacity. A careful examination of the numerical results show that q need not be very large for the asymptotic results to give a very accurate approximation to the capacity of these channels. Also the asymptotic value for the optimum number of simultaneous users is a good approximation for the actual value for finite q . For the asynchronous case without side information the upper and lower bounds were virtually identical for the case of $q = 50$. The tightness of the bounds is due to the fact

Fig. 5. Normalized sum capacity for synchronous hopping with $q = 50$.Fig. 6. Normalized sum capacity for asynchronous hopping with $q = 50$.

that for even reasonable values of q the sequence of errors in the channel is essentially an i.i.d. process. For $M > 2$, in the cases with perfect side information (i.e., $e_e = 1$) the sum capacity differs from that in the $M = 2$ case by just a scale factor. In the cases with no side information the optimum K for a given q seems to be larger.

In this paper, we have determined the multiple-access capability of frequency-hopped spread-spectrum for four different models. The interference is either modeled as causing errors with a given probability when two or more users hopped to the same frequency at the same time or as causing erasures with a certain probability. The key result was identifying the underlying Markov chains, (H_j^L, H_j^R) or (H_j^L, H_j^R, R_j) . Using the Markovian properties of the underlying process also allows one to recursively compute the error probabilities of block codes for these channels (see [8]) and for channels with combinations of errors and erasures.

APPENDIX A

Lemma 1: (H_j^L, H_j^R) is a Markov chain.

Proof:

$$\begin{aligned} & P(H_j^L, H_j^R | H_{j-1}^L, H_{j-1}^R, H_{j-2}^L, H_{j-2}^R, H_{j-3}^L, H_{j-3}^R, \dots) \\ &= \frac{P(H_j^L, H_j^R, H_{j-1}^L, H_{j-1}^R, H_{j-2}^L, H_{j-2}^R, H_{j-3}^L, H_{j-3}^R, \dots)}{P(H_{j-1}^L, H_{j-1}^R, H_{j-2}^L, H_{j-2}^R, \dots)} \\ &= \frac{A}{B} \text{ (say).} \end{aligned}$$

We write A as follows:

$$A = P(F_{1,j} \in {}^L_j \tilde{F}_{j-1}, F_{1,j} \in {}^R_j \tilde{F}_j, F_{1,j-1} \in {}^L_{j-1} \tilde{F}_{j-2}, \dots, F_{1,j-1} \in {}^R_{j-1} \tilde{F}_{j-1} \dots)$$

where $\in {}^L_j$ is \in if $H_j^L = 1$ and \notin if $H_j^L = 0$ and $\in {}^R_j$ is \in if $H_j^R = 1$ and \notin if $H_j^R = 0$. Now

$$A = \sum_{f_{1,j-1}} P(F_{1,j} \in {}^L_j \tilde{F}_{j-1}, F_{1,j} \in {}^R_j \tilde{F}_j, F_{1,j-1} \in {}^L_{j-1} \tilde{F}_{j-2}, \dots)$$

$$\begin{aligned} & P(F_{1,j-1} \in {}^R_{j-1} \tilde{F}_{j-1}, \dots | F_{1,j-1} = f_{1,j-1}) \\ & \cdot P(F_{1,j-1} = f_{1,j-1}) \\ &= \sum_{f_{1,j-1}} P(F_{1,j} \in {}^L_j \tilde{F}_{j-1}, F_{1,j} \in {}^R_j \tilde{F}_j, f_{1,j-1} \in {}^L_{j-1} \tilde{F}_{j-2}, \dots) \\ & \cdot P(f_{1,j-1} \in {}^R_{j-1} \tilde{F}_{j-1} \dots) \frac{1}{q} \\ &= \sum_{f_{1,j-1}} P(F_{1,j} \in {}^L_j \tilde{F}_{j-1}, F_{1,j} \in {}^R_j \tilde{F}_j, f_{1,j-1} \in {}^R_{j-1} \tilde{F}_{j-1}) \\ & \cdot P(f_{1,j-1} \in {}^L_{j-1} \tilde{F}_{j-2}, F_{1,j-2} \in {}^L_{j-2} \tilde{F}_{j-3} \dots) \frac{1}{q} \end{aligned}$$

using the independence of $F_{1,j}, F_{1,j-1}, F_{1,j-2}, \dots, \tilde{F}_j, \tilde{F}_{j-1}, \tilde{F}_{j-2}, \dots$ in the last equality. Now from the fact that $F_{i,j}$ for each user i is a random variable uniformly distributed over the set $\{1, \dots, q\}$ and $F_{i,j}$ and $F_{k,j}$ are independent and identically distributed for $i \neq k$ we see that $P(F_{1,j} \in {}^L_j \tilde{F}_{j-1}, F_{1,j} \in {}^R_j \tilde{F}_j, f_{1,j-1} \in {}^R_{j-1} \tilde{F}_{j-1})$ is functionally independent of $f_{1,j-1}$. Thus,

$$\begin{aligned} A &= P(F_{1,j} \in {}^L_j \tilde{F}_{j-1}, F_{1,j} \in {}^R_j \tilde{F}_j, f_{1,j-1} \in {}^R_{j-1} \tilde{F}_{j-1}) \\ & \cdot \sum_{f_{1,j-1}} \frac{1}{q} P(f_{1,j-1} \in {}^L_{j-1} \tilde{F}_{j-2}, F_{1,j-2} \in {}^L_{j-2} \tilde{F}_{j-3} \dots) \\ &= P(F_{1,j} \in {}^L_j \tilde{F}_{j-1}, F_{1,j} \in {}^R_j \tilde{F}_j, f_{1,j-1} \in {}^R_{j-1} \tilde{F}_{j-1}) \\ & \cdot P(F_{1,j-1} \in {}^L_{j-1} \tilde{F}_{j-2}, F_{1,j-2} \in {}^L_{j-2} \tilde{F}_{j-3} \dots). \end{aligned}$$

Similarly it can be seen that

$$B = P(f_{1,j-1} \in {}^R_{j-1} \tilde{F}_{j-1}) \cdot P(F_{1,j-1} \in {}^L_{j-1} \tilde{F}_{j-2}, F_{1,j-2} \in {}^L_{j-2} \tilde{F}_{j-3} \dots)$$

and so

$$\begin{aligned} &= \frac{P(F_{1,j} \in {}^L_j \tilde{F}_{j-1}, F_{1,j} \in {}^R_j \tilde{F}_j, f_{1,j-1} \in {}^R_{j-1} \tilde{F}_{j-1})}{P(f_{1,j-1} \in {}^R_{j-1} \tilde{F}_{j-1})} \\ &= P(H_j^L, H_j^R | H_{j-1}^R). \end{aligned}$$

Clearly, $P(H_j^L, H_j^R | H_{j-1}^L, H_{j-1}^R)$ will also be equal to $P(H_j^L, H_j^R | H_{j-1}^R)$. Thus, the Lemma follows.

APPENDIX B

In this appendix, we calculate the stationary probability distribution and transition probabilities for the Markov chain shown in Fig. 5. We will show how to calculate the stationary probability for one particular state. The calculations for the other states are similar and so we just state the result.

$$\begin{aligned} & P\{H_j^L = 0, H_j^R = 0\} \\ &= P\{F_{1,j} \notin \tilde{F}_{j-1}, F_{1,j} \notin \tilde{F}_j\} \\ &= \sum_{f_{1,j}} P\{f_{1,j} \notin \tilde{F}_{j-1}, f_{1,j} \notin \tilde{F}_j | F_{1,j} = f_{1,j}\} P\{F_{1,j} = f_{1,j}\} \\ &= \frac{1}{q} \sum_{f_{1,j}} P\{f_{1,j} \notin \tilde{F}_{j-1} | F_{1,j} = f_{1,j}\} P\{f_{1,j} \notin \tilde{F}_j | F_{1,j} = f_{1,j}\} \\ &= \frac{1}{q} \sum_{f_{1,j}} \left(1 - \frac{1}{q}\right)^{K-1} \left(1 - \frac{1}{q}\right)^{K-1} \\ &= \left(1 - \frac{1}{q}\right)^{2(K-1)}. \end{aligned}$$

Similarly,

$$P\{H_j^L = 0, H_j^R = 1\} = \left(1 - \frac{1}{q}\right)^{K-1} \left[1 - \left(1 - \frac{1}{q}\right)^{K-1}\right],$$

$$P\{H_j^L = 1, H_j^R = 0\} = \left(1 - \frac{1}{q}\right)^{K-1} \left[1 - \left(1 - \frac{1}{q}\right)^{K-1}\right],$$

$$P\{H_j^L = 1, H_j^R = 1\} = \left[1 - \left(1 - \frac{1}{q}\right)^{(K-1)}\right]^2.$$

The transition probabilities of the Markov chain are easily determined once $q(i, k) = P\{H_j^L = i, H_{j-1}^R = k\}$ is determined. Let $\alpha = (1 - 1/q)^{K-1}$ and $\beta = (1 - 2/q)^{K-1}$. Then

$$\begin{aligned} q(0, 0) &= P\{H_j^L = 0, H_{j-1}^R = 0\} \\ &= \frac{1}{q^2} \sum_{f_{1,j}, f_{1,j-1}} P\{f_{1,j} \notin \tilde{F}_{j-1}, f_{1,j-1} \notin \tilde{F}_{j-1}\} \\ &= \frac{1}{q^2} [q\alpha + q(q-1)\beta] \\ &= \frac{1}{q}\alpha + \left(1 - \frac{1}{q}\right)\beta, \end{aligned}$$

$$\begin{aligned} q(1, 1) &= P\{H_j^L = 1, H_{j-1}^R = 1\} \\ &= \frac{1}{q^2} \sum_{f_{1,j}, f_{1,j-1}} P\{f_{1,j} \in \tilde{F}_{j-1}, f_{1,j-1} \in \tilde{F}_{j-1}\} \\ &= \frac{1}{q^2} [q(1-\alpha) + q(q-1)\{2(1-\alpha) - (1-\beta)\}] \\ &= \frac{1}{q}(1-\alpha) + \left(1 - \frac{1}{q}\right)[2(1-\alpha) - (1-\beta)]. \end{aligned}$$

Due to symmetry it is easy to see that $q(0, 1) = q(1, 0)$ and thus

$$\begin{aligned} q(0, 1) &= q(1, 0) = (1 - q(0, 0) - q(1, 1))/2 \\ &= \left(1 - \frac{1}{q}\right)(\alpha - \beta). \end{aligned}$$

We now turn to the calculation of the transition probabilities for the Markov chain.

$$\begin{aligned} P\{H_j^L = l, H_j^R = m | H_{j-1}^R = n\} \\ = \frac{P\{H_j^L = l, H_j^R = m, H_{j-1}^R = n\}}{P\{H_{j-1}^R = n\}}. \end{aligned}$$

For the case $l = 0, m = 1, n = 0$ the numerator in the above expression can be written as

$$\begin{aligned} P\{H_j^L = l, H_j^R = m, H_{j-1}^R = n\} \\ = \frac{1}{q^2} \sum_{f_{1,j}, f_{1,j-1}} P\{f_{1,j} \notin \tilde{F}_{j-1}, f_{1,j-1} \notin \tilde{F}_{j-1}\} P\{f_{1,j} \in \tilde{F}_j\}. \end{aligned}$$

Since the last term does not depend on $f_{1,j}$ this term can be taken out of the summation and we have

$$\begin{aligned} P\{H_j^L = 0, H_j^R = 1, H_{j-1}^R = 0\} \\ = P\{H_j^L = 0, H_{j-1}^R = 1\} P\{H_j^R = 0\}. \end{aligned}$$

It is easy to see that these operations also hold for any value l, m, n

and so we have in general that

$$\begin{aligned} P\{H_j^L = l, H_j^R = m, H_{j-1}^R = n\} \\ = P\{H_j^L = l, H_{j-1}^R = m\} P\{H_j^R = n\}. \end{aligned}$$

Thus,

$$\begin{aligned} p(l, m|n) &\triangleq P\{H_j^L = l, H_j^R = m | H_{j-1}^R = n\} \\ &= \frac{P\{H_j^L = l, H_{j-1}^R = n\} P\{H_j^R = m\}}{P\{H_{j-1}^R = n\}} \\ &= \frac{q(l, n)p(m)}{p(n)} \end{aligned}$$

where $p(k) = P\{H_j^R = k\}$. Letting $a = (0, 0)$, $b = (0, 1)$, $c = (1, 0)$, and $d = (1, 1)$ and $p_{i,l} = P\{H_j^L = i, H_{j-1}^R = l\}$, the transition probabilities, are given as

$$p_{a,a} = p_{a,c} = p(0, 0|0) = \frac{1}{q}\alpha + \left(1 - \frac{1}{q}\right)\beta,$$

$$p_{b,a} = p_{b,c} = p(0, 1|0) = \left[\frac{1}{q}\alpha + \left(1 - \frac{1}{q}\right)\beta\right] \left(\frac{1-\alpha}{\alpha}\right),$$

$$p_{c,a} = p_{c,c} = p(1, 0|0) = \left(1 - \frac{1}{q}\right)(\alpha - \beta),$$

$$p_{d,a} = p_{d,c} = p(1, 1|0) = \left(1 - \frac{1}{q}\right)(\alpha - \beta) \left(\frac{1-\alpha}{\alpha}\right),$$

$$p_{a,b} = p_{a,d} = p(0, 0|1) = \left(1 - \frac{1}{q}\right)(\alpha - \beta) \left(\frac{\alpha}{1-\alpha}\right),$$

$$p_{b,b} = p_{b,d} = p(0, 1|1) = \left(1 - \frac{1}{q}\right)(\alpha - \beta),$$

$$\begin{aligned} p_{c,b} = p_{c,d} = p(1, 0|1) &= \left[\frac{1}{q}(1-\alpha) \right. \\ &\quad \left. + \left(1 - \frac{1}{q}\right)(2(1-\alpha) - (1-\beta))\right] \left(\frac{\alpha}{1-\alpha}\right), \end{aligned}$$

$$\begin{aligned} p_{d,b} = p_{d,d} = p(1, 1|1) &= \frac{1}{q}(1-\alpha) \\ &\quad + \left(1 - \frac{1}{q}\right)[2(1-\alpha) - (1-\beta)]. \end{aligned}$$

APPENDIX C

$$I_Q(X^n; Y^n) = H(Y^n) - H(Y^n|X^n).$$

Let $W_i = 1$ if the i th symbol is erased and be 0 otherwise. Then

$$H(Y^n, W^n) = H(Y^n) + H(W^n|Y^n) = H(Y^n)$$

since $H(W^n|Y^n)$ is 0 as W^n is a deterministic function of Y^n . Hence, $H(Y^n) = H(Y^n, W^n)$. Now,

$$H(Y^n, W^n) = H(W^n) + H(Y^n|W^n)$$

and

$$H(Y^n|W^n) = \sum_{w_1, w_2, \dots, w_n} P(w_1, w_2, \dots, w_n) H(Y^n|w_1, w_2, \dots, w_n).$$

For each (w_1, w_2, \dots, w_n) such that l of the w 's are 1

$$\begin{aligned} H(Y^n | w_1, w_2, \dots, w_n) &= -M^{n-l} \left(\frac{1}{M}\right)^{n-l} \log_2 \left(\frac{1}{M}\right)^{n-l} \\ &= (n-l) \log_2 M. \end{aligned}$$

Therefore,

$$\begin{aligned} H(Y^n | W^n) &= \sum_{w_1, w_2, \dots, w_n} P(w_1, w_2, \dots, w_n) (n-l) \log_2 M \\ &= \sum_{l=0}^n P(E_1^n = l) (n-l) \log_2 M \end{aligned}$$

where E_1^n is the number of symbols out of symbols 1 through n which have been erased.

Similarly,

$$\begin{aligned} H(Y^n | X^n) &= H(Y^n | X^n) + H(W^n | X^n, Y^n) \\ &= H(Y^n, W^n | X^n) \\ &= H(W^n | X^n) + H(Y^n | W^n, X^n) \\ &= H(W^n | X^n) \\ &= H(W^n) \end{aligned}$$

since W^n is independent of X^n . Thus,

$$I_Q(X^n; Y^n) = \sum_{l=0}^n P(S_1^n = l) (n-l) \log_2 M.$$

Thus,

$$\begin{aligned} \lim_{n \rightarrow \infty} \max_{Q_n(X^n)} \frac{I_Q(X^n; Y^n)}{n} &= \lim_{n \rightarrow \infty} P(E_1^n = l) \frac{(n-l)}{n} \log_2 M \\ &= \log_2 M \left(1 - \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{l=0}^n l P(E_1^n = l) \right) \\ &= \log_2 M \left(1 - \lim_{n \rightarrow \infty} \frac{1}{n} E(E_1^n) \right) \\ &= (1 - \epsilon_C) \log_2 M. \quad [10]. \end{aligned}$$

APPENDIX D

$$\begin{aligned} H(Y^n | X^n) &= H(Y^n | X^n) + H(V^n | X^n, Y^n) \\ &= H(Y^n, V^n | X^n) \end{aligned}$$

(where $V_n = 1$ if an error occurred on the n th symbol and is 0 otherwise) since $H(V^n | X^n, Y^n) = 0$ as V^n is a deterministic function of (X^n, Y^n) . Hence,

$$\begin{aligned} H(Y^n | X^n) &= H(V^n | X^n) + H(Y^n | X^n, V^n) \\ &= H(V^n) + H(Y^n | X^n, V^n) \\ &= H(V^n) + \sum_{i=0}^n P(T_1^n = i) \log_2 (M-1)^i \\ &= H(V^n) + \sum_{i=0}^n i P(T_1^n = i) \log_2 (M-1) \end{aligned}$$

since V^n is independent of X^n .

Hence,

$$\begin{aligned} \lim_{n \rightarrow \infty} \max_{Q_n(X^n)} \frac{H(Y^n | X^n)}{n} &= H_\infty(V) + \lim_{n \rightarrow \infty} E \left(\frac{T_1^n}{n} \right) \log_2 (M-1) \\ &= H_\infty(V) + P(V=1) \log_2 (M-1) [10] \\ &= H_\infty(V) + e_0 \left(1 - \left(1 - \frac{1}{q} \right)^{2(K-1)} \right) \log_2 (M-1). \end{aligned}$$

APPENDIX E

In this appendix, we give a few sample calculations for the joint distributions of the random variable V_j , a function of the Markov chain $W_j = (H_j^L, H_j^R, R_j)$. That this is a Markov chain is an easy consequence of the fact that (H_j^L, H_j^R) is a Markov chain and is independent of $\{R_j\}$ which is an i.i.d. process.

First, let $U_j = (H_j^L, H_j^R)$ with $a = (0, 0)$, $b = (0, 1)$, $c = (1, 0)$, and $d = (1, 1)$. The upper bound to the entropy of V_j is determined from the joint distribution of V_j . We will do a sample calculation of the joint distribution for one particular argument for $n=2$ and $n=3$ and list the results for other arguments. The distributions of V_j will be calculated in terms of the distributions of the Markov chain U_j and the joint distribution of the process $\{R_j\}$. Since R_j is an i.i.d. process the joint distribution is easy to calculate. The joint distribution of U_j is easily calculated since it is a Markov chain.

The first order distribution of V_j is calculated as follows:

$$\begin{aligned} P(V_0 = 0) &= P(H_0 = 0 \text{ or } R_0 = 0) \\ &= P(H_0 = 0) + P(H_0 = 1)P(R_0 = 0) \\ &= P(U_0 = a) + P(U_0 \in B)P(R_0 = 0), \\ P(V_0 = 1) &= P(H_0 = 1, R_0 = 1) \\ &= P(H_0 = 1)P(R_0 = 1) \\ &= P(U_0 \in B)P(R_0 = 1). \end{aligned}$$

The second-order distribution is calculated as follows:

$$\begin{aligned} P(V_1 = 0, V_0 = 0) &= P(H_1 = 0 \text{ or } R_1 = 0, H_0 = 0 \text{ or } R_0 = 0) \\ &= P(H_1 = 0, H_0 = 0 \text{ or } R_0 = 0) \\ &\quad + P(H_1 = 1, R_1 = 0, H_0 = 0 \text{ or } R_0 = 0) \\ &= P(H_1 = 0, H_0 = 0) \\ &\quad + P(H_1 = 0, H_0 = 1, R_0 = 0) \\ &\quad + P(H_1 = 1, R_1 = 0, H_0 = 0) \\ &\quad + P(H_1 = 1, R_1 = 0, H_0 = 1, R_0 = 0) \\ &= P(H_1 = 0, H_0 = 0) \\ &\quad + P(H_1 = 0, H_0 = 1)P(R_0 = 0) \\ &\quad + P(H_1 = 1, H_0 = 0)P(R_1 = 0) \\ &\quad + P(H_1 = 1, H_0 = 1)P(R_1 = 0, R_0 = 0) \\ &= P(U_1 = a, U_0 = a) \\ &\quad + P(U_1 = a, U_0 \in B)P(R_0 = 0) \\ &\quad + P(U_1 \in B, U_0 = a)P(R_1 = 0) \\ &\quad + P(U_1 \in B, U_0 \in B)P(R_1 = 0, R_0 = 0). \end{aligned}$$

Later we determine the joint distribution of (U_1, U_0) that will allow us to complete this calculation. The remaining components of the distribution are calculated in a similar fashion and so we just state

the results.

$$\begin{aligned}
 P(V_1 = 0, V_0 = 1) &= P(H_1 = 0 \text{ or } R_1 = 0, H_0 = 1, R_0 = 1) \\
 &= P(U_1 = a, U_0 \in B)P(R_0 = 1) \\
 &\quad + P(U_1 \in B, U_0 \in B)P(R_1 = 0)P(R_0 = 1) \\
 P(V_1 = 1, V_0 = 0) &= P(H_1 = 1, R_1 = 1, H_0 = 0 \text{ or } R_0 = 0) \\
 &= P(U_1 \in B, U_0 = a)P(R_1 = 1) \\
 &\quad + P(U_1 \in B, U_0 \in B)P(R_1 = 1)P(R_0 = 0) \\
 P(V_1 = 1, V_0 = 1) &= 1 - P(V_1 = 1, V_0 = 0) \\
 &\quad - P(V_1 = 0, V_0 = 1) - P(V_1 = 0, V_0 = 0).
 \end{aligned}$$

For $n = 3$ the joint distribution is calculated using the same method as for $n = 2$. We obtain

$$\begin{aligned}
 P(V_2 = 0, V_1 = 0, V_0 = 0) &= P(H_2 = 0 \text{ or } R_2 = 0, \\
 &\quad H_1 = 0 \text{ or } R_1 = 0, H_0 = 0 \text{ or } R_0 = 0) \\
 &= P(U_2 = a, U_1 = a, U_0 = a) \\
 &\quad + P(U_2 = a, U_1 \in B, U_0 = a)P(R_1 = 0) \\
 &\quad + P(U_2 = a, U_1 = a, U_0 \in B)P(R_0 = 0) \\
 &\quad + P(U_2 = a, U_1 \in B, U_0 \in B)P(R_1 = 0, R_0 = 0) \\
 &\quad + P(U_2 \in B, U_1 = a, U_0 = a)P(R_2 = 0) \\
 &\quad + P(U_2 \in B, U_1 \in B, U_0 = a)P(R_2 = 0, R_1 = 0) \\
 &\quad + P(U_2 \in B, U_1 = a, U_0 \in B)P(R_2 = 0, R_0 = 0) \\
 &\quad + P(U_2 \in B, U_1 \in B, U_0 \in B)P(R_2 = 0, \\
 &\quad R_1 = 0, R_0 = 0),
 \end{aligned}$$

$$\begin{aligned}
 P(V_2 = 1, V_1 = 0, V_0 = 0) &= P(H_2 = 1, R_2 = 1, \\
 &\quad H_1 = 0 \text{ or } R_1 = 0, H_0 = 0 \text{ or } R_0 = 0) \\
 &= P(U_2 \in B, U_1 = a, U_0 = a)P(R_2 = 1) \\
 &\quad + P(U_2 \in B, U_1 \in B, U_0 = a)P(R_2 = 1, R_1 = 0) \\
 &\quad + P(U_2 \in B, U_1 = a, U_0 \in B)P(R_2 = 1, R_0 = 0) \\
 &\quad + P(U_2 \in B, U_1 \in B, U_0 \in B)P(R_2 = 1, \\
 &\quad R_1 = 0, R_0 = 0),
 \end{aligned}$$

$$\begin{aligned}
 P(V_2 = 0, V_1 = 1, V_0 = 0) &= P(H_2 = 0 \text{ or } R_2 = 0, \\
 &\quad H_1 = 1, R_1 = 1, H_0 = 0 \text{ or } R_0 = 0) \\
 &= P(U_2 = a, U_1 \in B, U_0 = a)P(R_1 = 1) \\
 &\quad + P(U_2 = a, U_1 \in B, U_0 \in B)P(R_1 = 1, R_0 = 0) \\
 &\quad + P(U_2 \in B, U_1 \in B, U_0 = a)P(R_2 = 0, R_1 = 1) \\
 &\quad + P(U_2 \in B, U_1 \in B, U_0 \in B)P(R_2 = 0, \\
 &\quad R_1 = 1, R_0 = 0),
 \end{aligned}$$

$$\begin{aligned}
 P(V_2 = 1, V_1 = 1, V_0 = 0) &= P(H_2 = 1, R_2 = 1, H_1 = 1, \\
 &\quad R_1 = 1, H_0 = 0 \text{ or } R_0 = 0) \\
 &= P(U_2 \in B, U_1 \in B, U_0 = a)P(R_2 = 1, R_1 = 1) \\
 &\quad + P(U_2 \in B, U_1 \in B, U_0 \in B)P(R_2 = 1, \\
 &\quad R_1 = 1, R_0 = 0),
 \end{aligned}$$

$$\begin{aligned}
 P(V_2 = 0, V_1 = 0, V_0 = 1) &= P(H_2 = 0 \text{ or } R_2 = 0, \\
 &\quad H_1 = 0 \text{ or } R_1 = 0, H_0 = 1, R_0 = 1) \\
 &= P(U_2 = a, U_1 = a, U_0 \in B)P(R_0 = 1) \\
 &\quad + P(U_2 = a, U_1 \in B, U_0 \in B)P(R_1 = 0, R_0 = 1) \\
 &\quad + P(U_2 \in B, U_1 = a, U_0 \in B)P(R_2 = 0, R_0 = 1) \\
 &\quad + P(U_2 \in B, U_1 \in B, U_0 \in B)P(R_2 = 0, \\
 &\quad R_1 = 0, R_0 = 1),
 \end{aligned}$$

$$\begin{aligned}
 P(V_2 = 1, V_1 = 0, V_0 = 1) &= P(H_2 = 1, R_2 = 1, \\
 &\quad H_1 = 0 \text{ or } R_1 = 0, H_0 = 1, R_0 = 1) \\
 &= P(U_2 \in B, U_1 = a, U_0 \in B)P(R_2 = 1, R_0 = 1) \\
 &\quad + P(U_2 \in B, U_1 \in B, U_0 \in B)P(R_2 = 1, \\
 &\quad R_1 = 0, R_0 = 1),
 \end{aligned}$$

$$\begin{aligned}
 P(V_2 = 0, V_1 = 1, V_0 = 1) &= P(H_2 = 0 \text{ or } R_2 = 0, H_1 = 1, \\
 &\quad R_1 = 1, H_0 = 1, R_0 = 1) \\
 &= P(U_2 = a, U_1 \in B, U_0 \in B)P(R_1 = 1, R_0 = 0) \\
 &\quad + P(U_2 \in B, U_1 \in B, U_0 \in B)P(R_2 = 0, \\
 &\quad R_1 = 1, R_0 = 1),
 \end{aligned}$$

$$\begin{aligned}
 P(V_2 = 1, V_1 = 1, V_0 = 1) &= P(H_2 = 1, R_2 = 1, H_1 = 1, \\
 &\quad R_1 = 1, H_0 = 1, R_0 = 1) \\
 &= P(U_2 \in B, U_1 \in B, U_0 \in B)P(R_2 = 1, \\
 &\quad R_1 = 1, R_0 = 0).
 \end{aligned}$$

Now since U_j is a Markov chain [10]

$$\begin{aligned}
 P(U_2 = a, U_1 = a, U_0 = a) &= P(U_2 = a|U_1 = a)P(U_1 = a|U_0 = a)P(U_0 = a)
 \end{aligned}$$

$$\begin{aligned}
 P(U_2 = a, U_1 = a, U_0 \in B) &= P(U_2 = a|U_1 = a)P(U_1 = a|U_0 \in B)P(U_0 \in B)
 \end{aligned}$$

$$\begin{aligned}
 P(U_2 = a, U_1 \in B, U_0 = a) &= \sum_{\gamma \in B} P(U_2 = a|U_1 = \gamma)P(U_1 = \gamma|U_0 = a)P(U_0 = a) \\
 &= \sum_{\gamma \in B} P(U_2 = a|U_1 = \gamma)P(U_1 = \gamma|U_0 \in B)P(U_0 \in B)
 \end{aligned}$$

$$\begin{aligned}
 P(U_2 \in B, U_1 = a, U_0 = a) &= P(U_2 \in B|U_1 = a)P(U_1 = a|U_0 = a)P(U_0 = a)
 \end{aligned}$$

$$\begin{aligned}
 P(U_2 \in B, U_1 = a, U_0 \in B) &= P(U_2 \in B|U_1 = a)P(U_1 = a|U_0 \in B)P(U_0 \in B)
 \end{aligned}$$

$$\begin{aligned}
 P(U_2 \in B, U_1 \in B, U_0 = a) &= \sum_{\gamma \in B} P(U_2 \in B|U_1 = \gamma)P(U_1 = \gamma|U_0 = a)P(U_0 = a)
 \end{aligned}$$

$$P(U_2 \in B, U_1 \in B, U_0 \in B) \\ = \sum_{\gamma \in B} P(U_2 \in B | U_1 = \gamma) P(U_1 = \gamma | U_0 \in B) P(U_0 \in B).$$

The transition probabilities above are calculated in terms of the transition probabilities of the Markov chain U_j which are determined in Appendix B.

$$P(U_j = a | U_{j-1} = a) = p_{a,a} \\ P(U_j = a | U_{j-1} \in B) = P(U_j = a, U_{j-1} \in B) / P(U_j \in B) \\ = \frac{[P(U_j = a, U_{j-1} = b) + P(U_j = a, U_{j-1} = c) + P(U_j = a, U_{j-1} = d)]}{P(U_{j-1} = b) + P(U_{j-1} = c) + P(U_{j-1} = d)} \\ = \frac{p_{a,b}p_b + p_{a,c}p_c + p_{a,d}p_d}{p_b + p_c + p_d} \\ P(U_j \in B | U_{j-1} = a) = P(U_j = b | U_{j-1} = a) + P(U_j = c | U_{j-1} = a) + P(U_j = d | U_{j-1} = a) \\ = p_{b,a} + p_{c,a} + p_{d,a}$$

for any integer j .

Now consider the lower bound to the entropy, namely,

$$H(V_n | V_{n-1}, \dots, V_1, W_0).$$

Since R_0 is independent of V_j for all j it is easy to see that this entropy is the same as

$$H(V_n | V_{n-1}, \dots, V_1, U_0).$$

To calculate this entropy we need to know the joint distribution of (V_n, \dots, V_1, U_0) . The bound we use will be with $n = 2$. The second-order distribution is given as follows:

$$P(V_2 = 0, V_1 = 0, U_0 = i) \\ = P(H_2 = 0 \text{ or } R_2 = 0, \\ H_1 = 0 \text{ or } R_1 = 0, U_0 = i) \\ = P(H_2 = 0, H_1 = 0, U_0 = i) \\ + P(H_2 = 0, H_1 = 1, R_1 = 0, U_0 = i) \\ + P(H_2 = 1, R_2 = 0, H_1 = 0, U_0 = i) \\ + P(H_2 = 1, R_2 = 0, H_1 = 1, \\ R_1 = 0, U_0 = i) \\ = P(H_2 = 0, H_1 = 0, U_0 = i) \\ + P(H_2 = 0, H_1 = 1, U_0 = i)P(R_1 = 0) \\ + P(H_2 = 1, H_1 = 0, U_0 = i)P(R_2 = 0) \\ + P(H_2 = 1, H_1 = 1, U_0 = i) \\ \cdot P(R_2 = 0, R_1 = 0) \\ = P(U_2 = a, U_1 = a, U_0 = i) \\ + P(U_2 = a, U_1 \in B, U_0 = i)P(R_1 = 0) \\ + P(U_2 \in B, U_1 = a, U_0 = i)P(R_2 = 0) \\ + P(U_2 \in B, U_1 \in B, U_0 = i)P(R_2 = 0, R_1 = 0),$$

$$P(V_2 = 1, V_1 = 0, U_0 = i) \\ = P(H_2 = 1, R_2 = 1, \\ H_1 = 0 \text{ or } R_1 = 0, U_0 = i) \\ = P(U_2 \in B, U_1 = a, U_0 = i)P(R_2 = 1) \\ + P(U_2 \in B, U_1 \in B, U_0 = i) \\ \cdot P(R_2 = 1, R_1 = 0),$$

$$P(V_2 = 0, V_1 = 1, U_0 = i) \\ = P(H_2 = 0 \text{ or } R_2 = 0, \\ H_1 = 1, R_1 = 1, U_0 = i) \\ = P(U_2 = a, U_1 \in B, U_0 = i)P(R_1 = 1) \\ + P(U_2 \in B, U_1 \in B, U_0 = i) \\ \cdot P(R_2 = 0, R_1 = 1),$$

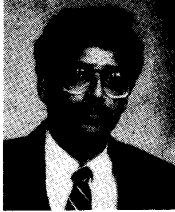
$$P(V_2 = 1, V_1 = 1, U_0 = i) \\ = P(H_2 = 1, R_2 = 1, \\ H_1 = 1, R_1 = 1, U_0 = i) \\ = P(U_2 \in B, U_1 \in B, U_0 = i) \\ \cdot P(R_2 = 1, R_1 = 1).$$

REFERENCES

- [1] S.-W. Kim and W. E. Stark, "Optimal rate Reed-Solomon coding for frequency-hopped spread-spectrum multiple-access channels," *IEEE Trans. Commun.*, vol. 37, pp. 138-144, Feb. 1989.
- [2] M. Hedge and W. E. Stark, "Multiple-access capability of frequency-hopped spread-spectrum communication," in *Proc. 1985 IEEE Military Commun. Conf.*, 1985, pp. 575-579.
- [3] M. B. Pursley, "Frequency-hop transmission for satellite packet switching and terrestrial packet radio networks," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 652-667, Sept. 1986.
- [4] U. Madhow, "Bounds and asymptotic results for the performance of asynchronous frequency-hop packet radio networks," Tech. Rep., U.S. Army Res. Office, Univ. of Illinois.
- [5] C. Frank and M. B. Pursley, "Comments on 'Packet error probabilities in frequency-hopped spread-spectrum packet radio networks—Memoryless frequency-hopping patterns considered,'" *IEEE Trans. Commun.*, to be published.
- [6] H. Sato, "Two-user communication channels," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 295-304, May 1977.
- [7] M. Georgiopoulos, "Packet error probabilities in frequency-hopped spread-spectrum packet radio networks—Memoryless frequency-hopping patterns considered," *IEEE Trans. Commun.*, vol. 36, p. 720-723, July 1988.
- [8] M. Hedge and W. E. Stark, "On the error probability of coded frequency-hopped spread-spectrum multiple-access systems," *IEEE Trans. Commun.*, to be published.
- [9] R. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.

- [10] E. Cinlar, *Introduction to Stochastic Processes*. Englewood Cliffs, NJ: Prentice-Hall, 1975.
- [11] D. Blackwell, "The entropy of functions of finite-state Markov chains," *First Prague Conf. Inform. Theory*, pp. 13-20, 1957.
- [12] J. J. Birch, "Approximations for the entropy for functions of Markov chains," *Ann. Mathematical Statist.*, vol. 33, pp. 930-938, 1962.

★



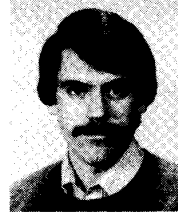
Manjunath V. Hegde (S'84-M'87) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology, Bombay, India, in 1979, the M.M.S. degree in finance from the University of Bombay, Bombay, India, in 1981, the M.S. degree in statistics from the University of Toledo, Toledo, OH, in 1983, and the Ph.D. degree in computer, information and control engineering from the University of Michigan, Ann Arbor, in 1987, where, in March 1987, he received the Outstanding Graduate Student Award for Computer

Information and Control Engineering.

From May 1981 to August 1982, he worked as a Financial Consultant for 20th Century Financial Services P. Ltd., Bombay where he was involved with Eurodollar syndications. Since August 1987 he has been an Assistant Professor of Electrical and Computer Engineering at Louisiana State University,

Baton Rouge. His research interests include communications and information theory, coding theory, game theory, and stochastic optimization.

★



Wayne E. Stark (S'77-M'82) was born on February 26, 1956. He received the B.S. (with highest honors), M.S., and Ph.D. degrees in electrical engineering from the University of Illinois, Urbana-Champaign, in 1978, 1979 and 1982 respectively.

Since 1982 he has been a faculty member at the University of Michigan where he is currently Associate Professor of Electrical Engineering and Computer Science. His research interests include information theory, coding theory, communication theory especially for spread-spectrum communication

systems.

Dr. Stark received the 1985 National Science Foundation's Presidential Young Investigator Award, was a member of the Board of Governors of the IEEE Information Theory Group and was an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS from 1984-1989.

He participated in the organization of the 1986 IEEE International Symposium on Information Theory held in Ann Arbor, Michigan. For the 1989 calendar year he is on sabbatical at IBM Zurich Research Laboratory, Rushlikon, Switzerland.