MATH1050 Dis-proofs

1. **What is 'dis-proving'?**

   To dis-prove a statement is the same as to prove the negation of the statement concerned. Equivalently we may prove that the statement concerned is false.

   To proceed to give a dis-proof for a statement, we have to first distinguish whether it starts with a universal quantifier or with a existential quantifier. For the former, we give a **dis-proof by counter-example**. As for the latter, we give a '**wholesale refutation**'.

2. **Dis-proofs by counter-example.**

   Consider a statement of the form below:

   M: '*Let so-and-so be an element of the set blah-blah-blah. Suppose so-and-so satisfies bleh-bleh-bleh. Then so-and-so satisfies bloh-bloh-bloh.*'

   And also consider its variation in the forms below:

   M_1: '*Let so-and-so be an element of the set blah-blah-blah. So-and-so satisfies bloh-bloh-bloh.*'

   M_2: '*Suppose so-and-so satisfies bleh-bleh-bleh. Then so-and-so satisfies bloh-bloh-bloh.*'

   M is actually a statement starting with a universal quantifier:

   $$(\forall x)(H(x) \to K(x)).$$

   $H(x)$ corresponds to the part '*so-and-so is an element of the set blah-blah-blah and so-and-so satisfies bleh-bleh-bleh*'. $K(x)$ corresponds to the part '*so-and-so satisfies bloh-bloh-bloh*'.

   The negation $\sim M$ of the statement M is a statement starting with an existential quantifier:

   $$(\exists x)(H(x) \wedge (\sim K(x))).$$

   In a 'wordy' form, it reads:

   $\sim M$: '*There exists so-and-so amongst the elements of the set blah-blah-blah such that so-and-so satisfies bleh-bleh-bleh and so-and-so does not satisfy bloh-bloh-bloh.*'

   Therefore to prove $\sim M$, we proceed by naming one 'concrete' so-and-so amongst the elements of the set *blah-blah-blah* which indeed satisfies *bleh-bleh-bleh* and which does not satisfy *bloh-bloh-bloh.* Such a concrete so-and-so is called a **counter-example** for the statement M which we dis-prove.

   More generally, to dis-prove a statement of the form

   $$\underbrace{(\forall x)(\forall y)\cdots(\forall z)}_{\text{all } \forall\text{'s}}(H(x, y, \cdots, z) \longrightarrow K(x, y, \cdots, z)),$$

   we prove its negation, which is the statement

   $$\underbrace{(\exists x)(\exists y)\cdots(\exists z)}_{\text{all } \exists\text{'s}}[H(x, y, \cdots, z) \wedge (\sim K(x, y, \cdots, z)].$$

   We refer to such an argument a dis-proof-by-counter-example.

3. **Simple examples of dis-proofs-by-counter-example.**

   (a) We want to dis-prove

   M: *Let* $x \in \mathbb{R}$. $x^2 > 0$.

   Very formally presented, M is:

   For any object x, *(if* $x \in \mathbb{R}$ *then* $x^2 > 0$*).*

   So the statement $\sim M$ reads:

   There exists some object x_0 *such that (*$x \in \mathbb{R}$ *and* $x^2 \leq 0$*).*

   A dis-proof by counter-example for the statement M is:

- Take $x_0 = 0$. Note that $x_0 \in \mathbb{R}$. Also ${x_0}^2 = 0^2 = 0 \leq 0$. So the statement '${x_0}^2 > 0$' is false.

(b) We want to dis-prove

> M: *Let $n \in \mathbb{N}$. Suppose n is divisible by 3. Then n is divisible by 5.*

Very formally presented, M is:

> *For any object n, if $n \in \mathbb{N}$ and n is divisible by 3 then n is divisible by 5.*

So $\sim M$ reads:

> *There exists some object n_0 such that ($n \in \mathbb{N}$ and n is divisible by 3 and n is not divisible by 5).*

A dis-proof by counter-example for the statement M is:

- Take $n_0 = 3$. 3 is divisible by 3. But 3 is not divisible by 5.

4. **Further examples of dis-proofs-by-counter-example.**

(a) We want to dis-prove

> M: *Let $x, y \in \mathbb{Z}$. Suppose x is divisible by y and y is divisible by x. Then $x = y$.*

Very formally presented, M is:

> *For any objects x, y, [if ($x \in \mathbb{Z}$, $y \in \mathbb{Z}$ and x is divisible by y and y is divisible by x) then $x = y$].*

So $\sim M$ reads:

> *There exist some objects x, y such that ($x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ and x is divisible by y and y is divisible by x) and $x \neq y$].*

A dis-proof by counter-example for the statement M is:

- Take $x_0 = 1$, $y_0 = -1$. $x_0, y_0 \in \mathbb{Z}$. x_0 is divisible by y_0 and y_0 is divisible by x_0. But $x_0 \neq y_0$.

(b) We want to dis-prove

> M: *Let a, b be rational numbers. $a + b\sqrt{2}$ is irrational.*

Very formally presented, M is:

> *For any objects a, b, [if (a is a rational number and b is a rational number) then $a + b\sqrt{2}$ is irrational].*

So $\sim M$ reads:

> *There exist some objects a, b such that (a is a rational number and b is a rational number and $a + b\sqrt{2}$ is not irrational).*

A dis-proof by counter-example for the statement M is:

- Take $a_0 = 0$, $b_0 = 0$. a_0, b_0 are rational numbers. $a_0 + b_0\sqrt{2} = 0$. $a_0 + b_0\sqrt{2}$ is not irrational.

(c) We want to dis-prove

> M: *Let $r, s, t \in \mathbb{R}$. Suppose r is a non-zero rational number and s is an irrational number. Then both $rs + t, rs - t$ are irrational numbers.*

A dis-proof by counter-example for the statement M is:

- Take $r_0 = 1$, $s_0 = \sqrt{2}$, $t_0 = \sqrt{2}$. r_0 is a non-zero rational number. s_0 is an irrational number. Note that $r_0 s_0 - t_0 = 0$. One of $r_0 s_0 + t_0, r_0 s_0 - t_0$, namely the latter, is not irrational.

(d) We want to dis-prove

> M: *The product of any two distinct irrational numbers is irrational.*

At first sight this statement is not of the form 'if blah-blah-blah then bleh-bleh-bleh'. However, M can be re-written in this way:

> *Let u, v be irrational numbers. Suppose $u \neq v$. Then uv is an irrational number.*

A dis-proof by counter-example for the statement M is:

- Take $u_0 = \sqrt{2}$, $v_0 = -\sqrt{2}$. u_0, v_0 are irrational numbers, and $u_0 \neq v_0$. $u_0 v_0 = -2$, and $u_0 v_0$ is not an irrational number.

(e) We want to dis-prove

> M: *Let A, B, C be sets. Suppose $A \cap B \neq \emptyset$ and $B \cap C \neq \emptyset$ and $C \cap A \neq \emptyset$. Then $A \cap B \cap C \neq \emptyset$.*

Very formally presented, M is:

For any sets A, B, C, if ($A \cap B \neq \emptyset$ and $B \cap C \neq \emptyset$ and $C \cap A \neq \emptyset$) then $A \cap B \cap C = \emptyset$.

So $\sim M$ reads:

There exist some sets A_0, B_0, C_0 such that ($A_0 \cap B_0 \neq \emptyset$ and $B_0 \cap C_0 \neq \emptyset$ and $C_0 \cap A_0 \neq \emptyset$ and $A_0 \cap B_0 \cap C_0 = \emptyset$).

A dis-proof by counter-example for the statement M is:

- Take $A_0 = \{0, 1\}$, $B_0 = \{1, 2\}$, $C_0 = \{0, 2\}$. Here $0, 1, 2$ are regarded as pairwise distinct objects.
  Note that $A_0 \cap B_0 = \{1\}$, $B_0 \cap C_0 = \{2\}$, $C_0 \cap A_0 = \{0\}$.
  So $A_0 \cap B_0 \neq \emptyset$ and $B_0 \cap C_0 \neq \emptyset$ and $C_0 \cap A_0 \neq \emptyset$.
  Note that $A_0 \cap B_0 \cap C_0 = \emptyset$.

(f) We want to dis-prove

M: *Let n be a positive integer, and P, Q be $(n \times n)$-square matrices with real entries. Suppose $PQ = 0$. Then $P = 0$ or $Q = 0$.*

(Here 0 stands for the zero (2×2)-square matrix.)

Very formally presented, M is:

For any positive integer n, for any $(n \times n)$-square matrices P, Q with real entries, if $PQ = 0$ then ($P = 0$ or $Q = 0$).

So $\sim M$ reads:

There exist some positive integer n, some $(n \times n)$-square matrices P, Q with real entries such that $PQ = 0$ and ($P \neq 0$ and $Q \neq 0$).

A dis-proof by counter-example for the statement M is:

- Take $n = 2$, $P = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $Q = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$. We have $P \neq 0$ and $Q \neq 0$.
  Note that $PQ = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$.

5. **Wholesale refutations.**

Consider a statement of the form below:

N: '*There exists some so-and-so amongst the elements of the set blah-blah-blah such that so-and-so satisfies bleh-bleh-bleh.*'

And also consider its variation below:

N_1: '*There exists some so-and-so amongst such that so-and-so is amongst elements of the set blah-blah-blah and so-and-so satisfies bleh-bleh-bleh.*'

N is a statement starting with an existential quantifier:

$$(\exists x)(J(x) \wedge L(x)).$$

$J(x)$ corresponds to the part '*so-and-so is an element of the set blah-blah-blah*'. $L(x)$ corresponds to the part '*so-and-so satisfies bleh-bleh-bleh*'.

To dis-prove the statement N, we may choose either of these two strategies:

(A) prove the statement $\sim N$.

(B) prove a statement of the form $N \longrightarrow C$, in which C is a known contradiction.

Both are equally 'legitimate' from the point of view of logic.

Depending on the 'concrete' situation, one strategy may be easier to implement than the other.

Whichever strategy is chosen, the argument is called **wholesale refutation** against N.

We consider these two strategies separately.

The negation $\sim N$ of the statement N is a statement starting with a universal quantifier:

$$(\forall x)((\sim J(x)) \vee (\sim L(x))).$$

As $J(x)$ refers to the part 'so-and-so is an element of the set *blah-blah-blah*', it is sometimes more convenient to write $\sim N$ as:

$$(\forall x)(J(x) \to (\sim L(x))).$$

In a 'wordy' form, it reads:

$\sim N$: '*For any so-and-so, if so-and-so is amongst the elements of the set blah-blah-blah then so-and-so does not satisfy bleh-bleh-bleh.*'

Hence to prove $\sim N$, we argue that every so-and-so amongst the elements of the set *blah-blah-blah* fails to satisfy *bleh-bleh-bleh.*

When we dis-prove N by directly proving $\sim N$, we proceed as described below:

(A) Pick any object so-and-so. (Throughout the rest of the argument this so-and-so is fixed.) Then we choose any one of the three approaches below:

- (A1) Suppose this so-and-so is amongst the elements of the set *blah-blah-blah.* Then deduce that this so-and-so fails to satisfy *bleh-bleh-bleh.*
- (A2) Suppose this so-and-so satisfies *bleh-bleh-bleh.* Then deduce that this so-and-so is not amongst the elements of the set *blah-blah-blah.*
- (A3) Suppose this so-and-so is amongst the elements of the set *blah-blah-blah* and also suppose this so-and-so satisfy *bleh-bleh-bleh.* Then look for a contradiction.

When we dis-prove N by proving a statement of the form $N \longrightarrow C$, in which C is a known contradiction, we proceed as described below:

(B) Suppose it were true that there existed some so-and-so amongst the elements of the set *blah-blah-blah* such that so-and-so satisfied *bleh-bleh-bleh.* Then look for a contradiction that arises from the existence of such a so-and-so.

This may be no easy task because the desired contradiction is not specified in the first place.

More generally, to dis-prove a statement of the form

$$\underbrace{(\exists x)(\exists y)\cdots(\exists z)}_{\text{all } \exists\text{'s}}(J(x, y, \cdots, z) \wedge L(x, y, \cdots, z)),$$

we may also choose either of these two strategies:

(A) prove its negation, which is the statement

$$\underbrace{(\forall x)(\forall y)\cdots(\forall z)}_{\text{all } \forall\text{'s}}[(\sim J(x, y, \cdots, z)) \vee (\sim L(x, y, \cdots, z)],$$

in any one of its formulation.

(B) prove a statement of the form

$$[\underbrace{(\exists x)(\exists y)\cdots(\exists z)}_{\text{all } \exists\text{'s}}(J(x, y, \cdots, z) \wedge L(x, y, \cdots, z))] \longrightarrow C,$$

in which C is a known contradiction.

6. **Examples of 'wholesale refutations'.**

   (a) We want to dis-prove

   N: *The equation $x^2 + 1 = 0$ has some real solution.*

   This statement is actually an existence statement in disguise:

   There exists some ρ such that ($\rho \in \mathbb{R}$ and $\rho^2 + 1 = 0$).

   (A) We may dis-prove N by proving $\sim N$ in this formulation:

   - *For any ρ, if $\rho \in \mathbb{R}$ then $\rho^2 + 1 \neq 0$.*

   Hence we write:

- Let ρ be an object. Suppose $\rho \in \mathbb{R}$. Then $\rho^2 \geq 0$. Therefore $\rho^2 + 1 \geq 1 > 0$. Hence $\rho^2 + 1 \neq 0$.

(B) We dis-prove N by obtaining a contradiction under the assumption N. Hence we write:

- Suppose it were true there existed some ρ such that $\rho \in \mathbb{R}$ and $\rho^2 + 1 = 0$. Since $\rho \in \mathbb{R}$, we would have $\rho^2 \geq 0$. Then $0 < 1 \leq \rho^2 + 1 = 0$. Contradiction arises.

(b) We want to dis-prove

N: *There exist some $z \in \mathbb{C}$ such that $|z| > |\mathsf{Re}(z)| + |\mathsf{Im}(z)|$.*

(A) We may dis-prove N by proving $\sim N$ in this formulation:

- *For any z, if $z \in \mathbb{C}$ then $|z| \leq |\mathsf{Re}(z)| + |\mathsf{Im}(z)|$.*

Hence we write:

- Let z be an object. Suppose $z \in \mathbb{C}$. Then $|z|^2 = |\mathsf{Re}(z)|^2 + |\mathsf{Im}(z)|^2 = (|\mathsf{Re}(z)| + |\mathsf{Im}(z)|)^2 - 2|\mathsf{Re}(z)| \cdot |\mathsf{Im}(z)| \leq (|\mathsf{Re}(z)| + |\mathsf{Im}(z)|)^2$. Therefore $|z| \leq |\mathsf{Re}(z)| + |\mathsf{Im}(z)|$.

(B) We may dis-prove N by obtaining a contradiction under the assumption N. Hence we write:

- Suppose there existed some $z \in \mathbb{C}$ such that $|z| > |\mathsf{Re}(z)| + |\mathsf{Im}(z)|$. Then $|z|^2 > (|\mathsf{Re}(z)| + |\mathsf{Im}(z)|)^2 = |\mathsf{Re}(z)|^2 + |\mathsf{Im}(z)|^2 + 2|\mathsf{Re}(z)| \cdot |\mathsf{Im}(z)| \geq |\mathsf{Re}(z)|^2 + |\mathsf{Im}(z)|^2 = |z|^2$. Contradiction arises.

(c) We want to dis-prove

N: *The set $[0, 1)$ has a greatest element.*

This statement is actually an existence statement in disguise:

There exists some $\lambda \in [0, 1)$ such that (for any $u \in [0, 1)$, $u \leq \lambda$).

(A) We may dis-prove N by proving $\sim N$ in this formulation:

- *For any $\lambda \in [0, 1)$, there exists some $u \in [0, 1)$ such that $u > \lambda$.*

Hence we write:

- Pick any $\lambda \in [0, 1)$. By definition, $0 \leq \lambda < 1$. Define $u = (\lambda + 1)/2$. We have $0 \leq \lambda < u < 1$. Hence $u \in [0, 1)$ and $u > \lambda$.

(B) We dis-prove N by obtaining a contradiction under the assumption N. Hence we write:

- Suppose $[0, 1)$ had a greatest element, say, λ. Since $\lambda \in [0, 1)$, we would have $0 \leq \lambda < 1$. Define $u = (\lambda + 1)/2$. We would have $0 \leq \lambda < u < 1$. Hence $u \in [0, 1)$ and $u > \lambda$. Contradiction arises.

(d) We want to dis-prove

N: *Some circle on the Argand plane passes through all four points $1, -1, i, 1 + i$.*

Very formally presented, the statement N is:

There exists some Γ such that Γ is a circle on the Argand plane and Γ passes through all four points $1, -1, i, 1+i$.

(A) We may dis-prove N by proving $\sim N$ directly. Hence we write:

- Let Γ be a circle on the Argand plane.
  The equation of Γ would be of the form $|z - \zeta| = r$ with unknown ζ in $\mathbb{C}$, in which ζ was a fixed complex number and r was a fixed non-negative real number.
  Suppose Γ passes through the points $1, -1, i$. Then $\zeta = 0$ and $r = 1$. Note that $|(1 + i) - \zeta| = \sqrt{2} \neq 1$. Then Γ does not pass through $1 + i$. Hence Γ does not pass through all four points $1, -1, i, 1 + i$.

(B) We dis-prove N by obtaining a contradiction under the assumption N. Hence we write:

- Suppose there existed some Γ such that Γ was a circle on the Argand plane and passed through all four points $1, -1, i, 1 + i$.
  The equation of Γ would be of the form $|z - \zeta| = r$ with unknown ζ in $\mathbb{C}$, in which ζ was a fixed complex number and r was a fixed non-negative real number.
  Since Γ passed through $1, -1, i$, we would have $\zeta = 0$ and $r = 1$.
  Note that $|(1 + i) - \zeta| = \sqrt{2} \neq 1$. Then Γ does not pass through $1 + i$. Contradiction arises.
  Hence it is false in the first place that some circle on the Argand plane passes through all four points $1, -1, i, 1 + i$.

(e) We want to dis-prove

N: *There exists some non-zero (3×3)-square matrix P such that P is symmetric and P is skew-symmetric.*

Very formally presented, the statement N is:

There exists some (3×3)-square matrix P such that P is non-zero and P is symmetric and P is skew-symmetric.

(A) We may dis-prove N by proving $\sim N$ directly.

Note that $\sim N$ can be formulated as:

For any (3×3)-square matrix P, if P is symmetric and P is skew-symmetric then $P = 0$.

Hence we write:

- Let P be a (3×3)-square matrix P.
  Suppose P is symmetric and P is skew-symmetric.
  Since P is symmetric, we have $P^t = P$.
  Also, since P is skew-symmetric, we have $P^t = -P$.
  Then $2P = P + P = P^t + (-P^t) = 0$. Therefore $P = 0$.

(B) We dis-prove N by obtaining a contradiction under the assumption N. Hence we write:

- Suppose there existed some (3×3)-square matrix P such that P was non-zero and P was symmetric and P was skew-symmetric.
  By assumption, since P was symmetric, $P^t = P$.
  Also, since P was skew-symmetric, $P^t = -P$.
  Then $2P = P + P = P^t + (-P^t) = 0$. Therefore $P = 0$.
  But P was non-zero by definition. Contradiction arises.
  Hence it is false in the first place that there existed some (3×3)-square matrix P such that P was non-zero and P was symmetric and P was skew-symmetric.

7. **Warning on common mistakes.**

(a) '$\sim((\forall x)P(x))$', '$(\forall x)(\sim P(x))$' are different statements.

'$\sim((\forall x \in S)Q(x))$', '$(\forall x \in S)(\sim Q(x))$' are different statements.

If you try to dis-prove a statement of the form

'*for any x, ($P(x)$ holds)*' (or '*for any $x \in S$, ($Q(x)$ holds)*' respectively)

by proceeding to prove the statement

'*for any x, ($P(x)$ does not hold)*' (or '*for any $x \in S$, ($Q(x)$ does not hold)*' respectively)

you will probably be attempting to achieve the impossible and end up nowhere.

(b) '$\sim((\forall x)(H(x) \to K(x))$', '$(\forall x)[H(x) \to (\sim K(x))]$' are different statements.

If you try to dis-prove a statement of the form

'*for any x, (if $H(x)$ holds then $K(x)$ holds)*'

by proceeding to prove the statement

'*for any x, (if $H(x)$ holds then $K(x)$ does not hold)*'

you will probably be attempting to achieve the impossible and end up nowhere.

(c) '$\sim((\exists x)P(x))$', '$(\exists x)(\sim P(x))$' are different statements.

'$\sim((\exists x \in S)Q(x))$', '$(\exists x \in S)(\sim Q(x))$' are different statements.

If you attempt to dis-prove a statement of the form

'*there exists some x such that ($P(x)$ holds)*' (or '*there exists some $x \in S$ such that ($Q(x)$ holds)*' respectively)

by proceeding to prove the statement

'*there exists some x such that ($P(x)$ does not hold)*' (or '*there exists some $x \in S$ such that ($Q(x)$ does not hold)*')

you will end up achieving too little of value.