10-1969

A Note on the Free Distance of a Convolutional Code

Alexander Miczo
Syracuse University

Luther D. Rudolph
Syracuse University

69-2

A NOTE ON THE FREE DISTANCE OF A CONVOLUTIONAL CODE

ALEXANDER MICZO

LUTHER D. RUDOLPH

OCTOBER, 1969

SUSE UNIVERSITY · SUOS CULTORES SCIENTIA CORONAT · FOUNDED A·D·1870

SYSTEMS AND INFORMATION SCIENCE

SYRACUSE UNIVERSITY

A NOTE ON THE FREE DISTANCE OF A CONVOLUTIONAL CODE

Alexander Miczo

Luther D. Rudolph

Systems and Information Science

Syracuse University

Syracuse, N. Y. 132~~04~~10

October, 1969

Abstract

A counterexample to a conjecture on the number of constraint lengths required to achieve the free distance of a rate 1/n systematic convolutional code is presented.

Footnotes

This work was supported by the National Science Foundation under Grant GK-4737.

[1] D.J. Costello, "A Construction Technique for Random - Error - Correcting Convolutional Codes," *IEEE Trans. Information Theory*, *IT-15*, pp. 631-636, September 1969.

A rate 1/n systematic convolutional code is the row space of a generator matrix of the form shown in Figure 1, where

$$\underline{g} = \left(1, g_0^{(2)}, \ldots, g_0^{(n)}, 0, g_1^{(2)}, \ldots, g_1^{(n)}, \ldots, 0, g_m^{(2)}, \ldots, g_m^{(n)}\right).$$

A code word t is thus defined by

$$\underline{t} = \underline{i}G$$

where $\underline{i} = (i_0, i_1, \ldots)$ is the input sequence. Let $\underline{i}_j = (i_0, i_1, \ldots, i_j)$. G_j denotes the matrix consisting of the first (j+1)n columns of G. Costello[1] defines the order j column distance, d_j, to be

$$d_j = \min_{i_0 \neq 0} W_H(\underline{i}_j G_j)$$

where $W_H(x)$ is the Hamming weight of x. He then defines the free distance to be

$$d_{free} = \lim_{j \to \infty} d_j .$$

Since d_j is a monitonically increasing function of j and d_{free} is upper bounded by $W_H(\underline{g})$, we have

$$d_j \leq d_{free} \leq W_H(\underline{g}) \qquad j = 0, 1, \ldots \quad .$$

For a systematic code, there exists an L such that $d_j = d_{free}$ for all $j \geq L$. Costello showed that $L \leq (n-1)(m+1)m$. If an algorithm for computing the free distance of a given code were dependent on this bound, it would probably be impractical for all but small codes. Costello conjectured that the bound could be improved to L = 2m.

This, however, is not the case. In fact there exists no fixed integer s such that $L = sm$ for all m, as we shall now show.

For simplicity, we will consider only rate 1/2 binary codes. It will be apparent that our result extends to rate 1/n codes. The generator matrix of a rate 1/2 systematic code can be written in the form shown in Figure 2. The weight of a code word $\underline{t}$ is then given by

$$W_H(\underline{t}) = W_H(\underline{i})+W_H(\underline{i}G^{(2)}).$$

Consider now a code of odd memory order m in which the subgenerator $\underline{g}^{(2)} = (g_0^{(2)},g_1^{(2)},\ldots,g_m^{(2)})$ is constrained as follows: $g_i^{(2)} = g_{i+\frac{m+1}{2}}^{(2)}$ for $i = 0,1,\ldots,\frac{m-1}{2}$. In this case, the matrix $G^{(2)}$ is of the form shown in Figure 3. The column distance of the code generated is bounded by

$$d_{\frac{km+k-2}{2}} \leq W_H(\underline{g}')+k \qquad k = 1,2,\ldots .$$

This can be seen by considering the code word constructed from the rows of G that correspond to the shaded blocks of $G^{(2)}$. Let k* denote the smallest integer for which

$$W_H(\underline{g}')+k^* = d_{free} .$$

Then

$$L \geq \frac{k^*m+k^*-2}{2} \geq \frac{k^*}{2}m \qquad \text{for } k^*>1.$$

Now suppose it is possible to find a class of codes for which $W_H(\underline{g}')$ is an increasing function of m and for which $d_{free} = 2W_H(\underline{g}')+1$.

Then

$$k^* = d_{free} - W_H(\underline{g}') = W_H(\underline{g}')+1$$

and

$$L \geq \frac{W_H(\underline{g}')+1}{2} m \quad ,$$

which shows that there exists no fixed integer s such that L = sm for all m. We now present such a class.

The generator polynomial for the k^{th} code in the class is defined by

$$\underline{g}_k'(x) = \underline{g}_{k-1}'(x)+x^{6\phi_{k-1}^2}$$

$$\phi_k = \deg(\underline{g}_k'(x))+1$$

$$\underline{g}_k^{(2)}(x) = \underline{g}_k'(x)(1+x^{2\phi_k})$$

where $\underline{g}_1'(x) = 1$. (Note that this construction inserts 0's between the two copies of $\underline{g}'$. This is not inconsistent with above; see Figure 4.)

<u>Theorem</u>

$$d_{free_k} = 2W_H(\underline{g}_k')+1 \qquad \text{for } k = 1,2,\ldots \quad .$$

<u>Proof</u>

For k = 1, $\underline{g}_k'(x) = 1$, $\phi_1 = 1$ and $\underline{g}_1^{(2)}(x) = 1+x^2$. The reader may easily verify that the free distance of the rate 1/2 binary systematic code with $g^{(2)} = 101$ is

$$d_{free_1} = 2W_H(\underline{g}_1')+1 = 3 .$$

Now assume that $d_{free_k} = 2W_H(\underline{g}_k')+1$. We must show that

$d_{free_{k+1}} = 2W_H(\underline{g}'_{k+1})+1$. Since $W_H(\underline{g}'_{k+1}) = W_H(\underline{g}'_k)+1$ by construction, this amounts to showing that $d_{free_{k+1}} = d_{free_k}+2$. Suppose $\underline{t}_{k+1}$ is a minimum weight code word in the (k+1)st code. The corresponding code word in the k^{th} code is $\underline{t}_k = \underline{i}G_k$. We claim that $W_H(\underline{t}_{k+1}) \geqq W_H(\underline{t}_k)+2$. This is most easily seen by reference to Figure 4. If $\underline{t}_{k+1}$ is to have minimum weight in the code, then it cannot be the sum of two disjoint code words. This requires that at least one out of every ϕ_k rows of G_k be included in the sum, $\underline{i}G_k$. There are two cases to consider.

(1) Suppose that $\underline{t}_{k+1}$ is formed from some combination of the first $5\phi_k^2$ rows of G_{k+1}. In this case, the 1 added in going from $\underline{g}'_k$ to $\underline{g}'_{k+1}$ cannot be cancelled because of the spacing allowed. Hence $\underline{t}_{k+1} = \underline{i}G_{k+1}$ will have at least two more 1's than $\underline{t}_k = \underline{i}G_k$.

(2) Suppose on the other hand that $\underline{t}_{k+1}$ is formed from some combination of rows that includes a row beyond the first $5\phi_k^2$ rows of G_{k+1}. In the case, the assumption that $\underline{t}_{k+1}$ has minimum weight requires that at least $5\phi_k^2/\phi_k = 5\phi_k$ rows be included. But then

$$W_H(\underline{t}_{k+1}) \geqq W_H(\underline{i}) \geqq 5\phi_k \geqq 5W_H(\underline{g}'_k) \geqq 2W_H(\underline{g}'_k)+3.$$

Therefore $d_{free_{k+1}} = d_{free_{k+1}}+2$ in either case and the proof is complete.

We have shown here that L increases more rapidly than m, and it seems unlikely that L increases as rapidly as m^2. This would appear to leave m log m as the next most likely candidate.

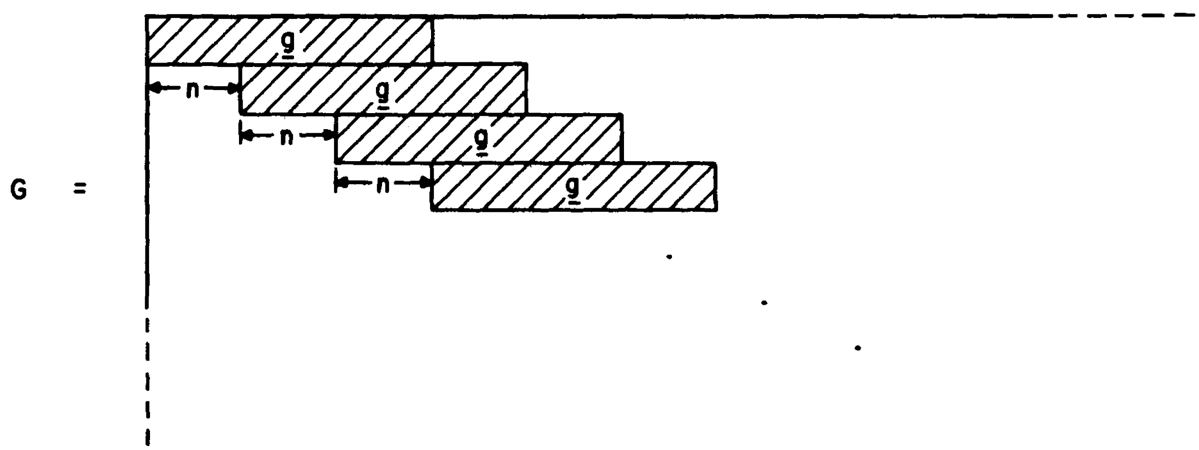

Figure 1

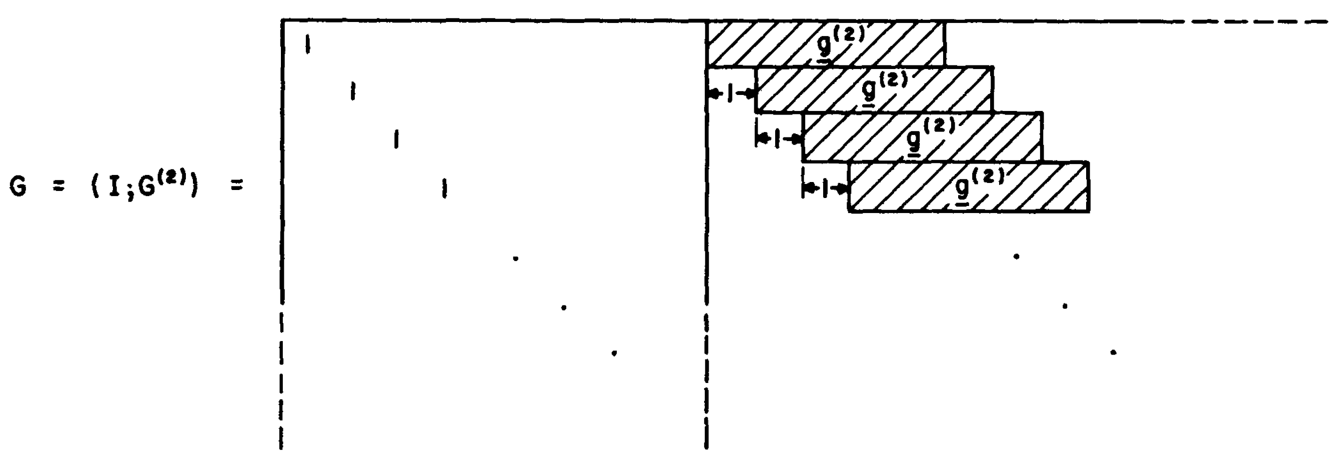

Figure 2

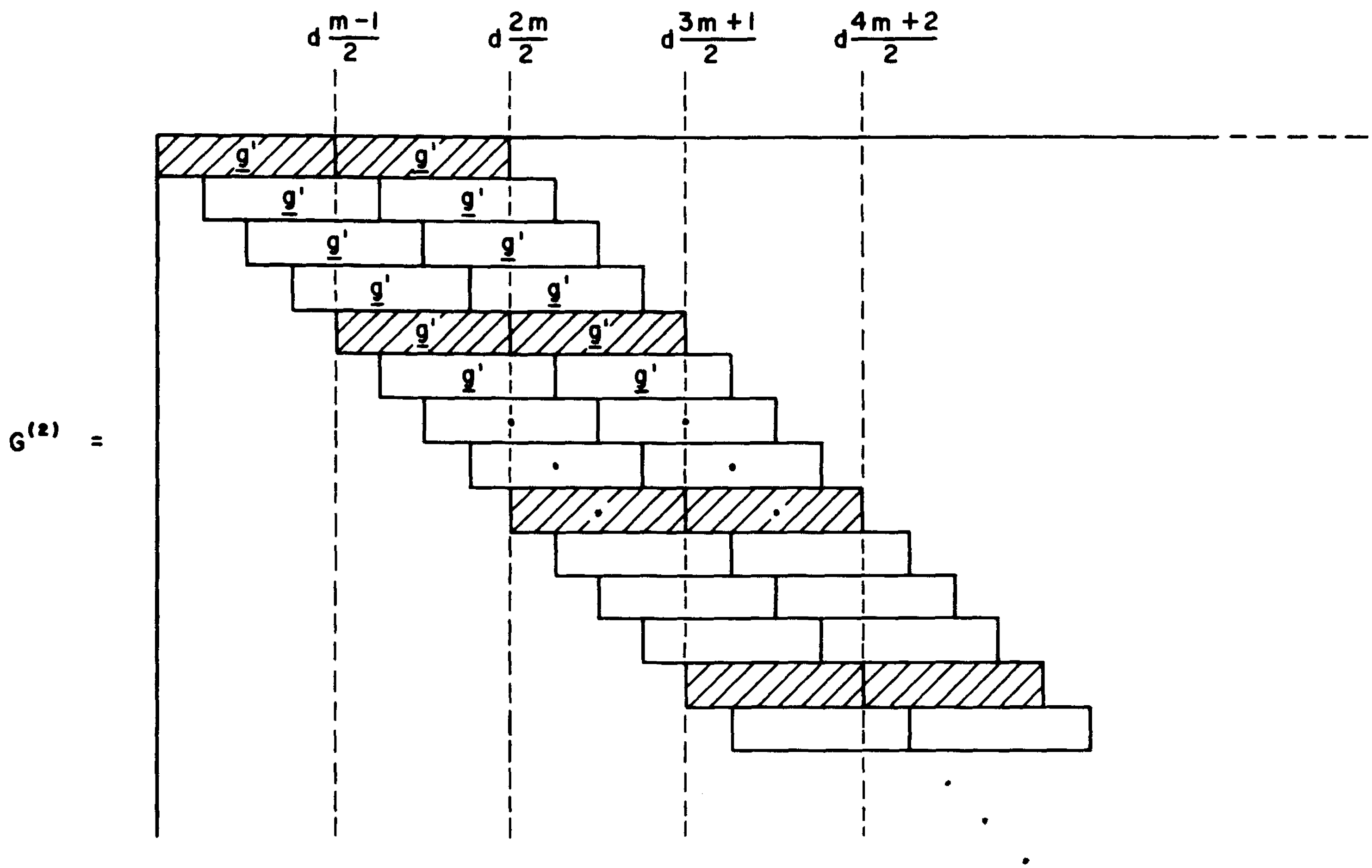

Figure 3

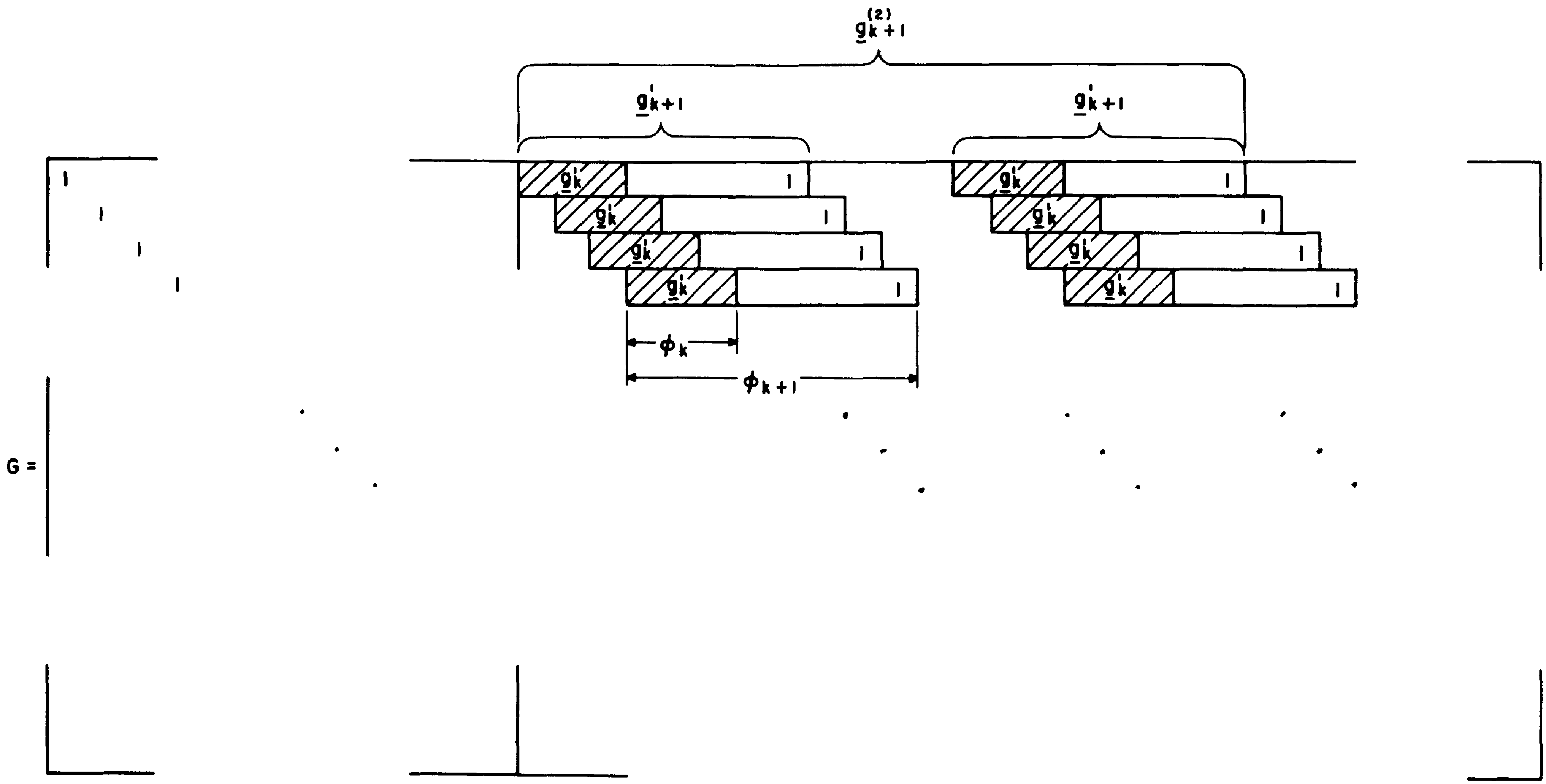

Figure 4