Introduction to Formal Reasoning 2018
Solutions Exam
(11/01/19)

1. This exercise is about the following formula of propositional logic:

$$a \to b \leftrightarrow a \vee b \wedge \neg a \to b$$

   (a) Write this formula with parentheses according to the official grammar from the course notes.
   The correct formula is:

$$((a \to b) \leftrightarrow ((a \vee (b \wedge \neg a)) \to b))$$

   (b) Give the full truth table of this formula.

a	b	$a \to b$	$\neg a$	$b \wedge \neg a$	$a \vee (b \wedge \neg a)$	$(a \vee (b \wedge \neg a)) \to b$	$(a \to b) \leftrightarrow (((a \vee (b \wedge \neg a))) \to b)$
0	0	1	1	0	0	1	1
0	1	1	1	1	1	1	1
1	0	0	0	0	1	0	1
1	1	1	0	0	1	1	1

2. Give a formula of propositional logic that formalizes the meaning of the following English sentence:

   I do not make New Year's resolutions, because if I make New Year's resolutions I do not keep them.

   Use for the dictionary:

M	I make New Year's resolutions
K	I keep my New Year's resolutions

   For instance:

$$\neg M \wedge (M \to \neg K)$$

3. Give a model v_3 of propositional logic that shows that:

$$a \to (b \to c) \not\equiv (a \to b) \to c$$

   Explain your answer.

   Take for instance model v_3 where $v_3(a) = 0$, $v_3(b) = 0$ and $v_3(c) = 0$. Then $v_3(a \to (b \to c)) = 1$ and $v_3((a \to b) \to c) = 0$. So there is a model for which the outcome is not the same, hence the formulas are not logically equivalent.

In fact there are more models that can be used here. We have marked all usable models with a $*$ in the table below.

v_3	a	b	c	$b \to c$	$a \to (b \to c)$	$a \to b$	$(a \to b) \to c$
$*$	0	0	0	1	1	1	0
	0	0	1	1	1	1	1
$*$	0	1	0	0	1	1	0
	0	1	1	1	1	1	1
	1	0	0	1	1	0	1
	1	0	1	1	1	0	1
	1	1	0	0	0	1	0
	1	1	1	1	1	1	1

4. Give an English sentence that corresponds to the meaning of the following formula of predicate logic with equality:

$$\forall x \in N \big[S(x) \leftrightarrow \exists y \in N \big[M(y,y,x) \wedge \forall z \in N \left[M(z,z,x) \to z = y\right]\big]\big]$$

Use for the dictionary:

N	the domain of natural numbers
$S(x)$	x is a square number
$A(x,y,z)$	$x + y = z$
$M(x,y,z)$	$x \cdot y = z$

Note: English sentences do not contain variable names.

A natural number is a square if and only if for this number there exists exactly one natural number such that the product of the second number multiplied by itself gives the first number.

5. Using the dictionary from the previous exercise, give a formula of predicate logic that formalizes the meaning of the following English sentence:

Every natural number can be written as the sum of four squares.

$$
\begin{array}{l}
\forall x \in N \quad [\\
\qquad \exists y, z \in N \quad [\\
\qquad\qquad A(y, z, x) \\
\qquad\qquad \wedge \\
\qquad\qquad \exists m, n \in N \quad [\\
\qquad\qquad\qquad A(m, n, y) \\
\qquad\qquad\qquad \wedge \\
\qquad\qquad\qquad S(m) \\
\qquad\qquad\qquad \wedge \\
\qquad\qquad\qquad S(n) \\
\qquad\qquad\qquad] \\
\qquad\qquad \wedge \\
\qquad\qquad \exists o, p \in N \quad [\\
\qquad\qquad\qquad A(o, p, z) \\
\qquad\qquad\qquad \wedge \\
\qquad\qquad\qquad S(o) \\
\qquad\qquad\qquad \wedge \\
\qquad\qquad\qquad S(p) \\
\qquad\qquad\qquad] \\
\qquad\qquad] \\
\qquad]
\end{array}
$$

This formula states that: for all natural numbers x, there exist natural numbers y and z such that x is the sum of y and z, where y is the sum of two natural numbers n and m where n is the square of some natural number a and m is the square of some natural number b, and likewise, where z is the sum of two natural numbers o and p where o is the square of some natural number c and p is the square of some natural number d.

Note that we could have reused the variable names m and n instead of o and p, because we took the scope as short as possible. A different approach where the scope is not as short as possible is:

$$
\begin{array}{llll}
\forall x \in N \quad [& & & \\
& \exists y_1, y_2, y_3, y_4 \in N \quad [& & \\
& & S(y_1) & \\
& & \wedge & \\
& & S(y_2) & \\
& & \wedge & \\
& & S(y_3) & \\
& & \wedge & \\
& & S(y_4) & \\
& & \wedge & \\
& & \exists z_1, z_2 \in N \quad [& \\
& & & A(y_1, y_2, z_1) \\
& & & \wedge \\
& & & A(y_3, y_4, z_2) \\
& & & \wedge \\
& & & A(z_1, z_2, x) \\
& &] & \\
&] & & \\
] & & &
\end{array}
$$

6. Explain the relation between the following two notions in the semantics of predicate logic that are both written with the 'double turnstile' symbol:

$$
\begin{aligned}
(M, I) &\vDash f \\
&\vDash f
\end{aligned}
$$

In your explanation explicitly state what the symbols M, I and f stand for.

Note that M stands for a *model*, a piece of the 'real' world, and I stands for an *interpretation*, a mapping of the symbols in the formula to the real world, and f stands for an arbitrary formula.

Now $(M, I) \vDash f$ means that formula f holds in model M under interpretation I. And $\vDash f$ means that formula f holds in all models under all interpretations.

7. Give an infinite language L_7 over the alphabet $\Sigma = \{a, b\}$ such that

$$
\begin{aligned}
L_7^* &= \Sigma^* \\
L_7^R &\neq L_7 \\
L_7 L_7 &\neq L_7
\end{aligned}
$$

Explain your answer.

Let us define $L_7 := \{a, b, ab\} \cup \{a^n \mid n \in \mathbb{N} \text{ and } n \geq 2\}$. We wrote this language in this strange way because the left part $\{a, b, ab\}$ is actually enough for complying to the three main requirements. The right part is only added to comply to the requirement of being an infinite language.

Now note that:

- L_7 is an infinite language over Σ.
- Because L_7 is defined over the alphabet Σ, automatically $L_7^* \subseteq \Sigma^*$. However, because $\Sigma \subseteq L_7$ we also have that $\Sigma^* \subseteq L_7^*$. Hence $L_7^* = \Sigma^*$.
- The language $L_7^R = \{a, b, ba\} \cup \{a^n \mid n \in \mathbb{N}\}$, which is indeed not equal to L_7.
- The language L_7L_7 contains the word aba, but aba is not in L_7, so L_7L_7 is indeed not equal to L_7.

Alternatives:

$$L_7 \quad := \quad L_{11} = \mathcal{L}(a^*b^*)$$

8. Give a regular expression for the language:

$$L_8 := \{w \in \{a,b\}^* \mid w \text{ contains an even number of } a\text{'s and at most one } b\}$$

So a word contains either and even number of a's and no b's, or one b surrounded on both sides by an even number of a's, or one b surrounded on both sides by an odd number of a's:

$$(aa)^* \cup (aa)^*b(aa)^* \cup (aa)^*aba(aa)^*$$

We can do some refactoring to get

$$(aa)^*(\lambda \cup (b \cup aba)(aa)^*)$$

9. Give a context-free grammar for the language:

$$L_9 := \{w \in \{a,b\}^* \mid w = w^R\}$$

Take for instance:

$$S \to \lambda \mid a \mid b \mid aSa \mid bSb$$

10. We define the context-free grammar G_{10}:

$$\begin{aligned} S &\to AB \\ A &\to aA \mid \lambda \\ B &\to bB \mid \lambda \end{aligned}$$

Someone proposes the property

$$P(w) := [w \text{ does not contain } ba]$$

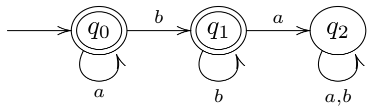
as an invariant, in order to show that $abab \notin \mathcal{L}(G_{10})$. Is that correct? Explain your answer. *Note:* You only have to explain why this property is sufficient or not to show that $abab \notin \mathcal{L}(G_{10})$. If you think it is not, you don't have to come up with an improved property!

It is not correct. Take $v = bA$ and $v' = baA$. Then clearly $P(v)$ holds. It is also true that $v \to v'$. But $P(v')$ does not hold. So $P(w)$ is not an invariant.

11. (a) Give a deterministic finite automaton M_{11} for the language

$$L_{11} := \mathcal{L}(a^*b^*)$$

So we want $L_{11} = L(M_{11})$.
Let M_{11} be:



(b) Give a right-linear context-free grammar G_{11} that corresponds to the automaton M_{11} from the previous sub-exercise.
This right-linear grammar really corresponds the automaton:

$$\begin{aligned} S &\to \lambda \mid aS \mid bA \\ A &\to \lambda \mid bA \mid aB \\ B &\to aB \mid bB \end{aligned}$$

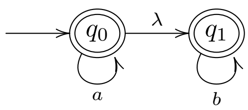
However, it can be simplified to this equivalent right-linear grammar:

$$\begin{aligned} S &\to aS \mid A \\ A &\to \lambda \mid bA \end{aligned}$$

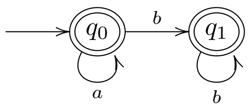
(But this last one is not a correct answer since it doesn't really *correspond* to the automaton.)

12. Give a non-deterministic finite automaton M_{12} with only two states, for which any *deterministic* finite automaton that recognizes the same language has at least three states.

Let M_{12} be:



or

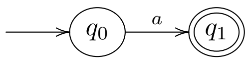


These non-deterministic automata both accept the language $L_{12} = L_{11} = \mathcal{L}(a^*b^*)$. If we try to create a deterministic automaton for this language we need at least three states:

- We need an initial state q_0.
- Because we need to be able to distinguish whether a b has been read, we need a second final state q_1.
- In addition we need a sink q_2 for redirecting all input that should not be accepted.

This cheapest construction gives the automaton M_{11} we have shown in exercise 11a.

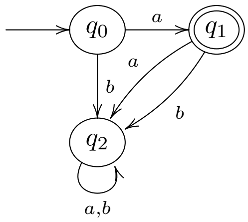
Now we present another solution with a simpler language and automaton. Let M_{12} be:



This non-deterministic automaton accepts the language $L_{12} = \{a\}$. If we try to create a deterministic automaton we need at least three states:

- We need an initial state q_0.
- Because λ is not accepted, the final state accepting a cannot be the initial state q_0 and we need a state q_1 for this.
- In addition we need a sink q_2 for redirecting all input that should not be accepted.

This cheapest construction gives:



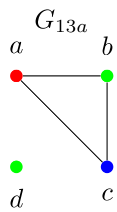
13. How many non-isomorphic graphs are there with four vertices and chromatic number three? Explain your answer.

There are three non-isomorphic graphs with four vertices and chromatic number three.

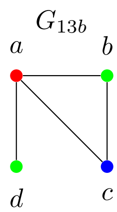
Let us assume that our graph has four vertices labeled a, b, c and d. If a graph with four vertices has chromatic number three, this implies that the graph has a cycle of odd length, which comes down to having a cycle of length three, or in other words a triangle.

Because we are searching for non-isomorphic graphs, we may assume that the triangle is between vertices a, b and c. So we only have to decide whether the edges $\{a, d\}$, $\{b, d\}$ and $\{c, d\}$ are part of the graph or not. So in total there are only $2^3 = 8$ graphs left to check.

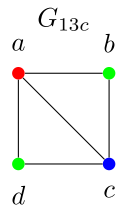
- None of the edges $\{a, d\}$, $\{b, d\}$ and $\{c, d\}$ is part of the graph, so we only have the triangle. Obviously, there is only one graph of this type modulo isomorphisms. Note that the vertices a, b and c all have degree two and vertex d has degree zero.



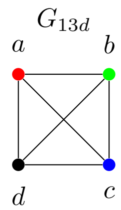
- Exactly one of the edges $\{a, d\}$, $\{b, d\}$ and $\{c, d\}$ is part of the graph. There are three options here, but all of them can be drawn as a triangle with a single tail. So all of these three graphs are isomorphic to each other. Note that there is exactly one vertex with degree three, which directly implies that this type is not isomorphic to the previous type.



- Exactly two of the edges $\{a,d\}$, $\{b,d\}$ and $\{c,d\}$ are part of the graph. Again, there are three options here, but all of them can be drawn as a square with a single diagonal. So all of these three graphs are isomorphic to each other. Note that there are exactly two vertices with degree three, which directly implies that this type is not isomorphic to the previous two types.



- All of the edges $\{a,d\}$, $\{b,d\}$ and $\{c,d\}$ are part of the graph. But then our graph is isomorphic to K_4, which means that the chromatic number is four, so this type doesn't count.



14. We use recursion to define:

$$a_0 = 0$$
$$a_{n+1} = a_n + 2n \qquad \text{for } n \geq 0$$

Prove by induction that for all $n \geq 0$:

$$a_n = n^2 - n$$

Proposition: 0

$a_n = n^2 - n$ for all $n \geq 0$.

Proof by induction on n. 1

We first define our predicate P as:

$$P(n) \quad := \quad a_n = n^2 - n$$ 2

Base Case. We show that $P(0)$ holds, i.e. we show that 3

$a_0 = 0^2 - 0$

This indeed holds, because by definition $a_0 = 0$ and $0 = 0^2 - 0$. 4

Induction Step. Let k be any natural number such that $k \geq 0$. 5

Assume that we already know that $P(k)$ holds, i.e. we assume that

$a_k = k^2 - k$ (Induction Hypothesis IH) 6

We now show that $P(k+1)$ also holds, i.e. we show that 7

$a_{k+1} = (k+1)^2 - (k+1)$

This indeed holds, because 8

$$
\begin{aligned}
a_{k+1} &= a_k + 2k \\
&\overset{\text{IH}}{=} k^2 - k + 2k \\
&= k^2 + 2k - k \\
&= k^2 + 2k + 1 - k - 1 \\
&= (k+1)^2 - (k+1)
\end{aligned}
$$

Hence it follows by induction that $P(n)$ holds for all $n \geq 0$. 9

15. Give the defining equations of the recursive definition of the binomial coefficients.

Let $n \in \mathbb{N}$ and let $k \in \mathbb{N}$ such that $k \leq n$.

$$
\begin{aligned}
\binom{n}{0} &= 1 \\
\binom{n}{n} &= 1 \\
\binom{n+1}{k+1} &= \binom{n}{k} + \binom{n}{k+1}
\end{aligned}
$$

Or an alternative definition. Let $n \in \mathbb{N}$ and let $k \in \mathbb{N}$.

$$
\begin{aligned}
\binom{n}{0} &= 1 \\
\binom{0}{k+1} &= 0 \\
\binom{n+1}{k+1} &= \binom{n}{k} + \binom{n}{k+1}
\end{aligned}
$$

16. I believe in Murphy's law, which says that anything that can go wrong will go wrong. This means that if I bring an umbrella because I believe it will be going to rain, then it probably will not rain.

Now consider the following English sentence, which expresses some variant of this:

> *I believe that if I believe that it will rain, then it will not rain.*

(a) Give a modal formula that formalizes the meaning of this sentence. Use for the dictionary:

R	it will rain

$$\Box(\Box R \to \neg R)$$

(b) What is the name of the logic in which the modal operators are interpreted as being about belief?

This is *doxastic* logic.

17. The modal logic D is the logic of serial Kripke models. A formula f is called true in the logic D if f is true in all serial Kripke models. The notation for this is $\models_D f$. Now show that:

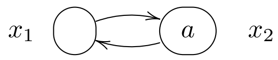
$$\not\models_D \Box a \to a$$

Explain your answer.

So we are looking for a serial Kripke model for which the formula $\Box a \to a$ does not hold in all of its worlds.

Let us take this model:

$\mathcal{M}_{17}$:



Note that:

- Because every world has at least one accessible world, this is a serial Kripke model.
- We have that $x_1 \Vdash \Box a$, because $R(x_1) = \{x_2\}$ and $a \in V(x_2) = \{a\}$.
- We have that $x_1 \nVdash a$, because $a \notin V(x_1) = \emptyset$.
- From this it follows that $x_1 \nVdash \Box a \to a$.
- And hence it follows that $\mathcal{M}_{17} \not\models \Box a \to a$.
- And hence it follows that $\not\models_D \Box a \to a$.

18. For each of the five mathematicians listed below, write down the notion from the course that was named after him, and for each of these notions give a *one line* description.

As an example, a description of 'Pascal's triangle' – named after Blaise Pascal (French mathematician, physicist, inventor, writer and Catholic theologian, 1623–1662) – might be 'triangular array of the binomial coefficients'.

(a) Sir Isaac Newton (English mathematician, physicist, astronomer, theologian and author, 1643–1727)
(b) Sir William Rowan Hamilton (Irish mathematician, 1805–1865)
(c) Augustus De Morgan (British mathematician and logician, 1806–1871)
(d) Eric Temple Bell (Scottish-born mathematician and science fiction writer, who lived in the United States for most of his life, 1883–1960)
(e) Stephen Cole Kleene (American mathematician, 1909–1994)

(a) *Newton's binomial theorem*: the algebraic expansion of $(x + y)^n$ using binomial coefficients.
(b) *Hamiltonian path/cycle*: path/cycle in a graph that visits each vertex exactly once.
(c) *De Morgan's laws*: $\neg(f \vee g) \equiv \neg f \wedge \neg g$ and $\neg(f \wedge g) \equiv \neg f \vee \neg g$.
(d) *Bell numbers*: numbers that count the number of possible partitions of a finite set.
(e) *Kleene star*: the language L^* that consists of concatenations of elements of L.