Symbolic Gossip

Joris Galema
Madeleine Gignoux
Djanira Gomes
Wouter Smit

Sunday 2$^{\text{nd}}$ June, 2024

Abstract

We extend the interpretability of output from SMCDEL's Knowledge Scenes for The Gossip Problem, implement the Transparent Gossip Problem using SMCDEL's existing Knowledge Transformer, and write a Simple Knowledge Transformer for computing the Synchronous Gossip Problem efficiently.

Contents

1 Introduction

The Gossip Problem or *Gossip* is the problem of sharing information in a network. Many variants of Gossip exist, each with their own computational challenges. Most notably, a distinction is made between the *Transparent* Gossip Problem - the situation where all agents know which agents exchange information at any update - and the *Synchronous* Gossip Problem, where agents know when an update occurs but not which agents exchange information during that update.

For modelling Gossip, an explicit model checker for Gossip called *GoMoChe* exists [Gat23]. Explicit model checkers are generally less efficient than symbolic ones, which aim to cut down on computation time. GoMoChe too is therefore computationally limited to small examples. On the other hand, a symbolic model checker for dynamic epistemic logic (DEL) called SMCDEL exists, which is much more general than *GoMoChe*. SMCDEL is implemented for both K and $S5$ and contains symbolic representations for various logic problems, including Gossip [Gat18]. However, in terms of Gossip, SMCDEL only covers an encoding of the Synchronous Gossip Problem (in standard S5 DEL), and the implementation of its update function causes the model to blow up in terms of complexity.

A solution to this exponential blowup was proposed in the unpublished master's thesis by [Rei23], in the shape of a *Simple Knowledge Transformer* that should replace the *Classic Knowledge Transformer* from SMCDEL. An existing implementation by [Yuk23] extends SMCDEL to incorporate updates with Simple Transformers, but an instance of this transformer tailored to the Gossip problem wasn't included.

This project expands on SMCDEL's functionality. Section 2 contains a description of the Classic Knowledge Transformer in SMCDEL, and specifically how it is used to model updates to the state in [Gat18]. Next, Section 3 contains a number of functions that provide an interpretation of the current state, which makes the Synchronous Gossip Problem already provided in SMCDEL more user-friendly. Next we create a variant of the Classic Transformer for the transparent variant of the Gossip Problem in Section 4. To conclude our work, Section 5 describes our implementation of the Simple Transformer, which cuts down on the complexity of computing the Synchronous Gossip Problem, with the tradeoff of losing higher-order knowledge. The code of Section 3, 4, and 5 is tested in Subsections B.1, B.2.2, and **??** respectively, and the necessary parts are benchmarked in Section 7.

2 Background

For the language and syntax of Gossip, please refer to [Gat18] (Section 6.6). We discuss how the Gossip Problem is approached in SMCDEL using [Gat18] (in particular, Section 6.6.5 on Symbolic Gossip). For an in-depth explanation, please refer to the aforementioned source.

The Gossip Problem models the flow of information called secrets. At the initial state of the problem, no information has been shared and each agent knows only their own secret. The goal is for the agents to exchange all secrets, which happens through *updates* on the model, which is called a *Knowledge Structure*. The Knowledge Structure and the actual state are described by the *vocabulary* (V), *state law* (θ), and *observations* (O_i for each agent i). The vocabulary V expresses all existing atomic propositions of the form S_ij, where S_ij denotes agent

i knowing agent j's secret. Next, the state law θ describes the possible worlds in the current model. Following the conceptual assumption that all agents are aware of the model they reside in, θ is common knowledge among the agents. Initially, θ states that nobody knows anyone else's secret. Finally, the observations O_i describe which propositional variables agent i observes; following [Gat18], the observations are initially empty for all agents. Throughout the run of the model, propositions are added to the observables, which encode which calls each agent can observe.

For the sake of simplicity, the notions of knowing one's own secret are completely removed. Equation 1 (from [Gat18], page 194) shows the tuple describing the initial Knowledge Structure F_{init}.

$$F_{\text{init}} = (V = \{S_i j \mid i, j \text{ Agents}, i \neq j\}, \theta = \bigwedge_{i \neq j} \neg S_i j, O_i = \emptyset) \tag{1}$$

In order to transform the model after a call happens, we use a Knowledge Transformer. The crux of this paper involves changing the Knowledge Transformer for the Synchronous Gossip Problem provided in SMCDEL to fit our needs.

The Knowledge Transformer explains how the state should change after an update, in this case an arbitrary call. The vocabulary is extended with propositional variables q_{ij}, which express that agent i called agent j. Recalling that we are dealing with the Synchronous Gossip Problem, where agents only know a call occurred, but not which two agents called, we encode this into two laws θ^+ and θ_-, where θ^+ (also: *preconditions* for a call) expresses that exactly one call happens, and θ_- (also: *postconditions* of a call) expresses the conditions under which agent i can learn agent j's secret. Finally, each agent i observes only calls they participate in, which we describe in O_i^+.

In short, the Knowledge Transformer for The Synchronous Gossip Problem is the quintuple $\chi_{\text{call}} = (V^+, \theta^+, V_-, \theta_-, O^+)$ (see [Gat18], page 195 for the exact encoding).

The design of the Knowledge Transformer allows it to encode and check higher-order knowledge, but it also poses a problem in the form blowup. The state law (θ) keeps track of the updates in the model and is itself updated using θ^+ and θ_-. Essentially, the state law after the final update forms a conjunction of the original state law with event laws (θ^+) for each update and `changelaws` (θ_-), such that the validity of a logical formula on a given Knowledge Structure can be evaluated by solely checking if it's implied by the state law.

However, it is possible for an update to create states that previously were excluded by the state law. In order to allow this type of flexibility, each update causes all propositional variables of the form $S_i j$ to be copied and labelled in the state law. For example, suppose Alice learns Bob's secret during update n. Any occurrence of the corresponding proposition $S_a b$ in the state law need to be flagged in update $n + 1$, just in case Alice would *forget* Bob's secret in some future update. A copy of $S_a b$ is added and now exists alongside the flagged version (denoted by $(S_a b)^o$ to indicate that it is an "old" proposition). Even for a small number of agents and calls (say, 4 agents and 3 calls), the blowup of the state law is as such that it's unfeasible to print an example of the representation of the resulting Knowledge Structure.

The possibility of the truth value $S_a b$ to change back to false is an unrealistic hypothetical in Gossip, as in this situation agents aren't modelled to forget any secrets. However, SMCDEL is implemented for a wide range of logical problems, which prevents it from making such assumptions.

The existing implementation in SMCDEL includes optimization functions that discard the redundant propositions (by checking which propositional variables are equivalent), but this optimization is only implemented to be run after running the model and is therefore not optimal.

With this background on how to model Gossip symbolically, we write our own transformer for modelling the transparant variant of The Gossip Problem, implement an adapted optimization that runs in between updates, and a simple transformer based on Daniel Reifsteck's master's thesis.

3 Gossip Scene Investigation

This section explains the functions that we created to make sense of the current state of a given gossip problem, i.e. gossip scene investigation. The functions only work on the unoptimized, Classic Transformer, since the code relies on the exact vocabulary being copied. First of all, the code makes use of the following imports:

```
module Explain where

import SMCDEL.Symbolic.S5
import SMCDEL.Language
import SMCDEL.Other.BDD2Form
import Data.Maybe
```

One remarkable property of the SMCDEL implementation [Gat18] is how the transformer updates the vocabulary by copying all of the secret propositions. This means that in any given transformation, there will be a propositional variable representing a secret S_ij, as well as a copy of said variable $(S_ij)^o$. Moreover, we have propositions for calls q_{ij}. In order to prevent overlap between the several groups of variables, a unique value is computed for each propositional variable. A propositional variable is of the form p_i, where i is generated using one of the following functions ([Gat18]):

```
-- a has the secret of b
hasSof :: Int -> Int -> Int -> Prp
hasSof n a b | a == b    = error "Let's not even talk about that."
             | otherwise = toEnum (n * a + b)

-- a calls b
thisCallProp :: (Int,Int) -> Prp
thisCallProp (i,j) | i < j     = P (100 + 10*i + j)
                   | otherwise = error $ "wrong call: " ++ show (i,j)
```

In order to make the description of a Knowledge Structure human-readable, we defined the following functions to translate the encoded propositions: `prpLibrary` checks whether a proposition denotes a secret, call proposition, or copy of a secret. The function takes the vocabulary as input, as well as the number of agents, and returns the library from which we can decipher propositions in our gossip scene investigation.

```
-- function to decode secrets propositions, takes list of propositions
-- and an amount of agents and returns decoded secrets as strings
secretDecoder ::  [Prp] -> Int -> [String]
secretDecoder [] _ = []
```

```haskell
secretDecoder ((P p):ps) n = ("s"++ show i ++ show j) : secretDecoder ps n
      where (i, j) = (p `quot` n, p `rem` n)

-- function that creates a library (list of tuples) containing translations/decodings
-- for a given list of propositions and amount of agents
-- !!! does not work for transparent transformer, therefore we have a different function
--     for the transparent transformer specifically
prpLibrary :: [Prp] -> Int  -> [(Prp,String)]
prpLibrary prps n = zip prps (prpLibraryHelper prps)
   where
      -- assign the propositions to secrets, calls, and copies of secrets
      -- and decode each with the appropriate decoder
      prpLibraryHelper :: [Prp]  -> [String]
      prpLibraryHelper [] = []
      prpLibraryHelper prps' = a ++ copyDecoder (drop (div (3*n*(n-1)) 2) prps') a "'"
         where
            a = secretDecoder (take (n*(n-1)) prps') n ++ callDecoder 0 (take (div (n*(n-1)
                ) 2) (drop (n*(n-1)) prps'))

      -- decode calls
      callDecoder :: Int -> [Prp] -> [String]
      callDecoder k calls | k >= div (n*(n-1)) 2 = []
                          | null calls = []
                          | otherwise = ("q" ++ show i ++ show j) : callDecoder (k + 1)
                            calls
         where
            (i, j) = getCNums k 0
            getCNums :: Int -> Int -> (Int,Int)
            getCNums k' r'' | (k'+1) < n = (r'',k'+1)
                            | otherwise = getCNums (k'-n+2+r'') (r''+1)

      -- decode copies
      copyDecoder :: [Prp] -> [String] -> String -> [String]
      copyDecoder [] _ _ = []
      copyDecoder props lib r = map (++r) lib ++ copyDecoder (drop (length lib) props) lib
          (r++"'")


prpLibraryTr :: [Prp] -> Int -> [(Int, Int)] -> [(Prp, String)]
prpLibraryTr prps n calls = zip prps (decSec ++ callsNcopies (drop nS prps) calls "'")
   where
      nS = (n-1)*n
      decSec = secretDecoder (take nS prps) n
      -- decode calls and append decoded Secrets primed (copies) recursively
      callsNcopies :: [Prp] -> [(Int, Int)] -> String -> [String]
      callsNcopies [] _ _ = []
      callsNcopies _ [] s = map (++s) decSec
      callsNcopies (_:ps) ((a,b):c) s = ["q"++show a++show b++tail s] ++ map (++s) decSec
          ++ callsNcopies (drop nS ps) c (s++"'")
```

Additionally, we wrote the (unsafe) function `explainPrp`, which takes in a proposition as well as the library, to return its meaning (as String).

```haskell
explainPrp :: Prp -> [(Prp,String)] -> String
explainPrp (P x) prpLib = fromJust (lookup (P x) prpLib)
```

We follow this up with `gsi`, our gossip scene investigation, which takes in a knowledge scene and a sequence f calls in case we use a transparent transformer ('Nothing' for other transformers). The function then uses `explainPrp` to make sense of the vocabulary and observations.

```haskell
-- Gossip Scene Investigation: GSI. ...like the tv show but with less crime and more gossip
   .
-- takes a knowledge scene and a Maybe [(Int,Int)] (Maybe call sequence) which is necessary
    in case
-- of a transparent transformer
gsi :: KnowScene -> Maybe [(Int, Int)] -> IO ()
gsi kns@(KnS voc stl obs, s) calls = do
    putStrLn "Vocabulary: "
    mapM_ (putStrLn . (++) " --  " . \p -> explainPrp p lib) voc
    putStrLn "State Law: "
```

```
    print (ppFormWith (`explainPrp` lib) (formOf stl))
    putStrLn "Observables: "
    mapM_ (putStrLn . (++) " --   " . (\ x -> fst x ++ ":   " ++ show (map (`explainPrp` lib)
          (snd x)) )) obs
    putStrLn "Actual state: "
    if null s then putStrLn " --  Nobody knows about any other secret"
      else
      mapM_ (putStrLn . (++) " --   " . \p -> explainPrp p lib) s
   where
      lib | isNothing calls = prpLibrary voc (length $ agentsOf kns)
          | otherwise = prpLibraryTr voc (length $ agentsOf kns) (fromJust calls)
```

We also have functions specific for the vocabulary (`gsiVoc`), state law (`gsiStLaw`), observables (`gsiObs`) and current state (`gsiState`) which work exactly the same as gsi but show only a specific part of the knowledge scene.

We can then run the following:

```
import SMCDEL.Examples.GossipS5
ghci> gsi (gossipInit 3) Nothing
Vocabulary:
 --   s01
 --   s02
 --   s10
 --   s12
 --   s20
 --   s21
State Law:
"(~s01 & ~s02 & ~s10 & ~s12 & ~s20 & ~s21)"
Observables:
 --   0:   []
 --   1:   []
 --   2:   []
Actual state:
 --   Nobody knows about any other secret

ghci> gsiVoc (doCall (gossipInit 3) (0,1)) Nothing
Vocabulary:
 --   s01
 --   s02
 --   s10
 --   s12
 --   s20
 --   s21
 --   q01
 --   q02
 --   q12
 --   s01'
 --   s02'
 --   s10'
 --   s12'
 --   s20'
 --   s21'

 ghci> gsiState (doCall (gossipInit 3) (0,1)) Nothing
 Actual state:
 --   s01
 --   s10
 --   q01

ghci> gsiObs (doCallTransparent (gossipInit 3) (0,1)) (Just [(0,1)])
Observables:
 --   0:   ["q01"]
 --   1:   ["q01"]
 --   2:   ["q01"]
```

In the future, we hope to also show the law as its BDD (Binary Decision Diagram [1]) using the tool *graphviz*.

[1]A Binary Decision Diagram provides a concise representation of a Boolean formula. SMCDEL uses BDDs

4 Transparent Transformer

This section describes a variant of the Classic Knowledge Transformer that is implemented for the Transparent Gossip Problem. This transformer is tailored to the actual call that happens, which makes sure that whenever a call happens, all agents know this and also know which agents participate.

```
module Transparent where

import SMCDEL.Examples.GossipS5
import SMCDEL.Language
import SMCDEL.Symbolic.S5
```

We chose to adapt the existing function `callTrf` from GossipS5, which is the call transformer for the Synchronous Gossip Problem. Instead of `Int -> KnowTransformer`, the function is now `Int -> Int -> Int -> KnowTransformer`, so that agents a and b are arguments for the transformer for call ab. As in Section 2, we redefine how to update the vocabulary, law, and observations of each agent.

First, the vocabulary V^+ (the `eventprops`), now simply consists of the call between agents a and b. As opposed to the synchronous case, we don't need extra vocabulary to describe all possible calls that could be happening: all agents know exactly which call happens.

The `eventlaw`, θ^+ (which originally stated that only one call happens at a time but not which), is simplified to be the call between agents a and b. The `changelaws`, θ_-, are quite different from those in the Classic Transformer: the conditions for the proposition S_ij to be true after *some* call happens, are simplified to the conditions S_ij to be true after the *actual* call ab happens.

For instance, if i is agent a, then i knows j's secret after call ab if either

1. i knew it already, or
2. j equals b, or
3. b told i the secret of j during their call.

Finally, the `eventobs`, O_i^+ for each agent i, are also simplified to call ab, since there is only one possible event happening and every agent observes it.

```
callTrfTransparent :: Int -> Int -> Int -> KnowTransformer
callTrfTransparent n a b = KnTrf eventprops eventlaw changelaws eventobs where
  thisCallHappens = thisCallProp (a,b)
  -- the only event proposition is the current call
  eventprops = [thisCallHappens]

  -- call ab takes place and no other calls happen
  eventlaw = PrpF thisCallHappens

  changelaws =
  -- i has secret of j
      -- case: i is not a and i is not b: then i can not have learned the secret unless it
          already knew it (has n i j)
    [(hasSof n i j, boolBddOf $ has n i j) | i <- gossipers n, j <- gossipers n, i /= j, i
        /= a, i /= b] ++
      -- case: i is a, j is not b: then i learned the secret if it already knew it, or b
          knew the secret of j
    [(hasSof n a j, boolBddOf $ Disj [ has n a j , has n b j ]) | j <- gossipers n, a /= j,
         b /= j ] ++
      -- case: i is a, j is b: then Top (also: i is b, j is a)
```

for the symbolic evaluation of logic problems.

```
    [(hasSof n a b, boolBddOf Top)] ++ [(hasSof n b a, boolBddOf Top)] ++
      -- case i is b, j is not a: synonymous to above
    [(hasSof n b j, boolBddOf $ Disj [ has n b j , has n a j ]) | j <- gossipers n, a /= j,
         b /= j ]

  eventobs = [(show k, [thisCallHappens]) | k <- gossipers n]
```

Since the transparent transformer has the same type as the synchronous variant, we inherited its update function. The following functions were adapted from the original implementation to perform the transparent update:

```
callTransparent :: Int -> (Int,Int) -> Event
callTransparent n (a,b) = (callTrfTransparent n a b, [thisCallProp (a,b)])

doCallTransparent :: KnowScene -> (Int,Int) -> KnowScene
doCallTransparent start (a,b) = start `update` callTransparent (length $ agentsOf start) (a
    ,b)

afterTransparent :: Int -> [(Int,Int)] -> KnowScene
afterTransparent n = foldl doCallTransparent (gossipInit n)

isSuccessTransparent :: Int -> [(Int,Int)] -> Bool
isSuccessTransparent n cs = evalViaBdd (afterTransparent n cs) (allExperts n)
```

5 Optimization

We will now look at improving the runtime of the synchronous case.

As mentioned before, the classical transformer defined in [Gat18] involves a considerable amount of inserted propositions and extensions of the state law.

This is further worsened by the nature of the gossip problem: both the event propositions (the calls) and the secret atoms grow rapidly as the number of agents increases. Moreover, the statelaw encodes all of the secret atoms.

The route of optimization therefore seems to be in limiting the amount of proposition insertions. We show two methods do that: using a optimization function to trim redundant propositions, and a different notion of transformer that avoids copying alltogether.

5.1 Using the `optimize` function

The SMCDEL library contains an `optimize` function which aims to minimize the size of the knowledge structure by removing redundant propositions. Usually this is run at the end of a sequence of calls, but we will now define a few wrappers to interleave the optimisation step between each individual call.

Simply trimming redundant propositions that were added by the classical transformer could potentially already provide a reasonable speed improvement.

```
doCallOpt :: [Prp] -> KnowScene -> (Int, Int) -> KnowScene
doCallOpt vocab start (a,b) = optimize vocab $
                                start `update` call (length $ agentsOf start) (a,b)

afterOpt :: Int -> [(Int,Int)] -> KnowScene
afterOpt n = foldl (doCallOpt $ vocabOf (gossipInit n)) (gossipInit n)
```

5.2 Simple Transformer

As we have seen, the (classical) implementation of transformer inserts propositions into the vocabulary and modfies the state law, which is suspected to be the main source of computation. We therefore consider a different notion of transformers called *Simple Transformers*, which was introduced by [Rei23]. There is a notion of such transformers with and without factual change. For gossip we will only use the simple transformers with factual change.

The simple transformer is a less expressive transformer that is 'simple' in the sense that it disregards complexities in the knowledge semantics. The benefit of this simplification is that it does not modify the vocabulary or state law, which are precisely the parts of the knowledge structure that grow uncontrollably in the classical case.

The transformer still uses the event propositions in V^+ and the change laws θ_- to determine the factual change V_-, but instead uses that result to modify the state rather than the knowledge structure.

Meanwhile, observables can be mutated similarly to the classical case, with the addition of the notion to remove observables from agents too. However, for Gossip we will not use the observable management and instead only rely on the transformer to compute the factual change.

5.2.1 Simple Initial Knowledge Scene

Due to the limitations in changing the knowledge structure with every update, we must make minimal changes to the initial knowledge scene.

The model is initialized by the `gossipInitSimple` function, which is a modification of the `gossipInit` function part of the Gossip implemenation in SMCDEL `GossipS5` file.

```
-- Initialize a gossip scene for the simple transformer
gossipInitSimple :: Int -> KnowScene
gossipInitSimple n = (KnS vocab law obs, actual) where
    vocab  = [ hasSof n i j | i <- gossipers n, j <- gossipers n, i /= j ]
    law    = boolBddOf Top                                           -- Top
    obs    = [ (show i, allSecretsOf n i) | i <- gossipers n ]       -- observe all
        own secret knowledge
    actual = [ ]

-- Retrieve for some agent x all secret atoms of the form $S_xi$
allSecretsOf :: Int -> Int -> [Prp]
allSecretsOf n x = [ hasSof n x j | j <- gossipers n, j /= x ]
```

The vocabulary `vocab` stays the same and contains all secret atoms from the language, the state law and observables however are modified.

Whereas the state law in `gossipInit` describes the situation in which agents only know their own secrets, this definition is too restrictive for the simple implementation: it prevents the learning of secrets. In order not to exclude any possible later states, we chose a simple state law of $\theta = \top$.

The observables `obs` are slightly different too. While in the classical case these were empty, in the simple transformer we want them to reflect each agent's own secret-knowledge atoms. That is, each agent x can observe the set $\{S_x j \mid j \in Ag \wedge x \neq j\}$ where Ag is the set of all agents.

Conceptually, these observables make sense to be true from the very start: an agent should be aware of what secrets they know themselves.

Analogous to the classic implementation, the state `actual` is initially empty as it describes all true propositions of the form "i knows the secret of agent j". Note specifically that we again ignore the atoms $S_a a$: while agents do know their own secrets, these are not encoded by propositions and therefore not mentioned in the state.

5.2.2 The Simple Transformer for Gossip

We wil now define the transformer itself. The function `CallTrfSimple` is the simple analogue of the classic transformer `callTrf` from [Gat18]. Note that we have a single transformer to execute any of the calls, in order for the semantics to be synchronous.

The event vocabulary V^+ contains again all fresh variables needed to describe the transformation, just like in the classical transformer.

The state law θ_- (`changelaws`) is similarly defined as in the classic transformer, allowing the update to compute the factual change V_- and modify the state

The transformation observables are each agent's own secret atoms, just like the initial state. In the definition of the update function, we will use this set of atoms to mimick "sharing what you know".

```
callTrfSimple :: Int -> SimpleTransformerWithFactual
callTrfSimple n = SimTrfWithF eventprops changelaws changeobs where
    -- helper functions to construct the required formulae
    thisCallHappens (i,j) = PrpF $ thisCallProp (i,j)
    isInCallForm k = Disj $ [ thisCallHappens (i,k) | i <- gossipers n \\ [k], i < k ]
                        ++ [ thisCallHappens (k,j) | j <- gossipers n \\ [k], k < j ]
    allCalls = [ (i,j) | i <- gossipers n, j <- gossipers n, i < j ]

    -- V+ event props stay the same as classic transformer
    eventprops = map thisCallProp allCalls

    -- theta- change law stays same as classic transformer
    changelaws =
      [(hasSof n i j, boolBddOf $              -- after a call, i has the secret of j iff
          Disj [ has n i j                     -- i already knew j, or
               , Conj (map isInCallForm [i,j]) -- i and j are both in the call or
               , Conj [ isInCallForm i         -- i is in the call and there is some k in
                       , Disj [ Conj [ isInCallForm k, has n k j ] -- the call who knew j
                             | k <- gossipers n \\ [j] ] ]
               ])
      | i <- gossipers n, j <- gossipers n, i /= j ]

    -- Change observables are empty as they are not used
    changeobs    = [ (show i, (allSecretsOf n i,[])) | i <- gossipers n ]
```

The following functions are analogues of those in originally defined in SMCDEL's `GossipS5.hs` and instead use the simple transformer.

```
-- construct a a single call event with a simple transformer
simpleCall :: Int -> (Int,Int) -> StwfEvent
simpleCall n (a,b) = (callTrfSimple n, [thisCallProp (a,b)])

-- execute a simple call event
doCallSimple :: KnowScene -> (Int,Int) -> KnowScene
doCallSimple start (a,b) = start `update` simpleCall (length $ agentsOf start) (a,b)

-- execute repeated calls using the simple transformer
afterSimple :: Int -> [(Int, Int)] -> KnowScene
afterSimple n = foldl doCallSimple (gossipInitSimple n)

-- evaluate if the sequence cs is successful for n agents
isSuccessSimple :: Int -> [(Int,Int)] -> Bool
isSuccessSimple n cs = evalViaBdd (afterSimple n cs) (allExperts n)
```

5.2.3 Updates using the Simple Transformer

While the original definition of the Simple Transformer in [Rei23] specifies how the new knowledge scene is constructed, we have to modify it for our Gossip-specific observable management to work as desired.

The following code extends the SMCDEL library, specifically the S5-specific symbolic implementation `SMCDEL.Symbolic.S5` with Simple Transformers with Factual Change.

We limit ourselves to the implementation of only the pointed update. Additionally, we do not extend the newly defined structures for existing SMCDEL functions such as `eval` or `bddOf`, as these extensions are not necessary for our case and should instead be made on the SMCDEL repository directly.

```
{-# LANGUAGE FlexibleInstances, MultiParamTypeClasses, ScopedTypeVariables #-}
{-# LANGUAGE InstanceSigs #-}

module SmpTrfS5 where

{-
- This file is a partial copy Symbolic.S5 of Haitian's fork of SMCDEL
  the file includes definitions for Simple Transformers (SmpTrf).
- The update function for SmpTrf with factual change is specific to Gossip
- NOTE: Due other changes in Haitian's fork and the SMCDEL main repo,
  dynamic operators in formulae do not work.
  Instead update the knowledge structure
-}
```

We first define the new datatype for the simple transformer. The following definitions were written by [Yuk23].

```
{-
    Simple transformer with factual change
-}
data SimpleTransformerWithFactual = SimTrfWithF
  [Prp]                        -- V+ is a set of new variables encoding of a set of events
  [(Prp,Bdd)]                  -- Theta- assigns a formula to each modified variable.
  [(Agent,([Prp],[Prp]))]      -- O+ and O- for each agent
  deriving (Eq,Show)

instance Pointed SimpleTransformerWithFactual State
type StwfEvent = (SimpleTransformerWithFactual,State)
```

While [Yuk23] also implemented the update function as defined by [Rei23], we here modify it to instead work specifically for our case of a Gossip transformation.

```
-- The following instance is modified from Haitian's implementation of the
-- general simple transformer definition
-- It is *only* applicable to synchronous Gossip calls
instance Update KnowScene StwfEvent where
  checks = [haveSameAgents]
  unsafeUpdate kns@(KnS v th obs,s) (SimTrfWithF _ thetaminus trfObs, x) = (newkns,
      newstate) where
    -- gossip helper functions to be able to find the current two agents in the call
    thisCallProp :: (Int,Int) -> Prp
    thisCallProp (i,j) | i < j     = P (100 + 10*i + j)
                       | otherwise = error $ "wrong call: " ++ show (i,j)

    n = length $ agentsOf kns
    gossipers :: [Int]
    gossipers = [0..(n-1)]

    allCalls = [ (i,j) | i <- gossipers, j <- gossipers, i < j ]
    allCallprops = map thisCallProp allCalls
    callPropResolve = zip allCallprops allCalls

    -- the transformation state x contains only 1 call proposition
```

```
inThisCall :: (Int, Int)
inThisCall = callPropResolve ! head x

-- Compute special observable management for Gossip
-- Calling agents get their own original observables O_i plus the secrets that they
    other know
-- which we define by the intersection of the other agent's observables with the (new)
    state
newobs = [ (show i,obs ! show i) | i <- gossipers, i < fst inThisCall ] ++
         [ (show (fst inThisCall) , callerObs ++ intersect newstate calleeTrfObs) ] ++
                    -- caller
         [ (show i,obs ! show i) | i <- gossipers, i > fst inThisCall, i < snd
             inThisCall ] ++
         [ (show (snd inThisCall) , calleeObs ++ intersect newstate callerTrfObs) ] ++
                    -- callee
         [ (show i,obs ! show i) | i <- gossipers, i > snd inThisCall  ] where
             -- determine the O and O^+ a for agents a,b that are calling (caller,
                 callee)
            callerObs :: [Prp]
            callerObs = obs ! show ( fst inThisCall)
            calleeObs :: [Prp]
            calleeObs = obs ! show ( snd inThisCall)
            callerTrfObs :: [Prp]
            callerTrfObs = fst $ trfObs ! show ( fst inThisCall)
            calleeTrfObs :: [Prp]
            calleeTrfObs = fst $ trfObs ! show ( snd inThisCall)

newkns = KnS v th newobs -- keep V and Theta but changes obs
newstate = sort ((s \\ map fst thetaminus) ++ filter (\ p -> bddEval (s ++ x) (
    thetaminus ! p)) (map fst thetaminus))
```

The update function has two elements: determining the new state and changing the obervables. We calculte the new state as defined in [Rei23], but change the observable management to bespecific to the semantics of a gossip call.

In particular, we do not add the O^+ for each agent to their own observables, but add the *other agent's* O^+ to the agent calling with them. This mimicks the symmetric exchange of secrets. We only do so for the specific two agents in the call.

We furthermore intersect O^+ with the (new) state before addng them to an agent's observables. Agents can only share secrets that they actually know, and if they know a secret, they wil remember it. This monotonicty of the atoms means that we can safely share observables that are already true, but not necessarily those that are not true yet. By intersecting with the state, we ensure only the known secrets get exchanged.

This method is a limited implementation of the effects of a call: in reality, more information can be inferred and more secret atoms might become observable to an agent.

It seems from our tests that agents cannot learn knowledge that they should not learn, i.e. make formulae true that should not be. If this is correct, the simple transformer could provide a suitable faster computation for simpler questions. We do note that a mathematical proof of this is required to ascertain such a claim.

6 Testing

We now discuss the results of the test suite written in `Hspec`. As this project relies heavily on the implementation of SMCDEL to execute updates to knowledge scenes, we assume the correctness of its code and only focus on the correctness of the transformer implementations for Gossip, as well as the correctness of the `gsi` function to decode propositions.

In this section we do not show all test cases, and only highlight the most interesting tests. For the full source code, please refer to the appendixB.

6.1 GSI Tests

The GSI suite is tested for correct and decoding of the propositions. Please note that the IO functions are not tested and only the pure functions are.

6.2 Gossip Transformer Test Suite

We developed a set of test cases that verifies the semantics of the gossip problem. The tests can be divided into roughly three sections:

- factual change of secret atoms (call effects)
- direct knowledge effects of agents directly invovled in the call
- inferred knowledge effects of calls that agents were not directly involved in

The factual change is identical regardless of the type of semantics used, which allows the tests for them to be used for all transformers. The knowledge tests moreover assume (at least) synchronous semantics, which conveniently means they hold for the transparent case too. We provide additional knowledge tests that hold only for the transparent semantics, and ascertain their negative result in the synchronous setting.

The 'inferred' knowledge tries to isolate cases where agents should learn about the (effects of) calls that they were not involved in. A typical case is with a synchronous setting of three agents a, b, and c: if the first call (a, b) happens, then c can observe that some call happened due to synchronicity. However, as c knows she was not invovled herself, and knows there are only two other agents, she must therefore conclude that the call was between (a, b). Agent c then knows already that $S_a b \wedge S_b a$ holds, without ever learning this in a gossip call herself.

6.2.1 Bugs in SMCDEL Implementation

Using our test suite we managed to find a bug in the classical transformer as implemented in SMCDEL. In particular the following case fails:

```
it "Knowledge: agent knows knowledge of other agent in same call" $ do
eval (after 4 [(0,1),(1,2)]) (K "2" (has 4 1 0)) `shouldBe` True
it "Knowledge (inferred): third agent infers knowledge of first agent after 2 calls (4
    agents)" $ do
eval (after 4 [(0,1),(1,2)]) (K "2" (has 4 0 1)) `shouldBe` True
```

We observe that the simple transformer implementation of the same semantics is able to satisfy the first test. It does fail the second test, but this should be caused by a limitation in its implementation. The transparent transformer that we defined in 4 satisfies both tests.

6.2.2 Limitations of the Simple transformer

The simple transformer implementation fails all 'inferred' knowledge tests. This makes sense as the only knowledge effects that can happen is when an agent is in a call and their observables are updated. Any other effect taking place, will only be revealed to the agent if they are in a call that shares these secret atoms.

As noted before, this limitation seems to

7 Benchmarks

The primary motivation for using symbolic model checking is to provide faster computation, as explicit model checking in DEL is generally slow even for small examples [Gat18].

We therefore benchmark the runtime of the various implementations and compare them. Comparing the resuls, we can find what parts of the knowledge structure or updates on it cause the slowdown.

We execute three different call sequences, dependent on the number of agents: with a higher number of agents, we use call sequences in which more agents participate. This prevents situations in which a model containing five agents is only tested on a call sequence that concerns only a small subset of those agents, which could skew the results of the tests for models with a large number of agents.

```
module Main where

import Criterion.Main
import SimpleTransformer
import OptimizedTransformer
import Transparent
import SMCDEL.Symbolic.S5
import SMCDEL.Examples.GossipS5
import SMCDEL.Language
import System.Random

{-
    This module benchmarks the various transformers.
    Currently we compare
    - the SimpleTransformer (SmpTrf)
    - the ClassicTransformer in Transparent setting (TnsTrf)
    - the ClassicTransformer using the SMCDEL optimization function (OptTrf)
    - the ClasicTransformer (ClsTrf)
    The program runs updates in various settings (3,4,5 agents and 1,2,3 calls)

    * Running the Benchmark
    To run the benchmark, execute ‘stack bench‘ from the root of the project
-}

-- The call sequences we apply
callsequence :: Int -> [(Int, Int)]
callsequence 3 = [(0,1),(1,2),(1,2),(0,2),(1,2)]
callsequence 4 = [(0,1),(1,2),(0,2),(2,3),(1,3)]
callsequence 5 = [(0,1),(1,2),(0,2),(3,4),(1,4)]
callsequence 15 = concat $ replicate 3 (callsequence 5)
callsequence 25 = concat $ replicate 5 (callsequence 5)
callsequence _ = []

genCallSeqWithAgentsOfLength :: Int -> Int ->
genCallSeqWithAgentsOfLength a n = getStdRandom (randomR (0,a-2))



-- The function we're benchmarking.
```

```haskell
-- Simple Transformer
benchSmpTrf :: Int -> Int -> Bool
benchSmpTrf a c = evalViaBdd (afterSimple a $ take c $ callsequence a) (K "0" $ allExperts
    a)

-- Classic Transformer
benchClsTrf :: Int -> Int -> Bool
benchClsTrf a c = evalViaBdd (after a $ take c $ callsequence a) (K "0" $ allExperts a)

-- Optimized Transformer
benchOptTrf :: Int -> Int -> Bool
benchOptTrf a c = evalViaBdd (afterOpt a $ take c $ callsequence a) (K "0" $ allExperts a)

-- Transparent Transformer
benchTnsTrf :: Int -> Int -> Bool
benchTnsTrf a c = evalViaBdd (afterTransparent a $ take c $ callsequence a) (K "0" $
    allExperts a)
```

```haskell
-- Our benchmark harness.
main :: IO ()
main = defaultMain [
  bgroup "SmpTrf - 3 agents"    [ bench "1 call"   $ whnf (benchSmpTrf 3) 1
                                , bench "3 calls"  $ whnf (benchSmpTrf 3) 3
                                , bench "5 calls"  $ whnf (benchSmpTrf 3) 5
                                ],
  bgroup "SmpTrf - 4 agents"    [ bench "1 call"   $ whnf (benchSmpTrf 4) 1
                                , bench "3 calls"  $ whnf (benchSmpTrf 4) 3
                                , bench "5 calls"  $ whnf (benchSmpTrf 4) 5
                                ],
  bgroup "SmpTrf - 5 agents"    [ bench "1 call"   $ whnf (benchSmpTrf 5) 1
                                , bench "3 calls"  $ whnf (benchSmpTrf 5) 3
                                , bench "5 calls"  $ whnf (benchSmpTrf 5) 5
                                , bench "15 calls" $ whnf (benchSmpTrf 5) 15
                                , bench "25 calls" $ whnf (benchSmpTrf 5) 25
                                ],
  bgroup "SmpTrf - 10 agents"   [ bench " 5 call"   $ whnf (benchSmpTrf 10) 5
                                , bench "15 calls"  $ whnf (benchSmpTrf 10) 15
                                , bench "25 calls"  $ whnf (benchSmpTrf 10) 25
                                ],
  bgroup "TnsTrf - 3 agents"    [ bench "1 call"   $ whnf (benchTnsTrf 3) 1
                                , bench "3 calls"  $ whnf (benchTnsTrf 3) 3
                                , bench "5 calls"  $ whnf (benchTnsTrf 3) 5
                                ],
  bgroup "TnsTrf - 4 agents"    [ bench "1 call"   $ whnf (benchTnsTrf 4) 1
                                , bench "3 calls"  $ whnf (benchTnsTrf 4) 3
                                , bench "5 calls"  $ whnf (benchTnsTrf 4) 5
                                ],
  bgroup "TnsTrf - 5 agents"    [ bench "1 call"   $ whnf (benchTnsTrf 5) 1
                                , bench "3 calls"  $ whnf (benchTnsTrf 5) 3
                                , bench "5 calls"  $ whnf (benchTnsTrf 5) 5
                                ],
  bgroup "OptTrf - 3 agents"    [ bench "1 call"   $ whnf (benchOptTrf 3) 1
                                , bench "3 calls"  $ whnf (benchOptTrf 3) 3
                                , bench "5 calls"  $ whnf (benchOptTrf 3) 5
                                ],
  bgroup "OptTrf - 4 agents"    [ bench "1 call"   $ whnf (benchOptTrf 4) 1
                                , bench "3 calls"  $ whnf (benchOptTrf 4) 3
                                , bench "5 calls"  $ whnf (benchOptTrf 4) 5
                                ],
  bgroup "OptTrf - 5 agents"    [ bench "1 call"   $ whnf (benchOptTrf 5) 1
                                , bench "3 calls"  $ whnf (benchOptTrf 5) 3
                                -- no case for 5 calls as it runs 45+ mins without result
                                ],
  bgroup "ClsTrf - 3 agents"    [ bench "1 call"   $ whnf (benchClsTrf 3) 1
                                , bench "3 calls"  $ whnf (benchClsTrf 3) 3
                                , bench "5 calls"  $ whnf (benchClsTrf 3) 5
                                ],
  bgroup "ClsTrf - 4 agents"    [ bench "1 call"   $ whnf (benchClsTrf 4) 1
                                , bench "3 calls"  $ whnf (benchClsTrf 4) 3
                                , bench "5 calls"  $ whnf (benchClsTrf 4) 5
                                ],
  bgroup "ClsTrf - 5 agents"    [ bench "1 call"   $ whnf (benchClsTrf 5) 1
                                , bench "3 calls"  $ whnf (benchClsTrf 5) 3
```

```
                              , bench "5 calls"  $ whnf (benchClsTrf 5) 5
                              ]
 ]
```

7.1 Benchmarking Results

We compared the performance of the Classic Transformer, the Optimized Classic Transformer, the Transparent variant and the Simple Transformer. The Optimized Transformer timed out at all runs and was therefore not included in the results. The relevant results of the other tests are discussed below.

The benchmarks evaluate the average running time needed to execute call sequences of different lengths, on models containing respectively three, four, and five agents. Below we highlight the results for three and five agents; for a complete documentation, we refer to the Appendix.

Table 1 compares the results on models containing three agents.

Table 1: Call sequences on models containing three agents

Nr. of calls	Classic	Transparent	Simple
1	388.4 μs	146.0 μs	88.29 μs
3	1.308 ms	331.4 μs	99.34 μs
5	1.876 ms	491.2 μs	486.2 μs

To illustrate the differences between the models on larger problems, the following table compares the results on models containing five agents.

Table 2: Call sequences on models containing five agents

Nr. of calls	Classic	Transparent	Simple
1	18.33 ms	477.0 μs	638.0 μs
3	63.01 ms	1.323 ms	2.153 ms
5	12.27 s	1.831 ms	2.096 ms

We see that the differences in performance grow with the number of agents and the length of call sequences: on larger models, the Transparent and Simple implementation are significantly faster than the Classic implementation. This is most apparent in the results for five calls between five agents (see table 2).

8 Conclusion

This project looked into how we can use the SMCDEL library to better understand and model Gossip. To the first point, we wrote `gsi`, our *Gossip Scene Investigation* function, to better understand SMCDEL's Knowledge Scenes as they pertain to The Gossip Problem. To the latter point, we used the existing notion of a Knowledge Transformer in SMCDEL to write a Knowledge Transformer for the Transparent Gossip Problem. Both of these aforementioned processes helped us build an understanding of how SMCDEL approaches Gossip, and specifically what makes it so computationally intensive. With this in mind, we tried using a pre-existing optimize function within SMCDEL's library to reduce complexity, as well as writing our own Simple Transformer, to target the blow up in vocabulary that the Classic Transformer implemented in SMCDEL encrues.

There are two ways we can analyze our work: by considering its speed and accuracy. In Section 7, we explore the first point. The Transparent Transformer and the Simple Transformer both had large improvements on computation time, specifically as the number of calls increased.

On the other hand, the correctness of our code still has room for improvement. We believe knowing the true differences between what information these transformers codify requires mathematics outside the scope of a programming project. However, it is our belief that the Simple Transformer makes *fewer* propositions true than the Classic Transformer, and therefore it doesn't recognize all instances of higher-order knowledge that are satisfied when the same instance of the problem is run on the Classic implementation.

In terms of further work, besides correctness, readability is a big focus. The Gossip Problem is a specific example within the area of DEL, and is therefore quite hard to work with a lack of background knowledge. This is part of the reason we wrote the `gsi` function, and we advise the reader to test its usability by running `main`. However, although we decode the propositional variables and observations, the state law is still a large BDD, and uninterpretable by the user. Future work could be done to make this more user friendly, perhaps by way of the tool *graphviz*.

A Benchmarks

The following benchmarks are most recently produced. To run the benchmarks, run `stack bench` from the root folder.

```
benchmarking SmpTrf - 3 agents/1 call
time                 91.61 us   (84.94 us .. 97.30 us)
                     0.975 R^2   (0.960 R^2 .. 0.988 R^2)
mean                 88.29 us   (85.05 us .. 93.54 us)
std dev              14.18 us   (10.70 us .. 20.56 us)
variance introduced by outliers: 92% (severely inflated)

benchmarking SmpTrf - 3 agents/3 calls
time                 100.8 us   (96.63 us .. 104.8 us)
                     0.982 R^2   (0.973 R^2 .. 0.990 R^2)
mean                 99.34 us   (95.63 us .. 103.9 us)
std dev              13.86 us   (11.42 us .. 17.02 us)
variance introduced by outliers: 90% (severely inflated)

benchmarking SmpTrf - 3 agents/5 calls
time                 475.9 us   (439.2 us .. 513.0 us)
                     0.959 R^2   (0.935 R^2 .. 0.978 R^2)
mean                 486.2 us   (458.0 us .. 514.8 us)
std dev              91.05 us   (76.93 us .. 111.1 us)
variance introduced by outliers: 93% (severely inflated)

benchmarking SmpTrf - 4 agents/1 call
time                 331.5 us   (307.4 us .. 355.1 us)
                     0.947 R^2   (0.900 R^2 .. 0.979 R^2)
mean                 289.8 us   (273.9 us .. 317.2 us)
std dev              66.15 us   (39.68 us .. 111.4 us)
variance introduced by outliers: 95% (severely inflated)

benchmarking SmpTrf - 4 agents/3 calls
time                 1.136 ms   (1.057 ms .. 1.213 ms)
                     0.960 R^2   (0.938 R^2 .. 0.977 R^2)
mean                 995.6 us   (942.0 us .. 1.052 ms)
std dev              174.4 us   (148.5 us .. 210.5 us)
variance introduced by outliers: 89% (severely inflated)

benchmarking SmpTrf - 4 agents/5 calls
time                 784.1 us   (749.8 us .. 847.3 us)
                     0.919 R^2   (0.875 R^2 .. 0.959 R^2)
mean                 976.6 us   (913.5 us .. 1.056 ms)
std dev              234.2 us   (203.3 us .. 267.9 us)
variance introduced by outliers: 94% (severely inflated)

benchmarking SmpTrf - 5 agents/1 call
time                 646.4 us   (633.2 us .. 663.3 us)
                     0.996 R^2   (0.994 R^2 .. 0.999 R^2)
mean                 638.0 us   (630.9 us .. 649.1 us)
std dev              29.30 us   (22.60 us .. 37.87 us)
variance introduced by outliers: 38% (moderately inflated)

benchmarking SmpTrf - 5 agents/3 calls
time                 2.447 ms   (2.187 ms .. 2.754 ms)
                     0.923 R^2   (0.887 R^2 .. 0.962 R^2)
mean                 2.153 ms   (2.035 ms .. 2.316 ms)
std dev              427.8 us   (323.7 us .. 546.3 us)
variance introduced by outliers: 90% (severely inflated)

benchmarking SmpTrf - 5 agents/5 calls
time                 2.167 ms   (2.073 ms .. 2.265 ms)
                     0.982 R^2   (0.968 R^2 .. 0.993 R^2)
mean                 2.096 ms   (2.037 ms .. 2.187 ms)
std dev              234.3 us   (174.3 us .. 380.6 us)
variance introduced by outliers: 74% (severely inflated)

benchmarking ClsTrf - 3 agents/1 call
time                 437.5 us   (404.4 us .. 456.3 us)
                     0.977 R^2   (0.971 R^2 .. 0.985 R^2)
```

```
mean                 388.4 us   (376.8 us .. 402.8 us)
std dev              43.75 us   (36.27 us .. 51.77 us)
variance introduced by outliers: 81% (severely inflated)

benchmarking ClsTrf - 3 agents/3 calls
time                 985.4 us   (957.6 us .. 1.008 ms)
                     0.955 R^2   (0.895 R^2 .. 0.986 R^2)
mean                 1.308 ms   (1.227 ms .. 1.405 ms)
std dev              323.5 us   (260.1 us .. 469.4 us)
variance introduced by outliers: 95% (severely inflated)

benchmarking ClsTrf - 3 agents/5 calls
time                 2.033 ms   (1.924 ms .. 2.171 ms)
                     0.976 R^2   (0.956 R^2 .. 0.992 R^2)
mean                 1.876 ms   (1.834 ms .. 1.961 ms)
std dev              191.9 us   (139.1 us .. 314.8 us)
variance introduced by outliers: 69% (severely inflated)

benchmarking ClsTrf - 4 agents/1 call
time                 2.847 ms   (2.591 ms .. 3.161 ms)
                     0.946 R^2   (0.910 R^2 .. 0.980 R^2)
mean                 2.736 ms   (2.617 ms .. 2.876 ms)
std dev              425.0 us   (357.2 us .. 627.7 us)
variance introduced by outliers: 83% (severely inflated)

benchmarking ClsTrf - 4 agents/3 calls
time                 9.385 ms   (8.941 ms .. 9.773 ms)
                     0.968 R^2   (0.930 R^2 .. 0.988 R^2)
mean                 8.423 ms   (8.039 ms .. 8.900 ms)
std dev              1.189 ms   (876.5 us .. 1.739 ms)
variance introduced by outliers: 71% (severely inflated)

benchmarking ClsTrf - 4 agents/5 calls
time                 12.53 ms   (9.774 ms .. 15.15 ms)
                     0.754 R^2   (0.475 R^2 .. 0.952 R^2)
mean                 19.57 ms   (17.57 ms .. 23.15 ms)
std dev              6.303 ms   (3.938 ms .. 8.712 ms)
variance introduced by outliers: 91% (severely inflated)

benchmarking ClsTrf - 5 agents/1 call
time                 17.66 ms   (12.66 ms .. 23.56 ms)
                     0.740 R^2   (0.583 R^2 .. 0.920 R^2)
mean                 18.33 ms   (16.58 ms .. 21.01 ms)
std dev              4.837 ms   (3.220 ms .. 7.050 ms)
variance introduced by outliers: 86% (severely inflated)

benchmarking ClsTrf - 5 agents/3 calls
time                 37.18 ms   (24.98 ms .. 43.50 ms)
                     0.750 R^2   (0.322 R^2 .. 0.960 R^2)
mean                 63.01 ms   (52.45 ms .. 79.43 ms)
std dev              25.10 ms   (15.74 ms .. 36.58 ms)
variance introduced by outliers: 92% (severely inflated)

benchmarking ClsTrf - 5 agents/5 calls
time                 12.81 s    (12.00 s .. 14.09 s)
                     0.999 R^2   (0.998 R^2 .. 1.000 R^2)
mean                 12.27 s    (12.10 s .. 12.55 s)
std dev              276.2 ms   (33.61 ms .. 351.3 ms)
variance introduced by outliers: 19% (moderately inflated)

benchmarking TnsTrf - 3 agents/1 call
time                 148.0 us   (146.3 us .. 149.8 us)
                     0.999 R^2   (0.998 R^2 .. 0.999 R^2)
mean                 146.0 us   (144.9 us .. 147.1 us)
std dev              3.788 us   (3.073 us .. 4.679 us)
variance introduced by outliers: 21% (moderately inflated)

benchmarking TnsTrf - 3 agents/3 calls
time                 293.6 us   (289.7 us .. 298.3 us)
                     0.991 R^2   (0.983 R^2 .. 0.996 R^2)
mean                 331.4 us   (319.3 us .. 347.0 us)
std dev              48.50 us   (39.34 us .. 63.12 us)
variance introduced by outliers: 89% (severely inflated)
```

```
benchmarking TnsTrf - 3 agents/5 calls
time                 524.9 us   (506.5 us .. 542.4 us)
                     0.986 R^2   (0.973 R^2 .. 0.995 R^2)
mean                 491.2 us   (477.7 us .. 511.9 us)
std dev              52.83 us   (34.29 us .. 87.06 us)
variance introduced by outliers: 79% (severely inflated)

benchmarking TnsTrf - 4 agents/1 call
time                 273.1 us   (255.5 us .. 292.6 us)
                     0.977 R^2   (0.969 R^2 .. 0.990 R^2)
mean                 265.8 us   (259.3 us .. 274.1 us)
std dev              24.61 us   (17.88 us .. 34.30 us)
variance introduced by outliers: 76% (severely inflated)

benchmarking TnsTrf - 4 agents/3 calls
time                 842.4 us   (831.4 us .. 855.0 us)
                     0.998 R^2   (0.996 R^2 .. 0.999 R^2)
mean                 830.4 us   (823.7 us .. 841.1 us)
std dev              26.04 us   (17.67 us .. 44.81 us)
variance introduced by outliers: 22% (moderately inflated)

benchmarking TnsTrf - 4 agents/5 calls
time                 1.193 ms   (1.112 ms .. 1.324 ms)
                     0.942 R^2   (0.907 R^2 .. 0.976 R^2)
mean                 1.433 ms   (1.377 ms .. 1.486 ms)
std dev              194.9 us   (166.4 us .. 230.8 us)
variance introduced by outliers: 82% (severely inflated)

benchmarking TnsTrf - 5 agents/1 call
time                 489.7 us   (467.9 us .. 508.6 us)
                     0.983 R^2   (0.971 R^2 .. 0.992 R^2)
mean                 477.0 us   (462.8 us .. 494.9 us)
std dev              54.69 us   (44.04 us .. 82.83 us)
variance introduced by outliers: 81% (severely inflated)

benchmarking TnsTrf - 5 agents/3 calls
time                 1.299 ms   (1.220 ms .. 1.370 ms)
                     0.979 R^2   (0.969 R^2 .. 0.988 R^2)
mean                 1.323 ms   (1.274 ms .. 1.389 ms)
std dev              192.9 us   (149.3 us .. 254.0 us)
variance introduced by outliers: 84% (severely inflated)

benchmarking TnsTrf - 5 agents/5 calls
time                 1.845 ms   (1.691 ms .. 2.010 ms)
                     0.966 R^2   (0.951 R^2 .. 0.986 R^2)
mean                 1.831 ms   (1.779 ms .. 1.913 ms)
std dev              216.7 us   (164.0 us .. 335.5 us)
variance introduced by outliers: 77% (severely inflated)
```

B Test Suite

B.1 Gossip Scene Investigation Tests

```haskell
module ExplainTestsSpec where

import Explain
import SMCDEL.Examples.GossipS5
import SMCDEL.Language
import SMCDEL.Symbolic.S5
-- import Test.QuickCheck
import Transparent

import Test.Hspec hiding (after)


spec :: Spec
```

```
spec = do
    describe "secret translation: " $ do
        it "single secrets " $ do
            secretDecoder [P (2*0 + 1)] 2 `shouldBe` ["s01"]
            secretDecoder [P (4*2 + 3)] 4 `shouldBe` ["s23"]
            secretDecoder [P (100*50 + 53)] 100 `shouldBe` ["s5053"]
        it "init " $ do
            prpLibrary (hasSofs 1) 1 `shouldBe` []
            prpLibrary (hasSofs 2) 2 `shouldBe` [(P 1, "s01"), (P 2, "s10")]
            prpLibrary (hasSofs 5) 5 `shouldBe` zip (hasSofs 5) (enumS 5)
            prpLibrary (hasSofs 10) 10 `shouldBe` zip (hasSofs 10) (enumS 10)
            prpLibraryTr (hasSofs 1) 1 [] `shouldBe` []
            prpLibraryTr (hasSofs 2) 2 [] `shouldBe` [(P 1, "s01"), (P 2, "s10")]
            prpLibraryTr (hasSofs 5) 5 [] `shouldBe` zip (hasSofs 5) (enumS 5)
            prpLibraryTr (hasSofs 10) 10 [] `shouldBe` zip (hasSofs 10) (enumS 10)
        it "synchronous calls: " $ do
            length (prpLibrary (callsVoc 3 [(0,1)]) 3) `shouldBe` 15
            length (prpLibrary (callsVoc 3 [(0,1), (1,2)]) 3) `shouldBe` 24
            length (prpLibrary (callsVoc 10 [(0,1), (1,2), (2,5), (7,8), (1,9)]) 10) `
                shouldBe` 765
        it "transparent calls: " $ do
            length (prpLibraryTr (callsVoc' 3 [(0,1)]) 3 [(0,1)]) `shouldBe` 13
            length (prpLibraryTr (callsVoc' 3 [(0,1), (1,2)]) 3 [(0,1), (1,2)]) `shouldBe`
                20
            length (prpLibraryTr (callsVoc' 10 [(0,1), (1,2), (2,5), (7,8), (1,9)]) 10
                [(0,1), (1,2), (2,5), (7,8), (1,9)]) `shouldBe` 545
          where
            hasSofs :: Int -> [Prp]
            hasSofs n = [ hasSof n i j | i <- gossipers n, j <- gossipers n, i /= j ]
            enumS :: Int -> [String]
            enumS n = ["s"++ show i ++ show j | i <- gossipers n, j <- gossipers n, i /= j
                ]
            callsVoc :: Int -> [(Int, Int)] -> [Prp]
            callsVoc n sequ = v
                where
                    (KnS v _ _, _) = after n sequ
            callsVoc' :: Int -> [(Int, Int)] -> [Prp]
            callsVoc' n sequ = v
                where
                    (KnS v _ _, _) = afterTransparent n sequ
```

B.2 Transformer Tests

We use the following functions (previously defined in [Gat18]) concerning experts[2], which define the formulas "agent a is an expert" and "all agents are experts".

```
    expert :: Int -> Int -> Form
    expert n a = Conj [ PrpF (hasSof n a b) | b <- gossipers n, a /= b ]

    allExperts :: Int -> Form
    allExperts n = Conj [ expert n a | a <- gossipers n ]

    isSuccess :: Int -> [(Int,Int)] -> Bool
    isSuccess n cs = evalViaBdd (after n cs) (allExperts n)

    isSuccessTransparent :: Int -> [(Int,Int)] -> Bool
    isSuccessTransparent n cs = evalViaBdd (afterTransparent n cs) (allExperts n)

    isSuccessSimple :: Int -> [(Int,Int)] -> Bool
    isSuccessSimple n cs = evalViaBdd (afterSimple n cs) (allExperts n)
```

B.2.1 Classic Transformer Tests

[2] An expert is an agent who knows all secrets, that is, `expert n a` is defined as $\bigwedge\{S_a b \mid b \in [1, ..., n]\}$

```haskell
module ClassicTransformerSpec where

import Test.Hspec hiding ( after )
import SMCDEL.Examples.GossipS5
import SMCDEL.Symbolic.S5
import SMCDEL.Language

spec :: Spec
spec = do
        -- Secret exchange tests (hold for sync and transparent)
        it "Secrets: all are experts after the correct call sequence" $ do
            isSuccess 3 [(0,1),(1,2),(0,2)] `shouldBe` True
        it "Secrets: call shares secrets between agents" $ do
            eval (after 4 [(0,1)]) (Conj [has 4 1 0, has 4 0 1]) `shouldBe` True
        it "Secrets: secrets from first call get exchanged to second call" $ do
            eval (after 4 [(0,1),(1,2)]) (has 4 2 0) `shouldBe` True
        it "Secrets: agent of first call does not learn secrets from second call" $ do
            eval (after 4 [(0,1),(1,2)]) (has 4 0 2) `shouldBe` False
        it "Secrets: no faulty experts" $ do
            eval (after 3 [(0,1)]) (Disj [expert 3 i | i <- [0..2]]) `shouldBe` False

        -- Tests about more direct knowledge
        it "Knowledge: initial knowledge of own secret atoms" $ do
            eval (gossipInit 3) (K "0" (Neg (has 3 0 1))) `shouldBe` True
        it "Knowledge: agent knows callee knows their secret after call" $ do
            eval (after 4 [(0,1),(1,2)]) (K "2" (has 4 1 2)) `shouldBe` True
        it "Knowledge: agent knows knowledge of other agent in same call" $ do
            eval (after 4 [(0,1),(1,2)]) (K "2" (has 4 1 0)) `shouldBe` True
        it "Knowledge: all agents know that all are experts after the explicit call
            sequence" $ do
            eval (after 3 [(0,1),(1,2),(0,2),(0,1),(1,2),(0,2)]) (Conj [ K (show i) (
                allExperts 3)
                                                                       | i <- [(0::Int)..2] ]) `
                                                                           shouldBe` True

        -- Tests about inferred knowledge
        it "Knowledge (inferred): initial inferred knowledge of other's secret atoms" $ do
            eval (gossipInit 3) (K "0" (Neg (has 3 1 0))) `shouldBe` True
        it "Knowledge (inferred): third agent infers knowledge of first agent after 2 calls
             (4 agents)" $ do
            eval (after 4 [(0,1),(1,2)]) (K "2" (has 4 0 1)) `shouldBe` True
        it "Knowledge (inferred): non-involed knows what call happened (3 agents)" $ do
            eval (after 3 [(0,1)]) (K "2" (has 3 0 1)) `shouldBe` True
        it "Knowledge (inferred): agents can reason about the limits of other agents'
            knowledge" $ do
            eval (after 3 [(0,1)]) (K "0" (Neg (has 3 2 1))) `shouldBe` True
        it "Knowledge (inferred): all agents infer they are all experts after minimal call
            sequence (3 agents)" $ do
            eval (after 3 [(0,1),(1,2),(0,2)]) (Conj [K (show i) (allExperts 3)
                                                                       | i <- [(0::Int)..2]]) `
                                                                           shouldBe` True

        -- transparent-specific knowledge
        it "Knowledge (transparent): call is observed by other agents should fail" $ do
            eval (after 4 [(0,1)]) (K "2" (has 3 0 1)) `shouldBe` False
        it "Knowledge (transparent): call sequence is observed by non-involed agents should
             fail" $ do
            eval (after 4 [(0,1),(1,2)]) (K "3" (has 3 2 0)) `shouldBe` False
```

B.2.2 Transparent Transformer Tests

```haskell
module TransparentTransformerSpec where

import Test.Hspec hiding ( after )
import SMCDEL.Examples.GossipS5
import SMCDEL.Language
import SMCDEL.Symbolic.S5
import Transparent (afterTransparent, isSuccessTransparent)
```

```haskell
spec :: Spec
spec = do
        -- Secret exchange tests (hold for sync and transparent)
        it "Secrets: all are experts after the correct call sequence" $ do
            isSuccessTransparent 3 [(0,1),(1,2),(0,2)] `shouldBe` True
        it "Secrets: call shares secrets between agents" $ do
            eval (afterTransparent 4 [(0,1)]) (Conj [has 4 1 0, has 4 0 1]) `shouldBe` True
        it "Secrets: secrets from first call get exchanged to second call" $ do
            eval (afterTransparent 4 [(0,1),(1,2)]) (has 4 2 0) `shouldBe` True
        it "Secrets: agent of first call does not learn secrets from second call" $ do
            eval (afterTransparent 4 [(0,1),(1,2)]) (has 4 0 2) `shouldBe` False
        it "Secrets: no faulty experts" $ do
            eval (afterTransparent 3 [(0,1)]) (Disj [expert 3 i | i <- [0..2]]) `shouldBe`
                False

        -- Tests about more direct knowledge
        it "Knowledge: initial knowledge of own secret atoms" $ do
            eval (gossipInit 3) (K "0" (Neg (has 3 0 1))) `shouldBe` True
        it "Knowledge: agent knows callee knows their secret after call" $ do
            eval (afterTransparent 4 [(0,1),(1,2)]) (K "2" (has 4 1 2)) `shouldBe` True
        it "Knowledge: agent knows knowledge of other agent in same call" $ do
            eval (afterTransparent 4 [(0,1),(1,2)]) (K "2" (has 4 1 0)) `shouldBe` True
        it "Knowledge: all agents know that all are experts after the explicit call
            sequence" $ do
            eval (afterTransparent 3 [(0,1),(1,2),(0,2),(0,1),(1,2),(0,2)]) (Conj [ K (show
                 i) (allExperts 3)
                                                            | i <- [(0::Int)..2] ]) `
                                                                shouldBe` True

        -- Tests about inferred knowledge
        it "Knowledge (inferred): initial inferred knowledge of other's secret atoms" $ do
            eval (gossipInit 3) (K "0" (Neg (has 3 1 0))) `shouldBe` True
        it "Knowledge (inferred): third agent infers knowledge of first agent after 2 calls
             (4 agents)" $ do
            eval (afterTransparent 4 [(0,1),(1,2)]) (K "2" (has 4 0 1)) `shouldBe` True
        it "Knowledge (inferred): non-involed knows what call happened (3 agents)" $ do
            eval (afterTransparent 3 [(0,1)]) (K "2" (has 3 0 1)) `shouldBe` True
        it "Knowledge (inferred): agents can reason about the limits of other agents'
            knowledge" $ do
            eval (afterTransparent 3 [(0,1)]) (K "0" (Neg (has 3 2 1))) `shouldBe` True
        it "Knowledge (inferred): all agents infer they are all experts after minimal call
            sequence (3 agents)" $ do
            eval (afterTransparent 3 [(0,1),(1,2),(0,2)]) (Conj [K (show i) (allExperts 3)
                                                            | i <- [(0::Int)..2]]) `
                                                                shouldBe` True

        -- transparent-specific knowledge
        it "Knowledge (transparent): call is observed by other agents" $ do
            eval (afterTransparent 4 [(0,1)]) (K "2" (has 3 0 1)) `shouldBe` True
        it "Knowledge (transparent): call sequence is observed by non-involed agents" $ do
            eval (afterTransparent 4 [(0,1),(1,2)]) (K "3" (has 3 2 0)) `shouldBe` True
```

B.2.3 Simple Transformer Tests

```haskell
module SimpleTransformerSpec where

import SimpleTransformer

import Test.Hspec hiding ( after )
import SMCDEL.Examples.GossipS5
import SMCDEL.Symbolic.S5
import SMCDEL.Language


spec :: Spec
spec = do
        -- Secret exchange tests (hold for sync and transparent)
        it "Secrets: all are experts after the correct call sequence" $ do
            isSuccessSimple 3 [(0,1),(1,2),(0,2)] `shouldBe` True
```

```haskell
    it "Secrets: call shares secrets between agents" $ do
        eval (afterSimple 4 [(0,1)]) (Conj [has 4 1 0, has 4 0 1]) `shouldBe` True
    it "Secrets: secrets from first call get exchanged to second call" $ do
        eval (afterSimple 4 [(0,1),(1,2)]) (has 4 2 0) `shouldBe` True
    it "Secrets: agent of first call does not learn secrets from second call" $ do
        eval (afterSimple 4 [(0,1),(1,2)]) (has 4 0 2) `shouldBe` False
    it "Secrets: no faulty experts" $ do
        eval (afterSimple 3 [(0,1)]) (Disj [expert 3 i | i <- [0..2]]) `shouldBe` False

    -- Tests about more direct knowledge
    it "Knowledge: initial knowledge of own secret atoms" $ do
        eval (gossipInitSimple 3) (K "0" (Neg (has 3 0 1))) `shouldBe` True
    it "Knowledge: agent knows callee knows their secret after call" $ do
        eval (afterSimple 4 [(0,1),(1,2)]) (K "2" (has 4 1 2)) `shouldBe` True
    it "Knowledge: agent knows knowledge of other agent in same call" $ do
        eval (afterSimple 4 [(0,1),(1,2)]) (K "2" (has 4 1 0)) `shouldBe` True
    it "Knowledge: all agents know that all are experts after the explicit call
        sequence" $ do
        eval (afterSimple 3 [(0,1),(1,2),(0,2),(0,1),(1,2),(0,2)]) (Conj [ K (show i) (
            allExperts 3)
                                                               | i <- [(0::Int)..2] ]) `
                                                                   shouldBe` True

    -- Tests about inferred knowledge
    it "Knowledge (inferred): initial inferred knowledge of other's secret atoms" $ do
        eval (gossipInitSimple 3) (K "0" (Neg (has 3 1 0))) `shouldBe` True
    it "Knowledge (inferred): third agent infers knowledge of first agent after 2 calls
         (4 agents)" $ do
        eval (afterSimple 4 [(0,1),(1,2)]) (K "2" (has 4 0 1)) `shouldBe` True
    it "Knowledge (inferred): non-involed knows what call happened (3 agents)" $ do
        eval (afterSimple 3 [(0,1)]) (K "2" (has 3 0 1)) `shouldBe` True
    it "Knowledge (inferred): agents can reason about the limits of other agents'
        knowledge" $ do
        eval (afterSimple 3 [(0,1)]) (K "0" (Neg (has 3 2 1))) `shouldBe` True
    it "Knowledge (inferred): all agents infer they are all experts after minimal call
        sequence (3 agents)" $ do
        eval (afterSimple 3 [(0,1),(1,2),(0,2)]) (Conj [K (show i) (allExperts 3)
                                                               | i <- [(0::Int)..2]]) `
                                                                   shouldBe` True

    -- transparent-specific knowledge
    it "Knowledge (transparent): call is observed by other agents should fail" $ do
        eval (afterSimple 4 [(0,1)]) (K "2" (has 3 0 1)) `shouldBe` False
    it "Knowledge (transparent): call sequence is observed by non-involed agents should
         fail" $ do
        eval (afterSimple 4 [(0,1),(1,2)]) (K "3" (has 3 2 0)) `shouldBe` False
```

References

[Gat18] Malvin Gattinger. *New Directions in Model Checking Dynamic Epistemic Logic*. PhD thesis, University of Amsterdam, 2018.

[Gat23] Malvin Gattinger. GoMoChe-gossip model checking. *Branch async from*, 1, 2023.

[Rei23] Daniel Reifsteck. Comparing state representations for del planning (not public). Master's thesis, University of Freiburg, April 2023.

[Yuk23] Haitian Yuki. SMCDEL-Hanabi. unpublished code / private git repository, 2023.