Mathematical basis

- The B Method is based on two well-known mathematical theories:
  - (first order) predicate calculus
  - set theory

Predicate Logic

- B uses the logic of the first order predicate calculus
- A predicate is a logical expression, i.e. a function from some set X to set BOOL (= {TRUE,FALSE})
- Standard operations:

$\wedge$	&	conjunction
$\vee$	or	disjunction
$\Rightarrow$	=>	implication
$\Leftrightarrow$	<=>	equivalence
$\neg$	not	negation

Constraining Predicates

- There some contexts where it is stated that a predicate P must *constrain* some list of variables z

- To constrain the variable x, P must contain predicates of the form: $x \in S$, $x \subseteq S$, $x \subset S$, or $x = E$ for some expression E

Universal Quantification

- Publication $\forall z. (P \Rightarrow Q)$
  ASCII `!(z).(P => Q)`
- For all values of z satisfying constraining predicate P, Q is true
- Notice that, if P is false (there are no values satisfying P), then $\forall z. (P \Rightarrow Q)$ is true – everything in the empty set can be assigned any property
- In a room that does not contain any elephants, you may assert that all the elephants in the room are pink!

Existential Quantification

- Publication $\exists z. (P \wedge Q)$
  ASCII `#(z).(P & Q)`
- There exist some values of z satisfying constraining predicate P for which Q is true
- Notice that, if P is false (there are no values satisfying P), then $\exists z. (P \wedge Q)$ is false – nothing in the empty set can be assigned any property
- In a room that does not contain any elephants, you cannot assert that any of elephants in the room is pink!

Set Theory

- B uses the mathematics of set theory
- A set is a collection of entities of some sort
- A set is completely defined by its elements
- Sets can be given
  - by listing their elements
  - by specifying properties that characterize their members

Set Theory (cont.)

- Sets have neither ordering or multiplicity, so $\{1,2\}$, $\{2,1\}$, and $\{2,1,2\}$ denote the same set
- Sets in B must be well typed. That is all the elements of a set must be of the same type
- Thus $\{1,\{1\}\}$ is not valid set in B; 1 is a number, but $\{1\}$ is a set of numbers

Assertions about Sets

$e \in S$	$e : S$	Set membership: "e belongs to S" or "e is an element of S"
$e \notin S$	$e /: S$	"e does not belong to S", i.e. $\neg(e \in S)$
$S \subseteq T$	$S <: T$	Set inclusion: "S is included in T"
$S \not\subseteq T$	$S /<: T$	"S is not included in T", i.e. $\neg(S \subseteq T)$
$S \subset T$	$S <<: T$	Strict set inclusion: "S is included in T, but not equal to T
$S \not\subset T$	$S /<<: T$	"S is not strictly included in T", i.e. $\neg(S \subset T)$

Some Sets

- Empty set $\{\}$. The set that contains no elements
- Singleton set $\{E\}$. The singleton set contains a single element, which itself may be a set. $\{1\}, \{dog\}, \{\{2\}\}$
- Enumerated set $\{E1, E2, \cdots\}$. The set contains some fixed number of given elements. $\{1, 2, 3\}, \{cat, dog\}, \{\{1\}, \{1, 2\}\}$
- Interval set $n_1..n_2$, where n_1,n_2 are natural numbers
- Predefined sets like NAT (natural numbers), NAT1 (positive natural numbers), BOOL (truth values) etc.

Set Expressions

$\{z \mid P\}$	$\{z \mid P\}$	Set comprehension: "set contains elements z satisfying P". P must contain constraining predicates, i.e. predicates of the form $x \in S$, $x = E$, $x \subset S$ or $x \subseteq S$, where x is a variable in z
$\{z \mid z \in R \land P\}$		"the subset of R such that P"
$S \times T$	$S * T$	Cartesian product $S \times T \ = \ \{x, y \mid x \in S \land x \in T\}$
$card(S)$	$card(S)$	Cardinality of a (finite) set, i.e. the number of elements

Set Expressions (cont.)

$S \cup T$	$S \backslash/ T$	Set union: the set of elements that are elements of S or T
$S \cap T$	$S /\backslash T$	Set intersection: the set of elements that are elements of both S and T
$S - T$	$S - T$	Set difference: the set of elements that are elements of S, but not of T
$\mathcal{P}(\mathcal{S})$	$POW(S)$	Power set: the set of all subsets of S
$\mathcal{P}_1(S)$	$POW1(S)$	The set of all non-empty subsets of S, $\mathcal{P}_1(S) = \mathcal{P}(\mathcal{S}) - \{\emptyset\}$
$\mathcal{F}(\mathcal{S})$	$FIN(S)$	The set of all finite subsets of S
$\mathcal{F}_1(S)$	$FIN1(S)$	The set of all non-empty finite subsets of S, $\mathcal{F}_1(S) = \mathcal{F}(\mathcal{S}) - \{\emptyset\}$

Substitution

- widely used in B Method
- expression E can be substituted for free variable x in predicate P, which is denoted

$$P[E/x]$$

- A variable x is *free* in an expression if it is not bound by quantifier
- Restriction: no free variable can become bound
- generalized (multiple) substitution:

$$P[E_1, ...E_n/x_1, ...x_n]$$