Exploitation des symétries dynamiques pour la résolution des problèmes SAT

Thèse de doctorat de Sorbonne Université

Hakan METIN

Supervisors:

SOUHEIB BAARIR	Maître de conférences, Université Paris Nanterre
FABRICE KORDON	Professeur, Sorbonne Université

Jury Members:

PASCAL FONTAINE	Maître de conférences, Université de Lorraine
LAURE PETRUCCI	Professeur, Université Paris 13
JEAN-MICHEL COUVREUR	Professeur, Université d'Orléans
EMANUELLE ENCRENAZ	Maître de conférences, Sorbonne Université
SOUHEIB BAARIR	Maître de conférences, Université Paris Nanterre
FABRICE KORDON	Professeur, Sorbonne Université

SCIENCES SORBONNE UNIVERSITÉ

LIP6

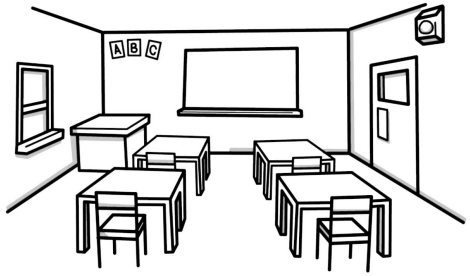
Motivation

SAT is widely used in different domains:

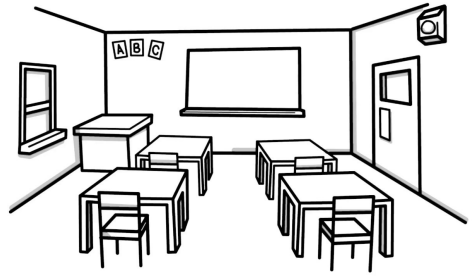
- Artificial intelligence (planning, games, ...)
- Bioinformatics (haplotype inference, ...)
- Security (cryptanalysis, inversion attack on hash function)
- Computationally hard problems (graph coloring, ...)
- Formal Methods (hardware model checking, ...)

Outline

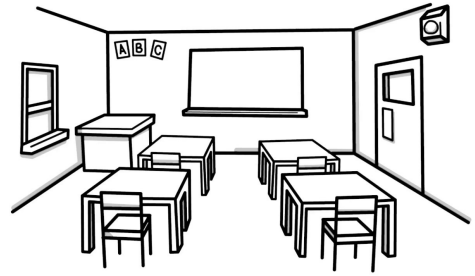
SAT an example



1

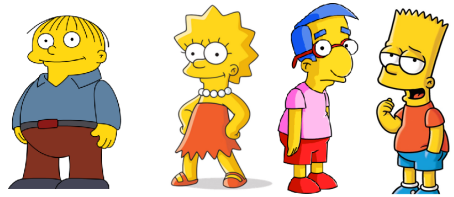


2

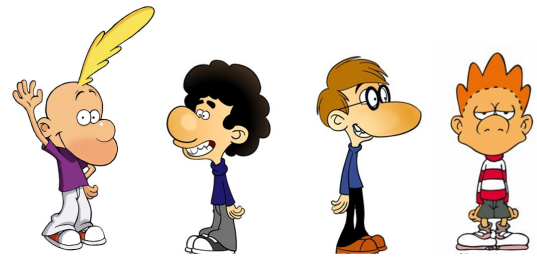


3

A



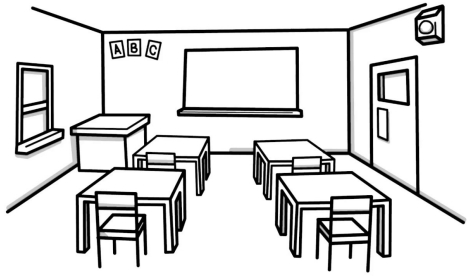
B

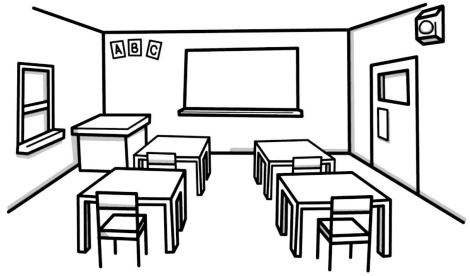


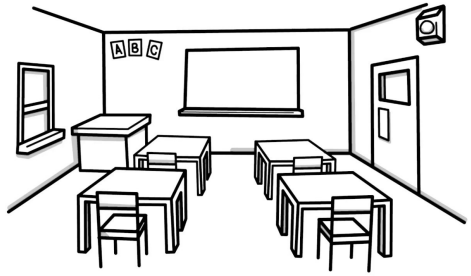
C

Is it possible to attribute each group to a classroom ?

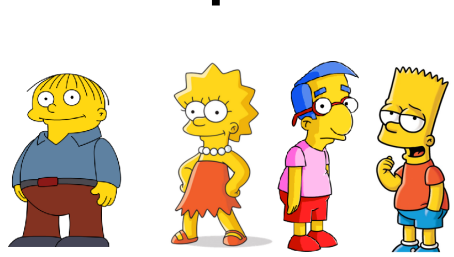
SAT an example

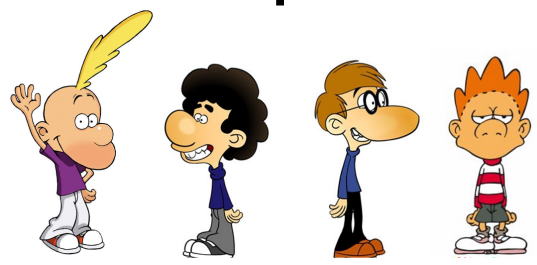






1 2 3



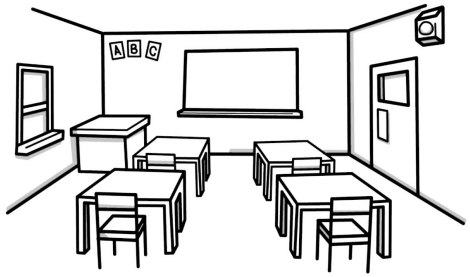
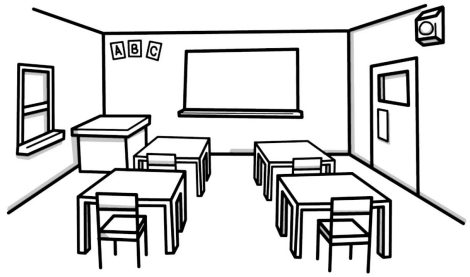
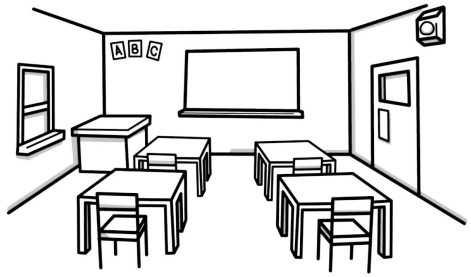


A B C

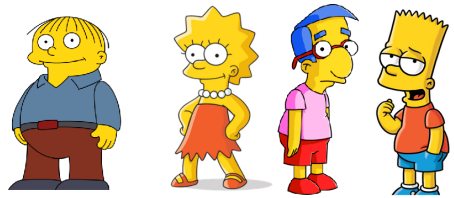
Is it possible to attribute each group to a classroom ?

YES!

SAT an example

1 2 3

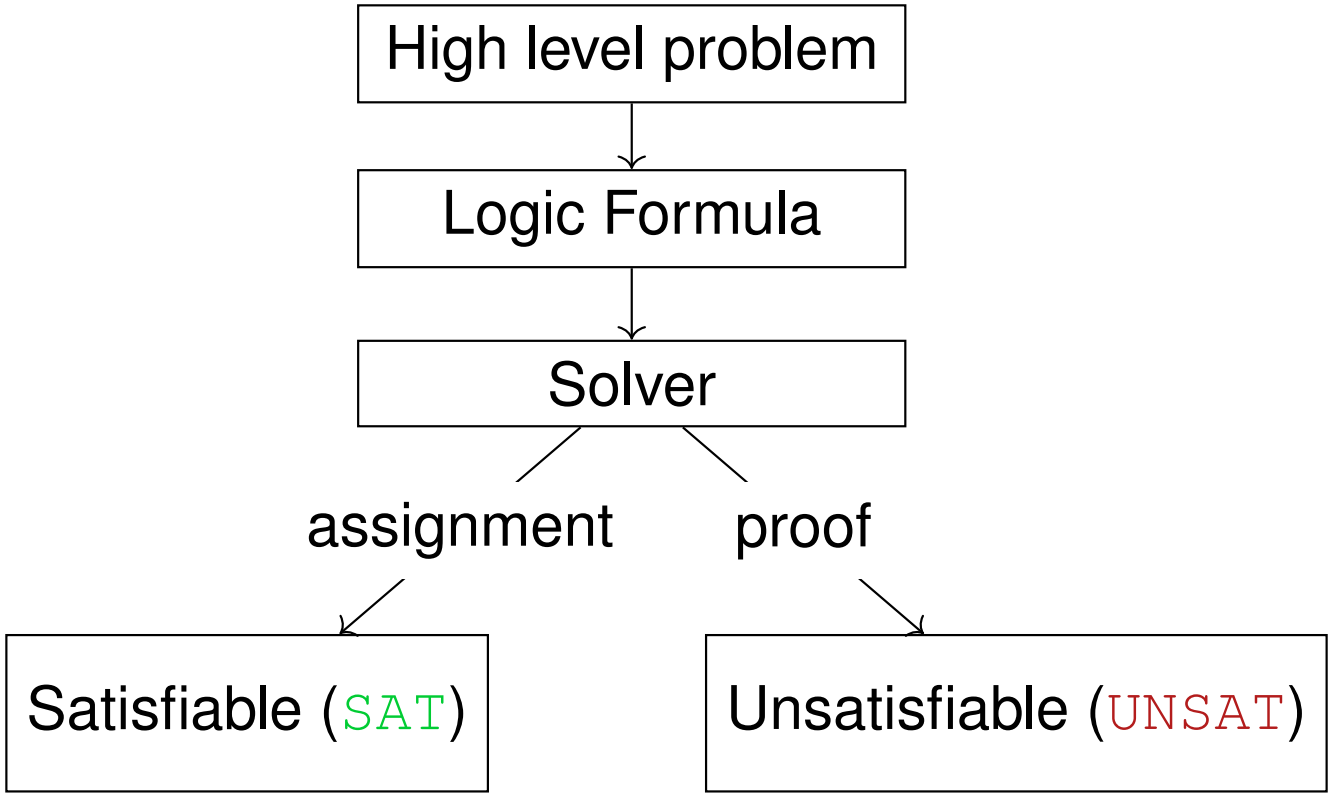




A B C

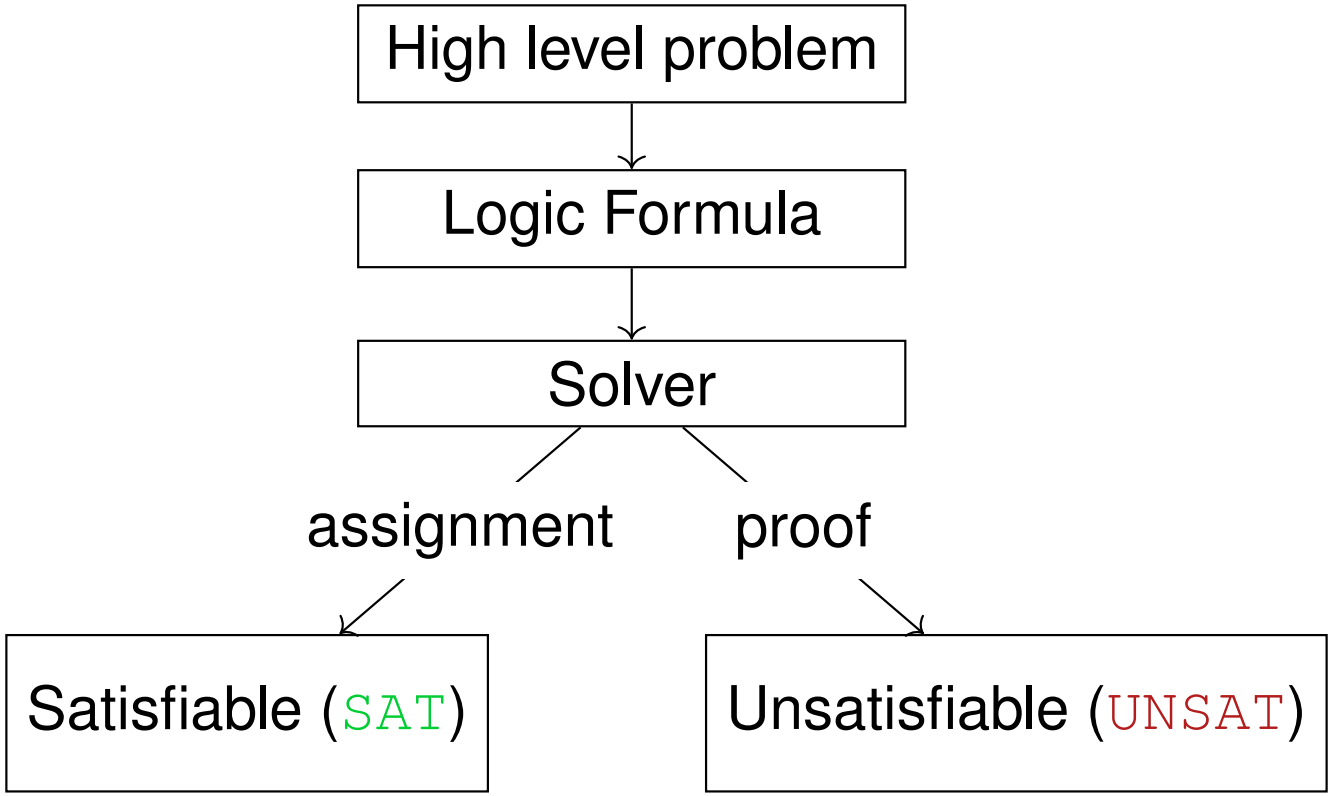
Is it possible to attribute each group to a classroom ?

YES! Many solutions

SAT


High level problem
Logic Formula
Solver
assignment
proof
Satisfiable (SAT)
Unsatisfiable (UNSAT)

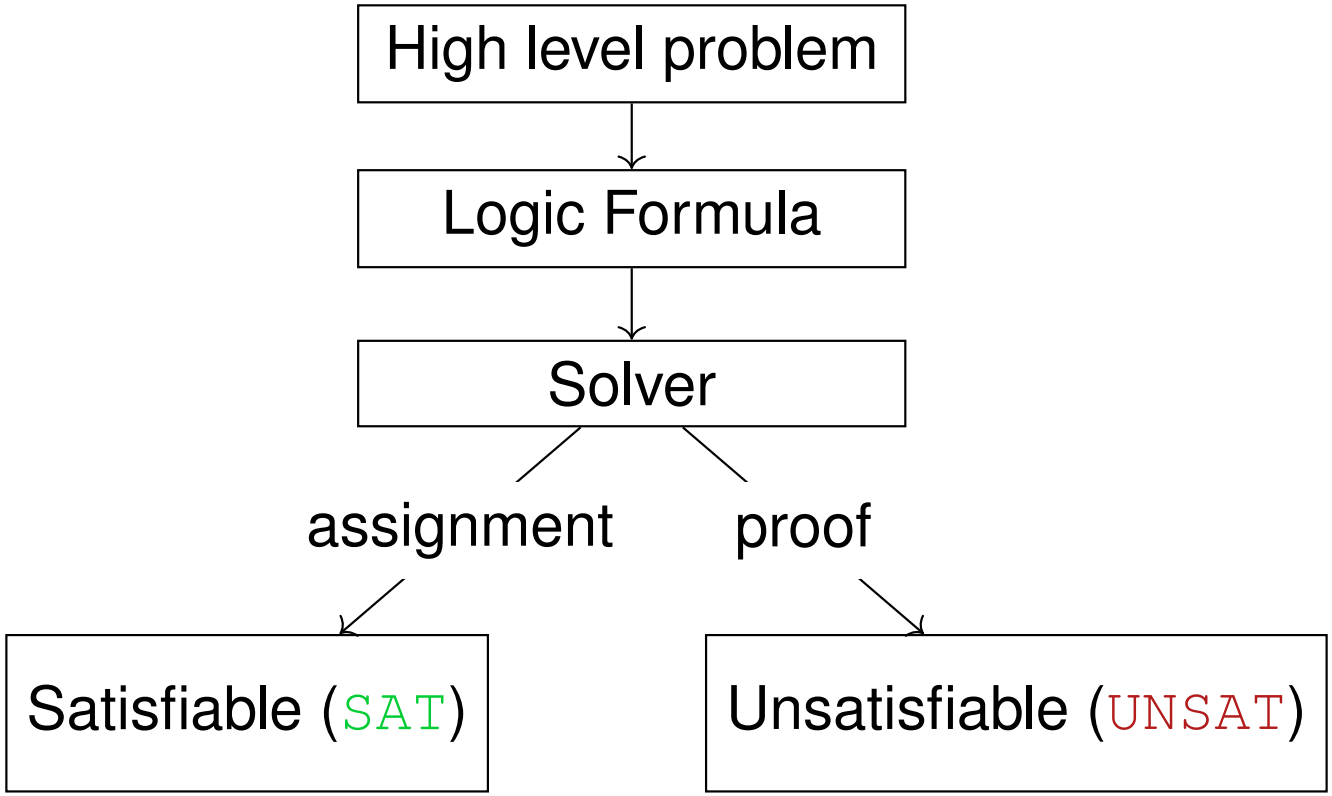
SAT



$$\underbrace{(x_1 \vee x_2 \vee \neg x_3)}$$

Clause with literals $x_1, x_2, \neg x_3$

SAT



$$\overbrace{\underbrace{(x_1 \vee x_2 \vee \neg x_3)}_{\textit{Clause}} \wedge (\neg x_1 \vee \neg x_2) \wedge (x_2 \vee \neg x_4)}^{\text{Formula (CNF)}}$$

Computing symmetries of a SAT problem

CNF formula

$$(x_1 \vee x_2 \vee x_3) \wedge (x_4 \vee x_5 \vee x_6) \wedge (x_7 \vee x_8 \vee x_9)$$
$$\wedge(\neg x_1 \vee \neg x_4) \wedge (\neg x_1 \vee \neg x_7) \wedge (\neg x_4 \vee \neg x_7)$$
$$\wedge(\neg x_2 \vee \neg x_5) \wedge (\neg x_2 \vee \neg x_8) \wedge (\neg x_5 \vee \neg x_8)$$
$$\wedge(\neg x_3 \vee \neg x_6) \wedge (\neg x_3 \vee \neg x_9) \wedge (\neg x_6 \vee \neg x_9)$$

[1] http://www.tcs.hut.fi/Software/bliss/

[2] http://vlsicad.eecs.umich.edu/BK/SAUCY/

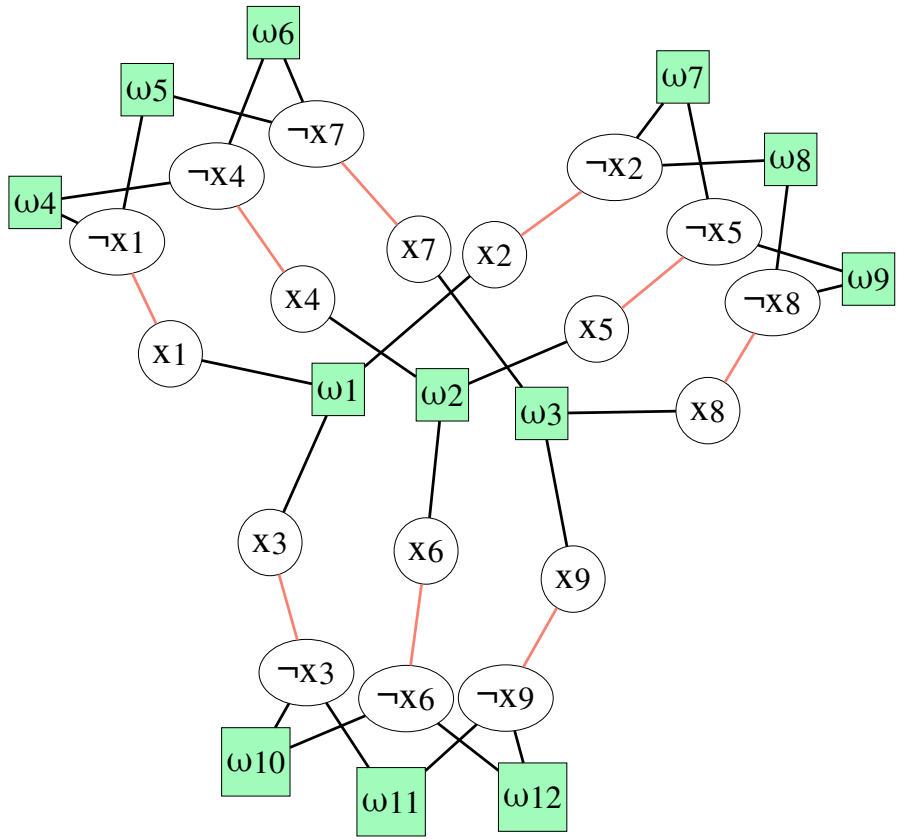
Computing symmetries of a SAT problem

CNF formula

$$(x_1 \vee x_2 \vee x_3) \wedge (x_4 \vee x_5 \vee x_6) \wedge (x_7 \vee x_8 \vee x_9)$$
$$\wedge(\neg x_1 \vee \neg x_4) \wedge (\neg x_1 \vee \neg x_7) \wedge (\neg x_4 \vee \neg x_7)$$
$$\wedge(\neg x_2 \vee \neg x_5) \wedge (\neg x_2 \vee \neg x_8) \wedge (\neg x_5 \vee \neg x_8)$$
$$\wedge(\neg x_3 \vee \neg x_6) \wedge (\neg x_3 \vee \neg x_9) \wedge (\neg x_6 \vee \neg x_9)$$

$\Downarrow$ $\Downarrow$

colored graph



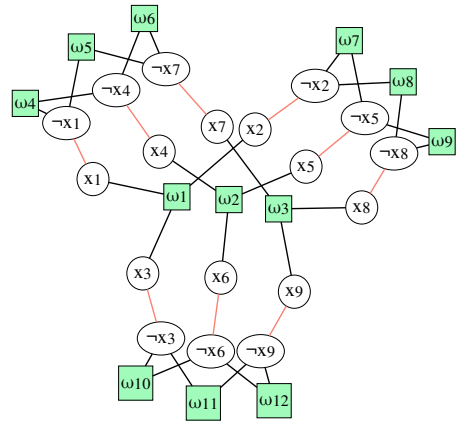
Computing symmetries of a SAT problem

CNF formula

$$(x_1 \vee x_2 \vee x_3) \wedge (x_4 \vee x_5 \vee x_6) \wedge (x_7 \vee x_8 \vee x_9)$$
$$\wedge(\neg x_1 \vee \neg x_4) \wedge (\neg x_1 \vee \neg x_7) \wedge (\neg x_4 \vee \neg x_7)$$
$$\wedge(\neg x_2 \vee \neg x_5) \wedge (\neg x_2 \vee \neg x_8) \wedge (\neg x_5 \vee \neg x_8)$$
$$\wedge(\neg x_3 \vee \neg x_6) \wedge (\neg x_3 \vee \neg x_9) \wedge (\neg x_6 \vee \neg x_9)$$

$\Downarrow$ $\Downarrow$

colored graph



$\|$ $\|$

graph automorphism (`bliss` [1] or `saucy` [2])

[1] http://www.tcs.hut.fi/Software/bliss/

[2] http://vlsicad.eecs.umich.edu/BK/SAUCY/

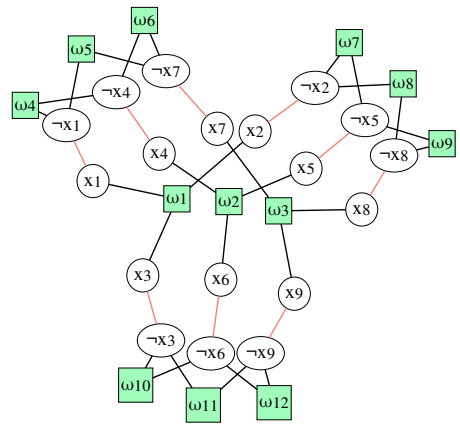
Computing symmetries of a SAT problem

CNF formula

$$(x_1 \vee x_2 \vee x_3) \wedge (x_4 \vee x_5 \vee x_6) \wedge (x_7 \vee x_8 \vee x_9)$$
$$\wedge(\neg x_1 \vee \neg x_4) \wedge (\neg x_1 \vee \neg x_7) \wedge (\neg x_4 \vee \neg x_7)$$
$$\wedge(\neg x_2 \vee \neg x_5) \wedge (\neg x_2 \vee \neg x_8) \wedge (\neg x_5 \vee \neg x_8)$$
$$\wedge(\neg x_3 \vee \neg x_6) \wedge (\neg x_3 \vee \neg x_9) \wedge (\neg x_6 \vee \neg x_9)$$

$\Downarrow$ $\qquad$ $\Downarrow$

colored graph



$\Vert$ $\qquad$ $\Vert$

graph automorphism $\qquad$ (`bliss` [1] or `saucy` [2])

$\Downarrow$ $\qquad$ $\Downarrow$

set of symmetries

$$g_1 = (x_2\ \ x_3)(x_5\ \ x_6)(x_8\ \ x_9)$$
$$g_2 = (x_4\ \ x_7)(x_5\ \ x_8)(x_6\ \ x_9)$$
$$g_3 = (x_1\ \ x_2)(x_4\ \ x_5)(x_7\ \ x_8)$$
$$g_4 = (x_1\ \ x_4)(x_2\ \ x_5)(x_3\ \ x_6)$$

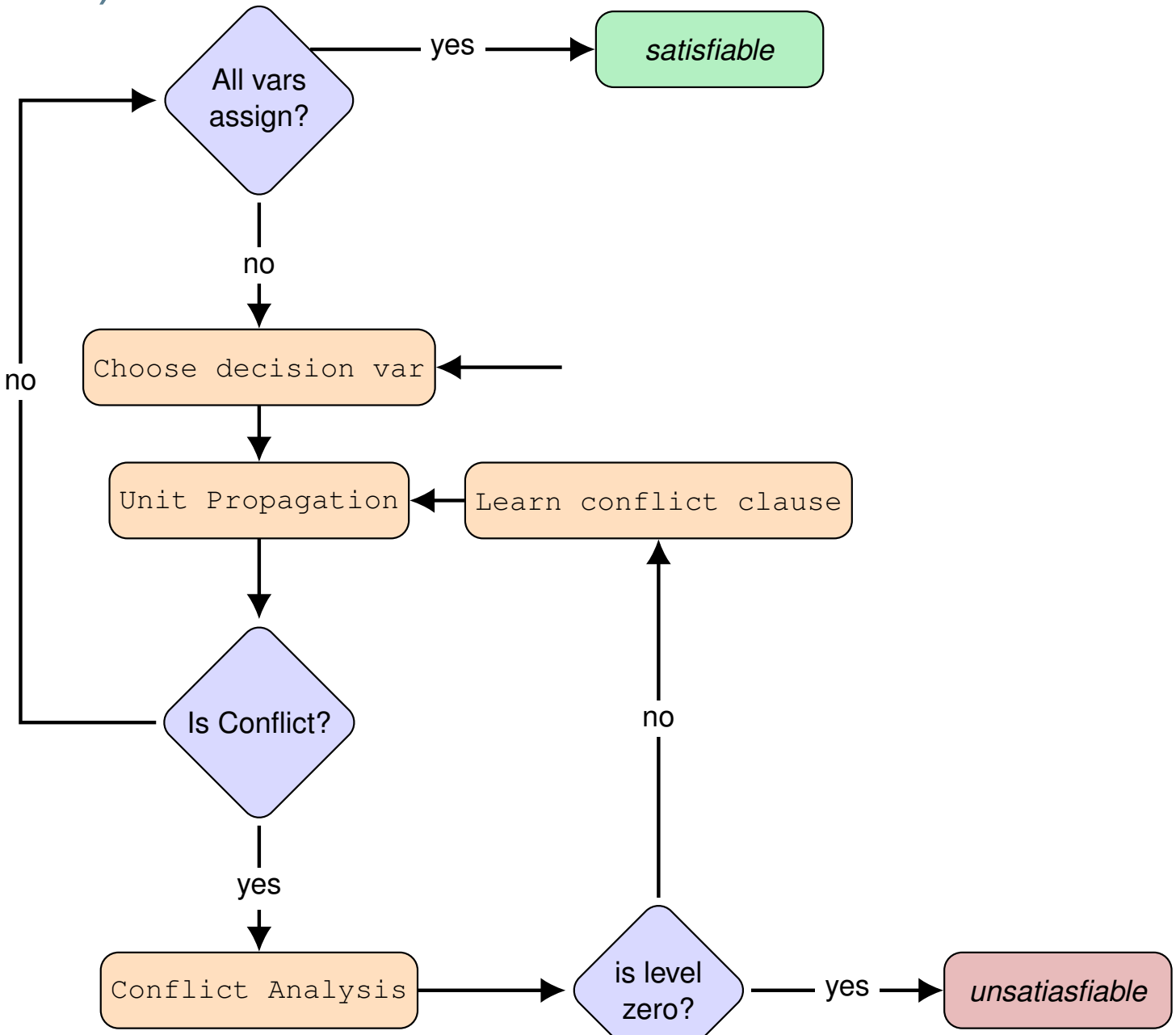
[1] http://www.tcs.hut.fi/Software/bliss/

[2] http://vlsicad.eecs.umich.edu/BK/SAUCY/

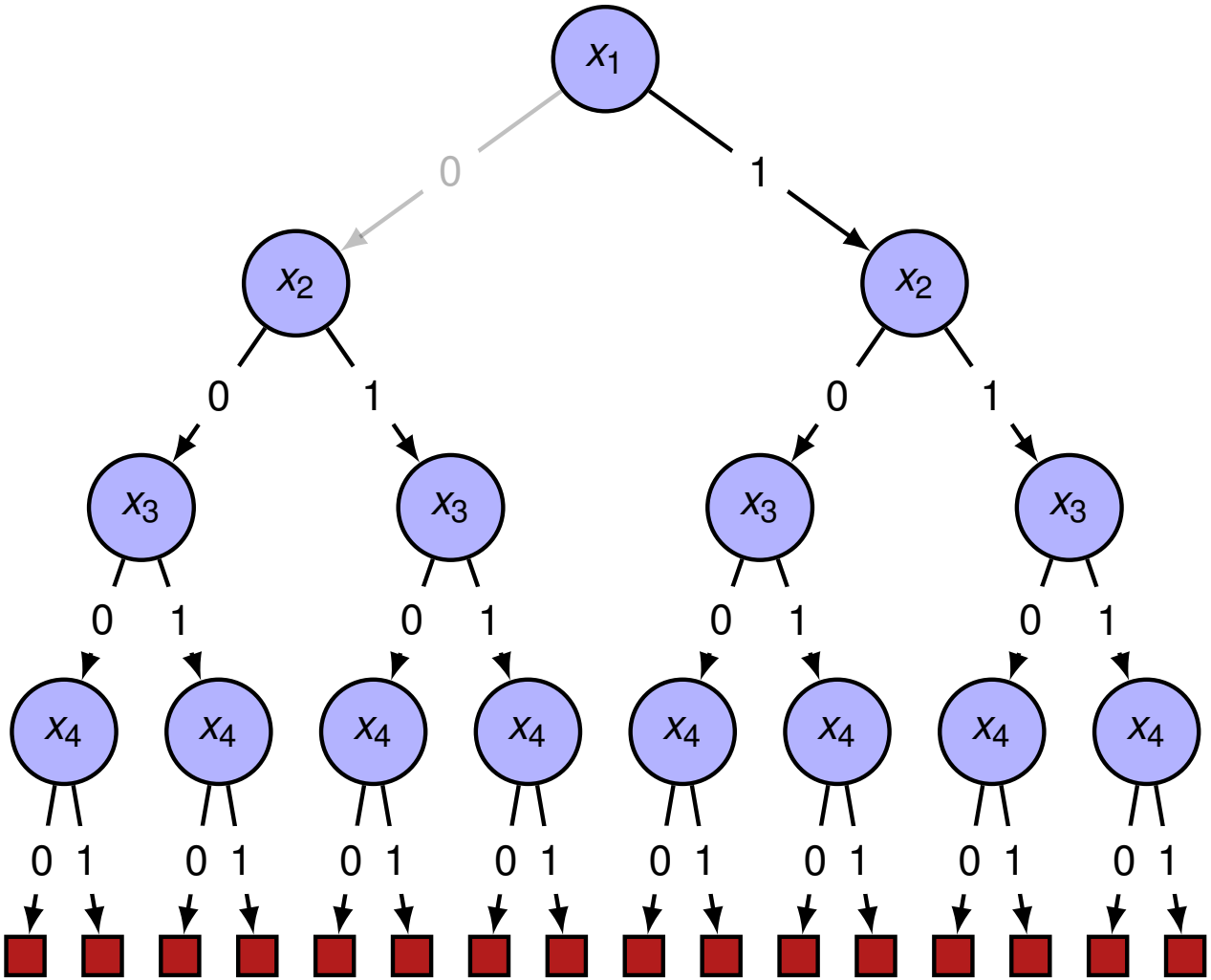
SAT

example solving arbre

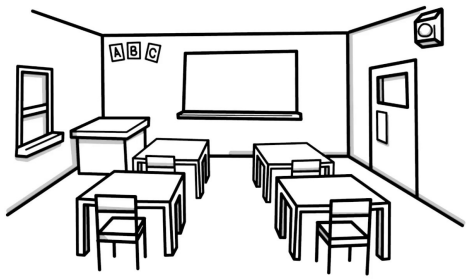
Conflict Driven Clause Learning Algorithm (CDCL)



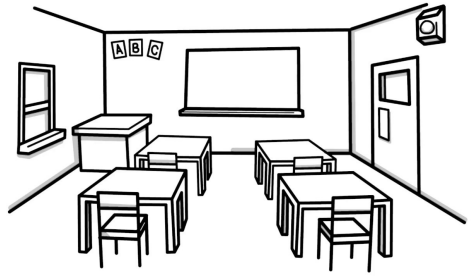
Tree


x_1
0
1
x_2
x_2
0
1
0
1
x_3
x_3
x_3
x_3
0 1
0 1
0 1
0 1
x_4 x_4 x_4 x_4 x_4 x_4 x_4 x_4
0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1

SAT an example 2

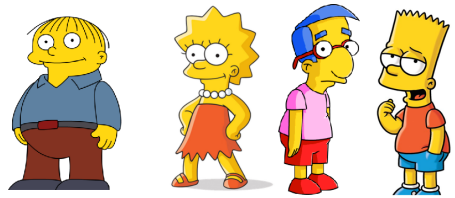


1

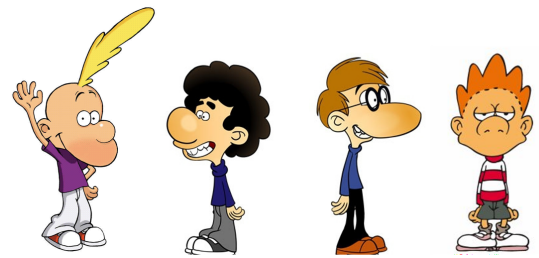


2

A



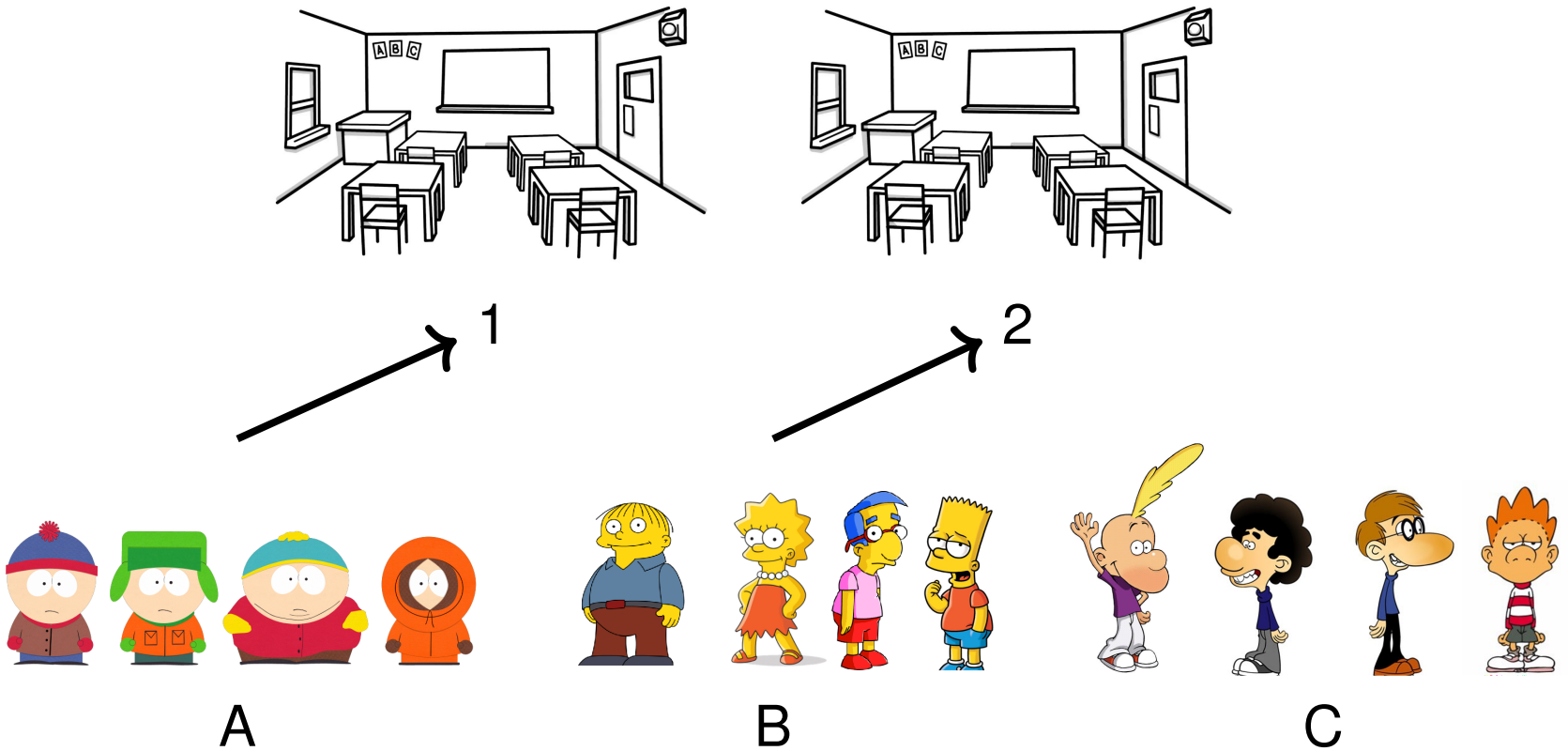
B



C

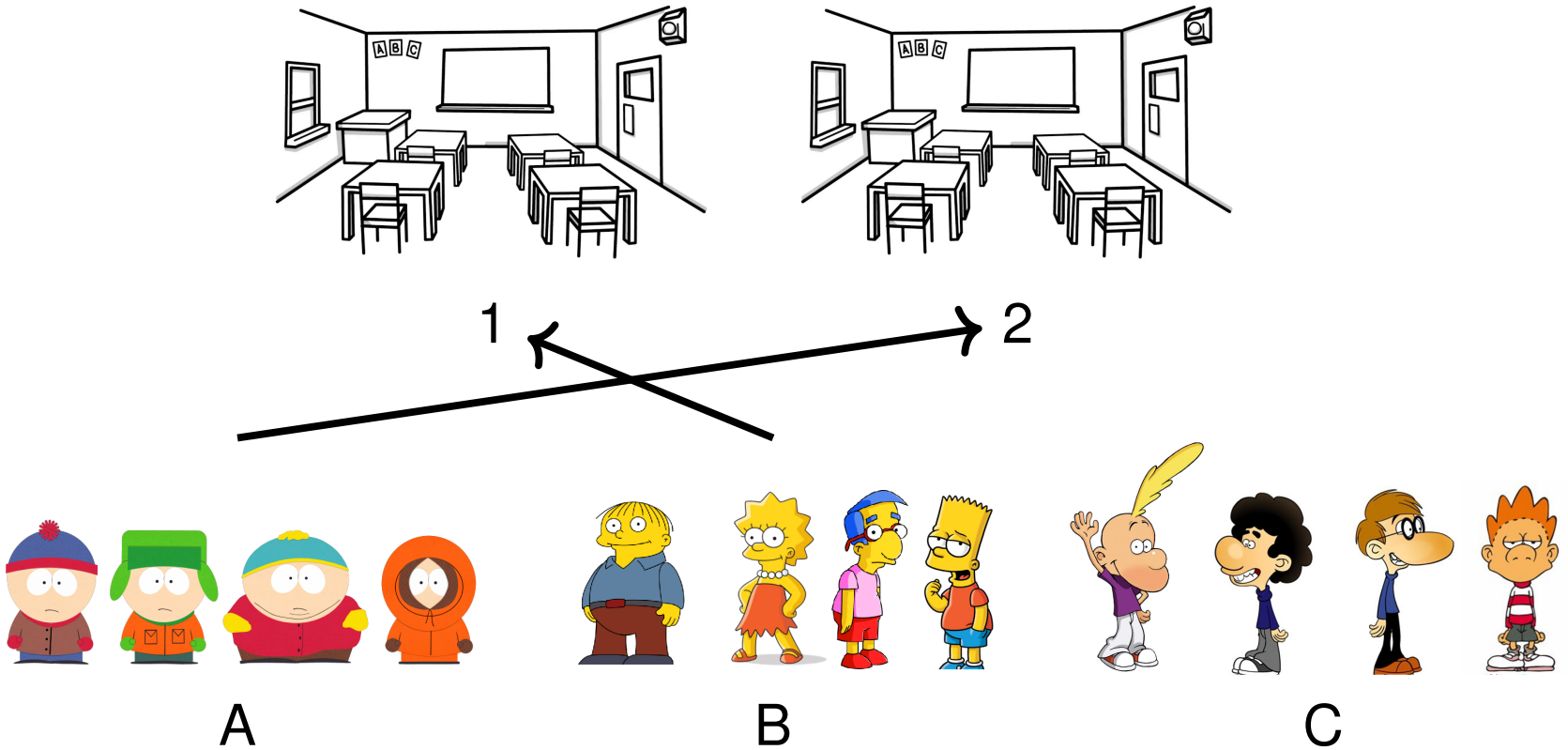
Attribute each group to a class room

SAT an example 2



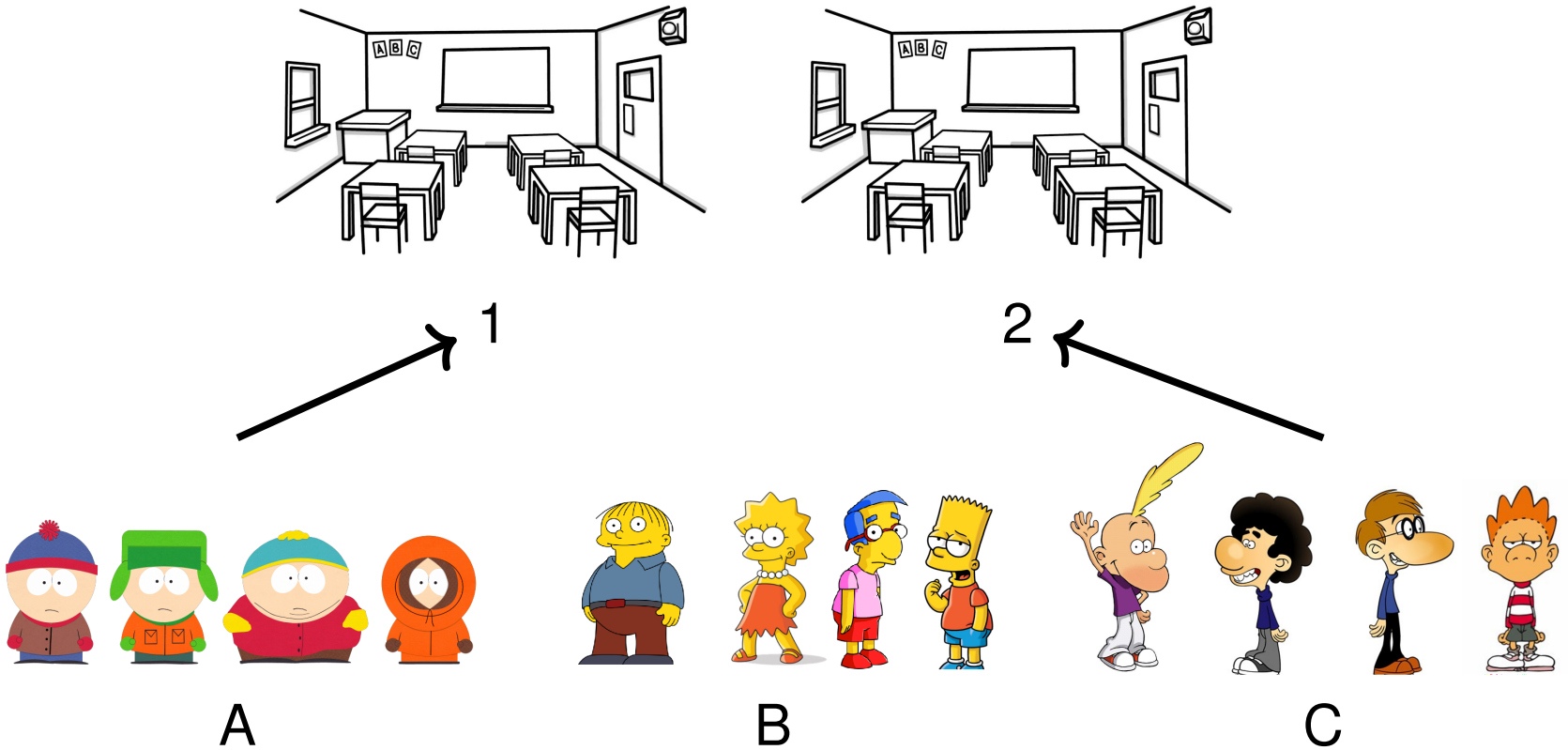
Attribute each group to a class room

SAT an example 2



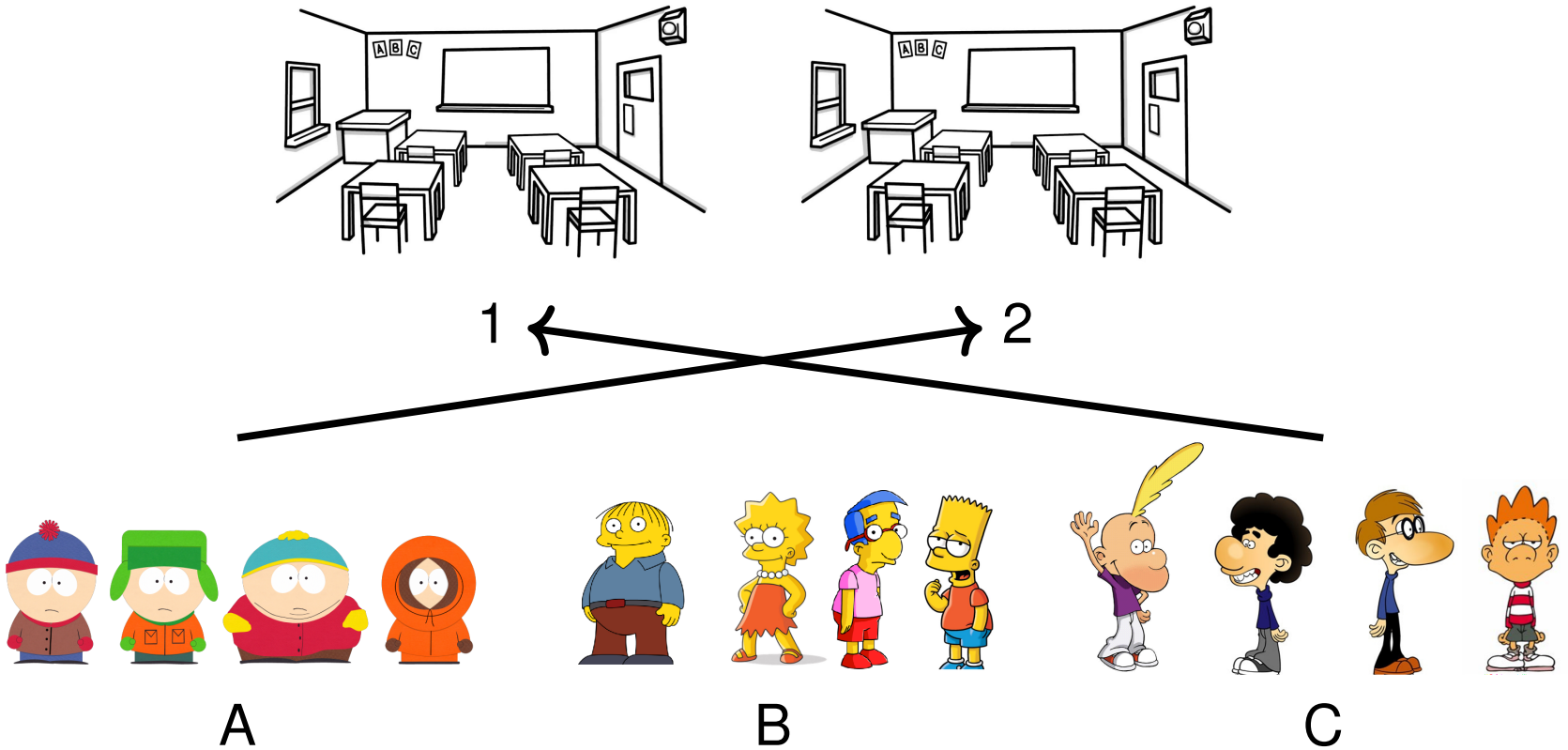
Attribute each group to a class room

SAT an example 2



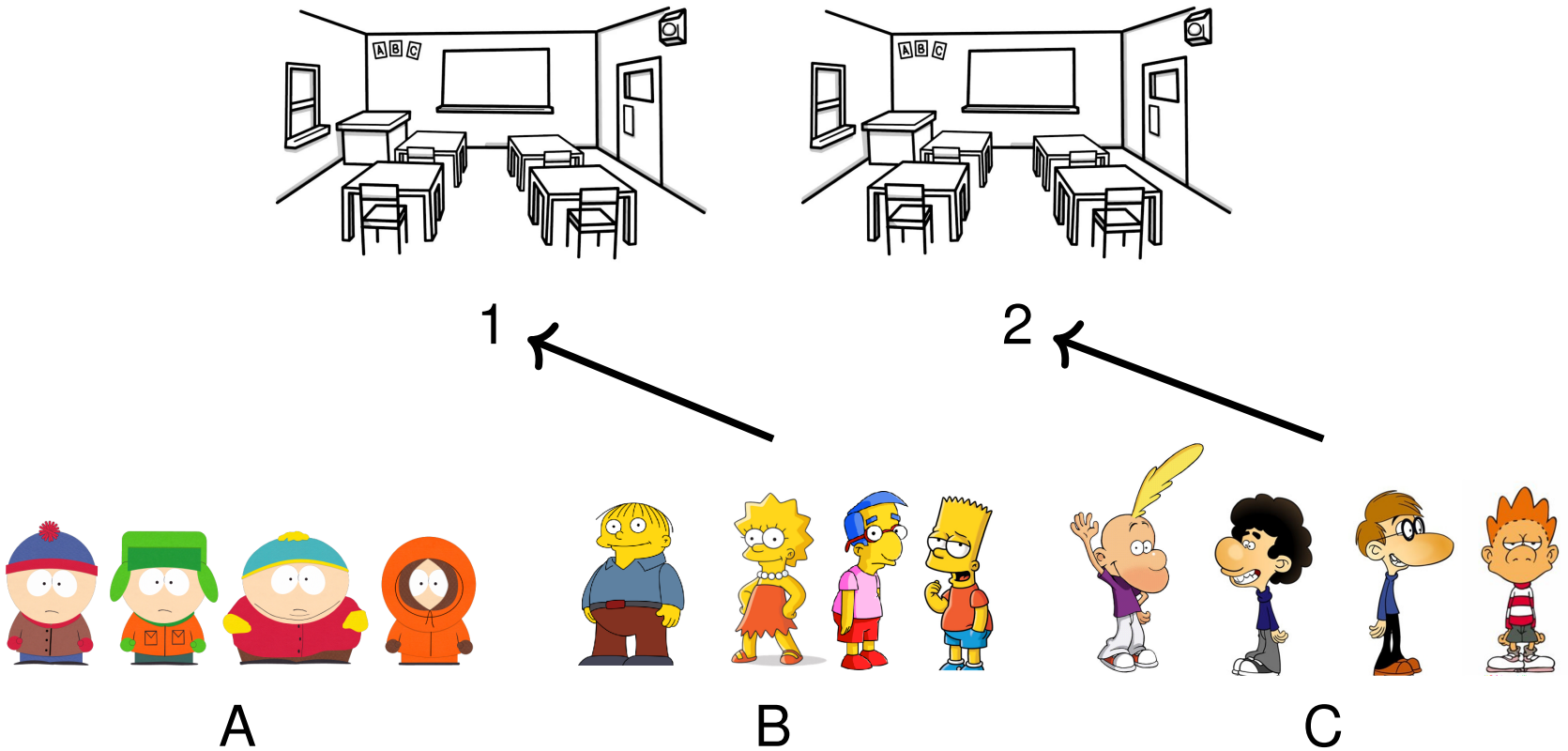
Attribute each group to a class room

SAT an example 2



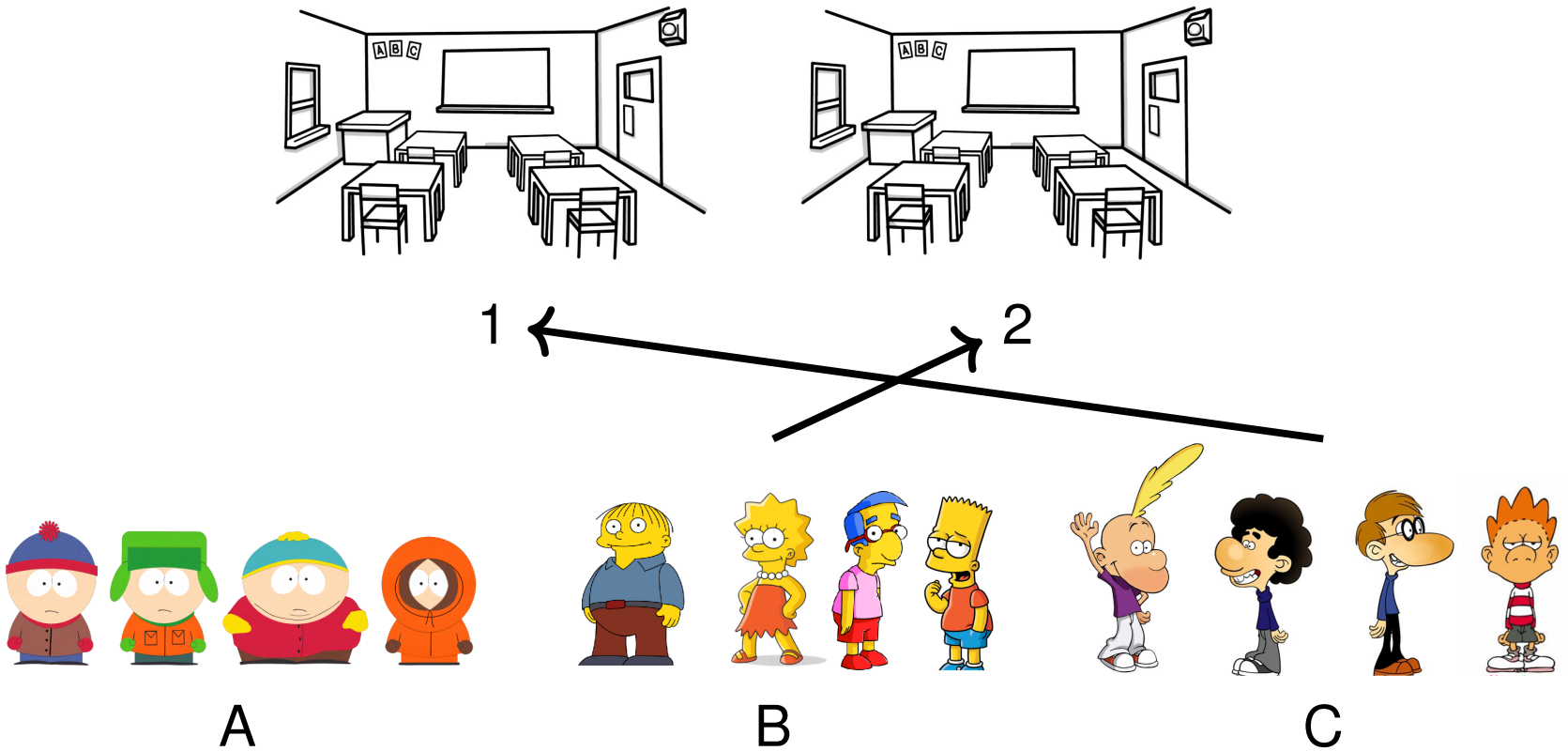
Attribute each group to a class room

SAT an example 2



Attribute each group to a class room

SAT an example 2



Attribute each group to a class room