Model Checking with BDDs
Sets as Propositions

- Consider the universe “ABCD”

\[
[(\text{'A'}, [\sim p_2, \sim p_1]), (\text{'B'}, [\sim p_2, p_1])
, (\text{'C'}, [p_2, \sim p_1]), (\text{'D'}, [p_2, p_1])]
\]

- Or the universe [1,5,6,79,13]

\[
[(1, [\sim p_3, \sim p_2, \sim p_1]), (5, [\sim p_3, \sim p_2, p_1])
, (6, [\sim p_3, p_2, \sim p_1]), (79, [\sim p_3, p_2, p_1])
, (13, [p_3, \sim p_2, \sim p_1])]
\]
Consider some subsets

subset "ABCD" "A"
~p1 \~p2

subset "ABCD" "AC"
(~p1 \~p2) (\~p1 \ p2)

subset "ABCD" "ACDB"
(~p1 \~p2) (p1 \~p2) (~p1 \ p2)
\ (p1 \ p2)

subset "ABCD" ""
Absurd
And their BDDs

- Set “ABCD” ""
- Absurd
\[
[(\text{a}', [\sim \text{p2}, \sim \text{p1}]), (\text{b}', [\sim \text{p2}, \text{p1}]), \\
(\text{c}', [\text{p2}, \sim \text{p1}]), (\text{d}', [\text{p2}, \text{p1}])]
\]

\text{subset "abcd" "a"}

\sim \text{p1} \lor \sim \text{p2}
subset "abcd" "ad"

\[(\sim p1 \land \sim p2) \lor (p1 \land p2)\]
subset "abcd" "adbc"

\[\begin{align*}
('a', [\sim p2, \sim p1]), ('b', [\sim p2, p1]), \\
('c', [p2, \sim p1]), ('d', [p2, p1])
\end{align*}\]
initial xs = zip xs (reverse (g 1))
   where n = numbits (length xs)
   g:: Int -> [[[Prop Int]]
   g m | m > n = [[[]]]
   g n = map (LetterP n:) ys ++ map ((NotP (LetterP n)):) ys
      where ys = (g (n+1))
subset univ set = foldr acc AbsurdP univ
   where acc x prop | elem x set = orOpt (get x) prop
                 acc x prop = prop
mapping = initial univ
get n = case lookup n mapping of
    Just literals -> andL literals
Membership test

• Represent an element of a set as the singleton subset

• \texttt{item univ x = subset univ [x]}

• Then membership uses the tautology
• \{x\} `elem` zs \iff \{x\} == \{x\} \cap zs
Lift to BDDs

\[
\text{subsetB } x \ y = \text{p2b} (\text{subset } x \ y) \\
\text{itemB } x \ y = \text{p2b} (\text{item } x \ y)
\]

\[
\text{mem univ } x \ xs = \text{same temp} (\text{conj temp (subsetB univ xs)})
\]
\[
\text{where temp } = (\text{itemB univ x} )
\]
A relation between two items in a set

\[
\left[
  (\text{'a'}, \left[\sim p_2, \sim p_1\right]),
  (\text{'b'}, \left[\sim p_2, p_1\right]),
  (\text{'c'}, \left[p_2, \sim p_1\right]),
  (\text{'d'}, \left[p_2, p_1\right])
\right]
\]

- \(R(\text{a}, \text{b}) = \text{True}\)
- \(R(\text{b}, \text{c}) = \text{True}\)
- \(R(\text{c}, \text{c}) = \text{True}\)
- \(R(\_\_\_, \_\_\_) = \text{False}\)
Graph transitions

• Consider the graph and its assignment of states to boolean formula
Recall how we represent subsets

- \( u_1 = [0, 1, 2, 3] \)
- \( \text{sub1} = \text{subset } u_1 \ [0] \)
- \( \neg p_0 \land \neg p_1 \)
Subset \{s2,s3\}

- \( u_1 = [0,1,2,3] \)
- \( \text{sub2} = \text{subset } u_1 [2,3] \)
- \( (p_0 \land \neg p_1) \lor (p_0 \land p_1) \)
Subset \( \{s_3\} \)

- \( u_1 = [0,1,2,3] \)
- \( \text{sub}_3 = \text{subset} \ u_1 \ [3] \)
- \( p_0 \land p_1 \)
Subset \{s_1, s_2, s_3\}

- \(u_1 = [0, 1, 2, 3]\)
- \(\text{sub4} = \text{subset } u_1 \ [1, 2, 3]\)
- \((\neg p_0 \land p_1) \lor (p_0 \land \neg p_1) \lor (p_0 \land p_1)\)
• Introduce new variables $p_2$ and $p_3$ that mirror $p_0$ and $p_1$

$$prop_1 =$$

\[
(\neg p_0 \land \neg p_1 \land \neg p_2 \land p_3) \\
\lor \\
(\neg p_0 \land \neg p_1 \land p_2 \land \neg p_3) \\
\lor \\
(\neg p_0 \land p_1 \land \neg p_2 \land \neg p_3) \\
\lor \\
(\neg p_0 \land p_1 \land p_2 \land \neg p_3) \\
\lor \\
p_0 \land \neg p_1 \land p_2 \\
\lor \\
(\neg p_0 \land p_1 \land p_2) \\
\lor \\
p_0 \land p_1 \land p_2
\]
As a BDD
States reachable in one step

• Let sub be a set of states
• What is reachable in one step?

• step set = prop1 ∩ set
To take a step
conjoin

• sub1={s0}  prop1  sub1 \And prop1

0

1

2

3

0

1

2

3

0

1

2

3

T

F

T

F

T

F

T

F

T

F

T

F

T

F

T

F

T

F

T

F
• Note the paths to True
• There are two of them
• Each corresponds to one next state
• The values of p2 and p3 tell what states \{s1, s2\}
Consider the solutions

- $\[(0,\text{False}),(1,\text{False}),(2,\text{False}),(3,\text{True})],$
- $\[(0,\text{False}),(1,\text{False}),(2,\text{True}),(3,\text{False})]\$

By throwing away the assignments to $p_0$ and $p_1$, and be renaming $p_2$ to $p_0$, and $p_3$ to $p_1$, we get to solutions

- $\neg p_0 \land p_1$
- $p_0 \land \neg p_1$

Coresponding to the states

- $\{s_1,s_2\}$
Start at the set \{s2,s3\}

- \([(0,\text{True}),(1,\text{False}),(2,\text{True}),(3,\text{False})]\)
- \([(0,\text{True}),(1,\text{True}),(2,\text{True}),(3,\text{True})]\)
- \(p0 \land \neg p1\)
- \(p0 \land p1\)
Start at the subset \{s1,s2,s3\}

- \sim p0 \land \sim p1
- p0
- p0 \land \sim p1
- p0 \land p1
\[ p_0 \lor (p_0 \land p_1) \lor (p_0 \land \neg p_1) \lor (\neg p_0 \land \neg p_1) \]

- This corresponds to the BDD
- Which is every state except \( s_2 \), which is exactly what can be reached from \( \{s_1, s_2, s_3\} \)
To take multiple steps

• Compute the states reachable in 1 step
• Union in the starting states
• And repeat
• sub1 = \{s0\}
• *LectureBDD> pnG (p2b sub1)
• *LectureBDD> pnG (p2b (step sub1))
• *LectureBDD> pnG (p2b (step (step sub1)))
• *LectureBDD> pnG (p2b (step (step (step sub1))))
• \( \text{sub3} = \{s3\} \)
• \( \text{LectureBDD} > \text{pnG} \ (p2b \ \text{sub3}) \)
• \( \text{LectureBDD} > \text{pnG} \ (p2b \ (\text{step sub3})) \)