CSE 21 Homework 4 Solutions

Chris Calabro

July 13, 2005

Exercises from Bender

Fn1.1

a

Suppose $f \in \underline{3}^{\{>,<,+,?\}}$ and that in 1-line notation $f = (3,1,2,3)$. f is not yet well-defined since no ordering on the set $\{>,<,+,?\}$ has been specified. However, any such f fails to be an injection since some 2 points in the domain both map to 3. f is a surjection since each element in $\underline{3}$ is mapped to.

b

Suppose $f \in \{>,<,+,?\}^{\underline{3}}$ and that in 1-line notation $f = (?,<,+)$. Then f is well-defined and in 2-line notation is $\begin{pmatrix} 1 & 2 & 3 \\ ? & < & + \end{pmatrix}$. f is an injection but not a surjection since nothing maps to $>$.

c

Suppose $f \in \underline{4}^{\underline{3}}$ and that $2 \to 3, 1 \to 4, 3 \to 2$. Then f is well-defined and in 2-line notation is $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 3 & 2 \end{pmatrix}$. f is an injection but not a surjection.

Fn1.2

To answer this question, we need a bit of machinery.

Theorem 1 (Pigeonhole principle). *Let $m, n \in \mathbb{N}$ with $m < n$ and suppose $f : \underline{n} \to \underline{m}$. Then f is not injective.*

Proof. Suppose indirectly that f is injective. Let m be the smallest natural number such that there is some $n \in \mathbb{N}$ with $m < n$ and injective function $f : \underline{n} \to \underline{m}$. (here we use the fact that $\mathbb{N}$ is well-ordered)

If $m = 0$, then f is not a function, so we may suppose that $m > 0$. Define $g : \underline{n-1} \to \underline{m-1}$ by

$$g(i) = \begin{cases} f(i) & \text{if } f(i) < f(n) \\ f(i) - 1 & \text{if } f(i) > f(n) \end{cases}.$$

Notice that $f(i) = f(n)$ cannot occur if $i \in \underline{n-1}$ since f is injective.

We claim that g is injective, contradicting the minimality of m. To see this, suppose $g(i) = g(j)$. We consider 4 cases:

- If $f(i) < f(n)$ and $f(j) < f(n)$, then $f(i) = g(i) = g(j) = f(j)$, which implies $i = j$.
- If $f(i) > f(n)$ and $f(j) > f(n)$, then $f(i) = g(i) + 1 = g(j) + 1 = f(j)$, which implies $i = j$.
- If $f(i) > f(n)$ and $f(j) < f(n)$, then $f(n) < f(i) = g(i) + 1 = g(j) + 1 = f(j) + 1 < f(n) + 1$, which implies the contradiction that there is some integer strictly between $f(n)$ and $f(n) + 1$ [1], namely $f(i)$. So this case cannot occur.
- The case where $f(i) < f(n)$ and $f(j) > f(n)$ is similar to the previous case.

□

Next we define the *size* of a set A to be the unique natural number equinumerous with it, if there is one [2] , i.e. $|A| = n$ iff $\exists$ bijection $f : \underline{n} \to A$. If there is such an $n \in \mathbb{N}$, then we say that A is finite.

We need to show that this definition is well-defined. I.e. that if $f : \underline{n} \to A$ and $g : \underline{m} \to A$ are both bijections then $m = n$. So suppose not. Wlog assume $m < n$. Then $h = g^{-1} \circ f : \underline{n} \to \underline{m}$ is a bijection, contradicting the pigeonhole principle.

a

Claim 2. *If A, B are finite sets and $f : A \to B$ is an injection, then $|A| \leq |B|$.*

Proof. Suppose $g : \underline{n} \to A$ and $h : \underline{m} \to B$ are bijections and that $n > m$. Then $h^{-1} \circ f \circ g : \underline{n} \to \underline{m}$ is an injection, contradicting the pigeonhole principle. □

It is tempting to think that this proof holds for infinite sets, but since we don't have any definition of what the size of an infinite set is (unless we resort to ordinals), the conclusion doesn't make any sense. After all, what are the 2 objects that we are comparing? What is the object $|A|$?

[1] This can be seen from the axiom of regularity if one defines $n + 1$ as $n \cup \{n\}$.

[2] More generally we could define the size of a set as the least ordinal equinumerous with it, but this would require an excursion into axiomatic set theory.

b

Claim 3. *If A, B are finite sets and $f : A \to B$ is a surjection, then $|A| \geq |B|$.*

Proof. Let $g : \underline{n} \to A, h : \underline{m} \to B$ be bijections and suppose indirectly that $n < m$. Then define $b : \underline{m} \to \underline{n}$ by $b(i) = \min g^{-1} \circ f^{-1} \circ h(i)$. b is well-defined because f is surjective and is injective because f is a function. But b contradicts the pigeonhole principle since $n < m$. □

c

Claim 4. *If A, B are finite sets and $f : A \to B$ is a bijection, then $|A| = |B|$.*

Proof. Combine the previous 2 claims: f is injective, so $|A| \leq |B|$, but f is surjective, so $|A| \geq |B|$. By antisymmetry, $|A| = |B|$. □

d

Claim 5. *If A, B are finite sets and $|A| = |B|$, then $f : A \to B$ is an injection iff it is a surjection.*

Proof. This proof relies heavily on the assumption that A, B are finite. It is false for infinite sets. E.g. let $A = B = \mathbb{N}$. Then $|A| = |B|$, but the successor function, mapping $n \mapsto n + 1$, is an injection that is *not* a surjection.

But since A, B are finite, let $g : \underline{n} \to A, h : \underline{n} \to B$ be bijections.

($\Rightarrow$) Assume f is an injection. Then $d = h^{-1} \circ f \circ g : \underline{n} \to \underline{n}$ is an injection. Suppose indirectly that f fails to be surjective. Then d fails to be surjective as well. Let x be any element of $\underline{n} - \operatorname{im} d$. Define $b : \underline{n} \to \underline{n-1}$ by

$$b(i) = \begin{cases} d(i) & \text{if } d(i) < x \\ d(i) - 1 & \text{if } d(i) > x \end{cases}.$$

Then b is injective, contradicting the pigeonhole principle.

To prove the second half, namely that if f is surjective then it is injective, notice that $b : \underline{n} \to \underline{n}$ defined by $b = \min \circ d^{-1}$ is injective. By the first half of the proof, this implies that it is surjective as well, which implies that d, and hence f, is injective. □

e

Claim 6. *If A, B are finite sets and $|A| = |B|$, then $f : A \to B$ is a bijection iff it is an injection or it is a surjection.*

Proof. Again this relies on finiteness. The forward implication is obvious. To show the reverse implication, use the previous claim. □

Fn1.4

Let $A = \{1, 2, 3\}, B = \{a, b, d\}$ and

$$S_1 = \{(3, a), (2, b), (1, a)\}$$
$$S_2 = \{(1, a), (2, b), (3, c)\}$$
$$S_3 = \{(1, a), (2, b), (1, d)\}$$
$$S_4 = \{(1, a), (2, b), (3, d), (1, b)\}.$$

Then S_1, S_3, S_4 are relations on $A \times B$ but S_2 is not since it involves a c.

S_1 is a functional relation on $A \times B$ but S_3, S_4 are not because they multiply define to what 1 maps and S_2 is not because it is not a relation on $A \times B$.

The inverse of S_3 is a functional relation on $B \times A$, but not S_1, S_4 since they multiply define to what a and b map (respectively) and not S_2 since its inverse is not a relation on $B \times A$.

Fn2.1

In the next few problems, we will use a comma-separated list to denote the cycle notation and a space-separated list to denote the 1-line notation.

a

The permutation $(1, 5, 7, 8)(2, 3)(4)(6)$ in 2 and 1-line forms is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 2 & 4 & 7 & 6 & 8 & 1 \end{pmatrix}$ and $\begin{pmatrix} 5 & 3 & 2 & 4 & 7 & 6 & 8 & 1 \end{pmatrix}$. Its inverse in all 3 forms is $(1, 8, 7, 5)(2, 3)(4)(6)$, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 2 & 4 & 1 & 6 & 5 & 7 \end{pmatrix}$, and $\begin{pmatrix} 8 & 3 & 2 & 4 & 1 & 6 & 5 & 7 \end{pmatrix}$.

b

The permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 7 & 2 & 6 & 4 & 5 & 1 \end{pmatrix}$ in 1-line and cycle form is $\begin{pmatrix} 8 & 3 & 7 & 2 & 6 & 4 & 5 & 1 \end{pmatrix}$ and $(1, 8)(2, 3, 7, 5, 6, 4)$. Its inverse in all 3 forms is $(1, 8)(2, 4, 6, 5, 7, 3)$, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 4 & 2 & 6 & 7 & 5 & 3 & 1 \end{pmatrix}$, and $\begin{pmatrix} 8 & 4 & 2 & 6 & 7 & 5 & 3 & 1 \end{pmatrix}$.

c

The permutation $\begin{pmatrix} 5 & 4 & 3 & 2 & 1 \end{pmatrix}$ in 2-line and cycle form is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$ and $(1, 5)(2, 4)(3)$. Its inverse in all 3 forms is the same as the above since it is its own inverse.

d

The permutation $(5,4,3,2,1)$ in 2 and 1-line forms is $\begin{pmatrix}1&2&3&4&5\\5&1&2&3&4\end{pmatrix}$ and $\begin{pmatrix}5&1&2&3&4\end{pmatrix}$. Its inverse in all 3 forms is $(1,2,3,4,5)$, $\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix}$, and $\begin{pmatrix}2&3&4&5&1\end{pmatrix}$.

Fn2.2

Suppose that we write the numbers $1,2,3,4$ in a row and then perform the following 3 swaps 5 times in a row: swap 1st and 3rd numbers, swap 1st and 4th numbers, swap 2nd and 3rd numbers. Then the location of the number originally in position i is given by the evaluation at i of the permutation $((2,3)(1,4)(1,3))^5 = (1,2,3,4)^5 = (1,2,3,4)$. Since this permutation maps 1 to 2, the number 1 is now in position 2.

Fn2.4

a

$(1,2,3)^{300} = (1)(2)(3)$ since the length of the cycle $(1,2,3)$ divides the exponent 300.

b

$((1,3)(2,5,4))^{300} = (1,3)^{300}(2,5,4)^{300} = (1)(2)(3)$ since the 2 cycles $(1,3)$ and $(2,5,4)$ are disjoint and each has a length that divides 300.

c

Let f be a permutation of $\underline{5}$. Then every cycle in the cyclic decomposition of f has one of the following sizes: $1,2,3,4,5$; the least common multiple of which is $3 \cdot 4 \cdot 5 = 60$. So f^{60} is the identity. So $f^{61} = f$.