**CECS 419-519, Writing Assignment 5, Due 8:00 am, March 1st, 2024, Dr. Ebert**

# Directions

Make sure name is on all pages. Order pages (front and back) so that solutions are presented in their original numerical order. **Please no staples or folding of corners (your papers won't get lost). A paper clip is OK** Show all necessary work and substantiate all claims. Avoid plagiarism.

# Problems

1. Let $\mathcal{E}$ be a $\sigma$-algebra of sets. Show that if $A, B \in \mathcal{E}$, then $A - B \in \mathcal{E}$. (10 pts)

   **Solution.** We have
   $$A - B = A \cap \overline{A \cap B} \in \mathcal{E}$$
   since $\mathcal{E}$ is closed under intersection and complement. □

2. For the sample space $\{0,1\}^\infty$, recall the event space consisting of sets of the form $A \subseteq \{0,1\}^*$, where $A$ is a finite minimal prefix code (see Example 1.5 of the Autoreducibility lecture). If $A = \{00, 010, 1011, 1101, 111\}$ and $B = \{000, 0110, 100, 1010, 11\}$, then provide minimal prefix codes $C$, $D$, and $F$, for which

   (a) $C\{0,1\}^\infty = \overline{A}\{0,1\}^\infty$,

   (b) $D\{0,1\}^\infty = A\{0,1\}^\infty \cup B\{0,1\}^\infty$, and

   (c) $E\{0,1\}^\infty = A\{0,1\}^\infty \cap B\{0,1\}^\infty$.

   (15 pts)

   **Solution.** We have

   (a) $C\{0,1\}^\infty = \overline{A}\{0,1\}^\infty \Rightarrow C = \{011, 100, 1010, 1100\}$.

   (b) $D\{0,1\}^\infty = A\{0,1\}^\infty \cup B\{0,1\}^\infty \Rightarrow D = \{00, 010, 0110, 1\}$.

   (c) $E\{0,1\}^\infty = A\{0,1\}^\infty \cap B\{0,1\}^\infty \Rightarrow E = \{010, 0110, 1101, 111\}$. □

3. Prove that if a finite minimal prefix code $A$ satisfies
   $$\mu(A) = \sum_{w \in A} 2^{-|w|} = 1,$$
   then $A = \{\lambda\}$, where $\lambda$ is the empty word. Hint: use mathematical induction on the length of the longest word(s) in $A$. (20 pts)

   **Solution.** We use induction on the maximum length $n$ of any word in $A$. Basis step: if $n = 0$, then we have $A = \lambda$ since $\lambda$ is the only word having length 0. Inductive step: assume the statement is true for all maximum lengths up to and including $n$ and suppose $w0 \in A$ has maximum length with $|w| = n$. Then, $w1$ must also be in $A$, since otherwise $\mu(A) < 1$ (i.e. with positive probability it is possible to generate a sequence prefixed by $w1$ and so is not covered by any word in $A$). But $w0$ and $w1$ both being in $A$ contradict the assumption that $A$ is a *minimal* prefix code. □

4. Let $P$ be a probability measure over $\sigma$-algebra $\mathcal{E}$, and suppose $E_1 \subseteq E_2 \subseteq \cdots$ is a nested sequence of sets, where $E_i \in \mathcal{E}$, for $i = 1, 2, \ldots$. Provide a summation formula for computing $\mu(\bigcup_{i=1}^{\infty} E_i)$. Hint: you may find Problem 1 helpful. (15 pts)

   **Solution.** We must measure $\bigcup_{i=1}^{\infty} E_i$ and, since $E_i \subseteq E_{i+1}$, for $i = 1, 2, \ldots$, we see that the union can be rewritten as a disjoint union of the sets

$$E_1 - E_0, E_2 - E_1, E_3 - E_2, \ldots,$$

   where $E_0 = \emptyset$. Therefore, by Exercise 1 and Kolmogorov's 2nd axiom we have

$$\mu(\bigcup_{i=1}^{\infty} E_i) = \sum_{i=1}^{\infty} \mu(E_i - E_{i-1}). \quad \square$$

5. Consider the set $\mathcal{B}$ of all infinite binary sequences $s$ for which every length-$n$ ($n$ divisible by 4) prefix of $s$ consists of exactly $3n/4$ 1's and $n/4$ 0's. Suppose we wish to make a null cover for $\mathcal{B}$ of the form

$$\mathcal{B} = \bigcap_{k=1}^{\infty} W_k\{0,1\}^{\infty},$$

   where $W_k$ consists of all binary words of some length $n_k$ so that

   (a) $n_k$ is divisible by 4,
   (b) $\mathcal{B} \subseteq W_k\{0,1\}^{\infty}$,
   (c) $\mu(W_k) \leq \frac{1}{2^k}$,
   (d) and every $w \in W_k$ has $n_k/4$ 0's.

   Provide a formula for computing an $n_k$ that satisfies the above constraints. Hint: use the following result from combinatorics. For any $n$ and $0 < \alpha < 1$,

$$\binom{n}{\alpha n} = \frac{1 + o(1)}{\sqrt{2\pi\alpha(1-\alpha)n}} \cdot 2^{n \cdot H(\alpha)},$$

   where $H(\alpha) = H(\alpha, 1-\alpha)$ is the entropy function. Your formula may ignore the $o(1)$ term since it becomes vanishingly small for increasing $k$. Is this null cover constructive? Explain. (20 pts)

   **Solution.** The idea is to let $W_k$ denote all words $w$ of some fixed length $n_k$ for which $w$ has $n_k/4$ 0's, where $n_k$ satisfies the conditions stated in the problem. Let $N > 0$ be so large that

$$\frac{1 + o(1)}{\sqrt{2\pi\alpha(1-\alpha)N}} \leq 1,$$

where $\alpha = 1/4$. Thus, so long as we require $n_k \geq N$, and $n_k$ divisible by 4, then it will be true that the fraction of words $w$ in $\{0,1\}^{n_k}$ for which $w$ has $n_k/4$ 0's, is less than or equal to

$$\frac{2^{H(\alpha)n_k}}{2^{n_k}} = \frac{1}{2^{(1-H(\alpha))n_k}} \leq \frac{1}{2^k}$$

which is true so long as

$$n_k \geq k/(1 - H(\alpha)),$$

which is possible since $H(1/4, 3/4) = 0.811$. Thus, we choose the length of the words in $W_k$ to be the first $n_k$ for which i) $n_k \geq N$, ii) $n_k$ is divisible by 4, and iii)

$$n_k \geq k/(1 - H(\alpha)).$$

Therefore, the $W_k$'s provide a null cover for $\mathcal{B}$, and the null cover is constructive, since there is a program which, on input $k$, first computes $n_k$ and then lists all words $w$ in $\{0,1\}^{n_k}$ that have exactly $n/4$ 0's. □

6. For the binary matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

Determine its rank (i.e. dimension of its column space) and nullity (dimension of its NULL space) and verify the Rank theorem for $A$. List each of the null vectors (there are 16 of them). Can you see why the 1-balls centered around these null vectors i) do not overlap with each other and ii) cover the entire space $\{0,1\}^7$? Note that all arithmetic is over the field $\{0,1\}$ with $\oplus$ as addition: $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. (20 pts)

**Solution.** Label the columns of $A$ with the letters/Boolean variables a-g. Then by reordering the columns as $a, b, d, c, e, f, g$ we arrive at a matrix in reduced row-echelon form. Moreover, columns/variables $c, e, f, g$ are the independent variables since they may assume any combination of 0's and 1's and their values will completely determine the values for variables $a$, $b$, and $d$ via the equations

$$a = c \oplus e \oplus g, b = c \oplus f \oplus g, \text{ and } d = e \oplus f \oplus g.$$

Therefore, $\text{rank}(A) = 3$ and $\text{nullity}(A) = 4$. Thus, there are 16 null vectors and each 1-ball that is centered by a null vector has 8 vectors for a total of $16 \times 8 = 128$ vectors. Thus, so long as the 1-balls do not overlap, *every* vector in $\{0,1\}$ will belong to exactly one 1-ball. The key to seeing that they do not overlap is from the fact that, for $i = 1, \ldots, 7$, $Ae_i = (i)_2$ (check this!). Therefore, if two 1-balls overlapped, then there would be null vectors $c_1$ and $c_2$, and $1 \leq i, j \leq 7$ for which

$$c_1 \oplus e_i = c_2 \oplus e_j.$$

But by linearity of matrix multiplication, this would imply that

$$A(c_1 \oplus e_i) = A(c_1) \oplus A(e_i) = 0 + (i)_2 = (i)_2 = (j)_2 = 0 + (j)_2 = A(c_2) \oplus Ae_j = A(c_2 \oplus e_j)$$

and so $i = j$. But then we have

$$c_1 \oplus e_i \oplus e_i = c_1 = c_2 \oplus e_j \oplus e_i = c_2,$$

and so there is no overlap between the 1-balls. □