

NAME: _____

SPIRE ID: _____

COMPSCI 250
Introduction to Computation
SOLUTIONS to First Midterm Fall 2024

D. A. M. Barrington and M. Golin

10 October 2024

DIRECTIONS:

- Answer the problems on the exam pages.
- There are four problems on pages 2-9, some with multiple parts, for 100 total points plus 5 extra credit. Final scale will be determined after the exam.
- Page 10 contains useful definitions and is given to you separately – do not put answers on it!
- If you need extra space use the back of a page – both sides are scanned.
But, if you do write on the back, you must explicitly have a note on the front stating that you used the back page.
- No books, notes, calculators, or collaboration.
- In case of a numerical answer, an arithmetic expression like “ $2^{17} - 4$ ” need not be reduced to a single integer.
- Your answers must be LEGIBLE, and not cramped. Write only short paragraphs with space between paragraphs

1	/10
2	/10
3	/20
4	/20
5	/20+5
6	/20
Total	/100+5

Dave's dogs Blaze and Rhonda are each served a meal in the morning, in the afternoon, and in the evening. Each is given their own bowl, but they do not always each eat their own food. In this problem you will determine which dog ate which meal at which time on a particular day.

Let D be the set $\{B, R\}$ of dogs consisting of Blaze and Rhonda. Let T be the set $\{m, a, e\}$ of meal times, consisting of "morning", "afternoon", and "evening". Let $A \subseteq D \times D \times T$ be a relation such that $A(x, y, t)$ means "dog x ate the designated meal for dog y at time t ".

Question 1 (10): (Translations) Translate each statement as according to the directions:

- (a, 2) (to symbols) (Statement I)

Rhonda ate Blaze's food in the morning, and if she did not also eat her own food in the morning, then she did not eat Blaze's food in the morning.

$$A(r, b, m) \wedge (\neg A(r, r, m) \rightarrow \neg A(r, b, m))$$

It was important that you need the right parentheses, so that $A(r, b, a)$ is definitely true. There were 27% wrong answers on this part, mostly either leaving off the parens or putting them in the wrong place. Many of those people with their bad translation for Q2 and got into serious trouble.

- (b, 2) (to English) (Statement II)

$$A(r, r, a) \rightarrow (A(r, b, m) \wedge \neg A(r, r, m))$$

If Rhonda ate her own food in the afternoon, then Rhonda ate Blaze's food in the morning but did not eat her own food in the morning.

This went well, with only 5% wrong.

- (c, 2) (to symbols) (Statement III)

At each time, each dog's meal was eaten by exactly one dog.

$$\forall t : \forall y : \exists x : \forall z : A(z, y, t) \leftrightarrow (z = x).$$

This was a hard question, and 77% of you got it wrong in one way or another. The most common error I marked was "need a for-all quantifier on a dog" – the four quantifiers in my solution above are all necessary, and the existential quantifier has to come in the right place. There are many other ways to write this, some by using the fact there are only two dogs in the set and using boolean operations instead of the quantifiers. Perhaps the shortest solution is $\forall t : \forall m : A(b, m, t) \oplus A(r, m, t)$, meaning "for any time and any meal, Blaze or Rhonda ate it, but not both".

- (d, 2) (to English) (Statement IV)

$$\forall t : A(b, b, t) \leftrightarrow (t = e)$$

Blaze ate her own food at a mealtime if and only if it was evening.

Here 35% of you were wrong, and my most common comment was “no \leftrightarrow ”, meaning that your version does not say both that Blaze ate it then and didn't eat it at other times.

- (e, 2) (to symbols) (Statement V)

At every meal time, Rhonda ate at least one meal.

$$\forall t : \exists y : A(r, y, t)$$

These were pretty good, some using quantifiers as I do above and some using boolean operations. There were 21% wrong.

Question 2 (10): (Boolean Proof) Both Questions 2 and 3 use the definitions, predicates, and statements above.

Using *only* Statements I and II, **prove** the truth value of each of the three propositions $p = A(r, b, m)$, $q = A(r, r, m)$, and $r = A(r, r, a)$.

You may use a truth table or a deductive sequence proof. Don't forget that if you use a deductive sequence proof, your argument must show both that your solution satisfies both of the statements, and that there is no other solution.

To keep you from getting off track for Question 3, we're going to tell you that p and q are true, and that r is false. But your answer to *this* question should prove those three assertions, not assume them.

Here's a truth table, using my format:

p	q	r	$(p \wedge (\neg q \rightarrow \neg p))$	\wedge	$(r \rightarrow (p \wedge \neg q))$
0	0	0	0	0	1
0	0	1	0	0	1
0	1	0	0	0	1
0	1	1	0	0	1
1	0	0	1	0	0
1	0	1	1	0	0
1	1	0	1	1	0
1	1	1	1	1	0

And here is a deductive proof:

From Statement I, derive p by Left Separation, $\neg q \rightarrow \neg p$ by Right Separation, $p \rightarrow q$ by Contrapositive, and q by Modus Ponens. If we then assume r , we derive a contradiction by using Modus Ponens on Statement II, getting $p \wedge \neg q$ and then $\neg q$ by Right Separation, contradicting q . So r must be false, by Contradiction.

For verification, Statement I evaluates to $1 \wedge (1 \rightarrow 1) \equiv 1$, and Statement II is true vacuously.

Here 27% of you got full credit, and an additional 42% of you got 9/10 because you gave a correct deductive proof but didn't make the check that your solution satisfied the statements. (I occasionally overlook such a check – if you think I did that, file a regrade request.) This is the first time we gave you the answer for the boolean dog proof, in the hope of cutting down cascading errors in the predicate proof. The drawback of this is that some of you tried to bluff when you didn't know how to do the proof, and it took some effort on my part to spot these bluffs, and to check the truth tables.

As usual, there are a variety of correct deductive proofs along with the one above.

Question 3 (20) (Predicate Proof) : This question also uses the definitions, predicates, and statements above. Now assume that all of Statements I-V are true. (You may quote the results of Question 2, given above, whether or not you proved them.)

Determine all twelve truth values for the relation A . That is, for all dogs x , for all dogs y , and all times t , determine the value of $A(x, y, t)$. To show your answer, for each of the 12 propositions, you should circle either True or False appropriately in the table below.

Each entry in the table needs to be justified, either from the premises or from answers that you have already determined. Since many of the premises involve quantifiers, your justifications will involve quantifier proofs as are typical in dog proofs in this course. Your justifications may use either English or symbolic notation, or a combination of both, but it should be clear to the reader when you are using each of the quantifier rules.

$A(b, b, m)$	True / False
$A(r, b, m)$	True / False
$A(r, r, m)$	True / False
$A(b, r, m)$	True / False
$A(b, b, a)$	True / False
$A(r, b, a)$	True / False
$A(r, r, a)$	True / False
$A(b, r, a)$	True / False
$A(b, b, e)$	True / False
$A(r, b, e)$	True / False
$A(r, r, e)$	True / False
$A(b, r, e)$	True / False

From Statements I and II, via Question 2, we know that $A(r, b, m)$ and $A(r, r, m)$ are true but $A(r, r, a)$ is false.

Statement IV tells us that $A(b, b, m)$ and $A(b, b, a)$ are false, but $A(b, b, e)$ is true.

Statement III, by Specification on $x = b$ and $t = e$, says that $A(r, b, e)$ is false because $A(b, b, e)$ is true.

Statement V, first Specification first on a and then on e , tells us that $A(r, b, a)$ is true (because $A(r, r, a)$ is false) and that $A(r, r, e)$ is true (because $A(r, b, e)$ is false).

Now, by Statement III, Specifying each of the three times in turn, $A(b, r, m)$ is false because $A(r, r, m)$ is true, $A(b, r, a)$ is true because $A(r, r, a)$ is false, and $A(b, r, e)$ is false because $A(r, r, e)$ is true.

So these were generally pretty good, with 73% getting 20/20, and a mean score of 18/20. There were better and worse answers among the correct ones, and perhaps I should have been harsher on overly terse answers. It was easy to tell whether your overall answer was correct, and then I had to determine whether your justification was convincing. The more clearly organized that was, the easier was the grading, and a lot of them were pretty well organized. Note that there were several different approaches to doing the proof, only one of which is given above.

Question 4 (20): (Binary Relations on a Set) Parts (a) and (b) deal with two binary relations P and Q , each from the same set $A = \{a, b, c, d\}$ to itself. Part (a) is on this page, part (b) on the next.

(a, 10) The relation $P \subseteq A \times A$ is a **partial order**.

It is known that $(b, c) \in P$, $(d, c) \in P$, $(c, a) \in P$ and $(a, c) \notin P$.

(i) In the table given below label all pairs that must be in P with a “ \checkmark ” and all pairs that cannot be in P with a “ \times .” For pairs that are neither, leave their entry blank. We start you off by labelling the four known pairs with the appropriate “ \checkmark ” or \times .

Justify your answers. That is, you must provide a brief explanation as to why each of the pairs you marked “ \checkmark ” are in P and those you marked “ \times ” are not in P .

Your explanations must reference the properties of P that are being used. They must also be consistent. That is, if you somewhere use the fact that $(x, y) \notin P$ where $(x, y) \neq (a, c)$, then you must have already previously proven that $(x, y) \notin P$.

(ii) How many partial orders P exist that satisfy $(b, c) \in P$, $(d, c) \in P$, $(c, a) \in P$ and $(a, c) \notin P$? Briefly explain how you know this.

(a, a)	(a, b)	(a, c)	(a, d)	(b, a)	(b, b)	(b, c)	(b, d)	(c, a)	(c, b)	(c, c)	(c, d)	(d, a)	(d, b)	(d, c)	(d, d)
		\times				\checkmark		\checkmark						\checkmark	

Solution:

i) Because P is a partial order, it is reflexive, anti-symmetric and transitive.

- From the reflexivity, $(x, x) \in P$ for all $x \in A$.
- From the transitivity: $(b, a) \in P$ from $(b, c), (c, a) \in P$; and $(d, a) \in P$ from $(d, c), (c, a) \in P$
- From the antisymmetry: all of $(a, b), (a, c), (a, d), (c, b), (c, d) \notin P$.

(a, a)	(a, b)	(a, c)	(a, d)	(b, a)	(b, b)	(b, c)	(b, d)	(c, a)	(c, b)	(c, c)	(c, d)	(d, a)	(d, b)	(d, c)	(d, d)
\checkmark	\times	\times	\times	\checkmark	\checkmark	\checkmark		\checkmark	\times	\checkmark	\times	\checkmark		\checkmark	\checkmark

ii) From part (i) we know that ANY partial order that satisfies the conditions must have all of the boxes, except (b, d) and (d, b) , filled in as shown. Furthermore, any partial order that has those boxes filled that way, is consistent with P .

The only flexibility is in how to fill in those two boxes (remaining consistent with the rules of partial orders).

There are three possible partial orders. These result by choosing exactly one of the following statements: (i) $(b, d) \in P$, and $(d, b) \notin P$, (ii) $(d, b) \in P$ and $(b, d) \notin P$, or (iii) $(b, d) \notin P$ and $(d, b) \notin P$.

(b, 10) The relation $Q \subseteq A \times A$ is an **equivalence relation**.
It is known that $(a, c) \in Q$, $(b, c) \in Q$ and $(a, d) \notin Q$.

(i) In the table given below, label all pairs that must be in Q with a “ \checkmark ” and all pairs that cannot be in Q with a “ \times .” For pairs that are neither, leave their entry blank. We start you off by labelling the three known pairs with the appropriate “ \checkmark ” or “ \times .”

Justify your answers following the same rules that were given in part (a).

(ii) How many partial orders Q exist that satisfy $(a, c) \in Q$, $(b, c) \in Q$, and $(a, d) \notin Q$? Briefly explain how you know this.

(a, a)	(a, b)	(a, c)	(a, d)	(b, a)	(b, b)	(b, c)	(b, d)	(c, a)	(c, b)	(c, c)	(c, d)	(d, a)	(d, b)	(d, c)	(d, d)
		\checkmark	\times			\checkmark									

Solution:

i) Because Q is an equivalence relation, it is reflexive, symmetric and transitive.

- From reflexivity, $(x, x) \in Q$ for all $x \in A$.
- From symmetry, (c, a) , and (c, b) are in Q and $(d, a) \notin Q$.
- From Transitivity, $(a, c) \in Q$ and $(c, b) \in Q$ imply $(a, b) \in Q$.
Symmetry then implies $(b, a) \in Q$
- If $(d, b) \in Q$ then, by transitivity with known $(b, a) \in Q$, $(d, a) \in Q$.
This contradicts known $(d, a) \notin A$. So $(d, b) \notin Q$
By symmetry $(b, d) \notin Q$
- If $(d, c) \in Q$ then, by transitivity with known $(c, a) \in Q$, $(d, a) \in Q$.
This contradicts known $(d, a) \notin A$. So $(d, c) \notin Q$
By symmetry $(c, d) \notin Q$

(a, a)	(a, b)	(a, c)	(a, d)	(b, a)	(b, b)	(b, c)	(b, d)	(c, a)	(c, b)	(c, c)	(c, d)	(d, a)	(d, b)	(d, c)	(d, d)
\checkmark	\checkmark	\checkmark	\times	\checkmark	\checkmark	\checkmark	\times	\checkmark	\checkmark	\checkmark	\times	\times	\times	\times	\checkmark

ii) Since all of the boxes have been filled in, this is the only relation Q that satisfies the conditions. So, there is only 1.

Grading Notes.

4.1: Full marks required full justifications.

For example, just saying in part a(i) that (b, a) exists because of transitivity, wasn't enough. You needed to write the full details, e.g., $(b, a) \in P$ follows from $(b, c), (c, a) \in P$ and transitivity.

Another related justification issue, again with example from a(i), is not performing the justifications in correct order. The example here is that you must justify that $(b, a) \in P$ using transitivity BEFORE justifying that $(a, b) \notin P$ due to anti-symmetry.

4.2: In both parts (a) and (b) some students left blank some pairs that could be proven false, instead of writing a \times and/or proving that they were false in the text.

For example, in (b) they left $(b, d), (c, d), (d, b), (d, c)$ blank. Showing that non of those could be in Q (due to transitivity) was a major part of the solution and not stating that resulted in points being deducted.

Question 5 (20+5): (Number Theory)

- (a, 4) In the box below, write down the complete statement of the Chinese Remainder Theorem (for two moduli) as it was taught in class. Be careful to explicitly state the conditions required to be able to use it.

Solution:

**If m and n are relatively prime positive naturals,
and $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ are two congruences,**

**then there exists some number c such that x satisfies the two congruences if
and only if $x \equiv c \pmod{mn}$.**

- (b, 8) The naturals 102 and 23 are relatively prime.
Use the Extended GCD algorithm as taught in class to find integers a and b satisfying the equation $102 \cdot a + 23 \cdot b = 1$. Show all of your work.

Solution:

$$\begin{array}{rcl}
 102 & = & 4 \cdot 23 + 10 \\
 23 & = & 2 \cdot 10 + 3 \\
 10 & = & 3 \cdot 3 + 1
 \end{array}
 \qquad
 \begin{array}{rcl}
 10 & = & 102 - 4 \cdot 23 \\
 3 & = & 23 - 2 \cdot 10 = 23 - 2(102 - 4 \cdot 23) = -2 \cdot 102 + 9 \cdot 23 \\
 1 & = & 10 - 3 \cdot 3 = (102 - 4 \cdot 23) - 3(-2 \cdot 102 + 9 \cdot 23) = 7 \cdot 102 - 31 \cdot 23.
 \end{array}$$

So $a = 7$ and $b = -31$.

- (c, 4) Using the results from the previous part, determine both an inverse of 23 modulo 102 and an inverse of 102 modulo 23.
For full credit, your answers should each be the smallest natural numbers that are inverses.

Solution: 7 is an inverse of 102 modulo 23.

-31 is an inverse of 23 modulo 102 but is not a natural. All inverses of 23 modulo 102 must be congruent to -31 modulo 102. So, $71 = -31 + 102$ is the smallest natural inverse of 23 modulo 102

- (d, 4) Using the results from the previous parts, determine the smallest natural x that solves both the congruences

$$x \equiv 2 \pmod{23} \quad \text{and} \quad x \equiv 1 \pmod{102}.$$

Solution:

$715 = 2 \cdot 7 \cdot 102 - 31 \cdot 23$ is a solution to the congruences.

Since *every* solution to the congruences must be of the form $715 + k \cdot 23 \cdot 102$, we can see that 715 is the answer since $715 - 1 \cdot 23 \cdot 102 < 0$

- (e, 5 extra credit) Find the smallest natural y that satisfies both the congruences in part (d) and also has a decimal representation ending in 9 (that is, $y \equiv 9 \pmod{10}$). Remember that you may give the result as an arithmetic expression, as long as you justify it.

Solution: As noted in the previous section, all solutions are in the form $715 + k \cdot 23 \cdot 102$ with 715 being the smallest natural in that form.

The solution to this problem must therefore have $k > 0$.

In addition, if we are only interested in the last digit, we must have that the last digit of $k \cdot 23 \cdot 102$ is 4, i.e., $k \cdot 3 \cdot 2$ having a last digit 4 i.e., $6k$ having a last digit 4.

This means that $k = 4$ and the answer will be $715 + 4 \cdot 23 \cdot 102$. Writing that would solve the problem.

Calculation gives $715 + 4 \cdot 23 \cdot 102 = 10099$ but, without a calculator, we weren't asking you to do this calculation.

Grading note: The Chinese remainder theorem could NOT be used here because 102 and 10 are not relatively prime.

Grading Notes: To receive full points for part (a) it was necessary to state that all solutions to the two congruences will satisfy $x \equiv c \pmod{mn}$, i.e., no other solutions exist. That's what the "if and only if" was there for.

More specifically, the statement of the CRT can be abstracted as

*"If $\gcd(m, n) = 1$, then,
for every a and b , there exists a constant c dependent upon m and n , such that
 x satisfies condition A
if and only if
 x satisfies Condition B.
"*

*where $\gcd(m, n)$ could be replaced by "m and n are relatively prime",
Condition A is that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$
and Condition B is that $x \equiv c \pmod{mn}$.*

It was necessary to be clear about what was being assumed and what was being proven. Some students started their statement by assuming that an x existed solving $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$, i.e., that x satisfied Condition A. That would be incorrect.

The ONLY correct initial assumption for the CRT was that $\gcd(m, n) = 1$.

The conclusion was that "Condition A is equivalent to Condition B".

It was also acceptable to write as a conclusion the logically equivalent statement that "any pair of congruences as described in Condition A have a joint solution and the set of solutions is EXACTLY the set of x that satisfy Condition B".

If your formulation was ambiguous about distinguishing between the assumptions and the conclusions, points were deducted.

Question 6 (20): The following are ten true/false questions, with no explanation needed or wanted, no partial credit for wrong answers, and no penalty for guessing.

After reading the questions, write the correct answer, either T (for true) or F (for false), in the corresponding column.

(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)

(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
T	F	T	F	F	F	T	F	T	F

- (a) If A is a finite set and R is a relation from A to A , and it is an injection (a one-to-one function), then R is a bijection.

TRUE. Functions with finite domain and codomain of the same size are one-to-one if and only if they are onto.

This had 34% incorrect, which was disappointing because it was a textbook answer.

- (b) If R is a reflexive and transitive relation from A to A and R is not antisymmetric, then R must be symmetric.

FALSE. A counterexample would be $R = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, c)\}$.

Another straightforward one, on which you did better, with only 17% incorrect.

- (c) Recall that " u^R " is the reversal of a string u . If u and v are any strings, then the reversal of the string uvu^R is $uv^R u^R$.

TRUE. The reversal of a concatenation is the concatenation of the reversals, in the opposite order.

These were bad, with 43% incorrect. We mentioned the rule $(uv)^R = v^R u^R$ in the textbook, and we'll come back to in Lecture 19, but we didn't have that rule on the slides, which may have been part of the problem.

- (d) The Sieve of Eratosthenes is used to solve a pair of congruences with different prime moduli.

FALSE. The Sieve is actually used to generate a list of all prime numbers of a particular size. The alleged use is part of the Chinese Remainder Theorem.

Someone asked in my (Dave's) lecture "will this (the SoE) be on the exam", so I wanted to ask one that should be easy if you knew anything about it. Since you should have known that the exact statement of the CRT was going to be important, I'm surprised that this one went so badly, with 41% incorrect.

- (e) Let X and Y be any finite sets. Then $|X \setminus Y| \leq |Y|$.

FALSE. It's true that $|X \setminus Y| \leq |X|$, but there are lots of counterexamples to the given statement, starting with Y being empty and X nonempty.

This went well, with only 18% incorrect. If you try a few examples, you should have hit a counterexample pretty quickly.

- (f) Suppose we are trying to prove a compound proposition X (where X involves boolean variables p and q plus possibly others), and our premise is $p \rightarrow q$. Then it is *insufficient* to prove the two cases $(p \wedge q) \rightarrow X$ and $\neg p \rightarrow X$.

FALSE. If $p \rightarrow q$ is true, then either p is false or both p and q are true. So these cases are enough.

So this was the hardest one, with 51% incorrect. The idea was to follow the clicker question about Proof By Cases, but the double negative may have confused some of you.

- (g) For all i in the set $S = \{1, 2, 3, 4\}$, let p_i and q_i each be prime numbers. If $p_1 p_2 p_3 p_4 = q_1 q_2 q_3 q_4$, then the statement $\forall i : \exists j : p_i = q_j$ is true, where the variables range over S . TRUE. This follows from the Fundamental Theorem of Arithmetic.

This had 27% incorrect. I don't know whether the wrong answers came from misinterpreting the quantified statement, or from any actual misunderstanding of the FTA.

- (h) Let A be a finite set. Then the empty string λ is a member of the language A^* if and only if A is non-empty.

FALSE. The empty string is a member of A^* for any set A at all.

This had 33% incorrect. It should be straightforward if you know the definition of the Kleene star operator, or the definition of A^ from the first lecture.*

- (i) There exists a positive natural m (*i.e.*, with $m \geq 1$) such that every prime number falls into the same congruence class modulo m .

TRUE, since if $m = 1$ every number falls into the same congruence class. If $m > 1$, this is true because 2 and 3 will be in different classes.

This, I thought, was the only really nasty trick question. I tried to help you by suggesting that $m = 1$ was one of the cases to consider, but in the event 43% of you got it wrong.

- (j) Let R be a relation from a finite set A to a finite set B . Assume that for every $a \in A$, there exists an element $b \in B$ such that $(a, b) \in R$. Then R is a function if and only if for every $b \in B$, there exists an element $a \in A$ such that $(a, b) \in R$.

FALSE. R is total, but may fail to be well-defined, if both (a, b) and (a, b') are both in R .

It should have been no surprise that you needed to know the definitions of "function", "one-to-one/injection", and "onto/surjection". There were 36% incorrect.

So overall these were disappointing, with a mean of 13/20 and only 7% perfect scores.

COMPSCI 250 First Midterm Supplementary Handout: 10 October 2024

Here are definitions of sets, predicates, and statements used on the exam.

Remember that the scope of any quantifier is always to the end of the statement it is in.

The scenario of Question 1-3 is as follows.

Dave's dogs Blaze and Rhonda are each served a meal in the morning, in the afternoon, and in the evening. Each is given their own bowl, but they do not always each eat their own food. In this problem you will determine which dog ate which meal at which time on a particular day.

Let D be the set $\{B, R\}$ of dogs consisting of Blaze and Rhonda. Let T be the set $\{m, a, e\}$ of meal times, consisting of "morning", "afternoon", and "evening". Let $A \subseteq D \times D \times T$ be a relation such that $A(x, y, t)$ means "dog x ate the designated meal for dog y at time t ".

The five statements of Question 1 are:

- (a, 2) (to symbols) (Statement I)
Rhonda ate Blaze's food in the morning, and if she did not also eat her own food in the morning, then she did not eat Blaze's food in the morning.

- (b, 2) (to English) (Statement II)
 $A(r, r, a) \rightarrow (A(r, b, m) \wedge \neg A(r, r, m))$

- (c, 2) (to symbols) (Statement III)
At each time, each dog's meal was eaten by exactly one dog.

- (d, 2) (to English) (Statement IV)
 $\forall t : (A(b, b, t) \leftrightarrow (t = e))$

- (e, 2) (to symbols) (Statement V)
At every meal time, Rhonda ate at least one meal.