ESSA TR ERL 174-ITS 111

A UNITED STATES DEPARTMENT OF COMMERCE PUBLICATION

ESSA Technical Report ERL 174-ITS 111

U.S. DEPARTMENT OF COMMERCE
Environmental Science Services Administration
Research Laboratories

Exhaustive Search for the Best Cyclic (20, 8) Code

L. R. ESPELAND

M. NESENBERGS

PENNSYLVANIA STATE UNIVERSITY
OCT 1 5 1970
DOCUMENTS COLLECTION

BOULDER, COLO.
APRIL 1970

ESSA RESEARCH LABORATORIES

The mission of the Research Laboratories is to study the oceans, inland waters, the lower and upper atmosphere, the space environment, and the earth, in search of the understanding needed to provide more useful services in improving man's prospects for survival as influenced by the physical environment. Laboratories contributing to these studies are:

Earth Sciences Laboratories: Geomagnetism, seismology, geodesy, and related earth sciences; earthquake processes, internal structure and accurate figure of the Earth, and distribution of the Earth's mass.

Atlantic Oceanographic and Meteorological Laboratories: Oceanography, with emphasis on the geology and geophysics of ocean basins, oceanic processes, sea-air interactions, hurricane research, and weather modification (Miami, Florida).

Pacific Oceanographic Laboratories: Oceanography; geology and geophysics of the Pacific Basin and margins; oceanic processes and dynamics; tsunami generation, propagation, modification, detection, and monitoring (Seattle, Washington).

Atmospheric Physics and Chemistry Laboratory: Cloud physics and precipitation; chemical composition and nucleating substances in the lower atmosphere; and laboratory and field experiments toward developing feasible methods of weather modification.

Air Resources Laboratories: Diffusion, transport, and dissipation of atmospheric contaminants; development of methods for prediction and control of atmospheric pollution (Silver Spring, Maryland).

Geophysical Fluid Dynamics Laboratory: Dynamics and physics of geophysical fluid systems; development of a theoretical basis, through mathematical modeling and computer simulation, for the behavior and properties of the atmosphere and the oceans (Princeton, New Jersey).

National Severe Storms Laboratory: Tornadoes, squall lines, thunderstorms, and other severe local convective phenomena toward achieving improved methods of forecasting, detecting, and providing advance warnings (Norman, Oklahoma).

Space Disturbances Laboratory: Nature, behavior, and mechanisms of space disturbances; development and use of techniques for continuous monitoring and early detection and reporting of important disturbances.

Aeronomy Laboratory: Theoretical, laboratory, rocket, and satellite studies of the physical and chemical processes controlling the ionosphere and exosphere of the earth and other planets.

Wave Propagation Laboratory: Development of new methods for remote sensing of the geophysical environment; special emphasis on propagation of sound waves, and electromagnetic waves at millimeter, infrared, and optical frequencies.

Institute for Telecommunication Sciences: Central federal agency for research and services in propagation of radio waves, radio properties of the earth and its atmosphere, nature of radio noise and interference, information transmission and antennas, and methods for the more effective use of the radio spectrum for telecommunications.

Research Flight Facility: Outfits and operates aircraft specially instrumented for research; and meets needs of ESSA and other groups for environmental measurements for aircraft (Miami, Florida).

ENVIRONMENTAL SCIENCE SERVICES ADMINISTRATION

BOULDER, COLORADO 80302

U. S. DEPARTMENT OF COMMERCE
Maurice H. Stans, Secretary

ENVIRONMENTAL SCIENCE SERVICES ADMINISTRATION
Robert M. White, Administrator

RESEARCH LABORATORIES
Wilmot N. Hess, Director

ESSA TECHNICAL REPORT ERL 174-ITS 111

Exhaustive Search for the Best Cyclic (20, 8) Code

L. R. ESPELAND

M. NESENBERGS

INSTITUTE FOR TELECOMMUNICATION SCIENCES
BOULDER, COLORADO
April 1970

For sale by the Superintendent of Documents, U. S. Government Printing Office, Washington, D. C. 20402
Price 35 cents

U. S. Depository Copy

Digitized by the Internet Archive
in 2012 with funding from
LYRASIS Members and Sloan Foundation

http://archive.org/details/exhaustivesearch00espe

TABLE OF CONTENTS

	Page
LIST OF FIGURES	iv
LIST OF TABLES	iv
ABSTRACT	1
1. INTRODUCTION	1
2. CODE WORD DISTANCE DISTRIBUTION	2
3. WORD ERROR PROBABILITY	8
4. COMPARISON OF (15, 5) AND (20, 8) CODES	11
4.1 Case of Identical Baud (Keying) Speed	11
4.2 Case of Same Transmission Rate	15
5. CONCLUSIONS	17
6. REFERENCES	18
APPENDIX A. Detailed Results - Computation and Tables	19
APPENDIX B. Upper Bounds on Word Error Probability	23

LIST OF FIGURES

Figure		Page
1.	A shift-register generator showing the feedback connections for the No. 1 (20, 8) code.	3
2.	Distribution of distances for the (15, 5) code and selected (20, 8) codes.	10
3.	Word error probability characteristics for selected (20, 8) codes.	12
4.	Word error probability comparison of the (15, 5) code (P_e) and the No. 1 (20, 8) code ($\underline{P_e}$) at identical baud speeds.	13
5.	Word error probability comparison of the (15, 5) code (P_e) with the No. 1 (20, 8) code ($\underline{P_e}$) at the same transmission rate.	16

LIST OF TABLES

Table		
1.	Word error probability and code distance structure	5
2.	Minimum distance values and selected cases for comparison	14

EXHAUSTIVE SEARCH FOR THE BEST CYCLIC (20, 8) CODE

L. R. Espeland and M. Nesenbergs

An exhaustive computer search for the best, simply implemented, cyclic (20, 8) codes was carried out, and the procedures and results are reported here. Some forty almost equally good (20, 8) codes are identified, but, alas, none of them appear to be better than the familiar (15, 5) Bose-Chaudhuri-Hocquenghem code.

1. INTRODUCTION

In the fall of 1969 development was initiated for an efficient medium speed digital transmission scheme using error correcting coding for low power VHF Ionospheric Scatter communications in polar regions. Presently, the design and implementation of the one-way error correcting system is nearing completion. The heart of the scheme is an interleaved nearly orthogonal (15, 5) BCH (for Bose-Chaudhuri-Hocquenghem) code of minimum distance 7 (Peterson, 1961) with a generating polynomial

$$g(x) = x^5 + x^3 + x + 1 \quad .$$

The decoder is a classical minimum distance (or codebook, or, under certain normal assumptions, a maximum likelihood, or optimum) decoder, that outputs the nearest valid codeword.

A number of issues regarding the optimality of the (15, 5) choice were raised because some convolutional, or other non-block code, might be better. This is a valid point still being investigated. First, the one-third rate of the code appears a little low. On the other hand, a rate of one-half is likely to be too high to combat the typically bursty and unpredictable errors on a VHF scatter channel. Second, the number of information symbols, $k = 5$, is not ideally suited for the manipulation of standard codewords of either 7 or 8 bits. Third, the hardware--size,

speed, and cost--should be as practical as possible. An alphabet size of $2^8 = 256$ and a block size of $n = 20$ look reasonable.

To satisfy items one through three, we have sought and found "the best" (20, 8) block code generated by a simple cyclic generator of eight registers.

This report relates how a computer search was carried out and which of the (20, 8) codes are the best. To manipulate and compare different codes, a number of tools were used. The most important ones were complete codeword distance distributions for all $2^7 = 128$ codes and word error probability bounds for these codes. Finally, the performance of the best cyclic (20, 8) code is compared to that of the (15, 5) BCH code.

2. CODEWORD DISTANCE DISTRIBUTION

In this section we explain the distance (or weight) distribution data computed in our search for an attractive (20, 8) code. The computed material pertains to a small and quite specific family of (20, 8) codes. We consider only those linear cyclic codes that are easily encoded (e.g., with the feedback device shown in fig. 1).

It is seen from figure 1 that such a (20, 8) code is fully determined by the feedback connections $(A_7, A_6, \ldots, A_1)$ from the encoder registers; $A_j = 0$ denotes no connection, and $A_j = 1$ denotes a connection from the j-th register to the exclusive - OR gate. There are a total of $2^7 = 128$ distinct feedback combinations, including all seven 0's and all seven 1's. Distinct feedback patterns do not however necessarily imply codes with different distance distributions. For each given code with a generator $\{A_j\}$, there is a conjugate generator $\{A_{8-j}\}$, $j = 1, 2, \ldots, 7$. The conjugate encoder has the reverse order of feedback leads. Moreover, some conjugate generators are the same as the original generators.

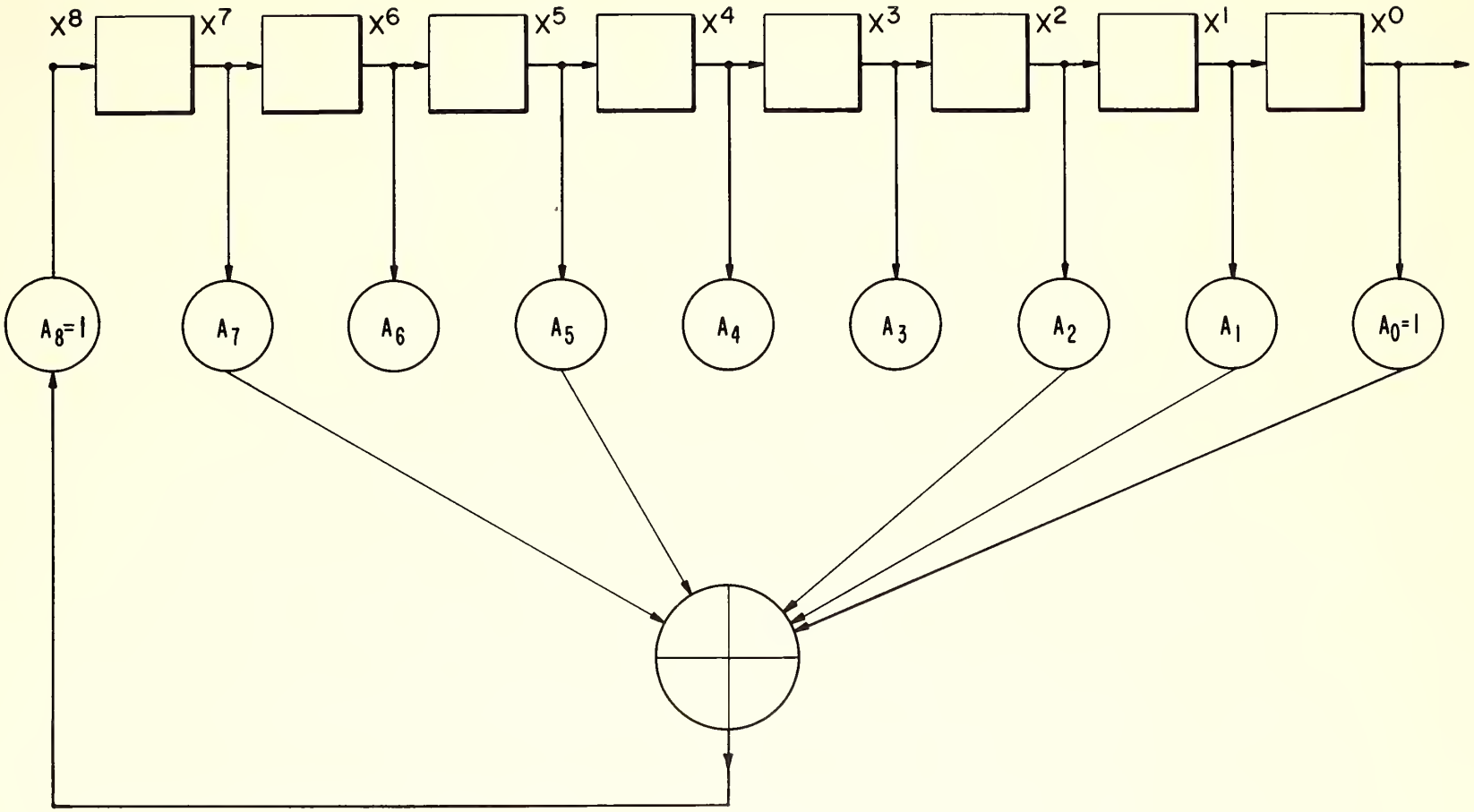

Figure 1. A shift-register generator showing the feedback connections for the No. 1 (20,8) code.

Clearly, this happens when $A_j = A_{8-j}$ for all j, i.e., when

$$A_7 = A_1 \ ,$$

$$A_6 = A_2 \ ,$$

$$A_5 = A_3 \ ,$$

while (A_4, A_3, A_2, A_1) are arbitrary; thus, there are $2^4 = 16$ invariant conjugates, including all 0's and all 1's. The remaining $\{A_j\}$ encoders must have distinct conjugates. There are exactly $\frac{1}{2}(128 - 16) = 56$ such "encoder and conjugate encoder" pairs. Observe that any code can be viewed as running forward or backward in time. Whatever the code is, a reversal must leave the weight distribution invariant. Yet the code generator, as for our (20, 8) code, must then become the above conjugate. We conclude that there can be no more than 16 + 56 = 72 codes with distinct distance distributions. Among them is the code generated by repetition of the eight information bits. This is the trivial "no connection" $A_7 = A_6 = \ldots = A_1 = 0$ case, which we prefer to ignore from now on. There remain 71 codes that are of interest. The distance distributions of all these 71 cases have been computed, and are tabulated (together with other entities) in table 1. See appendix A for background material and details of the computed data.

Consider a particular (20, 8) code among the eligible 71. The code consists of $2^8 = 256$ distinct codewords w_m, m = 0, 1, ..., 255. Let d_{mn} denote the Hamming distance between two codewords w_m and w_n. We seek the distribution of $\{d_{mn}\}$ (m, n = 0, 1, ..., 255) for the code at hand, and for the other seventy (20, 8) codes.

As is well known (Peterson, 1961), the distance distribution of a linear code is the same as the one for the subset pertaining to a particular reference word, vis., $\{d_{m_o n}\}$ for any m_o. In particular, one

Table 1. Word Error Probability and Code Distance Structure

	CODE↓PE→	3.16-001	1.00-001	3.16-002	1.00-002	1.00-003	1.00-004
	647	3.76+001	4.94-001	7.33-003	1.55-004	1.23-007	1.20-010
1	713 MD OF 6 NCW	6 28 39 36	36 36 39	28 6 (1)**			
	711	3.76+001	4.94-001	7.43-003	1.62-004	1.33-007	1.30-010
2	447 MD OF 5 NCW	1 6 19 39	52 42 32	24 19 16 5			
	677	3.75+001	4.86-001	7.42-003	1.68-004	1.43-007	1.40-010
3	773 MD OF 6 NCW	7 32 27 32	58 32 27	32 7 (1)			
	611	3.75+001	4.89-001	7.52-003	1.69-004	1.43-007	1.40-010
4	443 MD OF 5 NCW	4 5 20 35	40 46 40	35 20 5 4 (1)			
	703H*	3.76+001	4.91-001	7.57-003	1.70-004	1.43-007	1.40-010
5	607 MD OF 6 NCW	7 25 34 44	42 38 36	12 7 9 1			
	747H*	3.76+001	4.92-001	7.60-003	1.70-004	1.43-007	1.40-010
6	717 MD OF 6 NCW	7 24 35 46	40 38 36	10 9 10			
	737	3.76+001	4.98-001	7.71-003	1.72-004	1.43-007	1.40-010
7	767 MD OF 6 NCW	7 28 35 36	42 36 35	28 7 (1)			
	543E*	3.76+001	4.99-001	7.72-003	1.72-004	1.43-007	1.40-010
8	615 MD OF 6 NCW	7 20 39 54	36 30 32	18 13 6			
	557	3.77+001	5.05-001	7.81-003	1.73-004	1.43-007	1.40-010
9	755 MD OF 6 NCW	7 19 41 52	38 34 22	20 19 3			
	641	3.76+001	5.11-001	8.04-003	1.76-004	1.44-007	1.40-010
10	413 MD OF 5 NCW	2 6 18 47	44 20 44	47 18 6 2 (1)			
	545E*	3.76+001	4.96-001	7.77-003	1.78-004	1.53-007	1.50-010
11	515 MD OF 5 NCW	1 7 22 33	44 52 38	20 19 13 4 2			
	477B	3.76+001	4.90-001	7.66-003	1.77-004	1.53-007	1.50-010
12	771 MD OF 5 NCW	1 7 24 30	42 54 40	24 13 11 8 1			
	573C	3.76+001	5.06-001	8.07-003	1.83-004	1.53-007	1.50-010
13	675 MD OF 5 NCW	5 5 11 45	62 22 18	50 29 5 3			
	661B	3.76+001	4.92-001	7.86-003	1.86-004	1.62-007	1.60-010
14	433 MD OF 6 NCW	8 25 28 46	54 32 26	18 10 7 1			
	511	3.75+001	4.94-001	7.94-003	1.87-004	1.63-007	1.60-010
15	445 MD OF 5 NCW	6 5 14 35	44 46 44	35 14 5 6 (1)			
	475	3.76+001	5.03-001	8.13-003	1.89-004	1.63-007	1.60-010
16	571 MD OF 5 NCW	2 7 22 35	40 42 40	35 22 7 2 (1)			
	435E*	3.82+001	5.48-001	8.99-003	2.05-004	1.74-007	1.70-010
17	561 MD OF 5 NCW	1 8 13 49	42 40 42	22 21 8 9			
	625	3.76+001	4.99-001	8.35-003	2.04-004	1.82-007	1.80-010
18	523 MD OF 5 NCW	6 6 13 32	44 52 50	28 6 6 9 3			
	473	3.76+001	5.05-001	8.45-003	2.06-004	1.82-007	1.80-010
19	671 MD OF 6 NCW	9 28 27 36	54 36 27	28 9 (1)			
	705	3.77+001	5.08-001	8.51-003	2.06-004	1.83-007	1.80-010
20	507 MD OF 6 NCW	9 24 30 44	50 36 24	20 13 4 1			
	563	3.76+001	5.18-001	8.79-003	2.10-004	1.83-007	1.80-010
21	635 MD OF 5 NCW	2 8 18 39	44 32 44	39 18 8 2 (1)			
	623	3.72+001	5.21-001	8.81-003	2.10-004	1.83-007	1.80-010
22	623 MD OF 6 NCW	9 20 38 44	38 44 28	20 9			
	741	3.76+001	5.07-001	8.67-003	2.15-004	1.92-007	1.90-010
23	417 MD OF 5 NCW	3 8 19 30	39 52 50	28 13 4 3 5 1			
	631	3.76+001	5.08-001	8.67-003	2.15-004	1.92-007	1.90-010
24	463 MD OF 5 NCW	1 9 19 30	50 50 38	24 13 13 7 1			

Table 1 Con't.

```
     CODE↓PE→   3.16-001   1.00-001   3.16-002   1.00-002   1.00-003   1.00-004

     551E*      3.76+001   5.12-001   8.80-003   2.16-004   1.93-007   1.90-010
25   455 MD OF 5 NCW   1   9  29  28  32  48  40  34  23   7   3   1

     467        3.76+001   5.19-001   8.95-003   2.18-004   1.93-007   1.90-010
26   731 MD OF 5 NCW   1   9  21  35  42  38  42  35  21   9   1  (1)

     547        3.75+001   5.01-001   8.69-003   2.21-004   2.02-007   2.00-010
27   715 MD OF 5 NCW   6   7  14  27  44  58  44  27  14   7   6  (1)

     527        3.76+001   5.21-001   9.16-003   2.27-004   2.03-007   2.00-010
28   725 MD OF 5 NCW   2   9  18  35  44  38  44  35  18   9   2  (1)

     533        3.77+001   5.32-001   9.40-003   2.30-004   2.03-007   2.00-010
29   665 MD OF 6 NCW  10  20  39  44  28  44  39  20  10  (1)

     517        3.76+001   5.23-001   9.33-003   2.35-004   2.12-007   2.10-010
30   745 MD OF 5 NCW   1  10  21  31  42  44  42  31  21  10   1  (1)

     643D       3.76+001   5.07-001   9.10-003   2.38-004   2.22-007   2.20-010
31   613 MD OF 5 NCW   2  10  18  22  52  60  36  24  10  10  10   1

     701        3.76+001   5.18-001   9.68-003   2.58-004   2.42-007   2.40-010
32   407 MD OF 5 NCW   4  10  16  23  44  60  44  23  16  10   4  (1)

     457        3.77+001   5.39-001   1.02-002   2.64-004   2.42-007   2.40-010
33   751 MD OF 6 NCW  12  20  31  44  40  44  31  20  12  (1)

     531        3.77+001   5.34-001   1.03-002   2.79-004   2.62-007   2.60-010
34   465 MD OF 5 NCW   2  12  18  24  50  50  34  30  20  10   4   1

     437        3.77+001   5.43-001   1.05-002   2.81-004   2.62-007   2.60-010
35   761 MD OF 6 NCW  13  20  27  44  46  44  27  20  13  (1)

     541        3.77+001   5.43-001   1.05-002   2.81-004   2.62-007   2.60-010
36   415 MD OF 6 NCW  13  20  27  44  46  44  27  20  13  (1)

     633        3.76+001   5.36-001   1.05-002   2.88-004   2.72-007   2.70-010
37   663 MD OF 5 NCW   5  11   9  27  50  50  50  27   9  11   5  (1)

     567B       3.77+001   5.51-001   1.12-002   3.09-004   2.92-007   2.90-010
38   735 MD OF 5 NCW   5  12  23  23  28  46  48  40  23   6   1

     727D       3.80+001   5.98-001   1.22-002   3.27-004   3.03-007   3.00-010
39   727 MD OF 6 NCW  15  36  29  32  34  32  34  16  15  12

     453F*      3.83+001   6.14-001   1.28-002   3.46-004   3.23-007   3.20-010
40   651 MD OF 6 NCW  16  20  37  28  36  44  34  36   4

     667        3.77+001   5.64-001   1.23-002   3.53-004   3.41-007   3.40-010
41   733 MD OF 5 NCW   6  14  20  17  32  52  44  38  26   6

     575        3.72+001   5.50-001   1.23-002   3.66-004   3.60-007   3.60-010
42   575 MD OF 5 NCW   6  15   8  13  50  55  56  42   2   1   0   0   6   1

     645        3.77+001   5.60-001   1.24-002   3.66-004   3.60-007   3.60-010
43   513 MD OF 5 NCW   6  15   8  13  60  66  24  18  30  15

     471A       3.81+001   6.20-001   1.36-002   3.81-004   3.62-007   3.60-010
44   471 MD OF 6 NCW  18  30  25  44  36  24  30  20  18  10

     605        3.75+001   5.11-001   1.21-002   7.22-004   6.09-006   6.01-008
45   503 MD OF 4 NCW   1   6   2  14  38  44  44  44  38  14   2   6   1  (1)

     637D       3.77+001   5.28-001   1.30-002   7.59-004   6.13-006   6.01-008
46   763 MD OF 4 NCW   1   4   5  12  35  52  46  44  31   8   5   8   4

     461        3.75+001   5.19-001   1.30-002   7.65-004   6.14-006   6.01-008
47   431 MD OF 4 NCW   1   5   5  17  26  42  62  42  26  17   5   5   1  (1)

     627        3.76+001   5.43-001   1.37-002   7.79-004   6.15-006   6.02-008
48   723 MD OF 4 NCW   1   2   7  18  34  44  42  44  34  18   7   2   1  (1)
```

Table 1 Con't.

	CODE↓PE→	3.16-001	1.00-001	3.16-002	1.00-002	1.00-003	1.00-004
	657	3.77+001	5.52-001	1.41-002	7.91-004	6.16-006	6.02-008
49	753 MD OF 4 NCW 1	5 6 21	35 34 36	42 43 25	6 1		
	617	3.76+001	5.48-001	1.41-002	7.97-004	6.17-006	6.02-008
50	743 MD OF 4 NCW 1	4 7 12	34 48 42	48 34 12	7 4	1 (1)	
	537F*	3.77+001	5.70-001	1.60-002	8.76-004	6.26-006	6.03-008
51	765 MD OF 4 NCW 1	7 10 11	21 48 54	40 33 17	8 5		
	653	3.76+001	5.48-001	1.82-002	1.34-003	1.21-005	1.20-007
52	653 MD OF 4 NCW 2	8 3 8	25 48 66	48 25 8	3 8	2 (1)	
	535	3.76+001	5.55-001	1.82-002	1.34-003	1.21-005	1.20-007
53	565 MD OF 4 NCW 2	3 5 19	25 42 62	42 25 19	5 3	2 (1)	
	577	3.76+001	5.57-001	1.84-002	1.35-003	1.21-005	1.20-007
54	775 MD OF 4 NCW 2	4 5 16	25 44 62	44 25 16	5 4	2 (1)	
	673	3.84+001	7.71-001	2.81-002	1.68-003	1.25-005	1.20-007
55	673 MD OF 4 NCW 2	16 16 12	25 28 36	44 28 20	20 8		
	621	3.77+001	5.85-001	2.28-002	1.88-003	1.81-005	1.80-007
56	423 MD OF 4 NCW 3	2 3 18	32 44 50	44 32 18	3 2	3 (1)	
	721	3.84+001	7.28-001	2.77-002	2.03-003	1.82-005	1.80-007
57	427 MD OF 4 NCW 3	6 8 26	44 32 28	32 19 26	20 6	5	
	707	3.87+001	8.74-001	3.96-002	2.87-003	2.45-005	2.40-007
58	707 MD OF 3 NCW 4	2 4 22	28 13 28	52 28 13	28 22	4 2 4 (1)	
	757	3.76+001	6.13-001	3.21-002	3.02-003	3.00-005	3.00-007
59	757 MD OF 4 NCW 5	4 0 20	10 40 96	40 10 20	0 4	5 (1)	
	553	3.78+001	6.57-001	3.31-002	3.03-003	3.00-005	3.00-007
60	655 MD OF 4 NCW 5	0 2 16	34 48 44	48 34 16	2 0	5 (1)	
	451	3.78+001	6.64-001	3.39-002	3.06-003	3.00-005	3.00-007
61	451 MD OF 4 NCW 5	0 4 16	26 48 56	48 26 16	4 0	5 (1)	
	601	3.78+001	6.98-001	3.60-002	3.14-003	3.01-005	3.00-007
62	403 MD OF 3 NCW 2	4 6 5	14 23 30	48 56 44	20 3		
	555	3.81+001	7.53-001	3.87-002	3.25-003	3.02-005	3.00-007
63	555 MD OF 4 NCW 5	4 12 12	10 48 72	48 10 12	12 4	5 (1)	
	501	3.79+001	7.71-001	4.41-002	3.84-003	3.62-005	3.60-007
64	405 MD OF 4 NCW 6	12 8 4	9 36 60	60 40 16	4		
	441	3.80+001	8.07-001	4.87-002	4.38-003	4.22-005	4.20-007
65	411 MD OF 4 NCW 7	6 8 8	19 44 36	56 53 14	4		
	521	3.84+001	8.70-001	5.03-002	4.42-003	4.22-005	4.20-007
66	425 MD OF 3 NCW 2	6 12 7	8 21 42	58 42 21	8 7	12 6 2 (1)	
	505	3.87+001	9.54-001	5.71-002	5.04-003	4.82-005	4.80-007
67	505 MD OF 3 NCW 4	6 8 10	16 25 36	44 36 25	16 10	8 6 4 (1)	
	421	3.89+001	1.04+000	6.23-002	5.24-003	4.84-005	4.80-007
68	421 MD OF 3 NCW 8	4 0 24	24 6 32	48 24 20	32 24	8 1	
	525	4.92+001	1.65+000	1.22-001	1.19-002	1.20-004	1.20-006
69	525 MD OF 4 NCW 20	0 0 0	110 0 0	0 100 0	0 0	25	
	777	4.01+001	1.52+000	1.28-001	1.26-002	1.26-004	1.26-006
70	777 MD OF 4 NCW 21	14 1 0	35 70 21	0 7 42	35 0	0 2 7	
	603	3.81+001	9.31-001	9.28-002	2.21-002	2.02-003	2.00-004
71	603 MD OF 2 NCW 1	6 0 6	15 2 27	50 40 50	27 2 6	15 6 0 1 0 1	

*indicates primitive binary polynomial

**indicates one codeword at distance 20

is justified to pick $m_o = 0$, with w_o the all zero codeword. We let $d_n = d_{on}$ and compute the 255 values d_n for all $n = 1, 2, \ldots, 255$ non-zero codewords.

For each code, we finally define the "distance distribution" as a set of twenty numbers $M(i)(i=1, \ldots, 20)$, where $M(i)$ is the number of codewords with $d_n = i$. While we do refer to appendix B for more details, it is clear that $\sum_i M(i) = 255$.

For each code, define a minimum distance, MD or d_o, as the smallest $i > 0$ for which $M(i) > 0$ holds. Clearly, the minimum distance and the distance distribution must play a role in a search for more effective codes (see second lines, table 1). How this comes to pass is the subject of the next section.

3. WORD ERROR PROBABILITY

The word error probability, P_e, is a standard performance criterion of a given code under specified conditions (Peterson, 1961; Gallager, 1968). As is always the case, a number of simplifying assumptions are needed to render the present P_e computing task tractable.

We assume that:

(a) The digital communications medium is a memoryless binary symmetric channel (BSC) with bit error (or transition) probability p_e.

(b) The binary message source is completely random, i.e., any source statistic is memoryless, symmetric, and mutually independent.

(c) The decoder performs a minimum distance decoding. A decoding error occurs, whenever the received word is at least as far from the transmitted codeword as from any other codeword.

Under these assumptions and subject to complete knowledge of codeword distance distribution M(i), an exact computation of word error probability P_e still represents a cumbersome task. In figure 2 we plot M(i), i = 1, 2, ... for (15, 5) BCH and selected (20, 8) codes. In appendix B we present and prove two upper bounds on P_e: "the union bound" $\overline{P}_e$ and the "minimum distance bound" $\overline{Q}_e$. Three features of the bounds are quite apparent:

(a) For p_e near one-half (i.e., $10^{-1} < p_e \leq \frac{1}{2}$) the minimum distance bound, $\overline{Q}_e$, is the best of the two. At least $\overline{Q}_e \leq 1$.

(b) The present union bound $\overline{P}_e$ is a sharpened version of previously used union bounds.

(c) For p_e values of greatest practical interest (i.e., $0 \leq p_e << 10^{-1}$) one always has $\overline{Q}_e > \overline{P}_e \cong P_e$.

The union bound $\overline{P}_e$ therefore is pertinent to our code evaluation. Since it is a sharp bound, we use it in place of actual word error probability P_e to assess performance of different codes (see similar arguments by Peterson (1961) and Wozencraft and Jacobs (1967)).

We have computed P_e's (viz., $\overline{P}_e$ and $\overline{Q}_e$) for all 71 structurally distinct cyclic (20, 8) codes, as well as for the (15, 5) code that is being implemented for the VHF Scatter Channel. The bit error probability values $p_e = 10^{-\frac{1}{2}}, 10^{-1}, 10^{-\frac{3}{2}}, 10^{-2}, 10^{-3}$, and 10^{-4} were used in the computation (see app. A and B for details). The bulk results are presented in table 1 with pertinent minimum distance and distance distribution information.

As an example of code performance comparison, consider the column $p_e = 10^{-2}$ in table 1. Code 1 has $p_e = 1.55(10^{-4})$, code 2 has $P_e = 1.62(10^{-4})$, and finally code 71 has $P_e = 2.21(10^{-2})$. One observes that the codes have been numbered in an order of monotonically

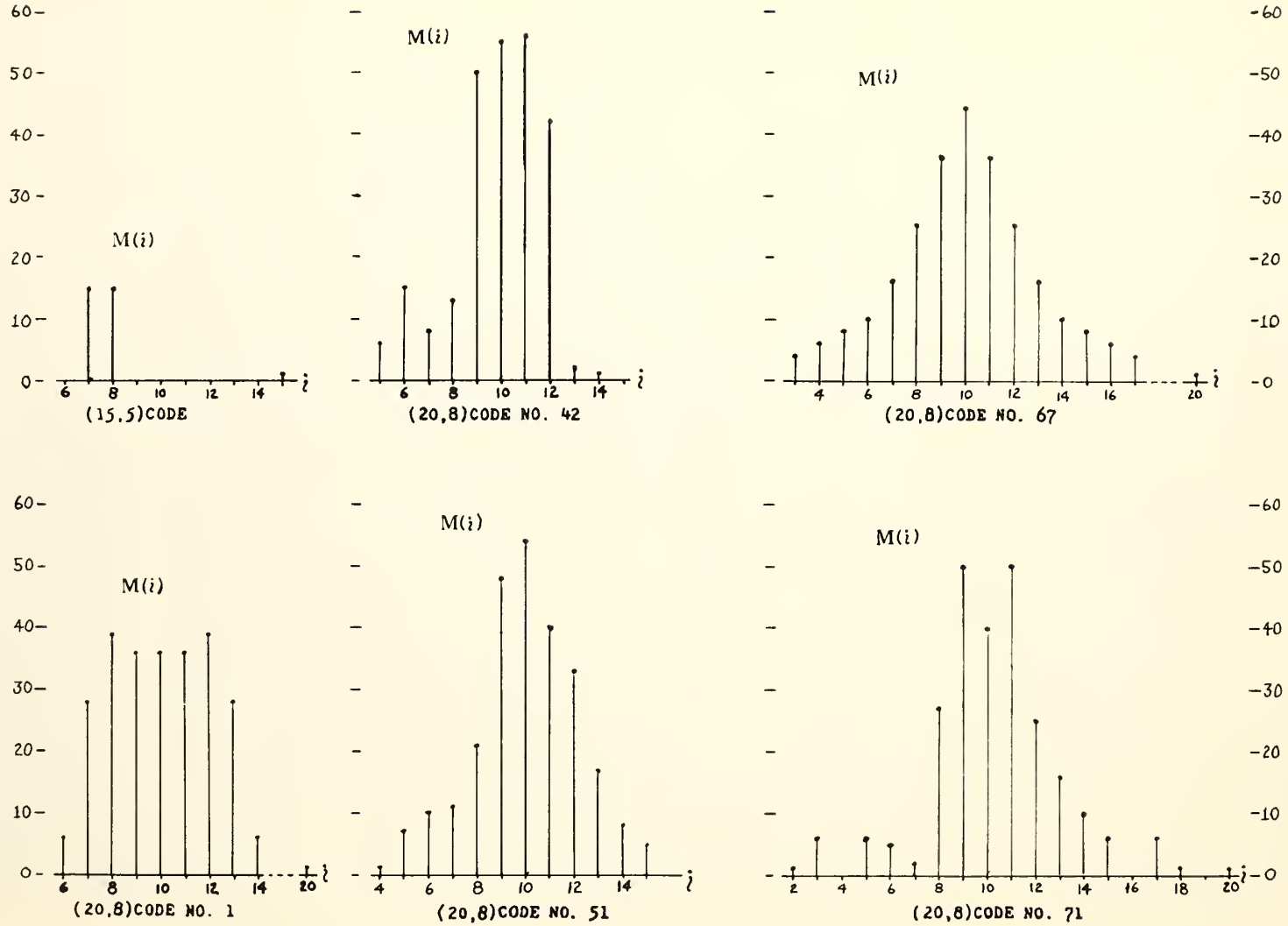

Figure 2. Distribution of distances for the (15,5) code and selected (20,8) codes.

decreasing performance (viz., increasing P_e). The main reason for different P_e values for (20, 8) codes is, by and large, not the entire distance distribution M(i), but rather the minimum distance properties. Note, that code 1 has MD = 6 and M(6) = 6, while code 71 has MD = 2 and M(2) = 1.

Figure 3 shows P_e versus p_e characteristics for selected (20, 8) codes, namely, those numbered 1, 42, 51, 67, and 71. It is clear that the best of these (20, 8) codes is code 1, although there are some forty other codes (2 through 42) that are almost as good as code 1.

4. COMPARISON OF (15, 5) and (20, 8) CODES

In this section we compare the performance characteristics of (15, 5) BCH code with the best (20, 8) code, code 1 of table 1. As is typically the case, the P_e characteristics depend strongly on one's point of view towards pertinent system's parameters. We present two distinct comparison cases, where different parameters are kept invariant, and where different trade-offs result.

4.1 Case of Identical Baud (Keying) Speed

To compare different coding schemes, let the modems be the same and p_e be independent of the code. First note that the transmission rates (i.e., the data throughputs) are not the same for the two codes,

$$\frac{R(20, 8)}{R(15, 5)} = \frac{8/20}{5/15} = \frac{6}{5} .$$

The (20, 8) code has a 20% speed superiority over the (15, 5) code, but this supremacy does not extend to error correcting ability.

Word error probabilities P_e have been computed for the (15, 5) BCH code and for the (20, 8) no. 1 code. The results are presented in figure 4 and in table 2. We now have an option: to compare the

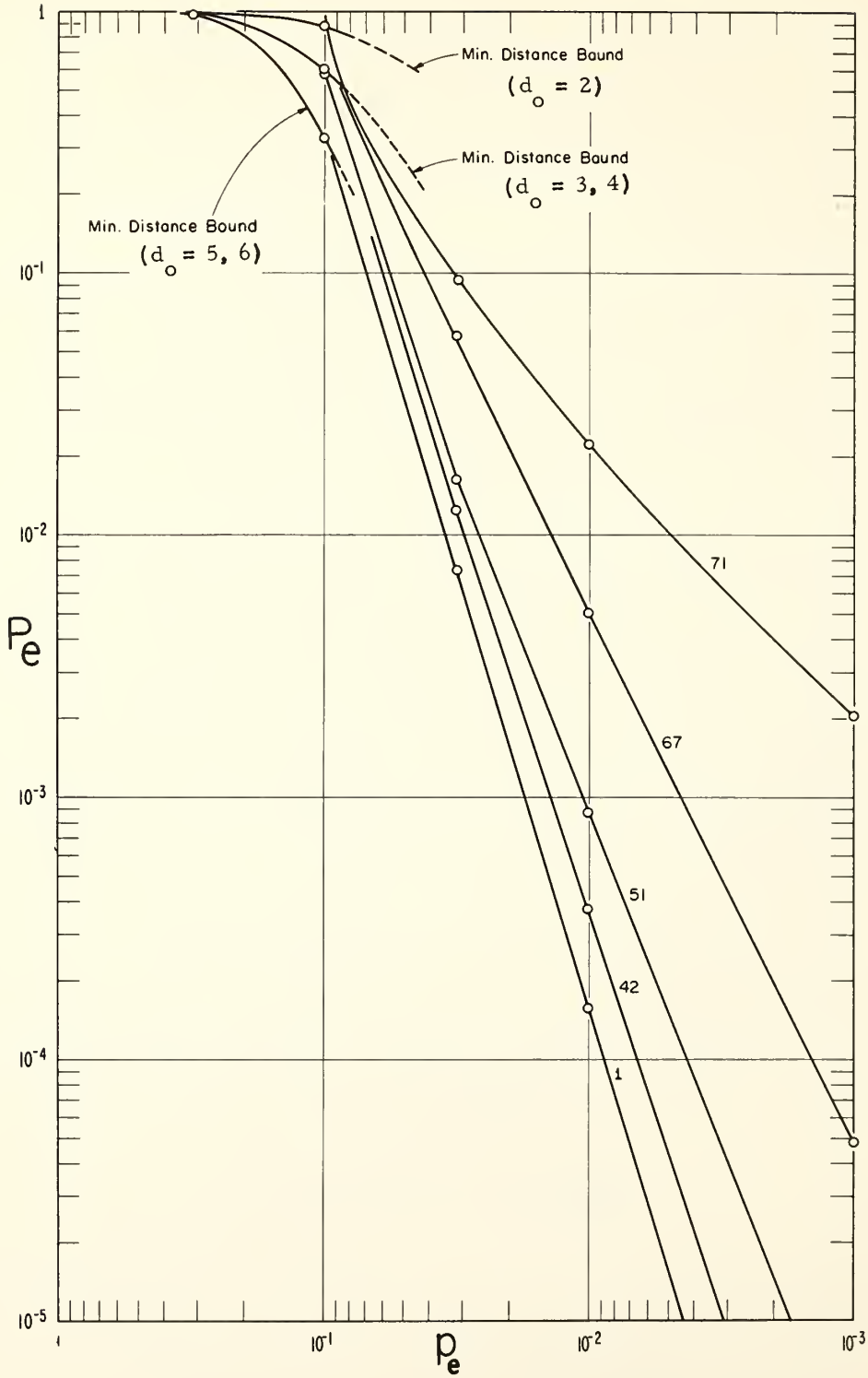

Figure 3. Word error probability characteristics for selected (20, 8) codes.

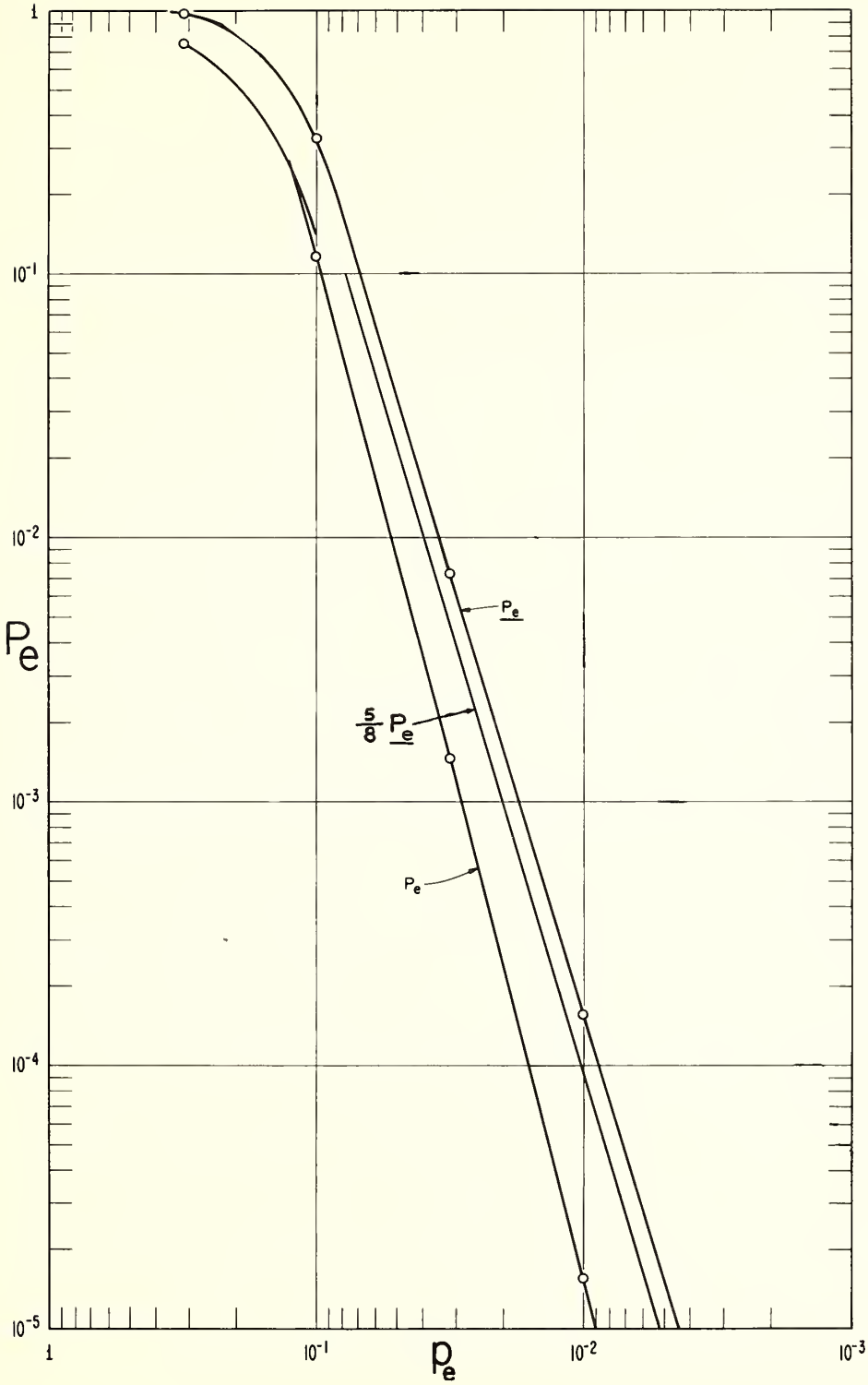

Figure 4. Word error probability comparison of the (15,5) code (P_e) with the No. 1 (20,8) code ($\underline{P_e}$) at identical baud speeds.

Table 2. Minimum Distance Values and Selected Cases for Comparison

Minimum Distance Values

	MIN. DIST. ↓ PE →	3.16-01	1.00-01	3.16-02	1.00-02
[20,8]	2	1.00+00	8.78-01	4.74-01	1.82-01
	3,4	9.95-01	6.08-01	1.31-01	1.69-02
	5,6	9.75-01	3.23-01	2.41-02	1.00-03
[15,5]	7	7.51-01	1.40-01	9.72-02	4.22-02

Selected Cases for Comparison

CODE ↓ PE →	3.16-01	1.00-01	3.16-02	1.00-02	1.00-03	1.00-04
$P_e = F_{(15,\ 5)}(p_e)$						
65	5.59+00	1.16-01	1.43-03	1.53-05	1.57-09	1.57-13
1 53 MD OF 7 NCW 15 15 (1)						
$\frac{5}{8}\underline{P_e} = \frac{5}{8}F_{(20,\ 8)}(p_e)$						
647	6.09-01	2.02-01	4.58-03	9.67-05	7.72-08	7.52-11
2 713 MD OF 6 NCW 6 28 39 36 36 36 39 28 6						
$\underline{P_e} = F_{(20,\ 8)}(2^{1/5}\ p_e^{\ 6/5})$						
	9.56-01	2.74-01	1.72-01	9.46-02		
647	2.73+01	1.47-01	1.11-03	1.30-05	2.91-09	7.24-13
3 713 MD OF 6 NCW 6 28 39 36 36 36 39 28 6						

P_e of (15, 5) with $\underline{P}_e$ of (20, 8) or with 5/8 $\underline{P}_e$ of the same (20, 8) code. The issue depends on the choice of data block size to be used as a "standard word." Choices of 5, 8, or $5 \times 8 = 40$ appear plausible. Regardless of one's preference, the (15, 5) code shows a substantial performance advantage over the best of the (20, 8) codes, hence over all cyclic (20, 8) codes.

4.2 Case of Same Transmission Rate

If transmission rates are set equal, baud speeds must differ by the earlier factor of 6/5. Let us assume a specific modem, noncoherent frequency shift keying (NCFSK). The bit error probability is an exponential function of the signal power-to-noise power density ratio times the baud time (Lawton, 1958; Wozencraft and Jacobs, 1967). It follows that, if p_e is the bit error probability for (15, 5) code, $(2p_e^6)^{1/5}$ must play the corresponding role for bit error rate in a (20, 8) code. Previous formulas now enable the computation of word error probabilities P_e.

The computer results for constant transmission rate are presented in table 2 and figure 5. Again, the best (20, 8) code (no. 1) is compared with the (15, 5) BCH code, and the results are much more even.

At $p_e \cong 5(10^{-2})$ the two systems are indistinguishable. For $p_e > 5(10^{-2})$ the (15, 5) code shows a slight advantage, while for $p_e < 5(10^{-2})$ the (20, 8) no. 1 code does better. One expects, that for very small p_e the asymptotic exponential nature of all modems (nonfading channels!) would guarantee a considerable superiority for the (20, 8) no. 1 code.

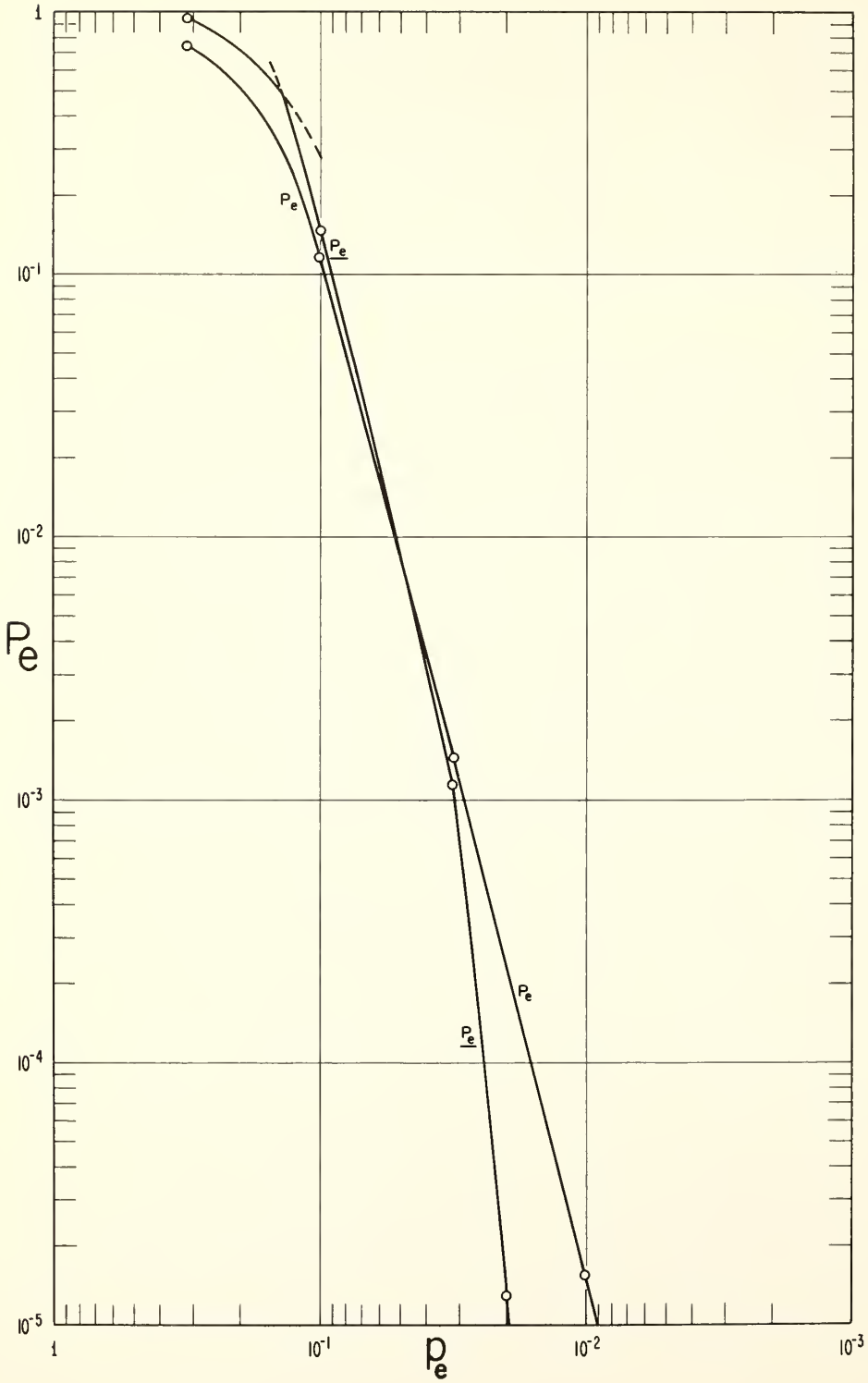

Figure 5. Word error probability comparison of the (15,5) code (P_e) with the No. 1 (20,8) code ($\underline{P_e}$) at same transmission rate.

5. CONCLUSIONS

The goal of this study was to find the best cyclic, simply generated (20, 8) block codes and to compare their performance with the well known (15, 5) BCH code. A search and performance scrutiny was carried out, and the results were disappointing. The very best (20, 8) code (no. 1 in table 1 with shift register generator 647 or 713, as shown in fig. 1) simply does not outperform the (15, 5) code. In the case (4.1) of identical baud speeds, the (20, 8) is worse. In the case (4.2) of identical data rates the two codes appear evenly matched, and the (20, 8) requires 5/6 less bandwidth.

6. REFERENCES

Feller, W. (1960), An Introduction to Probability Theory and Its Applications, I, 23, 41-45 (John Wiley & Sons, Inc., New York, N. Y.).

Gallager, R. G. (1968), Information Theory and Reliable Communication, 116-135 (John Wiley & Sons, Inc., New York, N. Y.).

Lawton, F. G. (1958), Comparison of binary data transmission systems, Second National Conference on Military Electronics.

Peterson, W. W. (1961), Error-Correcting Codes, 30-47, 107-161, 251-270 (The M.I.T. Press and John Wiley & Sons, Inc., New York, N. Y.).

Wozencraft, J. M. and I. M. Jacobs (1967), Principles of Communication Engineering, 264-266, 519-524 (John Wiley & Sons, Inc., New York, N. Y.).

APPENDIX A
Detailed Results - Computation and Tables

A cyclic code may be generated using a linear feedback shift register circuit (Peterson, 1961). The feedback is formed by an "exclusive OR" (sum modulo 2) gate of certain register stage outputs. These outputs are represented as the nonvanishing terms in a generator polynomial

$$g(x) = x^8 + A_7 x^7 + \ldots + A_1 x^1 + 1 . \qquad \text{(A-1)}$$

This equation yields a nine-bit representation for the feedback connections in the generator circuit. The first and last (x^8 and 1) coefficients are always unity. The binary number that represents the coefficients has nine digits, or three digits of octal notation (Peterson, 1961). If one reverses the order of the connections, then a new code results:

$$110\,100\,111 = 647$$
$$111\,001\,011 = 713 \; .$$

This symmetry yields the same distance structure for both codes; therefore, the number of structurally distinct codes (excluding all zeros) is about half of the total, i.e., $\frac{1}{2}(2^7) = 64$. A detailed count reveals 71 distinct cases.

The simulation of a shift register was done on a CDC 6400 computer. For each code one can easily generate the 2^8 -1 nonzero combinations of the eight information bits and corresponding codewords and the subsequent count of ones in the words relative to the base codeword of all zeros. The count M(i), of codewords at distance i from the all zero word is given in the second line for each code in table 1. For example
1 713 MD OF 6 NCW 6 28 39 36 36 36 39 28 6 (1),
where (1) stands for one codeword of weight 20, states that code 647 and

713 has a minimum distance word of 6, and that the number of codewords at distance 6 is 6, at distance 7 is 28, at distance 8 is 39, etc. Some of the code numbers are followed by a letter that has the identical representation, as in Peterson (1961). The asterisk indicates codes that represent primitive binary polynomials (A-1).

The first line for each code of table 1 gives the codeword probability of error (see app. B):

$$\bar{P}_e = \sum_{i=1}^{N} M(i)\, p_e^{\boxed{i}} (1 - p_e)^{N - \boxed{i}} \sum_{k=0}^{N - \boxed{i}} A_{ki} \left(\frac{p_e}{1 - p_e} \right)^k \tag{A-2}$$

where $\boxed{i} = \left[\frac{i+1}{2} \right]$ and

$$A_{ki} = \sum_{j=\boxed{i}}^{\bar{i}} \binom{i}{j} \binom{N - i}{\boxed{i} + k - j}, \quad \bar{i} = \min[k + \boxed{i},\ i] \tag{A-3}$$

is computed for each of six discrete values of p_e listed at the top of each page of table 1.

The union bound nature in (A-2) leads to excessively large $\bar{P}_e$ for p_e around 10^{-1} or larger. Another familiar upper bound, the minimum distance bound, is used (see app. B):

$$\bar{Q}_e = 1 - \sum_{n=0}^{\boxed{d_o} - 1} \binom{N}{n} p_e^{\,n} (1 - p_e)^{N - n} . \tag{A-4}$$

This leads to the same expression $\overline{Q}_e$ for certain pairs of minimum distance values d_o. For example, $\boxed{4} = \boxed{5} = 3$ and therefore $d_o = 4$ and $d_o = 5$ have identical $\overline{Q}_e$ values. The least of the two bounds ($\overline{P}_e$ and $\overline{Q}_e$) is clearly the best and should be used.

In table 2 we find the first entries are the $\overline{Q}_e$ (A-4) bounds that are based on minimum distance properties of the code. Note that the last row applies to the (15, 5) BCH code only. Later entries in the table show additional word error probability computations presented in the style of table 1 except the entry no. 3 whose first line is the $\overline{Q}_e$ bound for this selected case.

APPENDIX B
Upper Bounds on Word Error Probability

The word error probability P_e is rather tedious to compute for most codes; however, P_e may be easily bounded in a number of different ways.

In this appendix we derive two upper bounds on P_e that are valid for the binary symmetric channel (BSC), and call them $\overline{P}_e$ and $\overline{Q}_e$. These bounds are functions of the binary error probability in the BSC. One is advised to use the least of the two bounds,

$$P_e \leq \min\left(\overline{P}_e, \overline{Q}_e\right) . \tag{B-1}$$

The newer "union bound" $\overline{P}_e$ and the familiar "minimum distance bound" $\overline{Q}_e$ are given next:

The Union Bound

$$\overline{P}_e = \sum_{i=1}^{N} M(i)\, p_e^{\boxed{i}} (1 - p_e)^{N - \boxed{i}} \sum_{k=0}^{N - \boxed{i}} A_{ki} \left(\frac{p_e}{1 - p_e}\right)^k ,$$

$$A_{ki} \equiv \sum_{j = \boxed{i}}^{\min(i,\, \boxed{i}+k)} \binom{i}{j} \binom{N - i}{\boxed{i} + k - j} , \tag{B-2}$$

where

p_e = BSC error probability,

N = code word or block length,

$M(i)$ = number of neighbors a distance i away from a given code word,

$\boxed{x}$ = integer part of $\frac{1}{2}(x+1)$.

The Minimum Distance Bound

$$\overline{Q}_e = 1 - \sum_{n=o}^{\boxed{d_o}-1} \binom{N}{n} p_e^{\,n} (1 - p_e)^{N-n} \quad , \tag{B-3}$$

where

d_o = minimum distance between code words.

Proof of the Union Bound

Consider a code (i.e., a finite set of code words) $w_o, w_1, \ldots, w_M$ - all of length N. Assume that the distance structure of this block code is known, and let these known distances be

$$d_m = d(w_o, w_m), \quad m = 1, \ldots, M \quad . \tag{B-4}$$

In this way we also know the neighbor counts that are exactly a distance i from w_o. Denote this count of i-neighbors by $M(i)$, $1 \le i \le N$.

$$M(i) = \sum_{m=1}^{M} \delta_{i, d_m} \quad , \tag{B-5}$$

where $\delta_{i,j}$ is the Kronecker delta symbol, and

$$\sum_{i=1}^{N} M(i) = M \quad . \tag{B-6}$$

As is customary, let w_e be the N bit error word, and let e be the number of errors (number of ones) in w_e. Clearly, $0 \le e \le N$ with the smaller e values much more likely in practice.

If a word w_o is sent, then $w_o + w_e$ is received. Decoding errors will occur whenever for some $m (m = 1, \ldots, M)$ w_m is as close or closer

to $w_o + w_e$ than w_o is. We denote the probability of this o to m error event by P_{em}. If a set of e errors contributes toward altering w_o into w_m, then each binary error must fall into one of two categories. Take an error that occurs in a bit where w_o and w_m agree. Clearly, this error must move w_o one unit away from w_m. We denote the number of such (moving away) errors by $e(\leftarrow m)$. An error in a digit where w_o and w_m differ must bring w_o one step toward w_m. We denote the number of errors in this second category (moving together) by $e(\rightarrow m)$. Immediately

$$e(\rightarrow m) + e(\leftarrow m) = e \quad , \tag{B-7}$$

a fact that is useful in bounding P_{em}.

$$\begin{aligned} P_{em} &\leq P\left[d(w_o + w_e, w_m) \leq d(w_o + w_e, w_o)\right] \\ &\leq P\left[d_m + e(\leftarrow m) - e(\rightarrow m) \leq e\right] \\ &\leq P\left[2e(\rightarrow m) \geq d_m\right] \qquad \text{(B-8)} \\ &\leq P\left[e(\rightarrow m) \geq \boxed{d_m}\right] \\ &\leq \sum_{n=\boxed{d_m}}^{N} P[e=n] \cdot P[e(\rightarrow m) \geq \boxed{d_m} \mid e=n] \quad . \end{aligned}$$

Both probabilities in the sum (B-8) are well known for BSC; thus, the $P[e = n]$ term is a mere binomial,

$$P[e = n] = \binom{N}{n} p_e^{\,n} (1 - p_e)^{N-n} \quad , \tag{B-9}$$

while the $P[\ldots \mid e = n]$ term can be interpreted as a random population problem (Feller, 1960). Let a population of N elements consist of d_m red and $N - d_m$ black elements. A group of n elements is chosen at random. We seek the probability that exactly j elements turn out to be red and n-j black. The well known answer is given by the hypergeometric distribution:

$$P[e(\rightarrow m) = j \mid e = n] = \frac{\binom{d_m}{j}\binom{N - d_m}{n - j}}{\binom{N}{n}} . \qquad \text{(B-10)}$$

A substitution of (B-9) and (B-10) into (B-8) yields a bound on P_{em},

$$P_{em} \leq \sum_{n = \boxed{d_m}}^{N} \sum_{j = \boxed{d_m}}^{\min(d_m, n)} \binom{d_m}{j}\binom{N - d_m}{n - j} p_e^{\,n}(1 - p_e)^{N - n} . \qquad \text{(B-11)}$$

It remains to take into account all code words $m = 1, \ldots, M$. The overall word error probability P_e must surely be upper bounded by the "union bound" (Feller, 1960, calls it the Boole's Inequality):

$$\begin{aligned} P_e &\leq \sum_{m = 1}^{M} P_{em} \\ &\leq \sum_{i = 1}^{N} M(i)\ P_{em}\Big|_{d_m = i} . \end{aligned} \qquad \text{(B-12)}$$

A substitution of (B-11) into (B-12) plus a few housekeeping tasks, such as dubbing a combinational coefficient A_{ki} and naming the entire right side $\overline{P}_e$ finally yields (B-2).

Proof of the Minimum Distance Bound

Equation (B-3) is well known and obvious; therefore the following is given only for sake of completeness.

Define the minimum distance d_o of a linear block code as

$$d_o \equiv \min_{1 \le m \le M} d_m \quad , \tag{B-13}$$

and a quantity

$$\overline{Q}_e \equiv P[\,2e \ge d_o\,] \quad . \tag{B-14}$$

Then for any e,

$$\begin{aligned} 1 &= P[\,2e < d_o\,] + P[\,2e \ge d_o\,] \\ &\le 1 - P_e + \overline{Q}_e \quad , \end{aligned} \tag{B-15}$$

and, necessarily, $P_e \le \overline{Q}_e$; while

$$\overline{Q}_e = 1 - P[\,e < \boxed{d_o}\,] \tag{B-16}$$

can be expressed with the aid of (B-9).

Note

The "union bound" (B-2) becomes poor whenever the underlying events have large intersections in common. In our case, this is guaranteed to occur for large p_e, say for $10^{-1} \le p_e \le \frac{1}{2}$. In such cases, $\overline{P}_e$ may even exceed unity--an altogether deplorable situation. But, then is the time to use the "minimum distance bound"(B-3), which is always less than one.

In the other extreme, when p_e is negligibly small $0 < p_e << 1$, $\overline{P}_e < \overline{Q}_e$ and the "union bound" is the tightest of these two upper bounds.

GPO 830-057

PENN STATE UNIVERSITY LIBRARIES
A000072020104