Propositions and operations

> ⓘ **Info**
>
> The course is split into 4 blocks, each ending with a *workshop* in which you and your group spend 6 hours working on a massive sheet about the contents of the block. During the exam you will present one of the four workshops, so be sure to write things down!

Propositions are declarative sentences that can be true or false. These are typically denoted with small letters, usually p, q, and r.

Operations

Negation is the "not" operator, using the symbol $\neg$. $\neg p$ is "not p", and this flips the truth value of the proposition p.
Conjunction is the "and" operator, which connects two propositions with the symbol $\land$. The conjunction of p and q is subsequently $p \land q$. $p \land q$ is true if, and only if, both p and q have a truth value of T, ie $v(p) = T \land v(q) = T$.
Disjunction is the "or" operator, connecting two propositions with the symbol $\lor$. The conjunction of p and q is $p \lor q$, and is true if p or q have a truth value of T, ie $v(p) = T \lor v(q) = T$.
Implication is the "if … then" operator, connecting two propositions with the symbol $\rightarrow$. The implication $p \rightarrow q$ is true if p "implicates" q. This is best understood by the truth tables.
Bi-implication is the "if and only if" operator, connecting two propositions with the symbol $\leftrightarrow$. The bi-implication $p \leftrightarrow q$ is true if the truth values of p and q are identical, ie $v(p) = v(q)$.

Truth tables and bit operations

Truth tables

A truth table can be used to show the relations between different propositions.

p	$\neg p$
T	F
F	T

p	q	$p \land q$	$p \lor q$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	T	T	T	T
T	F	F	T	F	F

p	q	$p \land q$	$p \lor q$	$p \to q$	$p \leftrightarrow q$
F	T	F	T	T	F
F	F	F	F	T	T

Bit operations

It's common to associate the bit value 1 with T and 0 with F. These operations are extended to bit strings of the same length by applying them to each component separately:

$$01100 \oplus 00111 = 01011$$

Logical equivalence, tautologies and contradictions

Tautology and contradiction

A compound proposition that is always true is called a tautology.
A compound proposition that is always false is called a contradiction.

p	$\neg p$	$p \lor \neg p$	$p \land \neg p$
T	F	T	F
F	T	T	F

Logical equivalence

If two compound propositions p and q have the same truth values for all possible cases, we call these propositions equivalent. This is denoted by $p \equiv q$. For example:

$$(p \to q) \land (q \to p) \equiv (p \leftrightarrow q)$$

There exist many useful, established logical equivalences which can be proven.

De Morgan's laws

$$\neg(q \lor p) \equiv \neg p \land \neg q$$

$$\neg(q \land p) \equiv \neg p \lor \neg q$$

Conditional disjunction equivalence

$$(p \to q) \equiv (\neg p \lor q)$$

Distributive laws

$$p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$$

$$p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$$

Quantors and propositional functions

Propositional functions

A propositional function is an expression, containing one of more variables, which becomes a proposition when each of the variables is replaced by some one of its values from a discourse domain (universe) of individuals.

Quantors

Universal quantor

The universal quantification of a propositional function $P(x)$ is the proposition

> $P(x)$ is true for all values of x in the domain.

We denote this by $\forall x P(x)$. This proposition is true if and only if $P(x)$ is true for all possible values of x. It is false as soon as in the domain one counterexample x exists for which $P(x)$ is false.

Existential quantor

The existential quantification of a propositional function $P(x)$ is the proposition

> There exists an element in x in the domain such that $P(x)$ is true.

We denote this by $\exists x P(x)$. This proposition is true if and only if $P(x)$ is true for at least one possible value of x. It is false if $P(x)$ is false for all x in the domain. $\exists! x P(x)$ means there exists *exactly* one x where $P(x)$ is true.

Sets

Sets

A set is an unordered collection of distinct objects, called elements or members. We write $e \in S$ if the element e is in the set S. A set is usually denoted by listing its elements:

$$B = \{0, 1\}$$

The empty set, $\emptyset$, is the set that contains no elements:

$$\emptyset = \{\}$$

A set can contain other sets:

$$S = \{\{\}, \{0\}, \{1\}, \{0, 1\}\}$$

A set containing a single element is often referred to as a singleton. For example, $\{a\}$ is a singleton of a.

Important sets

There are a few important sets denoted by double-lined capital letters:

$$\begin{aligned}
\mathbb{N}_0 &= \{0, 1, 2, 3, \ldots\} \text{ (the natural numbers including 0)} \\
\mathbb{N} &= \{1, 2, 3, \ldots\} \text{ (the natural numbers excluding 0)} \\
\mathbb{Z} &= \{\ldots, -1, -2, 0, 1, 2, \ldots\} \text{ (all integers, including 0 and negative numbers)} \\
\mathbb{Q} &\text{ is the set of all rational numbers, so excluding } \pi \text{, for example.} \\
\mathbb{R} &\text{ is the set of all real numbers, so including } \pi \text{, but excluding all complex numbers.} \\
\mathbb{C} &\text{ is the set of all complex numbers.}
\end{aligned}$$

This styling of the symbols is called blackboard bold. Not relevant but good to know.

Set builder notation

Not all sets can be described by listing the elements. The set builder notation can be used to describe which elements belong to the set in this case. Let D be a domain of discourse and P be a propositional function, then

$$S = \{e \in D | Q(e)\}$$

is the set of all elements in D for which $Q(e)$ is true. For example, we can describe the set of all even naturals as

$$\mathbb{E} = \{x \in \mathbb{N} | \exists k \in \mathbb{N}, x = 2k\}.$$

Here, we are essentially saying: "the set, $\mathbb{E}$, is the set of all natural numbers x where it is true that for some natural number k, $x = 2k$." Of course, this makes x even, as $2k$ is obviously divisible by 2.

Cardinality of sets

A set S is finite if it contains a finite number n of elements. The size $|S|$ (cardinality) of a finite set S is then defined to be the number n of elements it contains. For example:

$$S = \{1, 2, 3\}$$

$$|S| = 3$$

Set operations

Union

The union of two sets A and B is the set containing all elements that are in A or B, denoted by $A \cup B$. In set builder notation (*SBN*):

$$A \cup B = \{x | x \in A \vee x \in B\}$$

Intersection

The intersection of two sets A and B is the set containing all elements that are in A and B, denoted by $A \cap B$. In SBN:

$$A \cap B = \{x | x \in A \wedge x \in B\}$$

Cardinality of intersection and union

If A and B are finite sets, then the following equation holds:

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

Difference

The difference of two sets A and B is the set containing all elements that are in A but not in B, denoted by $A - B$ or $A \setminus B$. In SBN:

$$A \setminus B = \{x | x \in A \wedge x \notin B\}$$

Complement

Let U be the universal set. The complement of a set A is the set containing all elements in U that are not in A ($U \setminus A$), denoted by $\overline{A}$. In SBN:

$$\overline{A} = \{x \in U | x \notin A\}$$

It always holds true that $\overline{\overline{S}} = S$, ie the complement of the complement of a set is merely the set.

Set identities

Set identities are analogous to predicate logic, so sets follow De Morgan's laws, the conditional disjunction equivalence, the distributive laws and all other laws of logic.

Subsets and power sets

Subsets

The set A is a subset of the set B if and only if every element of A is also an element of B.

$$\forall x \in A, x \in B$$

$$\forall x (x \in A \rightarrow x \in B)$$

For any set S it holds that $\emptyset \subseteq S$ and $S \subseteq S$.

Proper subsets

A is a proper subset of B if $A \subseteq B$, but $A \neq B$. Here we use the notation $A \subset B$.

What is ***not*** a subset?

There are cases where it may be confusing whether one set is a subset of another set. For example:

$$\{a\} \not\subseteq \{\{a\}, \{b\}\}$$

Since $\{a\}$ is actually an element *in* the set on the right, therefore it is only the case that

$$\begin{gathered} \{a\} \in \{\{a\}, \{b\}\}, \\ \{\{a\}\} \subseteq \{\{a\}, \{b\}\}. \end{gathered}$$

Power sets

A power set of a set, A, notated as $\mathcal{P}(A)$, is the set containing all possible subsets of A. This can be represented as

$$x \in \mathcal{P}(A) \iff x \subseteq A.$$

In set builder notation, this can be represented as

$$\mathcal{P}(A) = \{x | x \subseteq A\},$$

where x is also a set. An example of a power set can look like this:

$$\begin{aligned} A &= \{a, b, c\} \\ \mathcal{P}(A) &= \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}, \emptyset\} \end{aligned}$$

As we can see, the set A containing 3 elements has a power set containing 8 elements. For each element in A, we have the choice of whether or not to add it to a possible subset. Therefore, the cardinality of a power set follows

$$|A| = n \implies |\mathcal{P}(A)| = 2^{|A|} = 2^n.$$

So if we have a set A with a cardinality of 8, for example, we get

$$|A| = 8 \implies |\mathcal{P}(A)| = 2^8 = 256.$$

Nested power sets create power towers when looking at the cardinality:

$$\begin{aligned} |A| &= m \\ |\mathcal{P}(\mathcal{P}(\mathcal{P}(A)))| &= 2^{|\mathcal{P}(\mathcal{P}(A))|} \\ &= 2^{2^{|\mathcal{P}(A)|}} \\ &= 2^{2^{2^{|A|}}} \\ &= 2^{2^{2^m}} \end{aligned}$$

Is A a subset of $\mathcal{P}(A)$?

It can be confusing to differentiate between the meanings of subsets and elements when talking about power sets. For a set A containing the empty set, we can observe that

$$A = \{\emptyset\} \implies \mathcal{P}(A) = \{\emptyset, \{\emptyset\}\}.$$

For this case, it is true that A is a subset of its own power set $\mathcal{P}(A)$, so

$$\exists A, A \subseteq p(A).$$

We must not be quick to assume that this is true for *every* A, however, since

$$A = \{a, b\} \implies \mathcal{P}(A) = \{\{a\}, \{b\}, \{a, b\}, \emptyset\}$$

In this case,

$$A \nsubseteq \mathcal{P}(A).$$

Because we have this counterexample, our final statement about whether A is a subset of $\mathcal{P}(A)$ must be

$$\exists A, A \subseteq \mathcal{P}(A) \land \neg(\forall A, A \subseteq \mathcal{P}(A)).$$

Or: while there exists a set which is a subset of its power set $\mathcal{P}(A)$, this is not true for all A. In fact, the only sets for which it is true that the set is a subset of its own power set, are sets that contain the empty set, or the empty set itself, since it is always true that $\emptyset \subseteq S$. At the same time, though, the following is true:

$$\forall A, A \in \mathcal{P}(A).$$

This is where the difference between a set being a subset of another set, and a set being a member of another set, or the difference between $A \subseteq B$ and $A \in B$, gets a little confusing. In (7), we can observe that $\{a, b, c\}$ is indeed a member of $\mathcal{P}(A)$, but it is **not** a subset, because if that were the case, it would be the case that

$$a \in \mathcal{P}(A) \wedge b \in \mathcal{P}(A) \wedge c \in \mathcal{P}(A),$$

and this is, in fact, not the case. Only the set *containing* a, b, and c are in the power set of A. Not the actual elements.

Cartesian products and ordered pairs

Ordered pairs

An ordered pair (a, b) is a set

$$\{\{a\}, \{a, b\}\}.$$

This structure ensures that $(a, b) \neq (b, a)$, since

$$\{\{a\}, \{a, b\}\} \neq \{\{b\}, \{b, a\}\}.$$

This holds true despite sets being unordered, since only one singleton, $\{a\}$ or $\{b\}$, is in the set. So while the subsets are the same ($\{a, b\} = \{b, a\}$), the standalone elements are unique. Effectively, this means the pair is *ordered*, since the order of appearance in (a, b) changes the meaning.

Cartesian products

The cartesian product $A \times B$ is the set

$$\{(a, b) | a \in A \wedge b \in B\}.$$

In other words, it's the set containing all possible ordered pairs constructed from the elements of two sets, where the element of the first set must come first in the ordered pair. Example:

$$(A = \{0, 1, 2\}) \wedge (B = \{0, 1\}) \iff A \times B = \{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1)\}$$

Note that $A \neq B \implies A \times B \neq B \times A$:

$$A \times B \neq B \times A \iff \{(0,0),(0,1),(1,0),(1,1),(2,0),(2,1)\} \neq \\ \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$$

This is once again due to the order of appearance being relevant in an ordered pair.

Cardinality of cartesian products

The following statement about cardinalities of cartesian products holds true:

$$|A| = n \land |B| = m \implies |A \times B| = nm$$

In other words:

> If the cardinality of a set A is n and the cardinality of a set B is m, then the cardinality of the cartesian product between A and B (in either order) must be nm.

Cartesian products of >2 sets

An ordered pair is also called a tuple of two elements. A tuple can contain more elements, however. A tuple is simply an ordered collection of things. Cartesian products between more than 2 sets produce tuples with more than 2 elements:

$$A \times B \times C = \{(a,b,c) | a \in A \land b \in B \land c \in C\}$$

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) | a_1 \in A_1 \land a_2 \in A_2 \land \ldots \land a_n \in A_n\}$$

Properties of tuples

> ⚠ **Not from course: This section contains information gathered from sources other than what the DTG course provides.**

The general rule for the identity of two n-tuples is

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \iff a_1 = b_1 \land a_2 = b_2 \land \ldots \land a_n = b_n.$$

This means that

1. A tuple can contain duplicates, ie $(1,2,2,3) \neq (1,2,3)$; conversely, a set $\{1,2,2,3\} = \{1,2,3\}$.
2. Tuple elements are ordered, ie $(1,2,3) \neq (3,2,1)$; conversely, a set $\{1,2,3\} = \{3,2,1\}$.
3. A tuple has a finite number of elements; conversely, a set may have an infinite number of elements, for example the set of all natural numbers.

Construction of n-tuples as ordered pairs

A tuple of 3 elements can be constructed as ordered pairs and therefore notated as a set:

$$(a,b,c) := ((a,b),c) = (\{\{a\},\{a,b\}\},c) = \{\{\{\{a\},\{a,b\}\}\},\{\{\{a\},\{a,b\}\},c\}\}$$

This process can be applied to a tuple of any n elements, for example a tuple of 6 elements has the recursive definition

$$(a,b,c,d,e,f) := (((((a,b),c),d),e),f).$$

Note that the "reverse" can also be used to represent an n-tuple as an ordered pair:

$$(a,b,c,d,e,f) := (a,(b,(c,(d,(e,f)))))$$

Any n-tuple can, in this way, be expanded to being expressed purely as a set, though it will look ridiculous.

Cartesian square

$A \times A$ can be written as A^2. For example, let $A = \{a,b\}$, then

$$A^2 = \{(a,a),(a,b),(b,a),(b,b)\}$$

Cartesian products involving the empty set

When the empty set is involved in a cartesian product, we get the empty set:

$$\begin{gathered}\text{Example: } A = \{a,b,c\} \\ A \times \emptyset = \emptyset \\ \emptyset \times A = \emptyset\end{gathered}$$

Relations

Binary relations

Let A and B be sets. A relation from A to B is a subset of $A \times B$. That is to say, a relation from A to B is a set containing some amount of ordered pairs (a,b) that fulfil the condition

$$a \in A \wedge b \in B.$$

For example, for

$$\begin{gathered}A = \{1,2,3\} \\ B = \{a,b,c\},\end{gathered}$$

a relation can be

$$R = \{(1,a),(1,b),(2,b),(2,c),(3,a)\}.$$

This is, of course, some subset of the cartesian product $A \times B$:

$$A \times B = \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c),(3,a),(3,b),(3,c)\}.$$

We can see that the elements of R are also in $A \times B$, which is the definition of a subset, so

$$R \subseteq A \times B.$$

This verifies that R is a relation from A to B. Obviously, the relation R in (3) is not the only possible relation from A to B. When $(s,b) \in R$, we say that a **is R-related to** b, and this can also be notated as

$$(a,b) \in R \iff a\,R\,b$$

A binary relation encodes the common concept of relation: an element x is related to an element y, if and only if the pair (x,y) belongs to the set of ordered pairs that defines the binary relation.

Homogenous relations

A binary relation on a set A is a subset of $A \times A$ or A^2. This is also called an **endorelation**, or a **homogenous relation**. For example, let A be a set, and

$$\begin{aligned} A &= \{1,2\} \\ A^2 &= \{(1,1),(1,2),(2,1),(2,2)\}. \end{aligned}$$

In this case, any subset of this cartesian square is a binary relation on the set A, for example:

$$\begin{aligned} R_1 &= \{(1,1),(2,2)\} \\ R_2 &= \{(1,2),(2,1)\}. \end{aligned}$$

Both R_1 and R_2 are binary relations on A, since they are both subsets of A^2. We can also construct a binary relation using set builder notation:

$$R = \{(a,b) | a \bmod b = 0\}$$

Or with the infix $a\,R\,b$ notation:

a\, R\, b&nbsp;\iff a\bmod b=0

Here, we are using the modulo operator to express that R is the binary relation on A where a is divisible by b. The contents of this set, in our example, would simply be

$$R = \{(1,1),(2,1),(2,2)\}.$$

The ordered pair $(1,2)$ is not in this relation, since 1 is not divisible by 2. Homogenous relations are especially useful as they can model a wide variety of concepts. For example, "is greater than", or $>$, is the relation on the reals $\mathbb{R}$ which encodes the concept of one number being greater than another. With this relation, and using the $a\,R\,b$ syntax, it very clearly encodes mappings like $5 > 3$, since $(5, 3) \in >$.

All possible relations between two sets

The set containing every possible relation between a set A and a set B is the power set of the cartesian product of A and B:

$$R_{A,B} = \mathcal{P}(A \times B)$$

This is of course because the power set of a set A is the set containing every possible subset of A. By definition, a relation is a subset of A where A is the cartesian product of two sets.

Properties of relations

There are different properties that a relation R may have.

Reflexive property

A homogenous relation R on a set A is **reflexive** if

$$\forall a \in A : a\,R\,a.$$

For all elements a in the set A, a is R-related to a. So a reflexive relation is one wherein there is an ordered pair (a, a) for every element a in A. Every element of A is R-related to itself. For example, let $\mathbb{R}$ be the set of real numbers, then a reflexive relation R could be

$$R = \{(a, b) | a \leq b\},$$

or alternatively

$$a\,R\,b \iff a \leq b.$$

This relation is reflexive since any real number is always lesser than or equal to itself. This also means that a relation does not have to only contain ordered pairs where both elements are the same, but that it must satisfy that condition for every element in A, so $5 \leq 10, 999 \leq 9999$ and so on obviously still apply even though the relation is reflexive. It is worth noting that reflexivity cannot be a property of a relation between two distinct sets A and B, since (a, a) existing for all $a \in A$ would only be possible if B were a superset of A.

Symmetric property

A relation R is symmetric if

$$\forall a, b \in A : a \, R \, b \iff b \, R \, a.$$

A relation is therefore symmetric whenever the existence of an ordered pair (a, b) in the relation implies the presence of the reverse, (b, a). For example, let A and B be sets, and

$$\begin{aligned} A &= \{1, 2, 3\} \\ B &= \{1, 2\} \\ A \times B &= \{(1,1), (1,2), (2,1), (2,2), (3,1), (3,2)\}, \end{aligned}$$

then a symmetric relation from A to B could be

$$R = \{(1,1), (1,2), (2,1)\},$$

as every ordered pair has a "reverse order" equivalent in the set. If, for example, $(3,1) \in R$, then the relation would no longer be symmetric, since there would be no $(1,3) \in R$. For a more general example, let R be a relation on the natural numbers $\mathbb{N}$, and

$$R = \{(a, b) | (\exists k \in \mathbb{N} : a = 2k + 1) \wedge (\exists m \in \mathbb{N} : b = 2m + 1)\}.$$

Here, we are describing the relation that both a and b are odd. This relation is of course symmetric, since if 3 and 5 are odd, then 5 and 3 are also odd. "and" is commutative, so to speak.

Antisymmetric property

A homogenous relation R on a set A is antisymmetric if

$$\forall a, b \in A : a \, R \, b \wedge b \, R \, a \implies a = b$$

In other words, a relation on a set is considered antisymmetric when there are no symmetric, distinct pairs in the relation. It can also be explained as

$$a \neq b \implies \neg(a \, R \, b \wedge b \, R \, a),$$

which essentially states that if a and b are distinct, then a being R-related to b and b being R-related to a must not both hold. So a relation containing no examples of $\{(a, b), (b, a)\}$ where $a \neq b$ is antisymmetric. For example, let A be a set

$$A = \{a, b, c\},$$

and let R be a relation

$$R = \{(a, b), (a, c)\}.$$

Here, R is an antisymmetric relation simply because it does not contain any two symmetric ordered pairs $\{(a, b), (b, a)\}$, where a and b would be distinct elements. If (b, a) or (c, a) were to be added to the set, R would no longer be antisymmetric, as it would violate the condition for antisymmetry as stated in (20).

Transitive property

A relation R on a set A is **transitive** if

$$\forall a, b, c, \in A : a\,R\,b \wedge b\,R\,c \implies a\,R\,c.$$

This is the same logic as a syllogism. If a is R-related to b, and b is R-related to c, then a is R-related to c. An example of a transitive relation on the set of reals $\mathbb{R}$ could be

$$R = \{(a, b) | a \leq b\}.$$

Here, we can observe that if a is lesser than b which is lesser than c, then a is obviously also lesser than c. This satisfies the requirement (24). It turns out to be true that all of the following relations on the reals are transitive: $>$, $<$, $\geq$, $\leq$, and $=$. The proofs for each of these follow the same structure, here I will prove the greater-than relation:

$$a > b \iff a - b > 0$$

$$b > c \iff b - c > 0$$

$$(a - b) + (b - c) > 0$$

$$a - c > 0$$

$$a > c$$

Closures of relations