Massachusetts Institute of Technology
6.042J/18.062J: Mathematics for Computer Science
Professors David Karger and Nancy Lynch

Handout 21
February 24, 2000

Problem Set 3 Solutions

Required Problems:

Problem 1. *The Towers of Hanoi.*

There are three poles. On the first pole there is a stack of rings of increasing size, with the smallest ring on top of the stack. The second and third poles are empty. The challenge is to move the entire stack of rings to the second pole, while obeying the following rules:

- Rings may only be moved one at a time from one pole to another.
- A ring may only be moved if it is on the top of a stack.
- A ring may only be placed on top of a larger ring.

Suppose there are $n \geq 1$ rings initially stacked on the first pole and rings are only moved according to these rules.

(a) Prove that no matter how many moves are made, the rings stacked on each pole, if any, increase in size from the top.

Proof. The proof is by induction on the number of moves — not the number of rings.

Let $P(k)$ be the predicate: "After k moves, the rings stacked on each pole increase in size from the top." The base case $P(0)$ follows because initially, that is, after zero moves, the rings are in increasing order.

Now assume $P(k)$, namely, that they are in order on every pole after k steps. Suppose on the $k+1$st move ring R is moved from pole i to pole $j \neq i$. Then the rings left on pole i, if any, are still in order. Also, the ring that was on top of pole j, if any, must be larger than R according to the rules, so the rings on pole j increase in size starting from ring R on top. Of course the rings on the remaining pole, if any, are unchanged, and so remain in increasing order. Hence all poles have rings in increasing order from the top after $k+1$ moves, that is, $P(k+1)$ holds. ■

(b) Prove that there is a way to move all the rings to the second pole in $2^n - 1$ moves.

Proof. The proof is by induction on the number of rings n. However, in order to simplify the proof, we strengthen the induction predicate. In particular, we allow there to be n *or more* rings initially stacked in increasing order on *any* given pole — not necessarily the "first" pole.

Let $P(n)$ be the predicate: "For $i \in \{1,2,3\}$, suppose there are $n \geq 1$ or more rings stacked on pole i in increasing order from the top. Suppose also that the rings, if any, on top of the other two poles are larger than the top n rings stacked on pole i. Then, the top n rings stacked on pole i can be moved to any other pole in $2^n - 1$ legal steps."

Notice that it follows as a special case of $P(n)$, that n rings stacked in order on pole 1 can be moved to pole 2 in $2^n - 1$ legal steps, as required.

Now we prove $P(n)$ by induction on the number of rings n. Without loss of generality, let i denote the pole on which the n rings are stacked initially, j denote the pole on which we must move the n rings initially stacked on pole i, and k denote the remaining pole.

Base Case:

$P(1)$ is true if the ring on top of pole j, if any, is larger than the ring on pole i, then the single ring on pole i can be moved in $2^1 - 1 = 1$ legal step onto pole j.

Inductive Step:

Assume $P(n)$ holds for some integer $n \geq 1$.

Now, we must prove that $P(n+1)$ holds. We assume that there are $n+1$ rings stacked in increasing order on pole i and that the rings on the other two poles are larger than the top $n+1$ rings stacked on pole i. By the induction hypothesis, we can move the top n rings from pole i to pole k in $2^n - 1$ moves. Subsequently, it is legal to move the top ring on pole i, which is the $n+1$th ring initially stacked on pole i, from pole i to pole j. Finally, by the induction hypothesis we can move the top n rings stacked on pole k to pole j in $2^n - 1$ more steps. Concluding, we have succeeded to move the top $n+1$ rings from pole i to pole j in a total of $(2^n - 1) + 1 + (2^n - 1) = 2^{n+1} - 1$ legal moves; that is, we have shown that $P(n+1)$ is true.

■

(c) Prove that the number of moves necessary to move all n rings from the first pole to the second is *at least* $2^n - 1$.

Proof. The solution to this part is similar to the solution to part (b). The key is in realizing that when the $n+1$st largest ring on pole i is first moved to pole j, the n rings stacked initially on top of pole i must, by part (a), appear in increasing order on pole k. Thus, by the induction hypothesis at least $2^n - 1$ moves must have occurred already. Similarly, at least another $2^n - 1$ moves are needed after the $n+1$st ring is placed on pole j in order to move the n rings from pole k to pole j. ■

Problem 2. Let R be a binary relation on the set $\{a,b,c,d,e\}$ defined as follows:

$$\begin{aligned} R \ = \{ \quad & (a,a),(a,b),(a,d),(b,a),(b,b),(b,c),(b,d), \\ & (c,b),(c,c),(c,d),(d,b),(d,c),(d,d),(e,e) \quad \} \end{aligned}$$

Answer yes or no to each of the following questions; if you answer no, then defend your answer.

(a) Is R reflexive?

Solution. Yes.

Is R symmetric?

Solution. No. R contains (a, d), but not (d, a).

Is R transitive?

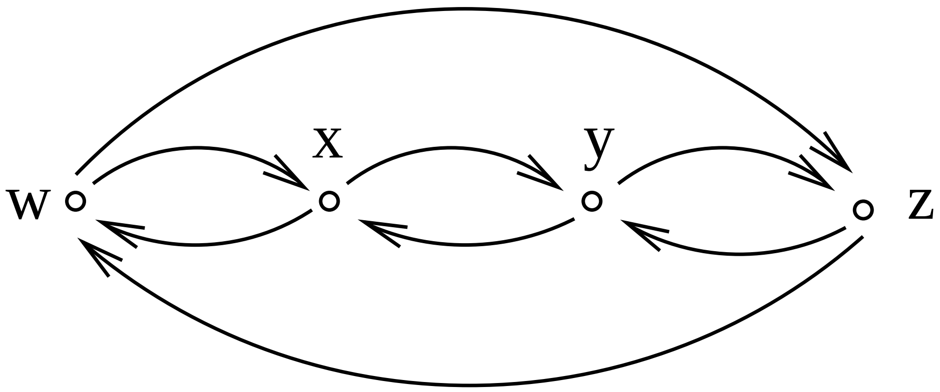
Solution. No. R contains (d, b) and (b, a), but not (d, a).

Problem 3. A relation R on a set A is *weakly transitive* if for all $a, b, c, d \in A$, the relations aRb, bRc, and cRd imply the relation aRd.

Prove or disprove the following statements.

(a) Every symmetric, weakly transitive relation is transitive.

Solution. The claim is false. The diagram below shows a counterexample.



Every reflexive, symmetric, weakly transitive relation is an equivalence relation.

Solution.

Proof. The relation R is an equivalence relation if it is reflexive, symmetric, and transitive. The first two properties hold by assumption; all that remains is to show that R is a transitive relation. Suppose that the relations aRb and bRc hold. Because R is reflexive, the relation aRa also holds. Because R is weakly transtive, the relations aRa, aRb, and bRc imply the relation aRc. Therefore, R is transitive. ∎

Problem 4. Let G_n be a directed graph with vertices numbered $0, 1, \ldots, n-1$. There is a directed edge from vertex i to vertex j if and only if $j \equiv i^2 + i + 1 \pmod{n}$. (See page 119 of Rosen for a definition of $\equiv$ and $\pmod{n}$. As a hint, however, no number theory is required to solve this problem.)

(a) Draw the directed graphs G_1, G_2, and G_3.

Solution.

Prove that if $n \geq 1$, then G_n is not a directed acyclic graph.

Solution.

Proof. Consider the following sequence of vertices in graph G_n.

$$\begin{aligned}
v_1 &= 0 \\
v_2 &= v_1^2 + v_1 + 1 \pmod{n} \\
v_3 &= v_2^2 + v_2 + 1 \pmod{n} \\
\ldots & \quad \ldots \\
v_{n+1} &= v_n^2 + v_n + 1 \pmod{n}
\end{aligned}$$

Note that there is a directed edge from v_i to v_{i+1} for all $1 \leq i \leq n$. Not all of the vertices $v_1, \ldots, v_{n+1}$ can be distinct, since the graph contains only n vertices. Suppose v_j is the first vertex in the sequence to appear a second time, and v_k was the initial appearance of that vertex. Than the sequence of vertices $v_k, v_{k+1}, \ldots, v_{j-1}$ forms a directed cycle. Therefore, G_n is not a directed acyclic graph. ■

Problem 5. A *linear extension* of a poset is a total order consistent with the partial order. That is, if $x > y$ in the partial order, then $x > y$ in the total order also. For example, in the poset defined by the Hasse diagram below, the following relationships hold: $a > b$, $a > c$, $a > d$, $a > e$, $b > c$, and $b > d$.

This poset has eight linear extensions, which are listed in the table below. To clarify the notation, the upper-left entry represents the total order where a is the largest element, b the second largest, and so forth. Note that all of the relationships that hold in the poset also hold for all the total orders listed below.

$a > b > c > d > e$	$a > b > d > c > e$
$a > b > c > e > d$	$a > b > d > e > c$
$a > b > e > c > d$	$a > b > e > d > c$
$a > e > b > c > d$	$a > e > b > d > c$

(a) List all the linear extensions of the poset represented by the Hasse diagram below.

Solution.

$a > b > c > e > d$	$a > c > b > e > d$
$a > b > c > d > e$	$a > c > b > d > e$
$a > b > d > c > e$	

After considering the above examples, Theory Pig formulated the following claim.

Claim. The number of linear extensions of a partially ordered set with n elements always divides $n!$.

Either prove that his claim is correct for all posets or else draw the Hasse diagram of a counterexample and list all linear extensions.

Solution. The claim is false. The 4-element poset depicted below has 5 linear extensions. This is a counterexample, because 5 does not divide 4!.

$$\begin{array}{ll} a > b > c > d & a > b > d > c \\ b > a > c > d & b > a > d > c \\ b > d > a > c & \end{array}$$

Problem 6. An *automorphism* of a graph is a relabeling of the vertices that preserves adjacency. For example, the graph on the left side of the figure below has the automorphism $a \to b, b \to a, c \to c, d \to d$. (Here the notation $x \to y$ means that the vertex labeled x is relabeled y.) The relabeled graph is shown on the right side of the figure. This relabeling is an automorphism because adjacency is preserved; that is, in the relabeled graph, just as in the original, a is adjacent to b and c; b is adjacent to a and c; c is adjacent to a, b, and d; and d is adjacent to c. Every graph has a *trivial automorphism* that assigns each node its original label.

(a) List all non-trivial automorphisms of the graph below using the $x \to y$ notation as in the example.

Solution.

$$\begin{array}{c} a \to e, b \to f, c \to c, d \to d, e \to a, f \to b, g \to g, h \to h \\ a \to e, b \to f, c \to c, d \to d, e \to a, f \to b, g \to h, h \to g \\ a \to a, b \to b, c \to c, d \to d, e \to e, f \to f, g \to h, h \to g \end{array}$$

Draw a graph with at least 2 nodes that has only the trivial automorphism.

Solution.

Problem 7. An n-node graph is said to be *tangled* if there is an edge leaving every set of $\lceil \frac{n}{3} \rceil$ or fewer vertices. As a special case, the graph consisting of a single node is considered tangled. (Recall that the notation $\lceil x \rceil$ refers to the smallest integer greater than or equal to x.)

(a) Find the error in the proof of the following claim.

Claim. Every non-empty, tangled graph is connected.

Proof. The proof is by strong induction on the number of vertices in the graph. Let $P(n)$ be the propostion that if an n-node graph is tangled, then it is connected. In the base case, $P(1)$ is true because the graph consisting of a single node is defined to be tangled and is trivially connected.

In the inductive step, for $n \geq 1$ assume $P(1), \ldots, P(n)$ to prove $P(n+1)$. That is, we want to prove that if an $(n+1)$-node graph is tangled, then it is connected. Let G be a tangled, $(n+1)$-node graph. Arbitrarily partition G into two pieces so that the first piece contains exactly $\lceil \frac{n}{3} \rceil$ vertices, and the second piece contains all remaining vertices. Note that since $n \geq 1$, the graph G has a least two vertices, and so both pieces contain at least one vertex. By induction, each of these two pieces is connected. Since the graph G is tangled, there is an edge leaving the first piece, joining it to the second piece. Therefore, the entire graph is connected. This shows that $P(1), \ldots, P(n)$ imply $P(n+1)$, and the claim is proved by strong induction. ∎

Solution. The error is in the statement, "By induction, each of these two pieces is connected." This is not what the induction hypothesis says; the induction hypothesis states that *if a graph is tangled*, then it is connected.

In abstract terms, we are proving an induction hypothesis of the form "if (this), then (that)". However, we erroneously use the induction hypothesis as if it were simply of the form "(that)'.

Draw a tangled graph that is not connected.

Solution.

An n-node graph is said to be *mangled* if there is an edge leaving every set of $\lceil \frac{n}{2} \rceil$ or fewer vertices. Again, as a special case, the graph consisting of a single node is considered mangled. Prove the following claim.

Claim. Every non-empty, mangled graph is connected.

Solution.

Proof. The proof is by contradiction. Assume for the purpose of contradiction that these exists an n-node graph that is mangled, but not connected. Then the graph must have at least two connected components. However, there can be at most one connected component with more than $\lceil \frac{n}{2} \rceil$ vertices, since the graph has only n vertices in total. Therefore, there exists a connected component with $\lceil \frac{n}{2} \rceil$ or fewer vertices. Since the graph is mangled, there is an edge leaving this component. But this contradicts the definition of a connected component. ∎

Problem 8. Let G and H be undirected graphs with no self-loops. The *product graph* $P = G \times H$ is defined as follows. The vertex set of P is the cartesian product of the vertex set of G and the vertex set of H. Thus, each vertex of P is an ordered pair (v, w) where v is a vertex of G and w is a vertex of H. The edges in the product graph P are of two types. First, for every edge (v_1, v_2) in

G and vertex w in H, there is an edge between (v_1, w) and (v_2, w) in P. Second, for every vertex v in G and edge (w_1, w_2) in H, there is an edge between (v, w_1) and (v, w_2) in P. Note that these two sets of edges are disjoint.

(a) Draw the product of the two graphs shown below. Your diagram must be tidy to receive full credit. In particular, label all the vertices, e.g. $(b, 3)$, and use two different colors or line styles (e.g. dashed and solid) to distinguish the two types of edge defined above.

Solution.

Let G be the graph consisting of two vertices connected by an edge. Let G^n be the product of n copies of G. Use induction to prove that G^n has 2^n vertices and $n2^{n-1}$ edges. (You may assume without proof that the $\times$ operation is associative.)

Solution.

Proof. The proof is by induction on n. Let $P(n)$ be the proposition that G^n has 2^n vertices and $n2^{n-1}$ edges. In the base case, $P(1)$ is true because G^1 has $2^1 = 2$ vertices and $1 \cdot 2^{1-1} = 1$ edge.

In the inductive step, for $n \geq 1$ assume that G^n has 2^n vertices and $n2^{n-1}$ edges to prove that G^{n+1} has 2^{n+1} vertices and $(n+1)2^n$ edges. The remainder of the argument uses the fact that $G^{n+1} = G^n \times G$.

The vertex set of G^{n+1} is the cartesian product of the vertex set of G^n and the vertex set of G. There are 2^n vertices in G^n by induction, and there are 2 vertices in G by the definition of the graph. Therefore, there are $2^n \cdot 2 = 2^{n+1}$ vertices in G^{n+1}.

The edges of $G^n \times G$ are of two types. First, for each edge (v_1, v_2) in G^n and vertex w in G, there is an edge between (v_1, w) and (v_2, w) in G^{n+1}. Thus, the number of edges of the first type is equal to the number of edges in G^n multiplied by the number of vertices in G, which gives $n2^{n-1} \cdot 2 = n2^n$. Second, for each vertex v in G^n and edge (w_1, w_2) in G, there is an edge between (v, w_1) and (v, w_2) in G^{n+1}. Thus, the number of edges of the second type is equal to the number of vertices in G^n multiplied by the number of edges in G, which gives $2^n \cdot 1 = 2^n$. Since these two sets of edges are disjoint, the total number of edges in G^{n+1} is equal to $n2^n + 2^n = (n+1)2^n$.

This shows that $P(n)$ implies $P(n+1)$, and the claim is proved by induction. ■

Problem 9. What's wrong with the following proof that for any sets A, B, C, and D, $(A \cup C) \times (B \cup D) \subseteq (A \times B) \cup (C \times D)$?

Proof. Suppose $(x, y) \in (A \cup C) \times (B \cup D)$. Then $x \in A \cup C$ and $y \in B \cup D$, so either $x \in A$ or $x \in C$, and either $y \in B$ or $y \in D$. We consider these cases separately.

Case 1. $x \in A$ and $y \in B$. Then $(x, y) \in A \times B$.
Case 2. $x \in C$ and $y \in D$. Then $(x, y) \in C \times D$.

Thus, either $(x, y) \in A \times B$ or $(x, y) \in C \times D$, so $(x, y) \in (A \times B) \cup (C \times D)$.

QED ■

Solution.

not done yet

Problem 10. Prove that for any sets A, B, C, and D, if $A \times B$ and $C \times D$ are disjoint, then either A and C are disjoint or B and D are disjoint.

Solution.

not done yet

Problem 11. Consider the following putative theorem:

Theorem? For any sets A, B, C, and D, if $A \times B \subseteq C \times D$ then $A \subseteq C$ and $B \subseteq D$.
Is the following proof correct? If so, what proof strategies does it use? If not, can it be fixed? Is the theorem correct?

Proof. Suppose $A \times B \subseteq C \times D$. Let a be an arbitrary element of A and let b be an arbitrary element of B. Then $(a, b) \in A \times B$, so since $A \times B \subseteq C \times D$, $(a, b) \in C \times D$. Therefore, $a \in C$ and $b \in D$. Since a and b were arbitrary elements of A and B, respectively, this shows that $A \subseteq C$ and $B \subseteq D$. ■

Solution.

not done yet

Problem 12. Suppose R is a relation from A to B and S and T are relations from B to C. Must the following statements be true? Justify your answers with proofs or counterexamples.

(a) If $S \subseteq T$ then $S composition R \subseteq T composition R$.

Solution.
not done yet

(b) $(S intersection T) composition R \subseteq (S composition R) intersection (T composition R)$.

Solution.
not done yet

(c) $(S intersection T) composition R = (S composition R) intersection (T composition R)$.

Solution.
not done yet

□

(d) $(S \cup T) composition R = (S composition R) \cup (T composition R)$.

Solution.
not done yet

□

Problem 13. Suppose R and S are binary relations on a set A. For each part, give either proofs or counterexamples to justify your answers.

(a) Suppose R and S are reflexive. Must $R intersection S$ be reflexive? What about $R \cup S$? What about R^{-1}? What about $R composition S$?

Solution. *not done yet*

□

(b) Suppose R and S are symmetric. Must $R \cup S$ be symmetric? What about $R \cup S$? What about R^{-1}? What about $R composition S$?

Solution. *not done yet*

□

(c) Suppose R and S are transitive. Must $R \cup S$ be transitive? What about $R \cup S$? What about R^{-1}? What about $R composition S$?

Solution. *not done yet*

□

Problem 14. Consider the following putative theorem:
Theorem? Suppose R is a relation on A. If R is symmetric and transitive, then R is reflexive.
Is the following proof correct? If so, what proof strategies does it use? If not, can it be fixed? Is the theorem correct?

Proof. Let x be an arbitrary eleemnt of A. Let y be any element of A such that xRy. Since R is symmetric, it follows that yRx. But then by transitivity, since xRy and yRx we can conclude that xRx. Since x was arbitrary, we have shown that $\forall x \in A(xRx)$, so R is reflexive.
QED. ■

Solution.

not done yet

□

Problem 15. Suppose R is a partial order on A and S is a partial order on B. Define a relation T on $A \times B$ as follows: $T = ((a,b),(a',b')) \in (A \times B) \times (A \times B) | aRa' and bSb'$. Show that T is a partial order on $A \times B$. If both R and S are total orders, will T also be a total order?

Solution. *not done yet*

□

Problem 16. Suppose R is a relation on A, and let S be the transitive closure of R. Prove that if R is symmetric, then so is S. (Hint: Assume that R is symmetric. Prove that $R \subseteq S^{-1}$ and S^{-1} is transitive. What can you conclude about S and S^{-1}?)

Solution. *not done yet*

□

Problem 17. Consider the following putative theorem:
Theorem? Suppose R is a reflexive, antisymmetric relation on A. Let S be the transitive closure of R. Then S is a partial order on A.
Is the following proof correct? If so, what proof strategies does it use? If not, can it be fixed? Is the theorem correct?

Proof. R is already reflexive and antisymmetric. To form the relation S we add more ordered pairs to make it transitive as well. Thus, S is reflexive, antisymmetric, and transitive, so it is a partial order.
QED ■

Solution. *not done yet*

□

Problem 18. Suppose R and S are equivalence relations on A. Must $R intersection S$ be an equivalence relation on A? What about $R \cup S$? What about $R composition S$?

Solution. *not done yet*

□

Problem 19. Let a, b be integers, and assume at least one of a and b is nonzero. Define a set $L_{a,b} \subseteq \mathbb{Z}$ inductively as follows:

- $a, b \in L_{a,b}$.
- If $c, d \in L_{a,b}$, then $c + d \in L_{a,b}$.
- If $c \in L_{a,b}$, then $cn \in L_{a,b}$ for all $n \in \mathbb{Z}$.

(a) Show by induction on the definition of $L_{a,b}$ that any common divisor of a and b also divides every member of $L_{a,b}$.

Solution.

Proof. The induction hypothesis $P(c)$ is "any common divisor of a and b also divides c."

Base case: $P(a)$ is immediate, since any common divisor of a and b certainly divides a. Likewise for $P(b)$.

$(c+d)$ case: Assuming $P(c)$ and $P(d)$, we must prove $P(c+d)$. So suppose e is a common divisor of a and b. Then $e \mid c$ by hypothesis $P(c)$ and $e \mid d$ by hypothesis $P(d)$. That is, $c = ef$ and $d = eg$ for some $f, g \in \mathbb{Z}$. Hence $c + d = ef + eg = e(f + g)$ so $e \mid c + d$, namely $P(c + d)$.

(cn) case: Assuming $P(c)$ and $n \in \mathbb{Z}$, we must prove $P(cn)$. So suppose e is a common divisor of a and b. Then $e \mid c$ by hypothesis. Hence $e \mid cn$, namely $P(cn)$. ∎

Show that if $c, d \in L_{a,b}$ and $c = dq + r$ for some $q, r \in \mathbb{Z}$, then $r \in L_{a,b}$.

Solution. Since $d \in L_{a,b}$, we have $d(-q) \in L_{a,b}$ by the (nc) case. Then since $c \in L_{a,b}$, we have $c + d(-q) = r \in L_{a,b}$ by $(c + d)$ case.

Show that there is a positive integer $g \in L_{a,b}$ which divides every member of $L_{a,b}$. *Hint*: Show that there is a least positive member of $L_{a,b}$.

Solution. At least one of the integers $a, -a, b, -b \in L_{a,b}$ must be positive. Hence by the well-ordering principle, there is a least positive integer $g \in L_{a,b}$.

Suppose $c \in L_{a,b}$. We must show that $g \mid c$.

We prove this by contradiction: if g does not divide c, then the remainder of c divided by g is a positive number smaller than g, which by the previous part is in $L_{a,b}$, contradicting the fact that g is the smallest such integer.

Conclude that $g = \gcd(a, b)$.

Solution. By part (a), any common divisor of a and b divides g. Also, since $a, b \in L_{a,b}$, part (c) implies g is a common divisor of a and b, which implies g is the greatest common divisor.

Conclude that $\gcd(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$.

Solution. It's easy to prove by structural induction that every element of $L_{a,b}$ is equal to $ax + by$ for some $x, y \in \mathbb{Z}$, so g is of this form.

Problem 20. Suppose we start with a sequence of fully parenthesized arithmetic or Scheme expressions, and then erase all the alphanumeric characters other than parentheses. The result is a string of parentheses which "match up".

For example, erasing non-parenthesis characters from the expression `(if (or x y) u v)` leaves the string `(())`. Similarly, erasing non-parentheses from the sequence of three arithmetic expressions

`(x * x), (y + (3 * (z - 9))), ((x + y) * (u + w))`

leaves the string

`()((()))(()())`.

On the other hand, even though the string `())(()` has an equal number of left and right parentheses, it cannot be obtained by erasing in this way—because the two middle parentheses don't match up. Also, no string of parentheses which begins with a right parenthesis or ends with a left parenthesis can match up.

We can give an inductive definition of the set, SMU, of "Strings which Match Up", as follows:

- The empty string (consisting of no parentheses) is an SMU.
- If s and t are SMU's, then the string $(s)t$ is an SMU. That is, the new string starts with a left parenthesis which is followed by the parenthesis characters in the string s, followed by a right parenthesis, followed by the parenthesis characters in the string t.

There is a simple test to determine whether a string of parentheses is an SMU: starting with zero, read the string from left to right adding one for each left parenthesis and -1 for each right parenthesis. A string *counts well* when the count never goes negative and is back to zero by the end of the string. Let CW be the set of strings of parentheses which Count Well.

(a) Prove that CW contains SMU.

Solution. We prove by induction on the definition of SMU (that is, structural induction) that every element of SMU counts well, so SMU is contained in CW. The induction hypothesis is

$$P(s) ::\equiv s \in \text{CW}.$$

Proof.
Base Case: $P(\text{empty string})$ holds since the count of the empty string ends when it starts at zero.
Inductive Step: Assume $P(s)$ and $P(t)$ are true. We need to show that $P((s)t)$ is true.
The count values for $(s)t$ start with 0. Reading the initial left parenthesis yields 1 as the next count value. This 1 serves as the start of a series of count values exactly equal to the count values of s, with each value incremented by one. Since $s \in \text{CW}$ by hypothesis, these incremented count values begin with 1, always stay positive, and end with 1. The right parenthesis immediately after s reduces the ending count to 0. This 0 serves as the start of the remaining count values which are exactly the count values of t. Since $t \in \text{CW}$, these remaining values never go negative and end at 0. Hence the entire sequence of count values for $(s)t$ starts with 0, never goes negative, and ends with 0, which proves that $(s)t \in \text{CW}$. ■

Conversely, prove that SMU contains CW.

Solution. We show that every string $r \in \text{CW}$ is an SMU by strong induction on the length of r. The induction hypothesis is

$$Q(n) ::\equiv \forall r \in \text{CW}(\text{if } r \text{ is length } n, \text{ then } r \in \text{SMU}).$$

Proof.

Base Case $n = 0$: In this case there is only one string of length n, namely the empty string, which is in SMU by definition, proving $Q(0)$.

Inductive Step: Assume that $Q(k)$ is true for all $k \leq n$, we need to prove that $Q(n+1)$ is also true.

So suppose r is a length $n+1$ string that counts well. We must prove that $r \in \text{SMU}$.

Now since r counts well, it must start with a left parenthesis (or else the count would immediately go negative). Likewise, since the count for r returns to the value 0 by the end, r must end with right parenthesis. So there must be a *first* right parenthesis in r after which the count returns to 0. Let s be the substring of r between the initial left parenthesis and this right parenthesis. So

$$r = (s)t$$

for some string t.

Since counts only change by one as each parenthesis character is read, and the count for r *first* returns to 0 after the right parenthesis following s, the count during s must start and end with 1 and must stay *positive* in between. But this implies that a count for s alone, which would start with 0, would also end with 0 and stay *nonnegative* in between. That is, s by itself counts well. Since the length of $s \in \text{CW}$ is less than the length of r, we have by strong induction that $s \in \text{SMU}$.

Further, we know the count for r returns to 0 after the right parenthesis following s, and since $r \in \text{CW}$, the count ends with 0 again and stays nonnegative in between. But this implies that t counts well, and since the length of t is less than the length of r, we have by strong induction that $t \in \text{SMU}$. Now by the second case in the definition of SMU, we conclude $(s)t$, namely r, is in SMU. ■

Problem 21. ???textforproblem???

Solution.

???solutiontoproblem???

□