CSC410 Tutorial #10

Model Checking in Action

Today

- Using Model Checkers
  - Promela language
  - Verifying a cryptographic protocol (SPIN)
  - Puzzle-solving (NuSMV)

- Review Checklist for Exam #2
- Office Hours (A4, Temporal Logic/Model Checking)

There will be additional office hours next Tue/Wed (4-5 in classroom)

SPIN and Promela

SPIN (https://spinroot.com/spin/whatispin.html) is a well-known model checker – originally developed in the 1980s!

Supports exhaustive verification of asynchronous processes

Explicit state model checker: generates state space, then searches

Input language: ProMeLa (Process MetaLanguage)

Verifying a Cryptographic Protocol

Alice and Bob want to communicate over an unsecure channel and arrive to some common (secret) knowledge

Meaning: They want to both have the pair (NA,NB) of numbers, such that no eavesdropper could also (NA,NB).

They have public keys (PuA, PuB) and private keys (PrA, PrB).

Verifying a Cryptographic Protocol

Needham-Schroeder Protocol

Alice initiates conversation with Bob.

Alice chooses NA at random, encrypts with PuB, and sends it to Bob.

Message includes “I am Alice”

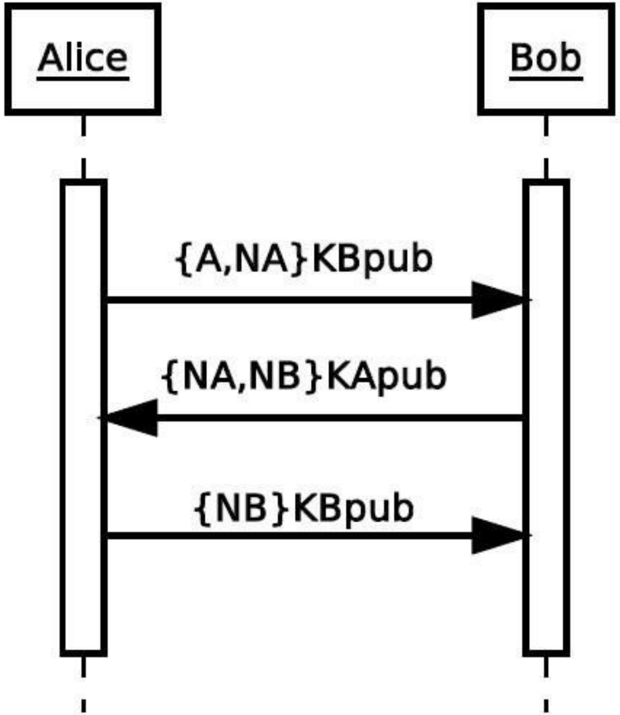
Bob receives the data and decrypts with PrB, yielding NA.

Bob chooses NB at random, encrypts with PuA, and sends it to Alice.

Alice receives the data and decrypts with PrA, yielding NB.

Alice and Bob – and *only* Alice and Bob – will have the pair (NA,NB)

Alice encrypts NB with PuB, and sends back to Bob so he knows secret is safe.



Verifying a Cryptographic Protocol

Add an *Intruder*, who can do the same as Bob:

- Can initiate protocol with Alice
- Can be sent messages from Alice (encrypted with Intruder’s public key)
- Can send messages to Alice and Bob.

Can the intruder learn (NA,NB)?

(Demo)

Explaining the Counterexample - Man-in-the-middle

Alice initiates conversation with Intruder, sends NA encrypted w/ Intruders' pubkey

Intruder gets NA and sends alongside "I am Alice" to Bob, encrypted with PuB.

Bob gets NA, and believes he is talking to Alice.

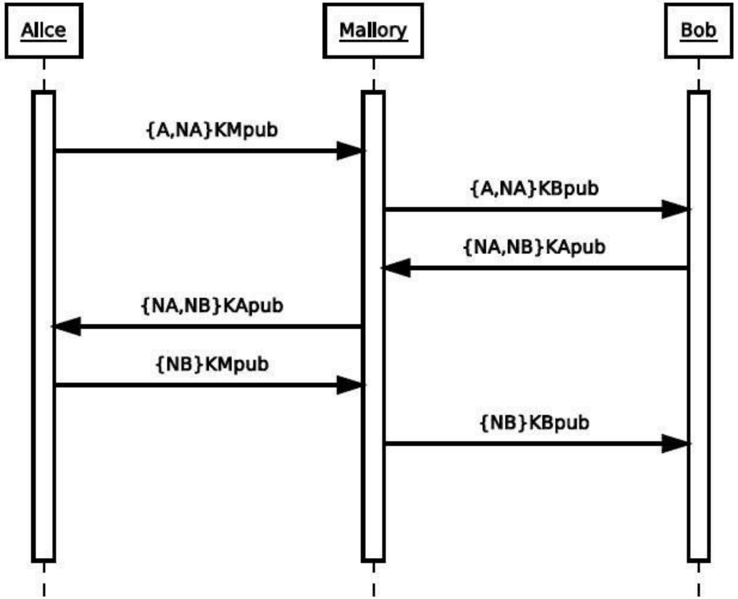
Bob sends Intruder NB encrypted with Alice's' public key.

Intruder sends (encrypted) NB to Alice, who thinks it is Intruder's secret.

Alice gets NB.

Alice sends NB, encrypted with Intruder's public key as confirmation

Intruder now decrypts NB, and have both NA and NB



Problem Solving with Model Checking

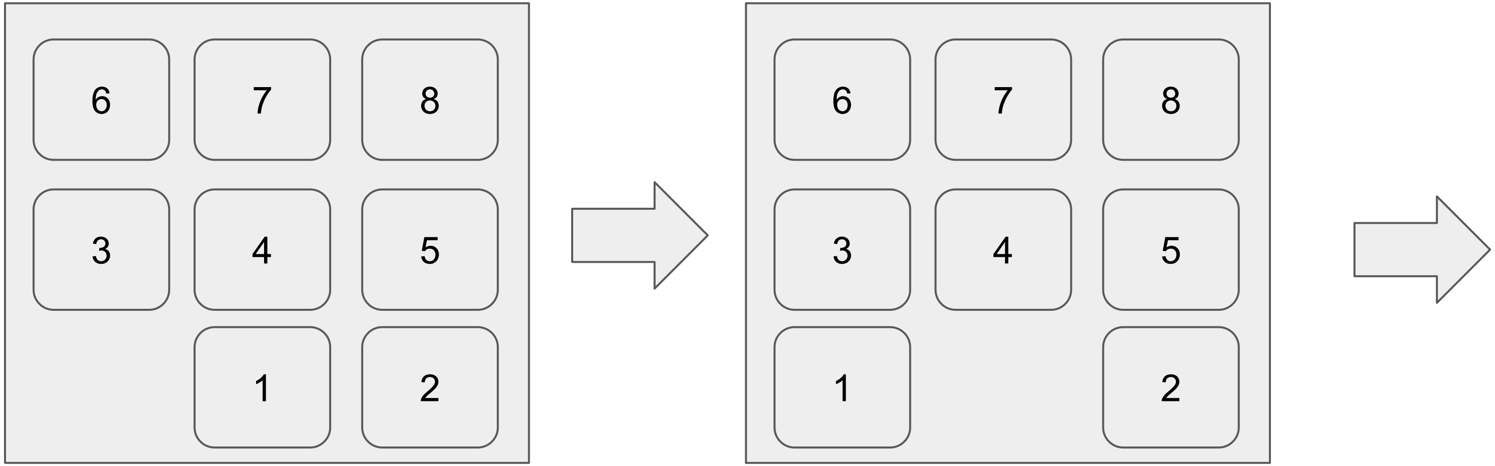
Typically model-checking workflow:

1) Define a model
2) Define a desirable property (safety, liveness)
3) Use model checker to verify that the property holds.
    a) Counterexample ⇒ bad!

However, like any reachability technique, model-checking can be used for *problem-solving*.

1) Define a problem
2) *Deny* the existence of a solution
3) Let the model-checker prove you wrong!
    a) Counterexample ⇒ good!

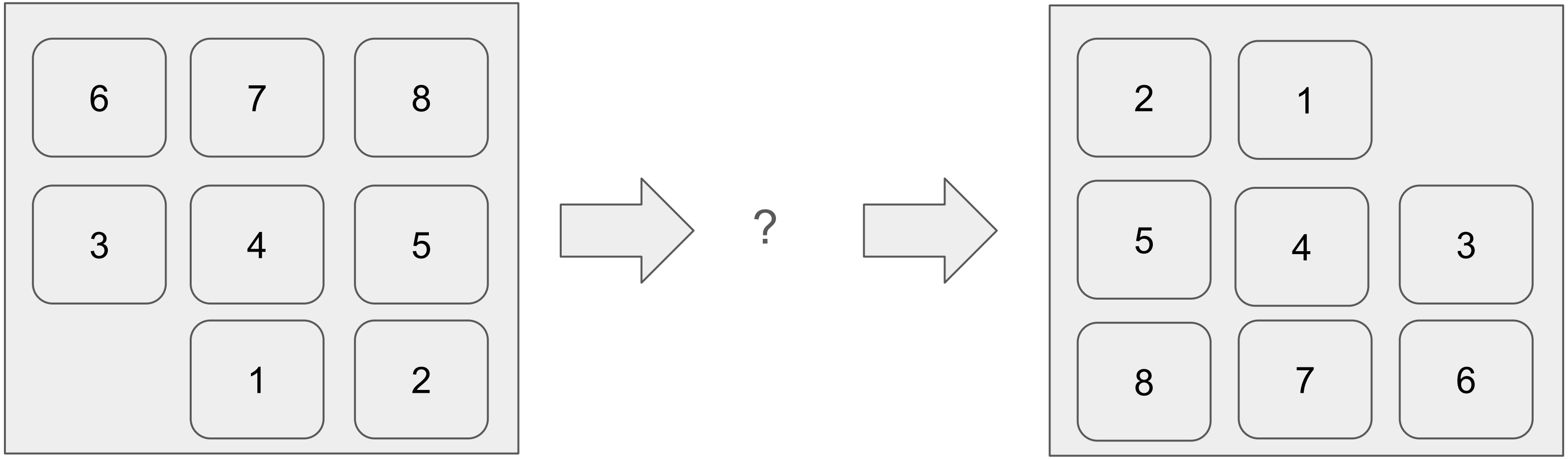
Example: 9-tile puzzle



6	7	8
3	4	5
	1	2

6	7	8
3	4	5
1		2

Example: 9-tile puzzle



6	7	8
3	4	5
	1	2

?

2	1	
5	4	3
8	7	6

Model Checking with NuSMV

NuSMV (https://nusmv.fbk.eu/)

A symbolic model checker

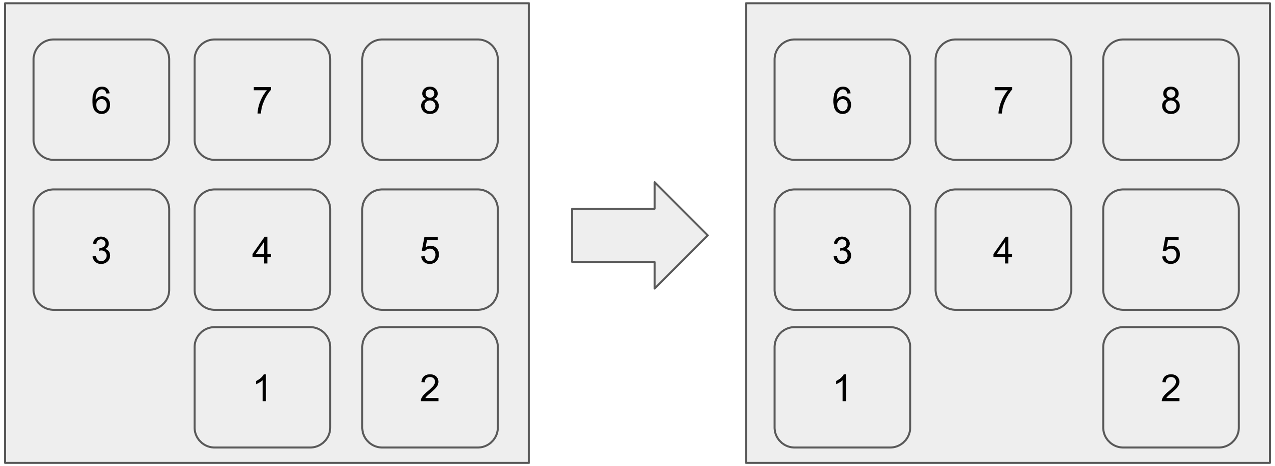
(uses symbolic encoding rather than explicit states)

Different (but similar) specification/modelling language

Solving the 9-tile puzzle

What is the state space? How big?

What are the transitions?



6	7	8
3	4	5
	1	2

6	7	8
3	4	5
1		2

(Demo)

Wrap-up:

What to review before the Exam #2

(Not everything will be tested; but if you are familiar with all of these, you will not face any surprises)

Decision Procedures

What is a decision procedure?

Basic concepts: satisfiability, validity soundness, completeness

Conjunctive Normal Form (CNF)

DPLL

Conflict-driven clause learning (CDL) , Boolean Constraint Propagation (BCP)

Basic theories (equality, uninterpreted functions, linear integer arithmetic) and relationship of SMT to SAT

Symbolic Reachability

What is the reachability problem?

What is the state explosion problem?

Symbolic encoding

The “obvious” symbolic reachability algorithm

Limitations of symbolic reachability

Temporal Logic and Model Checking

What is model checking?

LTL

1. Model of time
2. Syntax
3. Semantics (satisfiability, validity)
4. Proofs

CTL

Same!

Relationship between CTL model checking algorithm, expansion laws, and fixpoints

End
(Office Hours)