Due: October 18, 2011.

Question 1 - Useful Approximations
Formalize and prove:
1. For a small $\delta > 0$, $H(\delta) \approx \delta \log \frac{1}{\delta}$.
2. For a small $\epsilon > 0$, $H\left(\frac{1}{2} - \epsilon\right) \approx 1 - \Theta(\epsilon^2)$.
3. For a large $q > 1$, $H_q(\delta) \approx \delta + O\left(\frac{q-1}{\delta}\right)$, where $H_q(\delta) = \delta \log_q \frac{1}{\delta} + (1 - \delta) \log_q \frac{1}{1 - \delta}$.

Question 2 - Random Codes
Let $0 < p < \frac{1}{2}$.

1. Show that the expected distance of a random code $C \subseteq \{0, 1\}^n$ of rate $1 - H(p)$ is $\ll pn$.
2. Show that by deleting a small fraction of the codewords in a random code $C \subseteq \{0, 1\}^n$ of rate $1 - H(p)$ one can obtain a code of distance $\approx pn$ with high probability.
3. Show that a random binary generator matrix whose dimensions are $n \times (1 - H(p))n$ yields a linear code $C \subseteq \{0, 1\}^n$ of distance $\approx pn$ with high probability.

Question 3 - $q$-ary Plotkin Bound
Prove that for any code of rate $R$ and relative distance $\delta$ over an alphabet of size $q$,
\[ R + \frac{q}{q - 1} \delta \leq 1. \]

Question 4 - $k$-wise Independence
Let $m = 2^r - 1$ and $k = 2t + 1$ such that $k \leq m$. Define $N = 2(m + 1)^t$. Describe an explicit construction of a 0-1 matrix $A$ with columns $a^{(1)}, \ldots, a^{(m)} \in \{0, 1\}^N$ such that:
- For every $1 \leq i \leq m$, the column $a^{(i)}$ has the same number of 0’s and 1’s.
- For every $1 \leq i_1 < \ldots < i_k \leq m$, the $k$ columns $a^{(i_1)}, \ldots, a^{(i_k)}$ contain every binary string of length $k$ in $N/2^k = 2^{2t - k + 1}$ rows.

(Such a matrix is very useful for construction of hash families and for derandomization of certain algorithms; see, for example, Luby and Wigderson’s survey “Pairwise independence and Derandomization”).

Hint: BCH codes.
Question 5 - $\varepsilon$-Biased Sets/Balanced Codes

We say that $S \subseteq \{0, 1\}^n$ is $\varepsilon$-biased if for every $c \neq 0 \in S$, the weight of $c$ (i.e., the number of non-zeros) satisfies:

$$\frac{1 - \varepsilon}{2} n \leq wt(c) \leq \frac{1 + \varepsilon}{2} n.$$

Show how to convert an $(n, k, d)_q$ code $C$ with distance $d = (1 - \frac{1}{q} - \varepsilon)n$ into a $(\varepsilon + 1/q)$-biased set $S \subseteq \{0, 1\}^{nq}$ of the same size.

Hint: Concatenation with Hadamard.

Question 6 - Finite Fields Drill

Show the following:

1. For every $\gamma \neq 0 \in \mathbb{F}_q$, there are $q + 1$ elements $\alpha \in \mathbb{F}_q^2$ such that $N(\alpha) = \gamma$.

2. For every $\gamma \in \mathbb{F}_q$, there are $q$ elements $\alpha \in \mathbb{F}_q^2$ such that $Tr(\alpha) = \gamma$. 