CS 70 Fall 2023	Discrete Mathematics and Probability Theory Rao, Tal	HW 01

1 Calculus Review

In the probability section of this course, you will be expected to compute derivatives, integrals, and double integrals. This question contains a couple examples of the kinds of calculus you will encounter.

(a) Compute the following integral:

$$\int_0^\infty \sin(t)e^{-t}\,\mathrm{d}t\,.$$

(b) Compute the values of $x \in (-2,2)$ that correspond to local maxima and minima of the function

$$f(x) = \int_0^{x^2} t\cos\left(\sqrt{t}\right)\mathrm{d}t\,.$$

Classify which x correspond to local maxima and which to local minima.

(c) Compute the double integral

$$\iint_R 2x + y\,\mathrm{d}A\,,$$

where R is the region bounded by the lines $x = 1$, $y = 0$, and $y = x$.

Solution:

(a) Let $I = \int \sin(t)e^{-t}\,\mathrm{d}t$.
Use integration by parts, with $u = \sin(t)$ and $\mathrm{d}v = e^{-t}$.
This means $\mathrm{d}u = \cos(t)$ and $v = -e^{-t}$.

$$\begin{aligned} I = \int \sin(t)e^{-t}\,\mathrm{d}t &= uv - \int v\cdot \mathrm{d}u \\ &= -\sin(t)e^{-t} + \int e^{-t}\cos(t)\,\mathrm{d}t \end{aligned}$$

Use integration by parts again on $\int e^{-t}\cos(t)\,\mathrm{d}t$, with $u = \cos(t)$ and $\mathrm{d}v = e^{-t}$. This means $\mathrm{d}u = -\sin(t)$ and $\mathrm{d}v = -e^{-t}$.

$$\begin{aligned} \int e^{-t}\cos(t)\,\mathrm{d}t &= uv - \int v\cdot \mathrm{d}u \\ &= -\cos(t)e^{-t} - \int e^{-t}\cdot\sin(t)\,\mathrm{d}t \\ &= -\cos(t)e^{-t} - I \end{aligned}$$

Combining these results:

$$\begin{aligned} I &= -\sin(t)e^{-t} - \cos(t)e^{-t} - I \\ \Rightarrow 2I &= -\sin(t)e^{-t} - \cos(t)e^{-t} \\ \Rightarrow I &= \frac{-\sin(t)e^{-t} - \cos(t)e^{-t}}{2} \end{aligned}$$

Finally, we have:

$$I\Big|_0^\infty = \frac{0-0}{2} - \frac{0-1}{2} = \frac{1}{2}.$$

(b) Compute the derivative of the function, and set it equal to 0. Let $y = x^2$. By the Chain Rule and the Fundamental Theorem of Calculus,

$$\begin{aligned} \frac{\mathrm{d}f}{\mathrm{d}x} &= \frac{\mathrm{d}f}{\mathrm{d}y} \cdot \frac{\mathrm{d}y}{\mathrm{d}x} \\ &= y\cos(\sqrt{y}) \cdot 2x \\ &= 2x^3\cos(|x|) \\ &= 2x^3\cos(x) = 0 \end{aligned}$$

We get that the derivative is 0 only when $x^* = 0$, or when $\cos(x^*) = 0$. On the interval $(-2, 2)$, this corresponds to critical points $-\pi/2, 0$, and $\pi/2$.

To classify which correspond to local maxima and which to local minima, we examine how the sign of the derivative changes.

Around $x = \pi/2$, the derivative is positive for $x < \pi/2$ and negative for $x > \pi/2$. The same holds for $x = -\pi/2$. Thus, $x = \pm\pi/2$ correspond to local maxima.

Around $x = 0$, the derivative is negative for $x < 0$ and positive for $x > 0$. Thus, $x = 0$ corresponds to a local minima.

(c) We may set up the integral over the region R as follows:

$$\int_0^1 \int_0^x 2x + y \,\mathrm{d}y\,\mathrm{d}x.$$

Evaluating this integral gives

$$\begin{aligned} \int_0^1 \int_0^x 2x + y \,\mathrm{d}y\,\mathrm{d}x &= \int_0^1 2xy + \frac{y^2}{2}\Big|_0^x \mathrm{d}x \\ &= \int_0^1 \frac{5x^2}{2}\,\mathrm{d}x \\ &= \frac{5x^3}{6}\Big|_0^1 \\ &= \frac{5}{6}. \end{aligned}$$

2 Logical Equivalence?

Note 1

Decide whether each of the following logical equivalences is correct and justify your answer.

(a) $\forall x\ (P(x) \land Q(x)) \stackrel{?}{\equiv} \forall x\, P(x) \land \forall x\, Q(x)$

(b) $\forall x\ (P(x) \lor Q(x)) \stackrel{?}{\equiv} \forall x\, P(x) \lor \forall x\, Q(x)$

(c) $\exists x\ (P(x) \lor Q(x)) \stackrel{?}{\equiv} \exists x\, P(x) \lor \exists x\, Q(x)$

(d) $\exists x\ (P(x) \land Q(x)) \stackrel{?}{\equiv} \exists x\, P(x) \land \exists x\, Q(x)$

Solution:

(a) **Correct**.

Assume that the left hand side is true. Then we know for an arbitrary x $P(x) \land Q(x)$ is true. This means that both $\forall x P(x)$ and $\forall x Q(x)$. Therefore the right hand side is true. Now for the other direction assume that the right hand side is true. Since for any x $P(x)$ and for any y $Q(y)$ holds, then for an arbitrary x both $P(x)$ and $Q(x)$ must be true. Thus the left hand side is true.

(b) **Incorrect**.

Note that there are many possible counterexamples not described here.

Suppose that the universe (i.e. the values that x can take on) is $\{1,2\}$ and that P and Q are truth functions defined on this universe. If we set $P(1)$ to be true, $Q(1)$ to be false, $P(2)$ to be false and $Q(2)$ to be true, the left-hand side will be true, but the right-hand side will be false. Hence, we can find a universe and truth functions P and Q for which these two expressions have different values, so they must be different.

Another more concrete example is if $P(x) = x < 0$ and $Q(x) = x \geq 0$, where the universe is the real numbers. For any $x \in \mathbb{R}$, exactly one of $P(x)$ or $Q(x)$ is true, but it is not the case that $P(x)$ holds for every x, and it is also not the case that $Q(x)$ holds for every x. Since the LHS and RHS have different values, the two sides are not equivalent.

(c) **Correct**

Assuming that the left hand side is true, we know there exists some x such that one of $P(x)$ and $Q(x)$ is true. Thus $\exists x P(x)$ or $\exists x Q(x)$ and the right hand side is true. To prove the other direction, assume the left hand side is false. Then there does not exists an x for which $P(x) \lor Q(x)$ is true, which means there is no x for which $P(x)$ or $Q(x)$ is true. Therefore the right hand side is false.

(d) **Incorrect**.

Note, there are many possible counterexamples not described here.

Suppose that the universe (i.e. the values that x can take on) is the natural numbers $\mathbb{N}$, and that P and Q are truth functions defined on this universe. Here, suppose we set $P(1)$ to be true and

$P(x)$ to be false for all other x, and $Q(2)$ to be true and $Q(x)$ to be false for all other x. (In other words, $P(x) = (x = 1)$ and $Q(x) = (x = 2)$.)

With these definitions, the right hand side would be true, since there exists some value of x that makes $P(x)$ true (namely, $x = 1$), and there exists some value of x that makes $Q(x)$ true (namely, $x = 2$). However, there would be no value of x at which both $P(x)$ and $Q(x)$ would be simultaneously true, so the left hand side would be false. Hence, we can find a universe and truth functions P and Q for which these two expressions have different values, so they must be different.

3 Equivalences with Quantifiers

Note 1 Evaluate whether the expressions on the left and right sides are equivalent in each part, and briefly justify your answers.

(a) $\forall x \exists y\, (P(x) \implies Q(x,y)) \stackrel{?}{\equiv} \forall x\, (P(x) \implies \exists y\, Q(x,y))$

(b) $\forall x\, ((\exists y\, Q(x,y)) \implies P(x)) \stackrel{?}{\equiv} \forall x \exists y\, (Q(x,y) \implies P(x))$

(c) $\neg \exists x \forall y\, (P(x,y) \implies \neg Q(x,y)) \stackrel{?}{\equiv} \forall x\, ((\exists y\, P(x,y)) \wedge (\exists y\, Q(x,y)))$

Solution:

(a) Equivalent.

Justification: We can rewrite the left side as

$$\forall x \exists y\, (P(x) \implies Q(x,y)) \equiv \forall x \exists y (\neg P(x) \vee Q(x,y)).$$

We can also rewrite the right side as

$$\forall x\, (P(x) \implies \exists y\, Q(x,y)) \equiv \forall x (\neg P(x) \vee \exists y\, Q(x,y)).$$

Clearly, the two sides are the same if $\neg P(x)$ is true. If $\neg P(x)$ is false, then the two sides are still the same, because

$$\forall x \exists y\, (\text{False} \vee Q(x,y)) \equiv \forall x \exists y Q(x,y) \equiv \forall x\, (\text{False} \vee (\exists y\, Q(x,y)))\,.$$

(b) Not equivalent.

Justification: We can rewrite the left side as

$$\begin{aligned}
\forall x\, ((\exists y\, Q(x,y)) \implies P(x)) &\equiv \forall x\, ((\neg(\exists y\, Q(x,y))) \vee P(x)) \\
&\equiv \forall x\, ((\forall y\, \neg Q(x,y)) \vee P(x)) \\
&\equiv \forall x \forall y\, (\neg Q(x,y) \vee P(x))\,,
\end{aligned}$$

noting that we can extract the $\forall y$ out of the inner $\vee$ expression, since $P(x)$ does not depend on y. (This can be shown in a similar fashion as the previous part.)

We can also rewrite the right side as

$$\forall x \exists y \, (Q(x,y) \implies P(x)) \equiv \forall x \exists y \, (\neg Q(x,y) \vee P(x)) \, .$$

This gives us

$$\forall x \forall y \, (\neg Q(x,y) \vee P(x)) \not\equiv \forall x \exists y \, (\neg Q(x,y) \vee P(x)) \, ,$$

so the two sides are not equivalent.

Another approach to the problem is to consider a linguistic example. Let x and y span the universe of all people, and let $Q(x,y)$ mean "Person x is Person y's offspring", and let $P(x)$ mean "Person x likes tofu".

The right side claims that, for all Persons x, there exists some Person y such that either Person x is not Person y's offspring or that Person x likes tofu.

The left side claims that, for all Persons x, if there exists a parent of Person x, then Person x likes tofu.

It should be clear that these are not the same.

(c) Not equivalent.

Justification: Using De Morgan's Laws to distribute the negation on the left side yields

$$\begin{aligned} \neg \exists x \forall y (P(x,y) \implies \neg Q(x,y)) &\equiv \forall x \neg \forall y (P(x,y) \implies \neg Q(x,y)) \\ &\equiv \forall x \exists y \neg (P(x,y) \implies \neg Q(x,y)) \\ &\equiv \forall x \exists y \neg (\neg P(x,y) \vee \neg Q(x,y)) \\ &\equiv \forall x \exists y (P(x,y) \wedge Q(x,y)) \end{aligned}$$

But $\exists$ does not distribute over $\wedge$. There could exist different values of y such that $P(x,y)$ and $Q(x,y)$ for a given x, but not necessarily the same value. This means that the two sides are not equivalent.

4 Prove or Disprove

Note 2

For each of the following, either prove the statement, or disprove by finding a counterexample.

(a) $(\forall n \in \mathbb{N})$ if n is odd then $n^2 + 4n$ is odd.

(b) $(\forall a, b \in \mathbb{R})$ if $a + b \leq 15$ then $a \leq 11$ or $b \leq 4$.

(c) $(\forall r \in \mathbb{R})$ if r^2 is irrational, then r is irrational.

(d) $(\forall n \in \mathbb{Z}^+)$ $5n^3 > n!$. (Note: $\mathbb{Z}^+$ is the set of positive integers)

(e) The product of a non-zero rational number and an irrational number is irrational.

Solution:

(a) **Answer**: True.

Proof. We will use a direct proof. Assume n is odd. By the definition of odd numbers, $n = 2k+1$ for some natural number k. This means that we have

$$\begin{aligned} n^2+4n &= (2k+1)^2+4(2k+1) \\ &= 4k^2+12k+5 \\ &= 2(2k^2+6k+2)+1 \end{aligned}$$

Since $2k^2+6k+2$ is a natural number, by the definition of odd numbers, n^2+4n is odd.

Alternatively, we could also factor the expression to get $n(n+4)$. Since n is odd, $n+4$ is also odd. The product of 2 odd numbers is also an odd number. Hence n^2+4n is odd. $\square$

(b) **Answer**: True.

Proof. We will use a proof by contraposition. Suppose that $a > 11$ and $b > 4$ (note that this is equivalent to $\neg(a \leq 11 \vee b \leq 4)$). Since $a > 11$ and $b > 4$, $a+b > 15$ (note that $a+b > 15$ is equivalent to $\neg\big(a+b \leq 15\big)$). Thus, if $a+b \leq 15$, then $a \leq 11$ or $b \leq 4$. $\square$

(c) **Answer**: True.

Proof. We will use a proof by contraposition. Assume that r is rational. Since r is rational, it can be written in the form $\frac{a}{b}$ where a and b are integers with $b \neq 0$. Then r^2 can be written as $\frac{a^2}{b^2}$. By the definition of rational numbers, r^2 is a rational number, since both a^2 and b^2 are integers, with $b \neq 0$. By contraposition, if r^2 is irrational, then r is irrational. $\square$

(d) **Answer**: False.

Proof. We will show a counterexample. Let $n = 7$. Here, $5 \cdot 7^3 = 1715$, but $7! = 5040$. Since $5n^3 < n!$, the claim is false.

A counterexample that is easier to see without much calculation is for a much larger number like $n = 100$; here, $100!$ is clearly more than $5 \cdot 100^3 = 100 \cdot 50 \cdot 25 \cdot 5 \cdot 4 \cdot 2$, since the latter product contains only a subset of the terms in $100!$. $\square$

(e) **Answer**: True.

Proof. We prove the statement by contradiction. Suppose that $ab = c$, where $a \neq 0$ is rational, b is irrational, and c is rational. Since a and b are not zero (because 0 is rational), c is also non-zero. Thus, we can express $a = \frac{p}{q}$ and $c = \frac{r}{s}$, where $p, q, r,$ and s are nonzero integers. Then

$$b = \frac{c}{a} = \frac{rq}{ps},$$

which is the ratio of two nonzero integers, giving that b is rational. This contradicts our initial assumption, so we conclude that the product of a nonzero rational number and an irrational number is irrational. $\square$

5 Twin Primes

Note 2

(a) Let $p > 3$ be a prime. Prove that p is of the form $3k+1$ or $3k-1$ for some integer k.

(b) *Twin primes* are pairs of prime numbers p and q that have a difference of 2. Use part (a) to prove that 5 is the only prime number that takes part in two different twin prime pairs.

Solution:

(a) First we note that any integer can be written in one of the forms $3k$, $3k+1$, or $3k+2$. (Note that $3k+2$ is equal to $3(k+1)-1$. Since k is arbitary, we can treat these as equivalent forms).

We can now prove the contrapositive: that any integer $m > 3$ of the form $3k$ must be composite. Any such integer is divisible by 3, so this is true right away. Thus our original claim is true as well.

(b) We can check all the primes up to 5 to see that of these, only 5 takes part in two twin prime pairs (3,5 and 5,7). What about primes > 5?

For any prime $m > 5$, we can check if $m+2$ and $m-2$ are both prime. Note that if $m > 5$, then $m+2 > 3$ and $m-2 > 3$ so we can apply part (a) and we can do a proof by cases based on the two forms from part (a).

Case 1: m is of the form $3k+1$. Then $m+2 = 3k+3$, which is divisible by 3. So $m+2$ is not prime.

Case 2: m is of the form $3k-1$. Then $m-2 = 3k-3$, which is divisible by 3. So $m-2$ is not prime.

So in either case, at least one of $m+2$ and $m-2$ is not prime.

6 Preserving Set Operations

Note 0
Note 2

For a function f, define the image of a set X to be the set $f(X) = \{y \mid y = f(x) \text{ for some } x \in X\}$. Define the inverse image or preimage of a set Y to be the set $f^{-1}(Y) = \{x \mid f(x) \in Y\}$. Prove the following statements, in which A and B are sets. By doing so, you will show that inverse images preserve set operations, but images typically do not.

Recall: For sets X and Y, $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$. To prove that $X \subseteq Y$, it is sufficient to show that $(\forall x)\ ((x \in X) \implies (x \in Y))$.

(a) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.

(b) $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$.

(c) $f(A \cap B) \subseteq f(A) \cap f(B)$, and give an example where equality does not hold.

(d) $f(A \setminus B) \supseteq f(A) \setminus f(B)$, and give an example where equality does not hold.

Solution:

In order to prove equality $A = B$, we need to prove that A is a subset of B, $A \subseteq B$ and that B is a subset of A, $B \subseteq A$. To prove that LHS is a subset of RHS we need to prove that if an element is a member of LHS then it is also an element of the RHS.

(a) Suppose x is such that $f(x) \in A \cap B$. Then $f(x)$ lies in both A and B, so x lies in both $f^{-1}(A)$ and $f^{-1}(B)$, so $x \in f^{-1}(A) \cap f^{-1}(B)$. So $f^{-1}(A \cap B) \subseteq f^{-1}(A) \cap f^{-1}(B)$.

Now, suppose that $x \in f^{-1}(A) \cap f^{-1}(B)$. Then, x is in both $f^{-1}(A)$ and $f^{-1}(B)$, so $f(x) \in A$ and $f(x) \in B$, so $f(x) \in A \cap B$, so $x \in f^{-1}(A \cap B)$. So $f^{-1}(A) \cap f^{-1}(B) \subseteq f^{-1}(A \cap B)$.

(b) Suppose x is such that $f(x) \in A \setminus B$. Then, $f(x) \in A$ and $f(x) \notin B$, which means that $x \in f^{-1}(A)$ and $x \notin f^{-1}(B)$, which means that $x \in f^{-1}(A) \setminus f^{-1}(B)$. So $f^{-1}(A \setminus B) \subseteq f^{-1}(A) \setminus f^{-1}(B)$.

Now, suppose that $x \in f^{-1}(A) \setminus f^{-1}(B)$. Then, $x \in f^{-1}(A)$ and $x \notin f^{-1}(B)$, so $f(x) \in A$ and $f(x) \notin B$, so $f(x) \in A \setminus B$, so $x \in f^{-1}(A \setminus B)$. So $f^{-1}(A) \setminus f^{-1}(B) \subseteq f^{-1}(A \setminus B)$.

(c) Suppose $x \in A \cap B$. Then, x lies in both A and B, so $f(x)$ lies in both $f(A)$ and $f(B)$, so $f(x) \in f(A) \cap f(B)$. Hence, $f(A \cap B) \subseteq f(A) \cap f(B)$.

Consider when there are elements $a \in A$ and $b \in B$ with $f(a) = f(b)$, but A and B are disjoint. Here, $f(a) = f(b) \in f(A) \cap f(B)$, but $f(A \cap B)$ is empty (since $A \cap B$ is empty).

For a more concrete counterexample, suppose $f(x) = |x|$, $A = \{x \in \mathbb{R} \mid x > 0\}$, and $B = \{x \in \mathbb{R} \mid x < 0\}$. Here, $f(A \cap B) = \varnothing$ since $A \cap B$ is empty, but $f(A) = f(B) = A$.

(d) Suppose $y \in f(A) \setminus f(B)$. Since y is not in $f(B)$, there are no elements in B which map to y. Let x be any element of A that maps to y; by the previous sentence, x cannot lie in B. Hence, $x \in A \setminus B$, so $y \in f(A \setminus B)$. Hence, $f(A) \setminus f(B) \subseteq f(A \setminus B)$.

Consider when $B = \{0\}$ and $A = \{0, 1\}$, with $f(0) = f(1) = 0$. One has $A \setminus B = \{1\}$, so $f(A \setminus B) = \{0\}$. However, $f(A) = f(B) = \{0\}$, so $f(A) \setminus f(B) = \varnothing$.

For another counterexample, suppose again that $f(x) = |x|$, $A = \{x \in \mathbb{R} \mid x > 0\}$, and $B = \{x \in \mathbb{R} \mid x < 0\}$. Here, $f(A \setminus B) = f(A) = A$, but $f(A) \setminus f(B) = A \setminus A = \varnothing$.

The purpose of this problem is to gain familiarity to naming thing precisely. In particular, we named an element in the LHS (or the pre-image of the LHS) and then argued about whether that element or its image was in the right hand side. By explicitly naming an element generically where it could be *any element in the set, we could argue about its membership in a set and or its image or preimage. With these different concepts floating around it is helpful to be clear in the argument.*