CSCI262 – Systems Security

More example on BLP Lattice

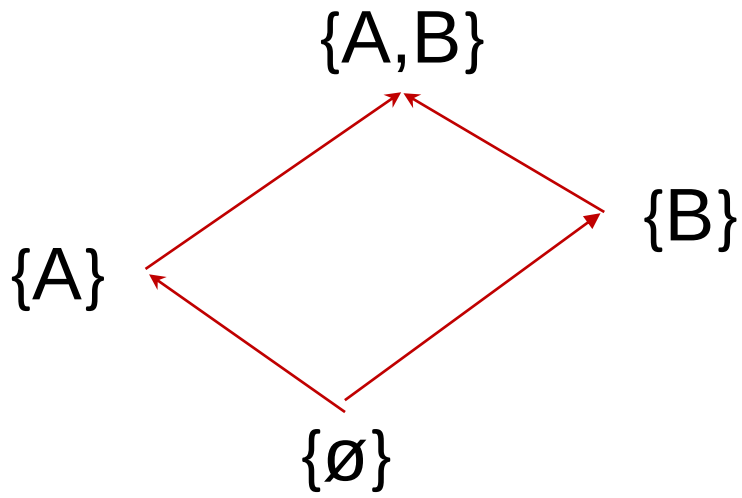
sjapit@uow.edu.au

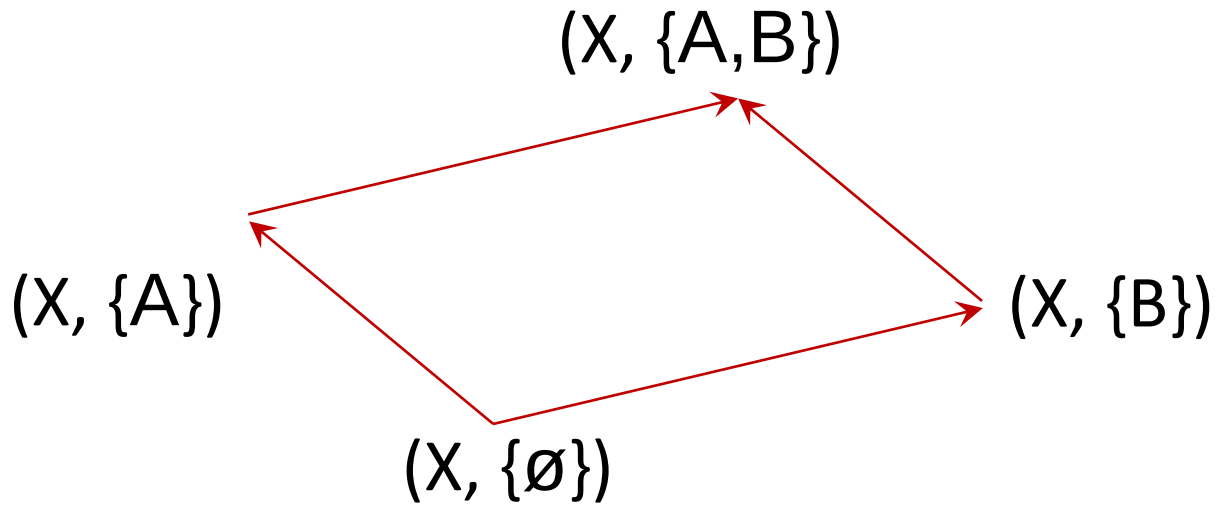
15 October 2020

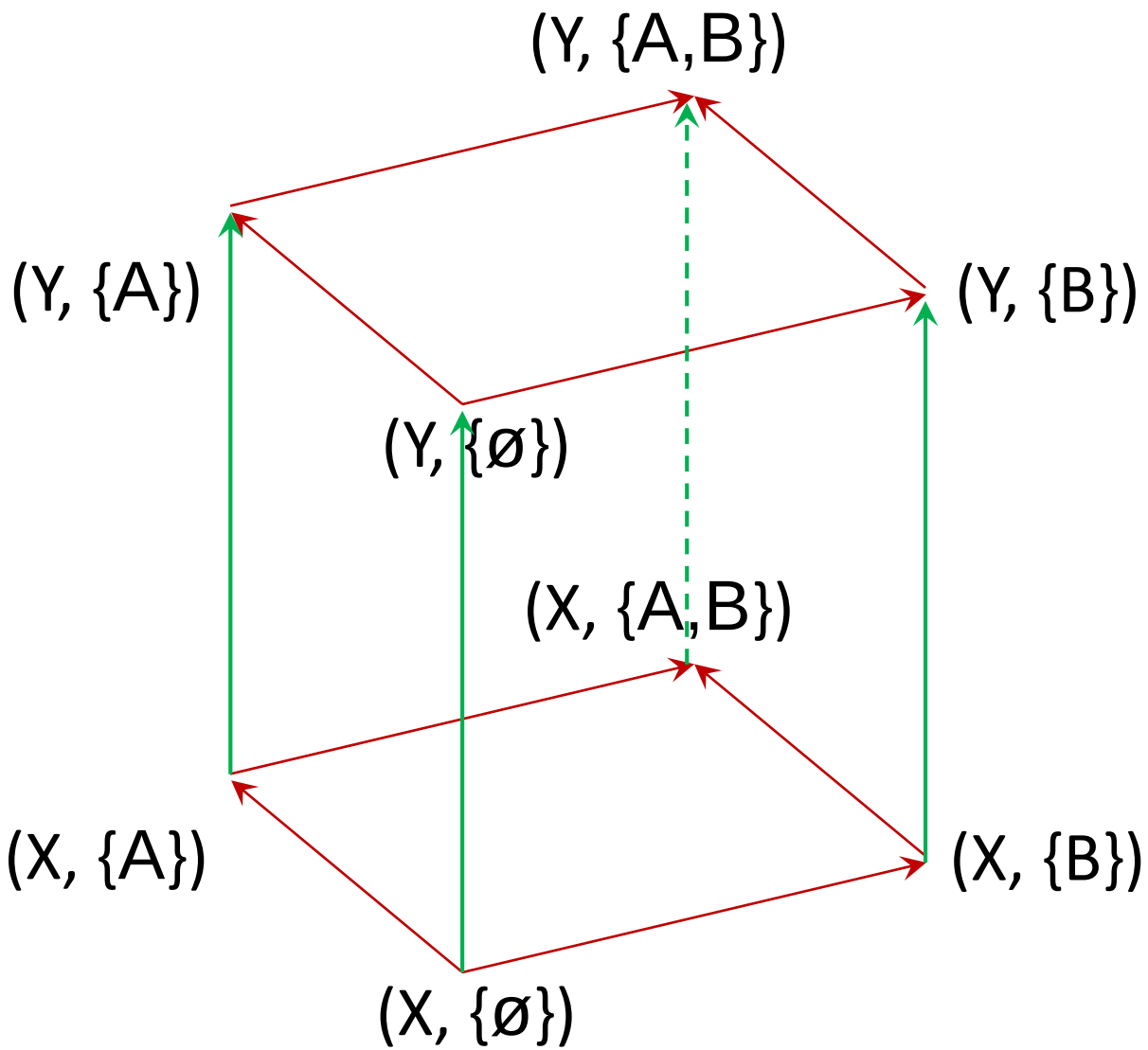
BLP Lattice

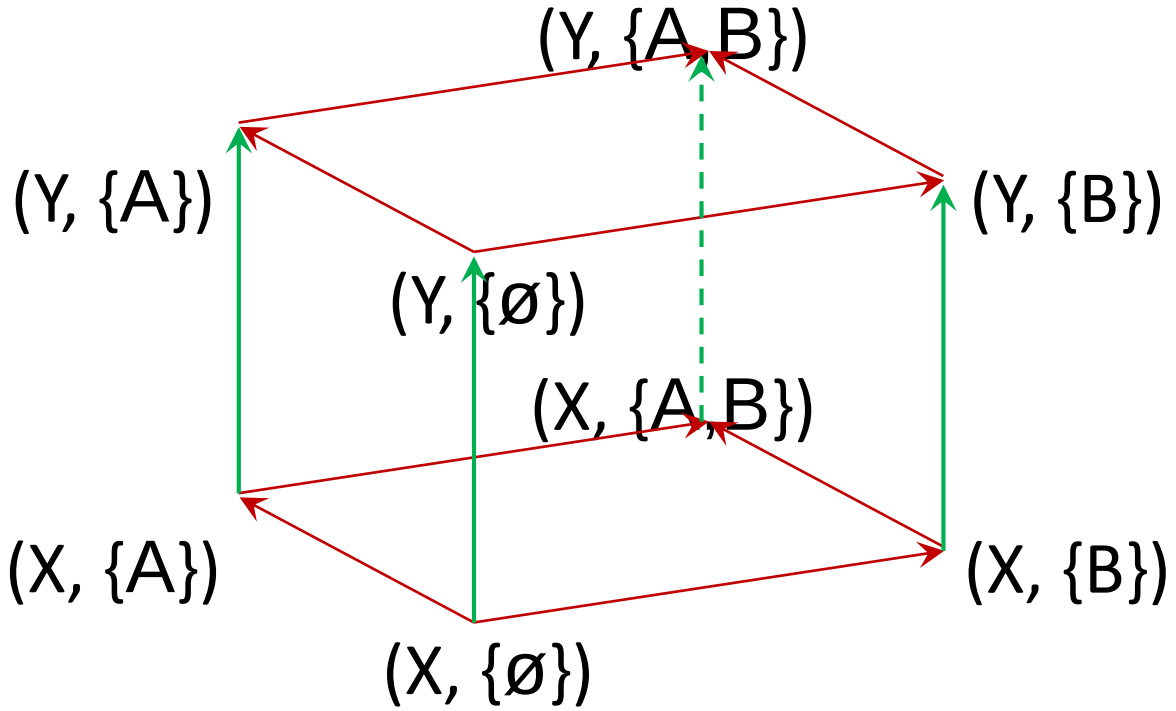
Consider a BLP lattice system with multilevel classifications $C = \{X, Y\}$ and multilateral categories $K = \{A, B\}$. Sketch a diagram to illustrate the relationship between the security levels in this system. Explain, with reference to your diagram, the concept of partial ordering. State the BLP rule and give an example, based on your diagram, to explain each aspect of it.

{A} {B}





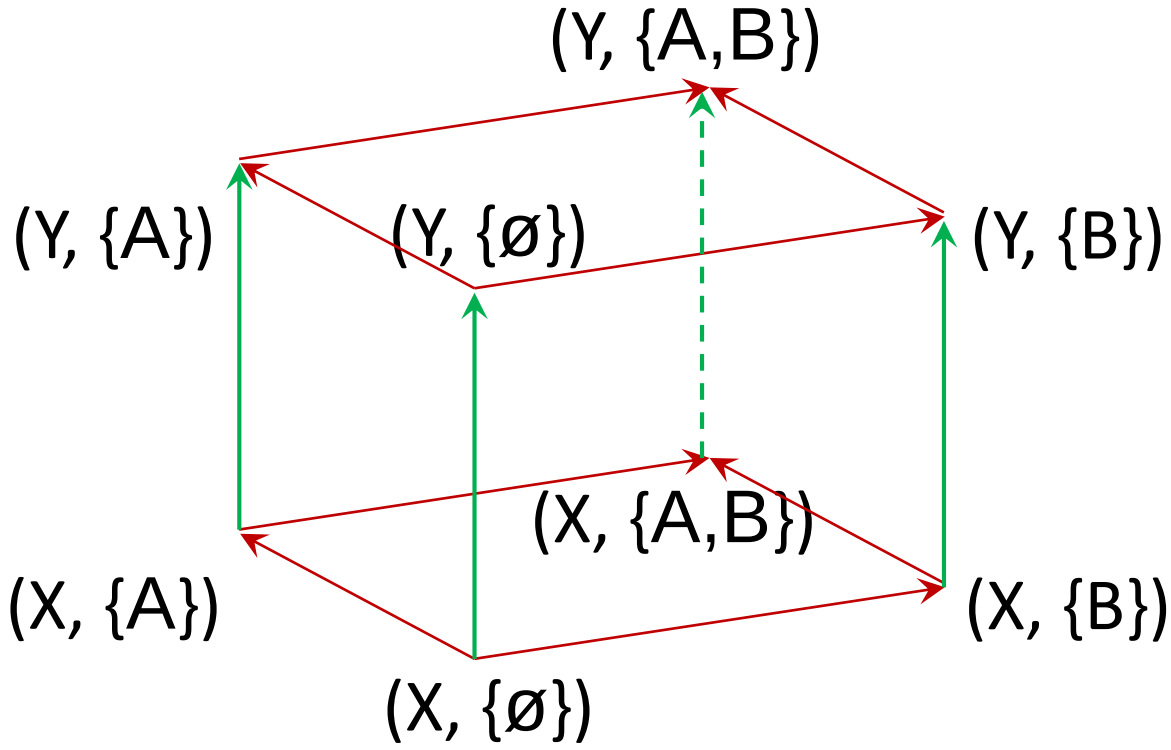

(Y, {A,B})
(Y, {A})
(Y, {B})
(Y, {ø})
(X, {A,B})
(X, {A})
(X, {B})
(X, {ø})


(Y, {A, B})
(Y, {A})
(Y, {B})
(Y, {ø})
(X, {A, B})
(X, {A})
(X, {B})
(X, {ø})

Example of the dominances:

(Y,{ø}) ≥ (X,{ø})
(Y,{A}) ≥ (X,{A})
(Y,{B}) ≥ (X,{B})
(Y,{A,B}) ≥ (X,{A,B})
(Y,{A}) ≥ (Y,{ø})
(Y,{B}) ≥ (Y,{ø})

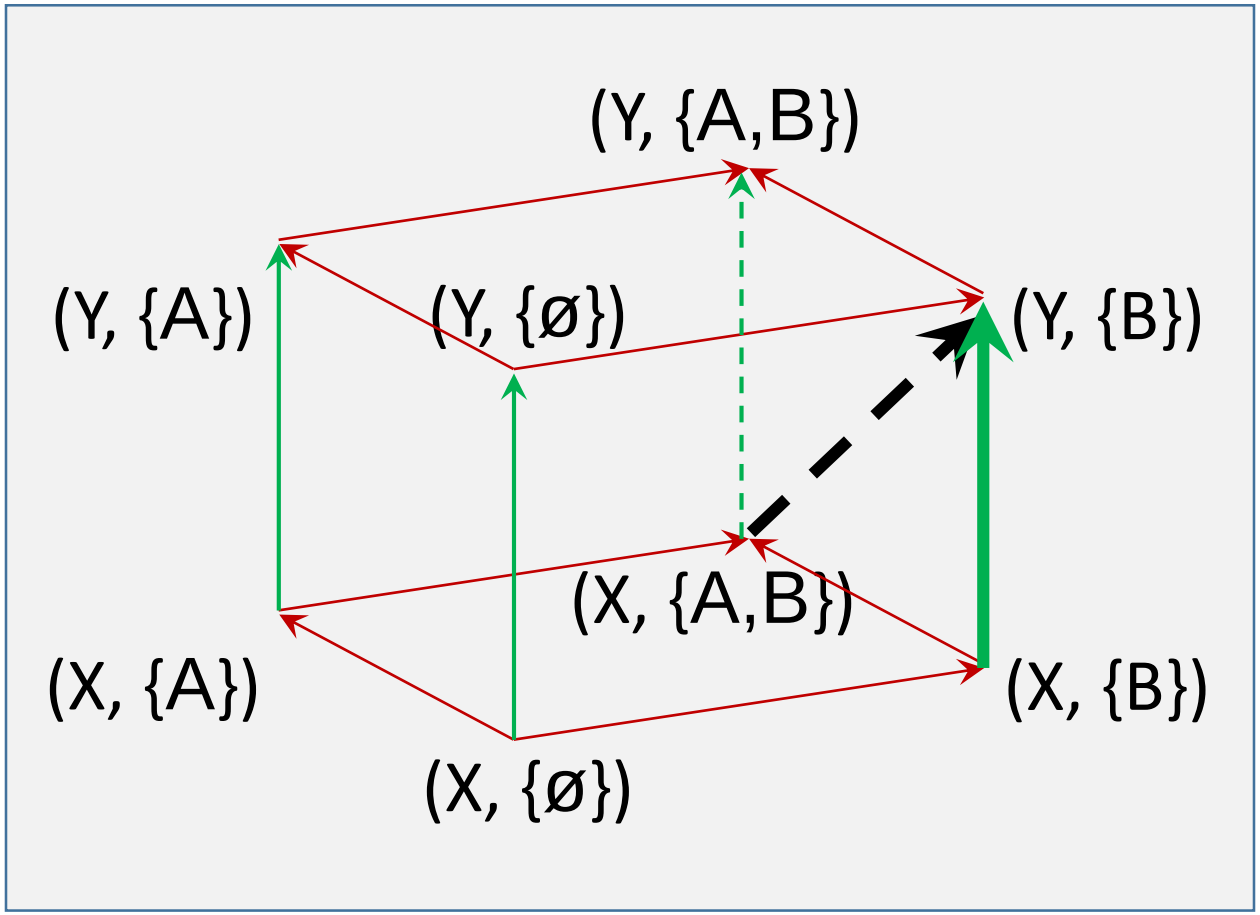
(X,{A}) ≥ (X,{ø})
(X,{B}) ≥ (X,{ø})
(X,{A,B}) ≥ (X,{A})
(X,{A,B}) ≥ (X,{B})



Partial Order

- The partial ordering <= is defined by (x, {A}) <= (y, {A}) if and only if x <= y and {A} <= {A}.

- Hence, in the above example, (Y,{B}) ≥ (X,{B}) forms a partial ordering because Y ≥ X and {B} ≥ {B}.



- However, (Y,{B}) ≥ (X, {A,B}) does not form a partial ordering because {B} does not dominate {A,B} although Y dominate X.

BLP properties (Rules)

- Ss-property
  - Subject S(n) can WRITE object O(n) iff level of clearance of subject L(S) is less than or equal the level of clearance of the object L(O), that is, L(S) ≤ L(O), and the subject has permission to WRITE the object.

- *-property
  - Subject S(n) can READ object O(n) iff level of clearance of subject L(S) is greater than or equal (dominant) the level of object L(O), that is, L(S) ≥ L(O), and the subject has permission to READ the object.

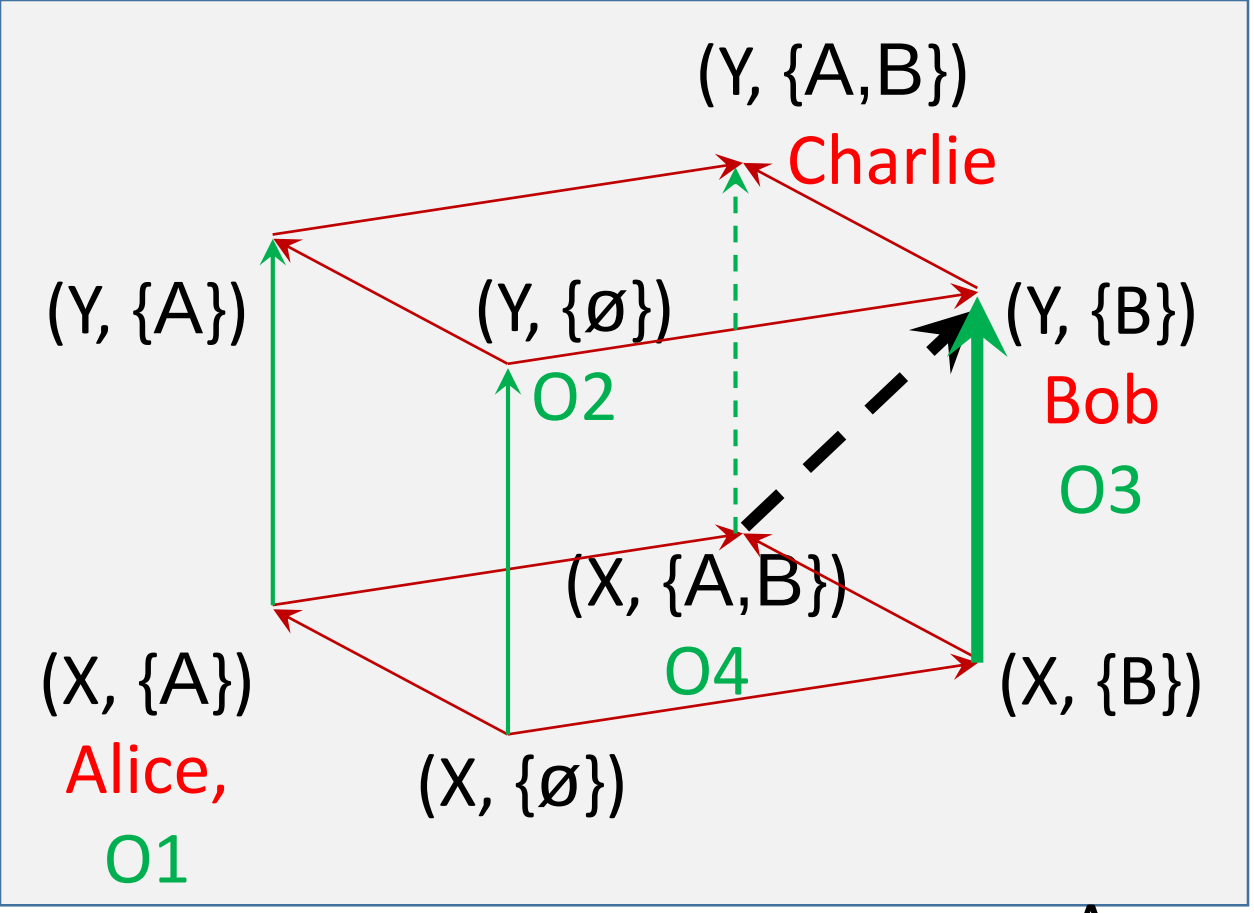
- Discretionary
  - Subject S(n) can discretionarily transfer his/her authorization to Subject at a different clearance level (subject to organization policy).

Subjects and Object at various level of clearance

- For example, we have three subjects Alice, Bob and Charlie and four objects O1, O2, O3 and O4 with the following level of clearance defined:

Subject	Level
Alice	(X,{A})
Bob	(Y,{B})
Charlie	(Y,{A,B})

Object	Level
O1	(X,{A})
O2	(Y,{ø})
O3	(Y,{B})
O4	(X, {A,B})



Subject	Level
Alice	(X,{A})
Bob	(Y,{B})
Charlie	(Y,{A,B})

Object	Level
O1	(X,{A})
O2	(Y,{ø})
O3	(Y,{B})
O4	(X, {A,B})

What if user want to allow Bob to access (read or write or both) O4?

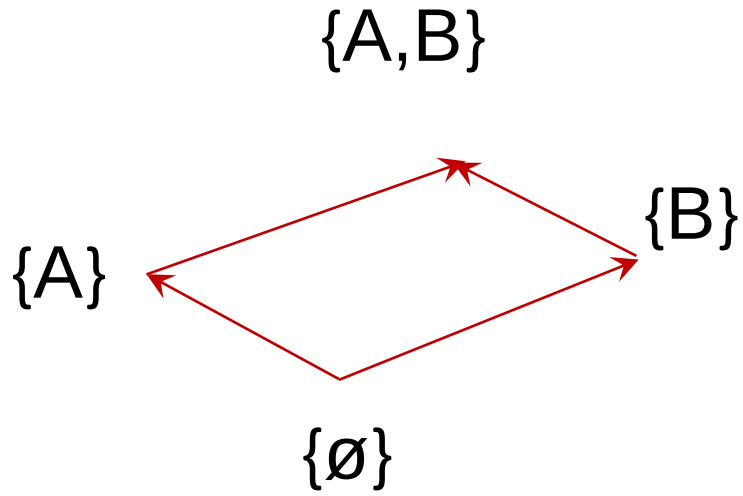
Access Control Matrix:

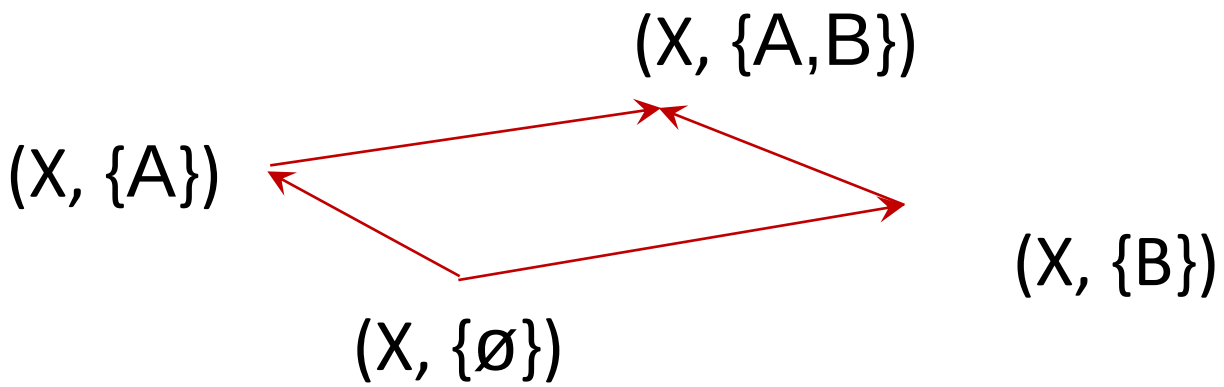
	O1	O2	O3	O4
Alice	R, W	-	-	W
Bob	-	R	R,W	-
Charlie	R	R	R	R

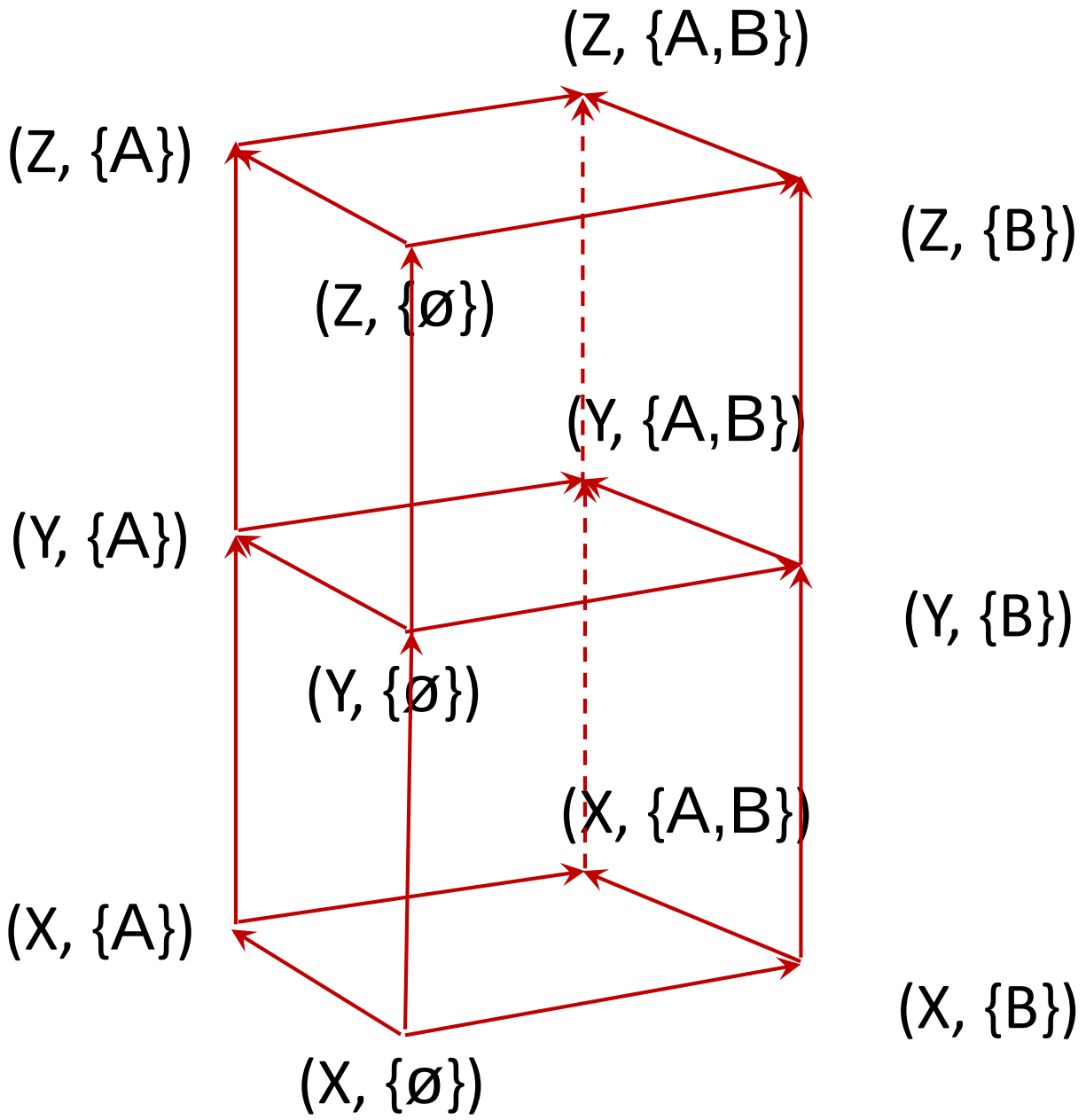
Yet anther BLP lattice example

5) A company has two department, A and B and has determined that it is appropriate to have three levels of sensitivity, in increasing order X, Y and Z. Draw a BLP lattice system to represent this scenario. Using examples, explain the three BLP rules, 2 mandatory and 1 discretionary.

{A} {B}

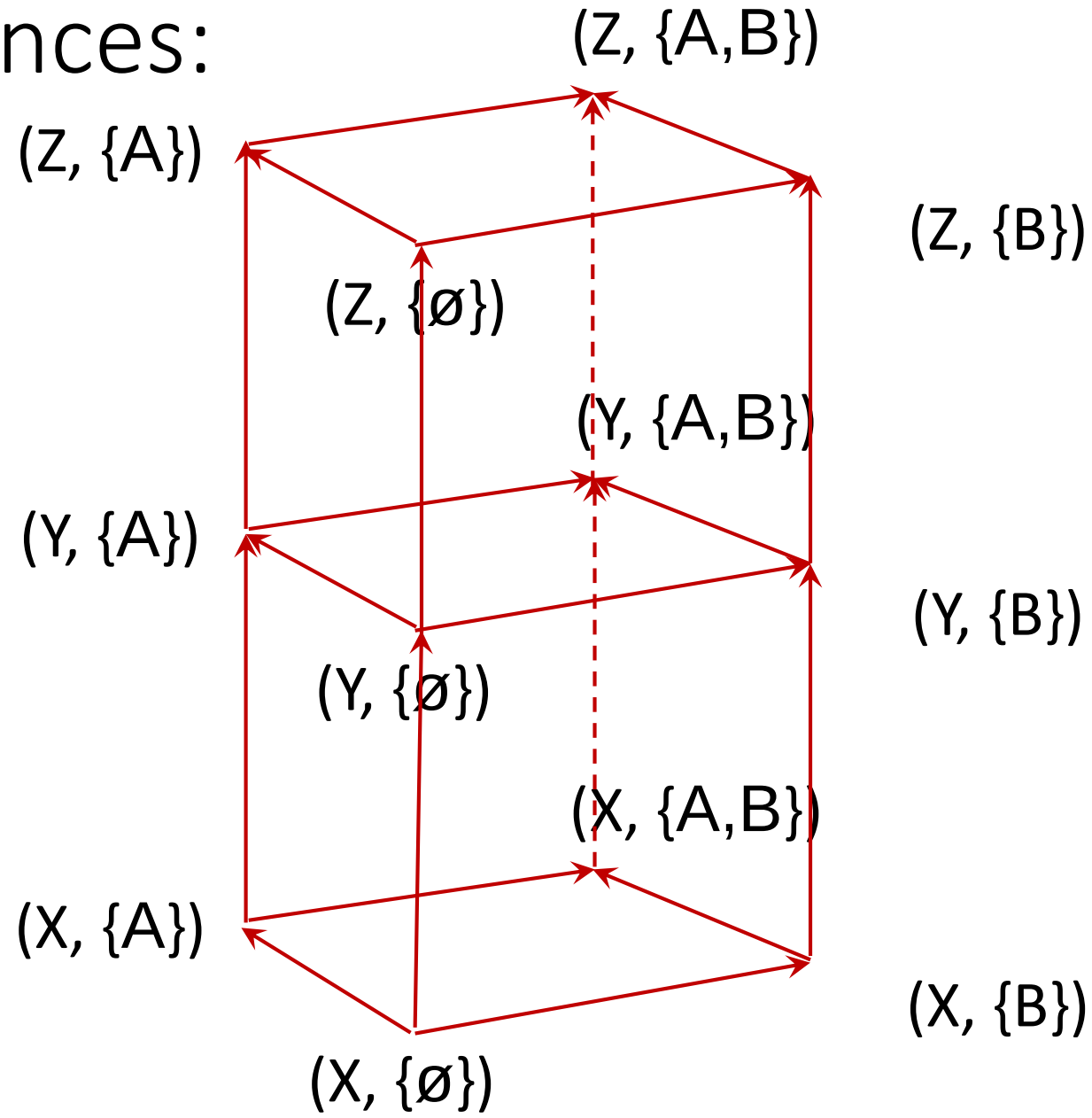





(Z, {A,B})
(Z, {A})
(Z, {B})
(Z, {ø})
(Y, {A,B})
(Y, {A})
(Y, {B})
(Y, {ø})
(X, {A,B})
(X, {A})
(X, {B})
(X, {ø})

Example of the dominances:

(Z,{ø}) ≥ (Y,{ø}) ≥ (X,{ø})
(Z,{A}) ≥ (Y,{A}) ≥ (X,{A})
(Z,{A}) ≥ (Z,{ø})
(Z,{B}) ≥ (Y,{B}) ≥ (X,{B})
(Z,{B}) ≥ (Z,{ø})
(Z,{A,B}) ≥ (Y,{A,B}) ≥ (X,{A,B})
(Z,{A,B}) ≥ (Z,{A})
(Z,{A,B}) ≥ (Z,{B})
(Y,{A}) ≥ (Y,{ø})
(Y,{B}) ≥ (Y,{ø})
(X,{A}) ≥ (X,{ø})
(X,{B}) ≥ (X,{ø})



BLP properties (Rules)

- Ss-property
  - Subject S(n) can WRITE object O(n) iff level of clearance of subject L(S) is less than or equal the level of clearance of the object L(O), that is, L(S) ≤ L(O), and the subject has permission to WRITE the object.

- *-property
  - Subject S(n) can READ object O(n) iff level of clearance of subject L(S) is greater than or equal (dominant) the level of object L(O), that is, L(S) ≥ L(O), and the subject has permission to READ the object.

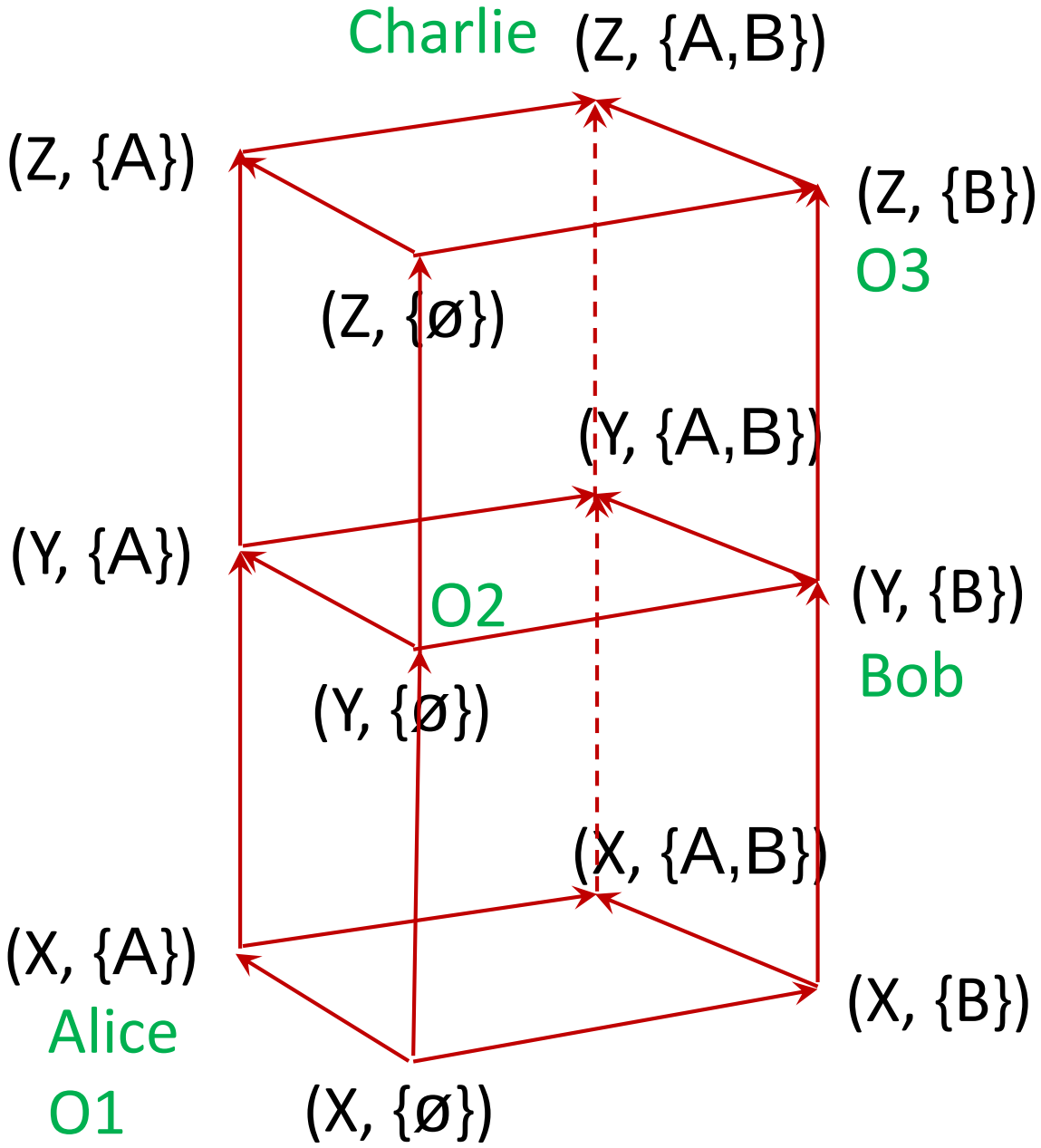
- Discretionary
  - Subject S(n) can discretionarily transfer his/her authorization to Subject at a different clearance level (subject to organization policy).

Subjects and Object at various level of clearance

- For example, we have three subjects Alice, Bob and Charlie and three objects O1, O2 and O3 with the following level of clearance defined:

Subject	Level
Alice	(X,{A})
Bob	(Y,{B})
Charlie	(Z,{A,B})

Object	Level
O1	(X,{A})
O2	(Y,{ø})
O3	(Z,{B})



Subject	Level
Alice	(X,{A})
Bob	(Y,{B})
Charlie	(Z,{A,B})

Object	Level
O1	(X,{A})
O2	(Y,{ø})
O3	(Z,{B})

Access Control Matrix:

	O1	**O2**	**O3**
Alice	R, W	-	-
Bob	-	R	W
Charlie	R	R	R