1 Exercise 2.3

1.1 Question

Let m be a positive integer. If m is not Prime, Prove the set $\{1, 2, \ldots, m-1\}$ is not a group under modulo-m multiplication.

1.2 Answer

If a group modulus is not Prime then there exists an elements a and b such that $a * b = m = 0$ which is not in the group.

2 Exercise 2.4

2.1 Question

Construct the field GF(11) with modulo 11 addition and multiplication. Find all the primitive elements, and determine the order of the remaining elements.

2.2 Answer

1 is a primitive element of the group and its order is 12
2 is a primitive element of the group and its order is 10
3 is not a primitive element of the group and its order is 5
4 is not a primitive element of the group and its order is 5
5 is not a primitive element of the group and its order is 5
6 is a primitive element of the group and its order is 10
7 is a primitive element of the group and its order is 10
8 is a primitive element of the group and its order is 10
9 is not primitive element of the group and its order is 5
10 is not a primitive element of the group and its order is 2

3 Exercise 2.6

3.1 Question

Consider the integer group $G = \{0, 1, 2, \ldots, 31\}$ under modulo-32 addition. Show that $H = \{0, 4, 8, 12, 16, 20, 24, 28\}$ forms a subgroup of G. Decompose G into cossets with respect to H (or modulo H).

3.2 Answer

All elements of H are a multiple of 4. Any multiple of 4 + another multiple of 4 modulo a multiple of 4 equals a multiple of 4. The cossets of G

are $H = \{0, 4, 8, 12, 16, 20, 24, 28\}$ $H + 1 = \{1, 5, 9, 13, 17, 21, 25, 29\}$ $H + 2 = \{2, 6, 10, 14, 18, 22, 26, 30\}$ $H + 3 = \{3, 7, 11, 15, 19, 23, 27, 31\}$

4 Exercise 2.7

4.1 Question

let λ be a characteristic of a Galois field GF(q). Let 1 be the unit element of GF(q). Show that the sums $\{1, \sum_{i=1}^{2} 1, \sum_{i=1}^{3} 1, \ldots, \sum_{i=1}^{\lambda-1} 1, \sum_{i=1}^{\lambda} 1\}$ form a subfield of GF(q)

4.2 Answer

The characteristic of a Finite field is equal to the modulo of the finite field. as such the given sums contained all of the field.

5 Exercise 2.8

5.1 Question

Prove that every finite field has a Primitive element

5.2 Answer

A primitive element is an element in the field that is also generator of the multiplicative group. Meaning its order is equal to that of the group.

Let n be the lowest number such that $a^n = 1$ for all a in the group. n is less than or equal to the order of the group. But the polynomial $a^n - 1$ has at most n distinct roots, and every non zero element of the field is a root of this polynomial. So n must be greater than or equal to the order of the group. Therefore n is equal to the order of the group.

Let k is the highest order of any element in the group, and its the order of an element b. And let c be an element of order ℓ. The order of bc will be the lowest common multiple of k and ℓ. By assumption this cannot exceed k and must equal k and therefore ℓ divides k.

Therefore $a^k = 1$ for all elements a in the group, and by the above $k = n$. And b is a primitive element.

6 Exercise 2.10

6.1 Question

Show that $X^5 + X^3 + 1$ is irreducible over GF(2)

6.2 Answer

The above polynomial has a trailing constant of 1 in the group GF(2). In order to have a polynomial with a trailing one that is the factor of two polynomial, both of the two must have 1 as the trailing constant. Next only way to get X^5 is with two polynomials of either a^1 and a^4 or a^2 and a^3. We can ignore the $X^1 * X^4$ because we also need X^3. Now list out all the degree two polynomials. $X^2, X^2+1, X^2+X^1,\ X^2+X^1+1$. First we can rule out all even termed and ones with out a trialling 1. That leaves X^2+X^1+1 to check if this polynomial times any polynomial of degree 3 works use long division. The result is $X^5+X^3+1/X^2+a+1 = a^3+a^2$. With a remainder of $a+1$, because the remainder is not 0 then X^5+X^3+1 cannot be factored.

7 Exercise 2.11

7.1 Question

Find all the irreducible polynomials of degree 5 over GF(2)

7.2 Answer

First get a list of all the polynomials of degree 5 and have a trailing one that leaves 16 possible polynomials: $1a^5+1a^4+1a^3+1a^2+1a^1+1E$
$1a^5+1a^4+1a^3+1a^2+0a^1+1IB1IB2$
$1a^5+1a^4+1a^3+0a^2+1a^1+1IB1IB2$
$1a^5+1a^4+1a^3+0a^2+0a^1+1E$
$1a^5+1a^4+0a^3+1a^2+1a^1+1IB1IB2$
$1a^5+1a^4+0a^3+1a^2+0a^1+1E$
$1a^5+1a^4+0a^3+0a^2+1a^1+1E$
$1a^5+1a^4+0a^3+0a^2+0a^1+1IB1IB2$
$1a^5+0a^4+1a^3+1a^2+1a^1+1IB1IB2$
$1a^5+0a^4+1a^3+1a^2+0a^1+1E$
$1a^5+0a^4+1a^3+0a^2+1a^1+1E$
$1a^5+0a^4+1a^3+0a^2+0a^1+1 = IB1IB2$
$1a^5+0a^4+0a^3+1a^2+1a^1+1E$
$1a^5+0a^4+0a^3+1a^2+0a^1+1IB1IB2$
$1a^5+0a^4+0a^3+0a^2+1a^1+1 = (a^3+a^2+1)(a^2+a+1)IB1$
$1a^5+0a^4+0a^3+0a^2+0a^1+1E$
Next wright an E next to all polynomials with even terms these are reducible, there are 8 even termed polynomials. Next all polynomials are of degree 5, in order to get a degree 5 with polynomials of a lesser degree then you need to combine either 2 and 3 or 1 and 4. By dividing by all the degree 2 polynomials you can eliminate the degree 3's, and same with 1 and 4. First by elimination above the only degree 1 polynomial that will work is $a+1$. Now divide all the remaining polynomials above by $a+1$. None of the remainders are 0 and so all the remaining polynomials are irreducible by 1 degree polynomials (IB1). Next

list out all the 2 degree polynomials with a trailing one: $1a^2 + 1a^1 + 1$
$1a^2 + 1$

8 Exercise 2.13

8.1 Question

Construct a table for the field $GF(2^3)$ based on the primitive polynomial $p(X) = 1 + X^2 + X^3$. Display the power, polynomial, and vector representations of each element. Determine the order of each element.

8.2 Answer

power	0	a^1	a^2	a^3	a^4	a^5	a^6	a^7
polynomial	$a^3 + a^2 + 1$	a^1	a^2	$a^2 + 1$	$a^2 + a^1$	a	$a^2 + a^1$	1
vector	1101	0010	0100	0101	0111	0010	0110	0001

9 Exercise 2.16

9.1 Question

Prove Theorem 2.21

9.2 Answer

If e_1 and e_2 are identity's, then $e_1 = e_1 * e_2 = e_2$

10 Exercise 2.19

10.1 Question

Let a be a primitive element in $GF(2^4)$. Use table 2.8 to solve the following equations for X, Y, and Z: $X + a5Y + Z = a^7$, $X + aY + a^7Z$, $a^2X + Y + a^6Z$.

10.2 Answer

The above is true for the set of variables a, X, Y, Z $\{z4, z4^3 + z4^2 + z4 + 1, z4^3 + 1, z4^2 + z4 + 1\}$.

11 Exercise 2.23

11.1 Question

Prove the set of polynomials over GF(2) with degree n-1 or less forms a vector space GF(2) with dimension n.

11.2 Answer

First prove the set of polynomials forms a group: Next show that the group is also a vector space.

Its much easier for me to make assumptions when working with bit string so convert all polynomials into bit strings of length n. To prove these bit strings form a group over bitwise XOR it needs to have associativity, an Identity, and an inverse for every element. Our group has associativity but I'm not sure how to show this other than a bunch of examples. The identity is the string of all zeros. and each elements inverse is its self. Now to show that our group is also a vector space it needs to have commutativity, Compatibility of scalar multiplication with field multiplication, Identity element of scalar multiplication, Distributivity of scalar multiplication with respect to vector addition, and Distributivity of scalar multiplication with respect to field addition. For commutativity is the same for associativity. For Compatibility of scalar multiplication with field multiplication just multiply every element in the vector by the scalar and mod by 2. The identity for this is 1. The Distributivity of scalar multiplication with respect to vector addition is proven by multiplying an odd number against any vector you get the same vector and multiplying and even number by any vector you get all zeros. Either way it has Distributivity. For Distributivity of scalar multiplication with respect to field addition $(a + b)v = av + bv$ must be true for all a, b, and v. If a is even then $av = 0$ and if b is odd then $bv = v$ and $0 + v = v$ then if you add a and b you get another odd number c and $cv = v = av + bv = 0 + bv = 0 + v = v$. Then if both a and b are odd $a + b = c$ and c is an even number so $cv = 0$, then because a and b are odd you get $av = v$ and $bv = v$ and $v + v = 0$ so we have $(a + b)v = cv = 0 = av + bv = v + v = 0$. And finally if a and b are both even then $(a+b)v = cv = 0 = av+bv = 0+0 = 0$. And so the bit strings we have stated form a vector space with dimension n.

12 Exercise 2.26

12.1 Question

12.2 Answer

The row space of G is defined by the set of vectors $(x, y, z) \in F^3$ of the form $[x + y, x + y + z, y + z, x + z, x, y, z]$. In order for the row space of G to be contained in the null space of H the following equations must be true for any x, y, and z. $x + y + x + y = 0$

$x + y + z + x + y + z = 0$
$x + z + x + z = 0$
This is always true because the number of each variable in the equation is equal. Next to show that the row space of G is the null space of H get the row space of H. The row space of H is defined by the set of vectors $(a, b, c, d) \in F^4$ of the form $[a, b, c, d, a + b + d, a + b + c, b + c + d]$. See that the dimension of the row space of H is 4 and the rank of H is 7. We know that the rank of a matrix is the sum of its row space and its null space, by this we know that the null space of H is the dimension of its row space minus its rank which is 3. So if the dimension of the row space of G is 3, and its contained in the null space of H and the dimension of the null space of H is 3, then the row space of G is equal to the null space of H. For the opposite given the definition of the row space of H above see the equations that must be satisfied for the row space of H to be contained in the null space of G. $a + b + d + a + b + d = 0$
$a + b + c + a + b + c = 0$
$b + c + d + b + c + d = 0$
Again the number of each variable in every equation is even and so they will always be true for any a, b, c, and d. Next the row space of H has dimension 4, to show that the null space of G has dimension 4 take its rank 7 and subtract its row space dimension 3.

13 Exercise 3.1

13.1 Question

Consider a systematic (8,4) code whose parity-check equations are:
$v_0 = u_1 + u_2 + u_3$
$v_1 = u_0 + u_1 + u_2$
$v_2 = u_0 + u_1 + u_3$
$v_3 = u_0 + u_2 + u_3$
Where u_0, u_1, u_2, and u_3 are message digits and v_0, v_1, v_2 and v_3 are parity-check digits. Find the generator and parity-check matrices for this code. Show that analytically the minimum distance for this code is 4.

13.2 Answer

First lets find the generator matrix given that we know the given equations are a parity check for a valid block code we need only generate k code words that satisfy the above equations to generate the matrix.
$(1, 0, 0, 0) = (0, 1, 1, 1, 1, 0, 0, 0)$
$(0, 1, 0, 0) = (1, 1, 1, 0, 0, 1, 0, 0)$
$(0, 0, 1, 0) = (1, 1, 0, 1, 0, 0, 1, 0)$
$(0, 0, 0, 1) = (1, 0, 1, 1, 0, 0, 0, 1)$
We can see now that a generator matrix for our (8,4) code is:

$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$ And by switching the first $n-k=4$ columns with the rest of the matrix you get the parity-check matrix $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$

14 Exercise 3.4

14.1 Question

Let H be the parity check matrix of a (n, k) linear code C that has both odd and even-weight codewords. Construct a new linear code C_1 with the following parity check-matrix.
a. Show that C_1 is an $(n+1, k)$ linear code. C_1 is an extension of C. b. Show that every codeword of C_1 has even weight. c. Show that C_1 can be obtained by C by adding an extra parity-check digit denoted by $v\,\mathrm{inf}$, to the left of each codeword v as follows: (1) if v has odd weight, then $v\,\mathrm{inf} = 1$, and (2) if v has even weight, then $v\,\mathrm{inf} = 0$. The parity check digit $v\,\mathrm{inf}$ is called an overall parity-check digit.

14.2 Answer

First show that C_1 is still linearly independent, the changes to the new H_1 was adding an additional row of all ones at the bottom and a column of all zeros at the beginning. For the new row all of the entries are the same as long as everything else is linearly independent then so will C_1, And given the above rows were linearly independent this is the case. Next for the added column again the bottom row is all zeros but where ever the old linearly independent matrix intersected with this new column we have zeros so its still linearly independent. Now because the first row is all zeros the message digits are still k but the new column adds an additional parity-check digit.

For part B the last row added by the changes is called an overall parity-check digit that is 1 when the rest of the code word is odd and it is 0 when it is even this is because the last row is all ones.

For part C This is what the last row and column of H_1 dose adds the odd-even parity-check digit to the left of every code word of C.

15 Exercise 3.7

15.1 Question

Prove that the Hamming distance satisfies the triangle inequality; that is, let x, y, and z be three n-tuples over $GF(2)$, and show that

$d(x, y) + d(y, z) \geq d(x, z)$.

15.2 Answer

To prove this we will take this bit by bit. To start if the right side is 1 then x dose not equal z in the first bit. Because were working with bits here if we have three variables, the first bits of x, y, and z, then two of them will be the same. We just stated that x dose not equal z if the first bit on the right is 1, so either x equals y or y equals z, Ie. either x dose not equal y or z dose not equal y, Meaning also either 0+1 or 1+0 equals 1 so the left equals the right if x dose not equal z. Now if x equals z then the right bit will be 0 and anything is greater or equal to 0 so were done.

16 Exercise 3.13

16.1 Question

16.2 Answer

First an example parity-check matrix of the proper form

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

No rows of the identity matrix on the right will work nor will any of the 4 on the left work on there own. For any rows used on the left a row must be used on the right because of the four by four identity square. Now because the original parity-check matrices are on thee left the minimum number of rows need on the left will be equal to the parity-check matrix with the largest minimum distance. Then you must double it because of the identity square giving you two times the greater minimum distance of d_1 or d_2, which will be greater or equal to $d_1 + d_2$.

17 Exercise 3.14

17.1 Question

Show that the linear code C given in problem 3.1 is self dual.

17.2 Answer

The dual code of a code is the code generated by the parity-check matrix of a code. If a code has its self as its parity-check matrix which is the case when $n = k/2$ then any code word multiplied by the transposition of G results in 0.

18 Exercise 4.1

18.1 Question

Form a parity-check matrix for the (15, 11) Hamming code. Devise a decoder for the code.

18.2 Answer

To start m is equal to four because $2^m - 1 = 15$ and $2^m - m - 1 = 11$ which is the n and k for the code. Its parity-check matrix consists of an identity matrix followed by all the m-tuples of weight two or more, There are exactly $2^m - m - 1$ m-tuples of weight 2 or more, resulting in 15 total columns.

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

To decode take the message and multiply it against the transpose of the parity-check matrix if the syndrome weight is zero we had no error so pass truncate the last 15 rows of the codeword. If its weight is greater than zero an error has occurred. Next given the 15 parity-check check equations we can find a number of error patterns that satisfy all the parity check equations given the digits of s. Then grab the lowest weight error pattern and add it to v and you'll get the corrected message.

19 Exercise 4.8

19.1 Question

19.2 Answer

First construct the v 32-tuples that make up the generator matrix of $R(2, 5)$:
$v_0 = 11111111111111111111111111111111$ $v_5 = 00000000000000001111111111111111$
$v_4 = 00000000111111110000000011111111$ $v_3 = 00001111000011110000111100001111$
$v_2 = 00110011001100110011001100110011$ $v_1 = 01010101010101010101010101010101$
$v_4v_5 = 00000000000000000000000011111111$ $v_3v_5 = 00000000000000000000111100001111$
$v_2v_5 = 00000000000000000011001100110011$ $v_1v_5 = 00000000000000000101010101010101$
$v_3v_4 = 00000000000011110000000000001111$ $v_2v_4 = 00000000001100110000000000110011$
$v_1v_4 = 00000000010101010000000001010101$ $v_2v_3 = 00000011000000110000001100000011$
$v_1v_3 = 00000101000001010000010100000101$ $v_1v_2 = 00010001000100010001000100010001$
The minimum distance of this code is 8. To decode a 32 length message let start

at the end of the message to get the 12 bit. Get the dot product of every four bits to get 8 different values. Then what every the majority equality is take that as the 12 bit. Next for the 13 bit you apply the pattern "11001100" to which bits you add up to get the 13 bit. And so on until you get all the double bits. Then subtract the code you have built up so far to get a code minus all the double bit sections. Then find more patterns to discern the single bits. Rules of the patters are the selections must be a power of 2 and you must select 2^r total bits which is four in our case. The goal is to find a pattern such that you get a single 1 in each selection.

20 Exercise 4.18

20.1 Question

Prove the (24, 12) Golay code is self-dual.

20.2 Answer

For a code to be self dual then the $G * G^T = 0$. Now the definition of the parity-check part of the generator matrix states that the ith column is the transpose of the ith row, as such it is also symmetrical along the diagonal axis. Meaning that $P = P^T$ and $P * P^T = I_12$. It follows that the dot product of any i row and column equals zero. And $G * G^T = (I_12P) * (PI_12) = I_12 * P + I_12 * I_12 + P * I_12 + P * P = P + I_12 + P + I_12 = P + P + I_12 + I_12 = 0 + 0 = 0$ proves the code is self dual

21 Exercise 4.20

21.1 Question

Decode 101101110010000011000011 And 001111110010000000000001

21.2 Answer

First get the P matrix and assemble the G and H matrix:

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

Then multiply $r_1 * H^T = 001110001001 = s$ Because the weight of S is greater than three find a row in the P matrix such that $s + p_i \leq 2$. Because no such row exists then $s * P = 100011101110$. Again because the weight of $S * P$ is greater than two find a row in the P matrix such that $s + p_i = 2$. Such a row exists $s * P + p_1 = 000000000011$ now set the e pattern to $(u_i, s * P + p_i)$. Now set the corrected v to $r + (u_i, s * P + p_i) = 001110011111000011000000$ Again for r_2 get s by $r_2 * H^T = 110000001100 = s_2$ Next find the row p_i such that $s_2 + p_i \leq 2$. Because no such row exist then $s_2 * P = 111000010000$. Again because the weight of $S * P$ is greater than two find a row in the P matrix such that $s + p_i = 2$. Again no such row exists and so we must declare a decoding fault and request a retransmission.

22 Exercise 5.1

22.1 Question

Consider the (15,11) cyclic Hamming code generated by $g(x) = 1 + X + X^4$.
a. Determine the parity polynomial $h(x)$ of this code.
b. Determine the generator polynomial of its dual code.
c. Find the generator and parity-check matrices of systematic form.

22.2 Answer

The definition of $h(x)$ is $(X^n + 1) = g(x)h(x)$ so if we do long division of $(X^n + 1)/g(x)$ where $n = 15$. We get $(X^{11} + X^8 + X^7 + X^5 + X^3 + X^2 + X + 1) * (X^4 + X + 1) = X^{15} + 1$ where $(X^{11} + X^8 + X^7 + X^5 + X^3 + X^2 + X + 1) = h(x)$.

For part b the definition of a dual space is the code generated by the parity-check matrix and as we already have $h(x)$ the parity-check polynomial, this is not the same a the generator polynomial for the dual code, the generator for the dual code is thee reciprocal of the parity-check polynomial. To get reciprocal

of $h(x)$ defined by $X^k * h(X^1) = X^{11} * (X^{-11} + X^{-8} + X^{-7} + X^{-5} + X^{-3} + X^{-2} + X^{-1} + 1) = (1 + X^3 + X^4 + X^6 + X^8 + X^9 + X^{10} + X^{11})$. You can see if we now layout the reciprocal of $h(x)$ like with did for $g(x)$ to get the generator of the matrix, You will again get it in non systematic form. After preforming some row operations you'll see that the generator matrix of the dual code is now equivalent to the parity-check matrix of the starting code.

For part c we merely need to find the systematic form of one of the two and by definition we can switch the identity and P sections to get the other. First get the generator matrix as is from the polynomial $X^4 + X + 1$ which is:

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

Then by preforming a bunch of row operations you can get it in systematic form:

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

And now that it is in systemic form we can transpose the P section and add a new 4 dimensional identity section to the right side.

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

23 Exercise 5.2

23.1 Question

Devise an encoder and a decoder for the (15,11) cyclic Hamming code generated by $g(x) = 1 + X + X^4$.

23.2 Answer

To encode:
1. Take a message of k digits and convert it to polynomial form.
2. Multiply your message polynomial by $X^{n-k} = X^{15-11} = X^4$.
3. The new polynomial by your generator polynomial and grab the remainder.
4. Form the code word by taking your remainder b adding the message polynomial multiplied by X^4.
To decode:
1. Multiply the received vector by the transposition of the parity-check matrix to get the syndrome.
2. If s is zero then truncate the last four digits of the received vector and you have the message .
3. If s is non zero then locate an error pattern that takes r to a valid code word given the parity check equations and s.
4. Add the error pattern to r and then truncate thee last four digits.

24 Exercise 5.6

24.1 Question

Let $g(x)$ be the generator of a binary cyclic code of length n.
a. Show that if $g(x)$ has $X + 1$ as a factor, The code contains no codewords of odd weight.
b. If n is odd and $g(x)$ dose not have a factor of $X + 1$, Show that the code word contains a codeword of all ones.
c. Show the code has minimum weight of at least three if n is the smallest integer such that $g(x)$ divides $X^n + 1$.

24.2 Answer

If a polynomial is a multiple of $X + 1$ then it will have an even number of coefficients. I am not sure how to prove the above fact but here are a couple of examples:
1. $(X + 1) * 1 = even$
2. $(X + 1) * X + X^2 + X^3 = X + X^2 + X^3 + X^2 + X^3 + X^4 = X + X^4 = even$
3. $(X + 1) * X + X^2 + X^4 + X^5 = X + X^2 + X^4 + X^5 + X^2 + X^3 + X^5 + X^6 = X + X^3 + X^4 + X^6 = even$
I can prove this by fact that if a polynomial has 1 as a root it is divisible by $X + 1$. And since $g(x)$ is a factor of $X + 1$ and all the code words are multiples of $g(x)$ then every codeword has $X + 1$ as a factor.

For part b we know that if polynomial has 1 as a root is is divisible by $X + 1$ and since the code word of all ones dose not have 1 as a root it dose not have

$X + 1$ as a factor either. And because the code polynomial of all ones shares a root with $g(x)$ then it is a multiple of $g(x)$ as well.

For part c each of the codes generated by a polynomial with degree $n - k$ and divides $X^n + 1$ is a cyclic hamming code and they all have minimum weight of three.

25 Exercise 5.10

25.1 Question

Consider the $(2^m - 1, 2^m - m - 1)$ cyclic Hamming code C generated by $g(x) = (X + 1)p(x)$ where $p(x)$ is a primitive polynomial of degree m. An error pattern of the form $e(x) = X^i + X^{i+1}$ is called a double adjacent error pattern. Show that no two double adjacent error patterns can be in the same coset of a standard array for C. Therefore the code is capable of correcting all the single-error and double-adjacent-error patterns.

25.2 Answer

$n = 2^m - 1$
$k = 2^m - m - 1$
That means there are m parity-check digits.
First $g(x)$ has (X + 1) as a factor so all the code words will be of even weight.
Second $g(x)$ is a factor of $X^{2^m-1} + 1$ and so $p(x)$ must also be a factor of $X^{2^m-1} + 1$.
Third $p(x)$ is a primitive polynomial of degree m as such it is a factor of $X^{2^m-1} + 1$. But not of any polynomial $X^{2^m-1} + 1$ of a degree lesser than $2^m - 1$. Fourth any codeword with a double adjacent error pattern is still an even weight polynomial.

P is irreducible and is a factor of $X^{2^m-1} + 1$.

The question asks if have an error patter that is double adjacent as the co set leader it will only generate one result that is not a valid code word meaning for all double adjacent error patterns e $e(x) * v(x) = v_i(x)$ where $v_i(x)$ is another valid codeword for all except one v(x) in this case $e(x) * v(x) = s(x)$ for one and only one $v(x)$ per e.

26 Exercise 5.16

26.1 Question

Construct all binary cyclic codes of length 15.

26.2 Answer

The generator of a code must be a factor of $X^{15}+1$ to generate a code of length 15. Below are all polynomials that are a factor of $X^{15}+1$.
1.$X+1$
2.$X^{11}+X^{10}+X^6+X^5+X+1$
3.X^4+X+1
4.$X^9+X^6+X^5+X^4+X+1$
5.X^7+X^3+X+1
6.X^5+X^3+X+1
7.$X^{13}+X^{12}+X^{10}+X^9+X^7+X^6+X^4+X^3+X+1$
8.$X^8+X^7+X^5+X^4+X^3+X+1$
9.X^2+X+1
10.$X^7+X^6+X^5+X^2+X+1$
11.$X^8+X^4+X^2+X+1$
12.$X^10+X^8+X^5+X^4+X^2+X+1$
13.$X^6+X^3+X^2+X+1$
14.$X^11+X^8+X^7+X^5+X^3+X^2+X+1$
15.$X^4+X^3+X^2+X+1$
16.$X^{14}+X^{13}+X^{12}+X^{11}+X^{10}+X^9+X^8+X^7+X^6+X^5+X^4+X^3+X^2+X+1$

27 Exercise 5.17

27.1 Question

Let β be non zero element in the field $GF(2^m)$, and $\beta \neq 1$. Let $\alpha(x)$ be the minimum polynomial of β. Is there a cyclic code with $\alpha(x)$ as the generator? If your answer is yes, Find the shortest cyclic code with $\alpha(x)$ as the generator polynomial.

27.2 Answer

From theorem 2.12 we know there exists a polynomial $X^{2^m-1}+1$ such that all the non zero elements of $GF(2^m)$ are roots. By 2.14 if $\alpha(x)$ is the minimum polynomial of an element, then either it is $X^{2^m-1}+1$ or it is a factor of $X^{2^m-1}+1$. Either way that means $\alpha(x)$ generates a $(2^m-1, 2^m-m-1)$ code. This code is also the smallest code that $\alpha(x)$ can generate.

28 Exercise 5.19

28.1 Question

Consider the field $GF(2^m)$, which is constructed based on the primitive polynomial $p(x)$ of degree m. Let β be a primitive element whose minimum polynomial is $p(x)$. Show that every code polynomial in the hamming code generated by

$p(x)$ has β and its conjugates as roots. Show that any binary polynomial of degree $2^m - 2$ or less that has β as a root is a code polynomial of the code generated by $p(x)$.

28.2 Answer

First from theorem 2.11 we know that if the primitive polynomial $p(x)$ has β as a root then it also has all of its conjugates as roots. From theorem 2.14 we know that if the polynomials that have $p(x)$ as a factor then they also have the roots of $p(x)$ as their roots as well. Again from 2.14 the reverse is true where if a polynomial has β as a roots then it is multiple of the minimum polynomial of β.