Proofs in algebra of sets

Duality of intersection and union
“take any valid expression, and switch unions with intersections, and empty sets with U. It is still true.”

Why, how, what?

-the duality holds for the basic rules (axioms).

Theorem 6.5

Commutativity:

$A \cap B = B \cap A \qquad A \cup B = B \cup A$

Associativity

$(A \cap B) \cap C = A \cap (B \cap C) \qquad (A \cup B) \cup C = A \cup (B \cup C)$

Distributivity:

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Idempotence

$A \cap A = A \qquad A \cup A = A$

De Morgan

$(A \cup B)^c = A^c \cap B^c \qquad (A \cap B)^c = A^c \cup B^c$

DUALS!

nul element (identity)

$A \cap \varnothing = \varnothing \qquad A \cup \varnothing = A$

identity element

$A \cap U = A \qquad A \cup U = U$

double complement (involution)

$(A^c)^c = A$

complementation rules

$A \cap A^c = \varnothing \qquad A \cup A^c = U$

Proofs in algebra of sets

Duality of intersection and union
“take any valid expression, and switch unions with intersections, and empty sets with U. It is still true.”

Why, how, what?

-the duality holds for the basic rules (axioms).
-any true statement can be expanded to a sequential application of the elementary rules.
-but we can apply duality to every step, so each step remains true after the substitute.

-so the first, and last remain true

EXAMPLE

$$A = A \cap (A \cup B) \qquad\qquad A = A \cup (A \cap B)$$

$$A = A \cup \emptyset \quad \longleftrightarrow \quad A = A \cap U$$

$$A \cup \emptyset = A \cup (B \cap \emptyset) \quad \longleftrightarrow \quad A \cap U = A \cap (B \cup U)$$

$$A \cup (B \cap \emptyset) = (A \cup B) \cap (A \cup \emptyset) \quad \longleftrightarrow \quad A \cap (B \cup U) = (A \cap B) \cup (A \cap U)$$

$$(A \cup B) \cap (A \cup \emptyset) = (A \cup B) \cap A \quad \longleftrightarrow \quad (A \cap B) \cup (A \cap U) = A \cup (A \cap B)$$

Proofs in algebra of sets

AN IDENTITY WHICH USES
$\cap, \cup, \emptyset, U$

Duality of intersection and union
“take any valid expression, and switch unions with intersections, and empty sets with U. It is still true.”

Why, how, what?

-the duality holds for the basic rules (axioms).
-any true statement can be expanded to a sequential application of the elementary rules.
-but we can apply duality to every step, so each step remains true after the substitute.

-so the first, and last remain true

Digression!

How would we formally define "expressions"?

(1) IF A IS A SET, A is AN EXPRESSION

(2) IF A, B ARE EXPRESSIONS

- $(A \cup B)$
- $(A \cap B)$

EXPRESSIONS

INDUCTIVE

Duality in mathematics

- *Duality*, generally speaking, translates concepts, theorems or mathematical structures into other concepts, theorems or structures
- in a one-to-one fashion
- often by an involution operation: if the dual of A is B, then the dual of B is A.

- Involutions sometimes have fixed points, so that the dual of A is A itself.

'In mathematical contexts, duality has numerous meanings although it is "a very pervasive and important concept in (modern) mathematics" and "an important general theme that has manifestations in almost every area of mathematics”.'

https://en.wikipedia.org/wiki/Duality_(mathematics)

Examples of using duality:

Prove, prove dual: $(U \cap A) \cup (A \cap B) = A$

Find dual: $A \cap (A \overset{\cup}{\cap} \emptyset)^c = \underline{A \cap U}$

A

$\underbrace{(U \cap A)}\cup(A \cap B) = A$

$= A \cup (A \cap B)$

$= A$

$\underbrace{(\emptyset \cup A)} \cap \underbrace{(A \cup B)} = A$

$\underline{A \cap (A \cup B)} = A$

$A \cup \underbrace{(A \cup U)}^c = A \cup \emptyset$

$A \cup \emptyset = A \cup \emptyset$

Sets as elements of sets

$A \in B$

Example:

$\{1,2\} \in \{\{1,2\}, \varnothing\}$

$\varnothing \notin \{\{1,2\}\}$

(BUT. $\varnothing \subseteq \{\{1,2\}\}$**!)**

Sets as elements of sets (constructions)

Definition: Given the set S, the powerset $\mathscr{P}(S)$ is the set of all subsets of B:

$$\mathscr{P}(S) := \{A \mid A \subseteq S\}$$

Examples: (IF NEEDED)

Sets as elements of sets (constructions)

Definition: Given the set S, **the powerset** $\mathscr{P}(S)$ **is the set of all subsets of** B:

$$\mathscr{P}(S) := \{A \mid A \subseteq S\}$$

Powerset, aka: 2^S

Cardinality: $|S|$; $|\mathscr{P}(S)| = 2^{|S|}$

Sets as elements of sets (constructions)

Definition: Given the set S, the powerset $\mathscr{P}(S)$ is the set of all subsets of B:

$$\mathscr{P}(S) := \{A \,|\, A \subseteq S\}$$

Bitstrings

Binary numbers,
or *bitstrings*

how many?

Sets as elements of sets (constructions)

Definition: Given the set S, the powerset $\mathscr{P}(S)$ is the set of all subsets of B:

$$\mathscr{P}(S) := \{A \mid A \subseteq S\}$$

Binary numbers,
or *bitstrings*

how many?

"if I add one more bit,
the count doubles"

Bitstrings

Sets as elements of sets (constructions)

Definition: Given the set S, the powerset $\mathscr{P}(S)$ is the set of all subsets of B:

$$\mathscr{P}(S) := \{A \mid A \subseteq S\}$$

Why is

$$|\{b_{n-1}b_{n-2}\ldots b_0 \mid b_k \in 0,1\}| =$$
$$= |\mathscr{P}(\{a_0, \ldots, a_{n-1}\})|$$

$\Rightarrow$ EACH BITSTRING SPECIFIES EXACTLY ONE SUBSET &

$\Leftarrow$ EACH SUBSET SPECIFIES EXACTLY ONE BITSTRING

Bitstrings v.s. powersets

a_0	0	"IS IT IN SUBSET
a_1	1	0 = NO 1 = YES
a_2	1	
$\vdots$	$\vdots$	
a_n	0	

$\hookrightarrow \{a_1, a_2 \ldots\}$

Sets as elements of sets (constructions)

Definition: Given the set S, the powerset $\mathscr{P}(S)$ is the set of all subsets of B:

$$\mathscr{P}(S) := \{A \mid A \subseteq S\}$$

Why is

$$\boxed{\begin{array}{c} |\{b_{n-1}b_{n-2}\ldots b_0 \mid b_k \in 0{,}1\}| = \\ = |\mathscr{P}(\{a_0, \ldots, a_{n-1}\})| \end{array}}$$

bitstrings

=

subsets

Bitstrings v.s. powersets

REMINDER: alphabets, strings, languages

SUPPLEMENTAL

- **Definition. An** ***alphabet*** **is a non-empty, finite set of** ***letters*****.**

- **Definition. A** ***string*** **(*****word*****) over the** *alphabet* **Σ is an ordered set of letters from the** *alphabet* **Σ**

- **Notation: Σ* - set of all strings from the** *alphabet* **Σ**

- **Definition. A** ***language*** **over the alphabet Σ is a set of** *strings* **(*words*)** *over* **Σ**

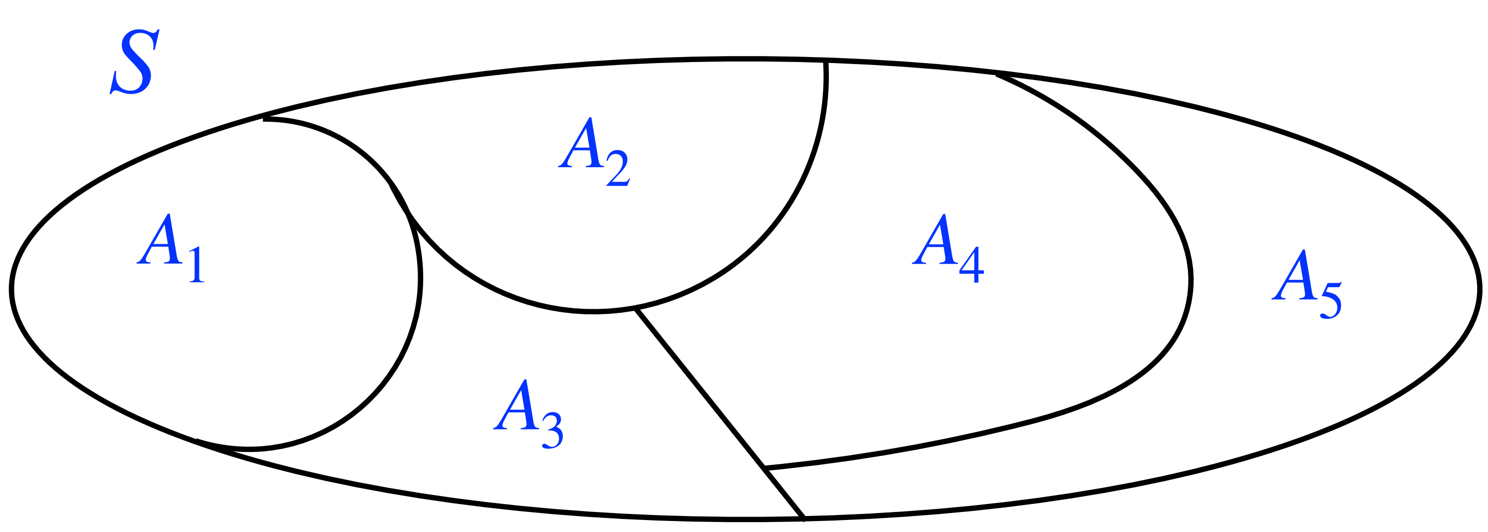
- **Notation:** $\mathscr{P}(\Sigma^*)$ **- all the languages over Σ**

Sets as elements of sets (constructions)

SUPPLEMENTAL

Definition: Given the set S, family of sets $P_s = \{A_1, A_2, A_3 \ldots\}$ is called a (countable) partition of S *if*

- $\varnothing \notin P_s$
- $S \in A_1 \cup A_2 \cup \cdots = \bigcup_{i \in I} A_i$ **[P_s covers S]**
- **For all i, j, $A_i \cap A_j = \varnothing$** **[elements of P_s are pairwise disjoint]**



Sets as elements of sets (constructions)

SUPPLEMENTAL

Definition: Given the set S, family of sets $P_s = \{A_1, A_2, A_3 \ldots\}$ is called a (countable) partition of S *if: a) no A_k is empty; b) they cover P c) pairwise disjoint*

Examples:

Important partitions: congruence classes (residue claseses)

VERY!

SUPPLEMENTAL

- **Defined relative to the universe $\mathbb{Z}$**
- **given** $k \in \mathbb{N}$, **and** $l \in \mathbb{Z}$, **the congruence class of** *l modulo k is:*

$$\bar{l} = \{\ldots, l+nk, \ldots l-2k, l-k, \quad l, \quad l+k, l+2k, \ldots, l+nk, \ldots\}$$

- **Example**: *congruence classes of 0,1,2 modulo 7:*

$$\bar{0} = \{\ldots. -14, -7, 0, 7, 14\ldots\}$$
$$\bar{1} = \{\ldots. -13, -6, 1, 8, 15\ldots\}$$
$$\bar{2} = \{\ldots. -12, -5, 2, 9, 16\ldots\}$$

Auxiliary

Important partitions:
congruence classes (residue claseses)

VERY!

SUPPLEMENTAL

- **Example**: *congruence classes of 0,1,2 modulo 7:*

$$\bar{0} = \{\ldots. -14, -7, 0, 7, 14\ldots\}$$
$$\bar{1} = \{\ldots. -13, -6, 1, 8, 15\ldots\}$$
$$\bar{2} = \{\ldots. -12, -5, 2, 9, 16\ldots\}$$

- **NB: congruence classes are sets. Recall when two sets are equal.**
- **work out a few other congruence classes modulo 7 (of some other number)**
- **for a given *k*, are there infinitely many classes? how many?**

VERY!

SUPPLEMENTAL

Important partitions:
congruence classes (residue claseses)

- **Example**: *congruence classes of 0,1,2 modulo 7:*

$$\bar{0} = \{\ldots. -14, -7, 0, 7, 14\ldots\}$$
$$\bar{1} = \{\ldots. -13, -6, 1, 8, 15\ldots\}$$
$$\bar{2} = \{\ldots. -12, -5, 2, 9, 16\ldots\}\ldots$$

- *Note: for mod 7:* $\bar{0} = \bar{7}$; $\bar{1} = \bar{8}$; *for mod k:* $\bar{l} = \overline{k+l}$; $\bar{l} = \overline{k+ml}$

Lets work this out:

VERY!

SUPPLEMENTAL

Important partitions: congruence classes (residue claseses)

- **Example**: *congruence classes of 0,1,2 modulo 7:*

$$\bar{0} = \{\ldots. -14, -7, 0, 7, 14\ldots\}$$
$$\bar{1} = \{\ldots. -13, -6, 1, 8, 15\ldots\}$$
$$\bar{2} = \{\ldots. -12, -5, 2, 9, 16\ldots\}\ldots$$

- **Partition of $\mathbb{Z}$!**
- $R_7 = \{\bar{0}, \bar{1}, \ldots, \bar{6}\}$ **(check properties!)**

Lets work this out:

Important partitions:
non-trivial infinite partition

SUPPLEMENTAL

$$A_0 = \{1,3,5,7\ldots\}$$
$$A_1 = \{2,6,10,14,\ldots\}$$
$$A_2 = \{4,12,20,28,\ldots\}$$

Important partitions: non-trivial infinite partition

SUPPLEMENTAL

$$A_0 = \{1,3,5,7\ldots\}$$
$$A_1 = \{2,6,10,14,\ldots\}$$
$$A_2 = \{4,12,20,28,\ldots\}$$

$$A_k = \{2^k \cdot 1, 2^k \cdot 3, 2^k \cdot 5, 2^k \cdot 7, \ldots\}$$

Important partitions:
non-trivial infinite partition

SUPPLEMENTAL

$$A_0 = \{1,3,5,7\ldots\}$$
$$A_1 = \{2,6,10,14,\ldots\}$$
$$A_2 = \{4,12,20,28,\ldots\}$$

$$A_k = \{2^k \cdot 1, 2^k \cdot 3, 2^k \cdot 5, 2^k \cdot 7,\ldots\}$$

Claim: this is a partition of the natural numbers. Prove!

Intermezzo! Binary numbers

Decimal numbers (base 10)

$d_{n-1}d_{n-2}\ldots d_0$, **with** $d_k \in \{0,\ldots,9\}$

$123 = 100 + 20 + 3 = 1 \cdot 10^2 + 2 \cdot 10^2 + 3 \cdot 10^2$

$d_{n-1}d_{n-2}\ldots d_0 = d_{n-1} \cdot \underline{10}^{n-1} + \underline{d_{n-2}} \cdot 10^{n-3} + \cdot + d_0 \cdot \underline{10}^0$

$b_{n-1}b_{n-2}\ldots b_0$, **with** $b_k \in \{0,1\}$

$b_{n-1} \times 2^{n-1} + b_{n-2} \times 2^{n-2} \cdots \underbrace{b_0 \cdot 2}_{0}{}^0$

Auxiliary

$(\underset{3}{1}\underset{2}{0}\underset{1}{1}\underset{0}{1})_2 = \underset{3}{1} \times 2^3 + \underset{2}{0} \times 2^2 + \underset{1}{1} \times 2^1 + \underset{0}{1} \times 2^0 = 8 + 2 + 1 = 11$

EXCERCISES ?

Auxiliary