Problem 1.1: Weighted codes. Let $s_1, s_2, \ldots, s_n$ be a sequence of digits, each in the range $0 \leq s_i < p$, where p is a prime number. The weighted sum is

$$W = ns_1 + (n-1)s_2 + (n-2)s_3 + \ldots + 2s_{n-1} + s_n$$

The final digit s_n is selected so that W modulo p is equal to 0. That is, $W \equiv 0 \pmod{p}$. W is called the checksum.

(a) Show that the weighted sum W can be computed by computing the cumulative sum sequence $t_1, t_2, \ldots, t_n$ by

$$t_1 = s_1,\ t_2 = s_1 + s_2,\ \ldots,\ t_n = s_1 + s_2 + \ldots + s_n$$

then computing the cumulative sum sequence

$$w_1 = t_1,\ w_2 = t_1 + t_2,\ \ldots,\ w_n = t_1 + t_2 + \ldots + t_n$$

with $W = w_n$.

(b) Suppose that the digits s_k and s_{k+1} are interchanged, with $s_k \neq s_{k+1}$, and then a new checksum W' is computed. Show that if the original sequence satisfies $W \equiv 0 \pmod{p}$, then the modified sequence cannot satisfy $W' \equiv 0 \pmod{p}$.

(c) For a sequence of digits of length $< p$, suppose that digit s_k is altered to some $s'_k \neq s_k$ and a new checksum W' is computed. Show that if the original sequence satisfies $W \equiv 0 \pmod{p}$, then the modified sequence cannot satisfy $W' \equiv 0 \pmod{p}$. Thus, a single modified sigit can be detected. Why do we need the added restriction on the length of the sequence?

(d) See if the ISBN 0-13-139072-4 is valid.

(e) See if the ISBN 0-13-193072-4 is valid

The solutions to problem 1.1 are given below:

(a) *Claim:* $W = w_n$, where w_n behaves as described in the problem statement.
Proof: From the problem statement, $w_n = \sum_{i=1}^{n} t_i$ and $t_i = \sum_{j=1}^{n} s_j$. Organize the values for t_i in a table as follows:

t_i					
t_1	s_1				
t_2	s_1	s_2			
t_3	s_1	s_2	s_3		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	
t_n	s_1	s_2	s_3	$\ldots$	s_n
$\sum_i^n t_i$	ns_1	$(n-1)s_2$	$(n-2)s_3$	$\ldots$	s_n

where row i contains the values of s_j for each j such that the sum of all elements in row i equal t_i. The value of w_n is then the sum of all s_j values in the table. If we sum first column-wise, then $\sum_{i=1}^{n} t_i = \sum_{i=1}^{n} s_i(n-i+1)$ which is (by definition) equal to w_n and W. Therefore, $w_n = W$.

(b) *Claim:* if the digits s_k and s_{k+1} are interchanged, the new checksum $W' \not\equiv 0 \pmod{p}$
Proof: We will proceed by way of contradiction. Assume that there exist values s_k and s_{k+1}, $s_k \neq s_{k+1}$ such that $W' \equiv 0 \pmod{p}$ when the two values were interchanged. This would imply that the difference between W and W' is also equivalent to zero modulo p. Because only s_k and s_{k+1} were affected, the difference becomes

$$\begin{aligned} W - W' &= [(n-k+1)s_k + (n-k+2)s_{k+1}] - [(n-k+1)s_{k+1} + (n-k+2)s_k] \\ &= s_{k+1} - s_k \end{aligned}$$

This implies that $s_{k+1} - s_k \equiv 0 \pmod{p}$. However, because both s_k and $s_{k+1} < p$, then their difference must also be less than p and so p cannot be a divisor of $s_{k+1} - s_k$. Because p is prime, $s_{k+1} - s_k$ cannot be a divisor of p and so $s_{k+1} - s_k \not\equiv 0 \pmod{p}$. Therefore, $W - W' \not\equiv 0 \pmod{p}$, and $W' \not\equiv 0 \pmod{p}$.

(c) *Claim:* For all $n < p$, if a digit s_k is altered to come $s'_k \neq s_k$, then the resulting $W' \not\equiv 0 \pmod{p}$.
Proof: Let $\delta = s'_k - s_k$ so that $s'_k = s_k + \delta$. Then

$$\begin{aligned} W' &= s_1 n + s_2(n-1) \ldots (s_k + \delta)(n-k+1) + \ldots s_1 \\ &= W + (n-k+1)\delta \\ &\equiv 0 + (n-k+1)\delta \pmod{p} \end{aligned}$$

Because $k \leq n < p$, we know that the difference $(n-k+1) < p$ as well. Additionally, s_k and s'_k are also less than p, making $\delta < p$. Because both values are less than p, then p cannot be a divisor of either $(n-k+1)$ or δ. Since p is prime, then $(n-k+1)$ nor δ are divisors of p and therefore $W' \not\equiv 0 \pmod{p}$. If the length n is greater or equal to p, then the assumption $n-k+1 < p$ would not be true for all values (consider the case where $p = 7, n = 10$, and $k = 4$) and you could potentially engineer a value for W' which would pass the checksum constraints with different values for s_k.

(d) For this ISBN, $W = 132$ which is equivalent to 0 mod 11, therefore this is a valid ISBN number.

(e) For this ISBN, $W = 138 \not\equiv 0$ mod 11, making this ISBN invalid.

Problem 1.2: See if the UPCs 0 59280 00020 0 and 0 41700 00037 9 are valid

---

If we hash the first UPC per the instructions in Section 1.2 for example 1.2 of the text, we get a hash of 60. Since this is divisible by 10, the value is a valid UPC code. The second UPC code yields a hash of 47. Since the second hash is not divisible by 10, this UPC code is invalid.

Problem 1.3: A coin having $P(\text{head}) = 0.001$ is tossed 10,000 times, each toss independent. What is the lower limit on the number of bits it would take to accurately describe the outcomes? Suppose it were possible to send only 100 bits of information to describe all 10,000 outcomes. What is the minimum average distortion per bit that must be accrued sending the information in this case?

The average information, in bits, of each *draw (or coin flip)* is defined as the entropy of the underlying distribution which we compute as

$$\begin{aligned} H(P) &= -\sum p_i \log(p_i) \\ &= -(0.001 * \log_2(0.001) + 0.999 * \log_2(0.999)) \\ &= 0.0114 \end{aligned}$$

If we multiply this by the number of draws, in this case 10,000, then the average information for the entire set of data would have a minimum bound of 114.0776 bits. If the channel we use to transmit this information has a capacity of 100 bits, then we can compute our rate as

$$r = \frac{100}{114.0755} = 0.8766$$

and we compute the distortion using the *rate-distortion theorem* so that

$$\begin{aligned} p &= H_2^{-1}(1-r) \\ &= H_2^{-1}(0.12339) \\ &= 0.0169 \end{aligned}$$

Therefore, for 10,000 draws, we would expect a distortion of $0.0169 * 10000 = 16.9$ bits.

Problem 1.4: Show that the entropy of a source X with M outcomes described by (1.1) is maximized when all the outcomes are equally probable: $p_1 = p_2 = \ldots = p_M$.

In this proof, we will use an idea from constrained optimization which states that for a constrained optimization

problem with equality constraints, the gradient of the equality constraint and that of the objective function are scalar multiples of each other, where the scaler multiple is known as a Lagrange multiplier, λ. In this case, our objective function is the entropy and the constraint is that the probability values must all sum to one. Formulating the objective function and equality constraint so that they are scalar multiples of each other allows us to say that

$$\begin{aligned}
&\nabla H_2(p) = \lambda \nabla \left[\sum_i p_i - 1 \right] \\
\implies &\frac{\ln(p_i) + 1}{\ln(2)} = \lambda \ \forall i \in 1, 2, \ldots, M \\
\implies &\ln(p_i) = \lambda \ln(2) - 1 \\
\implies &p_i = e^{\lambda \ln(2) - 1}
\end{aligned}$$

Therefore, p_i is equal to the same value for all values of i and the entropy is maximized when all outcomes are equally probable.

Problem 1.11 Consider a series of M BSCs, each with transition probability p, where the outputs of each BSC is connected to the inputs of the next in the series. Show that the resulting overall channel is a BSC and determine the crossover probability as a function of M. What happens as $m \to \infty$?

Consider the case where only 0 enters the system. We know that 0 will exit the other side when an even number of "flip" events occure. The transition probability will then be the sum of probability values for paths with even numbers of "flip" events. If the number of BSCs is m, then the number of possible paths with n flip events is

$$\binom{m}{n}$$

and the probability of taking a path with n flip events is

$$p^n (1-p)^{m-n}.$$

Therefore, the probability of taking a path with an even number of "flip" events is

$$p_{\text{even}} = \sum_{i=\text{even}}^{m} \binom{m}{i} p^i (1-p)^{m-i}$$

and consequently that the probability of the takinga path with an odd number of "flip" events is

$$p_{\text{odd}} = \sum_{i=\text{odd}}^{m} \binom{m}{i} p^i (1-p)^{m-i}$$

We can also observe that

$$\begin{aligned}
p_{\text{even}} &= \frac{1}{2} 2 p_{\text{even}} \\
\implies p_{\text{even}} &= \frac{1}{2} (p_{\text{even}} + p_{\text{odd}} - p_{\text{odd}} + p_{\text{even}}) \\
\implies p_{\text{even}} &= \frac{1}{2} \left(2 \left[\sum_{i=\text{even}}^{m} \binom{m}{i} p^i (1-p)^{m-i} \right] + \left[\sum_{i=\text{odd}}^{m} \binom{m}{i} p^i (1-p)^{m-i} \right] - \left[\sum_{i=\text{odd}}^{m} \binom{m}{i} p^i (1-p)^{m-i} \right] \right)
\end{aligned}$$

Next, we observe that when i is odd, $-p^i = (-p)^i$ so that

$$\begin{aligned}
p_{\text{even}} &= \frac{1}{2} \left(\left[\sum_{i=\text{even+odd}}^{m} \binom{m}{i} p^i (1-p)^{m-i} \right] + \left[\sum_{i=\text{even}}^{m} \binom{m}{i} (-p)^i (1-p)^{m-i} \right] + \left[\sum_{i=\text{odd}}^{m} \binom{m}{i} (-p)^i (1-p)^{m-i} \right] \right) \\
\implies p_{\text{even}} &= \frac{1}{2} \left(\left[\sum_{i=\text{even+odd}}^{m} \binom{m}{i} p^i (1-p)^{m-i} \right] + \left[\sum_{i=\text{even+odd}}^{m} \binom{m}{i} (-p)^i (1-p)^{m-i} \right] \right) \\
\implies p_{\text{even}} &= \frac{1}{2} \left(\left[\sum_{i=0}^{m} \binom{m}{i} p^i (1-p)^{m-i} \right] + \left[\sum_{i=0}^{m} \binom{m}{i} (-p)^i (1-p)^{m-i} \right] \right)
\end{aligned}$$

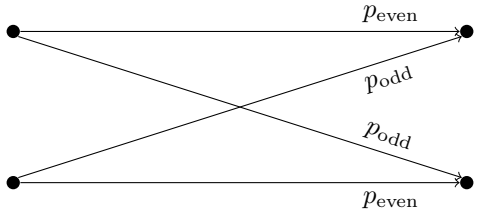
Theh binomial theorom, which states that $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$ can also be referenced to show that

$$\begin{aligned} p_{\text{even}} &= \frac{1}{2}\left([p+(1-p)]^m] + [-p+(1-p)]^m\right) \\ \implies p_{\text{even}} &= \frac{1}{2}\left([1]^m] + [1-2p]^m\right) \\ \implies p_{\text{even}} &= \frac{1}{2}\left(1 + [1-2p]^m\right) \\ \implies p_{\text{even}} &= \frac{1+(1-2p)^m}{2} \end{aligned}$$

Both $p_{\text{even}} + p_{\text{odd}}$ must sum to one, therefore we can express p_{odd} as

$$\begin{aligned} p_{\text{odd}} &= 1 - p_{\text{even}} \\ \implies p_{\text{odd}} &= 1 - \frac{1+(1-2p)^m}{2} \\ \implies p_{\text{odd}} &= \frac{2-1-(1-2p)^m}{2} \\ \implies p_{\text{odd}} &= \frac{1-(1-2p)^m}{2} \end{aligned}$$

This is true for both the 0 and 1 ends of the channel as the probabilities are symmetric. Therefore, a sequence of m BSC's can be represented as



Note how the structure of the new source channel matches that of a binary source channel.

Problem 1.13 Let $V_2(n,t)$ be the number of points in a Hamming sphere of "radius" t around a binary codwrord of length n. That is, it is the number of points within a Hamming distance t of a binary vector. Determine a formula for $V_2(n,t)$.

The hamming distance of one codeward from another is the number of bits which differ between the two. If we have a codeword, then the number of points that are a hamming "distance" i from our codeward would be

$$\binom{n}{i}$$

Therefore, the number of points *within* radius t would be the sum of all points that are hamming distance t or less from the center codeward so that

$$V_2(n,t) = \sum_{i=0}^{t} \binom{n}{i}.$$

Problem 1.14 Show that the Hamming distance satisfies the triangle inequality. That is, for three binary vectors $\mathbf{x}$,$\mathbf{y}$, and $\mathbf{z}$ of length n, show that

$$d_H(\mathbf{x},\mathbf{z}) \leq d_H(\mathbf{x},\mathbf{y}) + d_H(\mathbf{y},\mathbf{z}).$$

Because the hamming distance of two n dimensional vectors is the sum of $d_H(x_i, z_i)$ over all indices, we will show

that the triangle inequality holds for the hamming distance by showing that it holds for each element in $\mathbf{x}, \mathbf{y}$, and $\mathbf{z}$, that is that

$$d_H(x_i, z_i) \leq d_H(x_i, y_i) + d_H(y_i, z_i).$$

We will prove that the Hamming distance holds for each element in $\mathbf{x}, \mathbf{y}$, and $\mathbf{z}$ by showing that the Hamming distance holds for all cases. First, we do not need to prove anything for the case where $d_H(x_i, z_i) = 0$, or that x_i and z_i are the same value because the hamming distance is non-negative and so it will be impossible for $d_H(x_i, y_i) + d_H(y_i, z_i)$ to be less than zero.

Next, we also do not need to show anything for the case where $d_H(x_i, y_i) = 0, d_H(y_i, z_i) = 0$ because x_i cannot equal y_i if $y_i = z_i$ as $x_i \neq z_i$ (note, this only holds because $\mathbf{x}$, $\mathbf{y}$, and $\mathbf{z}$ are binary vectors. For other constallations, we would need to prove this point). Next, we may also ignore the case for $d_H(x_i, y_i) = 1, d_H(y_i, z_i) = 1$ because this implies that x_i, y_i, and z_i are all different, which cannot happend when there are only two elements in our constallation. Therefore the two remaining cases that remain are $d_H(x_i, z_i) = 1, d_H(x_i, y_i) = 1, d_H(y_i, z_i) = 0$ and $d_H(x_i, z_i) = 1, d_H(x_i, y_i) = 0, d_H(y_i, z_i) = 1$.

In the case where $d_H(x_i, z_i) = 1, d_H(x_i, y_i) = 1, d_H(y_i, z_i) = 0$, we observe that $1 \leq 1 + 0$ which is true. For the second case where $d_H(x_i, z_i) = 1, d_H(x_i, y_i) = 0, d_H(y_i, z_i) = 1$ we observe that $1 \leq 0 + 1$ is also a true statement. Therefore, the triangle inequality holds for the given values.

Problem 1.16 In this problem, we will demonstrate that the probability of error for a repetition code decreases exponentially with the code length. Several other useful facts will also be introduced by this problem.

(a) Show that

$$2^{-nH_2(p)} = (1-p)^n \left(\frac{p}{1-p}\right)^{np}$$

(b) For the fact

$$0 \leq p \leq \frac{1}{2} \implies \sum_{0 \leq i \leq pn} \binom{n}{i} \leq 2^{nH_2(p)},$$

justify the following steps of its proof:

$$\begin{aligned} 1 = (p + (1-p))^n &\geq \sum_{0 \leq i \leq pn} \binom{n}{i} p^i (1-p)^{n-i} \\ &\geq \sum_{0 \leq i \leq pn} \binom{n}{i} (1-p)^n \left(\frac{p}{1-p}\right)^{pn} \\ &= 2^{-nH_2(p)} \sum_{0 \leq i \leq pn} \binom{n}{i} \end{aligned}$$

(c) Show that the probability of error for a repetition code can be written as

$$P_e^n = \sum_{j=0}^{n-(t+1)} \binom{n}{j} (1-p)^j p^{(n-j)}$$

where $t = \lfloor (n-1)/2 \rfloor$.

(d) Show that

$$P_e^n \leq \left[2\sqrt{p(1-p)}\right]^n$$

The proofs for this problem are given as:

(a) *Claim:* $2^{-nH_2(p)} = (1-p)^n \left(\frac{p}{1-p}\right)^{np}$

Proof: First we apply the definition of entropy, assuming that our units are in bits so that log is base-2 so that

$$2^{-nH_2(p)} = 2^{-n(p\log_2(p) + (1-p)\log_2(1-p)}$$

Next, we distribute like terms and rearrange the terms in the exponent to show that

$$\begin{aligned} 2^{-n(p\log_2(p)+(1-p)\log_2(1-p)} &= 2^{np(\log_2(p)-\log_2(1-p))+n\log_2(1-p)} \\ &= 2^{np(\log_2(\frac{p}{1-p}))+n\log_2(1-p)} \\ &= 2^{\log_2(\frac{p}{1-p})^{np}+\log_2(1-p)^n} \\ &= (1-p)^n\left(\frac{p}{1-p}\right)^{np} \end{aligned}$$

(b) For this section we will proove several claims.

Claim: $1 = (p + (1-p))^n$

Proof: This proof uses properties of a field to justify the given relationship including the fact that 1 is the multiplicative identity, for every value there exists an additive inverse, and the fact that values are commutative. Doing so allows us to state that

$$\begin{aligned} 1 &= 1^n \\ &= (1+p-p)^n \\ &= (p+(1-p))^n. \end{aligned}$$

Claim: $(p + (1-p))^n \geq \sum_{0\leq i\leq pn} \binom{n}{i} p^i(1-p)^{n-i}$

Proof: Recall from the binomial theorem that

$$\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i} = (x+y)^n.$$

Substituting the definition for the Binomial Theorem into the left side of the claim yields

$$\begin{aligned} &\sum_{i=0}^{n} \binom{n}{i} p^i(1-p)^{n-i} \geq \sum_{i=0}^{pn} p^i(1-p)^{n-i} \\ \implies &\sum_{i=np+1}^{n} p^i(1-p)^{n-i} + \sum_{i=0}^{np} \binom{n}{i} p^i(1-p)^{n-i} \geq \sum_{i=0}^{np} p^i(1-p)^{n-i} \\ \implies &\sum_{i=np+1}^{n} p^i(1-p)^{n-i} \geq \sum_{i=0}^{np} p^i(1-p)^{n-i} - \sum_{i=0}^{np} \binom{n}{i} p^i(1-p)^{n-i} \\ \implies &\sum_{i=np+1}^{n} p^i(1-p)^{n-i} \geq 0 \end{aligned}$$

which is true because $0 \leq p \leq 0.5$.

Claim: $\sum_{i=0}^{np} \binom{n}{i}(1-p)^{n-i}p^i \geq \sum_{i=0}^{np} \binom{n}{i}(1-p)^n \left(\frac{p}{1-p}\right)^{np}$

Proof: Begin by arranging terms so that the two expressions can be more easily compared by acknowledging

that

$$\begin{aligned}
&\sum_{i=0}^{np}\binom{n}{i}(1-p)^{n-i}p^i \geq \sum_{i=0}^{np}\binom{n}{i}(1-p)^n\left(\frac{p}{1-p}\right)^{np} \\
\implies &\sum_{i=0}^{np}\binom{n}{i}(1-p)^n\left(\frac{p}{1-p}\right)^{i} \geq \sum_{i=0}^{np}\binom{n}{i}(1-p)^n\left(\frac{p}{1-p}\right)^{np} \\
\implies &\sum_{i=0}^{np}\binom{n}{i}(1-p)^n\left[\left(\frac{p}{1-p}\right)^{i} - \left(\frac{p}{1-p}\right)^{np}\right] \geq 0 \\
\implies &\sum_{i=0}^{np}\binom{n}{i}(1-p)^n\left[\frac{p^i}{(1-p)^i} - \frac{p^{np}}{(1-p)^{np}}\right] \geq 0 \\
\implies &\sum_{i=0}^{np}\binom{n}{i}(1-p)^n\left[\frac{p^i(1-p)^{np} - p^{np}(1-p)^i}{(1-p)^{npi}}\right] \geq 0 \\
\implies &\sum_{i=0}^{np}\binom{n}{i}(1-p)^n\left[\frac{(1-p)^{np-i} - p^{np-i}}{(1-p)^{np}p^{-i}}\right] \geq 0
\end{aligned}$$

Next, we note that the only place in this expression which can be greater than zero is the numerator of the fracional value. Therefore, by showing that

$$(1-p)^{np-i} - p^{np-i} \geq 0$$

we will effectively validate the claim because there will be no negative values in the expression left of zero so that their sum must necessarily be non-negative. Begin by recognizing that

$$\begin{aligned}
(1-p)^{np-i} - p^{np-i} \geq 0 &\implies (1-p)^{np-i} \geq p^{np-i} \\
&\implies 1-p \geq p
\end{aligned}$$

which we know because $0 \leq p \leq 1/2$.

Claim: $\sum_{i=0}^{np}\binom{n}{i}(1-p)^n\left(\frac{p}{1-p}\right)^{np} = 2^{-H_2(p)}\sum_{i=0}^{np}\binom{n}{i}$

Proof: Recall that

$$\begin{aligned}
\sum_{i=0}^{np}\binom{n}{i}(1-p)^n\left(\frac{p}{1-p}\right)^{np} = 2^{-H_2(p)}\sum_{i=0}^{np}\binom{n}{i} &\implies \sum_{i=0}^{np}\binom{n}{i}(1-p)^n\left(\frac{p}{1-p}\right)^{np} = 2^{-H_2(p)}\sum_{i=0}^{np}\binom{n}{i} \\
&\implies \sum_{i=0}^{np}\binom{n}{i}(1-p)^n\left(\frac{p}{1-p}\right)^{np} = (1-p)^n\left(\frac{p}{1-p}\right)^{np}\sum_{i=0}^{np}\binom{n}{i} \\
&\implies \sum_{i=0}^{np}\binom{n}{i}(1-p)^n\left(\frac{p}{1-p}\right)^{np} = \sum_{i=0}^{np}\binom{n}{i}(1-p)^n\left(\frac{p}{1-p}\right)^{np}
\end{aligned}$$

where the second step comes from the first claim we proved as part of this problem.

(c) *Claim:* $P_e^n = \sum_{j=0}^{n-(t+1)}\binom{n}{j}(1-P)^j p^{n-j}$

Proof: When using a repetition code, each bit is sent through the channel, and then whichever bit is in the majority is selected. Therefore, the probability of an error for a repetition code is the probability that half or more of the transmitted bits are incorrect. Because each transmitted bit is independent, the probability of any $n-j$ bits being incorrect is the probability of j *correct* bits times the probability of $n-j$ *incorrect* bits so that

$$p(j) = (1-p)^j p^{n-j}.$$

however, this does not account for various permutations. The number of total permutations with j correct bits is $\binom{n}{j}$, making the probability of j correct bits

$$p(j) = \binom{n}{j}(1-p)^j p^{n-j}.$$

Next, we sum over the probability of all $j \leq n/2$, making the probability of error

$$\begin{aligned} P_e^n &= \sum_{i=0}^{n-(\lfloor \frac{n-1}{2} \rfloor + 1)} \binom{n}{j} (1-p)^j p^{n-j} \\ &= \sum_{i=0}^{n-(t+1)} \binom{n}{j} (1-p)^j p^{n-j}, \quad t = \left\lfloor \frac{n-1}{2} \right\rfloor \end{aligned}$$

(d) *Claim:* $P_e^n \leq \left[2\sqrt{p(1-p)}\right]^n$

Proof: Recall from the previous proof that

$$P_e^n = \sum_{j=0}^{n-(t+1)} \binom{n}{j} (1-p)^j p^{n-j}$$

where $t = \lfloor (n-1)/2 \rfloor$. Using this definition for P_e^n, we can rephrase the claim as

$$\sum_{j=0}^{n-(t+1)} \binom{n}{j} (1-p)^j p^{n-j} \leq 2^n p^{n/2} (1-p)^{n/2}$$

and use the binomial theorem to say that

$$\sum_{j=0}^{n-(t+1)} \binom{n}{j} (1-p)^j p^{n-j} \leq 2^n p^{n/2} (1-p)^{n/2} \implies \sum_{j=0}^{n-(t+1)} \binom{n}{j} (1-p)^j p^{n-j} \leq \sum_{i=0}^{n} \binom{n}{i} p^{n/2} (1-p)^{n/2}$$

Note how $n - (t+1) < n/2$ which implies that $j < n/2$ and $n - j > n/2 \ \forall j$. For the remainder of this proof, we will show that $(1-p)^j p^{n-j} \leq p^{n/2}(1-p)^{n/2}$. By doing so, we demonstrate that

$$\begin{aligned} &\sum_{j=0}^{n-(t+1)} \binom{n}{j} (1-p)^j p^{n-j} \leq \sum_{i=0}^{n-(t+1)} \binom{n}{i} p^{n/2} (1-p)^{n/2} \\ \implies &\sum_{j=0}^{n-(t+1)} \binom{n}{j} (1-p)^j p^{n-j} \leq \sum_{i=0}^{n} \binom{n}{i} p^{n/2} (1-p)^{n/2} \\ \implies &\sum_{j=0}^{n-(t+1)} \binom{n}{j} (1-p)^j p^{n-j} \leq \left[2\sqrt{p(1-p)}\right]^n \\ \implies &P_e^n \leq \left[2\sqrt{p(1-p)}\right]^n. \end{aligned}$$

To show that $(1-p)^j p^{n-j} \leq p^{n/2}(1-p)^{n/2}$, we start by noting that

$$\begin{aligned} (1-p)^j p^{n-j} \leq p^{n/2}(1-p)^{n/2} &\implies 0 \leq p^{n/2}(1-p)^{n/2} - (1-p)^j p^{n-j} \\ &\implies 0 \leq (1-p)^j \left[(1-p)^{n/2-j} p^{n/2} - p^{n-j}\right] \\ &\implies 0 \leq (1-p)^j \left[(1-p)^{n/2-j} - p^{n-j-n/2}\right] p^{n/2} \\ &\implies 0 \leq (1-p)^j \left[(1-p)^{n/2-j} - p^{n/2-j}\right] p^{n/2}. \end{aligned}$$

Note that

$$0 \leq (1-p)^j \left[(1-p)^{n/2-j} - p^{n/2-j}\right] p^{n/2} \iff (1-p)^{n/2-j} - p^{n/2-j} \geq 0$$

because $(1-p)^j$ and $p^{n/2}$ are necessarily greater than zero. This implies that

$$(1-p)^{n/2-j} \geq p^{n/2-j} \implies 1 - p \geq p.$$

Which is true be definition. If the probability of an incorrect transition were greater that the probability of a correct transmission, then you would reverse the two to increase performance. Therefore,

$$P_e^n \leq \left[2\sqrt{p(1-p)}\right]^n$$

Problem 1.18 Show that for soft-decision decoding on the $(n, 1)$ repetition code, (1.33) is correct.

Claim: The probability of error for a soft decoding repetition code with n repeats is $Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$.

Proof: Recall that when a zero is send, each observation r_i is normally distributed with mean $\sqrt{E_c}$ and variance σ^2. From section 1.8.2 of the book, we also know that our optimal decision rule is to choose $\hat{s} = \sqrt{E_c}$ if $\sum_i^n r_i > 0$. We also know that the sum of independent gaussian random variables is distributed as gaussian with a mean and variance that are the respective sum of the individual mean and variances. Therefore, we can also say that

$$\begin{aligned}
&\sum_i^n r_i \sim \mathcal{N}(n\sqrt{N_c}, n\sigma^2) \\
\implies &\sum_i^n r_i \sim \mathcal{N}\left(n\sqrt{\frac{N_b}{n}}, n\sigma^2\right) \qquad \text{Recall that } E_c = \frac{E_b}{n} \\
\implies &\sum_i^n r_i \sim \mathcal{N}\left(n\sqrt{\frac{N_b}{n}}, \frac{nN_0}{2}\right) \qquad \text{Because } \sigma^2 = \frac{N_0}{2}
\end{aligned}$$

with this in mind, note that the probability of error is the probability that the sum of observations is less than zero, or

$$\begin{aligned}
P_{\text{error}} &= P\left(\sum_i^n r_i < 0\right) \\
\implies P_{\text{error}} &= \Phi\left(\frac{0 - \sqrt{nE_b}}{\sqrt{\frac{nN_0}{2}}}\right) \\
\implies P_{\text{error}} &= \Phi\left(-\sqrt{\frac{-nE_b}{\frac{nN_0}{2}}}\right) \\
\implies P_{\text{error}} &= \Phi\left(-\sqrt{\frac{2E_b}{N_0}}\right)
\end{aligned}$$

where $\Phi(x)$ is the standard normal cdf function. Next, we observe that $\Phi(-x) = Q(x)$ because the gaussian distribution is symmetric about the mean. Therefore,

$$P_{\text{error}} = \Phi\left(-\sqrt{\frac{2E_b}{N_0}}\right) \implies P_{\text{error}} = Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$$

Problem 1.19 For the $(n, 1)$ code used over a BSC with crossover probability p, what is the probability that an error event occurs which is not detected?

Error events would not be detected when all n bits were modified in transmission, which happens with probability p (per bit). Assuming that each bit is transmitted independently of the others, the probability that an error event is not detected would be p^n.

Problem 1.21 For the $(7, 4)$ Hamming code generator polynomial $g(x) = 1 + x + x^3$, generate all possible code polynomials $c(x)$. Verify that they correspond to the codewords in (1.35). Take a nonzero codeword $c(x)$ and compute $c(x)h(x)$ modulo $x^7 + 1$. Do this also for two other nonzero codewords. What is the check condition for this code?

Recall that a polynomial $c(x)$ is a code word if $c(x)h(x) \equiv 0 \pmod{(x^7 + 1)}$. We also know that $h(x) = \frac{x^7+1}{g(x)} \pmod 2$, which implies that $h(x)c(x) \equiv 0 \pmod{(x^7 + 1)}$ if $g(x)$ divides $c(x)$ and $c(x)$ is an element of the set of all polynomials of degree 6 (or less). Because $g(x)$ must divide $c(x)$, we already know that the values in $c(x)$ are multiples of $g(x)$. Our search must then include all elements in the set of polynomials of degree less than or equal to 4. Each of these elements is then multiplied by $g(x)$ to form a code word $c(x)$.

$$\begin{bmatrix} 0 \\ x^2 \\ x \\ x^2 + x \\ 1 \\ x^2 + 1 \\ x + 1 \\ x^2 + x + 1 \\ x^3 \\ x^3 + x^2 \\ x^3 + x \\ x^3 + x^2 + x \\ x^3 + 1 \\ x^3 + x^2 + 1 \\ x^3 + x + 1 \\ x^3 + x^2 + x + 1 \end{bmatrix} g(x)$$

$$= \begin{bmatrix} 0 \\ x^5 + x^3 + x^2 \\ x^4 + x^2 + x \\ x^5 + x^4 + x^3 + x \\ x^3 + x + 1 \\ x^5 + x^2 + x + 1 \\ x^4 + x^3 + x^2 + 1 \\ x^5 + x^4 + 1 \\ x^6 + x^4 + x^3 \\ x^6 + x^5 + x^4 + x^2 \\ x^6 + x^3 + x^2 + x \\ x^6 + x^5 + x \\ x^6 + x^4 + x + 1 \\ x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ x^6 + x^2 + 1 \\ x^6 + x^5 + x^3 + 1 \end{bmatrix}$$

If we take the coefficients that correspond to the powers in the polynomials given above, we get

	1	x	x^2	x^3	x^4	x^5	x^6
$c_1(x)$	0	0	0	0	0	0	0
$c_2(x)$	0	0	1	1	0	1	0
$c_3(x)$	0	1	1	0	1	0	0
$c_4(x)$	0	1	0	1	1	1	0
$c_5(x)$	1	1	0	1	0	0	0
$c_6(x)$	1	1	1	0	0	1	0
$c_7(x)$	1	0	1	1	1	0	0
$c_8(x)$	1	0	0	0	1	1	0
$c_9(x)$	0	0	0	1	1	0	1
$c_{10}(x)$	0	0	1	0	1	1	1
$c_{11}(x)$	0	1	1	1	0	0	1
$c_{12}(x)$	0	1	0	0	0	1	1
$c_{13}(x)$	1	1	0	0	1	0	1
$c_{14}(x)$	1	1	1	1	1	1	1
$c_{15}(x)$	1	0	1	0	0	0	1
$c_{16}(x)$	1	0	0	1	0	1	1

which match the code words in 1.35. As a check, we can multiple the values that correspond to $c_4(x), c_{11}(x)$, and $c_{16}(x)$ by $h(x) = x^4+x^2+x+1$ which yield $c_4(x)h(x) = x^10+x^9+x^8+x^7+x^3+x^2+x+1, c_{11}(x)g(x) = x^10+x^8+x^3+x$, and $c_{16}(x)h(x) = x^9 + x^8 + x^2 + x$ respectively all of which divide by $1 + x^7$ without remainder.

Problem 1.22 Is it possible that the polynomial $g(x) = x^4 + x^3 + x^2 + 1$ is a generator polyomial for a cyclic code of length $n = 7$?

We will verify that the polynomial $g(x) = x^4 + x^3 + x^2 + 1$ can in fact be a generator polynomical for a cyclic code of length $n = 7$ by showing that it divides $x^7 + 1$ and therefore has a parity-check polynomial.

$$
\begin{array}{rr}
 & x^3 - x^2 - 1 \\
\cline{2-2}
x^4 + x^3 + x^2 + 1 \big) & x^7 + 1 \\
 & -\ x^7 + x^6 + x^5 \quad + x^3 \\
\cline{2-2}
 & -x^6 - x^5 - x^3 + 1 \\
 & -\ -x^6 - x^5 - x^4 \quad - x^2 \\
\cline{2-2}
 & +x^4 - x^3 + x^2 + 1 \\
 & -\ -x^4 - x^3 - x^2 - 1 \\
\cline{2-2}
 & 2x^4 + 2x^2 + 2
\end{array}
$$

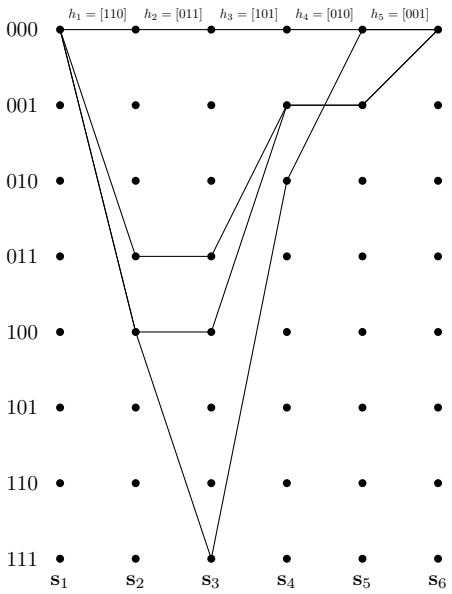
Note how the remainder from long devision yields an expression that is equivalent to zero modulo 2, which implies that the polynomial $x^3 + x^3 + x^2 + 1$ divides $x^7 + 1$ and thus that $g(x)$ may serve as a generator polynomial for a cyclic code of length $n = 7$.

Problem 1.23 For the parity check matrix

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

draw the wolf trellis and the Tanner graph.

We draw the wolf trellis graph for all paths which end in all zeros as



Consider the parity check matrix H from the problem statement with the following labels:

$$\begin{array}{c} \\ z_1 \\ z_2 \\ z_3 \end{array} \begin{array}{c} \begin{array}{ccccc} c_1 & c_2 & c_3 & c_4 & c_5 \end{array} \\ \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix} \end{array}.$$

We construct the Tanner graph by creating an edge between a *bit* node c_j and a *check* node z_i when the parity matrix is equal to 1 at $H_{i,j}$, which is given as