KØBENHAVNS UNIVERSITET

Diskret Matematik og Formelle Sprog: Problem Set 3

Due: Monday March 8 at 23:59 CET.
Submission: Please submit your solutions via *Absalon* as PDF file. State your name and e-mail address close to the top of the first page. Solutions should be written in LaTeX or some other math-aware typesetting system with reasonable margins on all sides (at least 2.5 cm). Please try to be precise and to the point in your solutions and refrain from vague statements. *Write so that a fellow student of yours can read, understand, and verify your solutions.* In addition to what is stated below, the general rules in the course information always apply.
Collaboration: Discussions of ideas in groups of two to three people are allowed—and indeed, encouraged—but you should always write up your solutions completely on your own, from start to finish, and you should understand all aspects of them fully. It is not allowed to compose draft solutions together and then continue editing individually, or to share any text, formulas, or pseudo-code. Also, no such material may be downloaded from the internet and/or used verbatim. Submitted solutions will be checked for plagiarism.
Grading: A score of 140 points is guaranteed to be enough to pass this problem set.
Questions: Please do not hesitate to ask the instructor or TAs if any problem statement is unclear, but please make sure to send private messages sometimes specific enough questions could give away the solution to your fellow students, and we want all of you to benefit from working on and learning on the problems. Good luck!

1 (40 p) For positive integers $a_1, a_2, \ldots, a_k$, define $\gcd(a_1, a_2, \ldots, a_k)$ to be the largest positive integer d such that d divides every a_i and any positive integer c that divides every a_i also has to divide d. Is it true that there are integers m_i, not necessarily positive, such that $d = \sum_{i=1}^{k} m_i a_i$? Prove this or give a simple counter-example.

Solution: This is true, and we can prove it by induction on the number of arguments of the function gcd.

Before starting the inductive argument, however, let us first make the observation that $\gcd(a_1, \ldots, a_k, a_{k+1}) = \gcd(\gcd(a_1, \ldots, a_k), a_{k+1})$. To see this, set $d = \gcd(a_1, \ldots, a_k, a_{k+1})$, $A = \gcd(a_1, \ldots, a_k)$, and $d' = \gcd(A, a_{k+1}) = \gcd(\gcd(a_1, \ldots, a_k), a_{k+1})$. We will prove that $d \mid d'$ and $d' \mid d$, meaning that $d = d'$ must hold. By definition, we have $d \mid a_i$ for all i, meaning (trivially) that d must divide both A and a_{k+1}. But, again by definition, any number with that property must divide $\gcd(A, a_{k+1}) = d'$. The other direction is very similar: since $d' \mid A$ we have $d' \mid a_i$ for $i = 1, \ldots, k$, and by assumption $d' \mid a_{k+1}$ also holds. That is, d' divides all the numbers $a_1, \ldots, a_k, a_{k+1}$, but by definition any such number also divides $d = \gcd(a_1, \ldots, a_k, a_{k+1})$ for some integers c_1 and c_2.

We now turn to the inductive proof. The base case is for two arguments, for which we know from the KBR textbook that $\gcd(a_1, a_2)$ can be written as linear combination $\gcd(a_1, a_2) = c_1 a_1 + c_2 a_2$ for some integers $c_1, \ldots, c_k$.

For the induction step, let us assume that for k numbers we can write $A = \gcd(a_1, a_2, \ldots, a_k) =$

$c_1a_1 + c_2a_2 + \ldots c_ka_k$. Then for $k+1$ arguments we get

$$\begin{aligned}
&\gcd(a_1, a_2, \ldots, a_k, a_{k+1}) = \\
&\qquad = \gcd(A, a_{k+1}) && \text{[by the reasoning above]} \\
&\qquad = mA + c_{k+1}a_{k+1} && \text{[by the base case]} \\
&\qquad = m \cdot \gcd(a_1, a_2, \ldots, a_k) + c_{k+1} \cdot a_{k+1} && \text{[just writing it out]} \\
&\qquad = m(c_1 \cdot a_1 + c_2 \cdot a_2 + \ldots c_k \cdot a_k) + c_{k+1} \cdot a_{k+1} && \text{[by the inductive hypothesis]} \\
&\qquad = mc_1 \cdot a_1 + mc_2 \cdot a_2 + \ldots mc_k \cdot a_k + c_{k+1} \cdot a_{k+1}
\end{aligned}$$

which is an expression exactly on the form we wanted. The claim follows by the induction principle.

2 (80 p) Decide for each of the propositional logic formulas below whether it is a tautology or a contradiction. If neither of these cases apply, then present a satisfying assignment for the formula. It is sufficient (and necessary) for a full score to justify all your answers by presenting truth tables for all the subformulas analogously to how we did it in class, but you are also encourage to *explain* why your answers are correct (and good explanations could compensate fully for minor slips in the truth tables).

(Note that logical not $\neg$ is assumed to bind harder than the binary connectives, but other than that all formulas are fully parenthesized for clarity. We write $\rightarrow$ for logical implication and $\leftrightarrow$ for equivalence.)

2a (20 p) $((p \rightarrow q) \rightarrow r) \rightarrow ((p \wedge q) \rightarrow r)$

Solution: For a full score the complete truth tables were needed. This is just mechanical work, and once the truth tables have been produced it is immediate to read off the correct answers. For Problem 2a we will both present the truth table and explain why the answer is correct, but for the other formulas we will skip the truth tables in these solution sketches and focus on the explanations.

The truth table for the formula in Problem 2a is as described below.

p	q	r	$p \rightarrow q$	$(p \rightarrow q) \rightarrow r$	$p \wedge q$	$(p \wedge q) \rightarrow r$	$((p \rightarrow q) \rightarrow r) \rightarrow ((p \wedge q) \rightarrow r)$
$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$
$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\top$
$\bot$	$\top$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$	$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\top$	$\top$
$\top$	$\top$	$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\top$
$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$

From the rightmost column in this table we can see that the formula is a tautology. Let us now explain why this is so.

An implication $A \rightarrow B$ is false if and only if $A = \top$ and $B = \bot$. With this in mind, for our formula to be falsified it is required that $((p \wedge q) \rightarrow r)$ evaluates to false and $(p \rightarrow q) \rightarrow r$ to true. For the first of these formulas to be false we must have $r = \bot$, $p = \top$, $q = \top$. If we insert these values into the second formula we get $(\top \rightarrow \top) \rightarrow \bot$, which means that it will also be false. Thus, there is no way to falsify the whole formula, meaning that it is a tautology.

2b (20 p) $((p \rightarrow q) \wedge (r \rightarrow s)) \leftrightarrow ((p \wedge r) \rightarrow (q \wedge s))$

Solution: This formula has a falsifying assignment $p = \top, r = \bot, q = \bot, s = \top$ and a satisfying assignment $p = \top, r = \top, q = \top, s = \top$. Hence, it is neither a tautology nor a contradiction.

2c (20 p) $((p \wedge \neg r) \vee (q \wedge \neg r)) \rightarrow ((p \vee q) \rightarrow r)$

Solution: This is again neither a tautology nor a contradiction. A satisfying assignment is $p, q, r = \top$ and a falsifying assignment is $p, q = \top$, $r = \bot$.

2d (20 p) $(p \rightarrow (q \vee r)) \vee (\neg(\neg p \vee q) \wedge \neg r)$

Solution: If we negate the formula $p \rightarrow (q \vee r)$ and rewrite it using the rules we have learned in class, then we get

$$\begin{aligned}
\neg(p \rightarrow (q \vee r)) &\iff \neg(\neg p \vee (q \vee r)) && [\text{since } A \rightarrow B \iff \neg A \vee B] \\
&\iff \neg((\neg p \vee q) \vee r) && [\text{since } A \vee (B \vee C) \iff (A \vee B) \vee C] \\
&\iff \neg(\neg p \vee q) \wedge \neg r && [\text{since } \neg(A \vee B) \iff \neg A \wedge \neg B]
\end{aligned}$$

and this final subformula exactly matches the second part of the formula we are interested in. This means that the whole formula is eqivalent to a formula of the form $A \vee \neg A$, which is a tautology.

3 (100 p) Consider a directed graph that consists of L layers numbered from 0 up to $L - 1$, with $i + 1$ vertices in every layer i numbered from 0 to i, and with outgoing edges from vertex j in layer i to vertices j and $j + 1$ in layer $i + 1$. See Figure 1a for an illustration of this graph with 7 layers. We can agree to call this graph a *lattice graph* (because it can be obtained from a fragment of the integer lattice in 2 dimensions as shown in Figure 1b, but this is actually completely irrelevant to this problem).

Suppose we start in the unique source vertex on level 0 and walk along edges in the graph, flipping a fair coin at every vertex to decide whether to go left or right, until we reach one of the sinks in the last layer. For instance, in Figure 1a the walk "left–left–right–left–right–right" would visit vertices z, y_0, x_0, w_1, v_1, u_2, and end in s_3.

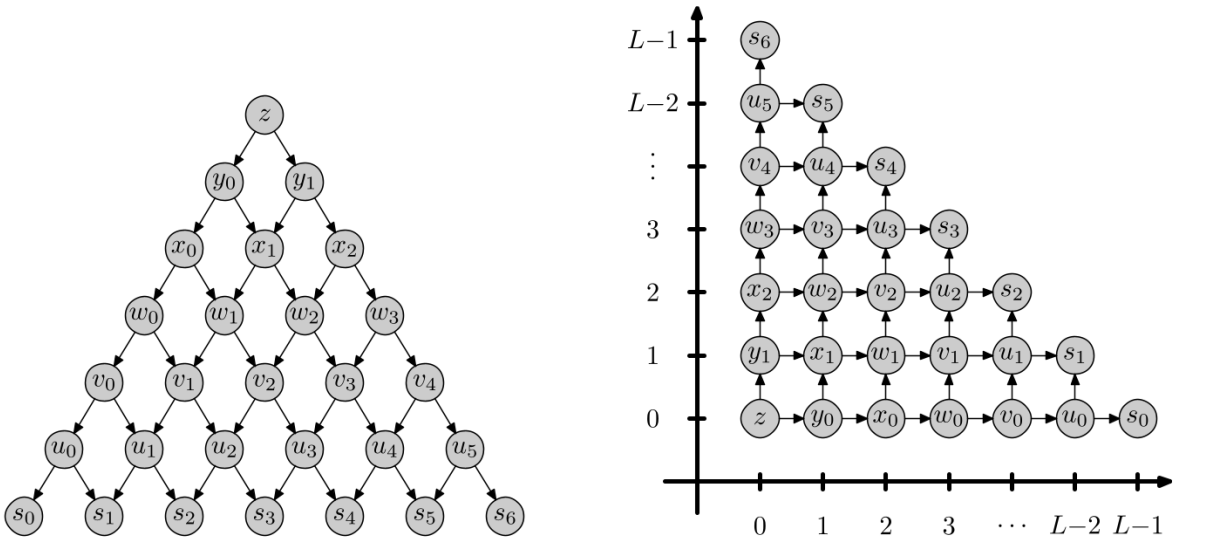
3a (40 p) For every vertex s_i in the lattice graph in Figure 1a, calculate the probability that such a walk ends in vertex s_i. Which vertex is the walk most likely to end up in?

3b (60 p) For a lattice graph with L layers, where $L \geq 2$ is a positive integer, calculate the probability that a walk as described above ends in vertex j in layer $L - 1$ for $j = 0, 1, \ldots, L - 1$.

Hint: Use the fact that all walks are equally likely to turn this into a counting problem.

Solution: Clearly, Problem 3a is a special case of Problem 3b, and here we will focus on the latter problem.

Using the hint, since a fair coin is being flipped we deduce that the probability of any particular walk is the same and is equal to $\left(\frac{1}{2}\right)^{L-1}$. In order to calculate the probability of reaching a certain leaf, it is sufficient to count the number of walks ending in that leaf. We can identify each walk with a binary sequence of length $L-1$, where 1 means going right and 0 means going left, say, so that the walk "left–left–right–left–right–right" in Figure 1a visiting vertices z, y_0, x_0, w_1, v_1, u_2, and s_3 is encoded as the sequence 001011.



(a) Lattice graph with 7 layers.

(b) Graph as connected points in 2D integer lattice.

Figure 1: Example graph for Problem 3.

Thinking a bit more, we realize that which leaf the walk ends up in is determined by the number of right turns in the walk, regardless of when these turns happen. Looking again at Figure 1a, any walk making exactly 3 right turns will end up in s_3. This means that the probability of reaching leaf j for $j = 0, 1, \ldots, L-1$ is proportional to the number of walks with j right turns, or the number of binary strings of length $L-1$ containing exactly j ones. But this number is nothing other than the binomial coefficient $\binom{L-1}{j}$. Thus, the probability of reaching leaf j can be written as

$$\Pr[\text{reaching leaf } j] = \binom{L-1}{j}\left(\frac{1}{2}\right)^{L-1} .$$

4 (60 p) In this problem we focus on relations. In particular, suppose that $A = \{e_1, e_2, \ldots, e_9, e_{10}\}$ is a set of 10 elements and consider the relation R on A represented by the matrix

$$M_R = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

(where element e_i corresponds to row and column i).

4a (20 p) Let us write T to denote the transitive closure of the relation R. What is the matrix representation of T in this case? Can you describe in words what the relation T is?

Solution: In R, we have that e_i is related to e_{i+1}. By transitivity, this gives us that e_i is related to e_{i+2}, and by induction we see that e_i is related to e_j for $i < j$, yielding the matrix

$$M_T = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

which is the matrix for a linear order relation (such as less-than).

4b (20 p) Suppose that we create a new relation S_1 from R by first taking the reflexive closure and then the symmetric closure. What does the matrix representation of S_1 look like? Can you describe in words what the relation S_1 is?

Solution: Taking the reflexive closure means adding an all-1s diagonal to the matrix for the relation (regardless of what the matrix is). Since e_i is related to e_{i+1} in R, taking the symmetric closure means that we will get that e_{i+1} is related to e_i also, while the all-1s diagonal is not affected. This leads to the matrix

$$M_{S_1} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

which shows that e_i is related to e_j if and only if $|i - j| \leq 1$.

4c (20 p) Suppose instead that we first take the symmetric closure and then the reflexive closure to derive another relation S_2 from R. Are S_1 and S_2 different relations, or are they the same relation in the end? If the latter case holds, is it true for any relation R on a set A that relations S_1 and S_2 derived in this way will be the same, or can they sometimes be different? Give a proof or present a simple counter-example.

Solution: As already written in the solution for Problem 4b, the reflexive closure just adds an all-1s diagonal, regardless of when this closure operator is applied, and does not affect any off-diagonal elements in the matrix representation. The symmetric closure adds the pair (e_j, e_i) for any pair (e_i, e_j) already in the relation, and thus leaves all diagonal entries unchanged. Therefore, it is true for any relation R that the relations S_1 and S_2 will be the same.