A FOL Fragment for Safety Checking in Infinite State Systems

Supratik Chakraborty and Abhisekh Sankaran

Introduction

- Given a state-transition system, the *safety checking* problem involves finding whether a certain *safety* property is true in all reachable states of the system.
- This can be translated to the problem of reachability of a state violating the safety property in the system.
- We look at reachability in infinite state systems. This is known to be undecidable in general.
- However we try to answer the reachability question by using a combination of inductive reasoning and bounded model checking in a semi-decision procedure.

InductionSolve

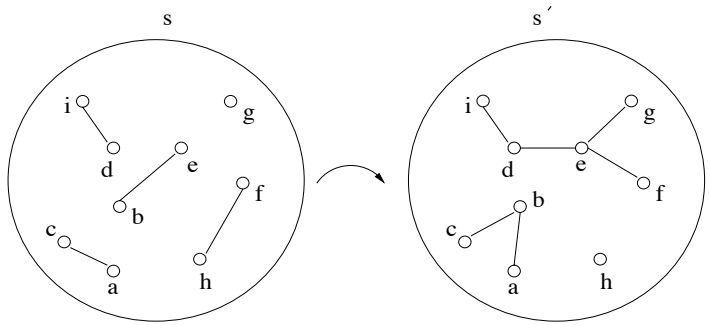
if *not* ***Sat*** $(\neg\mathcal{P}(s))$ **then** return **True**;
if ***Sat*** $(\mathcal{I}(s) \wedge \neg\mathcal{P}(s))$ **then** return counterexample s;
else
$k := 1$;
while ***True*** **do**
if *not* ***Sat*** $(\bigwedge_{i=1}^{i=k}(\mathcal{P}(s_i) \wedge \mathcal{T}(s_i, s_{i+1})) \wedge$
$\bigwedge_{1 \leq i < j \leq k+1}(s_i \neq s_j) \wedge \neg\mathcal{P}(s_{k+1}))$ **then** return **True**;
if ***Sat*** $(\mathcal{I}(s_1) \wedge \bigwedge_{i=1}^{i=k}(\mathcal{P}(s_i) \wedge \mathcal{T}(s_i, s_{i+1})) \wedge$
$\bigwedge_{1 \leq i < j \leq k+1}(s_i \neq s_j) \wedge \neg\mathcal{P}(s_{k+1}))$ **then** return counterexample s;
else
k := k + 1;

end

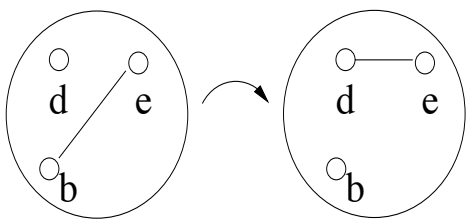
InductionSolve (Contd..)

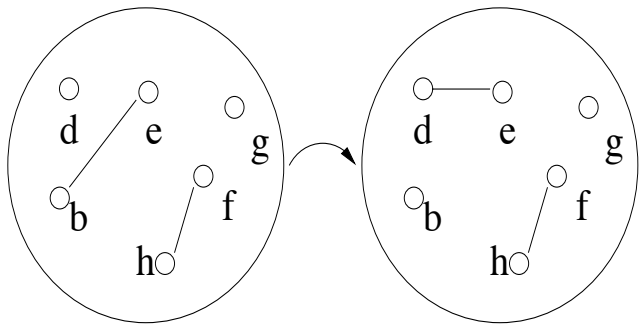
- Let
  $IS1(k) = \bigwedge_{i=1}^{i=k}(\mathcal{P}(s_i) \wedge \mathcal{T}(s_i, s_{i+1})) \wedge \neg\mathcal{P}(s_{k+1})$.
  $IS2(k) = \mathcal{I}(s_1) \wedge \bigwedge_{i=1}^{i=k}(\mathcal{P}(s_i) \wedge \mathcal{T}(s_i, s_{i+1})) \wedge \neg\mathcal{P}(s_{k+1})$.
- Non-termination of InductionSolve can be due to (a) non-termination of SAT solver or (b) unbounded increase of k.
- Halting problem can be expressed as a reachability problem where we can decide the satisfiability of $IS1(k)$ and $IS2(k)$.
- We hence try to identify classes of $\mathcal{P}$, $\mathcal{T}$ and $\mathcal{I}$ for which we can decide $IS1(k)$ and $IS2(k)$.

An Example



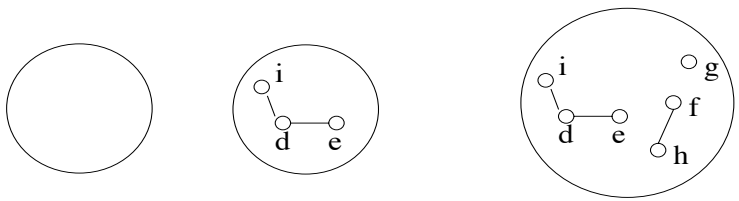
- $\mathcal{T}(s, s') \equiv \exists x, y, z(E(x, y) \wedge \neg E(y, z) \wedge \neg E'(x, y) \wedge E'(y, z))$
  $\mathcal{P}(s) = \forall x, y, z \neg(E(x, y) \wedge E(y, z))$. Then
  $IS1(1) = \mathcal{P}(s) \wedge \mathcal{T}(s, s') \wedge \neg\mathcal{P}(s')$ is true.
- The following sub-graphs (having 3 nodes) also satisfy $\mathcal{T}(s, s')$. Further no matter how you extend them (by adding nodes) the resulting graphs still satisfy $\mathcal{T}(s, s')$.



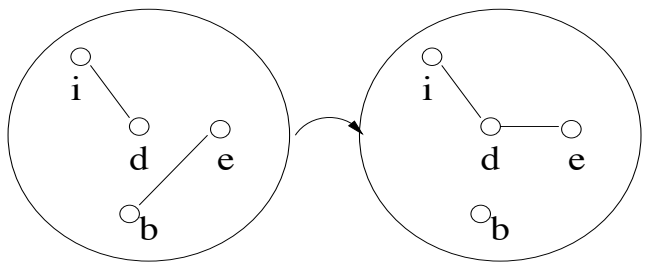


An Example (Contd..)

- The following sub-graphs (having 0 and 3 nodes resp.) also satisfy $\mathcal{P}(s)$ and $\neg\mathcal{P}(s')$. Extending them, $\mathcal{P}(s)$ and $\mathcal{P}(s')$ still hold true.

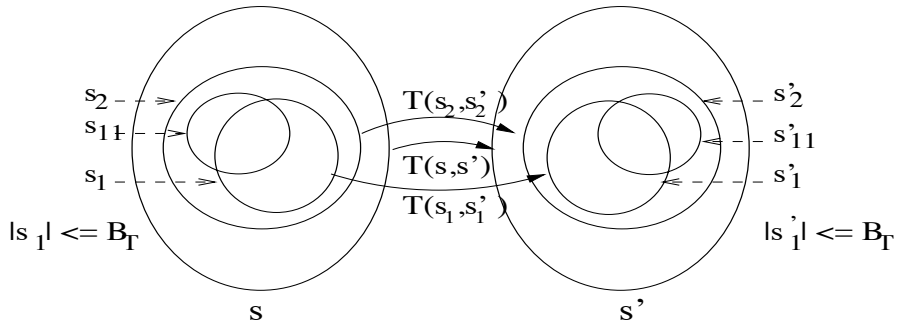


- Putting the above sub-graphs together the following subgraphs having atmost 3 + 0 + 3 = 6 nodes satisfy $IS1(1)$.

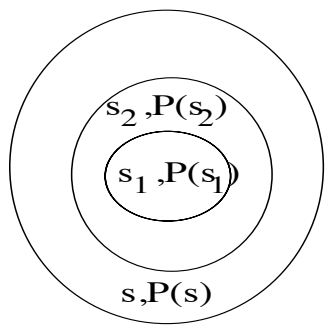


A General Procedure for Deciding $IS1(k)$ and $IS2(k)$

- Suppose $\mathcal{T}(s, s')$ has the following property.

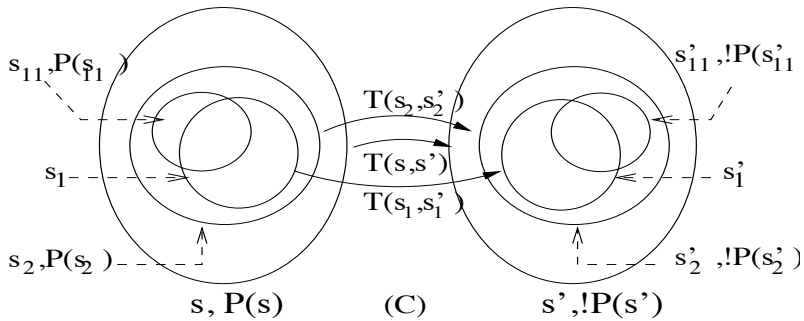


- Suppose $\mathcal{P}(s)$ (and likewise $\neg\mathcal{P}(s)$, $\mathcal{I}(s)$ and $\neg\mathcal{I}(s)$) have the following property.



A General Procedure for Deciding $IS1(k)$ and $IS2(k)$

- Then if $IS1(1)$ has a model, we can construct a bounded (sub)model of size $\mathcal{B} = \mathcal{B}_{\mathcal{T}} + \mathcal{B}_{\mathcal{P}} + \mathcal{B}_{\neg\mathcal{P}}$.



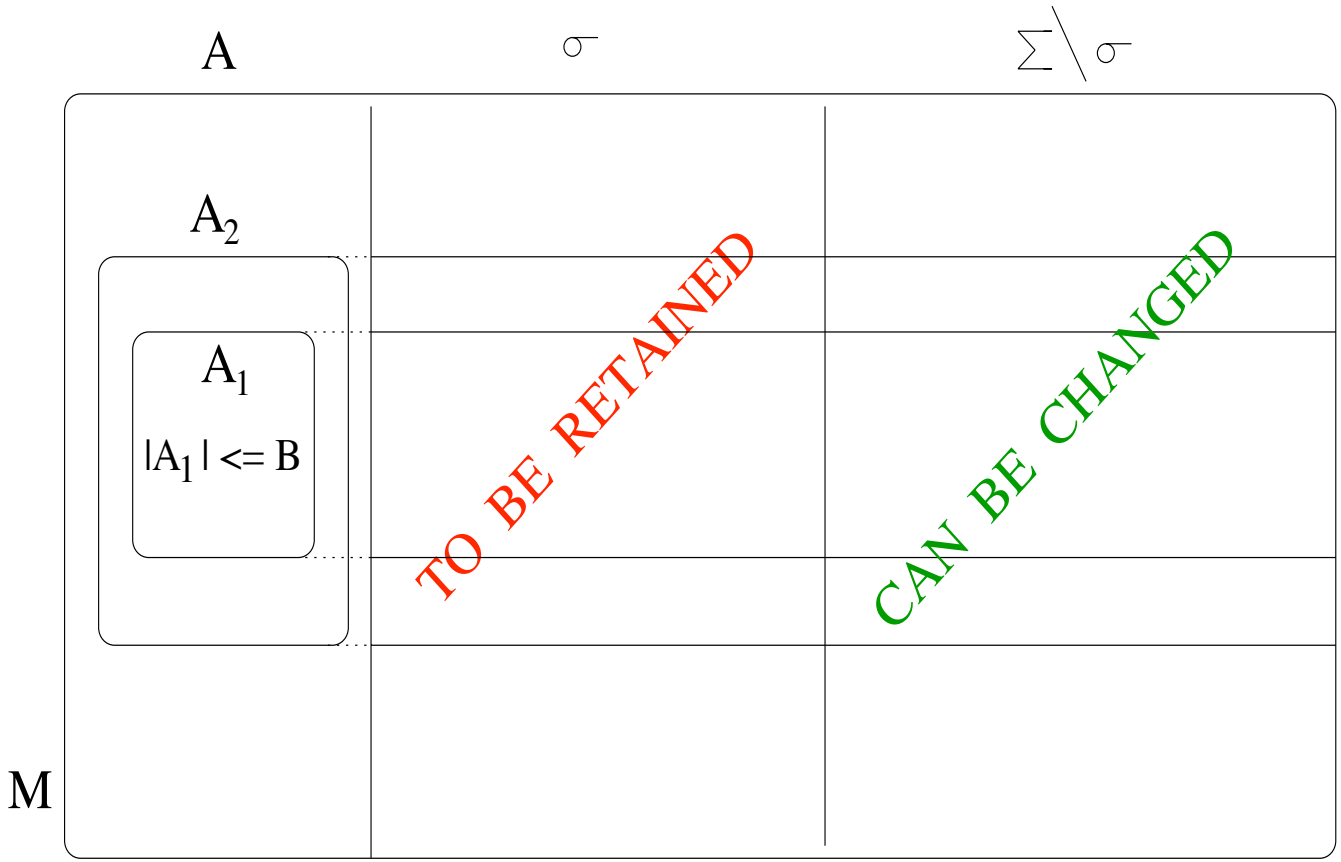
- We can do likewise for $IS1(k)$ and $IS2(k)$ for any k.
- Then for each formula, if it has a model, it has a model of bounded size $\mathcal{B}$. Enumerate all models of size upto $\mathcal{B}$. If you find a model, you are done, else you know there cannot exist a model.

The Extensible Bounded Submodel Property (EBS)

A formula $\varphi(\mathbf{x})$ over Σ is said to satisfy the **Extensible Bounded Submodel** property with respect to $\sigma \subseteq \Sigma$ (denoted as $\varphi(\mathbf{x}) \in \mathbf{EBS}_{\Sigma}(\sigma)$) if there exists a cardinal $\mathcal{B}_{\varphi,\sigma}$ such that for every $\Sigma-$structure M having universe A with $|A| \geq \mathcal{B}_{\varphi,\sigma}$ and for every $\mathbf{a} \in A^{|\mathbf{x}|}$, if $M \models \varphi(\mathbf{a})$ then there exists $A_1 \subseteq A$ such that

1. $\mathbf{a} \in A_1^{|\mathbf{x}|}$
2. $|A_1| \leq \mathcal{B}_{\varphi,\sigma}$
3. For all A_2 such that $A_1 \subseteq A_2 \subseteq A$, if M_2' is the substructure of M generated by A_2, then there exists a $\Sigma-$structure M_2 such that $M_2|_{\sigma} = M_2'|_{\sigma}$ and $M_2 \models \varphi(\mathbf{a})$.

The EBS property pictorially



Its easy to see that for $\sigma_1 \subseteq \sigma_2 \subseteq \Sigma$, $\mathbf{EBS}_\Sigma(\sigma_2) \subseteq \mathbf{EBS}_\Sigma(\sigma_1)$.

Some Examples

- Bernays-Schönfinkel ($\exists^*\forall^*(..)$) is in $\mathbf{EBS}_\Sigma(\Sigma)$. For a sentence φ, $B_{\varphi,\Sigma}$ = No. of existential quantifiers in φ.
- In the example shown earlier, the sentence is
  $\exists x_1, x_2, x_3, y_1, y_2, y_3 \forall z_1, z_2, z_3$
  $(E(x_1, x_2) \wedge \neg E(x_2, x_3) \wedge \neg(E(z_1, z_2) \wedge E(z_2, z_3)) \wedge$
  $\neg E'(x_1, x_2) \wedge E'(x_2, x_3) \wedge E'(y_1, y_2) \wedge E'(y_2, y_3))$
  and hence has bound of 6.
- Löwenheim class (monadic FO) $\in \mathbf{EBS}_\Sigma(\Sigma)$. $B_{\varphi,\Sigma} = k.2^m$ (k = Rank of φ, $m = |\Sigma|$).
- If $\phi = \forall x \exists y P(x, y)$, then $\phi \in \mathbf{EBS}_\Sigma(\emptyset)$.

EBS and other classes of FO

- EBS $\not\to$ bounded submodel property.
  Consider $\varphi = \forall x \exists y P(x, y)$. The infinite chain is a model but there is no bounded submodel of it satisfying φ. Yet $\varphi \in \mathbf{EBS}_\Sigma(\emptyset)$ as seen earlier.
- EBS $\neq$ finite satisfiability
  Let φ_1 express there exists exactly one element and φ_2 express an infinite chain. Then

Finitely sat	In EBS	Eg formula
Yes	Yes	φ_1
Yes	No	$\varphi_1 \vee \varphi_2$
No	Yes	$\varphi_1 \wedge \varphi_2$ (= **False**)
No	No	φ_2

Closure properties of EBS

Let $\varphi_i(\mathbf{x}_i) \in \mathbf{EBS}_{\Sigma_i}(\sigma_i)$ for some $\sigma_i \subseteq \Sigma_i$. Let condition $\mathcal{C} = (\Sigma_1 \cap \Sigma_2 = \sigma_1 \cap \sigma_2)$. Let $Z(\varphi_i)$ denote free variables of φ_i.

1. $\wedge$-Closure: Let $\varphi(\mathbf{x}) = \varphi_1(\mathbf{x}_1) \wedge \varphi_2(\mathbf{x}_2), \Sigma = \Sigma_1 \cup \Sigma_2$. If $\mathcal{C}$ holds, then $\varphi(\mathbf{x}) \in \mathbf{EBS}_{\Sigma}(\sigma_1 \cup \sigma_2) \subseteq \mathcal{EBS}$ with $\mathcal{B}_{\varphi,\sigma_1\cup\sigma_2} = \mathcal{B}_{\varphi_1,\sigma_1} + \mathcal{B}_{\varphi_2,\sigma_2}$.
2. $\vee$-Closure: Let $\varphi(\mathbf{x}) = \varphi_1(\mathbf{x}_1) \vee \varphi_2(\mathbf{x}_2), \Sigma = \Sigma_1 \cup \Sigma_2$. Then $\varphi(\mathbf{x}) \in \mathbf{EBS}_{\Sigma}(\sigma)$ with $\sigma = ((\Sigma_1 - \Sigma_2) \cup \sigma_2) \bigcap ((\Sigma_2 - \Sigma_1) \cup \sigma_1)$, $\mathcal{B}_{\varphi,\sigma} = \mathbf{max}\{\mathcal{B}_{\varphi_1,\sigma_1}, \mathcal{B}_{\varphi_2,\sigma_2}\} + \mathbf{max}(|Z(\varphi_1) \setminus Z(\varphi_2)|, |Z(\varphi_2) \setminus Z(\varphi_1)|)$.
3. $\neg$ -(Non)Closure: $\mathcal{EBS}$ is not closed under negation.
4. $\exists-$Closure: Let $\varphi(\mathbf{x}) = \exists z \varphi_1(\mathbf{x}_1)$ where $z \in Z(\varphi_1)$. Then $\varphi(\mathbf{x}) \in \mathbf{EBS}_{\Sigma_1}(\sigma_1) \subseteq \mathcal{EBS}$ with $\mathcal{B}_{\varphi,\sigma} = \mathcal{B}_{\varphi_1,\sigma_1}$.

A Syntactic Subclass of EBS - Some Terminology

Consider $\varphi(\mathbf{x})$ in prenex normal form with all its variables named uniquely. Let

- $V(\varphi)$ = set of all free variables $\bigcup$ the leftmost $\exists$ quantified variables of φ.
- $AV(\varphi)$ = set of all $\forall$ quantified variables of φ and
- $EV(\varphi)$ = set of all $\exists$ quantified variables of φ except the leftmost ones.

A Syntactic Subclass of EBS - Some Terminology (Contd..)

A predicate P is called

- *free* if each argument of every instance of P in φ is in $V(\varphi)$.
- *universal* if no argument of any instance of P is from $EV(\varphi)$ and atleast one argument of some instance of P is from $AV(\varphi)$.
- *existential* if atleast one argument of some instance of P is from $EV(\varphi)$.
- *mixed* if, for some i, the i^{th} argument of one instance of P is from $AV(\varphi)$ while the i^{th} argument of another instance of P is from $EV(\varphi)$.

A Syntactic Subclass of EBS - Some Terminology (Contd..)

- The *free support set (fss)* of an instance of P in φ is the set of all variables in $V(\varphi)$ appearing as arguments in that instance of P. The *aggregated free support set (afss)* of predicate P is the union of the free support sets of all instances of P in φ.
- The *universal support set (uss)* of an instance of P in φ is the set of all variables of $AV(\varphi)$ appearing as arguments in that instance of P. The *aggregated universal support set (auss)* of P is the union of the universal support sets of all instances of P in φ.

A Syntactic Subclass of EBS - Some Terminology (Contd..)

- The *existential support set (ess)* of an instance of P in φ is the set of all variables of $EV(\varphi)$ appearing as arguments in that instance of P. The *aggregated existential support set (aess)* of P is the union of the existential support sets of all instances of P in φ.
- Two instances of predicate P in $\varphi(\mathbf{x})$ are said to be *distinguishable* with respect to variable v if there is an integer i such that v occurs as the i^{th} argument of one instance but not as the i^{th} argument of the other instance.

An Example

Consider φ given as below.

$\varphi(u,x) = \exists w \forall y \exists z\, P(x,z) \wedge (P(y,z) \vee \neg P(u,w)) \wedge (Q(y) \vee \neg Q(x) \vee S(u)) \vee (R(y,x) \wedge R(u,y)) \wedge (T(y,z) \wedge T(z,w))$

- $V(\varphi) = \{u,x,w\}$, $AV(\varphi) = \{y\}$, $EV(\varphi) = \{z\}$.
- P is existential, Q, R are universal, S is free, T is mixed.
- For P, *fss* of first instance is $\{x\}$, *uss* is $\{\}$ and *ess* is $\{z\}$. For P, *afss* = $\{x,u,w\}$, *auss* = $\{y\}$ and *aess* = $\{z\}$.
- Variable y distinguishes the two instances of Q.

A Syntactic Subclass of EBS - Definition

Let $\varphi(\mathbf{x})$ be a FOL formula in prenex normal form with uniquely named variables and signature Σ. Formula $\varphi(\mathbf{x})$ is said to have **Existentially Distinguishable and Unmixed Predicates** with respect to $\sigma \subseteq \Sigma$ (denoted $\varphi(\mathbf{x}) \in \mathit{EDUP}_{\Sigma}(\sigma)$) if:

1. Every predicate in σ is nullary, unary, free or universal.
2. There is no equality.
3. Every predicate $P \in \Sigma$ with arity ≥ 2 satisfies the following:

   - P is not mixed in $\varphi(\mathbf{x})$.
   - Let P^1 and P^2 be two syntactically distinct instances of P. Let E_U^{σ} be the union of aggregated existential support sets of unary predicates in σ, and $E_{1,2}$ be the union of existential support sets of P^1 and P^2. Then P^1 and P^2 are either distinguishable with respect to every variable in $E_{1,2}$ or with respect to some variable in $E_{1,2} \setminus E_U^{\sigma}$.

An Example

Consider the same example as before.
$\varphi(u,x) = \exists w \forall y \exists z\, P(x,z) \wedge (P(y,z) \vee \neg P(u,w)) \wedge (Q(y) \vee \neg Q(x) \vee S(u)) \vee (R(y,x) \wedge R(u,y)) \wedge (T(y,z) \wedge T(z,w))$.

- $\varphi \notin EDUP_{\Sigma}(\sigma)$ for any σ as T is mixed.
- $\varphi \notin EDUP_{\Sigma}(\sigma)$ also since the second argument of the first two P instances is same i.e. z.
- Suppose the last clause is dropped and the second argument of the first P instance is changed to u. Then if $P \notin \sigma, \varphi \in EDUP_{\Sigma}(\sigma)$ else not.

Some Results on EDUP

Lemma

Let $\varphi(\boldsymbol{x})$ be a formula in prenex normal form with signature Σ in which (a) every predicate of arity ≥ 2 in Σ appears exactly once and (b)there is no equality predicate. Then there exists $\sigma \subseteq \Sigma$ such that $\varphi(\boldsymbol{x}) \in EDUP_{\Sigma}(\sigma)$.

Let *BS* be the Bernay's Schönfinkel class and *L* be the Löwenheim class of FO formulae over Σ.

Lemma

$(BS \cup L) \subseteq EDUP_{\Sigma}(\Sigma)$.

Some Results on EDUP (Contd..)

Lemma

If $L \not\subseteq BS$, *then* $(L \cup BS) \subsetneq EDUP_{\Sigma}(\Sigma)$.

Theorem

Let $\varphi(\boldsymbol{x}) \in EDUP_{\Sigma}(\sigma)$. *Let* m *and* k *be the number of constants and unary predicates, resp. in* Σ. *Let* l *be the number of existential instances of predicates of arity* ≥ 2 *in* $\varphi(\boldsymbol{x})$. *Then* $\varphi(\boldsymbol{x}) \in \boldsymbol{EBS}_{\Sigma}(\sigma)$ *with* $\mathcal{B}_{\varphi,\sigma} = m + |V(\varphi(\boldsymbol{x}))| + |EV(\varphi(\boldsymbol{x})| \cdot 2^{k+l}$.

Conclusion

- We looked at a semantic property called EBS to give us a semi-decision procedure for the reachability problem in infinite state systems.
- We studied the EBS class with regards to its relation with other classes, deciding the membership in the EBS class and its closure properties.
- We then looked at a syntactic subclass of EBS called EDUP which is defined by placing restrictions on the way quantified variables appear as the arguments of predicates and looked at some results concerning this class.
- The EDUP class generalises two well known classes namely Bernays Sch*ö*nfinkel and L*ö*wenheim and is a decidable class.
- We intend to get explore more syntactic subclasses of EBS.