6.440 Essential Coding Theory	MIT, Fall 2011
Problem Set 1	
Instructor: Dana Moshkovitz	September 13, 2011

Due: September 27, 2011.

Question 1

In this question we consider different ways to generalize the $(7, 4, 3)$ Hamming code we saw in class.

For $l \geq 1$, consider the $l \times (2^l - 1)$ parity check matrix H_1, whose columns are the binary representations of the numbers 1 to 2^l. Let $\mathcal{H}_1$ be the Hamming code defined by H_1.

1. What are the rate and distance of $\mathcal{H}_1$? How many errors can it correct?
2. Show that $\mathcal{H}_1$ is a *perfect code*, i.e., has the largest possible number of codewords given its length and distance

   Consider the following encoding $E_2 : \{0,1\}^{4r} \to \{0,1\}^{7r}$: Think of $x \in \{0,1\}^{4r}$ as consisting of r blocks of 4 bits each. E_2 encodes each of the blocks using the $(7, 4, 3)$ Hamming code. Let $\mathcal{H}_2$ be the code that is defined by E_2.

3. What are the rate and distance of $\mathcal{H}_2$? How many errors can it correct?
4. Is $\mathcal{H}_2$ also a perfect code? When would you rather use $\mathcal{H}_1$, and when would you rather use $\mathcal{H}_2$?

Question 2

In the following X and Y are random variables over a finite sample space Ω. Prove:

1. $H(X) \geq 0$. Equality holds iff X is constant.
2. $H(X) \leq \log |\Omega|$. Equality holds iff X is uniform over Ω.
3. $H(X|Y) \geq 0$. Equality holds iff Y determines X.
4. $H(X|Y) \leq H(X)$. Equality holds iff X and Y are independent.
5. $H(X) - H(X|Y) = H(Y) - H(Y|X)$.

   Let the volume of a Hamming Ball of radius γn in $\{0,1\}^n$ be $B := \sum_{i=0}^{\gamma n} \binom{n}{i}$.

6. $B \leq 2^{H(\gamma)n}$. **Hint:** use the binomial expansion of $(\gamma + (1-\gamma))^n$.
7. $\lim_{n\to\infty} \frac{\log B}{n} = H(\gamma)$. **Hint:** use Stirling's formula.