EE 605: Error Correcting Codes

Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay
Autumn 2011

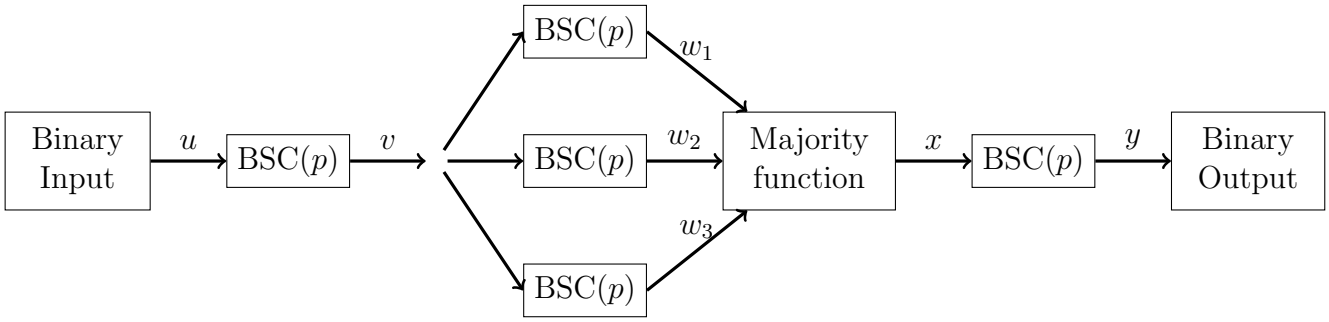
Solutions to Assignment 1

1. Prove that the Hamming distance satisfies the triangle inequality, i.e. $d(\mathbf{u}, \mathbf{v}) \leq d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v})$ for all n-tuples $\mathbf{u}, \mathbf{v}, \mathbf{w}$.
Solution: For a set A, let $|A|$ denote its cardinality. We know that $|A \cup B| \leq |A| + |B|$ and $|A| \leq |A \cup B|$. Also, if $|A| \leq |B|$ then $|A^c| \geq |B^c|$.

   Note that $d(\mathbf{u}, \mathbf{v}) = |A|$ where $A = \{i | u_i \neq v_i\}$.

$$\begin{aligned}
A^c &= \{i | u_i = v_i\} \\
\Rightarrow A^c &= \{i | u_i = v_i = w_i\} \cup \{i | u_i = v_i \neq w_i\} \\
\Rightarrow |A^c| &\geq |\{i | u_i = v_i = w_i\}| = |\{i | u_i = w_i\} \cap \{i | v_i = w_i\}| \\
\Rightarrow |A| &\leq |\{i | u_i = w_i\}^c \cup \{i | v_i = w_i\}^c| = |\{i | u_i \neq w_i\} \cup \{i | v_i \neq w_i\}| \\
\Rightarrow |A| &\leq |\{i | u_i \neq w_i\}| + |\{i | v_i \neq w_i\}| \\
\Rightarrow d(\mathbf{u}, \mathbf{v}) &\leq d(\mathbf{u}, \mathbf{w}) + d(\mathbf{w}, \mathbf{v})
\end{aligned}$$

2. Calculate the crossover probability of the binary symmetric channel which is equivalent to the system below.



Solution: The crossover probability of the equivalent binary symmetric channel is $\Pr[u \neq y]$.

$$\begin{aligned}
\Pr[u \neq y] &= \Pr[u \neq v] \Pr[v = y] + \Pr[u = v] \Pr[v \neq y] \\
&= (1-p) \Pr[v = y] + p \Pr[v \neq y] \\
&= (1-p) \{\Pr[v \neq x] \Pr[x \neq y] + \Pr[v = x] \Pr[x = y]\} \\
&\quad + p \{\Pr[v \neq x] \Pr[x = y] + \Pr[v = x] \Pr[x \neq y]\} \\
&= (1-p) \{\Pr[v \neq x] p + \Pr[v = x](1-p)\} + p \{\Pr[v \neq x](1-p) + \Pr[v = x] p\} \\
&= 2p(1-p) \Pr[v \neq x] + [p^2 + (1-p)^2] \Pr[v = x]
\end{aligned}$$

The calculation is complete if we can calculate $\Pr[v = x]$ which is equal to the probability that at most one of w_1, w_2, w_3 is different from v because the majority function can correct at most one error. This probability is equal to $(1-p)^3+3p(1-p)^2$.

3. Derive the optimal decoding rule for a $2n$-repetition code for use over a binary symmetric channel with crossover probability p. Is the optimal decoding rule unique? Calculate the average probability of error for this code when the optimal decoding rule is used.
Solution: If the codewords are equally, the optimal decoding rule for the $2n$-repetition code over a BSC is the minimum distance decoding rule. For each received vector, its distance to the all zeros and all ones $2n$-tuples is calculated. We decide the all zeros codeword was sent if the distance of the received vector to it is smaller and the all ones codeword was sent otherwise. But every received vector which has n zeros and n ones is equidistant to the all zeros and all ones codewords. Such received vectors can be decoded as either codeword without changing the average probability of error. Thus the optimal decoder is not unique. The average probability of error of the minimum distance decoder is

$$P_e = \sum_{i=n+1}^{2n} \binom{2n}{i} p^i (1-p)^{2n-i} + \frac{1}{2}\binom{2n}{n} p^n (1-p)^n$$

4. Consider a binary block code C of length n having minimum distance d_{min} where d_{min} is an odd integer. Show that when a overall parity bit is added to all the codewords in C we obtain a code of length $n+1$ and minimum distance $d_{min}+1$.
Solution: Consider any pair of codewords $\mathbf{u}, \mathbf{v}$ which are at a distance d_{min} from each other. Since d_{min} is odd, $\mathbf{u}$ and $\mathbf{v}$ differ in an odd number of locations. If we add an overall parity bit to $\mathbf{u}$ and $\mathbf{v}$, their parity bits will differ. For example, suppose $\sum_{i=1}^{n} v_i = 0$, then $\sum_{i=1}^{n} u_i$ has to be 1 since we are changing an odd number of terms in the summation. So any pair of codewords in C which are at a distance d_{min} will be at a distance $d_{min}+1$ after the addition of the overall parity check.

   Now consider any pair of codewords which are not a minimum distance d_{min}. They are at a distance of at least $d_{min}+1$. After the addition of the overall parity check bit, the distance between them will remain the same if their parity bits are the same or increase by one if their parity bits are different. So they will still be at a distance of at least $d_{min}+1$.

   Hence the minimum distance of the new code is $d_{min}+1$.