CS481F01 Solutions 0

A. Demers

12 Sep 2001

1: Facts about enumerations.

(a) Prove: if $\mathbf{S}$ has an enumeration consistent with $\sqsubset$ then $\sqsubset$ is well-founded.

Answer: Suppose $\mathbf{S}$ has an enumeration f consistent with $\sqsubset$. Then for any $x \in \mathbf{S}$, there exists some $j \in \mathbb{N}$ such that $x = f(j)$. By definition of consistency,

$$(y \sqsubset x) \wedge (y = f(i)) \quad \Rightarrow \quad (i < j)$$

So

$$|\{y | y \sqsubset x\}| \quad \leq \quad |\{i | i < j\}| \ \text{ is finite}$$

as required.

(b) Prove: there is no enumeration of the rational numbers consistent with $<$, the usual arithmetic ordering.

Answer: By part (a), it suffices to argue that $<$ over the rationals is not well-founded. It is enough to exhibit a single rational such that infinitely many rationals are less than it. For example, the set

$$\{\frac{1}{2^i} \mid i > 0\}$$

is an infinite set of rationals less that 1, showing that $<$ over the rationals is not well-founded.

(c) Prove: the rational numbers are countable.

Answer: We need to show that there is an enumeration of the rationals. Our definition of an enumeration of **S** requires that the function $f : \mathbb{N} \to \mathbf{S}$ be onto, but not necessarily one-to-one. That's convenient – it means we can just enumerate the ordered pairs $\langle i, j \rangle$, and we don't have to worry about the fact that every rational can be expressed in infinitely many ways as a quotient, for example

$$\frac{1}{2} \quad = \quad \frac{2}{4} \quad = \quad \frac{3}{6} \quad = \quad \ldots.$$

In fact, we even can enumerate the ordered pairs redundantly if we wish. We can use the Fundamental Theorem of Arithmetic (a.k.a. the Prime Factorization Theorem) to define

$$f(n) \quad = \quad \frac{i}{j+1} \quad \text{where} \quad n = 2^i 3^j 5^k \ldots \text{is the prime factorization of } n$$

Clearly this enumeration is onto, since

$$(\forall i \geq 0, k > 0) \quad f(2^i 3^{k-1}) \quad = \quad \frac{i}{k}$$

This enumeration is infinitely redundant, since

$$f(2^i 3^{k-1}) \;=\; f(2^i 3^{k-1} 5) \;=\; f(2^i 3^{k-1} 5^2) \;=\; f(2^i 3^{k-1} 5^3) \;=\; \ldots$$

Although it is redundant, the enumeration shows that the rationals are countable.

(d) Let Σ be a finite alphabet with a total order defined on the symbols. Assume Σ has at least two symbols. Prove: there is no enumeration of Σ^* consistent with lexicographical order.

Answer: Like part (b), this simply requires us to show that lexicographical ordering (we'll call it $\sqsubset$) on Σ^* is not well-founded. Let a and b be distinct symbols of Σ such that $a \sqsubset b$ (this is where we need the assumption that $|\Sigma| \geq 2$). Then

$$(\forall i \geq 0) \quad a^{i+1} b \;\sqsubset\; a^i b$$

is easily proved by induction on i. Thus, $\sqsubset$ contains the infinite descending chain

$$b \sqsupset ab \sqsupset a^2b \sqsupset a^3b \sqsupset \dots$$

and is not well-founded. So by part (a), Σ^* cannot be enumerated in lexicographical order.

(e) Prove that Σ^* is countable.

Answer: As in part c, we will generate a redundant enumeration. Let $k = 1 + |\Sigma|$. Number the symbols of Σ

$$a_1, a_2, \ \dots \ a_{k-1}$$

in an arbitrary order (this does not have to be related to the $\sqsubset$ order). Then define $f : \mathbb{N} \to \Sigma^*$ inductively by

$$\begin{array}{rcl} f(n) & = & \varepsilon \quad \text{if } (n \equiv 0 \pmod{k}) \\ f(n) & = & a_{(n \bmod k)} f(\lfloor \frac{n}{k} \rfloor) \quad \text{o.w.} \end{array}$$

This is easily shown to be onto. Intuitively, we treat n as a base-$(1 + |\Sigma|)$ number, truncate at the first occurence of 0, and map digits to the symbols of Σ.

2: A problem about strings. This problem might remind you of famous Euclid's famous GCD algorithm. Let Σ be a finite alphabet, and let $x, y \in \Sigma^*$. Prove that

$$(xy = yx) \quad \Leftrightarrow \quad \exists s \in \Sigma^*, i, j \in \mathbb{N} \ . \ (x = s^i \ \wedge \ y = s^j)$$

That is, s is a "factor" of both x and y.
□

Answer: This can be proved by induction on $|xy|$.

Basis: If $|xy|$ is 0, then x and y are both ε, so the theorem is satisfied by arbitrary s with $i = j = 0$.

Ind: Note the case $|x| = |y|$ is trivial. So assume wlog (that is, "without loss of generality") that $|x| > |y|$. Let z be the first $|x| - |y|$ characters of x, so

$$x \quad = \quad zw \quad \text{where} \quad |z| = |x| - |y| \quad \text{and} \quad |w| = |y|$$

Now we have

$$xy \quad = \quad yx \quad = \quad yzw$$

where the first equality is by hypothesis and the second by definition of z. By equating the first $|x|$ symbols of xy and yzw we obtain

$$x \quad = \quad yz$$

By equating the last $|y|$ symbols we obtain

$$y \quad = \quad w$$

From this and the definition $x = zw$ we obtain

$$x \quad = \quad zy$$

So we have

$$zy \quad = \quad x \quad = \quad yz$$

Since $|zy| < |xy|$, the inductive hypothesis applies to y and z, and we conclude there exist s, j and k such that

$$y \;=\; s^j \quad \wedge \quad z \;=\; s^k \qquad \text{(by i.h.)}$$

Now, from the definition of z we can say

$$x \quad = \quad zw \quad = \quad zy \quad = \quad s^k s^j \quad = \quad s^{k+j}$$

By setting $i = k + j$ we get

$$y \;=\; s^j \quad \wedge \quad x \;=\; s^i$$

and the theorem follows at last.

3: More infinite sets. An *arithmetic progression* over $\mathbb{N}$ is a set of the form

$$\mathcal{A}_{a,b} = \{ a + ib \mid i \geq 0\}$$

where $a \geq 0$, $b > 0$.

Certainly there are subsets of $\mathbb{N}$ that intersect every arithmetic progression – for example, $\mathbb{N}$ itself is such a subset.

(a) Prove: no finite subset of $\mathbb{N}$ intersects every arithmetic progression.

Answer: If S is finite, let n be the largest element of S. Consider the arithmetic progression $\mathcal{A}_{n+1,1}$, comprising

$$n + 1, (n + 1) + 1, \ldots, (n + 1) + i, \ldots$$

Clearly the intersection of $\mathcal{A}_{n+1,1}$ with S is empty, since every element of $\mathcal{A}_{n+1,1}$ is larger than the largest element of S.

(b) Prove there is a co-infinite subset of $\mathbb{N}$ intersects every arithmetic progression. (A co-infinite set is the complement of an infinite set; i.e., a set $\mathbf{S}$ such that $\mathbb{N} - \mathbf{S}$ is infinite).

Answer: We need to exhibit a co-infinite subset $S \subset \mathbb{N}$ that intersects every arithmetic progression. Equivalently, we can choose an infinite set for $\bar{S}$ and show that no arithmetic progression is entirely contained in our chosen $\bar{S}$. We'll use this second approach.

Choose

$$\bar{S} = \{ n^2 \mid n \geq 0 \}$$

that is, the set of perfect squares. We need to show that no arithmetic progression is entirely contained $\bar{S}$. To show this, given a and b, we choose an r such that

$$2r + 1 > b$$

Now consider the (unique) j such that

$$r^2 < a + bj \leq r^2 + b$$

Clearly such a j exists. Our choice of r guarantees that

$$r^2 \;<\; a+bj \;\leq\; r^2+b \;<\; r^2+2r+1 \;=\; (r+1)^2$$

Thus, $a+bj$ is not a perfect square, since it is strictly between r^2 and $(r+1)^2$. So the arithmetic progression $\mathcal{A}_{a,b}$ is not a subset of $\bar{S}$. Since our choice of a and b was arbitrary, this proves the result.

(c) Does the answer to part (b) change if we weaken the definition of an arithmetic progression to allow $b \geq 0$ instead of $b > 0$?

Answer: It certainly does. Otherwise, why would I have asked the question? Consider the sets

$$\mathcal{A}_{a,0} \;=\; \{\; a+(0i) \mid i \geq 0\} \;=\; \{\; a \;\}$$

Under the revised definition, every singleton set is an arithmetic progression, and the only set that intersects every singleton set is $\mathbb{N}$ itself, which is not co-infinite.

(d) Show that all arithmetic progressions can be intersected by sets that are arbitrarily sparse in the following sense: for every function $f : \mathbb{N} \to \mathbb{N}$ there exists a function $g : \mathbb{N} \to \mathbb{N}$ such that $g \geq f$ and $\mathbf{range}(g)$ intersects every arithmetic progression. That is, g enumerates a set that intersects every arithmetic progression and is more sparse than $\mathbf{range}(f)$.

Answer: Here is a direct construction of a g that works.

First, recall (from the solution to 1c) that there is an enumeration of the ordered pairs of natural numbers

$$\mathbb{N} \times \mathbb{N} \;\;=\;\; \{\langle u_i, v_i\rangle \mid i \geq 0\;\}$$

in some order. This allows us to enumerate the arithmetic progressions

$$\{\; \mathcal{A}_{u_i,v_i+1} \mid i \geq 0 \;\}$$

Both enumerations are redundant, but that won't matter. Now define g by

$$g(i) \;\;=\;\; \min\{\; x \mid (x > f(i)) \wedge (x \in \mathcal{A}_{u_i,v_i+1}) \;\}$$

The set on the right hand side of this expression is clearly nonempty. By construction, $g > f$, and $\mathbf{range}(g)$ intersects the progression $\mathcal{A}_{u_i,v_i+1}$ for all i. Since every arithmetic progression is equal to $\mathcal{A}_{u_i,v_i+1}$ for some i, the desired result follows.