

Multistage Decoding of Frequency-Hopped FSK System

By UZI TIMOR

(Manuscript received July 17, 1980)

A recent paper described an improved decoding scheme for a frequency-hopped multilevel FSK system. We examined this multiple access communication system for possible application in satellite communication and mobile radio telephony. The new decoder, using the known algebraic structure of the users' addresses, reduces mutual interference and achieves a 50 to 60 percent increase in efficiency over conventional decoding. The present paper shows how additional decoding can further increase the efficiency, bringing it very close (within half a percent) to optimum. The scheme makes use of information derived while decoding the messages of other users and thus is especially attractive for the base station, where such information is readily available and does not require a significant increase in complexity. Compared to conventional decoding, the new scheme more than doubles the number of simultaneous users.

I. INTRODUCTION

In a recent paper¹ a new decoding scheme for a frequency-hopped multilevel FSK system was described. This system, where M users share a common frequency band, has been examined for applications in multiple access satellite communication² and mobile radio telephony.³ Each user conveys a K -bit message every T seconds by transmitting a sequence of L tones (chips) chosen from an alphabet of 2^K sinewaves of duration $\tau (=T/L)$. Each user is assigned an address (code) and the message is modulated onto the address. The receiver, knowing the address, decodes the received signal and extracts the message. However, transmissions by other users can combine to cause an erroneous message resulting in an ambiguous reception. Thus, even without channel impairments the number of simultaneous users the system can support at a given error probability is interference limited.

Whenever an ambiguous reception occurs, i.e., more than one mes-

sage value is decoded, the conventional decoder can't identify the correct message. The new decoder¹ makes use of the algebraic structure of the addresses to eliminate erroneous messages that come from interference. Each one of the L chips comprising a message is checked to determine whether it is part of an interference pattern, i.e., a possible sequence transmitted by some other user. An interference message will always be identified as such. The correct message will usually fail to have interference patterns for some chips and thus will be identified and correctly decoded.

This additional decoding (stage 2) results in a substantial improvement in performance over conventional decoding, allowing a 50 to 60 percent increase in the number of users that can simultaneously share the system at a given error probability. Yet it is not optimal and it can be further improved.

In performing stage 2 decoding interference patterns are sought but the (addresses of the) users who might have caused them do not have to be identified. This information is readily available and can be used to eliminate pseudo interference patterns. For example, an interference pattern might "belong" to a user who is not active at the moment. Even if it belongs to an active user it might not be his sequence but a combination of others.

This paper describes how additional decoding (stage 3) eliminates pseudo interference patterns and thus further improves the performance of the system. There is a clear distinction between decoding at the base station and at the mobile unit. The base station decodes the messages of all users and thus any information required for stage 3 decoding is already available. Therefore, additional decoding with improved performance can be accomplished without a significant increase in complexity. In the mobile unit, on the other hand, the additional decoding requires an increase in complexity as the messages of other users have to be decoded.

Upper bounds on the number of simultaneous users that the system can accommodate at a given error probability as well as simulation results are presented. A comparison with a hypothetical decoder, which fails only when the correct message coincides with an interference message (and therefore is undecodable), shows that the stage 3 decoder is very close (within half a percent) to the optimum decoder.

In the noiseless case where the system has a total bandwidth of 20 MHz and the data rate of each user is 32 kilobit/s, the number of users that can simultaneously share the system at a bit error probability of 10^{-3} is increased from 216 (in conventional decoding) through 345 (in stage 2 decoding) to 450 (in stage 3 decoding)—a total improvement of 108 percent. The resulting efficiency (total rate transmitted through the system per unit bandwidth) of stage 3 decoding is 72 percent.

Under noisy and multipath conditions, the number of simultaneous users is reduced but a comparable advantage of the new decoder over the conventional one is maintained.

II. SYSTEM DESCRIPTION

We briefly describe the system here. A detailed description is given in Refs. 2 and 3.

The elementary signals of the system are a set of 2^K sinewaves, which are orthogonal over the chip duration τ . Each user conveys a K -bit message every T seconds by transmitting a sequence of L tones of duration τ chosen from the signal set. The sequence is determined by the user's address and his K -bit message.

Let the address of the m th user be denoted by a vector \mathbf{a}_m ,

$$\mathbf{a}_m = (a_{m1}, a_{m2}, \dots, a_{mL}), \quad (1)$$

where each a_{mi} is a K -bit number corresponding to one of the 2^K frequencies of the system.

The transmitted sequence is

$$\mathbf{Y}_m = \mathbf{a}_m + X_m \cdot \mathbf{1}, \quad (2)$$

where X_m is the K -bit message, and

$$\mathbf{1} = \underbrace{(1, 1, \dots, 1)}_L.$$

Let us denote the 2^K frequencies of the system as elements of $GF(2^K)$, the finite field (Galois field) of 2^K elements $0, 1, \dots, 2^K - 1$. Accordingly, the message X_m , the components of \mathbf{a}_m and \mathbf{Y}_m can be expressed as elements of $GF(2^K)$, and the operations of addition (subtraction) and multiplication (division) are performed according to the rules of $GF(2^K)$. The transmitted sequence \mathbf{Y}_m can be described as a pattern in the $L \times 2^K$ time-frequency matrix A . Simultaneous transmissions by M users will result in up to $L \times M$ entries in A . The receiver performs every τ seconds a spectral analysis of the composite received signal and decides which of the 2^K frequency cells contain energy. Thus, after T seconds, assuming no channel impairments, a duplicate of A is generated at the receiver. To decode X_m , the receiver adds $-\mathbf{a}_m$ to each column of A to obtain user m 's decoded matrix A_m . The message appears as a complete row in A_m . Ambiguous decoding occurs when transmissions by other users combine to form other complete rows in A_m .

III. ADDRESS ASSIGNMENT

The interference between users can be minimized by a proper choice of addresses with minimum cross correlation. Schemes for assigning

2^K addresses that guarantee minimum mutual interference between 2^K or fewer users have been proposed⁴ using an algebraic approach.

Let us consider the following address structure: The address of user m is defined to be⁴

$$\mathbf{a}_m = (\gamma_m, \gamma_m\beta, \dots, \gamma_m\beta^{L-1}), \quad (3)$$

where γ_m is the element in $GF(2^K)$ assigned uniquely to user m and β is a primitive element in $GF(2^K)$, which is fixed for the system.

Note that the modulation (2) and address assignment (3) are not unique. Other schemes are possible (see for example Refs. 4 and 5) and the analysis and results that follow can be extended to such systems.

IV. STAGE 2 DECODING

Let M be the number of simultaneous users of the system. Each user i transmits a sequence \mathbf{Y}_i (2) where the address \mathbf{a}_i is assigned according to (3) and the message value is X_i .

In the decoded matrix A_m of user m , X_m appears as a complete row $X_m \cdot \mathbf{1}$. Suppose we have another complete row X' in A_m that is the result of interference. According to the address assignment, each chip in X' must come from a different user, so at least L users i_1, \dots, i_L have combined to cause this interference. We denote by i_n the user that contributes the interference in column n of X' . (If more than one user caused this interference, i_n can be any one of them.) To simplify notation, let us denote the address element (γ_{i_n}) and the message value (X_{i_n}) of user i_n by γ_{in} and X_{in} , respectively.

As mentioned in the previous section, the number (location) of each row in A_m is an element of $GF(2^K)$. We can subtract (the number of) row X' from all rows in A_m to obtain a new matrix $D_{X'}$, where row X' will now be at row zero.

Let $q_n(j)$ denote an entry in row q_n and column j in $D_{X'}$.

It was shown¹ that a necessary condition for row X' in A_m to be caused by interference is the existence of L nonzero numbers δ_n in $GF(2^K)$ such that all entries,

$$q_n(j) = \delta_n(\beta^{j-1} - \beta^{n-1}), \quad j, n = 1, \dots, L, \quad (4)$$

appear in $D_{X'}$. The entries $q_n(j)$ are the contribution of user i_n with address element $\gamma_{in} = \delta_n + \gamma_m$, where γ_m is the address element of user m . From (4) we can derive the following relation:

$$q_n(n+1) = q_n(j)f_{j-n}, \quad n = 1, \dots, L-1, \quad (5)$$

$$q_L(L-1) = q_L(j)f_{j-L}^*, \quad (6)$$

where

$$f_{j-n} = \frac{\Delta}{\beta^{j-n} - 1}, \quad j = 1, \dots, L, \quad j \neq n, \quad (7)$$

$$f_{j-L}^* = \frac{1}{\beta} f_{j-L}. \quad (8)$$

To check the condition (4) for $n = 1, \dots, L$ we multiply all entries (i.e., their row numbers) of column j in $D_{X'}$ ($j = 1, \dots, L, j \neq n, j \neq n + 1$) by f_{j-n} (or f_{j-L}^*) and look for a "complete" row (complete except the n th term). If we find such a row, then there exists a possible interferer contributing to column n of X' .

If the condition is satisfied for all $n = 1, \dots, L$, we assume that row X' in A_m is the result of interference. Using this decoding scheme, all interference rows will be identified as such. The correct row X_m will usually fail to satisfy the condition for some n and thus could be identified and decoded as the correct message.

It was shown¹ that a simple way to perform the column multiplications required during the test is to express each row number by an exponent of β . Since β is a primitive element of $GF(2^K)$ this is equivalent to a (fixed) row permutation of $D_{X'}$. This way the multiplications can be substituted by cycle shifting of columns, which is easy to implement. Thus, stage 2 decoding requires a small increase in complexity (of an order of L^2 cycle shifts) yet achieves a substantial improvement in performance. We show below how additional decoding can further improve the performance.

V. STAGE 3 DECODING

5.1 Discussion

Stage 2 decoding fails to identify the correct message X_m when for every n ($n = 1, \dots, L$) a possible interferer i_n exists such that all entries $q_n(j)$, $j = 1, \dots, L$, appear in D_{X_m} .

If such L interferers actually exist, that is, if X_m coincides with an interference row, there is no way to distinguish between X_m and any other interference row and no decoder can identify the correct message.

There are however many cases when only $L - j$ chips of X_m are (also) the result of interference and the remaining j chips, although not caused by interference, satisfy the interference condition. That is, entries from other users combine to form interference patterns at those chips. If those pseudo interferences can be identified, for at least one chip, X_m will be identified and correctly decoded. This will be done by making use of available information, derived but not used in stage 2 decoding.

Recall that a possible interference pattern at chip n of X_m was

identified as a "complete" row (complete except for the term in the n th column) in D_{X_m} . From (4) to (6) this row will be at row number q_n , where

$$q_n = \begin{cases} \delta_n(\beta^n - \beta^{n-1}), & n = 1, \dots, L-1, \\ \delta_L(\beta^{L-2} - \beta^{L-1}), & n = L. \end{cases} \quad (9)$$

Knowing q_n (which is found during the test), we can easily compute δ_n and the address $\gamma_{in} = \delta_n + \gamma_m$ of the possible interferer. The message value X^* associated with this interference can be computed as follows: The transmitted sequence of user i_n with message value X^* is (2),

$$Y_{in} = \gamma_{in}\beta^{j-1} + X^* \cdot 1. \quad (10)$$

The entry at column n of A_m will be at row number

$$\gamma_{in}\beta^{n-1} + X^* - \gamma_m\beta^{n-1} = \delta_n\beta^{n-1} + X^*. \quad (11)$$

But by definition i_n is the user who contributes the interference at column n of X_m . Thus,

$$\delta_n\beta^{n-1} + X^* = X_m$$

or

$$X^* = X_m - \delta_n\beta^{n-1}. \quad (12)$$

Substituting δ_n from (9), we can write

$$X^* = \begin{cases} X_m - \frac{q_n}{\beta - 1}, & n = 1, \dots, L-1, \\ X_m - \frac{q_L\beta}{1 - \beta}, & n = L. \end{cases} \quad (13)$$

5.2 Principle of decoding

Let us assume that the list of (the addresses of) the active users (those who are currently using the system) is known. This is certainly the case for the base station that communicates with all its active users, but the list could also be relayed to the mobile unit.

Thus, if an address γ_{in} of a possible interferer belongs to a user who is not active, the interference can be immediately identified as pseudo interference and eliminated.

If the address γ_{in} belongs to an active user, there are two possibilities:

(i) $X^* = X_{in}$. The transmitted message X_{in} and the computed message X^* associated with the interference pattern are the same. In this case the interference was actually caused by user i_n .

(ii) $X^* \neq X_{in}$. In this case the interference pattern was not caused by user i_n , but is the result of a combination of (at least) $L-1$ other users. Thus, this is a pseudo interference and should be eliminated.

Consider the decoded matrix A_{in} of user i_n . His transmitted sequence

will appear as a complete row at row number X_{in} . If $X^* \neq X_{in}$, then we will have another complete row (an interference row) in A_{in} at row number X^* . By decoding A_{in} (stage 2 or stage 3 when necessary) the correct message X_{in} will usually be identified. Thus, if $X^* \neq X_{in}$, it will be identified as pseudo interference of user m and discarded.

If there are several possible interferers at column n of X_m (more than one "complete" row is found in the test) all of them must be checked and discarded before we can conclude that interference is not at that column. If we find (at least) one of the L chips for which no actual interference exists, we can conclude that X_m is the correct message.

If we cannot assume knowledge of the list of active users, then the pseudo interference pattern attributed to nonactive users cannot be identified as such since there is no message X_{in} to be decoded.

VI. DECODING AT THE BASE STATION AND AT THE MOBILE UNIT

6.1 Base station

The base station has a list of all active users and decodes their messages. The decoding procedure can be described as follows.

Step 1 (for each user m)

(i) The decoded matrix A_m is generated and searched for complete rows. If there is only one such row, the message is decoded and listed in a list ($L1$) of users whose decoding is completed.

(ii) If there is more than one complete row, stage 2 decoding is performed. If the message is decoded it is transferred to $L1$.

(iii) If the message is not identified, the address and message values of possible interferers are computed [according to (9) and (13)]. Those are compared with the list of nonactive users and with $L1$ to eliminate a pseudo interference pattern.

At any stage, if the message is decoded it is transferred to $L1$. Similarly, if the message is found to be undecodable (i.e., all interference patterns are found to be true interferences) it is transferred to list $L2$ of undecodable users.

At the end of step 1 (for all users) we have N_1 users in list $L1$, N_2 users in $L2$ and $N_3 = M - (N_1 + N_2)$ users, each with a list of possible interferers and associated message values for some of its chips. If $N_3 > 0$, we proceed to step 2.

Step 2 (for users who have not been decoded)

For each of the N_3 users, we compare his list of possible interferers with $L1$ to eliminate pseudo interferers. As list $L1$ is increased, more possible interferers can be checked and more users decoded.

The procedure terminates when $N_3 = 0$ or when $L1$ remains unchanged after a complete cycle of checking all N_3 users.

6.2 Mobile unit (user m)

(i) The decoded matrix A_m is generated and searched for complete rows. If (up to) stage 2 decoding does not identify the message a list of possible interferers and their associated message values is computed.

(ii) Pseudo interferences from nonactive users (if list is available) are identified and discarded.

(iii) If the message is still undecoded, the decoded matrices of possible interferers have to be generated and decoded (stage 2) until enough pseudo interferences are identified to decode the message.

We define this as stage 3/2 decoding since the messages of possible interferers are decoded up to stage 2.

We could in principle perform stage 3 decoding of the possible interferers; however, the complexity increases exponentially as more and more users have to be decoded.

7. ERROR PROBABILITIES

7.1 Upper bounds

We have an ambiguity in decoding when the following two conditions are satisfied.

(i) There are two or more complete rows in A_m .

(ii) The correct row cannot be identified, i.e., all its chips have interference patterns (actual interference or unidentified pseudo interference).

When this happens, we choose one of the complete rows at random and decode it as the message.

Although not strictly independent, it can be shown using random coding arguments that the two conditions can be assumed to be independent with a negligible effect on the probability of error. Thus, $P_E^{(i)}$, the word-error probability when stage i decoding is performed, is given by

$$P_E^{(i)} = P_1 P_2^{(i)}, \quad (14)$$

where P_1 is the probability of condition 1 and $P_2^{(i)}$ is that of condition 2 when stage i decoding is performed.

If 2^K is the number of frequencies, L is the length of the sequence and M is the number of simultaneous users, P_1 can be upper-bounded² by

$$P_1 < (2^K - 1)p^L, \quad (15)$$

where

$$p = 1 - (1 - 2^{-K})^{M-1}. \quad (16)$$

Let $P_{2,j}^{(i)}$ be the probability of condition 2 (stage i decoding) when j

chips in X_m come from interference and the remaining $L-j$ chips have a pseudo interference pattern. We then have

$$P_2^{(i)} = \sum_{j=0}^L P_{2,j}^{(i)}. \quad (17)$$

(a) Stage 2 decoding

For stage 2 decoding we have shown¹ that $P_{2,j}^{(2)}$ can be upper-bounded by

$$P_{2,j}^{(2)} < p^L \binom{L}{j} S^j, \quad (18)$$

where

$$S = (2^K - 1)(1 - p)p^{L-2} \quad (19)$$

Thus,

$$P_2^{(2)} < p^L(1 + S)^L, \quad (20)$$

and as long as $p(1 + S) < 1$ the word-error probability can be upper-bounded by

$$P_E^{(2)} < (2^K - 1)(1 + S)^L p^{2L} \quad (21)$$

and the bit-error probability by

$$P_b^{(2)} < 2^{K-2}(1 + S)^L p^{2L} \quad (22)$$

(b) Stage 3 decoding

$P_{2,L}^{(3)}$ corresponds to the case where all interference patterns actually come from other users (i.e., X_m coincides with an interference row in A_m). Thus,

$$P_{2,L}^{(3)} = P_{2,L}^{(2)} < p^L \quad (23)$$

Consider the case where $L-1$ chips in X_m actually come from interference and the remaining chip has a pseudo interference pattern. This pseudo interference will correspond to an active user with probability.

$$\bar{p} = \frac{M-1}{2^K-1} \quad (24)$$

The probability that the correct message of this user (and therefore the pseudo interference) will not be identified as such when stage 3 decoding is performed for that user is $P_2^{(3)}$. Thus we can upper-bound

$$P_{2,L-1}^{(3)} < P_{2,L-1}^{(2)} \bar{p} P_2^{(3)}. \quad (25)$$

Similarly,

$$P_{2,L-j}^{(3)} < P_{2,L-j}^{(2)} (\bar{p} P_2^{(3)})^j. \quad (26)$$

From (17), (18), and (26) we get

$$P_2^{(3)} < p^L (1 + S \bar{p} P_2^{(3)})^L. \quad (27)$$

Let P_2^* be the solution of (27) when an equality is substituted for the inequality. Then

$$P_2^{(3)} < P_2^* = p^L (1 + S \bar{p} P_2^*)^L. \quad (28)$$

(c) Stage 3/2 decoding

In a similar way we can upper-bound $P_2^{(3/2)}$, the probability of error of condition 2 when the messages of possible interferers are decoded up to stage 2. This is relevant only to the mobile unit (see section 6.2).

Case 1: List of active users available

Substituting $P_2^{(2)}$ for $P_2^{(3)}$ in (25) yields

$$P_2^{(3/2)} < p^L (1 + S \bar{p} P_2^{(2)})^L, \quad (29)$$

where $P_2^{(2)}$ is given by (20).

Case 2: List of active users unknown

In this case we will always have an error when a possible interferer is not an active user (which occurs with probability $1 - \bar{p}$) since there is no correct message to be decoded. Thus

$$P_2^{(3/2)} < p^L [1 + S(\bar{p} P_2^{(2)} + 1 - \bar{p})]^L. \quad (30)$$

(d) Coincidence of X_m with an interference

Whenever we have two or more interference rows in A_m and the correct row coincides with one of them, it cannot be identified and decoded. An optimal decoder can do no better than a decoder which fails only when such a coincidence occurs. Thus, it is of interest to compare the various schemes with such a (hypothetical, not necessarily achievable) decoder.

The probability of condition 2 for such a decoder is given by (23)

$$P_2^{(\text{coin})} < p^L. \quad (31)$$

We can summarize the performance of the various schemes as follows: The word-error and the bit-error probabilities are upper-bounded by

$$P_E^{(i)} < (2^K - 1) g_i^L p^{2L}, \quad (32)$$

$$P_b^{(i)} < 2^{K-2} g_i p^{2L}, \quad (33)$$

where

$$g_i = \begin{cases} 1 + S, & \text{stage 2 decoding,} \\ 1 + S\bar{p}P_2^*, & \text{stage 3 decoding,} \\ 1 + S\bar{p}P_2^{(2)}, & \text{stage 3/2 decoding} \\ & \text{(list of users known),} \\ 1 + S(\bar{p}P_2^{(2)} + 1 - \bar{p}), & \text{stage 3/2 decoding} \\ & \text{(list of users unknown),} \\ 1, & \text{coincidence fail decoder,} \end{cases} \quad (34)$$

and S , $P_2^{(2)}$, \bar{p} , and P_2^* are given by (19), (20), (22), and (28), respectively.

The upper bounds of the various schemes as a function of the number of simultaneous users (M) are depicted in Fig. 1 for the case $K = 9$ (512 frequencies) and $L = 11$ (which is optimal when the total bandwidth is 20 MHz and each user's rate is 32 kilobit/s).

As can be seen, at small error probabilities the performance of stage 3 decoding is very close to the probability of coincidence, that is, almost all messages which do not coincide with an interference are correctly decoded. As the number of users is increased, a strong threshold effect occurs (at $M = 475$ in the above example) and the performance deteriorates rapidly. This is due to the fact that as M increases, the interference is so high that a large number of users cannot be decoded (stage 2) and thus the information (decoded message values of possible interferers) required for stage 3 decoding is not available.

As M is decreased, all the above bounds converge to the coincidence bound.

7.2 Simulations

The various decoding schemes were simulated on a Digital Equipment Corporation PDP 11 computer. Figure 1 shows simulation results for stage 2, stage 3, and stage 3/2 (when the list of active users is known) decoding as well as for the probability of coincidence.

It can be seen that for bit-error probabilities up to 10^{-3} , the simulated results are within 5 percent of the upper bounds on the number of simultaneous users.

The threshold effect of stage 3 decoding is clearly seen. As M increases there are some K -bit blocks where the majority of users (60 percent and more) are undecodable. The percentage of undecodable blocks increases from 6 percent at $M = 478$ to over 75 percent at $M = 490$.

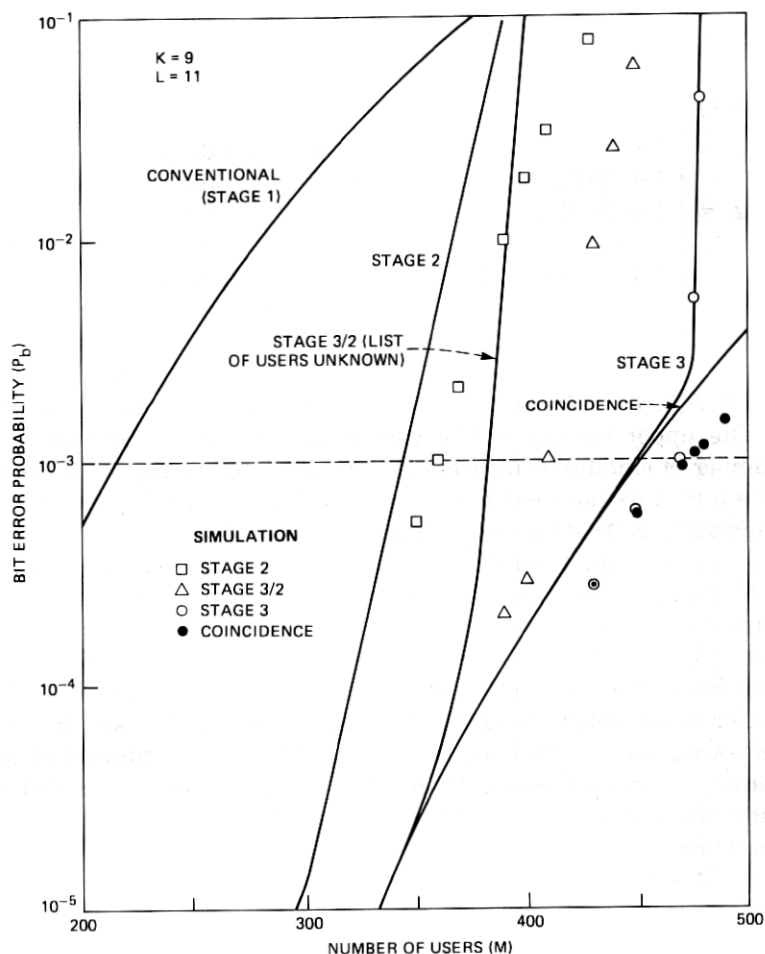


Fig. 1—Upper bounds and simulations of the bit-error probabilities as a function of the number of users M for stage 2, stage 3/2 (list of active user known), and stage 3 decoding and for coincidence of the message with interference. The system parameters are $W = 20$ MHz, $R = 32$ kbit/s, $K = 9$, and $L = 11$.

VIII. CONCLUSIONS

The performance of the frequency-hopped multilevel FSK system can be substantially improved by making use of the known structure of the addresses to perform additional decoding. In stage 2 decoding additional checks are performed on the user's own decoded matrix but no reference to the decoded matrices of other users is needed. The stage 3 decoder achieves a performance that is very close to optimum by referring to results obtained in decoding the sequences of other users.

In the base station, where all users are decoded anyway, stage 3 decoding can be realized without a significant increase in complexity. This is not the case at the mobile unit; therefore, an intermediate stage of decoding (stage 3/2) was proposed, requiring a moderate increase in complexity.

When the total bandwidth is 20 MHz and the transmission rate of each user is 32 kilobit/s, the number of simultaneous users that the system can accommodate at bit-error probability of 10^{-3} is increased from 216 (conventional decoding) through 345 (stage 2) to 383 (stage 3/2) and 450 (stage 3). The corresponding efficiencies of the system (total rate transmitted through the system per unit bandwidth) are 35 percent (conventional), 55 percent (stage 2), 61 percent (stage 3/2), and 72 percent (stage 3). As can be seen, stage 3 decoding more than doubles the efficiency. Simulation results show that an efficiency up to 75 percent can be obtained with stage 3 decoding.

REFERENCES

1. U. Timor, "Improved Decoding Scheme for Frequency Hopped FSK System," B.S.T.J., 59, No. 10 (December 1980), pp. 1839-55.
2. A. J. Viterbi, "A Processing Satellite Transponder for Multiple Access by Low-Rate Mobile Users," Digital Satellite Communications Conference, Montreal, October 23-25, 1978.
3. D. J. Goodman, P. S. Henry, and V. K. Prabhu, "Frequency Hopped Multilevel FSK for Mobile Radio," B.S.T.J., 59, No. 7 (September 1980), pp. 1257-75.
4. G. Einarsson, "Address Assignment for a Time-Frequency-Coded Spread-Spectrum System," B.S.T.J., 59, No. 7 (September 1980), pp. 1241-55.
5. B. G. Haskell, "Computer Simulation Results on Frequency Hopped MFSK Mobile Radio—Noiseless Case," IEEE Trans. Commun., COM-29, No 2 (February 1981), pp. 125-32.

