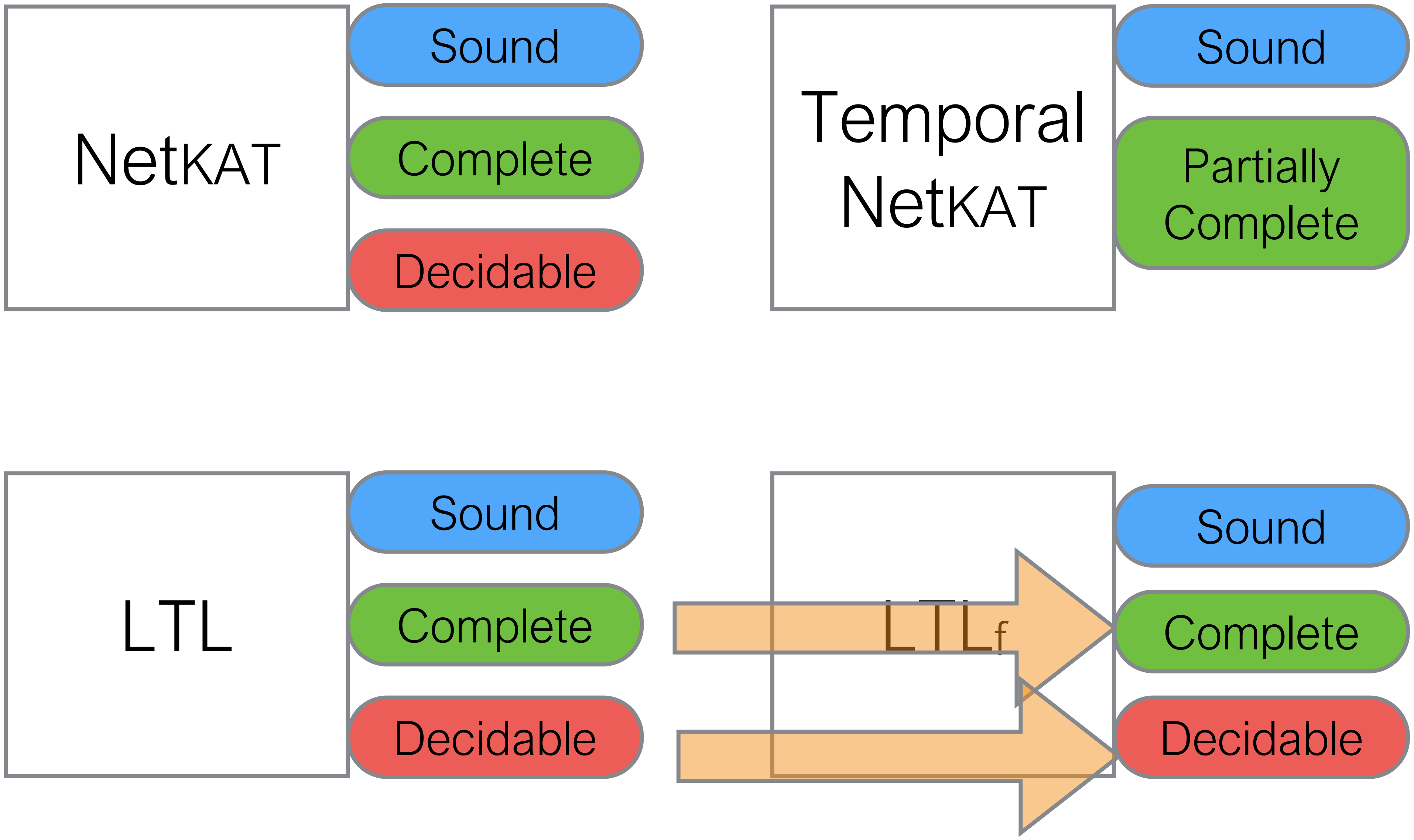
Temporal NetKAT

Eric Campbell

Ryan Beckett   Michael Greenberg   Dave Walker

About Me

My Research



NetKAT

Sound

Complete

Decidable

Temporal NetKAT

Sound

Partially Complete

LTL

Sound

Complete

Decidable

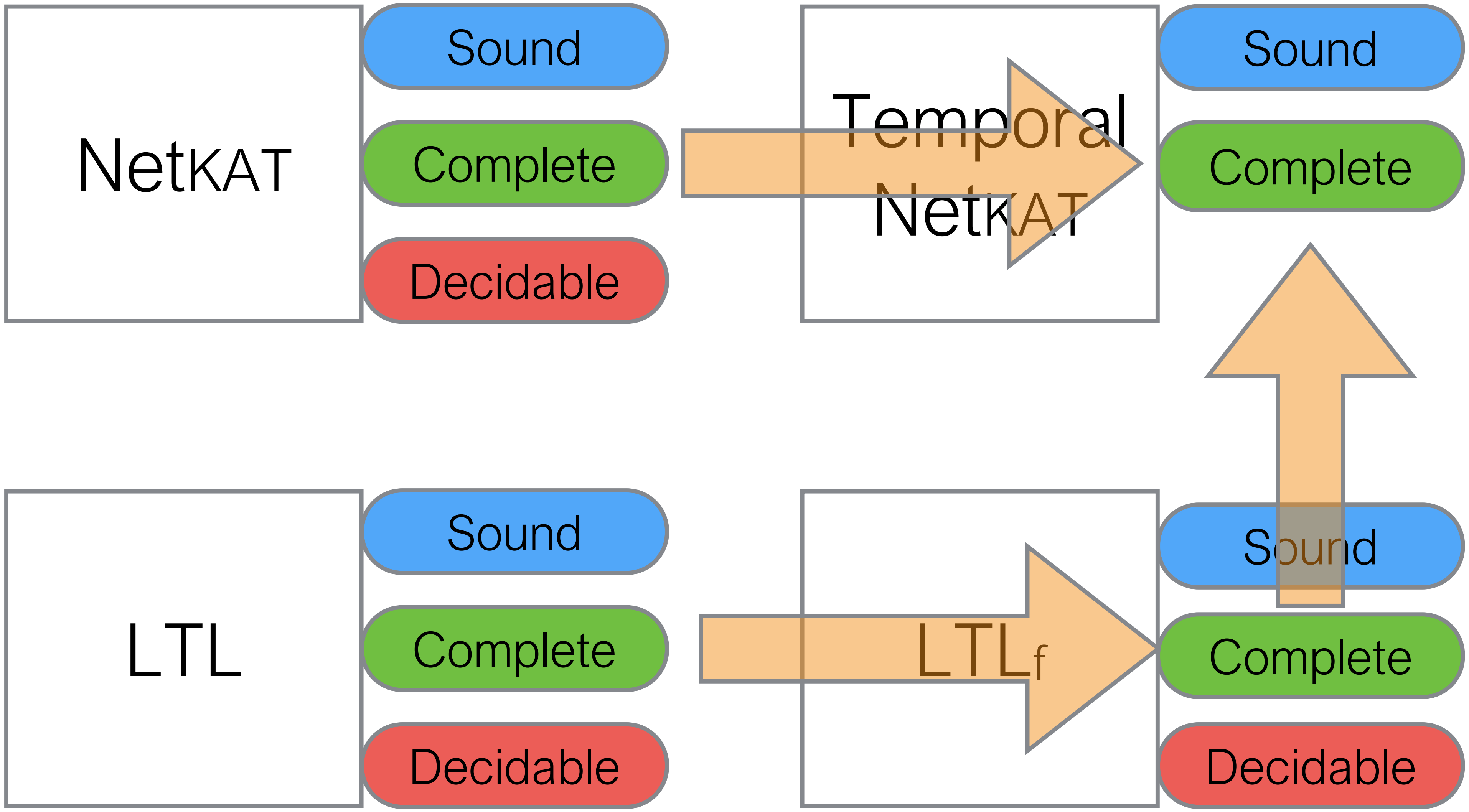
LTL$_f$

Sound

Complete

Decidable

My Research



NetKAT

Sound

Complete

Decidable

Temporal NetKAT

Sound

Complete

LTL

Sound

Complete

Decidable

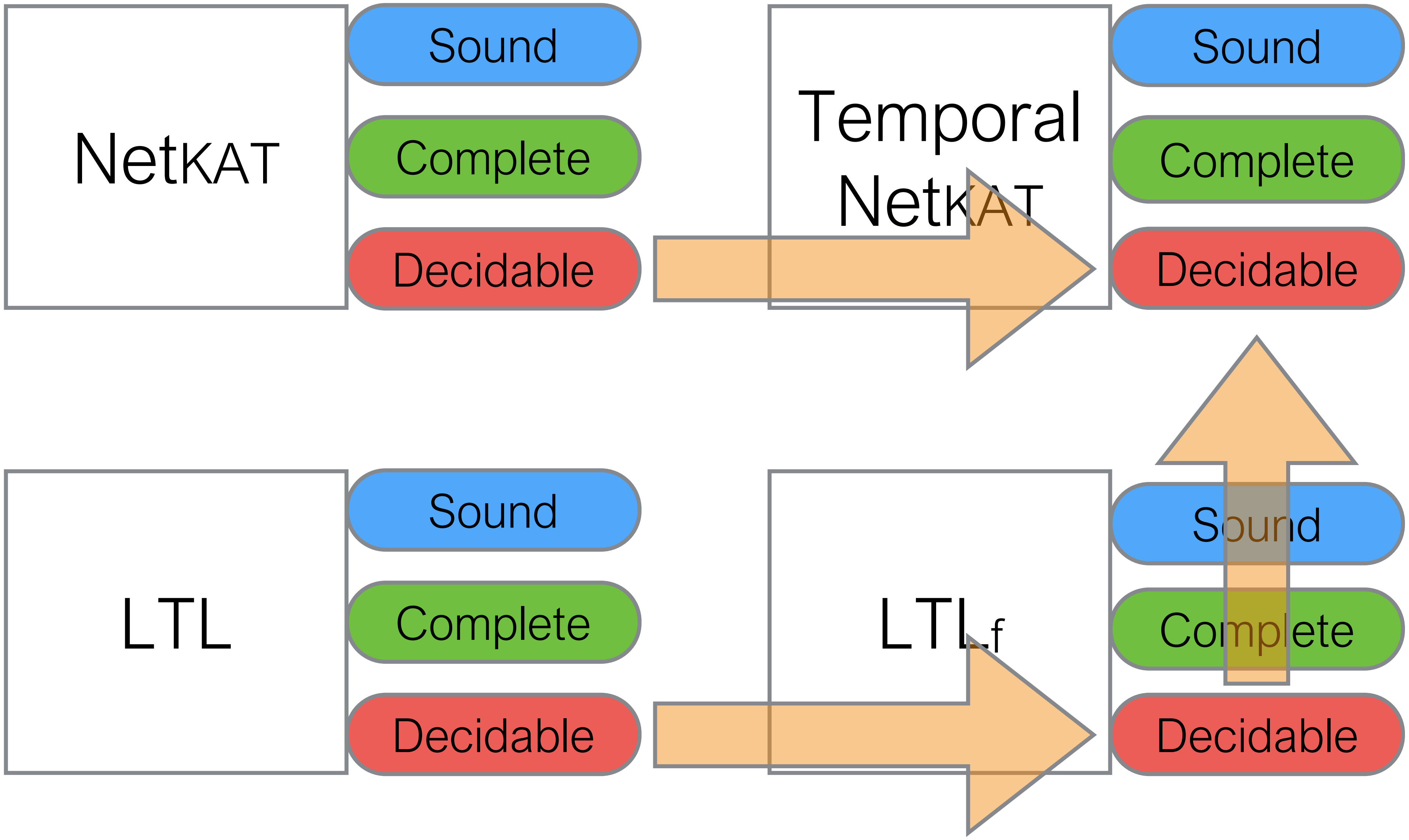
LTL_f

Sound

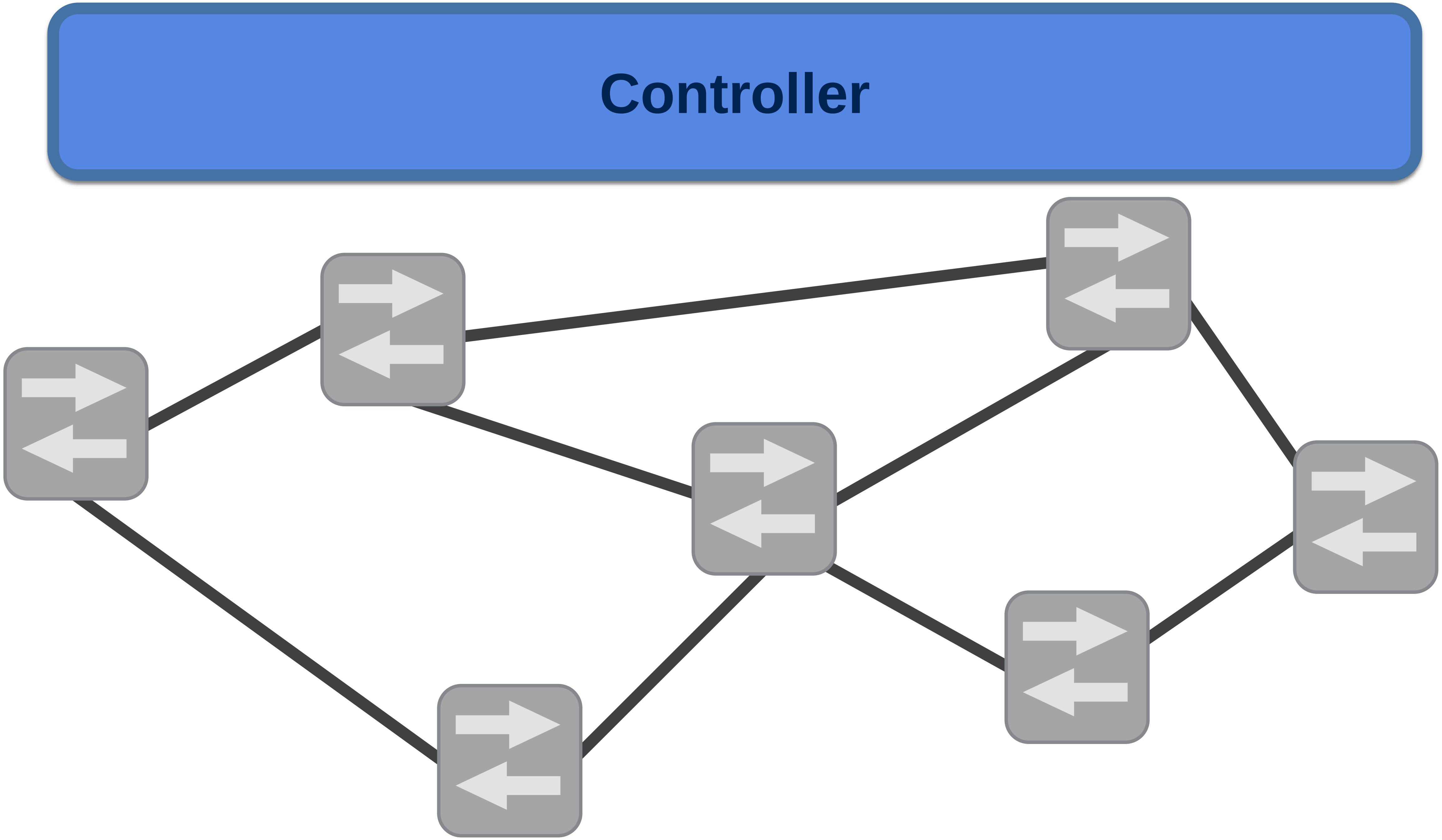
Complete

Decidable

My Research


NetKAT
Sound
Complete
Decidable
Temporal NetKAT
Sound
Complete
Decidable
LTL
Sound
Complete
Decidable
LTL_f
Sound
Complete
Decidable

Software Defined Networking



NetKAT

Predicates

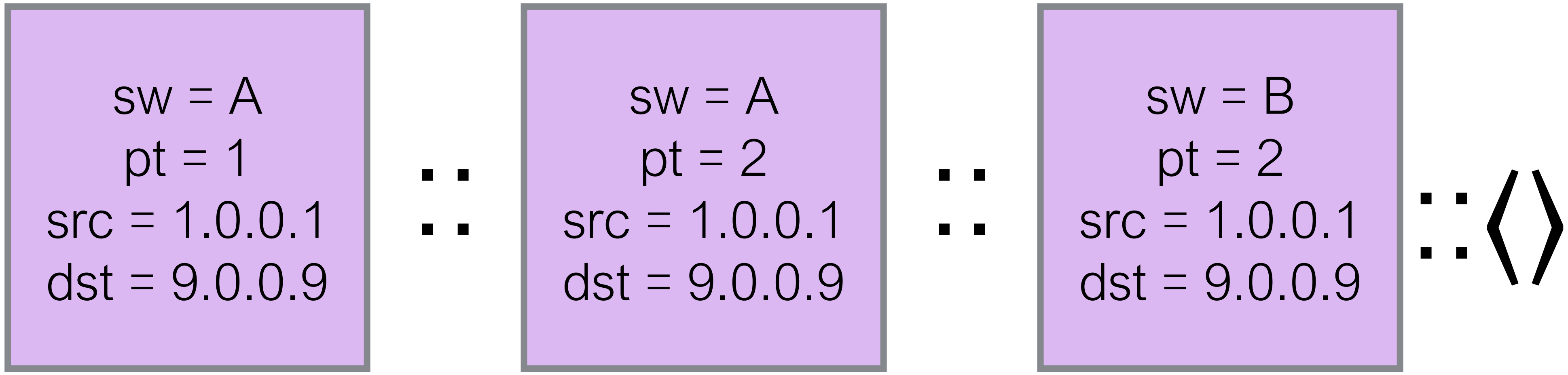
a,b ::= 1	id
| 0	drop
| f = n	test
| a + b	or
| a ; b	and
| ¬ a	negation

Policies

p,q ::= a	predicate
| f ← n	assign
| p + q	union
| p ; q	sequence
| p*	iteration
| dup	duplication

Packet History

Packet History is a list of packets:



sw = A
pt = 1
src = 1.0.0.1
dst = 9.0.0.9

::

sw = A
pt = 2
src = 1.0.0.1
dst = 9.0.0.9

::

sw = B
pt = 2
src = 1.0.0.1
dst = 9.0.0.9

::⟨⟩

Packet Histories

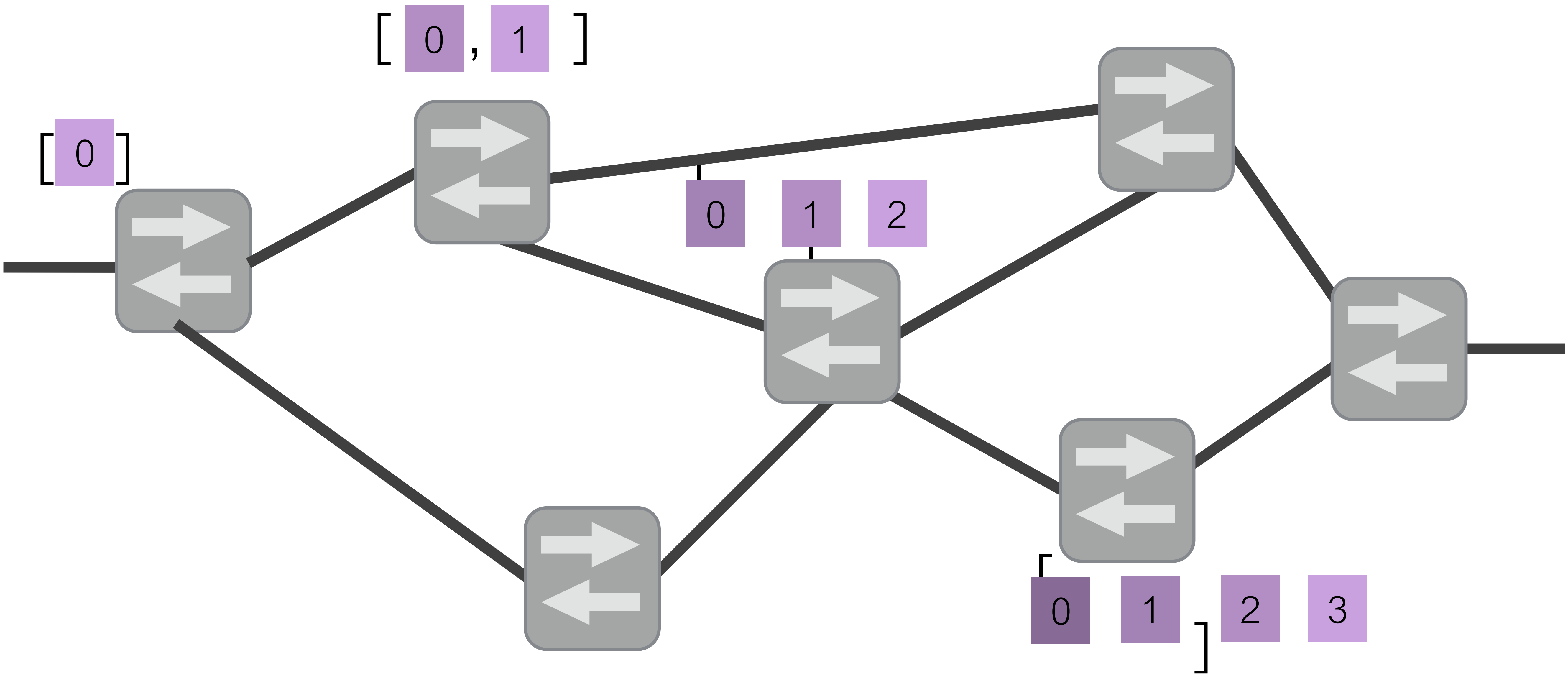
A policy denotes a function from
a packet history to a set of packet histories

$$\llbracket p \rrbracket \ : \mathrm{Hist} \rightarrow \mathbf{2}^{\mathrm{Hist}}$$

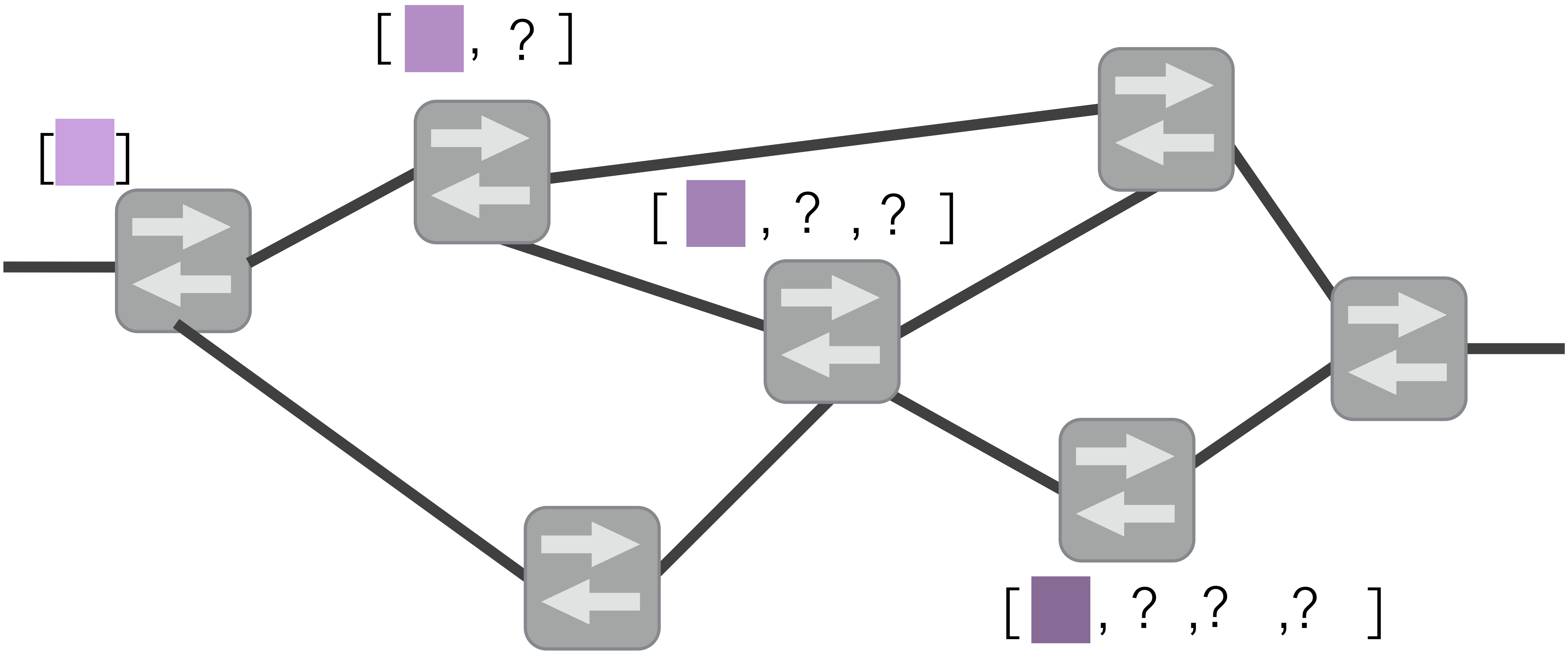
$$\llbracket 1 \rrbracket\ h \triangleq \{h\}$$
$$\llbracket 0 \rrbracket\ h \triangleq \{\}$$
$$\llbracket p + q \rrbracket\ h \triangleq \llbracket p \rrbracket\ h \cup \llbracket q \rrbracket\ h$$
$$\llbracket \neg a \rrbracket\ h \triangleq \{h\} \setminus \llbracket a \rrbracket\ h$$

…..

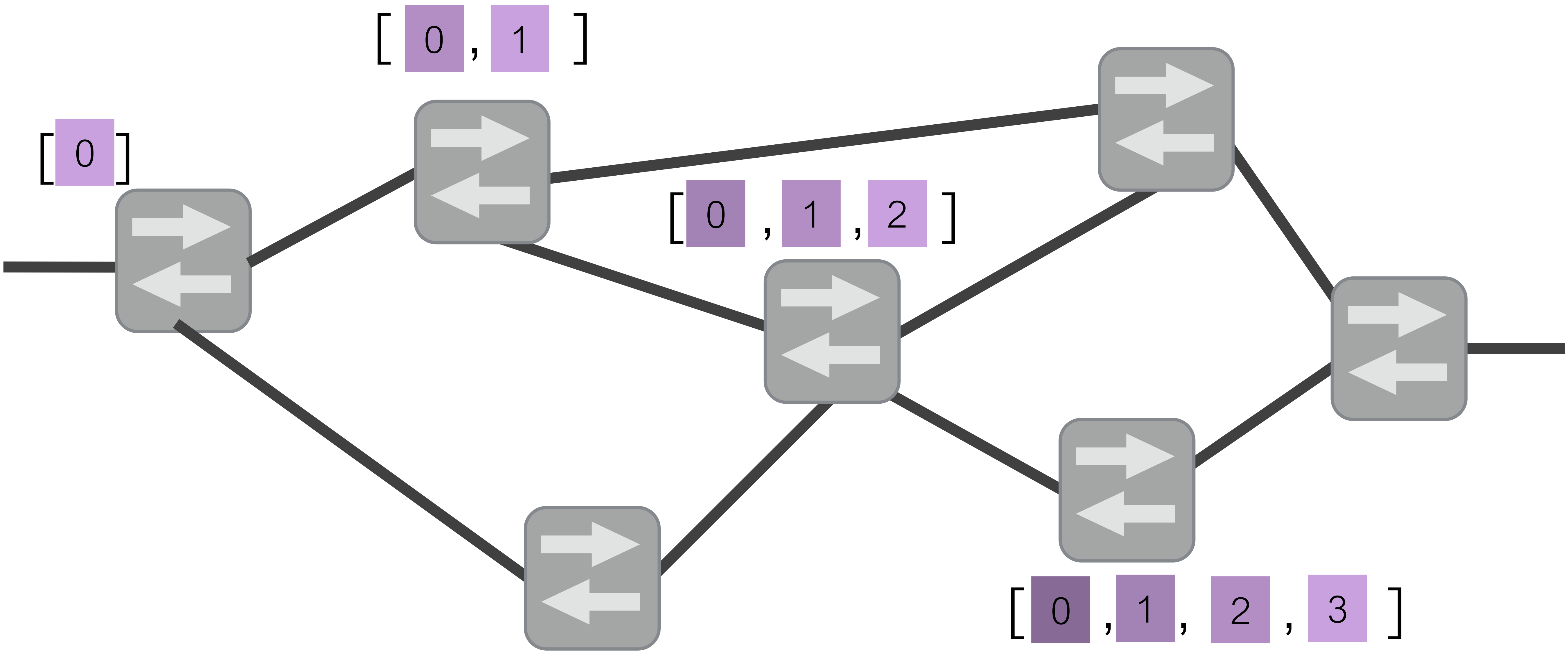
Packet Histories



Packet Histories



Packet Histories



Temporal NetKAT = NetKAT + LTL$_f$

Predicates

a,b ::=

…

| ○ a   last

| a S b   since

| ◇ a   ever

| □ a   always

| start   beginning of time

Temporal NetKAT = NetKAT + LTL_f

Predicates

a,b ::=

…

| ◯ a   last

| a S b   since

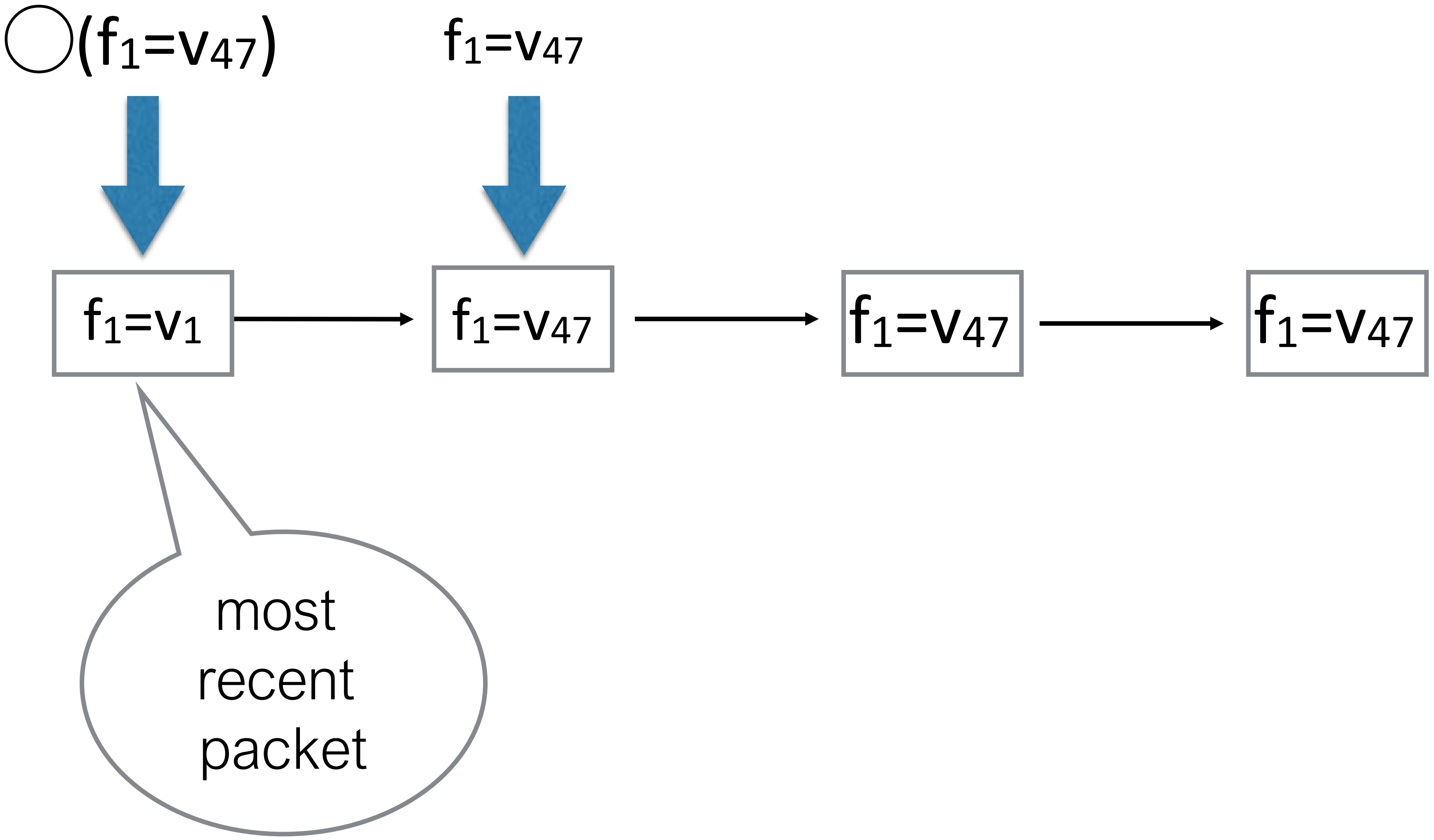
◇ a = 1 S a

□ a = ¬◇¬ a

start = ¬◯1

Temporal NetKAT = NetKAT + LTL_f

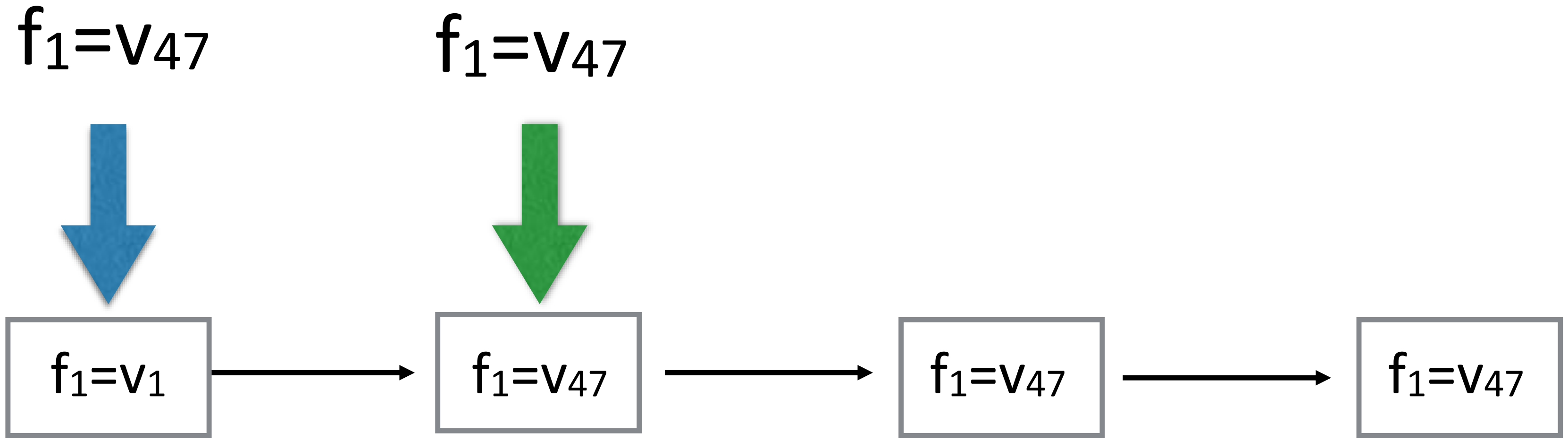
○a   last



Temporal NetKAT = NetKAT + LTL_f

$\Diamond a$ ever

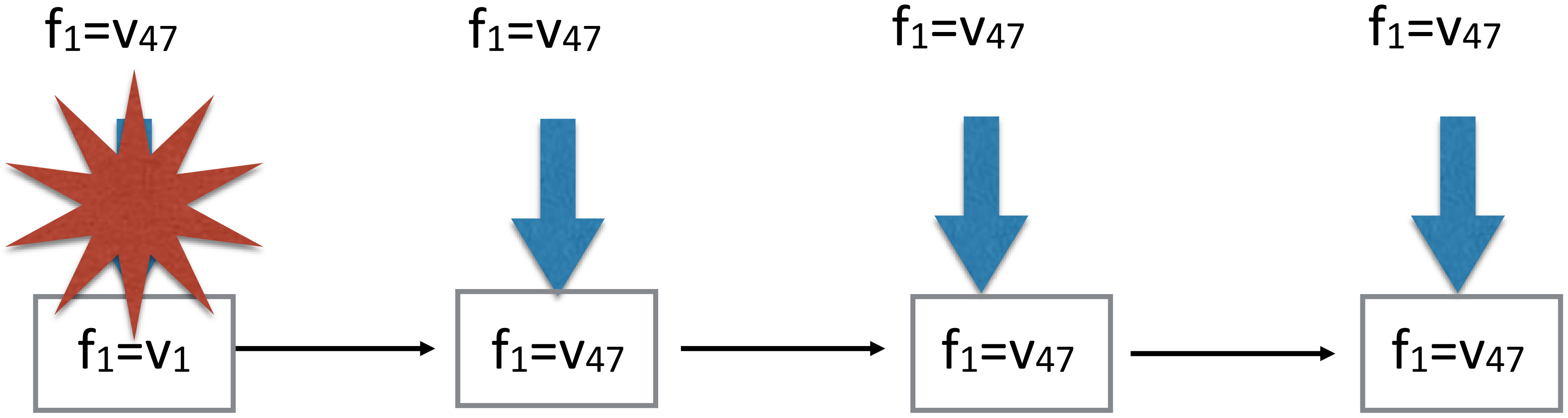
$\Diamond(f_1=v_{47})$ = True



Temporal NetKAT = NetKAT + LTL_f

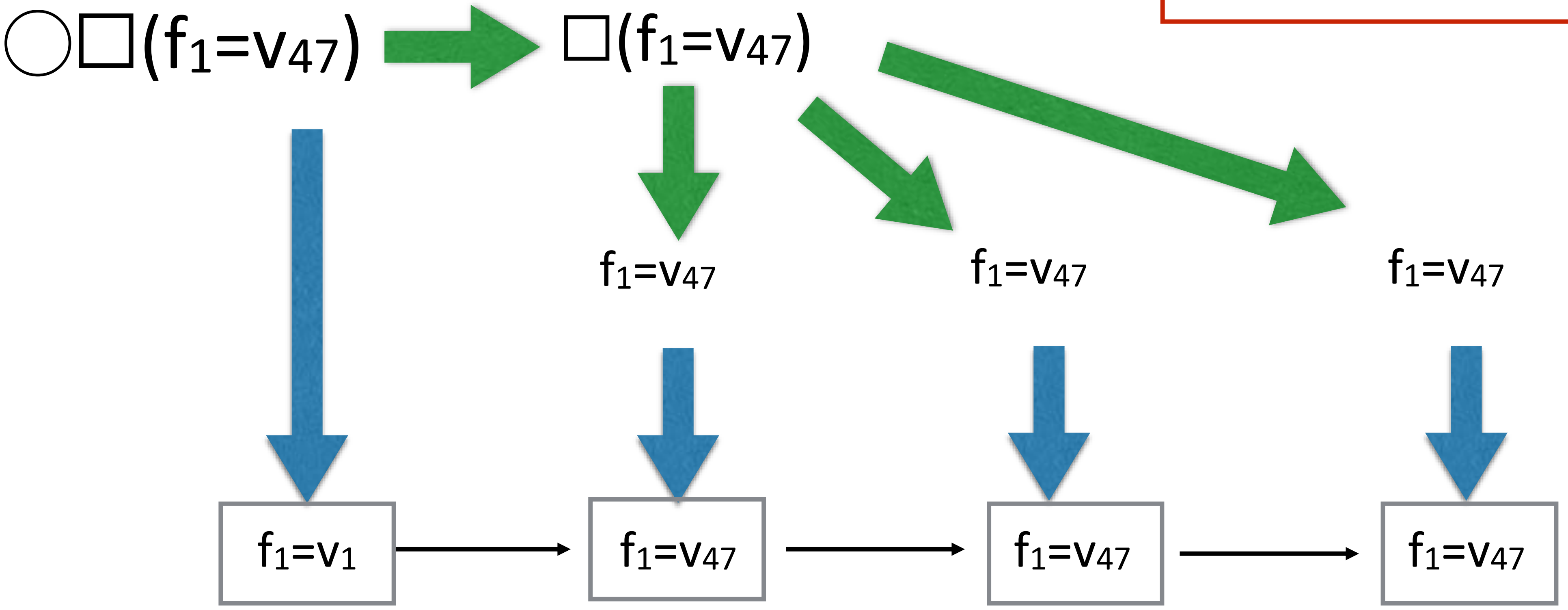
□a always

$\square(f_1=v_{47})$ = False



Temporal NetKAT = NetKAT + LTL_f

□a   last



$\bigcirc\square(f_1=v_{47})$

$\square(f_1=v_{47})$

$f_1=v_{47}$

$f_1=v_{47}$

$f_1=v_{47}$

$f_1=v_1$

$f_1=v_{47}$

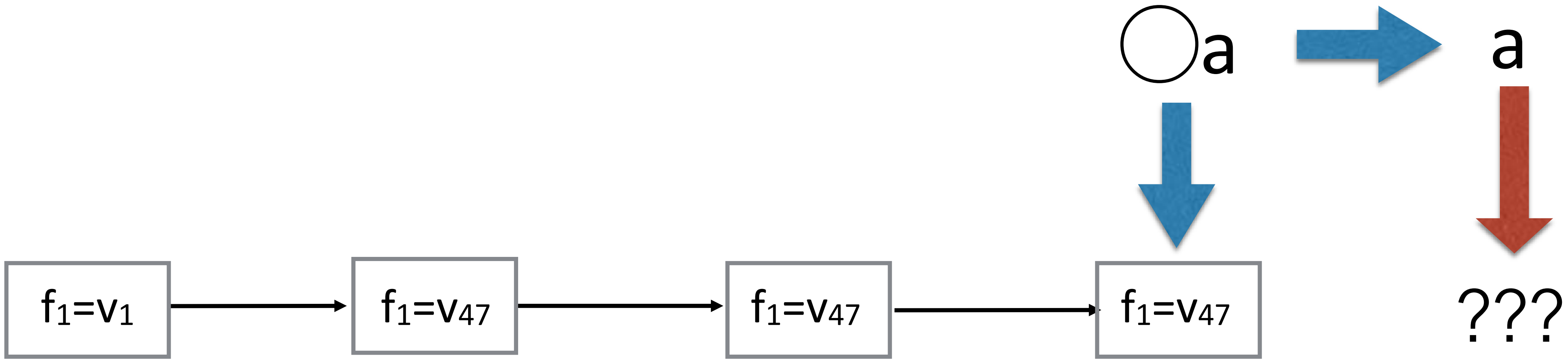
$f_1=v_{47}$

$f_1=v_{47}$

$\circ\square(f_1=v_{47})$ = True!

Temporal NetKAT = NetKAT + LTL$_f$

What about the start of time?



$\bigcirc a$

a

$f_1=v_1$

$f_1=v_{47}$

$f_1=v_{47}$

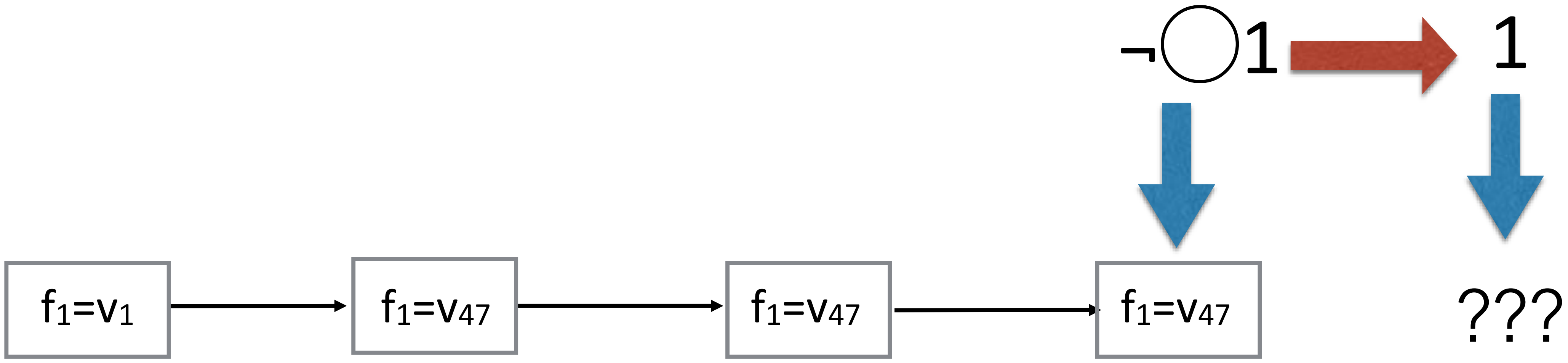
$f_1=v_{47}$

???

Temporal NetKAT = NetKAT + LTL_f

start:= $\neg\bigcirc 1$

start := $\neg\bigcirc 1$ is True!



$\neg\bigcirc 1$

1

$f_1=v_1$

$f_1=v_{47}$

$f_1=v_{47}$

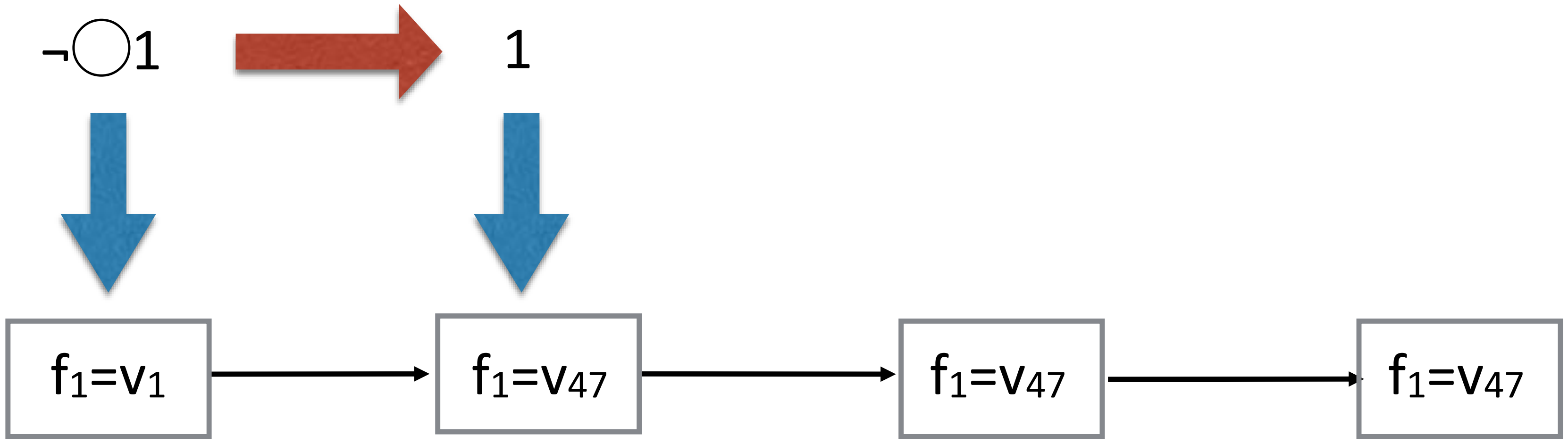
$f_1=v_{47}$

???

Temporal NetKAT = NetKAT + LTL_f

start:= ¬◯1

start := ¬◯1 is False



¬◯1

1

$f_1=v_1$

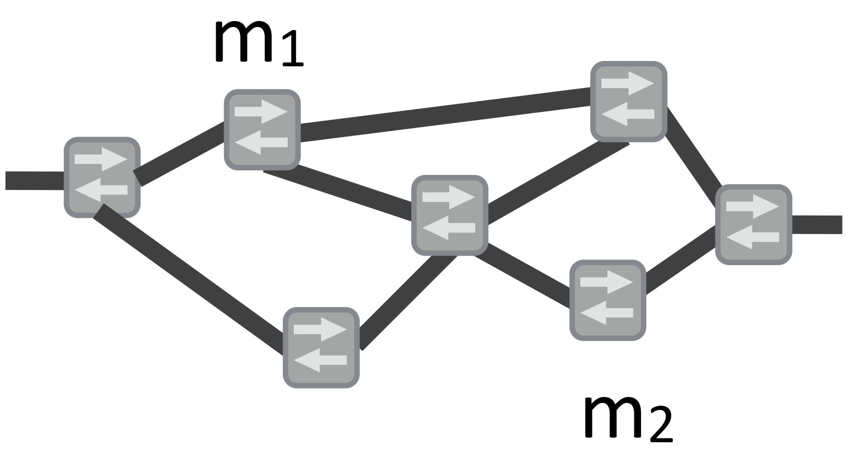
$f_1=v_{47}$

$f_1=v_{47}$

$f_1=v_{47}$

What can Temporal NetKAT do?

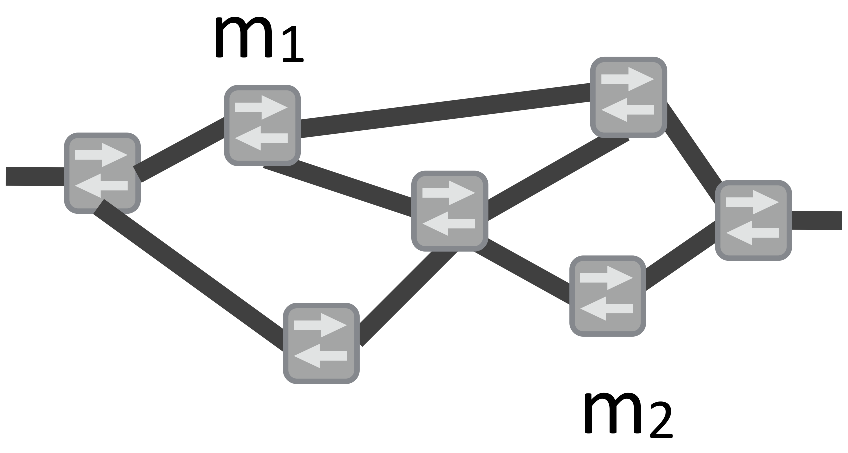
Waypointing in NetKAT



prog := (pol;top;dup)*

WTS
dup;prog ≤ dup;prog; sw=m_1;prog;sw=m_2;prog

Waypointing in TNK



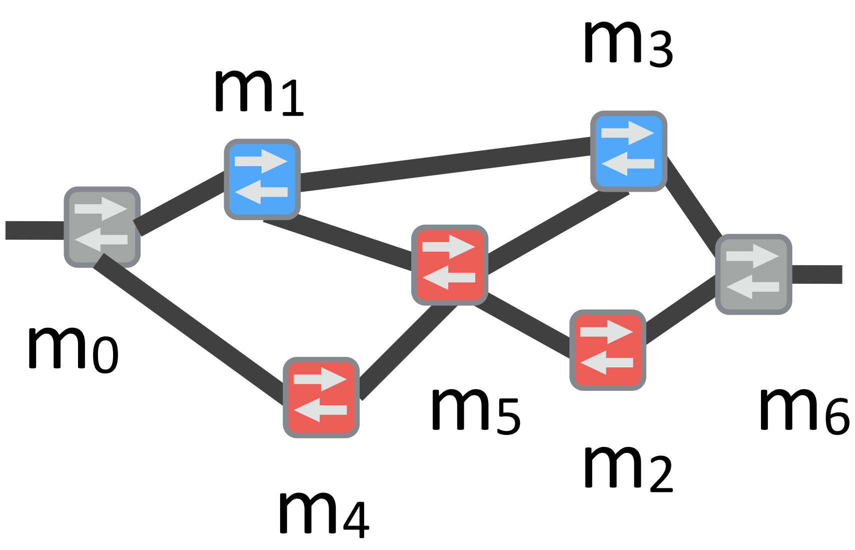
prog := (pol;top)*

query := $\Diamond(\mathrm{sw}=m_2;\Diamond(\mathrm{sw}=m_1))$

WTS prog ≡ prog; query

Highly Modular!

Isolation in TNK



prog := (pol;top)*

query := $\Box(m_1+m_3+ m_0+m_6) +$
$\Box(m_2+m_4+m_5+ m_0+m_6)$

WTS prog ≡ prog; query

Highly Modular!

Proof Theory

Proof Theory

Semiring Laws

$p + (q + r) \equiv (p + q) + r$

$p + q \equiv q + p$

$p + 0 \equiv p$

$p + p \equiv p$

$p;(q;r) \equiv (p;q);r$

$1;p \equiv p;1 \equiv p$

$p;(q + r) \equiv p;q + p;r$

$(p + q);r \equiv p;r + q;r$

$0;p \equiv 0$

$p;0 \equiv 0$

Packet Axioms

$f \leftarrow v;f'=v' \equiv f'=v';f \leftarrow v$

$f \leftarrow v;f=v \equiv f \leftarrow v$

$f=v;f=v' \equiv 0$

Boolean Subalgebra

$a + (b;c) \equiv (a + b);(a + c)$

$a + 1 \equiv 1$

$a + \neg a \equiv 1$

$a;b \equiv b;a$

$a;\neg a \equiv 0$

$a;a \equiv a$

Kleene star Laws

$1 + p;p^* \equiv p^*$

$1 + p^*;p = p^*$

$q + p;r \leq r \Rightarrow p^*;r \leq r$

$p + q;r \leq q \Rightarrow p;r^* \leq q$

LTL$_f$ Axioms

$\bigcirc(a;b) \equiv \bigcirc a;\bigcirc b$

$\bigcirc(a + b) \equiv \bigcirc a + \bigcirc b$

$a \mathrel{S} b \equiv b + a;\bigcirc(a \mathrel{S} b)$

$a \leq \bullet a;b \Rightarrow a \leq \Box b$

$\Box a \leq \Diamond(\mathit{start}; a)$

$\bullet 1 \equiv 1$

Packet LTL$_f$

$f \leftarrow v;\mathit{start} \equiv 0$

$f \leftarrow v;\bigcirc a \equiv a;f \leftarrow v$

Removed from NetKAT

$f=v; f \leftarrow v \equiv f=v$

$f \leftarrow v; f \leftarrow v' \equiv f \leftarrow v'$

$f \leftarrow v; f' \leftarrow v' \equiv f' \leftarrow v';f \leftarrow v$

Metatheory

Metatheory

What we have (PLDI 2016)

- Soundness
- Whole Network Completeness
- A Fast Temporal NetKAT compiler

Coming Soon

- Compositional Completeness
- Decidability
- A new proof method for KATs

Metatheory

NetKAT

Soundness
If $p \equiv q$, then $[\![p]\!] = [\![q]\!]$

Completeness
If $[\![p]\!] = [\![q]\!]$, then $p \equiv q$

Temporal NetKAT

Soundness
If $p \equiv q$, then $[\![p]\!] = [\![q]\!]$

Network-Wide Completeness
If $[\![\text{start};p]\!] = [\![\text{start};q]\!]$,
then $\text{start};p \equiv \text{start};q$

The goal for my thesis:
get a full completeness result!

Linear Temporal Logic over Finite Traces

LTL$_f$ — Syntax

```
a,b ::= 1        true
      | 0        false
      | a → b    implication
      | ◯a       last
      | a S b    since
      | ◇a       ever
      | □a       always
      | start    start of time
```

LTL$_f$ — Semantics

Definition. Finite Kripke Structure, written K^n, is a finite tuple of valuation functions:

$$K^n = (\eta_1 , \eta_2 , \eta_3 , \ldots , \eta_n)$$

The function $K^n_i : LTL_f \rightarrow 2$ evaluates an LTL$_f$ term at point *i*

LTL$_f$ — Semantics

🟩 $\Box(a + b)$ 🟩 $\Diamond(\text{start})$ 🟥 $\Box(b \rightarrow a)$

$K^5 = ($

🟩	a	b a	a	b	b start
🟥	b start	start	b start	a start	a

$)$

Definition (Validity).

Given a formula a, write ⊨a if

For every K^n, and i = 1, …, n, $K^n_i(a)$ = True

LTL_f — Proof Theory

$\vdash$all propositional tauts

$\vdash \bigcirc(a \rightarrow b) \leftrightarrow (\bigcirc a \rightarrow \bigcirc b)$

$\vdash \mathrm{start} \rightarrow \neg \bigcirc a$

$\vdash \Diamond(\mathrm{start})$

$\vdash a \; B \; b \leftrightarrow b + a; \bullet(a \; B \; b)$

$a \vdash \bullet a$

$a \rightarrow b, a \rightarrow \bullet a \vdash a \rightarrow \Box b$

LTL_f — Proof Theory

A weird Quirk:

$$a \vdash b \;\cancel{\text{iff}}\; \vdash a \rightarrow b$$

$$a \vdash b \text{ iff } \vdash (\Box a) \rightarrow b$$

LTL_f — Metatheory

Soundness
If ⊢a , then ⊨ a

Proof. By induction ✓

Completeness
If ⊨ a, then ⊢a

Proof. By making a graph

Decidability
Satisfiability is decidable

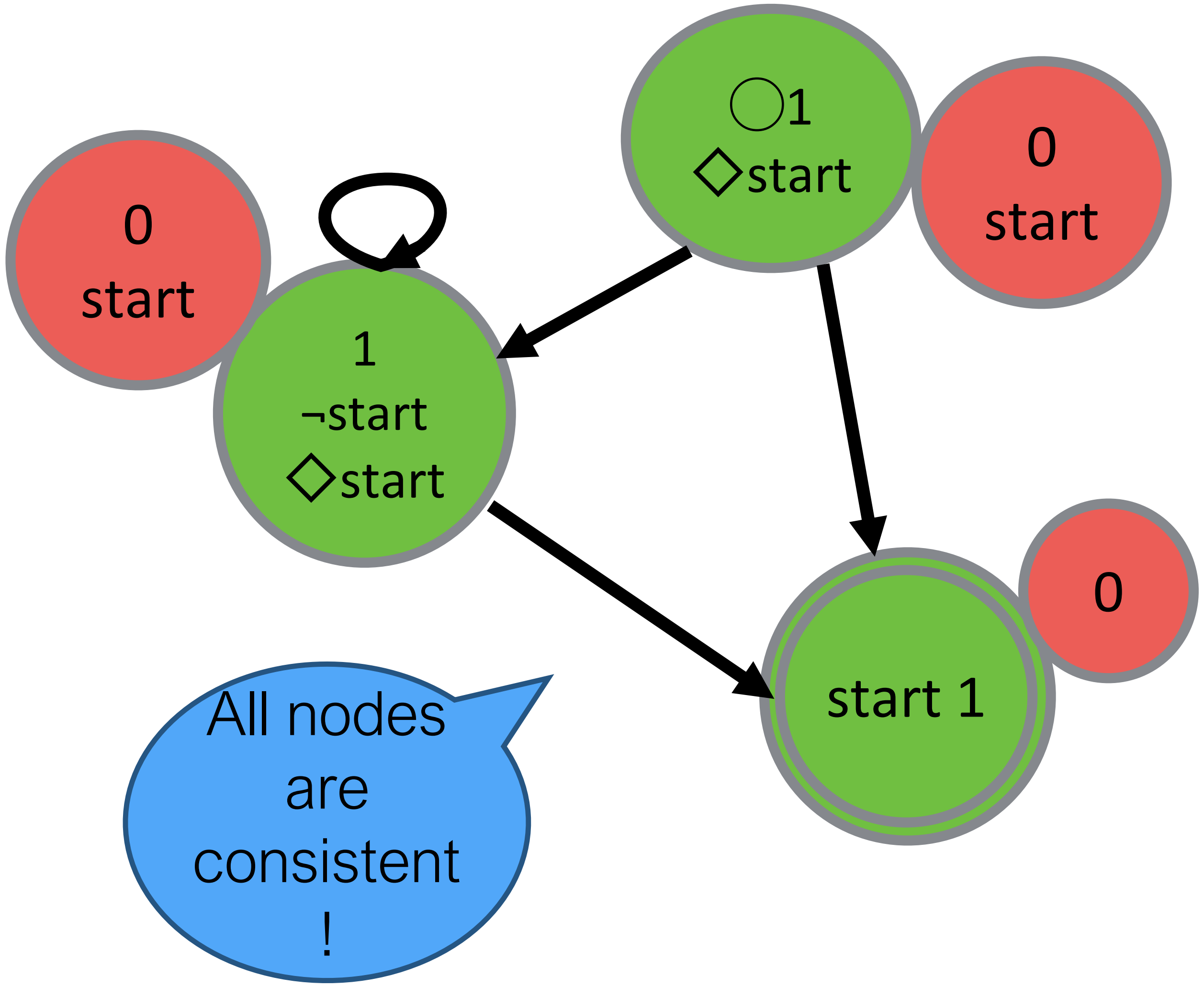
Proof. By making a tableau

LTL$_f$ —Completeness

Theorem. Completeness
If ⊨ a, then ⊢a

Positive-Negative Pair (PNP) P = 🟢🔴

form(P) = $\prod_{a\,\in\,🟢} a \;;\; \prod_{b\,\in\,🔴} \neg b$

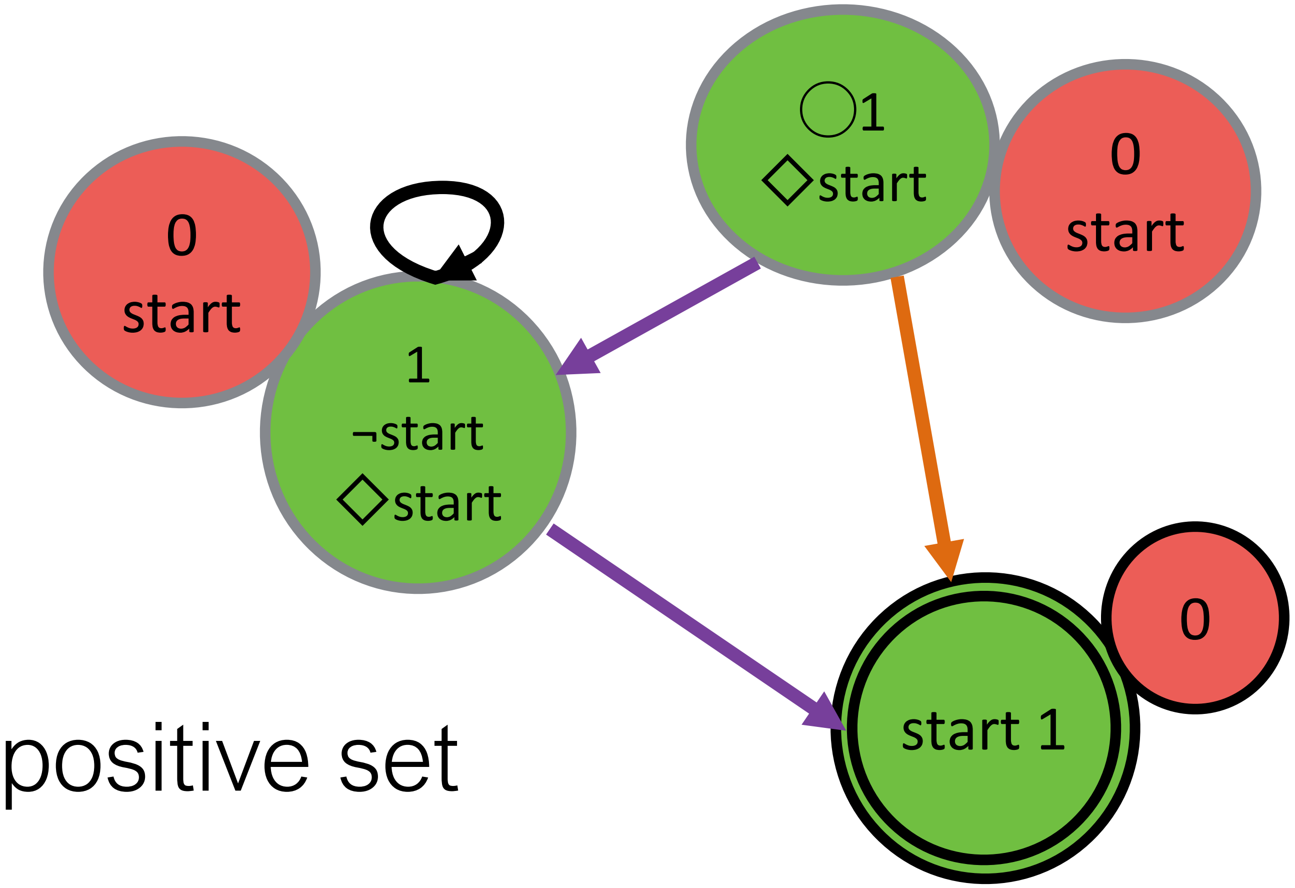


All nodes are consistent!

P is called *inconsistent* if
⊢¬form(P)
and *consistent* otherwise.

LTL_f —Completeness

Theorem. Completeness
If ⊨ a, then ⊢a



A *terminal node* has **start** in the positive set

A *terminal path* starts at the root
and ends in a terminal node

LTL$_f$ —Completeness

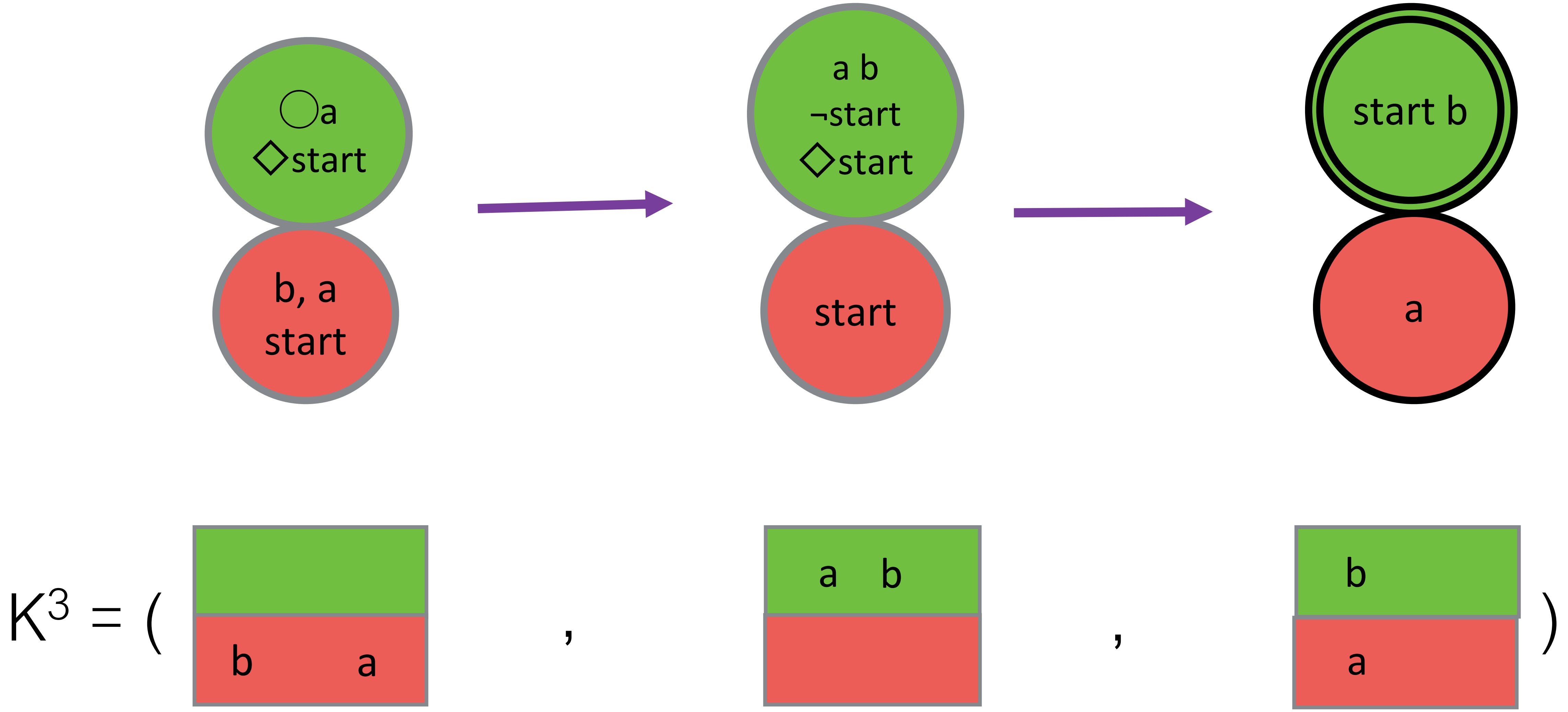
Theorem. Completeness

If ⊨ a, then ⊢a

Lemma 1.

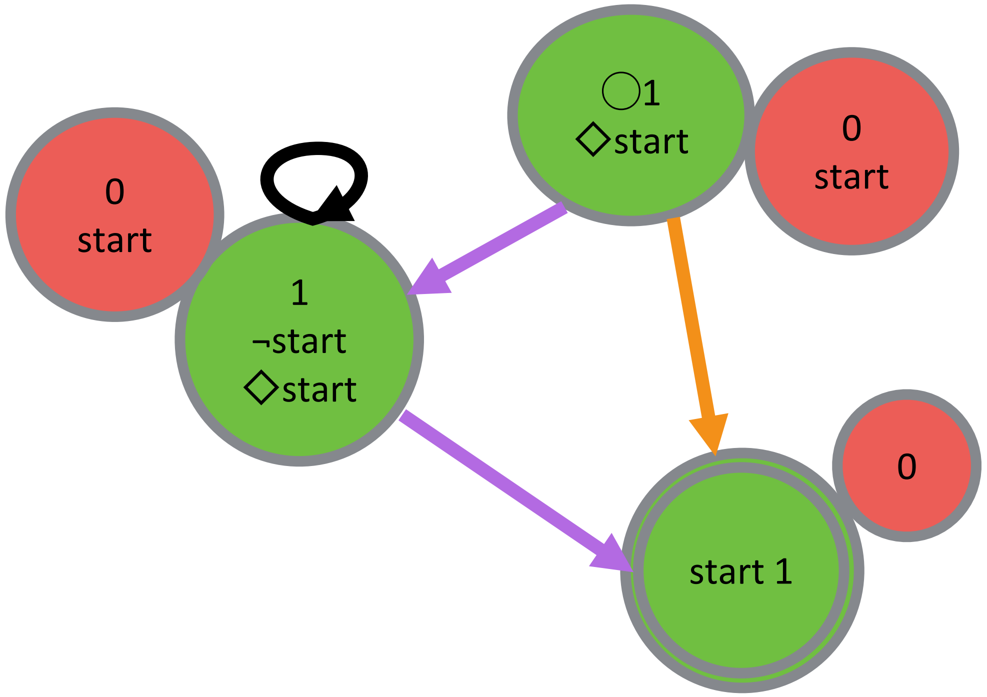
Consistent PNP ⇒

Existence of Terminal Path



LTL$_f$ —Completeness

Theorem. Completeness
If ⊨ a, then ⊢a



Lemma 3.
P consistent ⇒ **form(P)** sat
Not proves not form(P) ⇒ not models not form(P)

□

LTL_f — Metatheory

Soundness
If ⊢a , then ⊨ a

Proof. By induction ✓

Completeness
If ⊨ a, then ⊢a

Proof. By making a graph ✓

Decidability!
Satisfiability is decidable

Proof. By making a tableau

LTL_f — Decidability

Construct a Tableau using PNPs as the nodes.

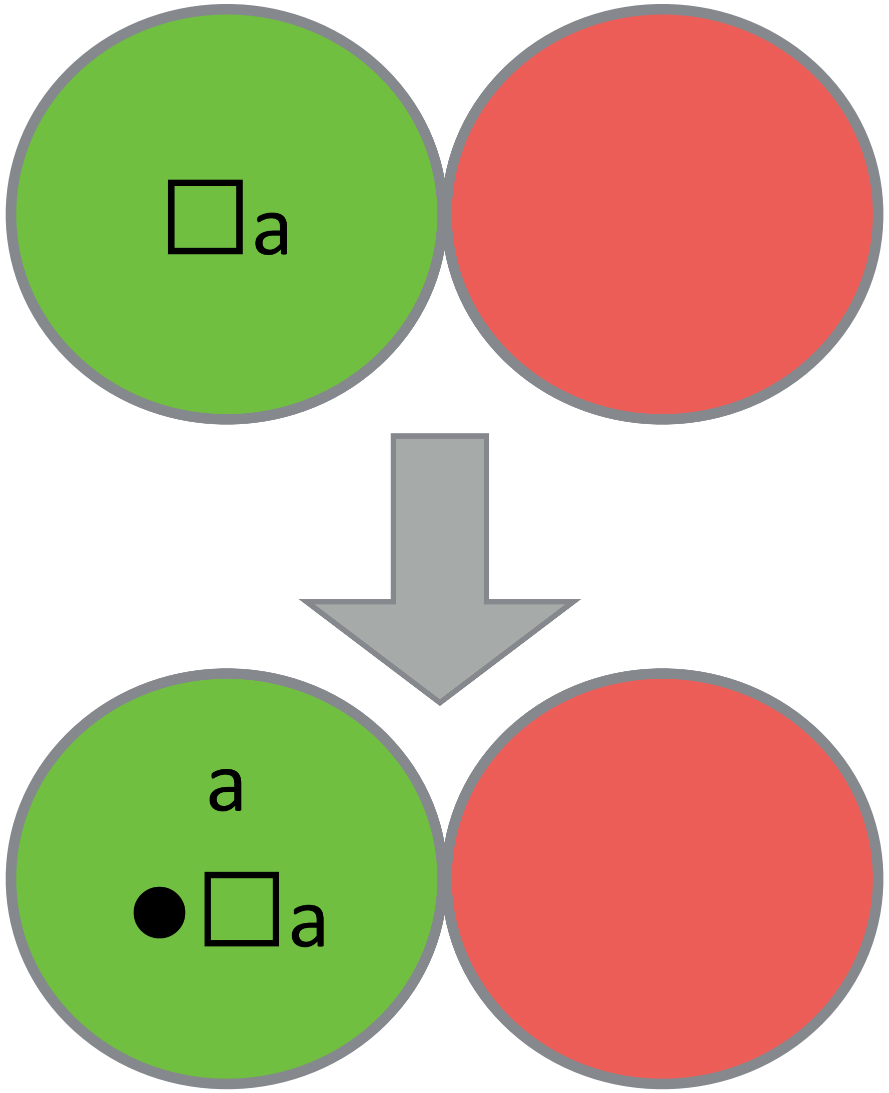
Find a path that ends in a terminal node

LTL_f — Decidability

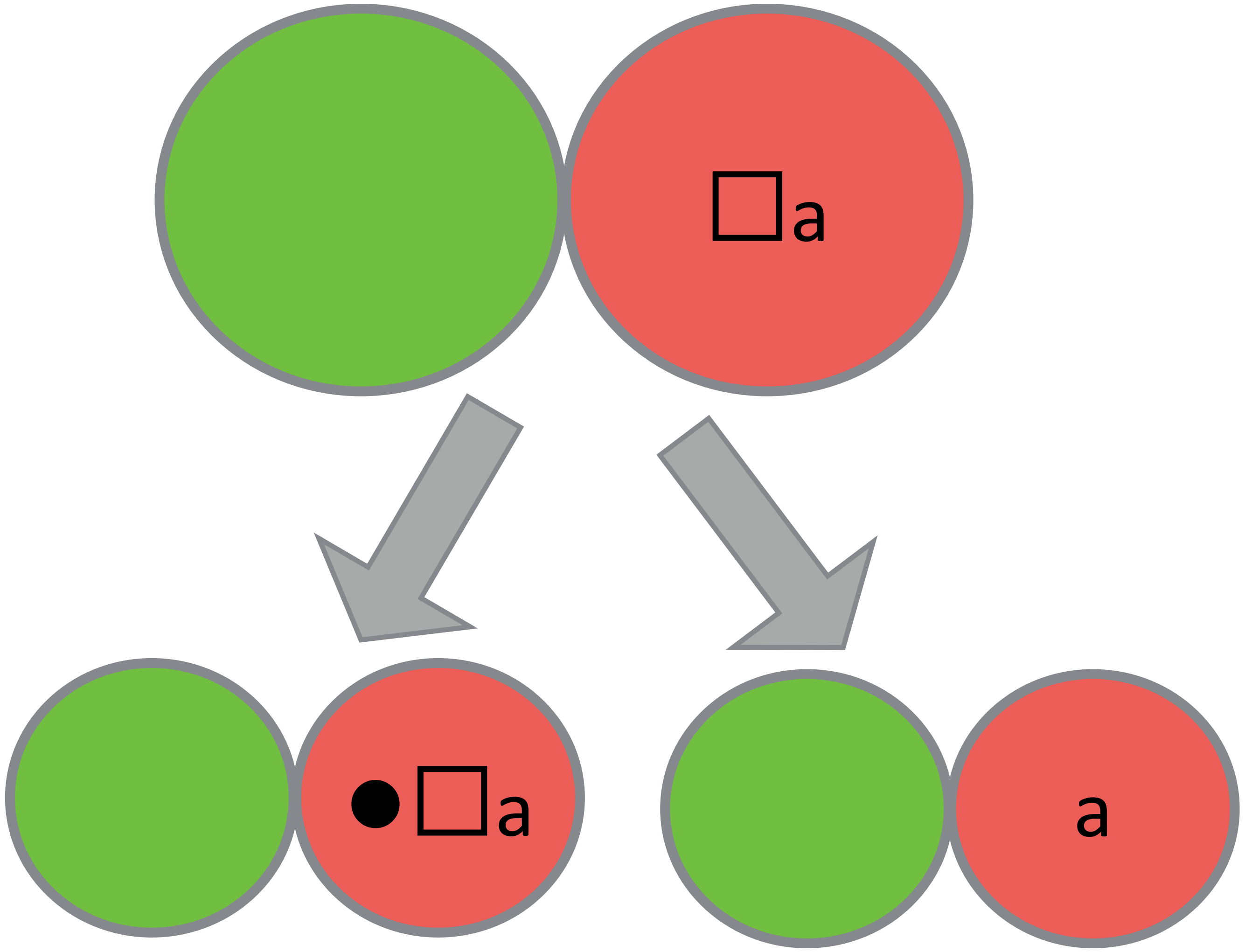
If we find a term like □a in the positive set of P,
Create a successor P’ just like P.
Add a and ●□a to the positive set of P’, remove □a

If we find a term like □a in the negative set of P,
Create successors P_L and P_R just like P.
Add a to the negative set of P_L, remove □a
Add ◯□a to the negative set of P_R, remove □a.

LTL_f — Decidability



$\Box a \equiv a ; \bullet \Box a$

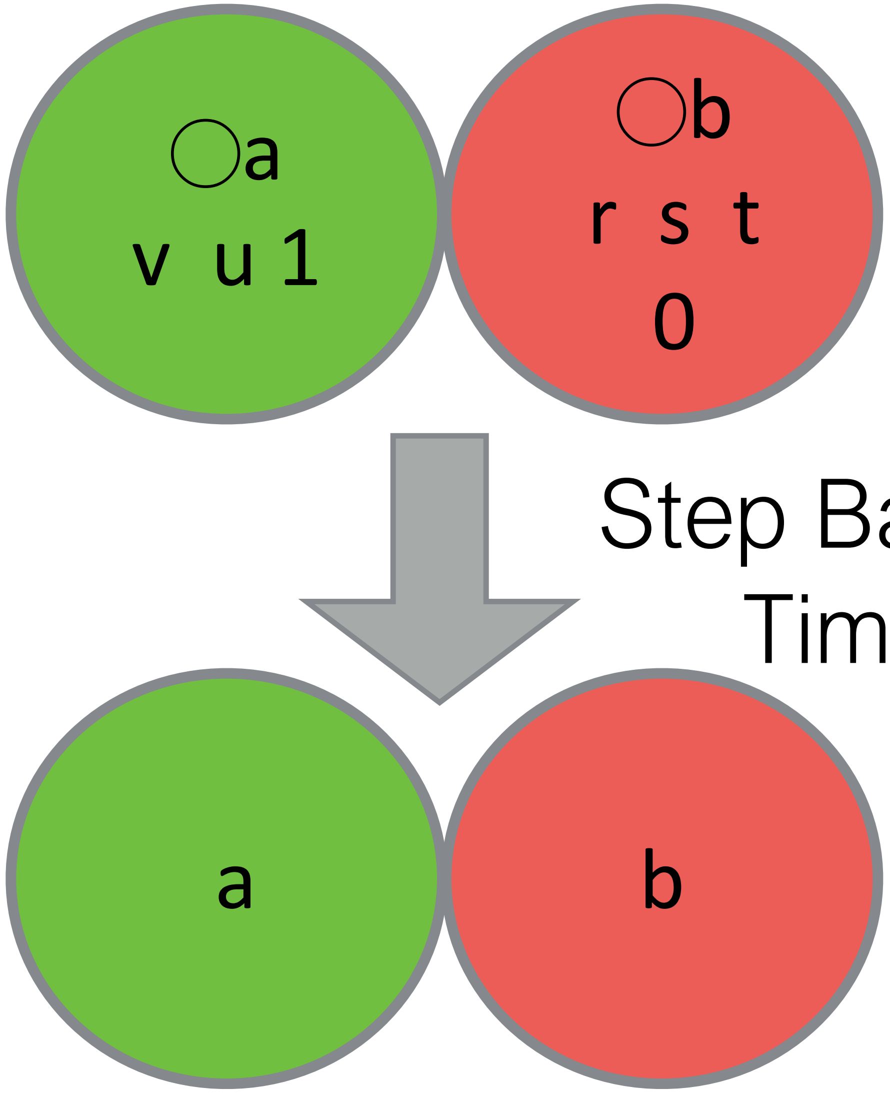


$\neg \Box a \equiv \neg a + \neg \bullet \Box a$

LTL_f — Decidability

If we find a term like $\bigcirc a$ in the positive set in P,
Create a successor P’ just like P.
Remove all variables, 0, and 1 from P’.
Add a to the positive set, remove $\bigcirc a$

LTL_f — Decidability



$\bigcirc a$

v u 1

$\bigcirc b$

r s t

0

Step Back in Time!

a

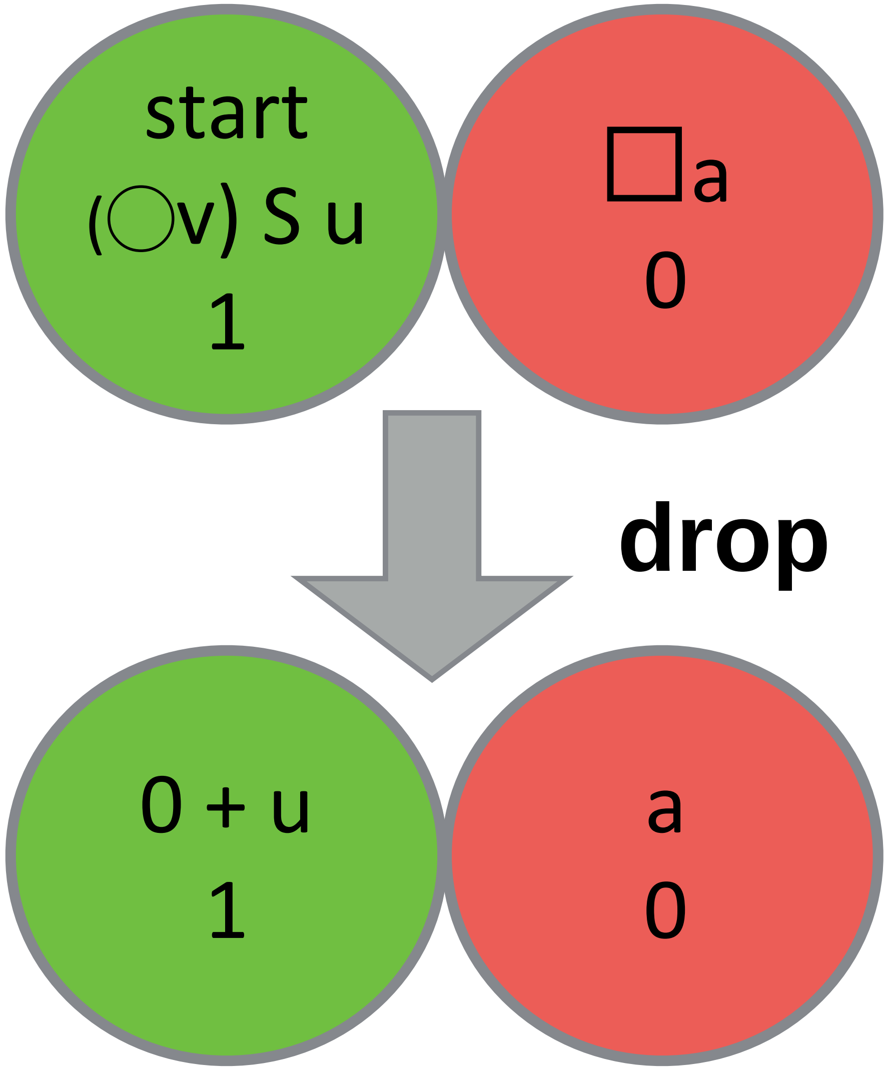
b

LTL$_f$ — Decidability

If we find a term like **start** in the positive set in P,
Create a successor P’ just like P.
Drop all temporal operators of P’.

drop(1) = 1
drop(0) = 0
drop(□a) = a
drop(◊a) = a
drop(◯a) = 0
drop(a ➞ b) = **drop**(a) ➞ **drop**(b)

LTL$_f$ — Decidability



LTL_f — Decidability

Procedure for Tableau Creation

Take a PNP P.

Create a root PNP P’ by injecting $\Diamond$start into P.

Until no new nodes can be created:

Apply syntactic Rules for $\rightarrow$, S, $\Box$, $\Diamond$

Stop when no rules apply

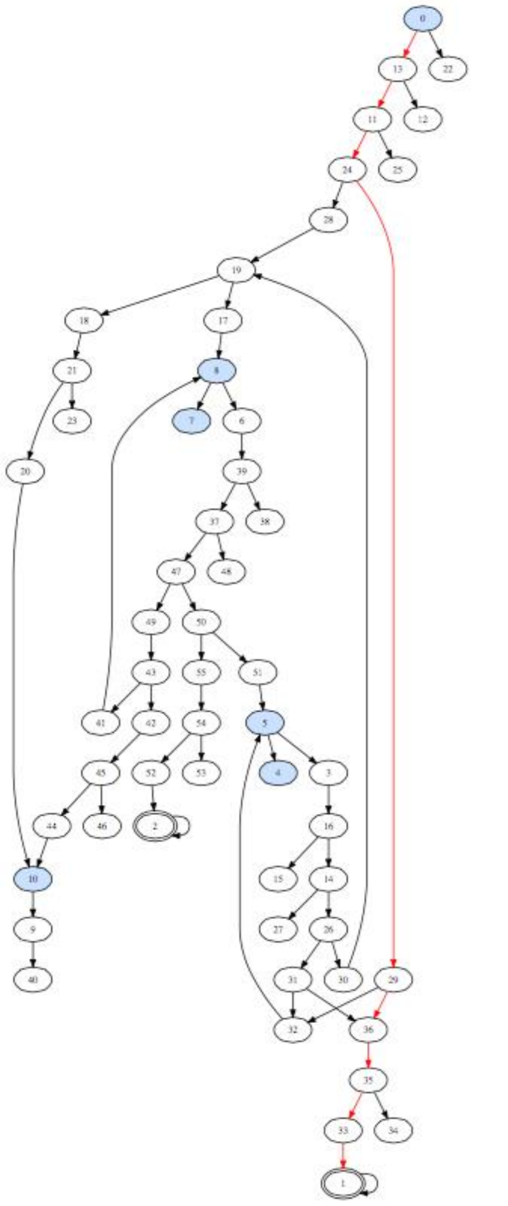
Apply a Rule for $\bigcirc$, start

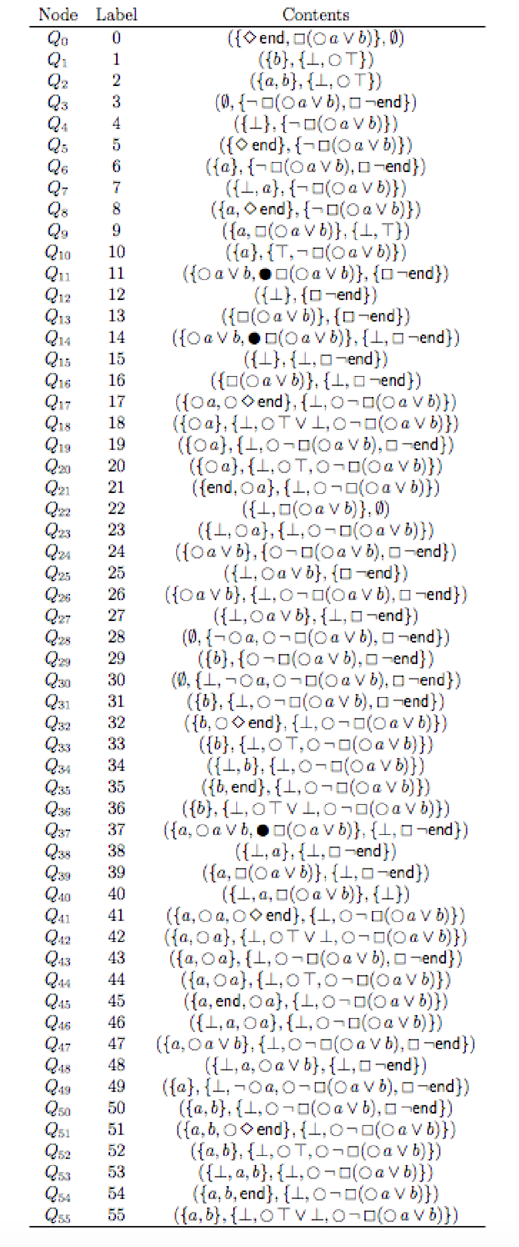
No Consistency Requirement!

Find a **terminal path** in this Tableau

LTL_f — Decidability

$\Box((\bigcirc a) + b)$





Node	Label	Contents
Q_0	0	$(\{\Diamond \mathsf{end}, \Box(\bigcirc a \vee b)\}, \emptyset)$
Q_1	1	$(\{b\}, \{\bot, \bigcirc\top\})$
Q_2	2	$(\{a, b\}, \{\bot, \bigcirc\top\})$
Q_3	3	$(\emptyset, \{\neg\Box(\bigcirc a \vee b), \Box\neg\mathsf{end}\})$
Q_4	4	$(\{\bot\}, \{\neg\Box(\bigcirc a \vee b)\})$
Q_5	5	$(\{\Diamond\mathsf{end}\}, \{\neg\Box(\bigcirc a \vee b)\})$
Q_6	6	$(\{a\}, \{\neg\Box(\bigcirc a \vee b), \Box\neg\mathsf{end}\})$
Q_7	7	$(\{\bot, a\}, \{\neg\Box(\bigcirc a \vee b)\})$
Q_8	8	$(\{a, \Diamond\mathsf{end}\}, \{\neg\Box(\bigcirc a \vee b)\})$
Q_9	9	$(\{a, \Box(\bigcirc a \vee b)\}, \{\bot, \top\})$
Q_{10}	10	$(\{a\}, \{\top, \neg\Box(\bigcirc a \vee b)\})$
Q_{11}	11	$(\{\bigcirc a \vee b, \bullet\Box(\bigcirc a \vee b)\}, \{\Box\neg\mathsf{end}\})$
Q_{12}	12	$(\{\bot\}, \{\Box\neg\mathsf{end}\})$
Q_{13}	13	$(\{\Box(\bigcirc a \vee b)\}, \{\Box\neg\mathsf{end}\})$
Q_{14}	14	$(\{\bigcirc a \vee b, \bullet\Box(\bigcirc a \vee b)\}, \{\bot, \Box\neg\mathsf{end}\})$
Q_{15}	15	$(\{\bot\}, \{\bot, \Box\neg\mathsf{end}\})$
Q_{16}	16	$(\{\Box(\bigcirc a \vee b)\}, \{\bot, \Box\neg\mathsf{end}\})$
Q_{17}	17	$(\{\bigcirc a, \bigcirc\Diamond\mathsf{end}\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{18}	18	$(\{\bigcirc a\}, \{\bot, \bigcirc\top \vee \bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{19}	19	$(\{\bigcirc a\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b), \Box\neg\mathsf{end}\})$
Q_{20}	20	$(\{\bigcirc a\}, \{\bot, \bigcirc\top, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{21}	21	$(\{\mathsf{end}, \bigcirc a\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{22}	22	$(\{\bot, \Box(\bigcirc a \vee b)\}, \emptyset)$
Q_{23}	23	$(\{\bot, \bigcirc a\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{24}	24	$(\{\bigcirc a \vee b\}, \{\bigcirc\neg\Box(\bigcirc a \vee b), \Box\neg\mathsf{end}\})$
Q_{25}	25	$(\{\bot, \bigcirc a \vee b\}, \{\Box\neg\mathsf{end}\})$
Q_{26}	26	$(\{\bigcirc a \vee b\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b), \Box\neg\mathsf{end}\})$
Q_{27}	27	$(\{\bot, \bigcirc a \vee b\}, \{\bot, \Box\neg\mathsf{end}\})$
Q_{28}	28	$(\emptyset, \{\neg\bigcirc a, \bigcirc\neg\Box(\bigcirc a \vee b), \Box\neg\mathsf{end}\})$
Q_{29}	29	$(\{b\}, \{\bigcirc\neg\Box(\bigcirc a \vee b), \Box\neg\mathsf{end}\})$
Q_{30}	30	$(\emptyset, \{\bot, \neg\bigcirc a, \bigcirc\neg\Box(\bigcirc a \vee b), \Box\neg\mathsf{end}\})$
Q_{31}	31	$(\{b\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b), \Box\neg\mathsf{end}\})$
Q_{32}	32	$(\{b, \bigcirc\Diamond\mathsf{end}\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{33}	33	$(\{b\}, \{\bot, \bigcirc\top, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{34}	34	$(\{\bot, b\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{35}	35	$(\{b, \mathsf{end}\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{36}	36	$(\{b\}, \{\bot, \bigcirc\top \vee \bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{37}	37	$(\{a, \bigcirc a \vee b, \bullet\Box(\bigcirc a \vee b)\}, \{\bot, \Box\neg\mathsf{end}\})$
Q_{38}	38	$(\{\bot, a\}, \{\bot, \Box\neg\mathsf{end}\})$
Q_{39}	39	$(\{a, \Box(\bigcirc a \vee b)\}, \{\bot, \Box\neg\mathsf{end}\})$
Q_{40}	40	$(\{\bot, a, \Box(\bigcirc a \vee b)\}, \{\bot\})$
Q_{41}	41	$(\{a, \bigcirc a, \bigcirc\Diamond\mathsf{end}\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{42}	42	$(\{a, \bigcirc a\}, \{\bot, \bigcirc\top \vee \bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{43}	43	$(\{a, \bigcirc a\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b), \Box\neg\mathsf{end}\})$
Q_{44}	44	$(\{a, \bigcirc a\}, \{\bot, \bigcirc\top, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{45}	45	$(\{a, \mathsf{end}, \bigcirc a\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{46}	46	$(\{\bot, a, \bigcirc a\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{47}	47	$(\{a, \bigcirc a \vee b\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b), \Box\neg\mathsf{end}\})$
Q_{48}	48	$(\{\bot, a, \bigcirc a \vee b\}, \{\bot, \Box\neg\mathsf{end}\})$
Q_{49}	49	$(\{a\}, \{\bot, \neg\bigcirc a, \bigcirc\neg\Box(\bigcirc a \vee b), \Box\neg\mathsf{end}\})$
Q_{50}	50	$(\{a, b\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b), \Box\neg\mathsf{end}\})$
Q_{51}	51	$(\{a, b, \bigcirc\Diamond\mathsf{end}\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{52}	52	$(\{a, b\}, \{\bot, \bigcirc\top, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{53}	53	$(\{\bot, a, b\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{54}	54	$(\{a, b, \mathsf{end}\}, \{\bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$
Q_{55}	55	$(\{a, b\}, \{\bot, \bigcirc\top \vee \bot, \bigcirc\neg\Box(\bigcirc a \vee b)\})$

LTL_f — Metatheory

Soundness
If $\vdash a$, then $\models a$

Proof. By induction ✓

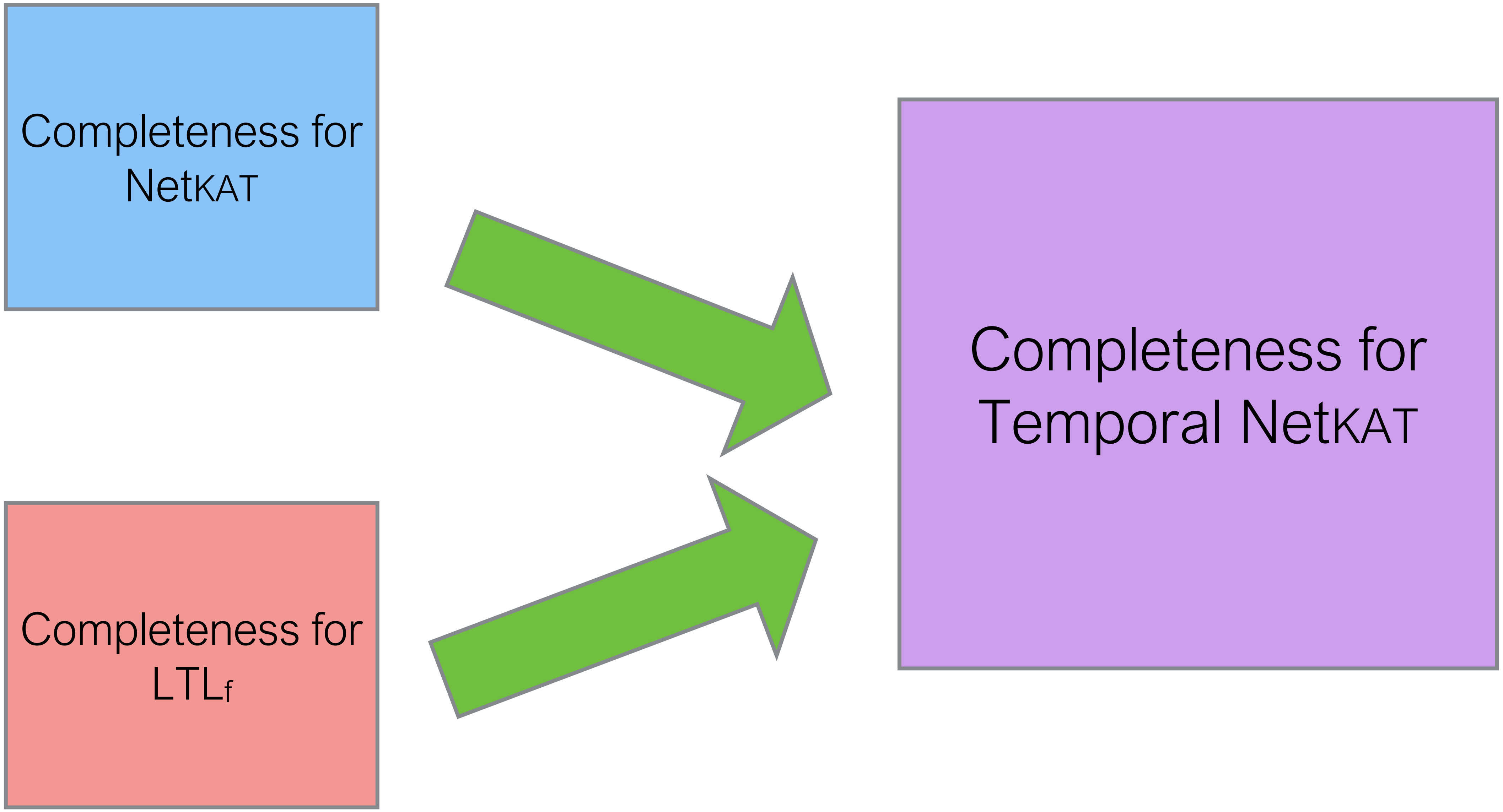
Completeness
If $\models a$, then $\vdash a$

Proof. By making a graph ✓

Decidability!
Satisfiability is decidable

Proof. By making a tableau ✓

Tying it all together

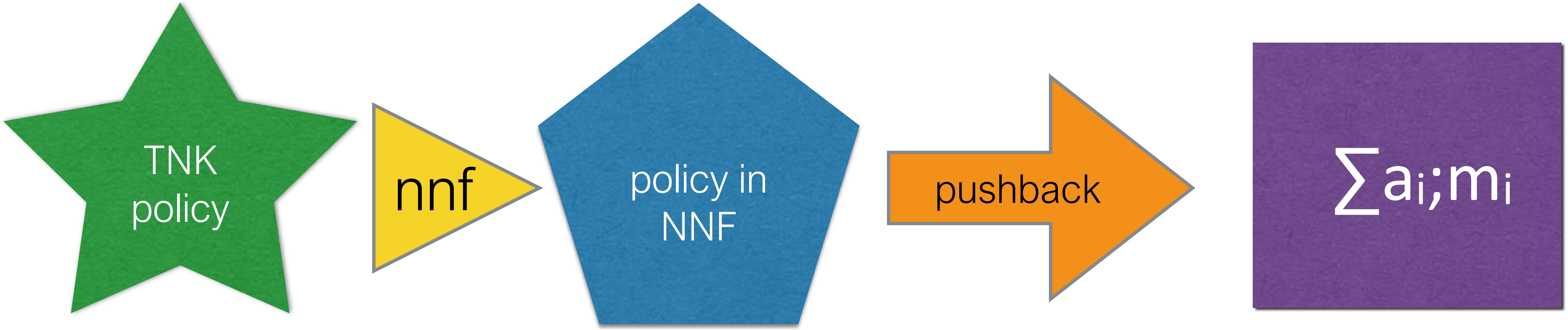


Completeness for NetKAT

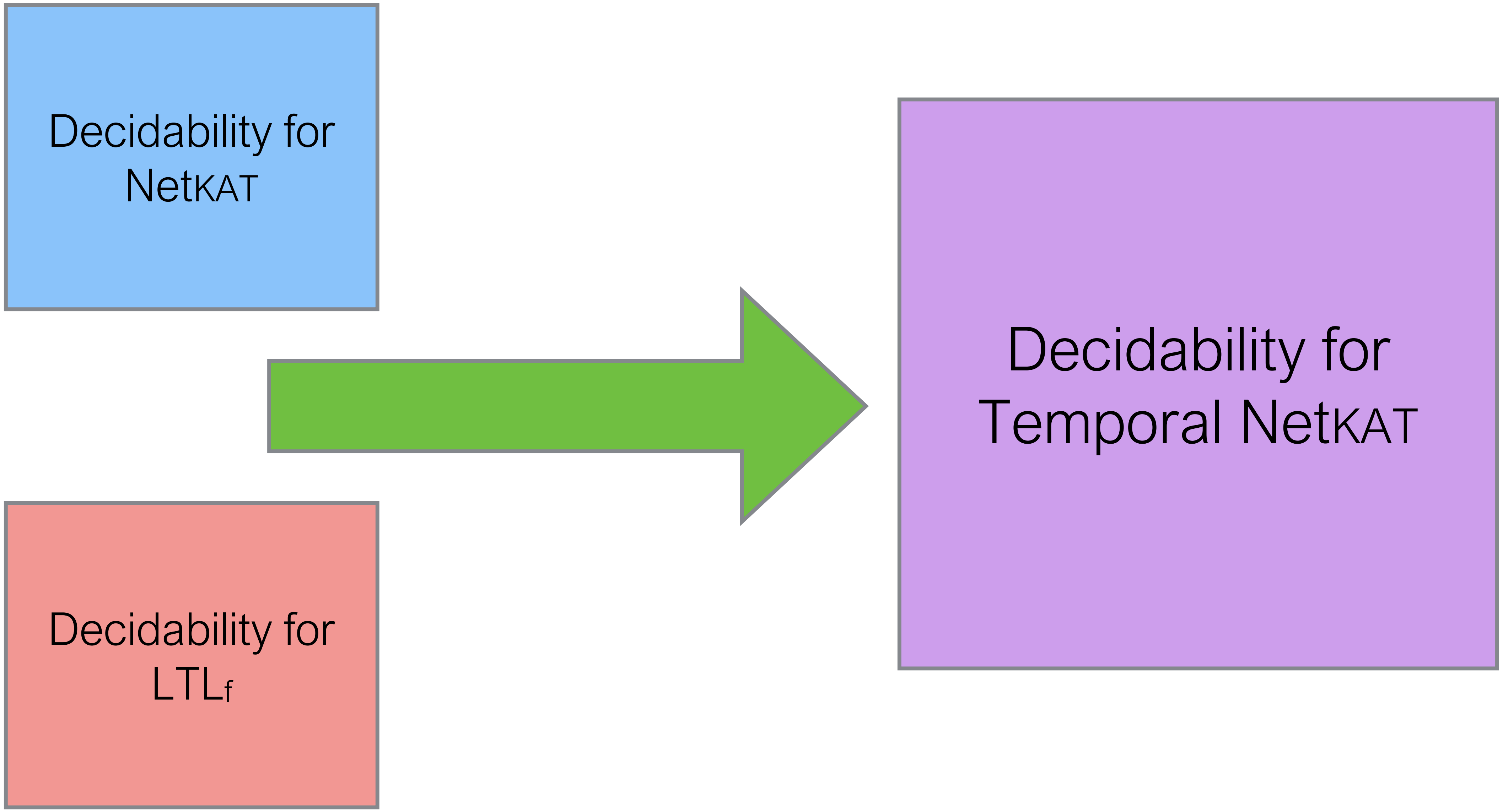
Completeness for LTL_f

Completeness for Temporal NetKAT

Temporal Netkat Completeness



Then, $\sum a_i;m_i \equiv \sum b_j;n_j$ comes from completeness of LTL_f and NetKAT



Decidability for NetKAT

Decidability for LTL_f

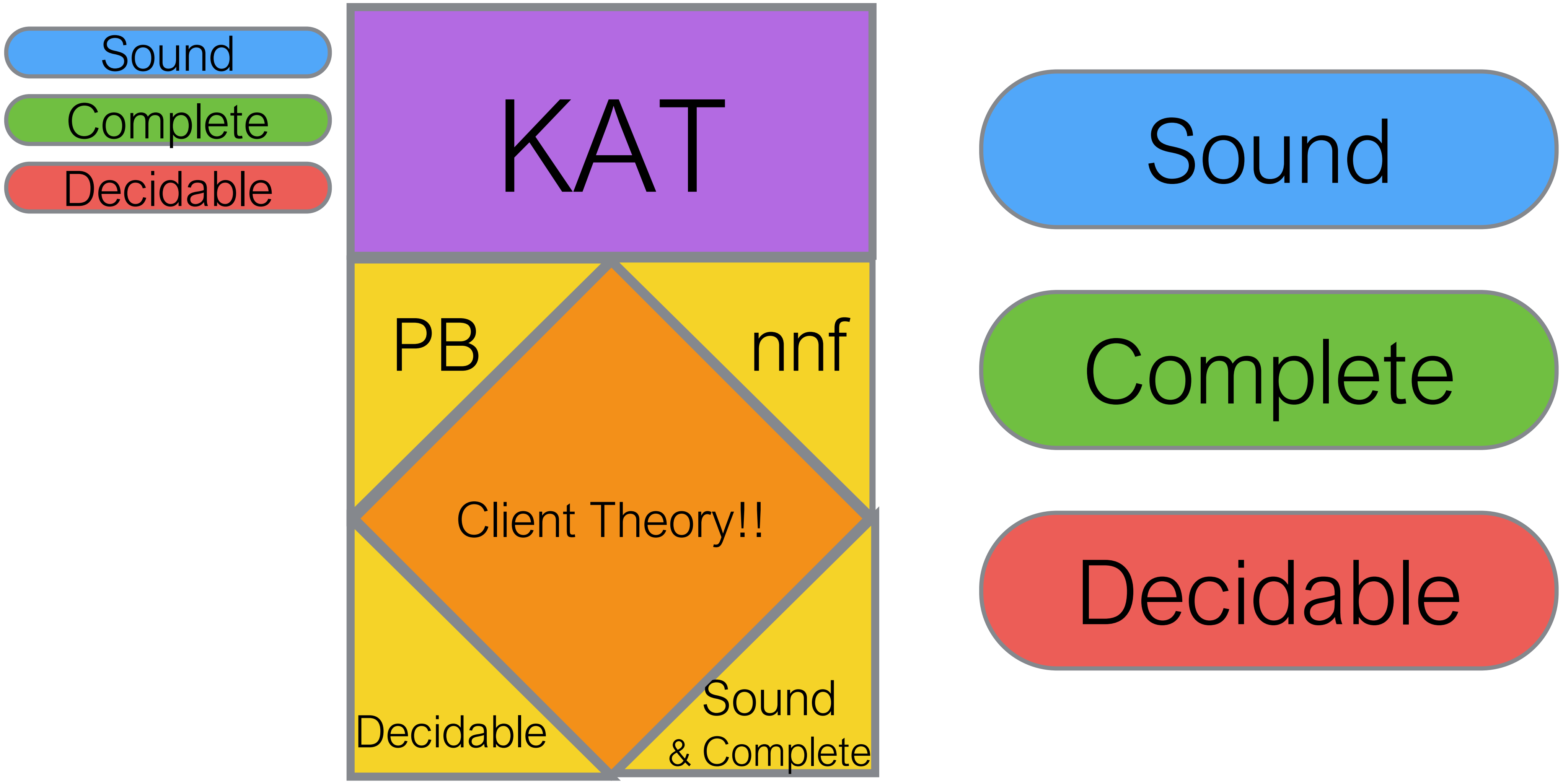
Decidability for Temporal NetKAT

Summary!

- Temporal NetKAT does cool stuff!
- So does LTLf
- LTL$_f$ is Sound, Complete, and Decidable
- So is NetKAT
- Our Normalization procedure lets us conclude that Temporal NetKAT is also Sound, Complete, and Decidable

What’s Next?

Generalize Pushback Procedure for KATs



Questions?