
Part I: Discrete Math.

1. Propositions. 10 points. 3/3/4

- (a) The following statement expresses the fact that there is a smallest number in the natural numbers, $(\exists y \in \mathbb{N}) (\forall x \in \mathbb{N}) (y \leq x)$. Write a statement that expresses the fact that there is no smallest number in the integers, \mathbb{Z} .

Answer: $\neg(\exists y \in \mathbb{Z}) (\forall x \in \mathbb{Z}) (y \leq x)$

or

$(\forall y \in \mathbb{Z}) (\exists x \in \mathbb{Z}) (y > x)$

- (b) The following statement could express Fermats Little Theorem, fill in the blank so that it does.

Let $\text{Prime}(p) = \forall d \in \mathbb{N}; d \geq 2, d < p \implies \neg(d|p)$,

$(\forall p \in \mathbb{N}) [\text{Prime}(p) \implies ((\forall a \in \mathbb{N}) ((______) \implies a^{p-1} \equiv 1 \pmod{p}))]$

Answer: $a \neq 0$

- (c) The statements,

$(\exists x \in S) ((\forall y \in S) P(x,y) \wedge (\forall y \in S) Q(x,y))$

and

$((\exists x \in S) (\forall y \in S) P(x,y)) \wedge ((\exists x \in S) (\forall y \in S) Q(x,y))$,

are not equivalent. Give a counterexample. That is, define an S , $P(x,y)$, and $Q(x,y)$ which cause the above statements to have different values.

Answer: $S = \{1, 2, 3, 4, 5\}$, $P(x,y) = "x \geq y"$, $Q(x,y) = "x \leq y"$.

2. Quick Short Answer. 34 points. Breakdown below.

Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

- (a) [4 Points.] What is the number of different n -men, n -women stable marriage *instances*? (Here the men and women are distinguishable. This, for example, means switching the preference lists of two different men corresponds to two different instances, as does switching the order of two women in a man's preference list.)

Answer: $(n!)^{2n}$

- (b) [3 Points.] In any run of the stable marriage algorithm, where the men propose, it is the case that the number of women receiving a proposal on each day is non-decreasing. This includes women receiving old proposals. (True/False)

Answer: True

The improvement lemma implies this.

- (c) [3 Points.] What is the inverse of 2 modulo n , if n is odd? (You should write an expression that may involve n . Simplicity matters.)

Answer: Let $n = 2k + 1$, then $2^{-1} = (k + 1)$ since $2(k + 1) \equiv 1 \pmod{(2k + 1)}$.

-
- (d) [3 Points.] If $\gcd(x, y) = 13$, what is $\gcd(x, x - 13y)$?

Answer: The correct answer is 13 or 169.

But the problem was designed to be 13. The reasoning was that $\gcd(x, x - y) = \gcd(x, y)$. Then use induction. But that doesn't work. Why? The problem should have read $\gcd(x, y - 13x)$ not $\gcd(x, x - 13y)$. Apologies.

- (e) [4 Points.] What is $3^{26} \pmod{35}$?

Answer: 9

$3^{24} \equiv 1 \pmod{35}$, and what's left is 3^2 .

- (f) [4 Points.] What is d for the RSA scheme where $p = 5$, and $q = 7$, and e is 5? (Do not worry about the security of such a scheme, just follow the definition of RSA.)

Answer: 5

$d = e^{-1} \pmod{24}$, which is 5.

- (g) [3 Points.] What degree polynomial should you use to tolerate 3 errors (corruptions) when sending a message consisting of 7 packets?

Answer: 6

The degree of the polynomial is 6 regardless of the number of errors.

We are giving some credit for 13, as it is too tricky that the polynomial does not change.

This is just remembering error correction with corruptions needs $n + 2k$ packets to tolerate k errors for a message of length n .

Consider a hypercube of dimension $d \geq 2$ for the next two parts. Recall that the vertices correspond to all the length d binary (bit) strings, and each vertex is adjacent to all vertices that differ in one bit position.

- (h) [2 Points.] Remove all vertices (and their incident edges) where the number of ones in the binary representation is even. How many connected components are in the remaining graph?

Answer: 2^{d-1}

All the edges incident to the remaining half of the vertices go to removed vertices since edges change the parity of the number of 1's in a vertex.

- (i) [2 Points.] Remove all vertices (and their incident edges) where the first bit is a 1. How many connected components are in the remaining graph?

Answer: 1.

You get the 0 subcube!

The hypercube problems are complete now.

- (j) [3 Points.] If you take a walk in a graph until you reach a vertex with no unused edges, this vertex is either the starting vertex or has ____ degree. (Possible answers: odd or even.)

Answer: odd.

If you enter an even degree vertex, you can always leave unless it is the starting vertex.

- (k) [3 Points.] What is the minimum number of edges one needs to remove from K_{2n} (the complete graph on $2n$ vertices) to leave exactly two components of equal size.

Answer: $\binom{2n}{2} - 2\binom{n}{2}$.

Get two complete graphs on half the nodes.

3. More Short Answer. 33 points. Breakdown below.

Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

- (a) [4 Points.] How many different anagrams of MISSISSIPPI are there that do not start or end with I? (For example, MISSISSIPPI should not be counted, as it ends with I. Note there are 11 characters: 1 M, 4 S's, 4 I's, and 2 P's. No need to simplify your expression.)

Answer: $\frac{11!}{4!4!2!} - 2\frac{10!}{4!3!2!} + \frac{9!}{4!2!2!}$

- (b) [4 Points.] If $ax + by = 6$ and $cx + dy = 5$, for integers a, b, c, d, x and y , what is the multiplicative inverse of x modulo y ? (Answer should be in terms of a, b, c and/or d modulo y .)

Answer: $a - c \pmod{y}$

Subtract the second equation from the first and one obtains $(a - c)x + (b - d)y = 1$. Taking the equation modulo y gives that $(a - c)x = 1 \pmod{y}$.

- (c) [4 Points.] What is the maximum number of solutions for the equation $10x = y \pmod{35}$, for any value of y , for $x, y \in \{0, 1, \dots, 34\}$.

Answer: 5

For any y where there is a solution, x , $x + 7k$ is also a solution.

- (d) [5 Points.] A degree 2 polynomial, $P(x)$, over arithmetic modulo 7 goes through points $(1, 0)$, $(2, 4)$, $(3, 0)$, what is $P(0)$?

Answer: 2

The polynomial is $a(x - 1)(x - 3)$ by where its roots are. Also, $a = 3$, plugging in for the value at 2. Finally, plug in the value 0 into the resulting polynomial.

- (e) [6 Points.] How many polynomials of degree exactly 2 modulo p are there that cannot be factored into two or more polynomial factor; are "irreducible"? (For example, $x^2 - 1$ is reducible as it factors into $(x - 1)(x + 1)$, x^2 is also reducible, $x^2 + 1$ is irreducible modulo 3 since it has no roots. Answer should be an expression involving p .)

Answer: $(p - 1)p^2 - (p - 1)(p) - (p - 1)\binom{p}{2}$

The total number of degree 2 polynomials without the perfect square polynomials and without the polynomials that are factored. The polynomials need to be scaled by leading coefficients.

- (f) [5 Points.] The problem of determining whether a program uses more than n^2 space (in bits) on an input of size n is undecidable. (True/False)

Answer: False.

Run your program P , if it ever uses more than n^2 space, answer that it does use more than n^2 space.

If it runs more than the $k2^{n^2}$ time, where k is the size of the program, than you have repeated a state (consisting of the memory and a program line), and thus it will be in an infinite loop. In this case you have determined that it does not use more than n^2 space.

So, if you run for at most $k2^{n^2}$ steps, you can make your determination.

- (g) [5 Points.] In any stable pairing where exactly half the men are paired with their optimal partner, at least half the women are paired with their pessimal partner. (True/False)

Answer:

True.

Consider any woman, M , paired with a man who is paired with his optimal partner, W . If he is not her pessimal partner, then another man is her pessimal partner in another a stable marriage S . But then (M, W) are a rogue couple in S .

4. Proofs. 22 points. 6/8/9

- (a) Show that if $n^2 - 1$ is not a multiple of d , than neither $n - 1$ nor $n + 1$ is a multiple of d .

Answer: If $n - 1$ or $n + 1$ is a multiple of d , then so is $(n - 1)(n + 1) = n^2 - 1$. This is a proof of the contrapositive. Q.E.D.

-
- (b) Prove that the problem of determining whether a program has *any* input which causes it to halt is undecidable. (True/False.)

Answer: By contradiction. Assume one has a program **EverHalts(P)** that determines whether P halts on any input.

We will implement **Halts(P,x)** by forming a program P' that ignores its input and calls P on x , and then calling **EveryHalts(P')**.

The program P halts on x if and only if P' ever halts, so we have implemented a **Halts(P,x)** program. That is undecidable, and thus we have a contradiction. Q.E.D.

- (c) Given a necklace of n red and n blue beads. Show that you can cut the necklace at a place such that every prefix of the resulting string of beads has at least as many red beads as blue. For example, the (circular) necklace $BBRR$ can be cut between the blue beads and red beads producing a string $RRBB$ where every prefix (R , RR , RRB , and $RRBB$) has more red beads than blue beads. (Advice: if you don't have an idea, maybe come back later.)

Answer: Induction:

Base: For $n = 1$, there is only one necklace BR , which works. by cutting between the blue bead and red bead.

Induction Step:

For $n + 1$, remove an adjacent RB pair of beads to obtain an n -necklace. Consider the string that we have by induction, if the pair appears as RB we continue to be fine, if it appears as BR , and we are not fine, the difference between the number of red beads and blue beads up this point must have been 0. The rest of the string must have all its prefixes have more reds than blues, as well as the string prior to this BR pair. This says we can put them together in either order.

In particular, cutting the new necklace in between B and R will produce a string consisting of the rest of R , the rest of the previous string, and the string prior to the BR pair, and a blue bead. Every prefix is fine in this setup. Q.E.D.

Part II: Probability.

1. True or False. No justification needed. 10 points. 2/2/3/3.

Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

- (a) If $\text{var}[X] \leq 1$, then $\Pr[X \geq 10] \leq 1\%$. (True or False.)

Answer: False. E.g., $X \equiv 100$.

- (b) Let X be uniform in $[0, 1]$. Then $E[X^5] = 1/6$. (True or False.)

Answer: True.

- (c) Let X, Y, Z be i.i.d.. Then $E[X + Y | X + Y + Z] = (2/3)(X + Y + Z)$. (True or False.)

Answer: True, by symmetry.

- (d) Let X, Y be two random variables and $Z = \min\{X, Y\}$. Then $E[Z] \leq \min\{E[X], E[Y]\}$. (True or False)

Answer: True. One has, $Z \leq X$, so that $E[Z] \leq E[X]$. Similarly, $E[Z] \leq E[Y]$.

2. Short Answers. 14 points: 3/4/3/4

Clearly indicate your answer and your derivation.

-
- (a) Let $\Omega = [0, 1]$ with the uniform distribution. Find $0 < a < b < 1$ so that the following two events of Ω are independent: $[0, 0.5]$ and $[a, b]$. [Hint: $(a, b) = (0, 1)$ do not satisfy the requirements and neither do $(a, b) = (0, 0)$ nor $(a, b) = (1, 1)$.]

Answer: We need $a < 0.5 < b$ and

$$\Pr[[0, 0.5] \cap [a, b]] = (0.5 - a) = \Pr[[0, 0.5]]\Pr[[a, b]] = 0.5(b - a),$$

i.e., $a + b = 1$.

- (b) Let X, Y be independent and $U[0, 1]$. Calculate $E[|X - Y|]$. [Hint: Note the absolute value!]

Answer: Place 0, X and Y on a clock with circumference 1, as in the busses example. By symmetry, $E[|X - Y|] = 1/3$.

Alternatively, one has $E[|X - Y| \mid X = x] = \int_0^x (x - y)dy + \int_x^1 (y - x)dy = \int_0^x ydy + \int_0^{1-x} ydy = x^2/2 + (1 - x)^2/2 = 1/2 - x + x^2$, so that $E[|X - Y|] = 1/2 - E[X] + E[X^2] = 1/3$.

- (c) A coin is equally likely to be fair or biased with $Pr[H] = 0.7$. You flip the coin 100 times. What is the expected number of heads?

Answer: It is 60. Indeed, $E[X|\text{fair}] = 50$ and $E[X|\text{biased}] = 70$. Hence, $E[X] = 60$.

- (d) A coin is equally likely to be fair or biased with $Pr[H] = 0.7$. You flip it twice and only get T s. Find the expected number of additional flips until you get H .

Answer: It is $\alpha/(0.5) + (1 - \alpha)/(0.7)$ where α is the probability that the coin is fair given that you flipped it 2 times and only got T s. By Bayes' Rule,

$$\alpha = (0.5(0.5)^2)/(0.5(0.5)^2 + 0.5(0.3)^2) = (1/4)/[(1/4) + 0.09] = 0.25/0.34.$$

Thus, the answer is $\alpha \frac{1}{0.5} + (1 - \alpha) \frac{1}{0.7} \approx 1.85$.

3. Short Problems. 18 points. 4/4/4/6

Clearly indicate your answer and your derivation.

- (a) Choose m real numbers uniformly at random in $[0, 1]$. Let X be the largest one of these numbers. What is the pdf $f_X(x)$? Find $E[X]$.

Answer: One has $Pr[X \leq x] = x^m$, so that $f_X(x) = mx^{m-1}$ and $E[X] = \int_0^1 xmx^{m-1} dx = m \int_0^1 x^m dx = m/(m+1)$.

- (b) Let X be a random variable with mean μ and variance σ^2 . Find the value a that minimizes $E[(X - a)^2]$.

Answer: The desired value is $a = \mu$. One has

$$E[(X - a)^2] = E[X^2] - 2aE[X] + a^2.$$

Setting the derivative with respect to a equal to zero, we find $-2E[X] + 2a = 0$, so that $a = E[X]$.

- (c) Let X be $Expo(1)$. Recall that this means that $f_X(x) = e^{-x}1\{x \geq 0\}$, so that $E[X] = 1$ and $F_X(x) = [1 - e^{-x}]1\{x \geq 0\}$.

(a) Show that $Pr[X > t + s | X > s] = Pr[X > t]$ for $s, t \geq 0$.

(b) Use that result to calculate $E[X | X > 5]$.

Answer:

(a) One has $Pr[X > t + s | X > s] = \frac{\exp\{-(t+s)\}}{\exp\{-s\}} = \exp\{-t\} = Pr[X > t]$.

(b) By the memoryless property we proved in (a), $E[X | X > 5] = 5 + E[X] = 6$.

- (d) Let X, Y, Z be i.i.d. $\mathcal{N}(0, 1)$ and $V = 2X + 3Y + 4Z, W = X + Y + Z$. Find $L[V|W]$.

Answer: We find that $E[V] = E[W] = 0; cov(V, W) = E[VW] = 2 + 3 + 4 = 9; var(W) = 3$. Hence, $L[V|W] = 3W$.

4. Less Short Problems. 58 points: 8/7/7/7/7/7/8/7

Clearly indicate your answer and your derivation.

- (a) Let $\Omega = \{1, 2, 3, 4, 5, 6\}$ be a uniform probability space. Let also $X(\omega)$ and $Y(\omega)$, for $\omega \in \Omega$, be the random variables defined as follows:

(i) Calculate $V = L[Y|X]$;

(ii) Calculate $W = E[Y|X]$;

(iii) Calculate $E[(Y - V)^2]$;

(iv) Calculate $E[(Y - W)^2]$.

Table 1: The random variables X and Y .

ω	1	2	3	4	5	6
$X(\omega)$	0	0	1	1	2	2
$Y(\omega)$	0	2	3	5	2	0

[Hint: Recall that $L[Y|X]$ and $E[Y|X]$ are functions of X and that you need to specify their value as a function of X .]

Answer:

(a) We find $E[X] = 1, E[Y] = 2, E[XY] = 2$, so that $cov(X, Y) = 0$ and $L[Y|X] = E[Y] = 2$.

(b) We see that $E[Y|X = 0] = 1, E[Y|X = 1] = 4, E[Y|X = 2] = 1$.

(c) $E[(Y - V)^2] = E[(Y - 2)^2] = (4 + 0 + 1 + 9 + 0 + 4)/6 = 3$.

(d) $E[(Y - W)^2] = (1 + 1 + 1 + 1 + 1 + 1)/6 = 1$.

- (b) A dart player is equally likely to be good or bad. If he is good, he shoots the dart uniformly in a circle with radius $1/2$. If he is bad, he shoots the dart uniformly in a circle with radius 1. The first dart of the player is at distance $1/3$ from the center. What is the expected distance of the second dart to the center of the target? [Hint: Condition on the distance being in $[1/3, 1/3 + \delta]$ for a small δ . Call that event A .]

Answer: If the player is bad, the expected distance is $\int_0^1 y f_Y(y) dy = \int_0^1 y \times 2y dy = 2/3$. Thus, if he is good, the expected distance is half as large, i.e., $1/3$. Let p be the probability that he is good given A . By Bayes' rule,

$$p = Pr[G|A] = \frac{(1/2)Pr[A|G]}{(1/2)Pr[A|G] + (1/2)Pr[A|B]}.$$

Now, $Pr[A|B] = f_Y(1/3)\delta = (2/3)\delta$, because the pdf of Y for a bad players is $2y$. For a good player, the pdf is $8y$ on $[0, 1/2]$, so that $Pr[A|B] = (8/3)\delta$. Hence,

$$p = \frac{(1/2)(8/3)}{(1/2)(8/3) + (1/2)(2/3)} = 4/5.$$

Thus, the expected distance of the second dart is $(4/5)(1/3) + (1/5)(2/3) = 2/5$.

- (c) You roll a balanced die n times. Let X_n be the number of different values that you got in the first n steps. For instance, if the successive rolls yield 5, 2, 5, 4, 2, 1, then $X_1 = 1, X_2 = 2, X_3 = 2, X_4 = 3, X_5 = 3$, and $X_6 = 4$. Calculate $E[X_n]$.

Answer: $E[X_{n+1}] = E[X_n + \frac{6-X_n}{6}] = 1 + E[X_n] \frac{5}{6}$. Thus, with $a = 5/6$, one has $E[X_1] = 1, E[X_2] = 1 + a, E[X_3] = 1 + (1 + a)a = 1 + a + a^2, \dots, E[X_n] = 1 + a + \dots + a^{n-1} = \frac{1-a^n}{1-a} = 6(1 - a^n)$.

Alternatively, the value k has not been seen in n rolls with probability a^n , so that the expected number of outcomes not seen in n rolls is $6a^n$ and the expected number of outcomes seen is $6 - 6a^n$.

- (d) One bin has 100 red balls. At step 1, you pick a ball at random from the bin and you replace it with a ball that is equally likely to be red or blue. You repeat that process. Let X_n be the number of red balls in the bin after n steps. Thus, $E[X_1] = 99.5$. Calculate $E[X_n]$. [Hint: Recall that $1 + a + \dots + a^k = (1 - a^{k+1})/(1 - a)$ for $a \neq 1$.]

Answer: $E[X_{n+1}|X_n] = 0.5 + 0.99X_n$. Hence,

$$E[X_2] = 0.5 + 0.99 \times 99.5$$

$$E[X_3] = 0.5 + 0.99[0.5 + 0.99 \times 99.5] = 0.5[1 + 0.99] + (0.99)^2 99.5$$

$$E[X_n] = 0.5[1 + 0.99 + \dots + 0.99^{n-2}] + (0.99)^{n-1} 99.5$$

$$= 0.5[1 - 0.99^{n-1}]/[1 - 0.99] + (0.99)^{n-1} 99.5 = 50 + 49.5(0.99)^{n-1}, n \geq 1.$$

- (e) Let X, Y be i.i.d. $U[-1, 1]$. Calculate $L[Y|Y + 2X]$. [Hint: Note that $\text{var}(X) = \text{var}[2Z]$ where $Z = U[0, 1]$.]

Answer: We know that

$$\begin{aligned} L[Y|Y + 2X] &= E[Y] + \frac{\text{cov}(Y + 2X, Y)}{\text{var}(Y + 2X)}(Y + 2X - E[Y + 2X]) \\ &= \frac{E[(Y + 2X)Y]}{\text{var}(Y) + 4\text{var}(X)}(Y + 2X) = \frac{1/3}{5/3}(Y + 2X) = \frac{1}{5}(Y + 2X). \end{aligned}$$

- (f) Let $\{X_1, \dots, X_n\}$ be the lifetimes of lightbulbs. We know that they are exponentially distributed with parameter λ and we know that $\lambda \geq 10$. Recall that $E[X_m] = \lambda^{-1}$ and $\text{var}[X_m] = \lambda^{-2}$.

- (1) Use Chebyshev's inequality to construct a 95%-confidence interval for λ^{-1} based on $\{X_1, \dots, X_n\}$.
- (2) Use the CLT to construct such a confidence interval.

[Hint: The answers should not contain λ , since this is what we are trying to estimate.]

Answer:

- (1) Let $A_n = (X_1 + \dots + X_n)/n$. By Chebyshev,

$$\Pr[|A_n - \lambda^{-1}| \geq a] \leq \frac{1}{na^2\lambda^2}.$$

Choosing a so that the upper bound is 5%, we need $na^2\lambda^2 = 20$, so that $a \approx 4.5\lambda^{-1}/\sqrt{n}$. Thus,

$$[A_n - 4.5\lambda^{-1}/\sqrt{n}, A_n + 4.5\lambda^{-1}/\sqrt{n}]$$

is a 95%-confidence interval for λ^{-1} . Since $\lambda \geq 10$,

$$[A_n - 0.45/\sqrt{n}, A_n + 0.45/\sqrt{n}]$$

is a 95%-confidence interval for λ .

- (2) Using the CLT, we know that the 95%-confidence interval is

$$[A_n - 2\sigma/\sqrt{n}, A_n + 2\sigma/\sqrt{n}]$$

where $\sigma = \lambda^{-1} \leq 0.1$. Hence,

$$[A_n - 0.2/\sqrt{n}, A_n + 0.2/\sqrt{n}]$$

is a 95%-confidence interval for λ^{-1} .

- (g) Consider the circuit in Figure 1. Nodes A and B are connected via five links. The links fail independently, each after an exponentially distributed time with mean 1. Calculate the expected time until the nodes A and B are disconnected, i.e., when there is no longer a path of working links between them. [Hint: Note that the time until the top path fails is the minimum of independent random variables; similarly for the bottom path. Recall what we know about the minimum of exponential random variables. Also, recall that if $X = \text{Exp}(\lambda)$, then $f_X(x) = \lambda e^{-\lambda x} 1\{x \geq 0\}$; also, for $x > 0$, $\Pr[X \leq x] = 1 - e^{-\lambda x}$ and $\Pr[X > x] = e^{-\lambda x}$, $E[X] = \int_0^\infty x\lambda e^{-\lambda x} dx = \lambda^{-1}$, $\text{var}(X) = \lambda^{-2}$.]

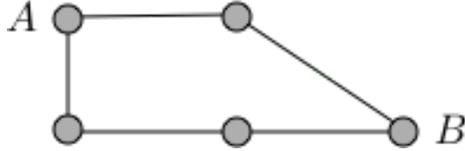


Figure 1: Circuit for problem.

Answer: Since the minimum of independent exponential random variables is exponential with the sum of their rates, we see that the time T until A and B are disconnected is such that $T = \max\{X, Y\}$ where $X = \text{Expo}(2)$ and $Y = \text{Expo}(3)$. Thus, for $u \geq 0$, the cdf of T is given by

$$\begin{aligned} F_T(u) &= \Pr[T \leq u] = \Pr[X \leq u] \Pr[Y \leq u] = (1 - \exp\{-2u\})(1 - \exp\{-3u\}) \\ &= 1 - \exp\{-2u\} - \exp\{-3u\} + \exp\{-5u\}. \end{aligned}$$

Consequently, the pdf of T is obtained by taking the derivative of the cdf:

$$f_T(u) = 2 \exp\{-2u\} + 3 \exp\{-3u\} - 5 \exp\{-5u\}.$$

Hence,

$$E[T] = \int_0^\infty u f_T(u) du = \frac{1}{2} + \frac{1}{3} - \frac{1}{5} = \frac{19}{30},$$

where we used the fact that $\int_0^\infty x \lambda e^{-\lambda x} dx = \lambda^{-1}$.

Alternatively, $E[T] = E[X + Y] - E[\min\{X, Y\}]$. Note that the method we used above extends to more than two exponential random variables, whereas this alternative approach works only for two.

(h) Let $X_n, n \geq 1$ be $\text{Expo}(1)$. Use Chernoff's inequality to find an upper bound on

$$\Pr\left[\frac{X_1 + \cdots + X_n}{n} \geq 2\right].$$

The bound should be of the form α^n for some $0 < \alpha < 1$. [Hint: Recall that $\int_0^\infty e^{-ax} dx = 1/a$ for $a > 0$.]

Answer: We have, for $\theta > 0$,

$$\Pr[X_1 + \cdots + X_n \geq 2n] \leq E[\exp\{\theta(X_1 + \cdots + X_n - 2n)\}] = e^{-2n\theta} E[e^{\theta X_1}]^n.$$

Now, for $0 < \theta < 1$.

$$E[e^{\theta X_1}] = \int_0^\infty e^{\theta x} e^{-x} dx = \frac{1}{1 - \theta}.$$

Hence,

$$\Pr[X_1 + \cdots + X_n \geq 2n] \leq [(1 - \theta)e^{2\theta}]^{-n}.$$

To minimize over $0 < \theta < 1$, we maximize $(1 - \theta)e^{2\theta}$. The maximizing θ is such that $-e^{2\theta} + 2(1 - \theta)e^{2\theta} = 0$, i.e, $\theta = 1/2$.

The resulting bound is

$$\Pr[X_1 + \cdots + X_n \geq 2n] \leq [2/e]^n.$$