Quiz EL405
Channel Coding: Linear Block Codes

Lucas Monteiro Nogueira

PROBLEMS

Problem 1 (Sklar, 2001, w/ permission)

Calculate the probability of message error for a 12-bit data sequence encoded with a (24,12) linear block code. Assume that the code corrects all 1-bit and 2-bit error patterns and assume that it corrects no error patterns with more than two errors. Also, assume that the probability of a channel symbol error is 10^{-3}.

Problem 2 (Sklar, 2001, w/ permission)

Calculate the improvement in probability of message error relative to an uncoded transmission for a (24,12) double-error-correcting linear block code. Assume that coherent BPSK modulation is used and that the received bit energy to noise spectral density E_b/N_0 = 10 dB.

Problem 3 (Sklar, 2001, w/ permission)

Consider a (24, 12) linear block code capable of double-error corrections. Assume that a noncoherently detected binary orthogonal frequency-shift keying (BFSK) modulation format is used and that the received E_b/N_0 = 14 dB.

Problem 3.1: Does the code provide any improvement in probability of message error? If it does, how much? If it does not, explain why not.

Problem 3.2: Repeat part 1 with E_b/N_0 = 10 dB.

Problem 4 (Proakis and Salehi, 2008, w/ permission)

$\mathcal{C}$ is a (6,3) linear block code whose generator matrix is given by

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Problem 4.1: What rate, minimum distance, and coding gain can $\mathcal{C}$ provide in *soft decision* decoding when BPSK is used over an AWGN channel?

Problem 4.2: Can you suggest another (6,3) linear block code that can provide a better coding gain? If the answer is yes, give the generator matrix for one such code. If the answer is no, why?

Problem 4.3: Suggest a parity check matrix $\boldsymbol{H}$ for $\mathcal{C}$.

Problem 5 (Proakis and Salehi, 2008, w/ permission)

A (k + 1,k) block code is generated by adding 1 extra bit to each information sequence of length k such that the overall parity of the code (i.e., the number of 1s in each code word) is an odd number. Two students, A and B, make the following arguments on the *error detection* capability of this code.

Student A: Since the weight of each code word is odd, any single error changes the weight to an even number. Hence, this code is capable of detecting any single error.

Student B: The all-zero information sequence 00 ... 0 (k zeros) will be encoded by adding one extra 1 to generate the code word 00 ... 01. This means that there is at least one code word of weight 1 in this code. Therefore, the minimal distance d_{min} = 1, and since any code can detect at most d_{min} − 1 errors, and for this code d_{min} − 1 = 0, this code cannot detect any errors.

One of the students is wrong. Which one? Why?

Problem 6 (Proakis and Salehi, 2008, w/ permission)

A code $\mathcal{C}$ consists of all binary sequences of length 6 and weight 3.

Problem 6.1: Is this code a linear block code? Why?
Problem 6.2: What are the rate and minimum distance of the code?
Problem 6.3: If the code is used for error detection, how many errors can it detect?
Problem 6.4: If the code is used on a binary symmetric channel with crossover probability of p, what is the probability that an undetectable error results?
Problem 6.5: Find the smallest linear block code $\mathcal{C}_1$ such that $\mathcal{C} \subseteq \mathcal{C}_1$ (by the smallest code we mean the code with the fewest code words).

Problem 7 (Sklar, 2001, w/ permission)

Consider a (7,4) code whose generator matrix is

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Problem 7.1: Find all the code words of the code.
Problem 7.2: Find H, the parity-check matrix of the code.
Problem 7.3: Compute the syndrome for the received vector 1 1 0 1 1 0 1. Is this a valid code vector?
Problem 7.4: What is the error-correcting capability of the code?
Problem 7.5: What is the error-detecting capability of the code?

Problem 8 (Sklar, 2001, w/ permission)

Consider the linear block code with the code word defined by

$$\mathbf{U} = m_1 + m_2 + m_4 + m_5,\ m_1 + m_3 + m_4 + m_5,\ m_1 + m_2 + m_3 + m_5$$
$$m_1 + m_2 + m_3 + m_4,\ m_1,\ m_2,\ m_3,\ m_4,\ m_5$$

where m_i are message digits.

Problem 8.1: Show the generator matrix.
Problem 8.2: Show the parity-check matrix.
Problem 8.3: Find n, k, and d_{min}.

Problem 9 (Sklar, 2001, w/ permission)

Consider a systematic block code whose parity-check equations are

$$p_1 = m_1 + m_2 + m_4$$
$$p_2 = m_1 + m_3 + m_4$$
$$p_3 = m_1 + m_2 + m_3$$
$$p_4 = m_2 + m_3 + m_4$$

where m_i are message digits and p_i are check digits.

Problem 9.1: Find the generator matrix and the parity-check matrix for this code.
Problem 9.2: How many errors can the code correct?
Problem 9.3: Is the vector 10101010 a code word?
Problem 9.4: Is the vector 01011100 a code word?

Problems 10 to 12 emphasize cyclic codes. We'll go back to linear block codes in Problem 14.

Problem 10 (Sklar, 2001, w/ permission)

Determine which, if any, of the following polynomials can generate a cyclic code with code word length $n \leq 7$. Find the (n,k) values of any such codes that can be generated.

Problem 10.1: $1 + X^3 + X^4$
Problem 10.2: $1 + X^2 + X^4$
Problem 10.3: $1 + X + X^2 + X^4$

Problem 11 (Sklar, 2001, w/ permission)

Encode the message **1 0 1** in systematic form using polynomial division and the generator $\boldsymbol{g}(X) = 1 + X + X^2 + X^4$.

Problem 12 (Sklar, 2001, w/ permission)

A (15,5) cyclic code has a generator polynomial as follows:

$$\mathbf{g}(X) = 1 + X + X^2 + X^5 + X^8 + X^{10}$$

Problem 12.1: Find the code polynomial (in systematic form) for the message $\boldsymbol{m}(X) = 1 + X^2 + X^4$.

Problem 12.2: Is $\boldsymbol{V}(X) = 1 + X^4 + X^6 + X^8 + X^{14}$ a code polynomial in this system? Justify your answer.

Problem 13 (Sklar, 2001, w/ permission)

Is a (7,3) code a perfect code? Is a (7,4) code a perfect code? Is a (15,11) code a perfect code? Justify your answers.

Problem 14 (Sklar, 2001, w/ permission)

A (15,11) linear block code can be defined by the following parity array:

$$\mathbf{P} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Problem 14.1: Show the parity-check matrix for this code.

Problem 14.2: List the coset leaders from the standard array. Is this code a perfect code? Justify your answer.

Problem 14.3: A received vector is $\boldsymbol{V}$ = 0 1 1 1 1 1 0 0 1 0 1 1 0 1 1. Compute the syndrome. Assuming that a single bit error has been made, find the correct code word.

Problem 14.4: How many erasures can this code correct? Explain.

Problem 15 (Sklar, 2001, w/ permission)

A message consists of English text (assume that each word in the message contains six letters). Each letter is encoded using the 7-bit ASCII character code. Thus, each word consists of a 42-bit sequence. The message is to be transmitted over a channel having a symbol error probability of 10^{-3}.

Problem 15.1: What is the probability that a word will be received in error?

Problem 15.2: If a repetition code is used such that each letter in each word is repeated three times, and at the receiver, majority voting is used to decode the message, what is the probability that a decoded word will be received in error?

Problem 15.3: If a (126,42) BCH code with error-correcting capability of $t = 14$ is used to encode each 42-bit word, what is the probability that a decoded word will be in error?

Problem 15.4: For a real system, it is not fair to compare uncoded versus coded message error performance on the basis of a fixed probability of channel symbol error, since this implies a fixed level of received channel symbol energy per noise density E_c/N_0, for all choices of coding (or lack of coding). Therefore, repeat parts 1 to 3 under the condition that the channel symbol error probability is determined by a bit-energy to noise density ratio, E_b/N_0, of 12 dB. Assume that the information rate must be the same for all choices of coding or lack of coding. Also assume that noncoherent, orthogonal binary FSK modulation is used over an AWGN channel.

Problem 15.5: Discuss the relative error performance capabilities of the above coding schemes under the two postulated conditions – fixed channel symbol error probability, and fixed bit energy to noise density ratio, E_b/N_0. Under what circumstances can a repetition code offer error performance improvement? When will it cause performance degradation?

Problem 16 (Sklar, 2001, w/ permission)

Information from a source is organized in 36-bit messages that are to be transmitted over an AWGN channel using noncoherently detected BFSK modulation.

Problem 16.1: If no error control coding is used, compute the bit energy to noise density ratio, E_b/N_0, required to provide a message error probability of 10^{-3}.

Problem 16.2: Consider the use of a (127, 36) linear block code (minimum distance is 31) in the transmission of these messages. Compute the coding gain for this code for a message error probability of 10^{-3}. (The coding gain is defined as the difference between the E_b/N_0 required without coding and the E_b/N_0 required with coding.)

Problem 17 (Sklar, 2001, w/ permission)

Problem 17.1: Using the generator polynomial for the (15,5) cyclic code introduced in Problem 12, encode the message sequence `1 1 0 1 1` in systematic form. Show the resulting code word polynomial. What property characterizes the degree of the generator polynomial?

Problem 17.2: Consider that the received code word is corrupted by an error pattern $e(X) = X^8 + X^{10} + X^{13}$. Show the corrupted code word polynomial.

Problem 17.3: Form the syndrome polynomial by using the generator and received-code word polynomials.

Problem 17.4: Form the syndrome polynomial by using the generator and error-pattern polynomials, and verify that this is the same syndrome computed in part 3.

Problem 17.5: Explain why the syndrome computations in parts 3 and 4 must yield identical results.

Problem 17.6: Using the properties of the standard array of a (15,5) linear block code, find the maximum amount of error correction possible for a code with these parameters. Is a (15,5) code a perfect code?

Problem 17.7: If we want to implement the (15,5) cyclic code to simultaneously correct two erasures and still perform error correction, how much error correction would have to be sacrificed?

ADDITIONAL INFORMATION

The following two pages show tabulated values of the Q function.

TABLE 8.2[3]
$Q(x)$

x	0.00	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09
0.0000	.5000	.4960	.4920	.4880	.4840	.4801	.4761	.4721	.4681	.4641
.1000	.4602	.4562	.4522	.4483	.4443	.4404	.4364	.4325	.4286	.4247
.2000	.4207	.4168	.4129	.4090	.4052	.4013	.3974	.3936	.3897	.3859
.3000	.3821	.3783	.3745	.3707	.3669	.3632	.3594	.3557	.3520	.3483
.4000	.3446	.3409	.3372	.3336	.3300	.3264	.3228	.3192	.3156	.3121
.5000	.3085	.3050	.3015	.2981	.2946	.2912	.2877	.2843	.2810	.2776
.6000	.2743	.2709	.2676	.2643	.2611	.2578	.2546	.2514	.2483	.2451
.7000	.2420	.2389	.2358	.2327	.2296	.2266	.2236	.2206	.2177	.2148
.8000	.2119	.2090	.2061	.2033	.2005	.1977	.1949	.1922	.1894	.1867
.9000	.1841	.1814	.1788	.1762	.1736	.1711	.1685	.1660	.1635	.1611
1.000	.1587	.1562	.1539	.1515	.1492	.1469	.1446	.1423	.1401	.1379
1.100	.1357	.1335	.1314	.1292	.1271	.1251	.1230	.1210	.1190	.1170
1.200	.1151	.1131	.1112	.1093	.1075	.1056	.1038	.1020	.1003	.9853E-01
1.300	.9680E-01	.9510E-01	.9342E-01	.9176E-01	.9012E-01	.8851E-01	.8691E-01	.8534E-01	.8379E-01	.8226E-01
1.400	.8076E-01	.7927E-01	.7780E-01	.7636E-01	.7493E-01	.7353E-01	.7215E-01	.7078E-01	.6944E-01	.6811E-01
1.500	.6681E-01	.6552E-01	.6426E-01	.6301E-01	.6178E-01	.6057E-01	.5938E-01	.5821E-01	.5705E-01	.5592E-01
1.600	.5480E-01	.5370E-01	.5262E-01	.5155E-01	.5050E-01	.4947E-01	.4846E-01	.4746E-01	.4648E-01	.4551E-01
1.700	.4457E-01	.4363E-01	.4272E-01	.4182E-01	.4093E-01	.4006E-01	.3920E-01	.3836E-01	.3754E-01	.3673E-01
1.800	.3593E-01	.3515E-01	.3438E-01	.3362E-01	.3288E-01	.3216E-01	.3144E-01	.3074E-01	.3005E-01	.2938E-01
1.900	.2872E-01	.2807E-01	.2743E-01	.2680E-01	.2619E-01	.2559E-01	.2500E-01	.2442E-01	.2385E-01	.2330E-01
2.000	.2275E-01	.2222E-01	.2169E-01	.2118E-01	.2068E-01	.2018E-01	.1970E-01	.1923E-01	.1876E-01	.1831E-01
2.100	.1786E-01	.1743E-01	.1700E-01	.1659E-01	.1618E-01	.1578E-01	.1539E-01	.1500E-01	.1463E-01	.1426E-01
2.200	.1390E-01	.1355E-01	.1321E-01	.1287E-01	.1255E-01	.1222E-01	.1191E-01	.1160E-01	.1130E-01	.1101E-01
2.300	.1072E-01	.1044E-01	.1017E-01	.9903E-02	.9642E-02	.9387E-02	.9137E-02	.8894E-02	.8656E-02	.8424E-02
2.400	.8198E-02	.7976E-02	.7760E-02	.7549E-02	.7344E-02	.7143E-02	.6947E-02	.6756E-02	.6569E-02	.6387E-02
2.500	.6210E-02	.6037E-02	.5868E-02	.5703E-02	.5543E-02	.5386E-02	.5234E-02	.5085E-02	.4940E-02	.4799E-02
2.600	.4661E-02	.4527E-02	.4396E-02	.4269E-02	.4145E-02	.4025E-02	.3907E-02	.3793E-02	.3681E-02	.3573E-02
2.700	.3467E-02	.3364E-02	.3264E-02	.3167E-02	.3072E-02	.2980E-02	.2890E-02	.2803E-02	.2718E-02	.2635E-02
2.800	.2555E-02	.2477E-02	.2401E-02	.2327E-02	.2256E-02	.2186E-02	.2118E-02	.2052E-02	.1988E-02	.1926E-02
2.900	.1866E-02	.1807E-02	.1750E-02	.1695E-02	.1641E-02	.1589E-02	.1538E-02	.1489E-02	.1441E-02	.1395E-02
3.000	.1350E-02	.1306E-02	.1264E-02	.1223E-02	.1183E-02	.1144E-02	.1107E-02	.1070E-02	.1035E-02	.1001E-02
3.100	.9676E-03	.9354E-03	.9043E-03	.8740E-03	.8447E-03	.8164E-03	.7888E-03	.7622E-03	.7364E-03	.7114E-03
3.200	.6871E-03	.6637E-03	.6410E-03	.6190E-03	.5976E-03	.5770E-03	.5571E-03	.5377E-03	.5190E-03	.5009E-03
3.300	.4834E-03	.4665E-03	.4501E-03	.4342E-03	.4189E-03	.4041E-03	.3897E-03	.3758E-03	.3624E-03	.3495E-03
3.400	.3369E-03	.3248E-03	.3131E-03	.3018E-03	.2909E-03	.2802E-03	.2701E-03	.2602E-03	.2507E-03	.2415E-03
3.500	.2326E-03	.2241E-03	.2158E-03	.2078E-03	.2001E-03	.1926E-03	.1854E-03	.1785E-03	.1718E-03	.1653E-03
3.600	.1591E-03	.1531E-03	.1473E-03	.1417E-03	.1363E-03	.1311E-03	.1261E-03	.1213E-03	.1166E-03	.1121E-03
3.700	.1078E-03	.1036E-03	.9961E-04	.9574E-04	.9201E-04	.8842E-04	.8496E-04	.8162E-04	.7841E-04	.7532E-04
3.800	.7235E-04	.6948E-04	.6673E-04	.6407E-04	.6152E-04	.5906E-04	.5669E-04	.5442E-04	.5223E-04	.5012E-04
3.900	.4810E-04	.4615E-04	.4427E-04	.4247E-04	.4074E-04	.3908E-04	.3747E-04	.3594E-04	.3446E-04	.3304E-04
4.000	.3167E-04	.3036E-04	.2910E-04	.2789E-04	.2673E-04	.2561E-04	.2454E-04	.2351E-04	.2252E-04	.2157E-04
4.100	.2066E-04	.1978E-04	.1894E-04	.1814E-04	.1737E-04	.1662E-04	.1591E-04	.1523E-04	.1458E-04	.1395E-04
4.200	.1335E-04	.1277E-04	.1222E-04	.1168E-04	.1118E-04	.1069E-04	.1022E-04	.9774E-05	.9345E-05	.8934E-05
4.300	.8540E-05	.8163E-05	.7801E-05	.7455E-05	.7124E-05	.8807E-05	.6503E-05	.6212E-05	.5934E-05	.5668E-05
4.400	.5413E-05	.5169E-05	.4935E-05	.4712E-05	.4498E-05	.4294E-05	.4098E-05	.3911E-05	.3732E-05	.3561E-05
4.500	.3398E-05	.3241E-05	.3092E-05	.2949E-05	.2813E-05	.2682E-05	.2558E-05	.2439E-05	.2325E-05	.2216E-05
4.600	.2112E-05	.2013E-05	.1919E-05	.1828E-05	.1742E-05	.1660E-05	.1581E-05	.1506E-05	.1434E-05	.1366E-05
4.700	.1301E-05	.1239E-05	.1179E-05	.1123E-05	.1069E-05	.1017E-05	.9680E-06	.9211E-06	.8765E-06	.8339E-06
4.800	.7933E-06	.7547E-06	.7178E-06	.6827E-06	.6492E-06	.6173E-06	.5869E-06	.5580E-06	.5304E-06	.5042E-06
4.900	.4792E-06	.4554E-06	.4327E-06	.4111E-06	.3906E-06	.3711E-06	.3525E-06	.3448E-06	.3179E-06	.3019E-06
5.000	.2867E-06	.2722E-06	.2584E-06	.2452E-06	.2328E-06	.2209E-06	.2096E-06	.1989E-06	.1887E-06	.1790E-06
5.100	.1698E-06	.1611E-06	.1528E-06	.1449E-06	.1374E-06	.1302E-06	.1235E-06	.1170E-06	.1109E-06	.1051E-06

(continued)

TABLE 8.2
Continued

x	0.00	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09
5.200	.9964E-07	.9442E-07	.8946E-07	.8476E-07	.8029E-07	.7605E-07	.7203E-07	.6821E-07	.6459E-07	.6116E-07
5.300	.5790E-07	.5481E-07	.5188E-07	.4911E-07	.4647E-07	.4398E-07	.4161E-07	.3937E-07	.3724E-07	.3523E-07
5.400	.3332E-07	.3151E-07	.2980E-07	.2818E-07	.2664E-07	.2518E-07	.2381E-07	.2250E-07	.2127E-07	.2010E-07
5.500	.1899E-07	.1794E-07	.1695E-07	.1601E-07	.1512E-07	.1428E-07	.1349E-07	.1274E-07	.1203E-07	.1135E-07
5.600	.1072E-07	.1012E-07	.9548E-08	.9010E-08	.8503E-08	.8022E-08	.7569E-08	.7140E-08	.6735E-08	.6352E-08
5.700	.5990E-08	.5649E-08	.5326E-08	.5022E-08	.4734E-08	.4462E-08	.4206E-08	.3964E-08	.3735E-08	.3519E-08
5.800	.3316E-08	.3124E-08	.2942E-08	.2771E-08	.2610E-08	.2458E-08	.2314E-08	.2179E-08	.2051E-08	.1931E-08
5.900	.1818E-08	.1711E-08	.1610E-08	.1515E-08	.1425E-08	.1341E-08	.1261E-08	.1186E-08	.1116E-08	.1049E-08
6.000	.9866E-09	.9276E-09	.8721E-09	.8198E-09	.7706E-09	.7242E-09	.6806E-09	.6396E-09	.6009E-09	.5646E-09
6.100	.5303E-09	.4982E-09	.4679E-09	.4394E-09	.4126E-09	.3874E-09	.3637E-09	.3414E-09	.3205E-09	.3008E-09
6.200	.2823E-09	.2649E-09	.2486E-09	.2332E-09	.2188E-09	.2052E-09	.1925E-09	.1805E-09	.1692E-09	.1587E-09
6.300	.1488E-09	.1395E-09	.1308E-09	.1226E-09	.1149E-09	.1077E-09	.1009E-09	.9451E-10	.8854E-10	.8294E-10
6.400	.7769E-10	.7276E-10	.6814E-10	.6380E-10	.5974E-10	.5593E-10	.5235E-10	.4900E-10	.4586E-10	.4292E-10
6.500	.4016E-10	.3758E-10	.3515E-10	.3288E-10	.3077E-10	.2877E-10	.2690E-10	.2516E-10	.2352E-10	.2199E-10
6.600	.2056E-10	.1922E-10	.1796E-10	.1678E-10	.1568E-10	.1465E-10	.1369E-10	.1279E-10	.1195E-10	.1116E-10
6.700	.1042E-10	.9731E-11	.9086E-11	.8483E-11	.7919E-11	.7392E-11	.6900E-11	.6439E-11	.6009E-11	.5607E-11
6.800	.5231E-11	.4880E-11	.4552E-11	.4246E-11	.3960E-11	.3692E-11	.3443E-11	.3210E-11	.2993E-11	.2790E-11
6.900	.2600E-11	.2423E-11	.2258E-11	.2104E-11	.1960E-11	.1826E-11	.1701E-11	.1585E-11	.1476E-11	.1374E-11
7.000	.1280E-11	.1192E-11	.1109E-11	.1033E-11	.9612E-12	.8946E-12	.8325E-12	.7747E-12	.7208E-12	.6706E-12
7.100	.6238E-12	.5802E-12	.5396E-12	.5018E-12	.4667E-12	.4339E-12	.4034E-12	.3750E-12	.3486E-12	.3240E-12
7.200	.3011E-12	.2798E-12	.2599E-12	.2415E-12	.2243E-12	.2084E-12	.1935E-12	.1797E-12	.1669E-12	.1550E-12
7.300	.1439E-12	.1336E-12	.1240E-12	.1151E-12	.1068E-12	.9910E-13	.9196E-13	.8531E-13	.7914E-13	.7341E-13
7.400	.6809E-13	.6315E-13	.5856E-13	.5430E-13	.5034E-13	.4667E-13	.4326E-13	.4010E-13	.3716E-13	.3444E-13
7.500	.3191E-13	.2956E-13	.2739E-13	.2537E-13	.2350E-13	.2176E-13	.2015E-13	.1866E-13	.1728E-13	.1600E-13
7.600	.1481E-13	.1370E-13	.1268E-13	.1174E-13	.1086E-13	.1005E-13	.9297E-14	.8600E-14	.7954E-14	.7357E-14
7.700	.6803E-14	.6291E-14	.5816E-14	.5377E-14	.4971E-14	.4595E-14	.4246E-14	.3924E-14	.3626E-14	.3350E-14
7.800	.3095E-14	.2859E-14	.2641E-14	.2439E-14	.2253E-14	.2080E-14	.1921E-14	.1773E-14	.1637E-14	.1511E-14
7.900	.1395E-14	.1287E-14	.1188E-14	.1096E-14	.1011E-14	.9326E-15	.8602E-15	.7934E-15	.7317E-15	.6747E-15
8.000	.6221E-15	.5735E-15	.5287E-15	.4874E-15	.4492E-15	.4140E-15	.3815E-15	.3515E-15	.3238E-15	.2983E-15
8.100	.2748E-15	.2531E-15	.2331E-15	.2146E-15	.1976E-15	.1820E-15	.1675E-15	.1542E-15	.1419E-15	.1306E-15
8.200	.1202E-15	.1106E-15	.1018E-15	.9361E-16	.8611E-16	.7920E-16	.7284E-16	.6698E-16	.6159E-16	.5662E-16
8.300	.5206E-16	.4785E-16	.4398E-16	.4042E-16	.3715E-16	.3413E-16	.3136E-16	.2881E-16	.2646E-16	.2431E-16
8.400	.2232E-16	.2050E-16	.1882E-16	.1728E-16	.1587E-16	.1457E-16	.1337E-16	.1227E-16	.1126E-16	.1033E-16
8.500	.9480E-17	.8697E-17	.7978E-17	.7317E-17	.6711E-17	.6154E-17	.5643E-17	.5174E-17	.4744E-17	.4348E-17
8.600	.3986E-17	.3653E-17	.3348E-17	.3068E-17	.2811E-17	.2575E-17	.2359E-17	.2161E-17	.1979E-17	.1812E-17
8.700	.1659E-17	.1519E-17	.1391E-17	.1273E-17	.1166E-17	.1067E-17	.9763E-18	.8933E-18	.8174E-18	.7478E-18
8.800	.6841E-18	.6257E-18	.5723E-18	.5234E-18	.4786E-18	.4376E-18	.4001E-18	.3657E-18	.3343E-18	.3055E-18
8.900	.2792E-18	.2552E-18	.2331E-18	.2130E-18	.1946E-18	.1777E-18	.1623E-18	.1483E-18	.1354E-18	.1236E-18
9.000	.1129E-18	.1030E-18	.9404E-19	.8584E-19	.7834E-19	.7148E-19	.6523E-19	.5951E-19	.5429E-19	.4952E-19
9.100	.4517E-19	.4119E-19	.3756E-19	.3425E-19	.3123E-19	.2847E-19	.2595E-19	.2365E-19	.2155E-19	.1964E-19
9.200	.1790E-19	.1631E-19	.1486E-19	.1353E-19	.1232E-19	.1122E-19	.1022E-19	.9307E-20	.8474E-20	.7714E-20
9.300	.7022E-20	.6392E-20	.5817E-20	.5294E-20	.4817E-20	.4382E-20	.3987E-20	.3627E-20	.3299E-20	.3000E-20
9.400	.2728E-20	.2481E-20	.2255E-20	.2050E-20	.1864E-20	.1694E-20	.1540E-20	.1399E-20	.1271E-20	.1155E-20
9.500	.1049E-20	.9533E-21	.8659E-21	.7864E-21	.7142E-21	.6485E-21	.5888E-21	.5345E-21	.4852E-21	.4404E-21
9.600	.3997E-21	.3627E-21	.3292E-21	.2986E-21	.2709E-21	.2458E-21	.2229E-21	.2022E-21	.1834E-21	.1663E-21
9.700	.1507E-21	.1367E-21	.1239E-21	.1123E-21	.1018E-21	.9223E-22	.8358E-22	.7573E-22	.6861E-22	.6215E-22
9.800	.5629E-22	.5098E-22	.4617E-22	.4181E-22	.3786E-22	.3427E-22	.3102E-22	.2808E-22	.2542E-22	.2300E-22
9.900	.2081E-22	.1883E-22	.1704E-22	.1541E-22	.1394E-22	.1261E-22	.1140E-22	.1031E-22	.9323E-23	.8429E-23
10.00	.7620E-23	.6888E-23	.6225E-23	.5626E-23	.5084E-23	.4593E-23	.4150E-23	.3749E-23	.3386E-23	.3058E-23

Notes: (1) E-01 should be read as $\times 10^{-1}$; E-02 should be read as $\times 10^{-2}$, and so on.

(2) This table lists $Q(x)$ for x in the range of 0 to 10 in the increments of 0.01. To find $Q(5.36)$, for example, look up the row starting with $x = 5.3$. The sixth entry in this row (under 0.06) is the desired value 0.4161×10^{-7}.

SOLUTIONS

P.1 Solution

If the linear block code corrects all 1-bit and 2-bit error patterns but corrects none of the error patterns with more than two errors, the probability of message error can be stated as

$$P_m = \sum_{k=3}^{24} \binom{24}{k} p^k (1-p)^{24-k} = \sum_{k=3}^{24} \binom{24}{k} (10^{-3})^k (1-10^{-3})^{24-k}$$

To find this sum, we apply the Mathematica code

```
In[82]:= Sum[Binomial[24, k] * 0.001^k * (1 - 0.001)^(24-k), {k, 3, 24}]

Out[82]= 1.99238 × 10^-6
```

That is, $P_m \approx 1.99\times10^{-3} \approx 0.2\%$.

P.2 Solution

At first, the uncoded symbol error probability is

$$p_u = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) = Q\left(\sqrt{2\times 10}\right) = Q(4.47)$$

Referring to the Q function table, $Q(4.47) = 0.3911\times10^{-5}$ or, equivalently, 3.91×10^{-6}. The corresponding probability of message error is computed as

$$P_m^u = 1-\left(1-3.91\times10^{-6}\right)^{12} = 4.69\times10^{-5}$$

For the (24,12) code, the code rate is 1/2. Thus, the data rate is double the uncoded rate, or the E_c/N_0 is 3 dB less than the E_b/N_0, giving E_c/N_0 = 7 dB = 5.01. The coded symbol error probability is then

$$p_c = Q\left(\sqrt{\frac{2E_c}{N_0}}\right) = Q\left(\sqrt{2\times 5.01}\right) = Q(3.17)$$

Referring to the Q function table, $Q(3.17) = 0.762\times10^{-3}$ or 7.62×10^{-4}. The corresponding probability of message error is

$$P_m^c = \sum_{k=3}^{24} \binom{24}{k} p^k (1-p)^{24-k} = \sum_{k=3}^{24} \binom{24}{k} (7.62\times10^{-4})^k (1-7.62\times10^{-4})^{24-k}$$

This summation can be evaluated with the Mathematica code

```
In[96]:= Sum[Binomial[24, k] * (7.62 * 10^-4)^k * (1 - 7.62 * 10^-4)^(24-k), {k, 3, 24}]

Out[96]= 8.84838 × 10^-7
```

That is, $P_m^c \approx 8.85\times10^{-7}$. The performance improvement in message error achieved is calculated to be

$$\text{Performance improvement} = \frac{4.69\times10^{-5}}{8.85\times10^{-7}} = \boxed{53.0}$$

or 17.2 dB.

P.3 Solution

Problem 3.1: First, note that E_b/N_0 = 14 dB = 25.1. For noncoherent BPSK, the uncoded symbol error is

$$p_u = \frac{1}{2} e^{-E_b/2N_0} = \frac{1}{2} e^{-25.1/2} = 1.77\times10^{-6}$$

and corresponds to a message error probability such that

$$P_m^u = 1-\left(1-1.77\times10^{-6}\right)^{12} = 2.12\times10^{-5}$$

For rate-1/2 coding, E_c/N_0 is 3 dB less than E_b/N_0, so E_c/N_0 = 11 dB = 12.6. The coded symbol error probability follows as

$$p_c = \frac{1}{2} e^{-E_c/2N_0} = \frac{1}{2} e^{-12.6/2} = 9.18\times10^{-4}$$

so that

$$P_m^c = \sum_{k=3}^{24} \binom{24}{k} p^k (1-p)^{24-k} = \sum_{k=3}^{24} \binom{24}{k} (9.18\times10^{-4})^k (1-9.18\times10^{-4})^{24-k}$$

```
In[106]:= Sum[Binomial[24, k] * (9.18 * 10^-4)^k * (1 - 9.18 * 10^-4)^(24-k), {k, 3, 24}]

Out[106]= 1.54333 × 10^-6
```

That is, $P_m^c \approx 1.54\times10^{-6}$. Lastly, the performance improvement is

$$\text{Performance improvement} = \frac{2.12\times10^{-5}}{1.54\times10^{-6}} = \boxed{13.8}$$

or 11.4 dB.

Problem 3.2: Now, E_b/N_0 = 10 dB = 10 and

$$p_u = \frac{1}{2} e^{-E_b/2N_0} = \frac{1}{2} e^{-10/2} = 3.37\times10^{-3}$$

$$P_m^u = 1-(1-3.37\times10^{-3})^{12} = 3.97\times10^{-2}$$

As before, we have rate-1/2 coding, so E_c/N_0 is 3 dB less than E_b/N_0, giving E_c/N_0 = 7 dB = 5.01. Thus,

$$p_c = \frac{1}{2} e^{-E_c/2N_0} = \frac{1}{2} e^{-5.01/2} = 4.08\times10^{-2}$$

$$P_m^c = \sum_{k=3}^{24} \binom{24}{k} p^k (1-p)^{24-k} = \sum_{k=3}^{24} \binom{24}{k} (9.18\times10^{-4})^k (1-9.18\times10^{-4})^{24-k}$$

$$\therefore P_m^c \approx \binom{24}{3} (4.08\times10^{-2})^3 (1-4.08\times10^{-2})^{24-3} = 5.73\times10^{-2}$$

Finally, the performance improvement is

$$\text{Performance improvement} = \frac{5.73\times10^{-2}}{3.97\times10^{-2}} = \boxed{1.44}$$

or 1.58 dB.

P.4 ➡ *Solution*

Problem 4.1: Since the rows of ***G*** all have weight four, no linear combination of them can have odd weight. Hence there exists no code word of weight 1, on the other hand, 000011 is a possible code word of weight 2; accordingly, minimum distance d_{min} = 2. The rate of the code is 1/2, and the coding gain is $R_c d_{\min}$ = 1/2 × 2 = 1, or zero dB.

Problem 4.2: We can design a linear block code with d_{min} of at least three. One example is

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Problem 4.3: One suggestion is

$$\mathbf{H} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

P.5 ➡ *Solution*

Since all code words of the new code have odd parity, the all-zero sequence is not a code word and hence the code is not linear. Student B's argument is not valid because for nonlinear codes the minimum Hamming distance and the minimum weight of the code are not the same. Although the minimum weight of the code is 1, the minimum Hamming distance is actually equal to 2.

P.6 ➡ *Solution*

Problem 6.1: This is a nonlinear code since the all-zero sequence is not a code word.

Problem 6.2: There are *Binomial*(6, 3) = 20 code words, hence the rate is $R = (1/6) \times log_2\, 20 = 0.720$. Since all code words have weight equal to 3, no two code words can have a distance of 1. On the other hand, 111000 and 011100 have a distance of 2, hence $d_{min} = 2$.

Problem 6.3: The code can detect $d_{min} - 1 = 1$ error.

Problem 6.4: The probability of an undetected error is the probability of receiving another code word. If 111000 is transmitted there exist 9 code words that are at distance 2 from it and 9 code words that are at distance 4 from it. There is a single code word that is at distance 6 from it. The probability of receiving these code words is the probability of an undetected error, namely

$$P_u = 9p^2(1-p)^4 + 9p^4(1-p)^2 + p^6$$

Problem 6.5: $\mathcal{C}_1$ must contain all code words of $\mathcal{C}$ and all linear combinations of them. Since for each code word in the original code there is another code word at distance 2 from it, all sequences of weight 2 have to be code words. With similar reasoning all sequences of weight 4 and the sequence of weight 6 are also code words. From the inclusion of sequences of sequences of weight 2 and 3, we conclude that all sequences of weights 1 and 5 should also be included. Hence $\mathcal{C}_1$ must be the set of all possible sequences of length 6.

P.7 ➡ *Solution*

Problem 7.1: To find the code words of the code, we must determine the matrix product between the vector of each possible 4-bit message and the generator matrix. For the message 0 0 0 1, for example, the code word is 1 1 0 0 0 0 1, as shown.

In[129]:= $\{0, 0, 0, 1\} . \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$

Out[129]= $\{1, 1, 0, 0, 0, 0, 1\}$

For an entry 0 0 1 1, the code word is {1, 1 + 1, 1, 0, 0, 1, 1} = {1, 0, 1, 0, 0, 1, 1}, as shown.

In[131]:= $\{0, 0, 1, 1\} . \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$

Out[131]= $\{1, 2, 1, 0, 0, 1, 1\}$

The full code word list is shown in continuation. The reader is challenged to write a Mathematica or MATLAB code that automates the process.

Messages	Code words
0000	0000000
0001	1100001
0010	0110010
0011	1010011
0100	1010100
0101	1010100
0110	0110101
0111	1100110
1000	0000111
1001	1111000
1010	0011001
1011	1001010
1100	0101011
1101	1001101
1110	0011110
1111	1111111

Problem 7.2: The parity-check matrix is such that, for each $(k \times n)$ generator matrix $\boldsymbol{G}$, there must be an $(n - k) \times n$ matrix $\boldsymbol{H}$ given by

$$\mathbf{H} = \left[\mathbf{I}_{n-k} \mid \mathbf{P}^T\right]$$

Here, $\boldsymbol{I}_{n-k}$ is the $(n - k) \times (n - k)$ identity matrix and $\boldsymbol{P}^T$ is the transpose of the parity array portion of the generator matrix. For the code at hand, $\boldsymbol{P}$ can be gleaned from the first three columns of the given matrix $\boldsymbol{G}$; that is,

$$\mathbf{G}=\begin{bmatrix}1&1&1&1&0&0&0\\1&0&1&0&1&0&0\\0&1&1&0&0&1&0\\1&1&0&0&0&0&1\end{bmatrix}\rightarrow\mathbf{P}=\begin{bmatrix}1&1&1\\1&0&1\\0&1&1\\1&1&0\end{bmatrix}$$

Transposing,

$$\mathbf{P}^T=\begin{bmatrix}1&1&0&1\\1&0&1&1\\1&1&1&0\end{bmatrix}$$

so that

$$\mathbf{H}=\left[\mathbf{I}_{n-k}\mid\mathbf{P}^T\right]=\begin{bmatrix}1&0&0&1&1&0&1\\0&1&0&1&0&1&1\\0&0&1&1&1&1&0\end{bmatrix}$$

Problem 7.3: To determine whether the code word ***r*** = 1101101 belongs to the code word set, we may compute the syndrome ***S***, which is given by

$$\mathbf{S}=\mathbf{r}\mathbf{H}^T=[1\;1\;0\;1\;1\;0\;1]\begin{bmatrix}1&0&0&1&1&0&1\\0&1&0&1&0&1&1\\0&0&1&1&1&1&0\end{bmatrix}^T=[0\;1\;0]$$

Since the syndrome is not the zero vector, we conclude that 1101101 does *not* belong to the code word set of the code at hand. We can verify this by noting that 1101101 indeed does not occur in the code word set listed in part 1.

Problem 7.4: The error-correcting capability of the code is given by $t = (d_{min} - 1)/2$, where d_{min} is the minimum distance. The minimum distance, in turn, is defined by the minimum number of 1's in an individual code word that constitutes the code word set, ruling out the all-zero sequence. Referring to the code word set given in part 1, we see that the minimum number of 1's a code word obtained in the current problem is 3. Thus, $d_{min} = 3$ and the error-correcting capability is determined as

$$t=\left\lfloor\frac{d_{\min}-1}{2}\right\rfloor=\left\lfloor\frac{3-1}{2}\right\rfloor=\boxed{1}$$

Problem 7.5: The error-correcting capability m is expressed as

$$m=d_{\min}-1=3-1=\boxed{2}$$

P.8 ➡ *Solution*

Problem 8.1: In general, the generator matrix for a systematic (n,k) linear block code can be expressed as

$$\mathbf{G}=\left[\mathbf{P}\mid\mathbf{I}_k\right]$$

where ***P*** is the parity array portion of the generator matrix p_{ij} = (0 or 1), and $\boldsymbol{I_k}$ is the $k \times k$ identity matrix. In the present case, the first column of the generator matrix can be found by noting that first parity bit has the form $1m_1 + 1m_2 + 0m_3 + 1m_4 + 1m_5$, so

$$\mathbf{G}=\begin{bmatrix}1&\\1&\\0&\ldots\\1&\\1&\end{bmatrix}$$

In a similar manner, the second parity bit can be stated as $1m_1 + 0m_2 + 1m_3 + 1m_4 + 1m_5$, so the second column of ***G*** is written as follows,

$$\mathbf{G} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1\ldots \\ 1 & 1 \\ 1 & 1 \end{bmatrix}$$

Proceeding similarly with the remainder of the code word, the generator matrix is found to be

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Problems 8.2 and 8.3: The parity-check matrix is such that, for each ($k \times n$) generator matrix $\boldsymbol{G}$, there exists an $(n-k) \times n$ matrix $\boldsymbol{H}$ given by

$$\mathbf{H} = \left[\mathbf{I}_{n-k} \mid \mathbf{P}^T\right]$$

Here, $\boldsymbol{I}_{n-k}$ is the $(n-k) \times (n-k)$ identity matrix and $\boldsymbol{P}^T$ is the transpose of the parity array portion of the generator matrix. Noting that the $k \times n$ generator matrix obtained in part 1 has 5 rows and 9 columns, it is easy to see that $k = 5$ and $n = 9$. Thus, $\boldsymbol{I}_{n-k} = \boldsymbol{I}_4$. Also, the parity array portion $\boldsymbol{P}$ of the generator matrix can be extracted from $\boldsymbol{G}$,

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \rightarrow \mathbf{P} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Transposing,

$$\mathbf{P}^T = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

so that

$$\mathbf{H} = \left[\mathbf{I}_{n-k} \mid \mathbf{P}^T\right] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Inspecting the columns of $\boldsymbol{P}^T$, it is apparent that $d_{min} = 3$.

P.9 ➡ *Solution*

Problem 9.1: The first four columns of the generator matrix can be found with reference to the parity-check equations. Since $p_1 = 1m_1 + 1m_2 + 0m_3 + 1m_4$ is the first parity-check equation, the first column of $\boldsymbol{G}$ will be 1 1 0 1, as shown. Likewise, the second parity-check equation is $p_2 = 1m_1 + 0m_2 + 1m_3 + 1m_4$, so the second column of $\boldsymbol{G}$ will be 1 0 1 1, as highlighted below. We proceed in the same vein with the remaining two parity-check equations. The remaining four columns consist of a 4×4 identity matrix pattern. The generator matrix is shown below.

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

To assemble the parity-check matrix, we place a 4×4 identity matrix pattern in the left half and the transpose of the parity array portion in the right half, as shown.

$$\mathbf{H} = \left[\mathbf{I}_4 \,|\, \mathbf{P}^T\right] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Problem 9.2: Since the parity-check equations are assembled with four message digits m_i, the minimum distance d_{min} = 4. The corresponding error-correcting capability is

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor = \left\lfloor \frac{4-1}{2} \right\rfloor = \boxed{1}$$

Problem 9.3: For $\boldsymbol{r_1}$ = (1 0 1 0 1 0 1 0) to be a code word, the syndrome $\boldsymbol{S}$ = $\boldsymbol{r_1 H^T}$ must yield the zero vector.

In[238]:= $\{1, 0, 1, 0, 1, 0, 1, 0\} . \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$

Out[238]= {2, 2, 3, 1}

Clearly, $\boldsymbol{S}$ = (1 + 1, 1 + 1, 1 + 1 + 1, 1) = (0,0,1,1); therefore, $\boldsymbol{r_1}$ is not a code word in this system.

Problem 9.4: Using the same reasoning as in the previous part, $\boldsymbol{r_2}$ = (0 1 0 1 1 1 0 0) will be a code word of the present system if the syndrome $\boldsymbol{S}$ = $\boldsymbol{r_2 H^T}$ is found to be the zero vector.

In[240]:= $\{0, 1, 0, 1, 1, 1, 0, 0\} . \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$

Out[240]= {2, 2, 2, 2}

That is, $\boldsymbol{S}$ = (1 + 1, 1 + 1, 1 + 1, 1 + 1) = (0,0,0,0). The syndrome is the zero vector, hence r_2 is a code word in this system.

P.10 ➡ *Solution*

Problem 10.1: A generator polynomial $g(X)$ of an *(n,k)* cyclic code is a factor of $X^n - 1$; that is, $X^n + 1 = g(X)h(X)$. Take the first polynomial, $g(X) = 1 + X^3 + X^4$. In this case, *n* – *k* = 4 so, for *k* = 1, 2, 3, we have *n* = 5, 6, 7. With *n* = 5, we divide $X^5 + 1$ by the given polynomial; one way to go is to combine Mathematica's *PolynomialQuotientRemainder* and *PolynomialMod* commands, with the latter set to 2 for modulo-2 division,

```
PolynomialMod[PolynomialQuotientRemainder[x^5 + 1, x^4 + x^3 + 1, x], 2]
Out[135]= {1 + x, x + x^3}
```

The remainder is different from zero, so a cyclic code *cannot* be generated with this polynomial when *n* = 5. Proceeding with *n* = 6, we divide $X^6 + 1$ by the given polynomial to obtain

```
In[136]:= PolynomialMod[PolynomialQuotientRemainder[x^6 + 1, x^4 + x^3 + 1, x], 2]
Out[136]= {1 + x + x^2, x + x^2 + x^3}
```

Again, the remainder is not zero, so a cyclic code cannot be generated with this polynomial when *n* = 6. Proceeding with *n* = 7, we divide $X^7 + 1$ by the given polynomial to obtain

```
In[137]:= PolynomialMod[PolynomialQuotientRemainder[x^7 + 1, x^4 + x^3 + 1, x], 2]
Out[137]= {1 + x + x^2 + x^3, x + x^2}
```

The remainder is nonzero, so the polynomial cannot yield a cyclic code with n set to 7 either.

Problem 10.2: The polynomial is now $g(X) = 1 + X^2 + X^4$. In this case, $n - k = 4$ and, for $k = 1, 2, 3$, we have $n = 5, 6, 7$ respectively. First, with n set to 5, we divide $X^5 + 1$ by the polynomial in question to obtain

```
In[138]:= PolynomialMod[PolynomialQuotientRemainder[x^5 + 1, x^4 + x^2 + 1, x], 2]
Out[138]= {x, 1 + x + x^3}
```

The remainder is different from zero, so a cyclic code cannot be generated with the given polynomial when $n = 5$. Next, we set $n = 6$ and divide the polynomial by $X^6 + 1$, giving

```
In[139]:= PolynomialMod[PolynomialQuotientRemainder[x^6 + 1, x^4 + x^2 + 1, x], 2]
Out[139]= {1 + x^2, 0}
```

The remainder is zero, which indicates that the polynomial can produce a cyclic code with n set to 6. Noting that $n - k = 4$, it follows that $k = 2$ and the code thus formed is $(n, k) = (6, 2)$.

Lastly, we set $n = 7$ and divide the polynomial by $X^7 + 1$, which leads to

```
In[140]:= PolynomialMod[PolynomialQuotientRemainder[x^7 + 1, x^4 + x^2 + 1, x], 2]
Out[140]= {x + x^3, 1 + x}
```

The remainder is different from zero, so a cyclic code cannot be formed with $n = 7$.

Problem 10.3: The polynomial is now $g(X) = 1 + X + X^2 + X^4$. In this case, $n - k = 4$ and, for $k = 1, 2, 3$, we have $n = 5, 6, 7$ respectively. First, with n set to 5, we divide $X^5 + 1$ by the polynomial in question to obtain

```
In[141]:= PolynomialMod[PolynomialQuotientRemainder[x^5 + 1, x^4 + x^2 + x + 1, x], 2]
Out[141]= {x, 1 + x + x^2 + x^3}
```

The remainder is nonzero, so a cyclic code cannot be formed with $n = 5$. Next, we set $n = 6$ and divide the polynomial by $X^6 + 1$, giving

```
In[142]:= PolynomialMod[PolynomialQuotientRemainder[x^6 + 1, x^4 + x^2 + x + 1, x], 2]
Out[142]= {1 + x^2, x + x^3}
```

Again, a cyclic code cannot be formed with $n = 6$. Lastly, with $n = 7$, we perform the usual division to obtain

```
In[143]:= PolynomialMod[PolynomialQuotientRemainder[x^7 + 1, x^4 + x^2 + x + 1, x], 2]
Out[143]= {1 + x + x^3, 0}
```

The remainder is zero, which indicates that the polynomial can produce a cyclic code with n set to 7. Noting that $n - k = 4$, it follows that $k = 3$ and the code thus formed is $(n, k) = (7, 3)$ in nature.

P.11 ➡ *Solution*

The message $m = 1\ \ 0\ \ 1$ can be represented by the polynomial $m(X) = 1 + 0 \times X + 1 \times X^2 = 1 + X^2$. From the length of the generator g, we may write $n - k = 4$; but the code word length $k = 3$, so $n = 7$. Upshifting the message $m(X)$ brings to

$$X^{n-k}m(X) = X^4\left(1 + X^2\right) = X^4 + X^6$$

To establish the code word, we need the remainder $r(X)$, which is related to other components of the algebraic encoding process by

$$X^{n-k}m(X) = q(X)g(X) + r(X)$$

Next, we divide the upshifted $m(X)$ by the generator $g(X) = 1 + X + X^2 + X^4$ to obtain

```
In[236]:= PolynomialMod[PolynomialQuotientRemainder[x^6 + x^4, x^4 + x^2 + x + 1, x], 2]
Out[236]= {x^2, x^2 + x^3}
```

We proceed to compute the desired code word,

$$r(X) + X^{n-k} m(X) = (X^2 + X^3) + X^4 + X^6$$
$$\therefore r(X) + X^{n-k} m(X) = 0011101$$

The bits in red are the parity part of the string, while the bits in blue are the message part of the string.

P.12 ➡ *Solution*

Problem 12.1: We first multiply the message polynomial by $X^{n-k} = X^{10}$, giving

$$X^{10} m(X) = X^{10} \times (1 + X^2 + X^4) = X^{10} + X^{12} + X^{14}$$

We proceed to divide this polynomial by the generator $\boldsymbol{g}(X) = 1 + X + X^2 + X^5 + X^8 + X^{10}$,

```
In[196]:= PolynomialMod[PolynomialQuotientRemainder[x^14 + x^12 + x^10, x^10 + x^8 + x^5 + x^2 + x + 1, x], 2]
Out[196]= {1 + x^4, 1 + x + x^2 + x^4 + x^6 + x^8 + x^9}
```

As can be seen, the remainder is $r(X) = 1 + X + X^2 + X^4 + X^6 + X^8 + X^9$. Accordingly, the code word we're looking for is

$$r(x) + X^{n-k} m(X) = (1 + X + X^2 + X^4 + X^6 + X^8 + X^9) + X^{10} + X^{12} + X^{14}$$
$$\therefore r(x) + X^{n-k} m(X) = 111010101110101$$

The bits in red are the parity part of the code word, while the bits in blue are the message part of the code word.

Problem 12.2: The basic test is to divide $\boldsymbol{V}(X)$ by the generator $\boldsymbol{g}(X)$; if the remainder $\boldsymbol{r}(X)$ is zero, $\boldsymbol{V}(X)$ is a code polynomial in the system in question. Appealing to Mathematica, we type the code

```
In[197]:= PolynomialMod[PolynomialQuotientRemainder[x^14 + x^8 + x^6 + x^4 + 1, x^10 + x^8 + x^5 + x^2 + x + 1, x], 2]
Out[197]= {1 + x^2 + x^4, x + x^3 + x^4 + x^7 + x^9}
```

Since the remainder $\boldsymbol{r}(X) = 1 + X^2 + X^4$, $\boldsymbol{V}(X)$ is not a code word in the system under consideration.

P.13 ➡ *Solution*

The standard array of a code such as the present one will have $2^k = 2^3 =$ 8 columns and $2^{n-k} = 2^{7-3} = 16$ rows, totaling 16 × 8 = 128 entries. The number of single- and double-error patterns are, respectively,

$$\text{Single-error patterns} = \binom{7}{1} = 7$$

$$\text{Double-error patterns} = \binom{7}{2} = 21$$

With 16 – 1 = 15 available rows, the coset leaders allow for the correction of all 7 single-error patterns, leaving us with 15 – 7 = 8 rows for the correction of double-error patterns. Since 21 > 8, the code can correct only 8/21 = 38% of the double-error patterns, and we conclude that the (7,3) code is *not* a perfect code.

Now, take the (7,4) code. The standard array of this code will have $2^4 =$ 16 columns and $2^{7-4} = 8$ rows, totaling 8 × 16 = 128 entries. The number of single-error patterns is *Binomial*(7,1) = 7. With 8 coset leaders (i.e., 7 rows), we can correct all single-error patterns and nothing more. It follows that the (7,4) code is a perfect code.

Now, take the (15,11) code. The standard array of this code will have 2^{11} = 2048 columns and $2^{15-11} = 16$ rows, totaling 16 × 2048 = 32,768 entries. The number of single-error patterns is *Binomial*(15,1) = 15. With 16 coset leaders (i.e., 15 rows), we can correct all single-error patterns and nothing more. Therefore, the (15,11) code is a perfect code.

P.14 ➡ *Solution*

Problem 14.1: The parity-check matrix ***H*** can be expressed as

$$\mathbf{H} = \left[\mathbf{I}_{n-k} \mid \mathbf{P}^T \right]$$

Noting that n = 15 and k = 11, the identity matrix component of ***H*** will be 4 × 4 in dimensions. The transpose of the parity array can be easily established with the given ***P***. We ultimately obtain

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Problem 14.2: The standard array is made up of 15-bit strings. Noting that n = 15 and k = 11, we surmise that there are 2^{15-11} = 16 coset leaders, as listed below.

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
0 0 0 0 0 0 0 0 0 0 0 0 0 1 0
0 0 0 0 0 0 0 0 0 0 0 0 1 0 0
0 0 0 0 0 0 0 0 0 0 0 1 0 0 0
0 0 0 0 0 0 0 0 0 0 1 0 0 0 0
0 0 0 0 0 0 0 0 0 1 0 0 0 0 0
0 0 0 0 0 0 0 0 1 0 0 0 0 0 0
0 0 0 0 0 0 0 1 0 0 0 0 0 0 0
0 0 0 0 0 0 1 0 0 0 0 0 0 0 0
0 0 0 0 0 1 0 0 0 0 0 0 0 0 0
0 0 0 0 1 0 0 0 0 0 0 0 0 0 0
0 0 0 1 0 0 0 0 0 0 0 0 0 0 0
0 0 1 0 0 0 0 0 0 0 0 0 0 0 0
0 1 0 0 0 0 0 0 0 0 0 0 0 0 0
1 0 0 0 0 0 0 0 0 0 0 0 0 0 0

The number of single-error patterns is *Binomial*(15,1) = 15. With 16 coset leaders (i.e., 15 rows), we can correct all single-error patterns and nothing more. It follows that the (15,11) code is perfect in nature.

Problem 14.3: To compute the syndrome S, we matrix-multiply the given vector ***r*** by the transpose of the parity-check matrix,

$$\mathbf{S} = \mathbf{r}\mathbf{H}^T = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix} \times \mathbf{H}^T$$

$$\therefore \mathbf{S} = \begin{bmatrix} 0\,1\,1\,0 \end{bmatrix}$$

Since the syndrome is not the zero vector, we conclude that ***r*** is *not* a code word. Mapping the syndrome S = [0 1 1 0] onto the parity-check matrix, we see that this syndrome is found at the eighth column of ***H***.

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Thus, the coset leader resulting in the syndrome [0 1 1 0] is the one that has a 1 at the eighth position of the sequence; the coset leader in question is 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0. The bit error is at the eighth positon, so the correct code word must be 0 1 1 1 1 1 0 1 1 0 1 1 0 1 1.

Problem 14.4: With the knowledge that the maximum error-correcting capability is t_{max} = 1, and inspecting the generator matrix ***G*** = [***P*** | ***I***$_k$], we glean a minimum distance d_{min} = 3.

P.15 ➡ *Solution*

Problem 15.1: Let P_m denote the probability that a word or message is in error. Determining the probability that a word (basically, a 42-bit sequence) will be received in error is calculated as

$$P_m = 1 - (1-p)^{7\times 6} = 1 - \left(1 - 10^{-3}\right)^{42} = \boxed{4.12 \times 10^{-2}}$$

Problem 15.2: Let P_c be the probability that a word is correct, and let P_{cc} be the probability that a character within the word is correct. The probability that a message will be in error, P_m, may be written in terms of P_c as

$$P_m = 1 - P_c \quad \text{(I)}$$

Also, $P_c = P_{cc}^6$. This latter term, P_{cc}, can be stated as

$$P_{cc} = (1-p)^{7\times 3} + \binom{3}{2}(1-p)^{7\times 2}\left[1-(1-p)^7\right]$$

where the first term denotes the probability that each of the 3 repetitions are decoded correctly, while the second denotes the probability that 2 of the 3 repetitions are decoded correctly and 1 is decoded incorrectly; these are the two scenarios in which a majority voting probability approach to 3 repetitions will lead to a correct reception. Substituting in (I) and noting that $p = 10^{-3}$, we get

$$P_m = 1 - P_c = 1 - P_{cc}^6$$

$$\therefore P_m = 1 - \left\{(1-10^{-3})^{21} + \binom{3}{2}(1-10^{-3})^{14}\left[1-(1-10^{-3})^7\right]\right\}^6 = \boxed{8.72\times 10^{-4}}$$

Problem 15.3: In this case, the probability that the message received will be in error can be estimated with the first term of the pertaining binomial expansion, namely

$$P_m \approx \binom{126}{15} p^{15}(1-p)^{111} = \binom{126}{15}(10^{-3})^{15}(1-10^{-3})^{111} = \boxed{9.21\times 10^{-27}}$$

Problem 15.4: First, with E_b/N_0 = 12 dB = 15.8, the channel error probability is established as

$$p = \frac{1}{2}e^{-15.8/2} = 1.85\times 10^{-4}$$

so that, updating the probability found in part 1,

$$P_m = 1-(1-p)^{7\times 6} = 1-(1-1.85\times 10^{-4})^{42} = \boxed{7.74\times 10^{-3}}$$

To update the result of part 2, first note that coding is rate-1/3, because 200% redundancy is introduced. It follows that

$$\frac{E_c}{N_0} = \frac{E_b}{3N_0} = \frac{15.8}{3} = 5.27$$

and

$$p = \frac{1}{2}e^{-5.27/2} = 3.59\times 10^{-2}$$

Finally,

$$P_m = 1 - \left\{(1-0.0359)^{21} + \binom{3}{2}(1-0.0359)^{14}\left[1-(1-0.0359)^7\right]\right\}^6 = \boxed{5.66\times 10^{-1}}$$

To update the result of part 3, we write

$$P_m \approx \binom{126}{15} p^{15}(1-p)^{111} = \binom{126}{15}(0.0359)^{15}(1-0.0359)^{111} = \boxed{3.77\times 10^{-5}}$$

Problem 15.5: Operating a communication system with the symbol error probability fixed regardless of the message redundancy implies that the bit energy to noise density E_b/N_0 must be increased for increased redundancy. Under such conditions we see that the repetition code provides about 16 dB error performance improvement over the uncoded case, and the BCH code provides an enormous improvement over the other two cases. A more realistic comparison of coding capability is one where the system operates with a fixed E_b/N_0. Here we see that the repetition code results in nearly 35 dB of degraded error performance, while the BCH code offers about 7 dB of coding gain compared to the uncoded case. Therefore, a repetition code offers improvement when the received E_b/N_0 is increased (i.e. by increasing transmission power or increasing transmission duration and thus delay). Otherwise, the repetition code causes degradation.

P.16 ➡ *Solution*

Problem 16.1: We first determine the uncoded symbol error probability p_u,

$$P_m^u = 1-(1-p_u)^{36} \approx 36 p_u$$

But the message error probability was given as 10^{-3}, therefore

$$P_m^u \approx 36 p_u = 10^{-3} \rightarrow p_u = \frac{10^{-3}}{36} = 2.78\times 10^{-5}$$

Now, for BFSK modulation the bit energy to noise density ratio can be stated as

$$p_u = \frac{1}{2}e^{-E_b/2N_0} \rightarrow \frac{E_b}{N_0} = -2\ln(2p_u)$$

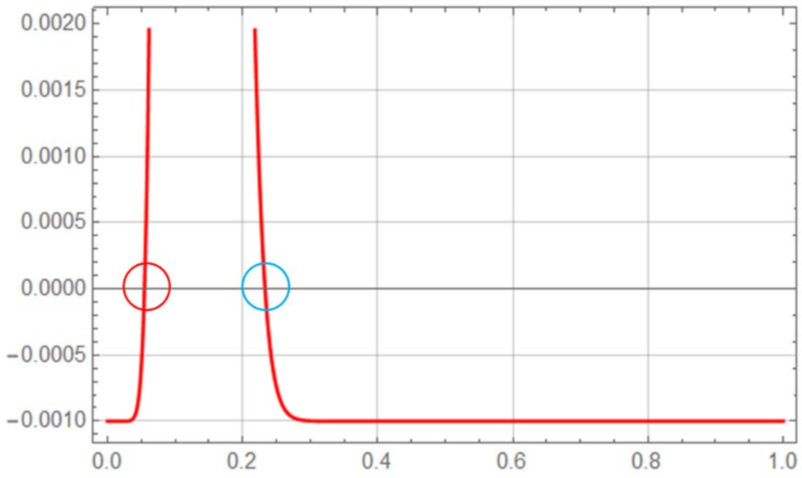
$$\therefore \frac{E_b}{N_0} = -2\ln\left[2\times\left(2.78\times 10^{-5}\right)\right] = 19.6$$

$$\therefore \frac{E_b}{N_0} = 10\log_{10}(19.6) = \boxed{12.9\,\text{dB}}$$

Problem 16.2: Use of a (127,36) code with minimal distance $d_{min} = 31$ can correct $t_{max} = 15$ errors. The probability that a coded message will be in error can be estimated from the greatest term of the pertaining binomial expansion, namely

$$P_m^c \approx \binom{127}{16} p_c^{16}(1-p_c)^{111} = 10^{-3}$$

The expression above is a polynomial equation of high degree and does not lend itself to simple methods of solution. Still, a value of p_c (i.e., a root) can be found by means of Mathematica's *FindRoot* command or MATLAB's *fzero* command. We first plot the equation from $p_c = 0$ to $p_c = 1$ to estimate an initial guess for use with either of these commands.



As can be seen, the equation has a root between 0 and 0.1, as circled in red, and another between 0.2 and 0.3, as circled in blue. The error probability p_c we're looking for is the lower probability, so an initial guess of 0.05 would seem reasonable. We proceed to apply MATLAB's *fzero* command,

```
function y = prob(x)
y = nchoosek(127,16)*x^16*(1-x)^111-0.001;

>>fun = @prob;
x0 = 0.1;
x = fzero(fun,x0)
```

The command returns $p_c = 0.0546$. From the error probability for BFSK modulation, we may write

$$p_u = \frac{1}{2}e^{-E_b/2N_0} \rightarrow \frac{E_b}{N_0} = -2\ln(2p_u)$$

$$\therefore \frac{E_b}{N_0} = -2\ln\left(2\times 0.0546\right) = 4.429 = 6.46\,\text{dB}$$

The corresponding code-bit energy per noise density is

$$\frac{E_c}{N_0} = \frac{127}{36}\frac{E_b}{N_0} = \frac{127}{36}\times 4.43 = 15.6 = \underline{11.9\,\text{dB}}$$

Comparing with the result of part 1, the coding gain is

$$\text{Coding gain} = 12.9 - 11.9 = \boxed{1.0\,\text{dB}}$$

P.17 ➡ *Solution*

Problem 17.1: First, a message m = 1 1 0 1 1 can be represented by the polynomial $m(X) = 1 + X + X^3 + X^4$. Noting that $n - k = 10$ as before, we may write

$$X^{10}m(X) = X^{10}\times\left(1 + X + X^3 + X^4\right) = X^{10} + X^{11} + X^{13} + X^{14}$$

The generator polynomial is $g(X) = 1 + X + X^2 + X^5 + X^8 + X^{10}$. The degree of the generator polynomial is precisely $n - k$; in the present case, n = 14 and k = 4, so $n - k = 10 = deg(g(X))$. We proceed to determine the parity polynomial $p(X)$, which is the remainder of the division of the upshifted $m(X)$ by the generator $g(X)$; that is,

```
In[198]:= PolynomialMod[PolynomialQuotientRemainder[x^14 + x^13 + x^11 + x^10, x^10 + x^8 + x^5 + x^2 + x + 1, x], 2]
Out[198]= {x^2 + x^3 + x^4, x^2 + x^4 + x^6 + x^7 + x^8 + x^9}
```

Clearly, $p(X) = X^9 + X^8 + X^7 + X^6 + X^4 + X^2$. The code word $U(X)$ is calculated to be

$$U(X) = X^{n-k}m(X) + p(X)$$

$$\therefore U(X) = X^2 + X^4 + X^6 + X^7 + X^8 + X^9 + X^{10} + X^{11} + X^{13} + X^{14}$$

$$\boxed{U(X) = 001010111111011}$$

As a safety check, dividing the code word polynomial $U(X)$ by the generator $g(X)$ should yield the same quotient $q(X) = X^2 + X^3 + X^4$ (see code snippet above) obtained in the division of the upshifted $m(X)$ by $g(X)$; also, the remainder must be zero. With these notes in mind, we type the code

```
In[199]:= PolynomialMod[PolynomialQuotientRemainder[x^14 + x^13 + x^11 + x^10 + x^9 + x^8 + x^7 + x^6 + x^4 + x^2,
    x^10 + x^8 + x^5 + x^2 + x + 1, x], 2]
Out[199]= {x^2 + x^3 + x^4, 0}
```

The results match our expectations.

Problem 17.2: The corrupted version $Z(X)$ of a polynomial $U(X)$ can be stated as

$$Z(X) = U(X) + e(X)$$

In the present case,

$$Z(X) = \left(X^2 + X^4 + X^6 + X^7 + \cancel{X^8} + X^9 + \cancel{X^{10}} + X^{11} + \cancel{X^{13}} + X^{14}\right)$$

$$+\left(\cancel{X^8} + \cancel{X^{10}} + \cancel{X^{13}}\right)$$

$$\boxed{Z(X) = X^2 + X^4 + X^6 + X^7 + X^9 + X^{11} + X^{14}}$$

Problem 17.3: To find the syndrome $S(X)$, first note that the code polynomials in question are related by

$$Z(X) = q(X)g(X) + S(X)$$

or, equivalently,

$$\frac{Z(X)}{g(X)} = q(X) + \frac{S(X)}{g(X)}$$

As can be seen, the syndrome polynomial $S(X)$ is the remainder of the division of received polynomial $Z(X)$ by the generator $g(X)$; that is,

```
In[201]:= PolynomialMod[PolynomialQuotientRemainder[x^14 + x^11 + x^9 + x^7 + x^6 + x^4 + x^2, x^10 + x^8 + x^5 + x^2 + x + 1, x],
  2]
Out[201]= {1 + x + x^2 + x^4, 1 + x^4 + x^6 + x^8 + x^9}
```

Thus,

$$\boxed{S(X) = 1 + X^4 + X^6 + X^8 + X^9}$$

Problem 17.4: Noting that

$$\frac{e(X)}{g(X)} = m(X) + q(X) + \frac{S(X)}{g(X)}$$

another way to obtain the syndrome $S(X)$ is to divide the error pattern polynomial $e(X) = X^8 + X^{10} + X^{13}$ by the generator $g(X)$; indeed,

```
In[202]:= PolynomialMod[PolynomialQuotientRemainder[x^13 + x^10 + x^8, x^10 + x^8 + x^5 + x^2 + x + 1, x], 2]
Out[202]= {1 + x + x^3, 1 + x^4 + x^6 + x^8 + x^9}
```

The remainder $S(X) = 1 + X^4 + X^6 + X^8 + X^9$ matches the result of the previous part.

Problem 17.5: A code word $U(X)$ is such that $U(X) = m(X)g(X)$, where $m(X)$ and $g(X)$ are the message and generator polynomials, respectively. The received polynomial $Z(X)$ equals the code word $U(X)$ plus the error pattern $e(X)$,

$$Z(X) = U(X) + e(X) \quad \text{(I)}$$

Equivalently, the received polynomial $Z(X)$ can be stated as

$$Z(X) = q(X)g(X) + S(X) \quad \text{(II)}$$

where $g(X)$ is the generator polynomial, $q(X)$ is the quotient of $Z(X)$ and $g(X)$, and $S(X)$ is the syndrome polynomial. Combining the definition of $U(X)$ and the two foregoing equations, we ultimately find

$$e(X) = \left[m(X) + q(X)\right]g(X) + S(X) \quad \text{(III)}$$

From (II) and (III), it is apparent that the syndrome $S(X)$ obtained as the remainder of $Z(X)$ modulo $g(X)$ is exactly the same polynomial as the remainder or $e(X)$ modulo $g(X)$.

Problem 17.6: A standard array for a (15,5) code has 2^5 columns and $2^{15-5} = 2^{10}$ rows, totaling $2^5 \times 2^{10} = 2^{15}$ entries. Thus, of the $2^{10} = 1024$ rows we calculate, the number of rows needed for single, double, etc. errors is as follows.

Single errors	Double errors	Triple errors	Quadruple errors
$\binom{15}{1} = 15$	$\binom{15}{2} = 105$	$\binom{15}{3} = 455$	$\binom{15}{4} = 1365$

With 15 rows for correction of single errors, we are left with 1023 – 15 = 1008 rows for higher-order errors. With 105 rows for correction of double errors, we are left with 1008 – 105 = 903 rows for correction of higher-order errors. With 455 triple errors, we are left with 903 – 455 = 448 rows for calculation of higher-order errors. We have 448 rows remaining, but correction of quadruple errors requires 1365 rows; we conclude that the code in question is not perfect, in that is can account for only 448/1365 ≈ 32.8% of quadruple errors.

Problem 17.7: The minimum distance is related to error correction α and the erasure correction γ by the simple expression

$$d_{\min} \geq 2\alpha + \gamma + 1$$

Taking a minimum error-correcting capability $t = 2$, d_{min} is calculated to be

$$d_{\min} = 2t + 1 = 2 \times 2 + 1 = 7$$

If the cyclic code is to simultaneously correct two erasures and still perform error correction, we must have $\gamma = 2$, giving

$$d_{\min} \geq 2\alpha + \gamma + 1 \rightarrow 7 \geq 2\alpha + 2 + 1$$

$$\therefore 7 \geq 2\alpha + 3$$
$$\therefore \alpha \leq 2$$

With $\alpha = 2$, the code must be implemented by sacrificing one unit of error-correction capability. The result is a double-error correcting, double-erasure correcting code.

REFERENCES

- PROAKIS, J.G. and SALEHI, M. (2008). *Digital Communications*. 5th edition. New York: McGraw-Hill.
- SKLAR, B. (2001). *Digital Communications*. 2nd edition. Upper Saddle River: Prentice-Hall.