Student Online Teaching Advice Notice

The materials and content presented within this session are intended solely for use in a context of teaching and learning at Trinity.

Any session recorded for subsequent review is made available solely for the purpose of enhancing student learning.

Students should not edit or modify the recording in any way, nor disseminate it for use outside of a context of teaching and learning at Trinity.

Please be mindful of your physical environment and conscious of what may be captured by the device camera and microphone during videoconferencing calls.

Recorded materials will be handled in compliance with Trinity's statutory duties under the Universities Act, 1997 and in accordance with the University's policies and procedures.

Further information on data protection and best practice when using videoconferencing software is available at https://www.tcd.ie/info_compliance/data-protection/.

© Trinity College Dublin 2020

5.3 Functions Defined on Finite Sets

Task: Derive conclusions about a function given the number of elements of the domain and codomain, if finite; understand the pigeonhole principle.

Proposition: Let A, B be sets and let $f : A \to B$ be a function. Assume A is finite. Then f is injective $\Leftrightarrow$ $f(A)$ has the same number of elements as A.

Proof:

A is finite so we can write it as $A = \{a_1, a_2, ..., a_p\}$ for some p. Then $f(A) = \{f(a_1), f(a_2), ..., f(a_p)\} \subseteq B$. A priori, some $f(a_i)$ might be the same as some $f(a_j)$. However, f injective $\Leftrightarrow f(a_i) \neq f(a_j)$ whenever $i \neq j \Leftrightarrow f(A)$ has exactly p elements just like A.

qed

Corollary 1 Let A, B be finite sets such that $\#(A) = \#(B)$. Let $f : A \to B$ be a function. f is injective $\Leftrightarrow$ f is bijective.

Proof:

"$\Rightarrow$" Suppose $f : A \to B$ is injective. Since A is finite, by the previous proposition, $f(A)$ has the same number of elements as A, but $f(A) \subseteq B$ and B has the same number of elements as $A \Rightarrow \#(A) = \#(f(A)) = \#(B)$, which means $f(A) = B$, **i.e.** f is also surjective $\Rightarrow$ f is bijective.

"$\Leftarrow$" f is bijective $\Rightarrow$ f is injective.

qed

Corollary 2 (The Pigeonhole Principle) Let A, B be finite sets, and let $f : A \to B$ be a function. If $\#(B) < \#(A)$, $\exists\, a, a' \in A$ with $a \neq a'$ such that $f(a) = f(a')$.

Remark: The name pigeonhole principle is due to Paul Erdös and Richard Rado. Before it was known as the principle of the drawers of Dirichlet. It has a simple statement, but it's a very powerful result in both mathematics and computer science.

Proof: Since $f(A) \subseteq B$ and $\#(B) < \#(A)$, $f(A)$ cannot have as many elements as A, so by the proposition, f cannot be injective, namely $\exists\, a, a' \in A$ with $a \neq a'$ (**i.e.** distinct elements) s.t. $f(a) = f(a')$.

qed

Examples:

1. You have 8 friends. At least two of them were born the same day of the week. #(days of the week) $= 7 < 8$.
2. A family of five gives each other presents for Christmas. There are 12 presents under the tree. We conclude at least one person got three presents or more.
3. In a list of 30 words in English, at least two will begin with the same letter. #(Letters in the English alphabet) $= 26 < 30$.

5.4 Behaviour of Functions on Infinite Sets

Let A be a set, and $f : A \to A$ be a function. If A is finite, then corollary 1 tells us f injective $\Leftrightarrow$ f bijective. What if A is not finite?

5.4.1 Hilbert's Hotel problem (jazzier name: Hilbert's paradox of the Grand Hotel)

A fully occupied hotel with infinitely many rooms can always accommodate an additional guest as follows: The person in Room 1 moves to Room 2. The person in Room 2 moves to Room 3 and so on, **i.e.** if the rooms are $x_1, x_2, x_3...$ define the function $f(x_1) = x_2, f(x_2) = x_3, ..., f(x_m) = x_{m+1}$.

Claim: As defined f is injective but not surjective (hence not bijective!). Let $H = \{x_1, x_2, ...\}$ be the hotel consisting of infinitely many rooms. $f : H \to H$ is given by $f(x_n) = x_{n+1}$. $f(H) = H\backslash\{x_1\}$. We can use this idea to prove:

Proposition: A set A is finite $\Leftrightarrow$ $\forall f : A \to A$ an injective function is also bijective.

Proof: "$\Rightarrow$" If the set A is finite, then it follows immediately from Corollary 1 that every injective function $f : A \to A$ is bijective.
"$\Leftarrow$" We prove the contrapositive. Suppose that the set A is infinite. We shall construct an injective function that is not bijective. Since A is infinite, there exists some infinite sequence $x_1, x_2, x_3, ...$ consisting of distinct elements of A, i.e. an element of A occurs at most once in this sequence. Then there exists a function $f : A \to A$ such that $f(x_n) = x_{n+1}$ for all integers $n \geq 1$ and $f(x) = x$ if x is an element of A that is not in the sequence $x_1, x_2, x_3, ...$ If x is not a member of the infinite sequence $x_1, x_2, x_3, ...$, then the only element of A that gets mapped to x is the element x itself; if $x = x_n$, where $n > 1$, then the only element of A that gets mapped to x is x_{n-1}. It follows that the function f is injective. It is not surjective, however, since no element of A gets mapped to x_1. This function f is thus an example of a function from the set A to itself, which is injective but not bijective.

qed

6 Mathematical Induction

Task: Understand how to construct a proof using mathematical induction.

$\mathbb{N} = \{0, 1, 2, ...\}$ set of natural numbers.
Recall that $\mathbb{N}$ is constructed using 2 axioms:

1. $0 \in \mathbb{N}$
2. If $n \in \mathbb{N}$, then $n + 1 \in \mathbb{N}$

Remarks:

1. This is exactly the process of counting.
2. If we start at 1, then we construct $\mathbb{N}^* = \{1, 2, 3, 4, ...\} = \mathbb{N} \backslash \{0\}$

via the axioms

1. $1 \in \mathbb{N}^*$
2. if $n \in \mathbb{N}^*$, then $n + 1 \in \mathbb{N}^*$

$\mathbb{N}$ or $\mathbb{N}^*$ is used for mathematical induction.

6.1 Mathematical Induction Consists of Two Steps:

Step 1 Prove statement $P(1)$ called <u>the base case</u>.

Step 2 For any n, assume $P(n)$ and prove $P(n+1)$. This is called <u>the inductive step</u>. In other words, step 2 proves the statement $\forall n P(n) \to P(n + 1)$

Remark: Step 2 is not just an implication but infinitely many! In logic notation, we have:

Step 1 $P(1)$

Step 2 $\forall n(P(n) \to P(n + 1))$
Therefore, $\forall n P(n)$
Let's see how the argument proceeds:

1. $P(1)$ Step 1 (base case)
2. $P(1) \to P(2)$ by Step 2 with $n = 1$
3. $P(2)$ by Modus Ponens (tautology #10) applied to 1 & 2
4. $P(2) \to P(3)$ by Step 2 with $n = 2$
5. $P(3)$ by Modus Ponens (tautology #10) applied to 3 & 4
6. $P(3) \to P(4)$ by Step 2 with $n = 3$

7. $P(4)$ by Modus Ponens (tautology #10) applied to 5 & 6

   $\vdots$

8. $P(n)$ for any n.
   This is like a row of dominos: knocking over the first one in a row makes all the others fall. Another idea is climbing a ladder.

Examples:

1. Prove $1 + 3 + 5 + ... + (2n - 1) = n^2$ by induction.

   Base Case: Verify statement for $n = 1$

   When $n = 1$, $2n - 1 = 2 \times 1 - 1 = 1^2$

   Inductive Step: Assume $P(n)$, **i.e.** $1 + 3 + 5 + ... + (2n - 1) = n^2$ and seek to prove $P(n+1)$, **i.e.** the statement $1+3+5...+(2n-1) + [2(n + 1) - 1] = (n + 1)^2$

   We start with LHS: $\underbrace{1 + 3 + 5 + ... + (2n - 1)}_{n^2} + [2(n + 1) - 1] =$

   $n^2 + 2n + 2 - 1 = n^2 + 2n + 1 = (n + 1)^2$

2. Prove $1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$ by induction.

   Base Case: Verify statement for $n = 1$

   When $n = 1, 1 = \frac{1\times(1+1)}{2} = \frac{1\times 2}{2} = 1$

   Inductive Step: Assume $P(n)$, **i.e.** $1 + 2 + 3 + ... + n = \frac{n\times(n+1)}{2}$ and seek to prove $1 + 2 + 3 + ... + n + (n + 1) = \frac{(n+1)(n+2)}{2}$

   $\underbrace{1 + 2 + 3 + ... + n}_{\frac{n(n+1)}{2}} + n + 1 = \frac{n(n+1)}{2} + n + 1 = (n + 1)(\frac{n}{2} + 1) =$

   $(n + 1)\frac{n+2}{2} = \frac{(n+1)(n+2)}{2}$ as needed.