Module 3.1: Stars and Bars

MCIT Online - CIT592 - Professor Val Tannen

Lecture Notes

Stars and bars I

Problem. How many different ways are there to buy a dozen (12) donuts when 5 given glazes (chocolate, dulce de leche, etc.) are available? Assume

(1) that there is an unlimited supply of donuts of each glaze.

(2) that donuts of the same glaze are indistinguishable.

Answer. Consider 12 donuts **before glazing** when they cannot be distinguished. Represent them by 12 stars in a row.

Now place 4 bars between some of the stars. For example:

$$***|**|*|****|**$$

This separates the unglazed donuts into 5 contiguous parts.

Glaze the donuts in the first part with chocolate (C), the second part with dulce de leche (D) and three other flavors, (E), (F), (G), as follows:

```
***|**|*|****|**
CCC DD E FFFF GG
```

Stars and bars II

Answer. (continued)

Note that you may not buy all the glazes. This is represented with bars at the beginning or end, or adjacent bars:

```
***||******|***|       ||*********|***|       *|*|||**********
CCC||EEEEEE|FFF|       ||EEEEEEEEE|FFF|       C|D|||GGGGGGGGGG
```

Note also that the ordering of `C,D,E,F,G` does not matter, only **how many** stars are in each part. Thus, to avoid overcounting, we **fix an ordering** of `C,D,E,F,G` and then we count.

The 12 stars and the 4 bars form a sequence with $12 + 4 = 16$ positions. Out of these, we choose 4 positions where we put the bars.

The answer is $\binom{16}{4}$.

Stars and bars

The donuts and glazes problem is an example of a general class of counting problems that can all be solved with **stars and bars**. These include:

- Counting the number of ways of putting n indistinguishable marbles in r distinguishable urns.
- Counting the number of ways of distributing n indistinguishable coins to r distinguishable children (see next).
- Counting the number of nonnegative solutions to the Diophantine equation $x_1 + x_2 + \cdots + x_r = n$ (see another segment in this module).
- Counting the number of bags/multisets of size n made from elements of a set of size r (see lecture segment "Counting anagrams" in this module).

In all these cases, stars and bars applies and the answer is :

$$\binom{n+r-1}{r-1}.$$

Coins to children I

Problem. In how many ways can we distribute 11 indistinguishable coins to 3 distinguishable children?

What if each child must receive at least one coin?

Answer. (to the first part) We notice the analogy: the coins correspond to the unglazed donuts and the glazes to the children!

Using stars and bars with children `A,B,C`:

```
***|******|**
AAA|BBBBBB|CC
```

The answer is $\binom{11+2}{2} = \binom{13}{2}$

Coins to children II

Answer. (to the second part)

We need to modify our solution to the first part, because now we need every child to have at least one coin. This is solved with a simple trick: we begin by giving each child a coin!

The remaining distributions of $11 - 3 = 8$ coins are counted by stars and bars.

The answer is $\binom{8+2}{2} = \binom{10}{2}$.

Activity : Counting Marbles

The goal of this activity is to count the number of ways in which n indistinguishable marbles can be put in r distinguishable urns such that each urn contains at least 2 marbles.

Before we get to the answer, let us first consider several questions:

Question: What are the minimum number of marbles that are needed?

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

Activity : Counting Marbles (Continued)

Answer: $\boxed{2r}$.

We have r urns, each of which needs at least 2 marbles.

Now consider:

Question: Draw a stars and bars diagram for $r = 4$ and $n = 15$.

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

Activity : Counting Marbles (Continued)

Answer: $*|*|**|***$

Any diagram with $15 - 2 \cdot 4 = 7$ stars and 3 bars is a correct answer for this question. We remove $2r$ marbles from the stars and bars diagram because they must belong to their respective urns.

Now we go back to the question asked in the beginning: count the number of ways in which n indistinguishable marbles can be put in r distinguishable urns such that each urn contains at least 2 marbles.

Question: What do you think could be the answer?

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

Activity : Counting Marbles (Continued)

Answer:

$$\binom{n-2r+r-1}{r-1} = \binom{n-r-1}{r-1}$$

We apply the stars and bars formula to $n-2r$ stars and $r-1$ bars, removing the ones that must belong to their respective urns from consideration.

Module 3.2: Negating Statements

MCIT Online - CIT592 - Professor Val Tannen

Lecture Notes

Disprove

Problem. Prove or disprove: 0 is both a natural number and a positive integer.

To **disprove** a statement P means to prove its **negation**: not P.

This problem is simple, but when we have complex statements we need **rules** for negating them.

In addition we will see that manipulating negation is very effective in some proof techniques.

Negation of disjunction/conjunction

Memorize: "the negation of disjunction is conjunction"
and "the negation of conjunction is disjunction"

In logical notation: $\neg(P_1 \vee P_2)$ is $(\neg P_1) \wedge (\neg P_2)$
and $\neg(P_1 \wedge P_2)$ is $(\neg P_1) \vee (\neg P_2)$

These are known as **De Morgan's Laws**.

Examples:

"not($x < 0$ or $x > 0$)" is "$x \geq 0$ and $x \leq 0$".

"not($x \in A \cup B$)" is "$x \notin A$ and $x \notin B$".

"not($x \in A \cap B$)" is "$x \notin A$ or $x \notin B$".

Negation of quantifiers

Memorize: "the negation of universal is existential"
and "the negation of existential is universal"

In logical notation: $\neg(\forall x\ P(x))$ is $\exists x\ \neg P(x)$
and $\neg(\exists x\ P(x))$ is $\forall x\ \neg P(x)$

Examples:

"not$(\forall x\ \exists y\ \mathit{loves}(x,y))$" is "$\exists x\ \forall y\ \neg \mathit{loves}(x,y)$"

"not(everybody loves somebody)" is "there is somebody who loves nobody".

"not$(\exists x\ \ x \in A \cap B)$" is "$\forall x\ \ x \notin A$ or $x \notin B$".

"not $(\exists k\ \ n = 2k)$" is "$\forall k\ \ n \neq 2k$"

(For simplicity we omitted the conditions that n and k are integers.)

Shouldn't the negation of "n is even" be the statement "n is odd"?

With some arithmetic help, yes! (See next activity.)

ACTIVITY : Negation of Even

Recall that you can always write any number n as $n = 2q + r$ where q is called quotient and r is called remainder.

Question:

What possible remainders are there when we divide a positive integer n by 2?

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

ACTIVITY : Negation of Even (Continued)

Answer: 0 and 1.

There are only two possibilities for n when we divide n by 2. Notice that $r = 0$ corresponds to our definition of even and $r = 1$ corresponds to our definition of odd.

Activity : Negation of Even (Continued)

Using this fact, we now prove that the negation of "n is even" is "n is odd." In other words, n is odd if and only if n is not even.

If n is not even, then by the definition of even, there is no integer k such that $n = 2k$. In particular, we cannot have $n = 2q$, so the remainder of n divided by 2 cannot be 0. The only other possibility is that the remainder is 1, meaning that $n = 2q + 1$, so n is odd.

On the other hand, if n is odd, then by the definition of odd there is some integer ℓ such that $n = 2\ell + 1$, so the remainder of n divided by 2 must be 1. This implies that there is no integer k such that $n = 2k$, so n is not even.

We will give proofs that use negation in future segments, and from now on we will assume that the negation of "n is even" is "n is odd" and the negation of "n is odd" is "n is even."

Negation of implication

Memorize: the negation of "if premise then conclusion" is
"premise **and** the negation of the conclusion"

In logical notation: $\neg(P_1 \Rightarrow P_2)$ is $P_1 \wedge \neg P_2$

Examples:

"not(if p is prime and p is even then $p = 2$)" is
"p is prime and p is even and $p \neq 2$"

"not(for all x if x is odd then x is prime)" is
"there is an x that is odd and not prime"

Counterexamples

Problem. Fermat: prove or disprove that for every natural number n, the number $2^{2^n} + 1$ is prime.

Answer. Euler disproved this, showing that $2^{2^5} + 1$ is not prime.

Terminology: we say that Euler showed that $n = 5$ is a **counterexample** for the universally quantified statement:

$$\forall n \;\; natural(n) \;\Rightarrow\; prime(2^{2^n} + 1)$$

A counterexample to this statement is a proof of its negation, which (by the rules we saw) is an existentially quantified statement:

$$\exists n \;\; natural(n) \;\wedge\; \neg prime(2^{2^n} + 1)$$

Quiz

According to our rules, the **negation** of “every prime number is odd” is

A. 2 is a prime number but is also an even number.

B. There exists a prime number that is not odd.

C. There exists a prime number that is not even.

Answer

According to our rules, the **negation** of "every prime number is odd" is

A. 2 is a prime number but is also an even number.
   Incorrect. This is true, but it is not the negation of the statement above.

B. There exists a prime number that is not odd.
   Correct. The negation of a universal quantifier is an existential qualifier.

C. There exists a prime number that is not even.
   Incorrect. This is true, but it is not the negation of the statement above.

More Information

The given statement "every prime number is odd" is false. Its negation is therefore true. Interestingly, all the answers are true statements, but only (B) is the negation of the given statement.

We can think of (A) as proving the negation statement, rather than the negation itself. Therefore (A) is a counterexample.

Module 3.3: Converse and Contrapositive

MCIT Online - CIT592 - Professor Val Tannen

Lecture Notes

Converse and contrapositive

Memorize:

the **converse** of "if P_1 then P_2" is "if P_2 then P_1", and

the **contrapositive** of "if P_1 then P_2" is "if (not P_2) then (not P_1)".

In logical notation:

the **converse** of $P_1 \Rightarrow P_2$ is $P_2 \Rightarrow P_1$, and

the **contrapositive** of $P_1 \Rightarrow P_2$ is $\neg P_2 \Rightarrow \neg P_1$.

The contrapositive is **logically equivalent** to the original implication. This leads to:

Proof pattern: instead of the implication, prove its contrapositive,

The converse is **not** logically equivalent to the original implication (in general).

A false converse I

Problem. Consider the statement "for all integers z, if z is divisible by 4 then it is even". Prove it. State the converse (of the implication under the quantifier) and disprove it.

Answer. (first part)

Assume that z is divisible by 4.

Then $z = 4k$ for some integer k.

Then $z = 2\ell$ where $\ell = 2k$.

ℓ is an integer, hence z is even.

A false converse II

Answer. (second part)

The converse is "for all integers z, if z is even then it is divisible by 4".

To disprove this, we prove the negation:

"there exists an even integer z that is not divisible by 4".

Of course there is such an integer! Take $z = 6$.

Often, we avoid stating the negation explicitly and we just say that $z = 6$ is a **counterexample**, as discussed in a prior slide.

In this problem we found an implication statement that is not logically equivalent to its converse since one is true and the other one is false.

A proof by contrapositive I

Problem. Consider the statement "for any integers x, y, if xy is even then at least one of x, y must be even". Write the contrapositive (of the implication under the quantifiers) and prove it.

Answer. Let's rewrite the statement :

"for any integers x, y, if xy is even then x is even or y is even"

Using De Morgan's Laws and recalling that we agreed that the negation of even is odd we write the contrapositive :

"for any integers x, y, if x is odd and y is odd then xy is odd"

A proof by contrapositive II

Answer. (continued) We wish to show that:

"for any integers x, y, if x is odd and y is odd then xy is odd"

Assume that x and y are both odd.

Then $x = 2k + 1$ for some integer k.
And $y = 2\ell + 1$ for some integer ℓ.

Then

$$. \qquad xy \;=\; (2k+1)(2\ell+1) \;=\; 4k\ell + 2k + 2\ell + 1 \;=\; 2(2k\ell + k + \ell) + 1$$

$2k\ell + k + \ell$ is an integer, hence xy is odd.

This was an example where the (logically equivalent) contrapositive was much easier to prove.

Module 3.4: Truth Tables

MCIT Online - CIT592 - Professor Val Tannen

Lecture Notes

From statements to boolean expressions

How are proof patterns **justified**? We will explain them with the help of **boolean expressions**.

The proof patterns were described **abstractly** using symbols: P_1, P_2, P_3 .

To justify the proof patterns **all that matters** is whether the symbols P_1, P_2, P_3 represent true or false statements.

So we replace them with **boolean variables** that can take one of two **truth values**: T (for true!), and F (for false!). We use $p, q, r, s, p_1, p_2, \ldots$.

Boolean expressions are obtained from boolean variables using logical connectives: $\vee, \wedge, \neg, \Rightarrow$.

Examples: $(p \wedge \neg q) \Rightarrow r \qquad p_1 \wedge (p_2 \Rightarrow s)$

Truth assignments and truth tables

A **truth assignment** gives each boolean variable a value, `T` or `F`.

Given a truth assignment to its variables, a boolean expression also yields `T` or `F`.

We use **truth tables** to specify this. For each logical connective:

p	$\neg p$
T	F
F	T

p	q	$p \wedge q$	$p \vee q$	$p \Rightarrow q$
T	T	T	T	T
T	F	F	T	F
F	T	F	T	T
F	F	F	F	T

Memorize these tables!

Quiz

Given the boolean expression $(p \wedge \neg p) \vee (\neg q)$ and a truth assignment $p = \mathtt{T}$ and $q = \mathtt{F}$, what is the resulting truth value?

A. `T`.

B. `F`.

Answer

Given the boolean expression $(p \wedge \neg p) \vee (\neg q)$ and a truth assignment $p = \mathtt{T}$ and $q = \mathtt{F}$, what is the resulting truth value?

A. T.

Correct. Please refer to the truth table in the next slide.

B. F.

Incorrect. Please refer to the truth table in the next slide.

More Information

This is the truth table for the boolean expression. As you can see, the quiz corresponds to the second line in this truth table.

p	q	$\neg p$	$\neg q$	$(p \wedge \neg p)$	$(p \wedge \neg p) \vee (\neg q)$
T	T	F	F	F	F
T	F	F	T	F	T
F	T	T	F	F	F
F	F	T	T	F	T

False implies anything!

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

If the premise is false then the implication is true, regardless of the conclusion.

Or, "false implies anything".

For example, consider

"if $2 + 2 = 5$ then there exist infinitely many twin primes".

This implication is true...

...although we don't know (as of the time of this writing) whether there are infinitely many twin primes (this is the **Twin Prime Conjecture**).

The implication will remain true even after the conjecture is settled!

Holds vacuously

Some people say that such implications, in which the premise is always false, "hold vacuously".

This is inspired by a particular case with implication under a universal quantifier. For example:

"for any natural number n such that $kn = k^2 + 1$ for some integer $k > 1$, there exist twin primes bigger than n"

But the set of natural numbers n such that $kn = k^2 + 1$ for some integer $k > 1$ is empty!

$$. \quad \{\, n \in \mathbb{N} \mid \exists k \in \mathbb{Z} \;\; k > 1 \wedge kn = k^2 + 1\} \; = \; \emptyset$$

ACTIVITY : Vacuously true statement

In this activity, we prove: "there are no natural numbers n such that $kn = k^2 + 1$ for some integer $k > 1$."

First consider the statement $kn = k^2 + 1$. We can rewrite this statement as $n = \frac{k^2+1}{k}$. For n to be a natural number we must have $k \mid (k^2 + 1)$.

Since $k \mid k^2$, it follows that the remainder of the division of for $k^2 + 1$ by k is 1. This problem then reduces to finding integers k for which $k \mid 1$.

Question: For what integers k do we have $k \mid 1$?

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

ACTIVITY : Vacuously true statement (Continued)

Answer: The only integers that divide 1 are -1 and 1.

We can now complete the proof.

There are **no** integers $k > 1$, such that $k \mid (k^2 + 1)$.

Therefore, there are **no** natural numbers n such that $kn = k^2 + 1$ for some integer $k > 1$.

We justify "by contrapositive"

Proof pattern. Instead of "if P_1 then P_2" you can prove "if (not P_2) then (not P_1)".

The contrapositive transformation on boolean expressions goes

from $p \Rightarrow q$2cm to $\neg q \Rightarrow \neg p$.

The following truth table justifies this transformation:

p	q	$p \Rightarrow q$	$\neg q$	$\neg p$	$\neg q \Rightarrow \neg p$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

We justify "by cases"

Proof pattern. To prove "if P_1 or P_2 then P_3" you prove "if P_1 then P_3 and if P_2 then P_3".

The by-cases transformation on boolean expressions goes

$$\text{from} \quad p \vee q \Rightarrow r \quad \text{to} \quad (p \Rightarrow r) \wedge (q \Rightarrow r).$$

The following justifies this (only 4 of 8 rows are shown):

p	q	r	$p \vee q$	$p \vee q \Rightarrow r$	$p \Rightarrow r$	$q \Rightarrow r$	$(p \Rightarrow r) \wedge (q \Rightarrow r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	T	T	T	T	T
T	F	F	T	F	F	T	F

ACTIVITY : "By-cases" Justification

Now we try finishing the truth table for the "by-cases" justification by providing the final 4 rows of the truth table.

Recall that we want to convert from $p \vee q \Rightarrow r$ to $(p \Rightarrow r) \wedge (q \Rightarrow r)$.

Question:

Assuming $p = \texttt{F}$, $q = \texttt{T}$ and $r = \texttt{T}$, what are the truth values of $p \vee q \Rightarrow r$ and $(p \Rightarrow r) \wedge (q \Rightarrow r)$? Are they the same?

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

Activity : "By-cases" Justification

Answer: Look at the first row below. Both truth values are T.

p	q	r	$p \vee q$	$p \vee q \Rightarrow r$	$p \Rightarrow r$	$q \Rightarrow r$	$(p \Rightarrow r) \wedge (q \Rightarrow r)$
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	F
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

Logical equivalence

Two boolean expressions are **logically equivalent** when they yield the same truth value for the same truth assignments to their variables. Notation: $\equiv$

Here are some logically equivalent boolean expressions:

$$\begin{aligned}
p \Rightarrow q &\equiv \neg q \Rightarrow \neg p \quad \text{(Contrapositive)} \\
p \vee q \Rightarrow r &\equiv (p \Rightarrow r) \wedge (q \Rightarrow r) \quad \text{(By-cases)} \\
p \Rightarrow q &\equiv \neg p \vee q \quad \text{(Law of Implication)} \\
\neg(p \Rightarrow q) &\equiv p \wedge \neg q \quad \text{(Disproving implication)} \\
\neg(p \vee q) &\equiv \neg p \wedge \neg q \quad \text{(De Morgan's Law I)} \\
\neg(p \wedge q) &\equiv \neg p \vee \neg q \quad \text{(De Morgan's Law II)} \\
\neg\neg p &\equiv p \quad \text{(Law of Double Negation)}
\end{aligned}$$

We verified the first two with the truth tables in the previous slides. More is discussed in the activities that follow.

ACTIVITY : More truth tables

The logical equivalence $p \wedge \neg p \equiv F$ is also known as **Law of Contradiction**. The truth table to verify this logical equivalence is shown below.

p	$\neg p$	$p \wedge \neg p$
T	F	F
F	T	F

ACTIVITY : More truth tables (Continued)

Similarly, $p \vee \neg p \;\equiv\; T$ is the **Law of the Excluded Middle**.

It is also known as **Tertium Non Datur** (Latin for "a third (possibility) is not given").

The truth table to verify this logical equivalence is shown below.

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

Module 3.5: Proofs by Contradiction

MCIT Online - CIT592 - Professor Val Tannen

LECTURE NOTES

Proofs by contradiction I

A statement of the form "P and (not P)" is called a **contradiction**. It is always **false**. In what follows C stands for a statement that is a contradiction.

Proof pattern. To prove "P" we can instead prove "if (not P) then C".

This proof pattern is justified by the following logical equivalence:

$$p \equiv \neg p \Rightarrow \mathtt{F}.$$

(Yes, F, and T, are also boolean expressions.)

We verify this logical equivalence with a truth table:

p	$\neg p$	$\neg p \Rightarrow \mathtt{F}$
T	F	T
F	T	F

Proofs by contradiction II

Proof pattern (variant). To prove "if P then Q" we can instead prove "if P and (not Q) then C".

This proof pattern is justified by the following logical equivalence:

$$. \quad p \Rightarrow q \quad \equiv \quad p \wedge \neg q \Rightarrow \mathtt{F}$$

We also verify this logical equivalence with a truth table:

p	q	$p \Rightarrow q$	$\neg q$	$p \wedge \neg q$	$p \wedge \neg q \Rightarrow \mathtt{F}$
T	T	T	F	F	T
T	F	F	T	T	F
F	T	T	F	F	T
F	F	T	T	F	T

Quiz

Is $p \wedge q \Rightarrow r$ logically equivalent to $p \Rightarrow (q \Rightarrow r)$? Before you answer, construct the truth table to see if they are logically equivalent.

A. Yes.

B. No.

Answer

Is $p \wedge q \Rightarrow r$ logically equivalent to $p \Rightarrow (q \Rightarrow r)$?

A. Yes.

   Correct. Refer to the truth table below.

B. No.

   Incorrect.

More Information

This is the complete truth table for the question above.

p	q	r	$p \wedge q$	$(p \wedge q) \Rightarrow r$	$q \Rightarrow r$	$p \Rightarrow (q \Rightarrow r)$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	T	T	T
T	F	F	F	T	T	T
F	T	T	F	T	T	T
F	T	F	F	T	F	T
F	F	T	F	T	T	T
F	F	F	F	T	T	T

A proof by contradiction

Problem. Prove that if $3n + 2$ is odd then n is odd.

Answer. Assume (toward a contradiction) that $3n + 2$ is odd but n is even.

Then there exists an integer k such that $n = 2k$.

Therefore we can write $3n + 2 = 3(2k) + 2 = 2(3k + 1)$

Since k is an integer, clearly $3k + 1$ is an integer.
Thus $3n + 2$ is even, by definition.

This contradicts the assumption that $3n + 2$ is odd.
(We have proven that $3n + 2$ is both even and odd!)

Square root of 2 is irrational I

Problem. Prove that $\sqrt{2}$ is not rational.

Answer. Assume (toward a contradiction) that $\sqrt{2}$ is rational.

Then $\sqrt{2}$ can be expressed as a fraction $\sqrt{2} = \frac{a}{b}$.
with $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$.

Moreover, we can assume **without loss of generality** (abbreviation w.l.o.g.) that a and b have no common divisors (factors) other than 1. Then

$$
\begin{aligned}
2 &= \frac{a^2}{b^2} && \text{(Squaring both sides)} \\
a^2 &= 2b^2 && \text{(Multiplying both sides by 2)}
\end{aligned}
$$

From the second equality it follows that a^2 is even.

Square root of 2 is irrational II

Lemma. Let z be an integer. If z^2 is even then z is even.

Proof of Lemma. We prove the contrapositive: if z is odd then z^2 is odd.
Assume that z is odd.

Then $z = 2k + 1$ for some integer k.

Then $z^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Therefore z^2 is also odd.

Square root of 2 is irrational III

Problem. Prove that $\sqrt{2}$ is not rational.

Answer (continued). The last two statements we have shown were

$$a^2 = 2b^2 \qquad \text{and} \qquad a^2 \ \text{is even.}$$

By the Lemma a is also even. That is, for some integer k, $a = 2k$.

$$\begin{aligned} a^2 &= 4k^2 && \text{(Squaring both sides)} \\ 4k^2 &= 2b^2 && \text{(Using } a^2 = 2b^2\text{)} \\ 2k^2 &= b^2 && \text{(Dividing by 2)} \end{aligned}$$

Hence b^2 is even and by the Lemma, b is even.

Therefore both a and b are even and this **contradicts** the assumption that a and b have no common factors except 1.

Activity : Proof techniques

Lemma: Let z be an integer. If z^2 is even then z is even.

Recall that we just proved this lemma by contrapositive. In this activity, we are going to prove the same lemma by contradiction.

In fact, any proof by contrapositive of $p \Rightarrow q$ can be transformed into a proof by contradiction that follows the variant pattern. We'll walk through this transformation using the example above.

Assume p. In this example, we assume that z^2 is even.

Assume toward a contradiction that $\neg q$. In this example we assume toward a contradiction that z is odd.

ACTIVITY : Proof techniques (Continued)

Now we insert the proof for the contrapositive $\neg q \Rightarrow \neg p$.

This is the same proof we saw in this segment:

If z is odd, then by definition of odd, $z = 2k + 1$ for some integer k.

Then by squaring both sides,

$$z^2 \; = \; 4k^2 + 4k + 1 \; = \; 2(2k^2 + 2k) + 1$$

Question: At this point what can we conclude?

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

ACTIVITY : Proof Techniques (Continued)

Answer:

Therefore z^2 is also odd.

Observe that we have derived $\neg p$ for this example.

Now you have reached a contradiction between $\neg p$ and p.

More generally, this activity demonstrates that any proof by contrapositive can be converted into a proof by contradiction.

Module 3.6: Counting Anagrams

MCIT Online - CIT592 - Professor Val Tannen

Lecture Notes

Counting anagrams I

An **anagram** is a reordering of the letters of a word.

Example. Anagrams (that make some sense in English) for `Mathematics`: `ThematicSam`, `MismatchTea`, `ActHammiest`.

Problem. How many anagrams does `mississippi` have (including itself)?

Answer. Notice that what matters is which letters occur, and how many times each. We use the following representation:

$$\{1 \cdot \mathtt{m},\, 4 \cdot \mathtt{i},\, 4 \cdot \mathtt{s},\, 2 \cdot \mathtt{p}\}$$

to capture all the information we need for the count.

`mississippi` and its anagrams are sequences of length 11 but it is pretty clear that the answer is not 11!, the number of permutations. Why?

Because we can swap around the different occurrences of the **same** letter and the sequence stays the **same**!

Counting anagrams II

Problem. How many anagrams does `mississippi` have (including itself)?

Answer (continued). Notice that we can construct an anagram as follows:

(1) Choose 1 out of 11 positions to put `m`. In $\binom{11}{1}$ ways.

(2) Choose 4 out of $11 - 1 = 10$ remaining positions to put `i`'s. In $\binom{10}{4}$ ways.

(3) Choose 4 out of $10 - 4 = 6$ remaining positions to put `s`'s. In $\binom{6}{4}$ ways.

(4) Choose 2 out of $6 - 4 = 2$ remaining positions to put `p`'s. In $\binom{2}{2}$ ways.

By the multiplication rule the answer is

$$\binom{11}{1} \cdot \binom{10}{4} \cdot \binom{6}{4} \cdot \binom{2}{2} = \frac{11!}{1! \cdot 10!} \cdot \frac{10!}{4! \cdot 6!} \cdot \frac{6!}{4! \cdot 2!} \cdot \frac{2!}{2! \cdot 0!} = \frac{11!}{1! \cdot 4! \cdot 4! \cdot 2!}$$

Counting anagrams III

Problem. How many anagrams does `mississippi` have (including itself)?

Alternative answer . We start with permutations of 11 letters. That's 11! and it would be correct if all 11 letters were distinct. As we saw, however, for `mississippi` this is **overcounting**. But by **how much**?

When we count all permutations the **same** anagram is counted as many times as there are

(1) Permutations of the 1 `m`. That's 1! times.
(2) Permutations of the 4 `i`'s. That's 4! times.
(3) Permutations of the 4 `s`'s. That's 4! times.
(4) Permutations of the 2 `p`'s. That's 2! times.

So the same anagram is counted $1! \cdot 4! \cdot 4! \cdot 2!$ times.

Therefore the number of anagrams is $\frac{11!}{1! \cdot 4! \cdot 4! \cdot 2!}$

Anagrams are permutations of bags

A **multiset** or **bag** is an unordered collection in which repetitions are allowed.

The letters in `mississippi` form a bag:

. $\{ 1 \cdot \mathtt{m}, 4 \cdot \mathtt{i}, 4 \cdot \mathtt{s}, 2 \cdot \mathtt{p} \}$ same as $\{ \mathtt{m,i,i,i,i,s,s,s,s,p,p} \}$

The **size** of a bag is the total number of elements, repetitions included. The bag $\{ \mathtt{m,i,i,i,i,s,s,s,s,p,p} \}$ has size 11.

A **permutation** of a bag lists all its elements, repetitions included, in some order. Thus, a permutation of $\{ \mathtt{m,i,i,i,i,s,s,s,s,p,p} \}$ is exactly an anagram of `mississippi`.

Consider the bag $\{ n_1 \cdot a_1, \ n_2 \cdot a_2, \ldots, \ n_k \cdot a_k \}$

The number of permutations of this bag is

$$\frac{(n_1 + n_2 + \ldots + n_k)!}{n_1! \cdot n_2! \cdots n_k!}$$

ACTIVITY : Example of distinguishable v. indistinguishable

Consider n distinguishable books (different titles) and k bins labeled $B_1, B_2, \ldots, B_k$. How many ways are there to distribute the books among the bins so that bin B_i receives n_i books and $n_1 + n_2 + \ldots + n_k = n$?

ACTIVITY : Example of distinguishable v. indistinguishable (continued)

Let the n distinguishable books be arranged in a sequence: $b_1, \ldots, b_n$. (In a moment we shall see that it does not matter in what order we arrange them, as long as the same ordering is used during the whole counting procedure.)

For each distribution of the books to the bins, modify the sequence above by replacing each book with a piece of paper on which is written the label of the bin the book goes into.

ACTIVITY : Example of distinguishable v. indistinguishable (continued)

Now it might help to think of the resulting sequences as words over the alphabet $B_1, \ldots, B_k$. The distributions correspond one-to-one to anagrams of length n using n_i copies of letter B_i, etc.! And now you see that it does not matter in what order we arranged the books originally.

As we learned in this segment, the answer is the number of permutations of the bag $\{n_1 \cdot B_1, \ldots, n_k \cdot B_k\}$, that is:

$$\binom{n}{n_1\ n_2\ \cdots\ n_k} = \frac{n!}{n_1!\, n_2! \cdots n_k!}$$

ACTIVITY : Example of distinguishable v. indistinguishable (continued)

Now suppose that the bins are still labeled but the books are all copies of "Moby Dick". In other words, the bins are distinguishable but the books are indistinguishable.

Question:

Now, how many ways are there to distribute the books among the bins?

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

ACTIVITY : Example of distinguishable v. indistinguishable (continued)

Answer:

1 way!

In this case we put any n_i copies of Moby in B_i for $i = 1 \ldots, k$ and this can be done in exactly 1 way!

ACTIVITY : Example of distinguishable v. indistinguishable (continued)

Finally suppose that both the bins and books are indistinguishable.

Question:

Now, how many ways are there to distribute the books among the bins?

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

ACTIVITY : Example of distinguishable v. indistinguishable (continued)

Answer: 1 way!

We can proceed in two steps.

In step 1 we label the bins with the labels $1, \ldots, k$. Since the bins were indistinguishable to begin with this can be done in exactly 1 way. (That is, any way will work!)

In step 2 we distribute the books among the bins just as we did in the previous question. As we saw there is only 1 way of doing this.

By the multiplication rule, there is exactly $1 \cdot 1 = 1$ way here too.

Self-paced Example: There are Infinitely Many Primes

Module 3

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.

Euclid's Proof of Infinitely Many Primes

Recall from an earlier module that we have defined a prime number as follows:

An integer m is **prime** when m has exactly two (positive) factors: 1 and itself, and moreover $m \geq 2$.

In this segment we explore an ancient proof (from Euclid) which shows that **there are infinitely many prime numbers**. It is a beautiful example of proof by contradiction and it illustrates how old mathematical reasoning really is.

Assume, for the sake of contradiction, that there are only finitely many primes. Let p be the largest prime number. Then all the prime numbers can be listed in increasing order as

$$2, 3, 5, 7, 11, 13, \ldots, p$$

In particular, no integer strictly bigger than p can be prime.

Our proof by contradiction aims to show that $2, 3, 5, 7, 11, 13, \ldots, p$ **cannot be all** the primes.

Consider an integer n that is formed by multiplying all these prime numbers and then adding 1. That is,

$$n = (2 \cdot 3 \cdot 5 \cdot 7 \cdots p) + 1$$

Observe that n is **not divisible** by any of $2, 3, 5, 7, \ldots p$ because the remainder for the division of n by each of these is 1.

(CONTINUED)

Euclid's Proof of Infinitely Many Primes

To continue the proof we use the following:

Proposition. Every integer has at least one prime factor only for integers > 1.

We omit the proof of this fact, except to note that it follows, for example, from the *Unique Prime Factorization Theorem* also known as the *Fundamental Theorem of Arithmetic* which is discussed in an optional segment in this module. Direct proofs are also possible, using concepts that we learn later in the course such as induction.

Therefore, in particular, the integer that we defined earlier, $n = (2 \cdot 3 \cdot 5 \cdot 7 \cdots p) + 1$ has a prime factor.

Since, as we have shown, n is not divisible by any of $2, 3, 5, 7, \ldots p$, these cannot be all the prime numbers. Contradiction, and this ends Euclid's proof.

By the way, a common mistake when trying to reproduce this proof is to claim that n must be prime and the contradiction is that n is bigger than the biggest assumed prime, p.

However, it does not follow from the definition of n that it must be prime. In fact, in general it is not a prime:

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 \;=\; 30031 \quad \text{which is divisible by} \;\; 59$$

Luckily, we do not need the primality of n to reach a contradiction. We just needed that n has a prime factor, like any integer.