Sets

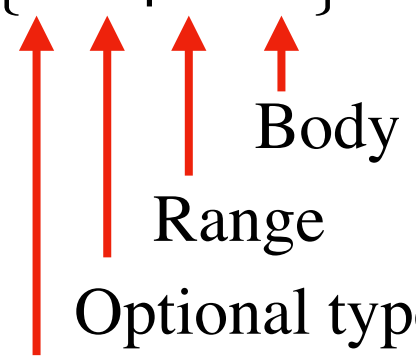
Set enumeration

List each element in the set.

Example: $\{0, 2, 4, 6, 8\}$

Set comprehension

$\{x : t \mid R : E\}$



Example: $\{x : \mathbb{Z} \mid 0 \leq x < 5 : 2 \cdot x\}$

Set comprehension

$$\{x : t \mid R : E\}$$

Set types

The type of the set is not the type of the body.

If E has type $t1$, the set has type $set(t1)$.

Type $t1$ is not necessarily the same as type t.

Example

$\{x : \mathbb{Z} \mid 0 \leq x < 5 : 2 \cdot x\}$ has type $set(\mathbb{Z})$.

Set comprehension

$$\{x : t \mid R : E\}$$

From comprehension to enumeration

$$\{i \mid 0 < i < 4 : i\} = \{1,2,3\}$$
$$\{i \mid 5 \leq i \leq 8 : 2 \cdot i\} = \{10,12,14,16\}$$
$$\{i \mid 9 \leq i \leq 17 \wedge \text{even}.i : i\} = \{10,12,14,16\}$$
$$\{x,y \mid 2 \leq x \leq 3 \leq y \leq 4 : x^y\} = \{2^3,2^4,3^3,3^4\}$$
$$\{x \mid 0 \leq x < 3 : x \cdot y\} = \{0 \cdot y, 1 \cdot y, 2 \cdot y\}$$
$$\{x \mid 0 \leq x < 0 : x \cdot y\} = \{\ \} \quad \text{the empty set}$$

(11.2) **Axiom, Enumeration:**

$$\{e_0, e_1, \ldots, e_{n-1}\} = \{x \mid x = e_0 \vee x = e_1 \vee \cdots \vee x = e_{n-1} : x\}$$

From enumeration to comprehension

$$\{6, 17\} = \{x \mid x = 6 \vee x = 17 : x\}$$

$$\{a, b, c\} = \{x \mid x = a \vee x = b \vee x = c : x\}$$

(11.3) **Axiom, Set membership:** Provided $\neg occurs(\text{`}x\text{'}, \text{`}F\text{'})$,

$$F \in \{x \mid R : E\} \equiv (\exists x \mid R : F = E)$$

Examples

$$2 \in \{i \mid 0 < i < 4 : i\} \quad \equiv \quad (\exists i \mid 0 < i < 4 : 2 = i)$$

$$13 \in \{i \mid 5 \leq i \leq 8 : 2 \cdot i\} \quad \equiv \quad (\exists i \mid 5 \leq i \leq 8 : 13 = 2 \cdot i)$$

A Logical Approach to Discrete Math

(11.3) **Axiom, Set membership:** Provided $\neg occurs(\text{`}x\text{'}, \text{`}F\text{'})$,

$$F \in \{x \mid R : E\} \equiv (\exists x \mid R : F = E)$$

$\in$ as a binary infix operator

$e \in S$

Element

Set expression

Example: $25 \in \{13, 25\} \equiv true$

$\in$ as a function

elementOf(e, S) returns true if e is an element of S.

Example: elementOf$(25, \{13, 25\})$ returns $true$.

In this example, the type of the function is

elementOf: $\mathbb{Z} \times set(\mathbb{Z}) \to \mathbb{B}$

(11.3) **Axiom, Set membership:** Provided $\neg occurs(\text{`}x\text{'}, \text{`}F\text{'})$,

$$F \in \{x \mid R : E\} \equiv (\exists x \mid R : F = E)$$

Theorem: $e \in \{e\}$

Proof

$e \in \{e\}$

$=$ $\langle$(11.2) Enumeration$\rangle$

$e \in \{x \mid x = e : x\}$

$=$ $\langle$(11.3) Set membeship$\rangle$

$(\exists x \mid x = e : e = x)$

$=$ $\langle$(8.14) One-point rule$\rangle$

$(e = x)[x := e]$

$=$ $\langle$Textual substitution$\rangle$

$e = e$ which is reflexivity of $=$ //

A Logical Approach to Discrete Math

A Theory of Sets

(11.2) **Axiom, Enumeration:** $\{e_0, e_1, \ldots, e_{n-1}\} = \{x \mid x = e_0 \vee x = e_1 \vee \cdots \vee x = e_{n-1} : x\}$

(11.3) **Axiom, Set membership:** Provided $\neg occurs(\text{`}x\text{'}, \text{`}F\text{'})$,

$F \in \{x \mid R : E\} \equiv (\exists x \mid R : F = E)$

(11.4) **Axiom, Extensionality:** $S = T \;\equiv\; (\forall x \mid : x \in S \;\equiv\; x \in T)$

(11.4.1) **Axiom, Empty set:** $\emptyset = \{x \mid false : E\}$

(11.4.2) $e \in \emptyset \;\equiv\; false$

(11.4.3) **Axiom, Universe:** $\mathbf{U} = \{x \mid : x\}$, $\mathbf{U}\colon set(t) = \{x\colon t \mid : x\}$

(11.4.4) $e \in \mathbf{U} \;\equiv\; true$, for $e\colon t$ and $\mathbf{U}\colon set(t)$

(11.5) $S = \{x \mid x \in S : x\}$

A Logical Approach to Discrete Math

(11.5.1) **Axiom, Abbreviation:** For x a single variable, $\{x \mid R\} = \{x \mid R : x\}$

(11.6) Provided $\neg occurs(\text{`}y\text{'}, \text{`}R\text{'})$ and $\neg occurs(\text{`}y\text{'}, \text{`}E\text{'})$,

$\{x \mid R : E\} = \{y \mid (\exists x \mid R : y = E)\}$

(11.7) $x \in \{x \mid R\} \equiv R$

R is the characteristic predicate of the set.

(11.7.1) $y \in \{x \mid R\} \equiv R[x := y]$ for any expression y

(11.9) $\{x \mid Q\} = \{x \mid R\} \equiv (\forall x \mid : Q \equiv R)$

(11.10) $\{x \mid Q\} = \{x \mid R\}$ is valid iff $Q \equiv R$ is valid.

(11.11) **Methods for proving set equality** $S = T$ **:**

(a) Use Leibniz directly.

(b) Use axiom Extensionality (11.4) and prove the (9.8) Lemma $v \in S \equiv v \in T$ for an arbitrary value v.

(c) Prove $Q \equiv R$ and conclude $\{x \mid Q\} = \{x \mid R\}$.

(11.4) **Axiom, Extensionality:** $S = T \equiv (\forall x \mid : x \in S \equiv x \in T)$

(9.8) $(\forall x \mid R : true) \equiv true$

Proving set equality

Use (11.4) and (9.8) to prove that two sets, S and T, are equal.

Lemma: A small theorem used as a step in the main theorem.

(11.4) **Axiom, Extensionality:** $S = T \equiv (\forall x \mid : x \in S \equiv x \in T)$

(9.8) $(\forall x \mid R : true) \equiv true$

Example

Prove (11.5) $S = \{x \mid x \in S : x\}$ without a lemma.

Proof

$$
\begin{array}{ll}
 & S = \{x \mid x \in S : x\} \\
= & \quad \langle (11.4)\ \text{Extentionality} \rangle \\
 & (\forall v \mid : v \in S \equiv v \in \{x \mid x \in S : x\}) \\
= & \ldots \\
 & (\forall v \mid : true) \\
= & \quad \langle (9.8) \rangle \\
 & true \quad //
\end{array}
$$

Example

Prove (11.5) $S = \{x \mid x \in S : x\}$ with a lemma.

The (9.8) lemma

Let v be an arbitrary element, and prove that

$v \in S \equiv v \in \{x \mid x \in S : x\}$

Proof

$v \in \{x \mid x \in S : x\}$

$=$ ⟨(11.3) Set membership⟩

$(\exists x \mid x \in S : v = x)$

$=$ ⟨(9.20.1) Existential double trading⟩

$(\exists x \mid v = x : x \in S)$

$=$ ⟨(8.14) One-point rule⟩

$v \in S$ //

A Logical Approach to Discrete Math

(11.4) **Axiom, Extensionality:** $S = T \equiv (\forall x \mid : x \in S \equiv x \in T)$

(9.8) $(\forall x \mid R : true) \equiv true$

The main proof

$$
\begin{array}{ll}
 & S = \{x \mid x \in S : x\} \\
= & \quad \langle (11.4)\ \text{Extentionality} \rangle \\
 & (\forall v \mid : v \in S \equiv v \in \{x \mid x \in S : x\}) \\
= & \quad \langle \text{The (9.8) lemma} \rangle \\
 & (\forall v \mid : true) \\
= & \quad \langle (9.8) \rangle \\
 & true \quad //
\end{array}
$$

From now on, you may omit the main proof.

A Logical Approach to Discrete Math

(11.5.1) **Axiom, Abbreviation:** For x a single variable, $\{x \mid R\} = \{x \mid R : x\}$

(11.6) Provided $\neg occurs(\text{`}y\text{'}, \text{`}R\text{'})$ and $\neg occurs(\text{`}y\text{'}, \text{`}E\text{'})$,

$\{x \mid R : E\} = \{y \mid (\exists x \mid R : y = E)\}$

(11.7) $x \in \{x \mid R\} \equiv R$

R is the characteristic predicate of the set.

(11.7.1) $y \in \{x \mid R\} \equiv R[x := y]$ for any expression y

(11.9) $\{x \mid Q\} = \{x \mid R\} \equiv (\forall x \mid : Q \equiv R)$

(11.10) $\{x \mid Q\} = \{x \mid R\}$ is valid iff $Q \equiv R$ is valid.

(11.11) **Methods for proving set equality** $S = T$ **:**

(a) Use Leibniz directly.

(b) Use axiom Extensionality (11.4) and prove the (9.8) Lemma $v \in S \equiv v \in T$ for an arbitrary value v.

(c) Prove $Q \equiv R$ and conclude $\{x \mid Q\} = \{x \mid R\}$.

Operations on sets.

(11.12) **Axiom, Size:** $\#S = (\Sigma x \mid x \in S : 1)$

(11.13) **Axiom, Subset:** $S \subseteq T \equiv (\forall x \mid x \in S : x \in T)$

(11.14) **Axiom, Proper subset:** $S \subset T \equiv S \subseteq T \wedge S \neq T$

(11.15) **Axiom, Superset:** $T \supseteq S \equiv S \subseteq T$

(11.16) **Axiom, Proper superset:** $T \supset S \equiv S \subset T$

(11.17) **Axiom, Complement:** $v \in\sim S \equiv v \in \mathbf{U} \wedge v \notin S$

(11.18) $v \in\sim S \equiv v \notin S$, for v in $\mathbf{U}$

(11.19) $\sim\sim S = S$

(11.20) **Axiom, Union:** $v \in S \cup T \equiv v \in S \vee v \in T$

(11.21) **Axiom, Intersection:** $v \in S \cap T \equiv v \in S \wedge v \in T$

(11.22) **Axiom, Difference:** $v \in S - T \equiv v \in S \wedge v \notin T$

(11.23) **Axiom, Power set:** $v \in \mathcal{P}S \equiv v \subseteq S$

(11.12) **Axiom, Size:** $\#S = (\Sigma x \mid x \in S : 1)$

Example

$\mathbf{U}: \{a, b, c, d, e, f\}$

$S: \{b, e, f\}$

$\#S = 1 + 1 + 1 = 3$

(11.13) **Axiom, Subset:** $S \subseteq T \equiv (\forall x \mid x \in S : x \in T)$

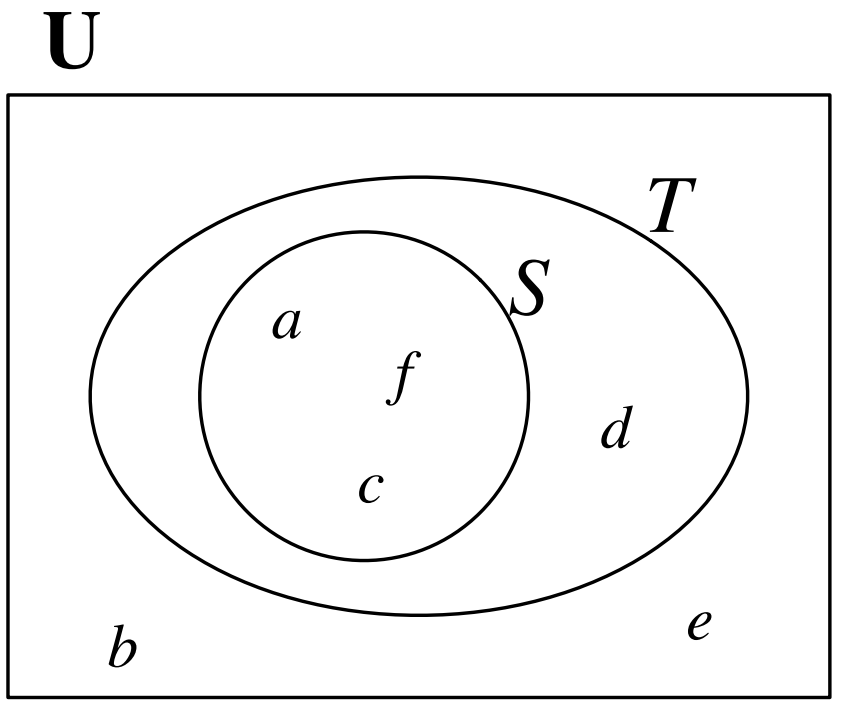
Example

$\mathbf{U}: \{a, b, c, d, e, f\}$

$S: \{a, c, f\}$

$T: \{d, f, c, a\}$

$S \subseteq T$



(11.13) **Axiom, Subset:** $S \subseteq T \equiv (\forall x \mid x \in S : x \in T)$

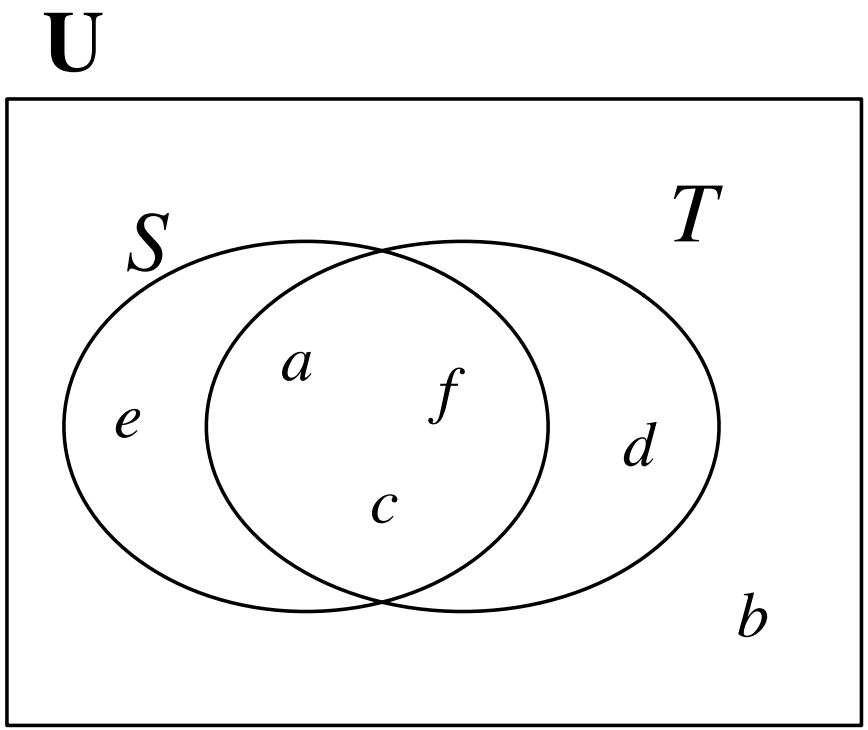
Example

$\mathbf{U}: \{a, b, c, d, e, f\}$

$S: \{a, c, f, e\}$

$T: \{d, f, c, a\}$

$S \not\subseteq T$



(11.13) **Axiom, Subset:** $S \subseteq T \equiv (\forall x \mid x \in S : x \in T)$

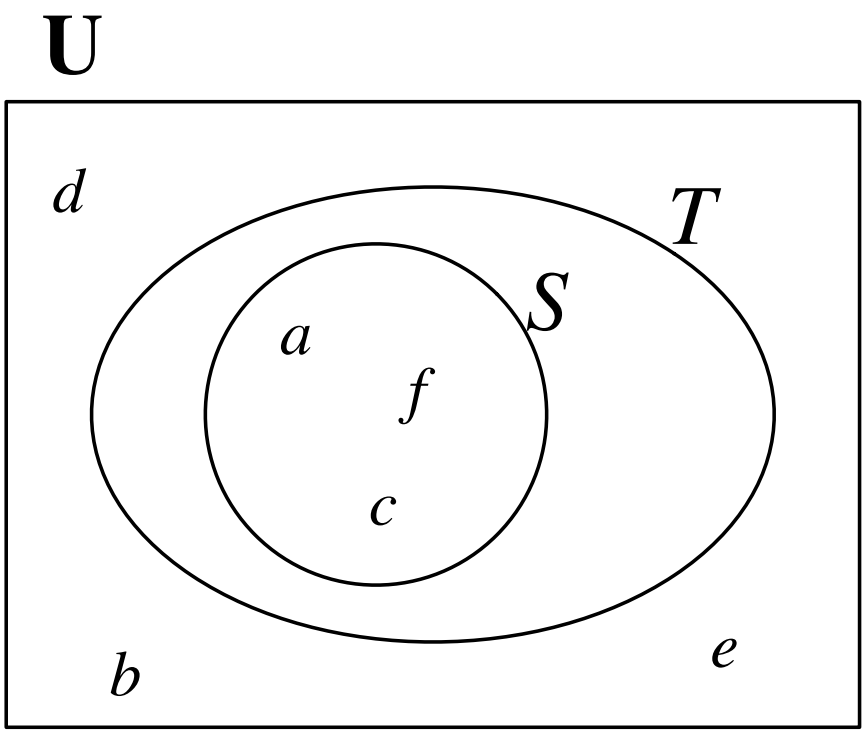
Example

$\mathbf{U}: \{a, b, c, d, e, f\}$

$S: \{a, c, f\}$

$T: \{f, c, a\}$

$S \subseteq T$



(11.14) **Axiom, Proper subset:** $S \subset T \equiv S \subseteq T \wedge S \neq T$

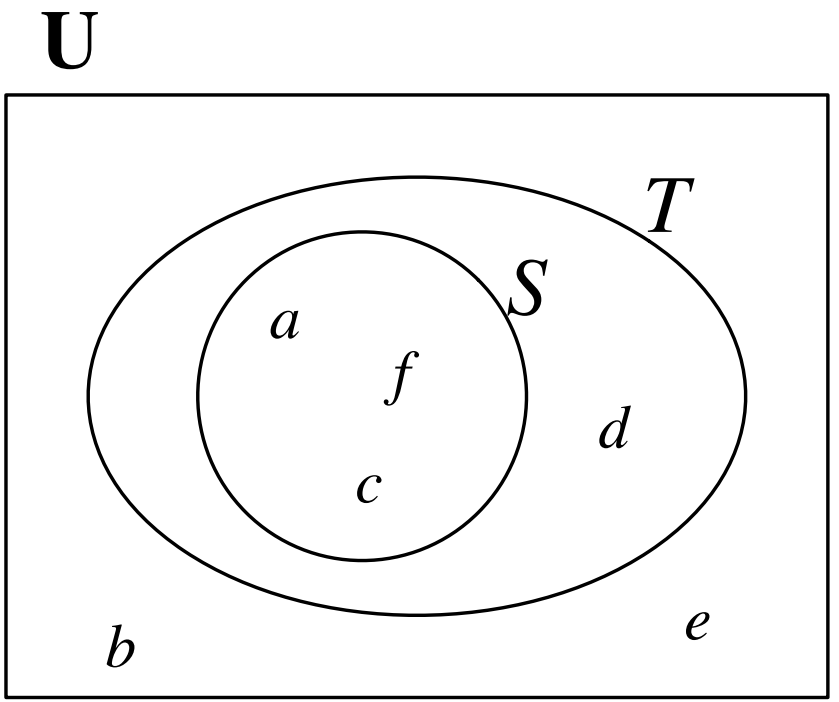
Example

$\mathbf{U}: \{a, b, c, d, e, f\}$

$S: \{a, c, f\}$

$T: \{d, f, c, a\}$

$S \subset T$



(11.14) **Axiom, Proper subset:** $S \subset T \equiv S \subseteq T \wedge S \neq T$

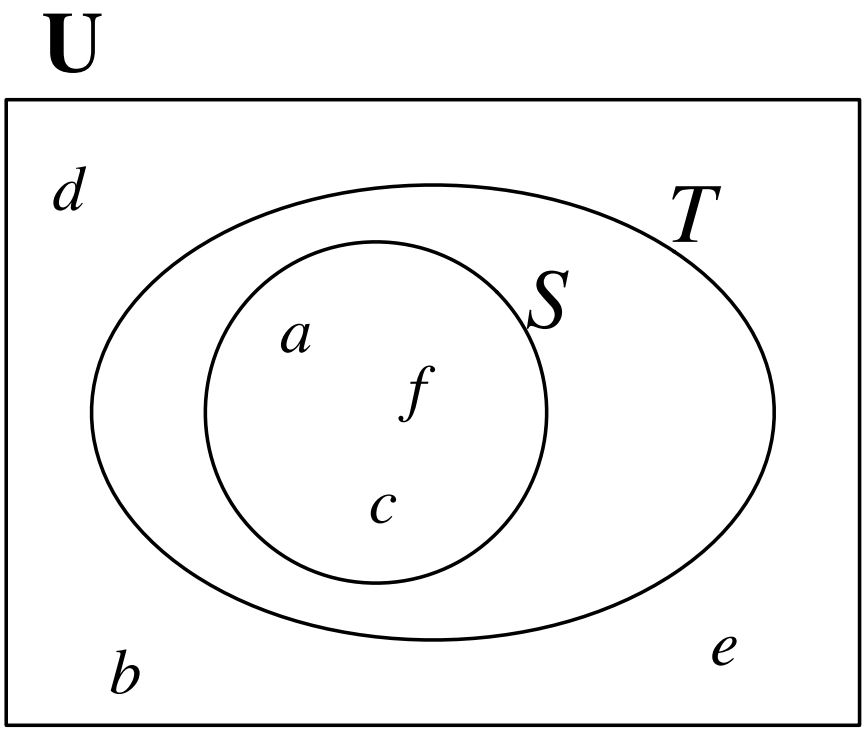
Example

$\mathbf{U}: \{a, b, c, d, e, f\}$

$S: \{a, c, f\}$

$T: \{f, c, a\}$

$S \not\subset T$



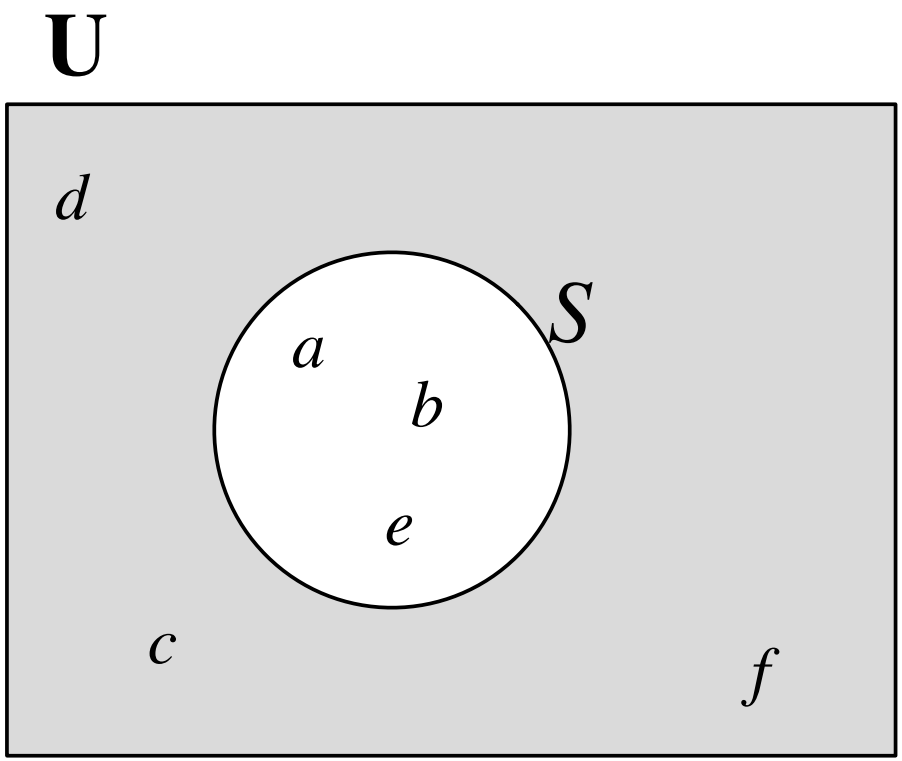
(11.17) **Axiom, Complement:** $v \in \sim S \equiv v \in \mathbf{U} \wedge v \notin S$

Example

$\mathbf{U}: \{a, b, c, d, e, f\}$

$S: \{a, b, e\}$

$\sim S = \{c, d, f\}$



(11.20) **Axiom, Union:** $v \in S \cup T \equiv v \in S \vee v \in T$

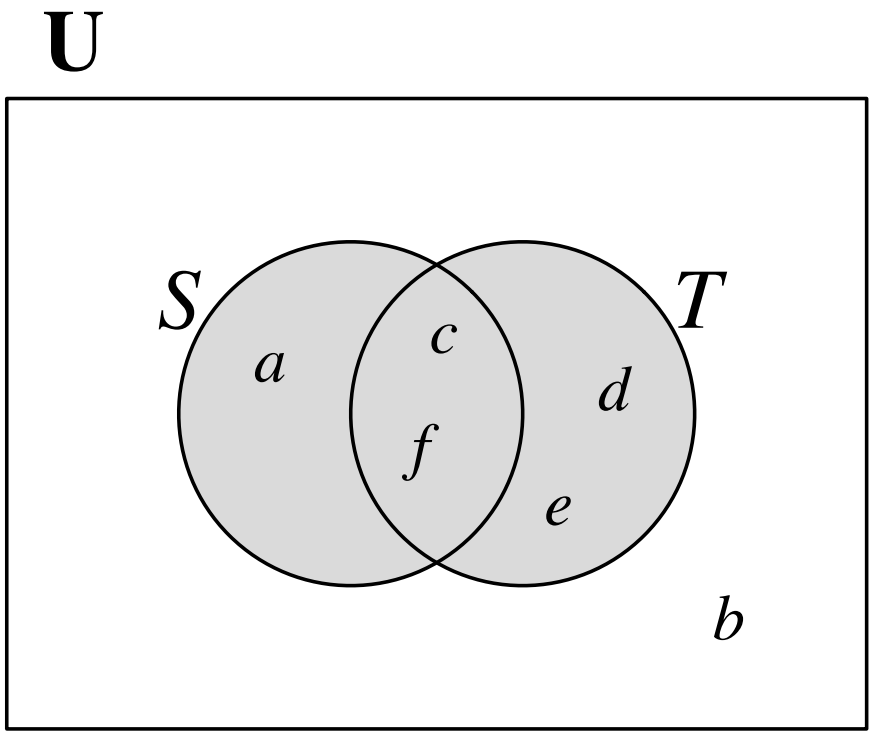
Example

$\mathbf{U}: \{a,b,c,d,e,f\}$

$S: \{a,c,f\}$

$T: \{c,d,e,f\}$

$S \cup T = \{a,c,d,e,f\}$



(11.21) **Axiom, Intersection:** $v \in S \cap T \equiv v \in S \wedge v \in T$

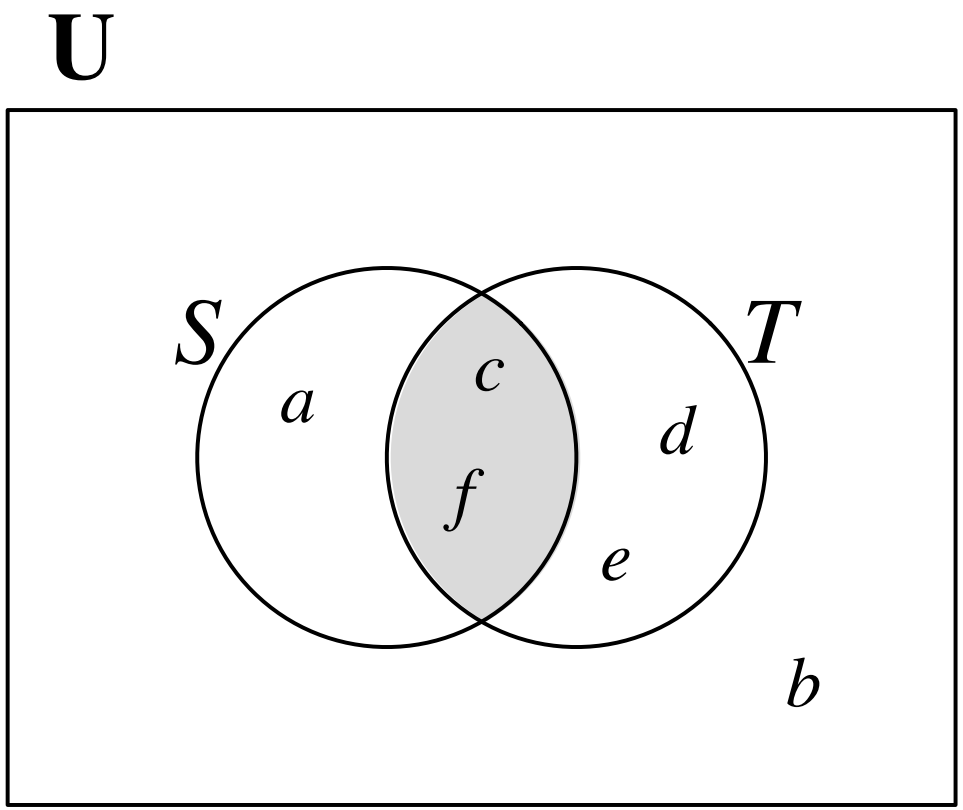
Example

$\mathbf{U}: \{a, b, c, d, e, f\}$

$S: \{a, c, f\}$

$T: \{c, d, e, f\}$

$S \cap T = \{c, f\}$



(11.22) **Axiom, Difference:** $v \in S - T \equiv v \in S \wedge v \notin T$

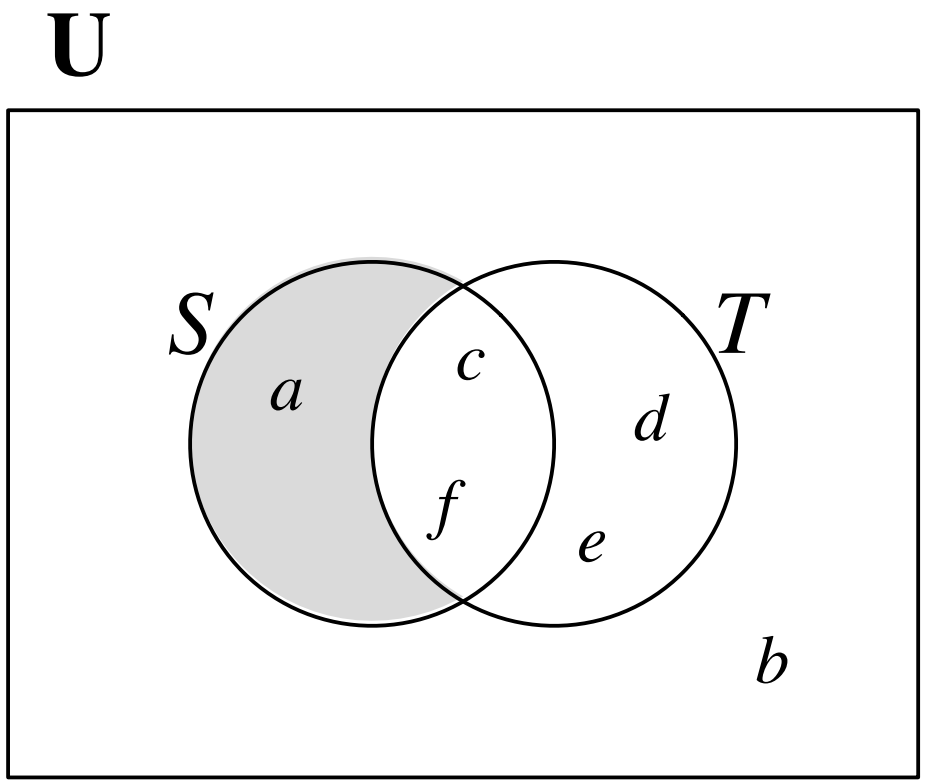
Example

$\mathbf{U}: \{a, b, c, d, e, f\}$

$S: \{a, c, f\}$

$T: \{c, d, e, f\}$

$S - T = \{a\}$



(11.23) **Axiom, Power set:** $v \in \mathscr{P}S \equiv v \subseteq S$

Example

$S: \{a,b\}$

$\mathcal{P}S = \{\{\},\{a\},\{b\},\{a,b\}\}$

Example

$S: \{a,b,c\}$

$\mathcal{P}S = \{\{\},\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\}$

A Logical Approach to Discrete Math

TABLE 11.1. TYPES OF SET EXPRESSIONS IN THEORY $set(t)$

Expression	Example (with types)	Type of result
Empty set, universe, variable	$\emptyset$ or $\mathbf{U}$ or S	$set(t)$
Set enumeration	$\{e_1{:}t, \ldots, e_n{:}t\}$	$set(t)$
Set comprehension	$\{x \mid R{:}\mathbb{B} : E{:}t\}$	$set(t)$
	$\{x{:}t \mid R{:}\mathbb{B}\}$	$set(t)$
Set membership	$x{:}t \in S{:}set(t)$	$\mathbb{B}$
Set equality	$S{:}set(t) = T{:}set(t)$	$\mathbb{B}$
Set size	$\# S{:}set(t)$	$\mathbb{N}$
$\subset$, $\supset$, $\subseteq$, $\supseteq$	$S{:}set(t) \subseteq T{:}set(t)$	$\mathbb{B}$
Complement	$\sim S{:}set(t)$	$set(t)$
$\cup$, $\cap$, $-$	$S{:}set(t) \cup T{:}set(t)$	$set(t)$
Power set	$(\mathcal{P}\ S){:}set(t)$	$set(set(t))$

(11.24) **Definition.** Let E_s be a set expression constructed from set variables, $\emptyset$, $\mathbf{U}$, $\sim$, $\cup$, and $\cap$. Then E_p is the expression constructed from E_s by replacing:
$\emptyset$ with $false$, $\mathbf{U}$ with $true$, $\cup$ with $\vee$, $\cap$ with $\wedge$, $\sim$ with $\neg$.
The construction is reversible: E_s can be constructed from E_p.

Example

E_s : $S \cup \sim S$ This S is a set expression.
E_p : $S \vee \neg S$ This S is a boolean expression.

Example

E_s : $\emptyset$ This is a set expression.
E_p : $false$ This is a boolean expression.

(11.25) **Metatheorem.** For any set expressions E_s and F_s:

(a) $E_s = F_s$ is valid iff $E_p \equiv F_p$ is valid,

(b) $E_s \subseteq F_s$ is valid iff $E_p \Rightarrow F_p$ is valid,

(c) $E_s = \mathbf{U}$ is valid iff E_p is valid.

Example

$S \cap \sim S = \emptyset$ is valid iff $S \wedge \neg S \equiv false$ is valid.

Example

$S \cap T \subseteq S$ is valid iff $S \wedge T \Rightarrow S$ is valid.

Prove (11.51) $S - \emptyset = S$

Proof

$S - \emptyset = S$

$=$ $\langle (11.49) \rangle$

$S \cap \sim \emptyset = S$

By Metatheorem (11.25a) $S \cap \sim \emptyset = S$ is valid

iff $S \wedge \neg false \equiv S$ is valid

$S \wedge \neg false$

$=$ $\langle (3.13) \rangle$

$S \wedge true$

$=$ $\langle (3.39) \rangle$

S //

CAUTION: You cannot use a metatheorem in a proof hint.

The following step is illegal.

Prove (11.51) $\quad S - \emptyset = S$

Proof

$$
\begin{aligned}
& S - \emptyset = S \\
= & \quad \langle (11.49) \rangle \\
& S \cap \sim \emptyset = S \\
= & \quad \langle (11.25a) \rangle \quad \longleftarrow \text{ Illegal} \\
& S \wedge \neg false \equiv S
\end{aligned}
$$

Quantifying union and intersection

(11.74.1) **Definition:** $v \in (\cup x \mid R : E) \equiv (\exists x \mid R : v \in E)$

(11.75.1) **Definition:** $v \in (\cap x \mid R : E) \equiv (\forall x \mid R : v \in E)$

Quantifying union $\cup$

$\cup$ is symmetric: (11.26) $S \cup T = T \cup S$

$\cup$ is associative: (11.27) $(S \cup T) \cup U = S \cup (T \cup U)$

$\cup$ has an identity: (11.30) $S \cup \emptyset = S$

Therefore, $\cup$ is an abelian monoid and can be quantified.

(11.76) **Axiom, Partition:** Set S partitions T if

(i) the sets in S are pairwise disjoint and

(ii) the union of the sets in S is T, that is, if

$$(\forall u, v \mid u \in S \wedge v \in S \wedge u \neq v : u \cap v = \emptyset) \wedge (\cup u \mid u \in S : u) = T$$

(11.76) **Axiom, Partition:** Set S partitions T if

(i) the sets in S are pairwise disjoint and

(ii) the union of the sets in S is T, that is, if

$$(\forall u, v \mid u \in S \wedge v \in S \wedge u \neq v : u \cap v = \emptyset) \wedge (\cup u \mid u \in S : u) = T$$

(11.76) **Axiom, Partition:** Set S partitions T if

(i) the sets in S are pairwise disjoint and

(ii) the union of the sets in S is T, that is, if

$$(\forall u, v \mid u \in S \wedge v \in S \wedge u \neq v : u \cap v = \emptyset) \wedge (\cup u \mid u \in S : u) = T$$

Example

T : $\{a, b, c, d, e, f\}$

S : $\{\{a, c\}, \{b, e, f\}, \{d\}\}$

S partitions T.

(11.76) **Axiom, Partition:** Set S partitions T if

(i) the sets in S are pairwise disjoint and

(ii) the union of the sets in S is T, that is, if

$$(\forall u, v \mid u \in S \wedge v \in S \wedge u \neq v : u \cap v = \emptyset) \wedge (\cup u \mid u \in S : u) = T$$

Example

T : $\{a, b, c, d, e, f\}$

S : $\{\{a, c\}, \{b, e, f\}, \{d, e\}\}$

S does not partition T because $\{b, e, f\} \cap \{d, e\} \neq \emptyset$.

(11.76) **Axiom, Partition:** Set S partitions T if

(i) the sets in S are pairwise disjoint and

(ii) the union of the sets in S is T, that is, if

$$(\forall u, v \mid u \in S \wedge v \in S \wedge u \neq v : u \cap v = \emptyset) \wedge (\cup u \mid u \in S : u) = T$$

Example

T : $\{a, b, c, d, e, f\}$

S : $\{\{a, c\}, \{e, f\}, \{d\}\}$

S does not partition T because $\{a, c\} \cup \{e, f\} \cup \{d\} \neq T$.

Bags

Same as sets, but duplicates allowed.

$$\{\!|x{:}\mathbb{N} \mid -2 \leq x \leq 2 : x^2|\!\} = \{\!|4,1,0,1,4|\!\}$$
$$\{x{:}\mathbb{N} \mid -2 \leq x \leq 2 : x^2\} = \{4,1,0\}$$

Bags

(11.79) **Axiom, Membership:** $v \in \{\!|x \mid R : E|\!\} \equiv (\exists x \mid R : v = E)$

(11.80) **Axiom, Size:** $\#\{\!|x \mid R : E|\!\} = (\Sigma x \mid R : 1)$

(11.81) **Axiom, Number of occurrences:**

$$v\#\{\!|x \mid R : E|\!\} = (\Sigma x \mid R \wedge v = E : 1)$$

(11.82) **Axiom, Bag equality:** $B = C \equiv (\forall v \mid : v \# B = v \# C)$

(11.83) **Axiom, Subbag:** $B \subseteq C = (\forall v \mid : v \# B \leq v \# C)$

(11.84) **Axiom, Proper subbag:** $B \subset C = B \subseteq C \wedge B \neq C$

(11.85) **Axiom, Union:** $B \cup C = \{\!|v, i \mid 0 \leq i < v \# B + v \# C : v|\!\}$

(11.86) **Axiom, Intersection:**

$$B \cap C = \{\!|v, i \mid 0 \leq i < v \# B \downarrow v \# C : v|\!\}$$

(11.87) **Axiom, Difference:**

$$B - C = \{\!|v, i \mid 0 \leq i < v \# B - v \# C : v|\!\}$$