Module 5.1: Bijections

MCIT Online - CIT592 - Professor Val Tannen

Lecture Notes

Bijective functions I

A function $f : A \to B$ is called **bijective** if it is both injective and surjective. A bijective function is also called a **bijection** or a **one-to-one correspondence**.

Example. $h : [0..n] \to [0..n]$ where $h(z) = n - z$.

h is injective because $n - z_1 = n - z_2 \Rightarrow z_1 = z_1$

h is surjective because for $y \in [0..n]$ we can take $z = n - y$ and check $n - (n - y) = y$.

The **bijection rule**: if we can define a bijective function with domain A and codomain B then $|A| = |B|$.

Recall from an earlier segment the one-to-one correspondence between subsets of a set with n elements and strings of bits of length n.

Bijective functions II

The **bijection rule (variant)**: if we can define an **injective** function $f : A \to B$ then $|A| = |\text{Ran}(f)|$.

(If $f : A \to B$ is injective then $f' : A \to \text{Ran}(f)$ where $f'(x) = f(x)$ is bijective.)

Example. $f : [m..n] \to \mathbb{Z}$ where $f(z) = z + p$.

f is injective and $\text{Ran}(f) = [(m + p)..(n + p)]$.

By the variant of the bijection rule $| [m..n] | = | [(m + p)..(n + p)] |$.

A bijection for counting pets I

Problem. Animal Rescue has 5 cats and 3 dogs. How many different groups of these pets that include at least one cat and at least one dog can you adopt?

Answer. (again) Let C be the set of the 5 cats and D the set of the 3 dogs. Let also, $P = C \cup D$ be the set of all pets.

A group of adopted pets is a subset $S \subseteq P$, that is, $S \in 2^P$.

Because pets are either cats or dogs (that is, C and D are **disjoint**) any $S \subseteq P$ is $S = A \cup B$ where $A \subseteq C$ and $B \subseteq D$.

Specifically, A is the set of those pets in S which are cats and B is the set of those pets in S which are dogs.

In set notation $A = S \cap C$ and $B = S \cap D$.

That is, A and B are completely **determined** by S.

A bijection for counting pets II

Answer. (continued) The discussion on the previous slide was in fact about the properties of

$$f : 2^C \times 2^D \to 2^P \qquad \text{where } f(A, B) = A \cup B$$

Indeed, f is **surjective** because any $S \in 2^P$ can be written
. $S = A \cup B$ where $A \in 2^C$ and $B \in 2^D$.

And f is **injective** because any $S = f(A, B)$ uniquely determines (A, B) since
. $A = S \cap C$ and $B = S \cap D$.

Therefore f is a **bijection**.

However, what about the condition "at least one cat and at least one dog"?

A bijection for counting pets III

Answer. (continued) Notation for the set of all **non-empty** subsets:

$$\text{nonempty}(2^X) \;=\; \{T \subseteq X \mid T \neq \emptyset\}$$

Define f' on pairs of non-empty subsets:

$$f' : \text{nonempty}(2^C) \times \text{nonempty}(2^D) \;\to\; 2^P \quad \text{where} \quad f'(A,B) \;=\; A \cup B$$

Because $f'(A,B) = f(A,B)$ and f is injective, f' is also **injective**.

Therefore, the **variant of the bijection rule** applies:

$$|\,\text{nonempty}(2^C) \times \text{nonempty}(2^D)\,| \;=\; |\,\text{Ran}(f')\,|$$

We already seen that $|\,\text{nonempty}(2^X)\,| \;=\; 2^{|X|} - 1$

The sets of pets in $\text{Ran}(f')$ are exactly the ones that have at least one cat and at least one dog! All this was implicit when we solved the problem the first time. The bijection rule is often used implicitly, as it was there.

Module 5.2: Counting Injections

MCIT Online - CIT592 - Professor Val Tannen

Lecture Notes

Counting injections I

We already counted the number of **arbitrary** functions: $|B^A| = |B|^{|A|}$.

Problem. Let A be a set with r elements and B be a set with n elements. How many injective functions with domain A and codomain B can be defined?

Answer. By the injection rule, there is no injective function when $r > n$.

Assume $r \leq n$. W.l.o.g., let $A = \{ a_1, \ldots, a_r \}$.
Why w.l.o.g? Because the **number** of functions should not depend on what the elements of A are, just on **how many** there are.

We construct a function $f \colon A \to B$ in r steps where in step (i) we map a_i to an element that we pick in B, making sure f is injective.

Counting injections II

Answer (continued). We assumed $r \leq n$ and $A = \{ a_1, \ldots, a_r \}$.

We construct an injection $f : A \to B$ in r steps as follows:

(1) Pick an element of B to map a_1 to. Can be done in n ways.

(2) Pick one of the remaining elements to map a_2 to. In $n - 1$ ways.

. . .

(r) Pick one of the remaining $n - (r - 1)20\text{mm}$ elements to map a_r to. In $n - (r - 1) = n - r + 1$ ways.

This is the same as counting partial permutations of r out of $n!$

The number of injections is therefore $\frac{n!}{(n-r)!}$.

Counting bijections

Problem. Let A be a set with r elements and B be a set with n elements. How many bijective functions with domain A and codomain B can be defined?

Answer. By the bijection rule, to have any bijective function $f : A \to B$ we must have $r = n$.

Then we can count bijections in the same way we counted injections, except that r is replaced by n.

The number of bijections is the same as the number of permutations of n elements, namely $n!$.

Activity : Bijections, injections and surjections

Let's assume that A and B have the same nonzero cardinality, n.

How many bijections are there? On the previous slide we showed there are $n!$ bijections.

Similarly, how many injections are there? There are $\frac{n!}{(n-n)!} = n!$ injections, according to how we counted them on a previous slide.

Therefore, there are as many bijections as injections: $n!$.

Question: Does this give a proof of the following?

Proposition If the domain and codomain have the same number of elements then every injection is also a surjection.

In the video, there is a box here for learners to put in an answer. As you read these notes, try it yourself using pen and paper!

Activity : Bijections, injections and surjections (continued)

Answer: Yes!

Let I, S and J be the set of injections, surjections, and bijections, respectively, from A to B.

Then the proposition follows from $J = I \cap S$ that we knew by definition and $|I| = |J|$ that we just observed.

Here are the details:

Since $J \subseteq I$ and $|I| = |J|$, we must have $I = J$.

Thus, every injection from A to B is a bijection, and therefore is also a surjection.

Counting surjections?

First of all, by the surjection rule, to have any surjective functions of domain A and codomain B it must be that $|A| \geq |B|$.

W.l.o.g., assume $A = \{ a_1, \ldots, a_r \}$. We only consider the particular case when B has 2 elements and we have $r \geq 2$. Again w.l.o.g., assume $B = \{0, 1\}$.

We count **complementarily**: we subtract from the total number of functions the number of those functions which are **not surjections**.

If a function $f : A \to B$ is not a surjection there must be some element of B that is not in $\text{Ran}(f)$. Define

$$F_0 = \{f : A \to \{0,1\} \mid 0 \notin \text{Ran}(f)\}$$
$$F_1 = \{f : A \to \{0,1\} \mid 1 \notin \text{Ran}(f)\}$$

Now, $F_0 \cup F_1$ is the set of functions $f : A \to \{0, 1\}$ that are not surjections. How many are there? We need $|F_0 \cup F_1|$.

Still counting surjections?

$$F_0 \cup F_1 \quad \text{where} \quad \begin{aligned} F_0 &= \{f : A \to \{0,1\} \mid 0 \notin \text{Ran}(f)\} \\ F_1 &= \{f : A \to \{0,1\} \mid 1 \notin \text{Ran}(f)\} \end{aligned}$$

Lemma. The sets of functions F_0 and F_1 are **disjoint**.

Proof of Lemma. Suppose (toward a contradiction) that there is some $f \in F_0 \cap F_1$. Then neither 0 nor 1 are in $\text{Ran}(f)$. Therefore $\text{Ran}(f) = \emptyset$, which is impossible.

By the Lemma and by the addition rule, $|F_0 \cup F_1| = |F_0| + |F_1|$. There is exactly one function in F_0, the one that maps all a_i's to 1. Similarly for F_1. Therefore $|F_0 \cup F_1| = 2$.

And the number of surjections is $2^r - 2$.

Module 5.3: Inclusion-exclusion for Cardinality

MCIT Online - CIT592 - Professor Val Tannen

Lecture Notes

Cardinality of union of two sets

When A, B are two **disjoint** sets we have $|A \cup B| = |A| + |B|$.

But what can we say when the sets are **not** disjoint?

$|A| + |B|$ **overcounts**. It counts twice the elements in **both** A and B.

Subtracting those, we get $|A \cup B| = |A| + |B| - |A \cap B|$.

This is called the **Principle of Inclusion-Exclusion (PIE)** for two sets.

Inclusion because we include the count of the elements of A and of B.
Exclusion because we exclude the count of the elements common to both A and B.

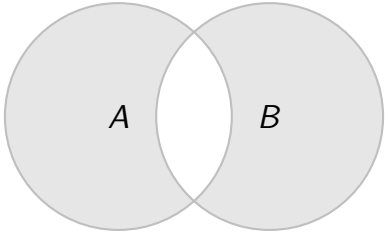
Activity : Principle of inclusion-exclusion

In this activity, we will prove the principle of inclusion-exclusion,

$$|A \cup B| = |A| + |B| - |A \cap B|,$$

in two ways.

First, consider an Euler-Venn diagram in which $B \setminus A$ and $A \setminus B$ and $A \cap B$ appear.



Activity : Principle of inclusion-exclusion (continued)

Observe that $A \setminus B$, $A \cap B$, and $B \setminus A$ are pairwise disjoint and that the following three equations hold.

$$\begin{aligned} A \cup B &= (A \setminus B) \cup (A \cap B) \cup (B \setminus A) \\ A &= (A \setminus B) \cup (A \cap B) \\ B &= (B \setminus A) \cup (A \cap B) . \end{aligned}$$

We can apply the addition rule to each equation to see that

$$\begin{aligned} |A \cup B| &= |A \setminus B| + |A \cap B| + |B \setminus A| \\ |A| &= |A \setminus B| + |A \cap B| \\ |B| &= |B \setminus A| + |A \cap B| . \end{aligned}$$

Activity : Principle of inclusion-exclusion (continued)

From these last three equations, we can derive the Principle of Inclusion-Exclusion:

$$\begin{aligned} |A \cup B| &= |A \setminus B| + |A \cap B| + |B \setminus A| \\ &= |A| - |A \cap B| + |A \cap B| + |B| - |A \cap B| \\ &= |A| + |B| - |A \cap B| \,. \end{aligned}$$

This completes the proof.

Activity : Principle of inclusion-exclusion (continued)

An alternative approach is applying the addition rule four times to see that

$$\begin{aligned} |A \cup B| &= |A| + |B \setminus A| \\ |A \cup B| &= |B| + |A \setminus B| \\ |A| &= |A \setminus B| + |A \cap B| \\ |B| &= |B \setminus A| + |A \cap B| \end{aligned}$$

The sum of the first two equations is

$$2|A \cup B| = |A| + |B| + |B \setminus A| + |A \setminus B| \,.$$

Substituting in the last two equations into this and canceling like terms gives

$$2|A \cup B| = 2|A| + 2|B| - 2|A \cap B| \,.$$

Dividing both sides by 2 yields the PIE.

Cardinality of union of three sets

The **Principle of Inclusion-Exclusion (PIE)** for **three** sets:

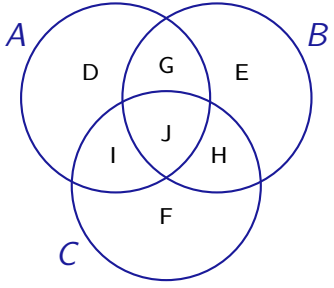
$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| \\ &\quad - |A \cap B| - |B \cap C| - |A \cap C| \\ &\quad + |A \cap B \cap C| \end{aligned}$$

We can justify this similarly. An element in $(A \cap B) \setminus (A \cap B \cap C)$ is added to the count **twice** in $|A| + |B| + |C|$. This justifies subtracting $-|A \cap B|$.

An element in $A \cap B \cap C$ is added to the count **three times** in $|A| + |B| + |C|$ and then subtracted **three times** in $-|A \cap B| - |B \cap C| - |A \cap C|$. This justifies adding $+|A \cap B \cap C|$ at the end.

Activity : Understanding PIE

Consider the following Euler-Venn diagram of sets A, B, and C, with regions labeled D through J.



Activity : Understanding PIE (Continued)

Question: Identify the three regions whose elements are counted exactly once in $|A| + |B| + |C|$.

In the video, there is a box here for learners to put in an answer. As you read these notes, try it yourself using pen and paper!

Activity : Understanding PIE (Continued)

Answer: The regions are D, E, and F.

The three regions whose elements are counted twice in $|A| + |B| + |C|$ and once in $|A \cap B| + |B \cap C| + |A \cap C|$ are $\boxed{\text{G, H, and I}}$.

The one region whose elements are counted three times in $|A| + |B| + |C|$ and three times in $|A \cap B| + |B \cap C| + |A \cap C|$ is $\boxed{\text{J}}$.

Counting by divisibility criteria I

Problem. How many integers in $[1..150]$ are divisible by 3, or by 5, or by 7?

Answer. Let's first ask a simpler question. Given integers $1 < k < n$, how many multiples of k are in $[1..n]$?

Let m be the largest multiple of k that is smaller than (or equal to) n.

Then there are m/k multiples of k in $[1..n]$. Why?

Because n lies between m (multiple of k) and $m+k$ (next multiple of k).

For example, there are $150/3 = 50$ multiples of 3 and $150/5 = 30$ multiples of 5 in [1..150].

As for the multiples of 7, note that 147 is a multiple of 7. Since $147/7 = 21$, there are 21 multiples of 5 in [1..150].

Quiz I

We divide 150 by 35. The (integer) quotient and the remainder are:

A. 3 and 45.

B. 10 and 4.

C. 4 and 10.

Answer

We divide 150 by 35. The (integer) quotient and the remainder are:

A. 3 and 45.
   Incorrect.

B. 10 and 4.
   Incorrect.

C. 4 and 10.
   Correct.

Counting by divisibility criteria II

Answer (continued). We introduce some notation:

$$A = \{n \mid n \in [1..150] \text{ and } 3 \mid n\}$$
$$B = \{n \mid n \in [1..150] \text{ and } 5 \mid n\}$$
$$C = \{n \mid n \in [1..150] \text{ and } 7 \mid n\}$$

The problem asks for $|A \cup B \cup C|$. Sets **overlap**: use PIE.

We saw on the previous slide that $|A| = 50, |B| = 30$ and $|C| = 21$.

Note that $3, 5, 7$ are primes. Therefore

$A \cap B$ consists of the multiples of $3 \cdot 5 = 15$,

$|A \cap C|$ consists of the multiples of $3 \cdot 7 = 21$,

$|B \cap C|$ consists of the multiples of $5 \cdot 7 = 35$,

$|A \cap B \cap C|$ consists of the multiples of $3 \cdot 5 \cdot 7 = 105$.

Counting by divisibility criteria III

Answer (continued).

Similarly to how we computed $|A|, |B|$ and $|C|$ we obtain:

$|A \cap B| = 150/15 = 10,$

$|A \cap C| = 147/21 = 7,$

$|B \cap C| = 140/35 = 4,$ and

$|A \cap B \cap C| = 105/105 = 1.$

By PIE we have

$$|A \cup B \cup C| = 50 + 30 + 21 - 10 - 7 - 4 + 1 = 81$$

Derangements I

Problem. n hat-wearing gangsters leave their distinguishable hats with a restaurant cloakroom attendant. After the meal, the attendant gives them back their hats in a such a way that none of the gangsters gets their own hat.

The returned hats form what is called a "derangement" or a "deranged permutation". How many derangements are possible?

Answer. Let's say the gangsters are $G_1, G_2, \ldots, G_n$ and their respective hats are $h_1, h_2, \ldots, h_n$ (G_i's hat is h_i).

A derangement is a permutation of the set $H = \{h_1, \ldots, h_n\}$ in which h_i does **not** occur in position i for any $i = 1, \ldots, n$.

For example, when $n = 3$ we have only 2 derangements:

. $h_2 h_3 h_1$ $h_3 h_1 h_2$

Quiz II

How many derangements of 4 elements are there?

A. 6

B. 8

C. 9

Answer

How many derangements of 4 elements are there?

A. 6

Incorrect. Please refer to the next slide for more information.

B. 8

Incorrect. Please refer to the next slide for more information.

C. 9

Correct. Please refer to the next slide for more information.

More Information

There are three cases for derangement of 4 elements.

Case 1: a_2 is in position 1.

Case 1.1: a_1 is in position 2. Then the rest of the elements must form a derangement of a set with two elements, and there is exactly one of those.

Case 1.2: a_1 is not in position 2. Then we can replace a_1 with a_2 and erase the first element of the sequence. The result is a derangement of a set with 3 elements and we counted those, there are two of them.

For Case 1, there are $\boxed{1 + 2 = 3}$ possible derangements.

Case 2: a_3 is in position 1. This case is symmetric to Case 1. Therefore, there are three derangements in this case.

Cases 3: a_4 is in position 1.This case is symmetric to Case 1. Therefore, there are three derangements in this case.

In total, there are $\boxed{3+3+3=9}$ derangements.

Derangements II

Problem. Count the number of derangements of n elements.

Answer (continued). The idea is to count **complementarily**.

Define B_i to be the set of permutations in which h_i **does** occur in position i.

Then the set of permutations that are **not** derangements is $B_1 \cup \cdots \cup B_n$.

The total number of permutations is $n!$.

Hence the number of derangements is $n! - |B_1 \cup \cdots \cup B_n|$.

This ends up as

$$n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\right)$$

$B_1, \ldots, B_n$ clearly overlap: need a general PIE!

Read the continuation in a segment entitled "Derangements".

Module 5.4: The Pigeonhole Principle

MCIT Online - CIT592 - Professor Val Tannen

Lecture Notes

The Pigeonhole Principle (PHP)

Get a pair of socks

Problem. A drawer in a dark room contains red, green, blue, and orange socks. How many socks must you take from the drawer to be sure that you have at least one matching pair? (We assume that any two socks of the same color form a matching pair.)

Answer. We apply PHP as follows:

Pigeons: single socks.

Pigeonholes: the four colors (red, green, blue, and orange).

If we pick five or more socks we are guaranteed to have a matching pair.

With similar reasoning: if you have three gloves then at least two of them are for the left hand or at least two of them are for the right hand.

PHP and the injection rule

PHP: Let $f : A \to B$ be a function. If $|A| > |B|$ then there exist at least two elements $x_1, x_2 \in A$ such that $x_1 \neq x_2$ but $f(x_1) = f(x_2)$.

This is saying that if $|A| > |B|$ then f is not injective!

From this formulation we see that the PHP is the **contrapositive** of the injection rule!

Coloring the points of the plane

Problem. Suppose that each point in the plane is colored either red or blue. Show that there always exist two points of the same color that are exactly one unit apart.

Answer. Consider an equilateral triangle ΔABC with the length of each side being one unit. Like all points in the plane, A, B, C are colored red or blue.

By PHP, two of the three points A, B, C must have the same color. By construction, these two are one unit apart.

(Although the set of points in the plane is infinite, we apply PHP to finite sets: the pigeons are A, B, C and the pigeonholes are red and blue.)

The Generalized PHP (GPHP)

In a big enough city there exist two people with exactly the same number of hairs on their head. Apparently the number of hairs on a person's head is at most 200,000. So this requires a city with 200,000 non-bald inhabitants. What about a city of 1M or 10M? There we can say more!

GPHP: r objects are placed into n boxes. For any integer k such that $r > k\,n$ there is at least one box containing at least $k+1$ objects.

Equivalently:

Let $f : A \to B$ and $k \in \mathbb{Z}^+$. If $|A| > k\,|B|$ then there exist at least $k+1$ pairwise distinct elements of A that f maps to the same element of B.

New York City (pop. 8.5M) may have as many as 42 people with the same number of hairs on their head. Because $8,500,000 > 42 \cdot 200,000$.

Quiz I

What is the fewest number of people we can ask to be sure that at least 10 of them are born in the same month?

A. 108

B. 109

C. 110

Answer

What is the fewest number of people we can ask to be sure that at least 10 of them are born in the same month?

A. 108

Incorrect. It could be that out of these 108, 9 are born in each month. $108 = 9 \cdot 12$.

B. 109

Correct. By GPHP, since $109 > 9 \cdot 12$.

C. 110

Incorrect. 110 is **enough** but not the fewest; see second answer.

Quiz II

How about if we want at least 10 of them to have been born in December?

A. 120

B. It is impossible.

C. 1440

Answer

How about if we want at least 10 of them to have been born in December?

A. 120

   Incorrect. See second answer!

B. It is impossible.

   Correct. For any number N we may have a set of N people all born outside of December. In fact they may all be born on January 1st.

C. 1440

   Incorrect. See second answer!

Module 5.5: Friends and Strangers

MCIT Online - CIT592 - Professor Val Tannen

Lecture Notes

Sums of consecutive subsequences I

Problem. Given any sequence of n integers (not necessarily distinct), show that we can always pick some of them (a **subsequence**) which appear in **consecutive** positions in the sequence and whose **sum** is a **multiple** of n.

Answer. Let's first look at some examples.

Sequence: 3 7 5 5
Consecutive subsequences whose sum is divisible by 4:
7 5 3 7 5 5

Sequence: 7 (-4) 7
Consecutive subsequences whose sum is divisible by 3:
7 (-4) (-4) 7

Sums of consecutive subsequences II

Answer (continued). Let $x_1\ x_2\ \cdots\ x_n$ be the sequence of n integers. Consider the following n sums.

$$s_1 = x_1$$

$$s_2 = x_1 + x_2$$

$$\cdots$$

$$s_n = x_1 + x_2 + \cdots + x_n$$

If any of $s_1, s_2, \ldots, s_n$ is divisible by n, then we are done.

On the next slide we consider the other case, namely when each of $s_1, s_2, \ldots, s_n$ is not divisible by n, that is, $n \nmid s_1, \ldots, n \nmid s_n$.

Sums of consecutive subsequences III

Answer (continued). In the case where $n \nmid s_1, \ldots, n \nmid s_n$.

Let r_i be the remainder of the integer division of s_i by n for $i = 1, \ldots, n$. Each $r_i \neq 0$.

Note that there are $n-1$ different possible non-zero remainders: $1, 2, \ldots, n-1$.

We apply PHP with $r_1, \ldots, r_n$ as pigeons and $1, 2, \ldots n-1$ as pigeonholes. Hence there exist distinct p and q such that $r_p = r_q$.

By integer division, for some integers k and ℓ we have

$$s_p = kn + r_p \quad \text{and} \quad s_q = \ell n + r_q$$

W.l.o.g. assume $p < q$. Subtracting both sides, since $r_p = r_q$ we get

$$s_q - s_p \;=\; x_{p+1} + \cdots + x_q \;=\; (\ell - k)n$$

We conclude that $x_{p+1} + \cdots + x_q$ is divisible by n.

The theorem of friends and strangers I

Theorem. In any group of 6 Facebook (FB) users, there are 3 that are pairwise FB **friends** or there are 3 that are pairwise FB **strangers** (that is, **not** FB friends).

(This theorem is a particular case of a famous result of Ramsey that created an entirely new branch of Combinatorics called Ramsey Theory. We will mention this again later.)

Proof. Let A, B, C, D, E, F be a group of six FB users.

Each of B, C, D, E, F is either friends with A or not.

We apply PHP placing B, C, D, E, F into the two categories "friend of A" / "not friend of A".

Since $5 > 2 \cdot 2$ at least 3 of B, C, D, E, F belong to the same category. W.l.o.g., let these 3 be B, C, D. Now we have two cases.

The theorem of friends and strangers II

Proof (continued).

Case 1: B, C, D are in the "friend of A" category. We continue with two subcases.

> **Subcase 1.1:** B, C, D are pairwise strangers. Done.
>
> **Subcase 1.2:** B, C, D are **not** pairwise strangers. Then at least two of them, say w.l.o.g. B and C, are friends. Therefore A, B, C are pairwise friends. Done again.

The theorem of friends and strangers III

Proof (continued).

Case 2: B, C, D are in the "not friend of A" category. Again we have two subcases.

> **Subcase 2.1:** B, C, D are pairwise friends. Done, yet again.
>
> **Subcase 2.2:** B, C, D are **not** pairwise friends. Then at least two of them, say w.l.o.g. B and C, are strangers. Therefore A, B, C are pairwise strangers. Finally, done!

Does it feel like we did some redundant work? Indeed Case 1 and Case 2 use exactly the same reasoning, except that "friend" and "stranger" are swapped! Mathematicians would skip Case 2 entirely, saying that it proceeds **analogously** or **similarly**. We shall do the same in the future!

Self-paced Example: Derangements

Module 5

MCIT Online - CIT592 - Professor Val Tannen

This is a segment that contains material meant to be learned *at your own pace*. We are trying to assist you in this endeavor by organizing the material in a manner similar to the way it is outlined in the recorded segments, however with one additional suggestion. When you see the following marker:

we suggest that you stop and make sure you thoroughly understood the material presented so far before you proceed further.

Derangements

Recall the derangements (gangsters and hats) problem from the lecture segment "Inclusion-exclusion for cardinality":

Problem. n hat-wearing gangsters (this problem is from the 1930s) leave their distinguishable hats with a restaurant cloakroom attendant. After the meal, the attendant gives them back their hats in such a way that none of the gangsters gets their own hat.

The returned hats form what is called a "derangement" or a "deranged permutation." How many **derangements** are possible?

In the lecture segment where we introduced the problem we did give the answer, but we did not go through the full justification. Here we will work with you through the answer in some detail.

Answer. As was mentioned in the lecture segment already, we start by denoting the gangsters as $G_1, G_2, \ldots, G_n$ and their respective hats as $h_1, h_2, \ldots, h_n$ where G_i's hat is h_i.

Using the above notation, a derangement is a permutation of the set $H = \{h_1, \ldots, h_n\}$ in which h_i does **not** occur in position i for any $i = 1, \ldots, n$.

For example, when $n = 3$ we have only 2 derangements:

$$h_2h_3h_1, \text{ and } h_3h_1h_2$$

As you must recall, the lecture segment also included an activity in which you computed the total number of derangements for $n = 4$ obtaining the answer 9.

Here we will show how to count the derangements for n elements, that is, we want to compute the number of permutations of $H = \{h_1, \ldots, h_n\}$ in which h_i does not occur in position i for any $i \in [1 \ldots n]$.

As mentioned in the segment where we introduced the problem, the idea is to count **complementarily**.

Counting derangements the rest of the argument (continued)

We define B_i to be the set of permutations in which h_i **does** occur in position i. It follows that $B_1 \cup \ldots \cup B_n$ is the set of permutations that are **not** derangements.

As we know, the total number of permutations is $n!$. It follows that the total number of derangements is:

$$n! - |B_1 \cup \ldots \cup B_n|$$

Recall that earlier in the module we used the Principle of Inclusion-Exclusion (PIE) to compute the cardinality of the union of two sets, and then you used it to compute the cardinality of the union of three sets. For four sets we may still have the patience to write down the inclusion-exclusion rule (do it!), but for five sets it takes utmost dedication. It is easier to figure out a way to write it in general:

$$|\bigcup_{i=1}^{n} A_i| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{\substack{J \subseteq [1\ldots n] \\ |J=j|}} |\bigcap_{j \in J} A_j|$$

We accept this without proof.

By applying the general formula for PIE we have that:

$$|B_1 \cup \ldots \cup B_n| = |\bigcup_{i=1}^{n} B_i| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{\substack{J \subseteq [1\ldots n] \\ |J=k|}} |\bigcap_{j \in J} B_j|$$

Therefore, the number of derangements is:

$$\begin{aligned} n! - |B_1 \cup \ldots \cup B_n| &= n! - |\bigcup_{i=1}^{n} B_i| \\ &= n! - \sum_{k=1}^{n} (-1)^{k-1} \sum_{\substack{J \subseteq [1\ldots n] \\ |J=k|}} |\bigcap_{j \in J} B_j| \end{aligned}$$

Counting derangements the rest of the argument (continued)

Consider any set $J \subseteq [1 \dots n]$ such that $|J| = k$ and observe that

$$|\bigcap_{j \in J} B_j| = (n-k)!$$

This is because we already know which elements go in the k positions from J and we are left with placing elements in the other $n-k$ positions.

Since there are $\binom{n}{k}$ such sets J, it follows that:

$$\sum_{\substack{J \subseteq [1 \dots n] \\ |J|=k}} |\bigcap_{j \in J} B_j| = \binom{n}{k}(n-k)!$$

Therefore, the number of derangements is:

$$\begin{aligned}
n! - |B_1 \cup \dots \cup B_n| &= n! - \sum_{k=1}^{n} (-1)^{k-1} \sum_{\substack{J \subseteq [1 \dots n] \\ |J|=j|}} |\bigcap_{j \in J} B_j| \\
&= n! - \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)! \\
&= n! - \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!(n-k)!} (n-k)! \\
&= n! - \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!}
\end{aligned}$$

Counting derangements the rest of the argument (continued)

By factoring out $n!$ and some algebra we get that the number of derangements is:

$$\begin{aligned} n! - n! \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k!} &= n!(1 - \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k!}) \\ &= n!(\frac{(-1)^0}{0!} + \sum_{k=1}^{n} \frac{(-1)^k}{k!}) \\ &= n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \end{aligned}$$

This formula does not apply only to hats and gangsters, of course!

In general, the number of derangements of a set of n elements is:

$$n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

Self-paced Example: Floor, Ceiling, and Pigeons

Module 5

MCIT Online - CIT592 - Professor Val Tannen

This is a segment that contains material meant to be learned *at your own pace*. We are trying to assist you in this endeavor by organizing the material in a manner similar to the way it is outlined in the recorded segments, however with one additional suggestion. When you see the following marker:

we suggest that you stop and make sure you thoroughly understood the material presented so far before you proceed further.

Floor, ceiling, and pigeons

First, let us introduce some notation that will prove useful later.

Ceiling and Floor Notation

Let $x \in \mathbb{R}$. The **ceiling** of x, denoted as $\lceil x \rceil$ is the **smallest** integer z such that $z \geq x$. Note that:

$$x \leq \lceil x \rceil < x + 1$$

The **floor** of x, denoted $\lfloor x \rfloor$ is the **largest** integer z such that $z \leq x$. Note that:

$$x - 1 \ < \ \lfloor x \rfloor \ \leq \ x$$

Examples:

- If $z \in \mathbb{Z}$ then $\lceil z \rceil = \lfloor z \rfloor = z$.
- $\lceil 1/2 \rceil = 1 \quad \lfloor 1/2 \rfloor = 0$
- $\lceil \pi \rceil = 4 \quad \lfloor \pi \rfloor = \lceil e \rceil = 3 \quad \lfloor e \rfloor = 2$

(CONTINUED)

Floor, ceiling, and pigeons (continued)

We can now provide an alternative formulation for the Generalized Pigeonhole Principle that we learned in the lecture segment "The pigeonhole principle."

Theorem. If r objects are placed into n boxes then there is at least one box containing at least $\lceil \frac{r}{n} \rceil$ objects.

Proof. We prove the contrapositive.
That is, we will show that if each box contains at most $\lceil \frac{r}{n} \rceil - 1$ objects, then the total number of objects is not equal to r.

Assume that each box contains at most $\lceil \frac{r}{n} \rceil - 1$ objects. Then the total number of objects is at most

$$n\left(\left\lceil \frac{r}{n} \right\rceil - 1\right) < n\left(\frac{r}{n} + 1 - 1\right) = r$$

Thus we have shown that the total number of objects is strictly less than r.

(CONTINUED)

Floor, ceiling, and pigeons (continued)

Let's try a harder problem involving PHP.

Problem. A chess master who has 11 weeks to prepare for a tournament decides to play at least one game every day but, in order not to tire himself, he decides not to play more than 12 games during any calendar week. Show that there exists consecutive days during which the chess master will have played exactly 21 games.

Answer. Let a_i, $1 \leq i \leq 77$, be the total number of games that the chess master has played during the first i days. Note that the sequence of numbers $a_1, a_2, \ldots, a_{77}$ is a strictly increasing sequence.

We have $1 \leq a_1 < a_2 < \ldots < a_{77} \leq 11 \times 12 = 132.$

Now consider the sequence $a_1 + 21, a_2 + 21, \ldots, a_{77} + 21$. We have

$$22 \leq a_1 + 21 < a_2 + 21 < \ldots < a_{77} + 21 \leq 153$$

Clearly, this sequence is also a strictly increasing sequence.

The numbers $a_1, a_2, \ldots, a_{77}, a_1 + 21, a_2 + 21, \ldots, a_{77} + 21$ (154 in all) belong to the set $\{1, 2, \ldots, 153\}$. By the pigeonhole principle there must be two numbers out of the 154 numbers that must be the same.

Since no two numbers in $a_1, a_2, \ldots, a_{77}$ are equal and no two numbers in $a_1 + 21, a_2 + 21, \ldots, a_{77} + 21$ are equal there must exist i and j such that $a_i = a_j + 21$. Hence during the days $j + 1, j + 2, \ldots, i$, exactly 21 games must have been played.

Self-paced Example: Inverse Functions

Module 5

MCIT Online - CIT592 - Professor Val Tannen

This is a segment that contains material meant to be learned *at your own pace*. We are trying to assist you in this endeavor by organizing the material in a manner similar to the way it is outlined in the recorded segments, however with one additional suggestion. When you see the following marker:

we suggest that you stop and make sure you thoroughly understood the material presented so far before you proceed further.

Inverse functions

Given $f : A \to B$, an **inverse** of f is a function $g : B \to A$ such that

$$\forall x \in A \quad g(f(x)) = x \qquad \text{and} \qquad \forall y \in B \quad f(g(y)) = y$$

The definition above implies that an inverse of f, if it exists, is completely determined by f. Therefore we will talk about **the** inverse of a function.

Examples:

- The inverse of $\quad \mathsf{squ} : [0, \infty) \to [0, \infty) \quad \mathsf{squ}(x) = x^2 \quad$ is the function $\mathsf{sqrt} : [0, \infty) \to [0, \infty) \quad \mathsf{sqrt}(x) = \sqrt{x}$.

- The inverse of $\quad \exp : \mathbb{R} \to (0, \infty) \quad \exp(x) = 2^x \quad$ is the function $\mathsf{loga} : (0, \infty) \to \mathbb{R} \quad \mathsf{loga}(x) = \log_2 x$.

- The inverse of $f : \{1, 2, 3\} \to \{a, b, c\}$ given by the table

$x \in \{1, 2, 3\}$	$f(x) \in \{a, b, c\}$
1	c
2	a
3	b

  is the function $g : \{a, b, c\} \to \{1, 2, 3\}$ given by the table

$y \in \{a, b, c\}$	$g(y) \in \{1, 2, 3\}$
a	2
b	3
c	1

Bijections and inverse functions

Proposition. A function has an inverse iff it is a bijection. The inverse of a bijection is also a bijection.

Proof. We have to prove an "iff". This means proving two implications.

Claim. If $f : A \to B$ has an inverse, $g : B \to A$, then f is a bijection.

To prove that f is bijection we have to prove that it is both an injection and a surjection.

1. f is injective.

   Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$. We are going to show that $x_1 = x_2$ thus verifying the contrapositive of the definition of injectivity.

   Using the definition of inverse, we have $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$. Done.

2. f is surjective.

   Let $y \in B$. We want to show that there exists $x \in A$ such that $f(x) = y$. For that, we can take $x = g(y)$. Indeed $f(g(y)) = y$ using the definition of inverse.

(CONTINUED)

Bijections and inverse functions (continued)

Claim. If $f : A \to B$ is a bijection, then it has an inverse, $g : B \to A$.

To define g observe that for any $y \in B$ there exists, because f is surjective, an $x \in A$ such that $f(x) = y$.
Moreover, that x is the only element of A that f maps to y, because f is injective.
Now we define $g(y)$ to be that x.

Since $f(x) = y$ we have $g(f(x)) = g(y) = x$. And since $g(y) = x$ we have $f(g(y)) = f(x) = y$. So f and g are inverses.

There is one more part to the proposition, namely to show that the inverse is also a bijection. But notice that the definition of inverses is **symmetric**. Therefore the argument made in the first Claim applies to the inverse!

(CONTINUED)

Functions and sequences

Let $n \in \mathbb{Z}^+$ and consider the set $F = \{0,1\}^{[1..n]}$ the elements of F are functions with domain $[1..n]$ and codomain $\{0,1\}$.

Consider also the set S of sequences of bits (elements of $\{0,1\}$) of length n. Notice that the positions in such a sequence are exactly the numbers in $[1..n]$.

We are going to show that the sets F and S are in one-to-one correspondence, that is, there is a bijection with domain F and codomain S.

And we will show this by defining a pair of inverse function.

Define $\varphi : F \to S$ as follows. For any function $f \in F$ define $\varphi(f)$ as the sequence of bits of length n that in position k has the bit $f(k)$, for all $k \in [1..n]$.

Now define $\psi : S \to F$ as follows. For any sequence of bits of length n, $s \in S$ define $\psi(s)$ as the function $f : [1..n] \to \{0,1\}$ that maps $k \in [1..n]$ to the bit in position k in s.

The hard work is done. Convince yourselves (intuition suffices) that φ and ψ are inverse to each other, that is,

$$\varphi(\psi(s)) \;=\; s \qquad\qquad \psi(\varphi(f)) \;=\; f$$

Many mathematicians do not distinguish between sequences and functions, even preferring to **define** a sequence as a special kind of function, making the one-to-one correspondence that we have shown **implicit**.

However the formalities involved in working with functions can obscure the intuition. It's better to think of sequences as their own kind of object studied in Discrete Mathematics.

Self-paced Example: The Erdős-Szekeres Theorem

Module 5

MCIT Online - CIT592 - Professor Val Tannen

This is a segment that contains material meant to be learned *at your own pace*. We are trying to assist you in this endeavor by organizing the material in a manner similar to the way it is outlined in the recorded segments, however with one additional suggestion. When you see the following marker:

we suggest that you stop and make sure you thoroughly understood the material presented so far before you proceed further.

Erdős-Szekeres Theorem

In a story recounted in this module you found out more about Erdős, the most prolific mathematician of the 20th century. Furthermore, in the previous segment you learned about the Pigeonhole Principle (PHP).

In this self-paced segment, we will learn about one of Erdős' theorems that he co-authored with the mathematician George Szekeres. This theorem is called the Erdős-Szekeres Theorem and utilizes the Pigeonhole Principle. Take a moment to recall PHP.

Erdős-Szekeres Theorem *Let n be a positive integer. Every sequence of n^2+1 distinct integers must contain a monotone (increasing or decreasing) subsequence of length $n+1$.*

Proof: Before we begin the proof, we should make precise the definition of a **subsequence**.

Subsequence means that some of the elements are chosen and listed in the same order. The elements of the subsequence need not be consecutive (next to each other) in the sequence.

Suppose we have a sequence of distinct integers. (We don't need this in the proof, but w.l.o.g. you can assume that they are positive; why?)

(CONTINUED)

Erdős-Szekeres Theorem (continued)

For each integer x in the sequence let u_x be the length of a **longest increasing subsequence** that starts at x (we count x in the length) and let d_x be the length of a **longest decreasing subsequence** that starts at x (again we count x in the length).

Before we proceed further in the proof, given our definitions of u_x and d_x, we present a lemma.

Lemma: If $x \neq y$ are distinct integers in the sequence such that x occurs before y then $(u_x, d_x) \neq (u_y, d_y)$.

Proof: We have two cases to consider: when $x < y$ and when $x > y$.

Indeed, if $x < y$ then $u_x > u_y$. Can you figure out why, on your own?

Indeed, this is because, if $x < y$, then we can consider the increasing sequence that starts with x and continues with y and a longest increasing sequence that starts at y. The length of this sequence is $1 + u_y$ so we must have $u_x \geq 1 + u_y$. Hence $u_x > u_y$ and therefore $(u_x, d_x) \neq (u_y, d_y)$.

Similarly, if $x > y$ then $d_x > d_y$ and thus $(u_x, d_x) \neq (u_y, d_y)$.

Now we can return to the proof of the theorem.

(CONTINUED)

Erdős-Szekeres Theorem (continued)

We prove the theorem by contradiction. Suppose that all monotone subsequences have length at most n. Then for each x in the sequence we have $u_x, d_x \in [1..n]$

We use PHP with the pairs $(i, j) \in [1..n] \times [1..n]$ as pigeonholes, with the integers in the sequence as pigeons, and with pigeon x being placed in pigeonhole (u_x, d_x).

Since we have $n^2 + 1$ integers in the sequence but only n^2 pairs in $[1..n] \times [1..n]$, we must have $(u_x, d_x) = (u_y, d_y)$ for some distinct $x \neq y$.

This contradicts the above lemma and so we have completed our proof of the Erdős-Szekeres theorem.