Endterm Reasoning and Logic (CSE1300)

Exam created by Stefan Hugtenburg & Neil Yorke-Smith

Please read the following information carefully!

- This exam consists of 16 multiple-choice questions and 9 open questions.
- The points for the multiple-choice part of the exam are computed as $1 + 9 \cdot \max(0, \frac{\text{score} - 0.25 * 0}{0.75 * 0})$. This accounts for a 25% guessing correction, corresponding to the four-choice questions we use.
- The grade for the open questions is computed as: $1 + 9 \cdot \frac{\text{score}}{65}$.
- The **final grade for the exam** is computed as: $0.4 \cdot MC + 0.6 \cdot Open$.
- This exam corresponds to all non-starred sections of the book: *Delftse Foundations of Computation* (version 1.1).
- You have 3 hours to complete this exam.
- Before you hand in your answers, check that the sheet contains your name and student number, both in the human and computer-readable formats.
- The use of the book, notes, calculators or other sources is **strictly prohibited**.
- Note that the order of the letters next to the boxes on your multiple-choice sheet may **not always be A-B-C-D**! Tip: mark your answers on this exam **first**, and only after you are certain of your answers, copy them to the multiple-choice answer form.
- Read every question properly and in the case of the open questions, give **all information** requested, which should always include a brief explanation of your answer. Do not however give irrelevant information – this could lead to a deduction of points.
- Note that the minimum score per (sub)question is 0 points.
- You may write on this exam paper and take it home.
-

Open questions:

Question:	17	18	19	20	21	22	23	24	25	Total:
Points:	6	6	5	9	6	10	5	6	12	65

Learning goals coverage, based on the objectives of all lectures (strongly paraphrased):

Goal	et 17	mc 18	mt 18	et 18	ret 18	mc 19	mt19	et19
translate logic to and from natural language		1,2	3,4	1	1	1-2,19-20	3,4	1
describe $\wedge$,$\vee$,$\neg$,$\rightarrow$, and $\leftrightarrow$ operators						3		
construct a truth table		3-5	1a,1b	31a	21a	4-5	1a	9,21a
determine prop. logic equivalence		6,7,19		2		6-8	1b	
rewrite logical connectives		8-10		31b	21c	9	1c	21b
describe contrapos, conv, and inv.		11,12			2	10		3
describe logic validity		13,14		3		11,12		
describe sufficient and necessary conditions		15		4		13	2a	
prove validty of argument in prop. logic		16-17	1b		3,21b	14		
describe the principle of explosion		18	1c			15		
explain why prop. logic is not suf. exp.		20					2b	
describe $\forall$ and $\exists$ quantifiers		21	2c	5		19		
evaluate negation stmt. in pred. logic		22			4	17-18		
construct a Tarski's world		23-25				21-22	5b	
construct a formal structure in pred. logic		26-27	2b	32a	22a	23	5a	
evaluate claims about formal structures		28-29	2a	6,32b	22b	24		4
construct counterexamples for claims		30	2a,2b,5c		5	25	6a	22
prove a predicate is satisfiable .							6b	5
describe the number sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$					6			6
describe a proof by div. into cases			5b	7				
describe a proof by contradiction					7		7b	
construct a proof by division into cases			7a				7b	7
construct a proof by contradiction								
describe a proof by contrapositive			5a					
construct a proof by contrapositive			7b				7a	
describe a proof by generalisation .			5a,5b					
construct a proof by generalisation								
construct an existence proof				9				8
identify proof to use for a given claim			5b					
compute a sequence of a rec. def .			6a	10	8		8	
construct/interpret rec. def .	3		6b,6c					
explain the principle of an induction proof	2			11	9			7
construct an ind proof for numbers				33a	23a		2c	23
construct an ind proof for algorithms	4			33b	10			12,26
construct recursive definitions on sets	12a			12,13	23b,24			10-11,27
construct a proof using struct. induction	12b			14,15	23c			19,28
explain and apply basic set operations.	1			16	11			6,29
construct Venn diagrams	5			17,18	12			29
construct ce for claims on sets	1,13			19,34b	25			22
compute the powerset of a set				20,21	13			2,24a
compute the cartesian product of two sets				22	14			20
construct proofs for claims on sets				34a	25			29
describe Cantor's proofs about infinite sets	11b			23	15			13,27
construct f or R from nat. language				24,25	26a			24b
describe the diff. between f and R				35a	16			14
determine the inverse of R and f	8			35b	26b			24c
determine if f is well-defined	6			26	17			15
determine if f is inj., surj., or bij.	7,11a,c			27	18			16
determine if R is sym., trans. or refl.	9			28,29	19			17
describe an equivalence relation	10			30	20,26c			18,25

Multiple-Choice questions

1. Consider the formal structure S with domain $D^S = \mathbb{N}$, and truth sets $P^S = \{0, 1, 3, 4\}$, $Q = \{5, 7, 9, 11\}$, and $R^S = \{(0, 823), (23, 127)\}$.
Which of the following statements is **true** for the structure S? Note carefully the order in which x and y are introduced and used in R!
   - A. $\forall x(P(x) \to \exists y((y < x \lor Q(y)) \land (R(y, x))))$
   - **B.** $\forall y(P(y) \to \exists x((y < x \land Q(x)) \lor (R(x, y))))$
   - C. $\forall x(P(x) \to (\exists y((y < x \land Q(y))) \lor \exists y(R(y, x))))$
   - D. $\forall y(P(y) \to (\exists x((y < x \land Q(x))) \land \exists x(R(x, y))))$

Answer:
- A. Counterexample: For $x = 1$ there is no value for y that makes $R(y, 1)$ true.
- **B. For all values for which P is true, we can take $x = 5$ to make the consequent of the implication true.**
- C. Counterexample: For $x = 1$ there is no value y in Q such that $y < 1$, nor is there a value in R such that $R(y, 1)$ is true.
- D. Counterexample: For $y = 1$ there is no value x such that $R(x, 1)$ is true.

2. Which of the following is **true** when we want to prove a property $Q(x)$ is true for all statements x in PROP?
   - **A. In the induction step we prove that $\forall x \in$ PROP$(Q(x) \to Q(\neg x))$.**
   - B. In the induction step we prove that $\forall x(x \in$ PROP $\to \neg x \in$ PROP $)$.
   - C. In the induction step we prove that $\forall x(Q(x) \in$ PROP $\to Q(\neg x) \in$ PROP $)$.
   - D. In the induction step we prove that if $Q(p_i)$ for a propositional variable p_i, then also $Q(\neg p_i)$.

Answer: Answer A describes exactly what we should do for the first recursive rule of PROP. Answer B is this rule, answer C is nonsense as $Q(x)$ is not in Prop, as $Q(x)$ is a predicate and the last one is not sufficiently generic.

3. Which of the following is **true** about all sets A?
   - A. If $\emptyset \in A$, then there is a set B, such that $\mathscr{P}(B) = A$.
   - **B. If $C \subseteq A$, then there is a set B such that $B \in \mathscr{P}(A)$ and $B \subseteq C$.**
   - C. If $|A|$ is divisible by 4, then there is a set B, such that $\mathscr{P}(B) = A$.
   - D. If there is a set B such that for all $x \in A$: $x \subseteq B$, then $\mathscr{P}(B) = A$.

Answer:
- A. Counterexample: Take $A = \{\emptyset, 1\}$. There is no set such that $1 \subseteq B$.
- **B. Take $B = \emptyset$, now this statement is true for every subset C of A.**
- C. Counterexample: Take $A = \{1, 2, 3, 4\}$. There is no set such that $1 \subseteq B$.
- D. Counterexample: Take $A = B = \emptyset$. Clearly all $x \in A$ are a subset of B, but A is not the power set of B.

4. On the multiple choice test of this course, in question 6 a mistake in the answers argued that $P \to Q \equiv Q \to P$ is not sufficient for $P \leftrightarrow Q$. Why is this a mistake?
   A. Because $(P \to Q) \leftrightarrow (Q \to P)$ is a tautology.
   B. Because $(P \to Q) \leftrightarrow (Q \to P)$ is a contradiction.
   C. Because $((P \to Q) \leftrightarrow (Q \to P)) \to (P \wedge \neg Q)$ is a contradiction.
   D. Because $((P \to Q) \leftrightarrow (Q \to P)) \to (\neg P \vee Q)$ is a contingency.

Answer: Ironically this question again contained a mistake, with no answer being correct.

5. Which of the following statements is **true**?
   A. $\mathbb{R} \subseteq \mathbb{Q}$
   B. $\mathbb{Q} \subseteq (\mathbb{N} \Delta \mathbb{Z})$
   C. $(\mathbb{Z} \setminus \mathbb{Q}) \subseteq \mathbb{N}$
   D. $(\mathbb{Q} \setminus \mathbb{Z}) \subseteq \mathbb{N}$

Answer:
   A. Counterexample: $\pi \in \mathbb{R}$ and $\pi \notin \mathbb{Q}$.
   B. Counterexample: $\frac{4}{3} \in \mathbb{Q}$ and $\frac{4}{3} \notin \mathbb{N}\Delta\mathbb{Z}$.
   C. Correct, $\mathbb{Z} \subset \mathbb{Q}$, so $\mathbb{Z} \setminus \mathbb{Q} = \emptyset$.
   D. Counterexample: $\frac{4}{3} \in \mathbb{Q} \setminus \mathbb{Z}$ and $\frac{4}{3} \notin \mathbb{N}$.

6. Which of the following statements is **true** about an arbitrary statement A?
   A. A is satisfiable iff A is valid.
   B. A is valid iff $\neg A$ is not valid.
   C. A is valid iff $\neg A$ is not satisfiable.
   D. A is satisfiable iff $\neg A$ is not satisfiable.

Answer: From slides of lecture 5:

- satisfiable: **a structure** makes the formula true
- unsatisfiable: **no structure** makes the formula is true
- valid: **every structure** makes the formula true

We can reduce unsatisfiability and validity to SAT solving:

- F is unsatisfiable iff F is not satisfiable (F has no model)
- F is valid iff $\neg F$ is unsatisfiable ($\neg F$ has no model)
  Because: a structure must either make F or $\neg F$ true,
  and thus every structure makes F true.

7. Someone wants to combine a proof by division into cases with a proof by induction to prove the property $P(n)$ for all integers $n \geq 6$. As a result her induction step does the following: "Take arbitrary k, such that $P(k)$ holds. If k is even: then we show $P(k+1)$ holds, if k is odd, then we show $P(k+3)$ holds." Which of the following should they prove in their base case to make the proof valid?

   A. $P(0) \wedge P(1)$

   B. $P(1) \wedge P(4)$

   C. $P(2) \wedge P(5)$

   D. $P(2) \wedge P(6)$

> **Answer:** The sequence we get in the induction step if $k \implies k+1 \implies k+4 \implies k+5 \implies k+8$ (assuming an even k). So starting from 0 and 2 we get:
>
> - $P(0) \implies P(1) \implies P(4) \implies P(5) \implies P(8) \implies P(9)$ etc.
> - $P(2) \implies P(3) \implies P(6) \implies P(7) \implies P(10) \implies P(11)$ etc.
>
> If we have one from each chain, we have all the numbers we need.

8. Let $f(P)$ be the number of ones in the column for the main connective of the compound proposition P, and let $a(P)$ be the number of unique propositional variables in P.
   Which of the following statements is **true**?

   A. If $a(P) = a(Q)$ then $f(P) = f(Q)$.

   B. If $a(P) > a(Q)$, then $f(P \wedge Q) > f(P \vee Q)$.

   C. If $a(P) = a(P \wedge Q)$, then $f(P) \geq f(P \wedge Q)$.

   D. If $a(P) < a(P \vee Q)$, then $f(P) \geq f(P \vee Q)$.

> **Answer:**
>
> A. Counterexample:$P = p \vee \neg p$, $Q = p \wedge \neg p$.
>
> B. Counterexample:$P = p \wedge \neg p \wedge q$, $Q = r$.
>
> **C. Correct, in general $f(P) \geq f(P \wedge Q)$ as an and operation cannot create more truths, provided Q does not introduce new atoms. Since $a(P) = a(P \wedge Q)$ all of the atoms from Q must also appear in P, thus it contains no new atoms.**
>
> D. Counterexample:$P = p$, $Q = q$, now $f(P) = 1$ and $f(P \vee Q) = 3$.

9. Consider the recursively defined set $A \subseteq \mathbb{Z}$ using the rules:

   I. $13 \in A$ and $3 \in A$

   II. $x \in A \rightarrow x - 12 \in A$

   III. $(3x \in A \wedge x \in \mathbb{Z}) \rightarrow x \in A$

   IV. Nothing other than created by the rules above is in A.

   Which of the following is **true**?

   A. $-23 \notin A$

   B. $0 \in A$

   C. $2 \in A$

   D. $25 \notin A$

Answer: Applying rule II gets us $1 \in A$, as well as $-9 \in A$ and a whole lot of negative numbers. Applying rule III gets us $1 \in A$ as well, as well as more negative numbers. So the only non-negative numbers in the set are $1, 3, 13$.

Thus $0 \notin A$, as that would require 12 to be in A or $3 \cdot 0 = 0$ to be in A. Furthermore $-23 \in A$, as we can apply rule 2 twice more on 1 to get $1 - 12 - 12 = -23$. Finally, $2 \notin A$ as that would require 14 to be in A or 6 to be in A. Neither of which can be created either.

10. Someone argues that if we add the rule: $x, y \in A \rightarrow 2x + y \in A$ to the set of rules above, then $A = \mathbb{Z}$. Is this correct?

    A. Yes
    B. No, as $0 \notin A$
    C. No, as $0.5 \notin A$
    D. No, as $5 \notin A$

Answer: Note that $\forall x \in A : 2 \nmid x$. Simplified proof:

Proof. Base case: $2 \nmid 13$ and $2 \nmid 3$ Inductive step: Take arbitrary $x, y \in A$ such that $2 \nmid x, y$. For every rule:

- $x - 12 = 2k + 1 - 12 = 2(k - 6) + 1$ so $2 \nmid x - 12$.
- If $x = 3k$ for some k and since if $2 \nmid 3k$, then $2 \nmid k$.

  Proof. Proof by contrapositive: $2 \mid k \rightarrow 2 \mid 3k$. Take arbitrary m such that $2 \mid m$. Now $3m = 3(2c) = 2(3c) = 2d$, so $2 \mid 3k$. Since the contrapositive is equivalent, and m was arbitrarily chosen <Blah>. QED

  Thus $2 \nmid k$ and thus an odd element is added to A by this rule.
- $2x + y = 2(2k+1) + 2m + 1 = 4k + 2 + 2m + 1 = 2(2k + 1 + m) + 1 = 2d + 1$ thus $2 \nmid 2x + y$.

QED

Hence 0 is not in A. $5 \in A$, as we can get to 9 with the new rule and $x = y = 3$, to 15 with the new rule and $x = 3, y = 9$. Then use rule II to divide by 3 and you get 5.

11. We say a set A is bounded iff $\exists x, y \in \mathbb{R}(\forall a \in A(x < a < y))$. Which of the following statements is **true**?

    A. $\mathbb{N}$ is bounded.
    B. There are finite sets that are **not** bounded.
    C. There are infinitely many bounded infinite sets.
    D. The intersection of a bounded set and an unbounded set is always finite.

Answer:

A. Nope there is no y that works for this.
B. Nope, take $x = \min(A) - 1$ and $y = \max(A) + 1$.
C. Correct for all $n \in \mathbb{N}$ **the set** $\{x \in \mathbb{R} \mid n \leq x \leq n + 1\}$ **is bounded and infinite.**
D. Nope, It is always bounded, but as we have just seen that does not mean it must be finite. Take for example the intersection of $\{x \in \mathbb{R} \mid 1 \leq x \leq 2\}$ and $\mathbb{R}$.

12. Which of the following relations is a well-defined function $f : A \to B$ with $A = \{a, b, c\}$ and $B = \{1, 2, 3\}$.
    A. $L = \emptyset$
    B. $I = \{(a, 1), (a, 2), (a, 3)\}$
    C. $N = \{(a, 1), (b, 1), (c, 1)\}$
    D. $K = \{(1, a), (2, b), (3, c)\}$

Answer:
A. All elements from A must be mapped.
B. All elements from A must be mapped.
C. This is fine.
D. Order matters in tuples.

13. Which of the following statements is **true**?
    A. If $f : A \to B$ and $A = B$, then f is injective.
    B. If $|A| \geq |B|$, then $f : A \to B$ **cannot** be injective.
    C. If $f : A \to B$ is injective and surjective, then $A = B$.
    D. If $f : A \to B$ is surjective and $|A| \geq |B|$, then f is injective.

Answer: This question also had no correct answers unfortunately.
A. Counterexample: $f : \mathbb{N} \to \mathbb{N}$ with $f(x) = 0$.
B. Counterexample: This only holds if $A < |B|$, when they are equal it can be bijective and thus also injective.
C. Counterexample: $f : \mathbb{N} \to \mathbb{Z}$ with $f(x) = \begin{cases} x/2 & \text{if } x \text{ is even} \\ -(x+1)/2 & \text{if } x \text{ is odd} \end{cases}$
D. Counterexample: $f : \{0, 1, 2\} \to \{0, 1\}$ with $f = \{(0, 0), (1, 0), (2, 1)\}$

14. Consider the following propositions:
    - p represents: "(NPC $\cap$ P) $= \emptyset$"
    - q represents: "P $=$ NP"
    - r represents: "You lose all your bitcoin."
    - s represents: "You give out your password."

    Which of the following statements accurately describes the following:
    "If (NPC $\cap$ P) $\neq \emptyset$, then P $=$ NP. If you give out your password or if P $=$ NP, then you lose all your bitcoin."
    A. $(p \to q) \land ((\neg q \lor s) \to r)$
    B. $(\neg p \to q) \land ((q \lor s) \to r)$
    C. $\neg p \to (\neg q \land ((q \lor s) \to r))$
    D. $\neg(p \to q) \land (\neg(q \lor s) \to r)$

> **Answer:** The two sentences should be translated separately and connected by a $\wedge$. Thus we get: $\neg p \to q$ for the first sentence and $(q \vee s) \to r$ for the second.

15. After their many adventures stepping on K-Maps and converting speeds, the Ducks and Sharks have accomplished their mission. On their way home however, the newly created friendship between Donald McDuck and Shirley McShark threatens to break down. They disagree about the notion of equivalence classes. The argument is sparked by the following diagram they find in some street art down at the sea, depicted in Figure 1.

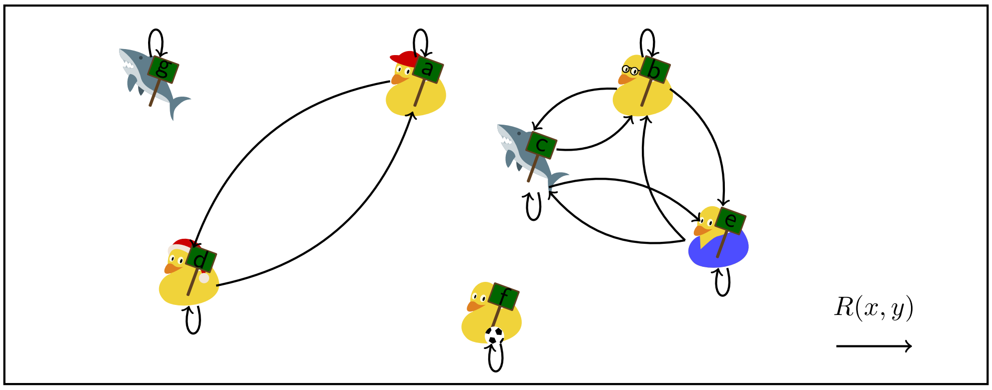


Figure 1: The street art by the sea

Which of the following statements is true about the relation R?

A. $[a] = [f]$ if we just add two elements to R.

B. $[g] = [f]$ if we just add two elements to R.

C. We can half the number of partitions by just adding two elements to R.

D. We can double the number of partitions by just removing two elements from R.

> **Answer:** Simply add $(g, f), (f, g)$.

16. Which of the following is **true**?

A. If $A \subset C$, then $A \times B \subseteq C \times B$.

B. If $A \subseteq B$, then $A \times B \subset B \times B$.

C. If $A = B$, then $A \times B \times A = (B \times A) \times B$.

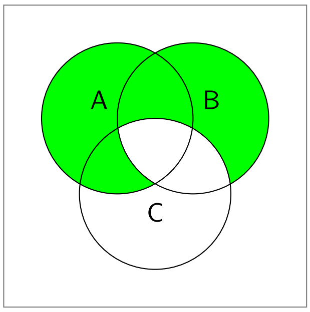
D. If $A = B$, then $A \times B \times A \subseteq B \times (A \times B)$.

> **Answer:**
>
> **A. Correct, but proof is left as an exercise to the reader.**
>
> B. Counterexample: $A = B$.
>
> C. Counterexample: $A = B = \{1\}$. $A \times B \times A = \{(1, 1, 1)\} \neq \{((1, 1), 1)\} = (B \times A) \times B$.
>
> D. Counterexample: $A = B = \{1\}$. $A \times B \times A = \{(1, 1, 1)\} \not\subseteq \{(1, (1, 1))\} = B \times (A \times B)$.

Open questions

17. (a) (1 point) Give a Venn Diagram for the set $(A - B) \cup (B - C)$.

Answer:



(b) (5 points) Claim: For all sets A if $|A|$ is odd and $\emptyset \notin A$ then there is **no** set B such that $\mathscr{P}(B) = A$. If the claim is true, prove it. If it is false, give a counterexample.

Answer:

Proof. Proof by contradiction: Assume there is a set A such that $|A|$ is odd, $\emptyset \notin A$ and there is also a set B such that $\mathscr{P}(B) = A$.

Since $\emptyset \subseteq B$, it must hold that $\emptyset \in \mathscr{P}(B)$. Thus $\emptyset \in A$, which contradicts the assumption that $\emptyset \notin A$. Thus by contradiction, it holds for all A. QED

Alternatively:

Proof. Proof by contrapositive: $\forall A(\exists B(\mathscr{P}(B) = A) \to (\exists k(|A| = 2k) \vee \emptyset \in A))$.
Take an arbitrary A such that there exists B with $\mathscr{P}(B) = A$.
Now consider the two exhaustive cases: $|B| = 0$ and $|B| \geq 1$.

- $|B| = 0$, this means that $B = \emptyset$, thus $A = \mathscr{P}(B) = \{\emptyset\}$. Thus $\emptyset \in A$, and therefore $\exists k(|A| = 2k) \vee \emptyset \in A$ is true.
- $|B| \geq 1$. We also know that $|A| = |\mathscr{P}(B)| = 2^{|B|}$. Since $|B| > 1$, this means $|A| = 2 \cdot 2^i$ for some $i \geq 0$. Thus $|A| = 2d$ for some d. Therefore $\exists k(|A| = 2k) \vee \emptyset \in A$ is true.

Since the claim holds in both cases and A was arbitrarily chosen, it holds for all A. QED

18. (6 points) Prove that for all integers $n \geq 1$: $7 \mid 2^{n+2} + 3^{2n+1}$. Make sure to show your intermediate steps.

Answer:

Proof. Proof by induction.
Base case ($n = 1$): $2^3 + 3^3 = 8 + 27 = 35 = 7 \cdot 5 = 7d$ with $d = 5$, hence $7 \mid 2^{1+2} + 3^{2+1}$.
Inductive step: Assume the claim holds for an arbitrary $k \geq 1$, that is: $7 \mid 2^{k+2} + 3^{2k+1}$ (IH).
To prove: $7 \mid 2^{(k+1)+2} + 3^{2(k+1)+1}$.

$$\begin{aligned} 2^{(k+1)+2} + 3^{2(k+1)+1} &= 2 \cdot 2^{k+2} + 9 \cdot 3^{2k+1} \\ &= 2(2^{k+2} + 3^{2k+1}) + 7 \cdot 3^{2k+1} \end{aligned}$$

By IH:

$$\begin{aligned} &= 2(7d) + 7 \cdot 3^{2k+1} \\ &= 7(2d + 3^{2k+1}) \\ &= 7e \end{aligned}$$

For $e = 2d + 3^{2k+1}$, thus $7 \mid 2^{(k+1)+2} + 3^{2(k+1)+1}$. Since k was arbitrarily chosen it holds for all integers ≥ 1. Thus by the principle of induction the claim holds for all integers ≥ 1. QED

19. (a) (2 points) What are the three properties an equivalence relation needs to fulfil? Give both the name and a brief description (or logically written definition) of the properties.

Answer:

- Reflexivity: $\forall x(R(x,x))$
- Symmetry: $\forall x \forall y(R(x,y) \rightarrow R(y,x))$
- Transitivity: $\forall x \forall y \forall z((R(x,y) \wedge R(y,z)) \rightarrow R(x,z))$

(b) (3 points) For following relation describe for each of the properties you gave us in question a, whether the relation satisfies that property and *why* it does (not). Two ducks a and b are in the relation R if a has more children than b.

Answer:

- Reflexivity: Nope, a duck does not have more children than itself. Take a duck with 2 kids, $2 > 2$ does not hold.
- Symmetry: Nope, if $R(a,b)$ then $c(a) > c(b)$, thus it is not possible for $c(b) > c(a)$ to also hold.
- Transitivity: Yes, if $c(a) > c(b)$ and $c(b) > c(c)$ then surely also $c(a) > c(c)$.

20. (a) (2 points) Consider: $(p \rightarrow q) \therefore (q \rightarrow p)$. If this argument is valid, prove it. If it is not give a counterexample and explanation to disprove it.

> **Answer:** $p = 0, q = 1$ makes the first half true and the second half false. This thus makes the implication false.

(b) (3 points) Consider: $(\exists x(P(x)) \wedge \exists y(Q(y))) \leftrightarrow \forall x(P(x) \wedge Q(x))$. If this is satisfiable, prove it. If it is not, explain why not.

> **Answer:** Take the structure S with $D^S = P^S = Q^S = \{a\}$. Clearly this satisfies the left and right hand side of the bi-implication.

(c) (4 points) Give a counterexample and explanation as to why it is a counterexample for the statement: for all sets A, B, C it holds that $(((A - B) \cap (C \cup B)) \subseteq B) \rightarrow A \cap B = \emptyset$.
Note that a Venn Diagram does not constitute a counterexample!

> **Answer:** To make the left-hand side true, $(A \cap C) - B$ must be empty. To make the second part false, $A \cap B$ must not be empty. Thus take: $A = \{1\}, B = \{1, 2\}, C = \{3\}$. This gives $(A - B) \cap (C \cup B) = (\emptyset \cap \{1, 2, 3\}) = \emptyset$, which is a subset of B. Yet $A \cap B = \{1\}$ so not empty.

21. Consider the sets $A = \{a, b, \{c, d\}\}$ and $B = \{1, 2, 3, 4, \{5, 6\}\}$.

(a) (2 points) Give the powerset of A.

> **Answer:** $\mathscr{P}(A) = \{\emptyset, \{a\}, \{b\}, \{\{c, d\}\}, \{a, b\}, \{a, \{c, d\}\}, \{b, \{c, d\}\}, A\}$

(b) (2 points) Give a function $f : A \rightarrow B$.

> **Answer:** $f = \{(a, 1), (b, 1), (\{c, d\}, 1)\}$.

(c) (2 points) If your function f has an inverse, give it. If it does not, explain why not.

> **Answer:** f cannot have an inverse. Since $|B| > |A|$ it cannot be surjective, and thus not bijective and thus there is no inverse.

22. (10 points) Consider the following function:

```
function Foo(A,B)
    x ← A
    y ← B
    p = 0
    while y ≠ 0 do
        if 2 | y then
            x ← 2 · x
            y ← y/2
        else
            p ← p + x
            y ← y − 1
        end if
    end while
    return p
end function
```

The ancient Egyptians already used this algorithm to compute $A \cdot B$ for $A, B \in \mathbb{N}$. Prove that this algorithm indeed computes the multiplication. Hint: You can prove $xy + p = AB$ to be a useful invariant.

Answer:

Proof. Take $xy + p = AB$ as our invariant:

I. Basis property: $x = A$, $y = B$, $p = 0$ so before the loop $xy + p = AB + 0 = AB$. Meaning the invariant holds.

II. Inductive property: Assume $x_{\text{old}}y_{\text{old}} + p_{\text{old}} = AB$. To prove: $x_{\text{new}}y_{\text{new}} + p_{\text{new}} = AB$. Division into cases:

- $2 \mid y_{\text{old}}$:

$$\begin{aligned} x_{\text{new}} &= x_{\text{old}} \cdot 2 \\ y_{\text{new}} &= y_{\text{old}}/2 \\ p_{\text{new}} &= p_{\text{old}} \end{aligned}$$

  So for what we need to prove:

$$\begin{aligned} x_{\text{new}}y_{\text{new}} + p_{\text{new}} &= x_{\text{old}} \cdot 2 \cdot y_{\text{old}}/2 + p_{\text{old}} \\ &= x_{\text{old}}y_{\text{old}} + p_{\text{old}} \end{aligned}$$

  By IH:

$$= AB$$

- $2 \nmid y_{\text{old}}$

$$\begin{aligned} x_{\text{new}} &= x_{\text{old}} \\ y_{\text{new}} &= y_{\text{old}} - 1 \\ p_{\text{new}} &= p_{\text{old}} + x_{\text{old}} \end{aligned}$$

  So for what we need to prove:

$$\begin{aligned} x_{\text{new}}y_{\text{new}} + p_{\text{new}} &= x_{\text{old}} \cdot (y_{\text{old}} - 1) + p_{\text{old}} + x_{\text{old}} \\ &= x_{\text{old}}y_{\text{old}} + p_{\text{old}} + x_{\text{old}} - x_{\text{old}} \\ &= x_{\text{old}}y_{\text{old}} + p_{\text{old}} \end{aligned}$$

  By IH:

$$= AB$$

III. Termination and falsity of guard: Since every iteration of the loop y decreases (either by a factor of 2 or a constant of 1) at some point it will be $= 0$. (It cannot be negative as this would require that we subtract 1 from 0, but since zero is even this will never happen).

IV. So at the end we know that $y = 0$ thus $xy + p = 0 \cdot x + p = p = AB$.

QED

23. (5 points) Consider the set $A = \{x \in \mathbb{N} \mid \exists y \in \mathbb{Z}(x = 4y)\}$.
Claim: Set A has the same cardinality as $\mathbb{Q}$.
If this claim is true, prove it. If this claim is false, disprove it. Start you answer with: "True" if you believe the claim to be true and with "False" if you believe the claim to be false.

Answer: True: Take the function $f : \mathbb{N} \to A$, with $f(x) = 4x$. Since f is injective ($f(x) = f(y)$, means that $4x = 4y$, means $x = y$.), and surjective (for any $y \in A$, we know $y = 4x$, so $y/4 = x \in \mathbb{N}$), it is also bijective. Therefore $\mathbb{N}$ and A have the same cardinality. And since $\mathbb{Q}$ and $\mathbb{N}$ have the same cardinality, so do A and $\mathbb{Q}$.

24. (a) (2 points) Create a truth table for $(p \wedge \neg q) \leftrightarrow \neg(q \vee p)$.

Answer:

p	q	$\overbrace{p \wedge \neg q}^{A}$	$\overbrace{(q \vee p)}^{B}$	$\neg B$	$A \leftrightarrow \neg B$
0	0	0	0	1	0
0	1	0	1	0	1
1	0	1	1	0	0
1	1	0	1	0	1

(b) (4 points) Consider a new normal form similar to DNF and CNF. The Implicative Normal Form (INF) requires propositions to be an implication (just the one!) of disjuctions. Similar to DNF and CNF, negations may only occur in front of literals, not on compound propositions. Examples of expressions in INF include $p \to q$, $p \vee q$, and $(p \vee q \vee z) \to (q \vee r)$.
Rewrite $(p \vee \neg q) \vee \neg(r \to p)$ to INF, simplify your answer as much as possible.

Answer:

$$\begin{aligned}(p \vee \neg q) \vee \neg(r \to p) &\equiv p \vee \neg q \vee (r \wedge \neg p)\\ &\equiv (p \vee \neg q \vee r) \wedge (p \vee \neg q \vee \neg p)\\ &\equiv (p \vee \neg q \vee r) \wedge T\\ &\equiv q \to (p \vee r)\end{aligned}$$

25. (a) (8 points) Consider the recursive definition of the set A:

I. $3 \in A$, $15 \in A$

II. $x \in A \to 8x + 24 \in A$

III. $x, y \in A \to 2x - 7y \in A$

IV. Nothing other than created by the rules above is in A.

Prove that every number in A is divisible by 3.

Answer:

Proof. Proof by structural induction:

- Base cases: $3 = 3 \cdot 1$ and $15 = 3 \cdot 5$, thus $3 \mid 3$ and $3 \mid 15$ both hold.
- Inductive step: Take arbitrary $k, m \in A$, such that $3 \mid k$ and $3 \mid m$ (IH). To prove: $3 \mid 8k + 24$, $3 \mid 2k - 7m$.

$$\begin{aligned} 8k + 24 &\overset{\text{IH}}{=} 8(3c) + 24 \\ &= 3(8c + 8) \\ &= 3d \\ 2k - 7m &\overset{\text{IH}}{=} 2(3c) - 7(3d) \\ &= 3(2c - 7d) \\ &= 3e \end{aligned}$$

So $3 \mid 8k + 24$ and $3 \mid 2k - 7m$.

Thus by the principle of induction it holds for all elements of A that they are divisible by 3. QED

Note: Many people lost one or two points for the IH here. You should include the following notions:

- k, m are arbitrary
- $k, m \in A$
- $3 \mid k$ and $3 \mid m$
- or alternatively $\exists c, d \in \mathbb{Z}$ such that $k = 3c$ and $m = 3d$

(b) (4 points) Create **a recursive definition** for a set $A \subseteq \mathbb{Z}$ that contains all numbers divisible by 11.

Answer:

I. $0 \in A$

II. $x \in A \to x + 11 \in A$

III. $x \in A \to x - 11 \in A$

IV. Nothing other than created by the rules above is in A.

End of the exam