**Application**: TPC-C

**Txn**: do\_new\_order

**Inv**: O\_OL\_CNT = [the number of rows in the ORDER-LINE table for the corresponding order]

**Similar Invariants**:

* sum(O\_OL\_CNT) = [number of rows in the ORDER-LINE table for this district]

**Inv Type**: Foreign Key(1:n)

**Contract (Initial):**

No contract.

**Counter Example (if SAT)**:

Order\_Add effect of current txn visible to invariant’s Order\_Get but

Orderline\_Add effect of current txn not visible to invariant’s Orderline\_Get. (Lost Update)

**Contract**:

f12 a b c d =

[oper(a)=oadd ^ oper(b)=oladd ^ oper(c)=oget ^ oper(d)=olget ^

so(a,b) ^ so(c,d) ^ sameobj(a,c) ^ sameobj(b,d)]

=>

(vis(b,d) ⬄ vis(a,c))

**Counter Example (if SAT)**:

Concurrent Order\_Add effect with same order id, warehouse id and district id visible to invariant. (Concurrent Update)

**Contract**:

f12' a b =

[o\_id(a)=o\_id(b) ^ o\_d\_id(a)=o\_d\_id(b) ^ o\_w\_id(a)=o\_w\_id(b)]

=>

a=b

**Counter Example (if SAT)**:

UNSAT

**Max k for which SAT occurred:** 10

**Time to find counter example:** 9.64s

**Max k verified in 1 hr:** 17

**BMC Time for k=15:** 541.44s

**Application**: TPC-C

**Txn**: do\_new\_order

**Inv**: D\_NEXT\_O\_ID - 1 = max(O\_ID)

**Similar Invariants**:

* max(O\_ID) = max(NO\_O\_ID), D\_NEXT\_O\_ID – 1= max(NO\_O\_ID),
* max(NO\_O\_ID) - min(NO\_O\_ID) + 1 = [number of rows in the NEW-ORDER table for this district]

**Inv Type**: Unique Sequential ID + Foreign key (1:1)

**Contract (Initial):**

No contract.

**Counter Example (if SAT)**:

District\_IncNextOid effect of current txn visible to invariant’s District\_Get but Order\_Add effect of current txn not visible to invariant’s Order\_Get. (Lost update)

**Contract**:

f11 a b c d =

[oper(a)= dincnoid ^ oper(b)=oadd ^ oper(c)=dget ^ oper(d)=oget ^

so(a,b) ^ so(c,d) ^ sameobj(a,c) ^ sameobj(b,d)]

=>

(vis(b,d) ⬄ vis(a,c))

**Counter Example (if SAT)**:

Concurrent District\_IncNextOid visible to invariant but not to current txn (Concurrent update)

**Contract:**

f11' a b =

[oper(a)=dincnoid ^ oper(b)=dget ^ currtxn(b) ^ sameobj(a,b)]

=>

sametxn(a,b) v vis(a,b)

**Counter Example (if SAT)**:

Concurrent District\_IncNextOid visible to current txn but not to invariant. (Concurrent update)

**Contract (Corrected Version of previous contract):**

f11' a b =

[oper(a)=dincnoid ^ oper(b)=dget ^ sameobj(a,b)]

=>

sametxn(a,b) v vis(a,b)

**Counter Example (if SAT)**:

UNSAT

**Max k for which SAT occurred:** 10

**Time to find counter example:** 9.74s

**Max k verified in 1 hr:** 17

**BMC Time for k=15:** 7m 4s

**Application**: TPC-C

**Txn**: do\_payment

**Inv**: W\_YTD = sum(H\_AMOUNT)

**Similar Invariants:**

* D\_YTD = sum(H\_AMOUNT),
* W\_YTD = sum(D\_YTD),

**Inv Type**: Foreign Key (1:1)

**Contract (Initial):**

No contract

**Counter Example (if SAT)**:

Current txn’s History\_Append effect is visible to invariant’s History\_Get but Current txn’s Warehouse\_AddYtd is not visible to invariant’s Warehouse\_Get. (Lost update)

**Contract:**

f23 a b c d =

[oper(a)=waddytd ^ oper(b)=hadd ^ oper(c)=wget ^ oper(d)=hget ^

so(a,b) ^ so(c,d) ^ sameobj(a,c) ^ sameobj(b,d)]

=>

(vis(b,d) ⬄ vis(a,c))

**Counter Example (if SAT)**: UNSAT

**Max k for which SAT occurred:** 5

**Time to find counter example:** 1.67s

**BMC Time for k=15:** 37m 4s

**Max k verified in 1 hr:** 16

**Application**: TPC-C

**Txn**: combination of do\_payment & do\_delivery

**Inv**: C\_BALANCE = sum(OL\_AMOUNT) - sum(H\_AMOUNT)

**Similar Invariants**:

* C\_BALANCE + C\_YTD\_PAYMENT = sum(OL\_AMOUNT)

**Inv Type**: Foreign Key (1:1, Multi transaction)

**do\_payment**

**Contract (Initial):**

No contract

**Counter Example (if SAT)**:

History\_Append of current txn is visible to History\_Get of invariant but the corresponding effects on Customer table is not visible to invariant. (Lost Update)

**Contract:**

f31 a b c d =

[oper(a)=caddbal ^ oper(b)=hadd ^ oper(c)=cget ^ oper(d)=hget ^

so(a,b) ^ so(c,d) ^ sameobj(a,c) ^ sameobj(b,d)]

=>

vis(b,d) ⬄ vis(a,c)

**Counter Example (if SAT)**:

UNSAT

**Max k for which SAT occurred:** 7

**Time to find counter example:** 3.28s

**BMC time for k=15:** 17m 23s

**Max k verified in 1 hr:** 15

**do\_delivery**

**Counter Example (if SAT):**

Order\_Add effect is visible to currtxn and invariant’s Order\_Get but the corresponding Orderline\_Add is only visible to curr txn. (Lost Update)

**Contract:**

f31' a b c d =

[oper(a)=oadd;oper(b)=oladd;oid(a)=olid(b);oper(c)=oget;

oper(d)@=olget;so(d,c)] =>

[vis(a,c) ⬄ vis(b,d)]

**Counter Example (if SAT):**

Order\_Add and Orderline\_Add are visible only to currtxn but not to inv. (Lost Updates)

**Contract (Corrected previous contract):**

let f31' a b c d e f =

mk\_and [oper(a)@=oadd;

oper(b)@=oladd;

(mk\_app oid [a]) @= (mk\_app olid [b]);

oper(c)@=oget;

oper(d)@=olget;

so(c,d);

currtxn(c);

sametxn(c,d);

oper(e)@=olget;

oper(f)@=oget;

so(e,f);

mk\_not(currtxn(e));

sametxn(e,f)] @=> (mk\_and [vis(a,c);vis(b,d)] @=>

mk\_and [vis(a,f);vis(b,e)])

**Counter Example (if SAT):**

Concurrent Customer\_Addbal with same customer id, warehouse id, district id visible to inv. (Concurrent update)

**Contract:**

let f31'' a b = mk\_and

[(mk\_app cid [a]) @= (mk\_app cid [b]);

(mk\_app cdid [a]) @= (mk\_app cdid [b]);

(mk\_app cwid [a]) @= (mk\_app cwid [b])] @=> (a@=b)

**Counter Example (if SAT):**

Order\_Add and Orderline\_Add are visible only to inv but not to currtxn. (Lost updates)

**Contract (Corrected previous contract):**

let f31' a b c d e f =

mk\_and [oper(a)@=oadd;

oper(b)@=oladd;

(mk\_app oid [a]) @= (mk\_app olid [b]);

oper(c)@=oget;

oper(d)@=olget;

so(c,d);

currtxn(c);

sametxn(c,d);

oper(e)@=olget;

oper(f)@=oget;

so(e,f);

mk\_not(currtxn(e));

sametxn(e,f)] @=> mk\_and [vis(a,c);vis(b,d)] @<=>

mk\_and [vis(a,f);vis(b,e)]

**Counter Example (if SAT):**

UNSAT

**Max k for which SAT occurred:** 10

**Time to find counter example:** 51.79s

**Max k verified in 1 hr:** 13 (43 min)

**BMC Time for k=15:** 5hrs 53 min

**Application**: TPC-C

**Txn**: do\_delivery

**Inv:** For any row in the ORDER-LINE table, OL\_DELIVERY\_D is set to a null date/time if and only if the corresponding row in the ORDER table has O\_CARRIER\_ID set to a null value.

**Similar Invariants:**

* For any row in the ORDER table, O\_CARRIER\_ID is set to a null value if and only if there is a corresponding row in the NEW-ORDER table.

**Inv type:** Foreign Key (1:1)

**Contract (Initial):**

No contract

**Counter Example (if SAT):**

The current txn’s Orderline\_SetDeliveryDate is visible to the invariant but the corresponding Order\_SetCarrierID is not visible. (Lost Update)

**Contract:**

let f41 a b c d =

mk\_and [oper(a)@=osetcarrier;

oper(b)@=olsetdel;

oper(c)@=oget;

oper(d)@=olget;

so(a,b);

so(c,d);

sameobj(a,c);

sameobj(b,d)] @=> (vis(b,d) @<=> vis(a,c))

**Counter Example (if SAT):**

UNSAT

**Max k for which SAT occurred:** 8

**Time to find counter example:** 4.37s

**Application**: Shopping cart

**Txn**: do\_addItemsToCart

**Inv**: When a customer is checking out, the quantities of the remaining stock of the corresponding items in the inventory should be >=0.

**Inv Type**: Attribute !<

**Contract (Initial):**

No contract

**Counter Example (if SAT):**

There exists a concurrent Item\_RemoveFromStock effect not visible to the current txn (do\_addItemToCart). (Concurrent update)

**Contract:**

let i1 a b =

mk\_and [oper(a) @= item\_rm;

notsametxn(a,b);

currtxn(b)] @=> vis(a, b)

**Counter Example (if SAT):**

There exists an Item\_AddItemToStock effect that is visible to the current txn, that is not visible to the invariant. (Lost update)

**Contract:**

let g1 a b c d =

mk\_and [oper(a) @= item\_add; oper(b) @= item\_get;

oper(c) @= item\_rm; so(b,c);

txn(b) @= add;

sametxn(b,c);

oper(d) @= item\_get;

vis(a,b) ; vis(c,d); sameobj(a,d)] @=> vis(a,d)

**Counter Example (if SAT):**

The qty of items added to the cart is negative.

**Contract:**

let h a = (mk\_app qty [a]) @>= (mk\_numeral\_i 0)

**Counter Example (if SAT):**

UNSAT

**Max k for which SAT occurred:** 6

**Time to find counter example:** 1.05s

**Application**: Shopping cart

**Txn**: do\_removeItemsFromCart

**Inv**: When a customer is checking out, the quantities of each item in the cart must be >=0.

**Inv Type**: Attribute !<

**Contract (Initial):**

From previous example,

let h a = (mk\_app qty [a]) @>= (mk\_numeral\_i 0)

**Counter Example (if SAT):**

There exists a concurrent Cart\_RemoveItemFromCart effect not visible to the current txn (do\_removeItemFromCart). (concurrent update)

**Contract:**

let i2 a b =

mk\_and [oper(a) @= cart\_rm;

notsametxn(a,b);

currtxn(b)] @=> vis(a, b)

**Counter Example (if SAT):**

There exists a Cart\_AddItemToCart effect that is visible to the current txn, that is not visible to the invariant. (Lost update)

**Contract:**

let g2 a b c d =

mk\_and [oper(a) @= cart\_add; oper(b) @= cart\_get;

oper(c) @= cart\_rm; so(b,c);

txn(b) @= rm;

sametxn(b,c);

oper(d) @= cart\_get;

vis(a,b) ; vis(c,d); sameobj(a,d)] @=> vis(a,d)

**Counter Example (if SAT):**

UNSAT

**Max k for which SAT occurred:** 6

**Time to find counter example:** 1.09s

**Application**: Rubis

**Txn**: do\_bid\_for\_item

**Inv:** For each bid a user places (Wallet\_Bid) there must be a corresponding entry in the Bids table.

**Inv type:** Foreign Key (1:1)

**Contract (Initial):**

No contract.

**Counter Example (if SAT):**

The current txn’s WalletBids\_AddWalletBid is visible to the invariant but the corresponding Bids\_AddBid effect is not visible. (Lost Update)

**Contract:**

f' a b c d =

mk\_and [oper(d) @= gt; so(a,b);

vis(a,c); so(c,d);

sameobj(a,c);sameobj(b,d)] @=> vis(a,d)

**Max k for which SAT occurred:** 4

**Time to find counter example:** 3.03s

**Application**: Rubis

**Txn**: do\_withdraw\_wallet

**Inv:** The user’s wallet balance must always be >= 0

**Inv type:** Attribute !<

**Contract (Initial):**

No contract.

**Counter Example (if SAT):**

There exists a Wallet\_Deposit effect visible to the current txn but not visible to the invariant. (Lost Update)

**Contract:**

let g a b c d =

mk\_and [oper(a) @= dp; oper(b) @= gb;

oper(c) @= wd; so(b,c);

txn(b) @= do\_withdraw;

sametxn(b,c);

oper(d) @= gb;

vis(a,b) ; vis(c,d); sameobj(a,d)] @=> vis(a,d)

**Counter Example (if SAT):**

User deposits a negative balance.

**Contract:**

let h a = (mk\_app amt [a]) @>= (mk\_numeral\_i 0)

**Counter Example (if SAT):**

There exists a concurrent Wallet\_Withdraw effect visible to the invariant. (Concurrent Update)

**Contract:**

let i a b =

mk\_and [oper(a) @= wd;

notsametxn(a,b);

currtxn(b)] @=> vis(a, b)

**Counter Example (if SAT):**

UNSAT

**Max k for which SAT occurred:** 5

**Time to find counter example:** 1.52s

**Application**: Microblog

**Txn**: do\_new\_tweet

**Inv:** For each tweet in the timeline of a user there must be a corresponding entry in the Tweets table.

**Inv type:** Foreign Key (1:1)

**Contract (Initial):**

No contract.

**Counter Example (if SAT):**

The current txn’s Userline\_NewTweet is visible to the invariant but the corresponding Tweet\_New effect is not visible. (Lost Update)

**Contract:**

f' a b c d =

mk\_and [oper(d) @= gt; so(a,b);

vis(a,c); so(c,d);

sameobj(a,c);sameobj(b,d)] @=> vis(a,d)

**Counter Example (if SAT):**

UNSAT

**Max k for which SAT occurred:** 5

**Time to find counter example:** 8.15s

**Application**: Bank Account

**Txn**: do\_withdraw

**Inv:** The user’s bank balance must always be >= 0

**Inv type:** Attribute !<

**Contract (Initial):**

No contract.

**Counter Example (if SAT):**

There exists a BA\_Deposit effect visible to the current txn but not visible to the invariant. (Lost Update)

**Contract:**

let g a b c d =

mk\_and [oper(a) @= dp; oper(b) @= gb;

oper(c) @= wd; so(b,c);

txn(b) @= do\_withdraw;

sametxn(b,c);

oper(d) @= gb;

vis(a,b) ; vis(c,d); sameobj(a,d)] @=> vis(a,d)

**Counter Example (if SAT):**

User deposits a negative balance.

**Contract:**

let h a = (mk\_app amt [a]) @>= (mk\_numeral\_i 0)

**Counter Example (if SAT):**

There exists a concurrent BA\_Withdraw effect visible to the invariant. (Concurrent Update)

**Contract:**

let i a b =

mk\_and [oper(a) @= wd;

notsametxn(a,b);

currtxn(b)] @=> vis(a, b)

**Counter Example (if SAT):**

UNSAT

**Max k for which SAT occurred:** 5

**Time to find counter example:** 0.28s

**Application**: TPC-E

**Txn**: trade\_order & trade\_result

**Inv:** B\_NUM\_TRADES = count(\*) TRADE

**Contract (Initial):**

No contract.

**Counter Example (if SAT):**

The Broker\_IncNumTrades effect of the current transaction is visible to the invariant but the corresponding Trade\_AddTrade is not visible.

**Contract:**

f1 a b c d =

mk\_and [oper(a)@=tadd;

oper(b)@=bincnum;

oper(c)@=tget;

oper(d)@=bget;

so(a,b);

so(c,d);

sameobj(a,c);

sameobj(b,d)] @=> (vis(b,d) @<=> vis(a,c))

**Counter Example (if SAT):**

There exists a Trade\_Add effect which is visible to the current transaction but not to the invariant

**Contract:**

let f1' a b c =

mk\_and [oper(a)@=tadd;

oper(b)@=tget;

currtxn(b);

sameobj(a,b);

oper(c)@=tget;

sameobj(a,c);

notsametxn(a,c);

vis(a,b)] @=> vis(a,c) in

**Counter Example (if SAT):**

There exists a concurrent Trade\_SetCmpltAndComm effect and a corresponding Broker\_IncNumTrades effect visible to the to the invariant.

let f1''' a b =

mk\_and [oper(a)@=tcmplt;

oper(b)@=tget;

sameobj(a,b)] @=> sametxn(a,b) @| vis(a,b) in

**Max k for which SAT occurred:** 10

**Time to find counter example:** 1m 53s

**BMC Time for k=15:** 5m 3s

**Application**: TPC-E

**Txn**: trade\_result

**Inv:** B\_COMM\_TOTAL = sum(T\_COMM)

**Contract (Initial):**

No contract.

**Counter Example (if SAT):**

The Broker\_AddComm effect of the current transaction is visible to the invariant but the corresponding Trade\_SetCmpltAndComm effect is not visible.

**Contract:**

f1 a b c d =

mk\_and [oper(a)@=tcmplt;

oper(b)@=baddcomm;

oper(c)@=tget;

oper(d)@=bget;

so(a,b);

so(c,d);

sameobj(a,c);

sameobj(b,d)] @=> (vis(b,d) @<=> vis(a,c))

**Counter Example (if SAT):**

UNSAT

**Max k for which SAT occurred:** 6

**BMC Time for k=15:** 15m 23s

**Application**: TPC-E

**Txn**: trade\_result

**Inv:** HS\_QTY = sum(H\_QTY)

**Contract (Initial):**

No contract.

**Counter Example (if SAT):**

The HoldingSummary\_AddQty effect of the current transaction is visible to the invariant but the corresponding Holding\_AddHolding is not visible.

**Contract:**

f1 a b c d =

mk\_and [oper(a)@=hsaddqty;

oper(b)@=hadd;

oper(c)@=hget;

oper(d)@=hsget;

so(a,b);

so(c,d);

sameobj(a,c);

sameobj(b,d)] @=> (vis(b,d) @<=> vis(a,c))

**Counter Example (if SAT):**

UNSAT

**Max k for which SAT occurred:** 6

**BMC Time for k=15:** 23m 33s