How to Identify Boundary Conditions with Contrasty Metric?

Weilin Luo[1], Hai Wan [1,*], Xiaotong Song [1], Binhao Yang [1], Hongzhen Zhong [1], Yin Chen [2]

[1] School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou, China
[2] School of Computer Science, South China Normal University, Guangzhou, China

Content

1 Motivation

2 Contrasty Metric

3 Joint Framework

4 Conclusion

Content

1 Motivation

2 Contrasty Metric

3 Joint Framework

4 Conclusion

Goal-oriented Requirement Engineering

Goal-oriented Requirement Engineering (GORE):

- attain correct software requirements specifications
- domain properties and goals in linear-time temporal logic (LTL)

Goal-oriented Requirement Engineering

Goal-oriented Requirement Engineering (GORE):

- attain correct software requirements specifications
- domain properties and goals in linear-time temporal logic (LTL)

Goal-Conflict Analysis in GORE:

- identification stage
- assessment stage
- resolution stage

Goal-oriented Requirement Engineering

Goal-oriented Requirement Engineering (GORE):

- attain correct software requirements specifications
- domain properties and goals in linear-time temporal logic (LTL)

Goal-Conflict Analysis in GORE:

- identification stage
- assessment stage
- resolution stage

Divergence:

- the goals of the requirement cannot be satisfied as a whole.
- it is captured by a **boundary condition (BC)**, which is an LTL formula.

Divergence and Boundary Condition

Example 1 (MinePump[1])

Domain Property (Dom):

1. **Name**: PumpEffect (d_1)
   Description: The pump is turned on for two time steps, then in the following one the water level is not high.
   Formula: $\Box((p \wedge \bigcirc p) \rightarrow \bigcirc(\bigcirc \neg h))$

Goals (G):

1. **Name**: NoFlooding (g_1)
   Description: When the water level is high, the system should turn on the pump.
   Formula: $\Box(h \rightarrow \bigcirc(p))$
2. **Name**: NoExplosion (g_2)
   Description: When there is methane in the environment, the pump should be turned off.
   Formula: $\Box(m \rightarrow \bigcirc(\neg p))$

Divergence and Boundary Condition

Example 1 (MinePump[1])

Domain Property (Dom):

1. **Name**: PumpEffect (d_1)
   Description: The pump is turned on for two time steps, then in the following one the water level is not high.
   Formula: $\Box((p \wedge \bigcirc p) \rightarrow \bigcirc(\bigcirc \neg h))$

Goals (G):

1. **Name**: NoFlooding (g_1)
   Description: When the water level is high, the system should turn on the pump.
   Formula: $\Box(h \rightarrow \bigcirc(p))$
2. **Name**: NoExplosion (g_2)
   Description: When there is methane in the environment, the pump should be turned off.
   Formula: $\Box(m \rightarrow \bigcirc(\neg p))$

One of the BCs is $\varphi_1 = \Diamond(h \wedge m)$.

Filtering out Redundant BCs

Identification of BCs:

- pattern-based approach [2]
- tableaux-based approach [3]
- genetic algorithm [4]

Filtering out Redundant BCs

Identification of BCs:

- pattern-based approach [2]
- tableaux-based approach [3]
- genetic algorithm [4]

Large number of identified BCs make assessing and resolving divergences expensive.

- more than 100 BCs in the case named London Ambulance Service [4]

Filtering out Redundant BCs

Identification of BCs:

- pattern-based approach [2]
- tableaux-based approach [3]
- genetic algorithm [4]

Large number of identified BCs make assessing and resolving divergences expensive.

- more than 100 BCs in the case named London Ambulance Service [4]

Definition 1 (Generality [4])

Let S be a set of BCs. A BC $\varphi_i \in S$ is *more general* than another BC $\varphi_j \in S$ if φ_j implies φ_i.

Definition 2 (General BC Set [4])

Let $\mathcal{B}_g$ be a set of BCs. $\mathcal{B}_g$ is general, iff $\forall \phi, \varphi \in \mathcal{B}_g \wedge \phi \neq \varphi$, $\phi \rightarrow \varphi$ and $\varphi \rightarrow \phi$ do not hold.

Filtering out Redundant BCs

Identification of BCs:

- pattern-based approach [2]
- tableaux-based approach [3]
- genetic algorithm [4]

Large number of identified BCs make assessing and resolving divergences expensive.

- more than 100 BCs in the case named London Ambulance Service [4]

Definition 1 (Generality [4])

Let S be a set of BCs. A BC $\varphi_i \in S$ is *more general* than another BC $\varphi_j \in S$ if φ_j implies φ_i.

Definition 2 (General BC Set [4])

Let $\mathcal{B}_g$ be a set of BCs. $\mathcal{B}_g$ is general, iff $\forall \phi, \varphi \in \mathcal{B}_g \land \phi \neq \varphi$, $\phi \to \varphi$ and $\varphi \to \phi$ do not hold.

Unfortunately, we observe that a set of general BCs still retains a large number of redundant BCs.

Redundant BCs in Generality Metric

Example 2 (Example 1 cont.)

Consider two BCs: $\varphi_1 = \Diamond(h \wedge m)$ and $\varphi_3 = \Diamond(h \wedge \neg m \wedge p \wedge \bigcirc(\neg h \wedge \neg p \vee h \wedge (m \vee \neg p)))$. φ_3 captures five circumstances as follows:

1. $\dots \rightarrow \{h, \neg m, p\} \rightarrow \{\neg h, m, \neg p\} \rightarrow \dots$
2. $\dots \rightarrow \{h, \neg m, p\} \rightarrow \{h, m, p\} \rightarrow \dots$
3. $\dots \rightarrow \{h, \neg m, p\} \rightarrow \{\neg h, \neg m, \neg p\} \rightarrow \dots$
4. $\dots \rightarrow \{h, \neg m, p\} \rightarrow \{h, m, \neg p\} \rightarrow \dots$
5. $\dots \rightarrow \{h, \neg m, p\} \rightarrow \{h, \neg m, \neg p\} \rightarrow \dots$

Redundant BCs in Generality Metric

Example 2 (Example 1 cont.)

Consider two BCs: $\varphi_1 = \Diamond(h \wedge m)$ and $\varphi_3 = \Diamond(h \wedge \neg m \wedge p \wedge \bigcirc(\neg h \wedge \neg p \vee h \wedge (m \vee \neg p)))$. φ_3 captures five circumstances as follows:

1. $\cdots \rightarrow \{h, \neg m, p\} \rightarrow \{\neg h, m, \neg p\} \rightarrow \ldots$
2. $\cdots \rightarrow \{h, \neg m, p\} \rightarrow \{h, m, p\} \rightarrow \ldots$
3. $\cdots \rightarrow \{h, \neg m, p\} \rightarrow \{\neg h, \neg m, \neg p\} \rightarrow \ldots$
4. $\cdots \rightarrow \{h, \neg m, p\} \rightarrow \{h, m, \neg p\} \rightarrow \ldots$
5. $\cdots \rightarrow \{h, \neg m, p\} \rightarrow \{h, \neg m, \neg p\} \rightarrow \ldots$

Apply the generality metric:

- The generality metric cannot evaluate φ_1 and φ_3.
- Engineers should prioritize φ_3 because φ_3 is more likely than φ_1 [5].

Redundant BCs in Generality Metric

Example 3 (Example 2 cont.)

Consider the goal NoFlooding (g_1): $\Box(h \rightarrow \bigcirc(p))$. φ_3 captures five circumstances as follows:

1. $\cdots \rightarrow \{h, \neg m, p\} \rightarrow \{\neg h, m, \neg p\} \rightarrow \ldots$
2. $\cdots \rightarrow \{h, \neg m, p\} \rightarrow \{h, m, p\} \rightarrow \ldots$
3. $\cdots \rightarrow \{h, \neg m, p\} \rightarrow \{\neg h, \neg m, \neg p\} \rightarrow \ldots$
4. $\cdots \rightarrow \{h, \neg m, p\} \rightarrow \{h, m, \neg p\} \rightarrow \ldots$
5. $\cdots \rightarrow \{h, \neg m, p\} \rightarrow \{h, \neg m, \neg p\} \rightarrow \ldots$

- The circumstances (red labeled) cannot capture the divergence in reality because they cannot satisfy the minimality of BC (they violate g_1).
- $\varphi_3' = \Diamond((h \wedge \neg m \wedge p) \wedge \bigcirc(h \wedge p \wedge m))$ stands for the circumstances captured by φ_3.
- φ_1 is more likely than φ_3' [5], so φ_1 should be prioritized.

Content

1 Motivation

2 Contrasty Metric

3 Joint Framework

4 Conclusion

Witness

Definition 3 (Witness)

Let f be an LTL formula and φ a BC. f is a *witness* of φ iff $\varphi \wedge \neg f$ is not a BC.

- The witness f of a BC φ indicates why φ is a BC.
- If f is a BC, it means that the divergence captured by φ is also captured by f.

Witness

Definition 3 (Witness)

Let f be an LTL formula and φ a BC. f is a *witness* of φ iff $\varphi \wedge \neg f$ is not a BC.

- The witness f of a BC φ indicates why φ is a BC.
- If f is a BC, it means that the divergence captured by φ is also captured by f.

Definition 4 (Contrasty)

Let ϕ and φ be BCs. ϕ and φ are *contrastive*, iff ϕ is not a witness of φ and φ is not a witness of ϕ.

Definition 5 (Contrastive BC Set)

Let $\mathcal{B}_c$ be a set of BCs. $\mathcal{B}_c$ is contrastive, iff $\forall \phi, \varphi \in \mathcal{B}_c \wedge \phi \neq \varphi$, ϕ and φ is contrastive.

Highlights of Contrasty Metric

A more finer-grained metric than generality metric (Theorem 2):

- There is not a general relation between any two BCs in a contrastive BC set.
- There can be a witness relation between some two BCs in a general BC set.
- Contrasty metric can filter out more redundant BCs than the generality metric.

Highlights of Contrasty Metric

A more finer-grained metric than generality metric (Theorem 2):

- There is not a general relation between any two BCs in a contrastive BC set.
- There can be a witness relation between some two BCs in a general BC set.
- Contrasty metric can filter out more redundant BCs than the generality metric.

A meaningful metric to filter out redundant BCs (Theorem 3):

- It is reasonable that engineers prioritize the BC, a witness of others, to resolve.
- Contrastive BCs capture different divergences.

Highlights of Contrasty Metric

A more finer-grained metric than generality metric (Theorem 2):

- There is not a general relation between any two BCs in a contrastive BC set.
- There can be a witness relation between some two BCs in a general BC set.
- Contrasty metric can filter out more redundant BCs than the generality metric.

A meaningful metric to filter out redundant BCs (Theorem 3):

- It is reasonable that engineers prioritize the BC, a witness of others, to resolve.
- Contrastive BCs capture different divergences.

A set of contrastive BCs should be recommended to engineers, rather than a set of general BCs.

Post-processing Framework

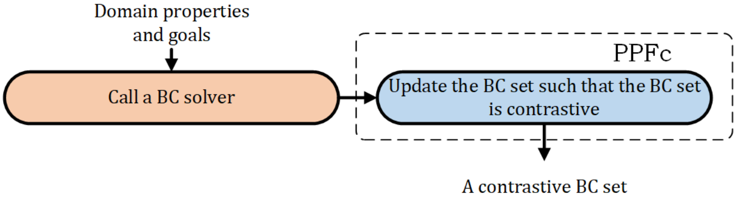

Figure 1: The post-processing framework for filtering the BCs based on the contrasty metric (PPFc). It takes a set of BCs ($\mathcal{B}$) identified by a BC solver as inputs. Its output is a set of contrastive BCs ($\mathcal{B}_c$).

Evaluation of Contrasty

RQ1. Compared with the generality metric, what are the advantages of the contrasty metric?

Evaluation of Contrasty

RQ1. Compared with the generality metric, what are the advantages of the contrasty metric?

Competitors

- generality metric [4] + likelihood [5]
- **contrasty metric (our method)** + likelihood [5]

Evaluation of Contrasty

RQ1. Compared with the generality metric, what are the advantages of the contrasty metric?

Competitors

- generality metric [4] + likelihood [5]
- **contrasty metric (our method)** + likelihood [5]

Benchmarks

- 16 different cases introduced by [4]

Table 1: The details of cases

Case	#Dom	#Goal	#Var	Size
RetractionPattern1 (RP1)	0	2	2	9
RetractionPattern2 (RP2)	0	2	4	10
Elevator (Ele)	1	1	3	10
TCP	0	2	3	14
AchieveAvoidPattern (AAP)	1	2	4	15
MinePump (MP)	1	2	3	21
ATM	1	2	3	22
Rail Road Crossing System (RRCS)	2	2	5	22
Telephone (Tel)	3	2	4	31
London Ambulance Service (LAS)	0	5	7	32
Prioritized Arbiter (PA)	6	1	6	57
Round Robin Arbiter (RRA)	6	3	4	77
Simple Arbiter (SA)	4	3	6	84
Load Balancer (LB)	3	7	5	85
LiftController (LC)	7	8	6	124
ARM's Advanced Microcontroller Bus Architecture (AMBA)	6	21	16	415

Evaluation of Contrasty

RQ1. Compared with the generality metric, what are the advantages of the contrasty metric?

Competitors

- generality metric [4] + likelihood [5]
- **contrasty metric (our method)** + likelihood [5]

Benchmarks

- 16 different cases introduced by [4]

Setups

- the state-of-the-art BC solver [4] denoted by `GA` to identify BCs
- Aalta [6] as the LTL satisfiability checker

Table 1: The details of cases

Case	#Dom	#Goal	#Var	Size
RetractionPattern1 (RP1)	0	2	2	9
RetractionPattern2 (RP2)	0	2	4	10
Elevator (Ele)	1	1	3	10
TCP	0	2	3	14
AchieveAvoidPattern (AAP)	1	2	4	15
MinePump (MP)	1	2	3	21
ATM	1	2	3	22
Rail Road Crossing System (RRCS)	2	2	5	22
Telephone (Tel)	3	2	4	31
London Ambulance Service (LAS)	0	5	7	32
Prioritized Arbiter (PA)	6	1	6	57
Round Robin Arbiter (RRA)	6	3	4	77
Simple Arbiter (SA)	4	3	6	84
Load Balancer (LB)	3	7	5	85
LiftController (LC)	7	8	6	124
ARM's Advanced Microcontroller Bus Architecture (AMBA)	6	21	16	415

Evaluation of Contrasty

Results

Table 2: The number of BC recommended by different metrics, where $\mathcal{B}$ indicates the number of BC computed by BC solver, $\mathcal{B}_g$ indicates the generality metrics, and $\mathcal{B}_c$ indicates the contrasty metrics.

Case	$\lvert\mathcal{B}\rvert$	$\lvert\mathcal{B}_g\rvert$	$\lvert\mathcal{B}_c\rvert$	#suc.
RP1	37.1	3.2	**1.2**	10
RP2	35.1	2.6	**1.2**	10
Ele	28	3.2	**2.6**	10
TCP	53.9	2.1	**1.5**	10
AAP	50.3	3.7	**1.8**	10
MP	40.7	4.5	**1.4**	10
ATM	64.4	3.4	**1.2**	10
RRCS	27.9	3	**1**	10
Tel	36.5	3	**1**	2
LAS	N/A	N/A	N/A	N/A
PA	N/A	N/A	N/A	N/A
RRA	40.571	3.14	**1**	7
SA	N/A	N/A	N/A	N/A
LB	N/A	N/A	N/A	N/A
LC	N/A	N/A	N/A	N/A
AMBA	N/A	N/A	N/A	N/A

Evaluation of Contrasty

Results

- Our method can solve all the cases that can be solved by `GA` to identify BCs.

Table 2: The number of BC recommended by different metrics, where $\mathcal{B}$ indicates the number of BC computed by BC solver, $\mathcal{B}_g$ indicates the generality metrics, and $\mathcal{B}_c$ indicates the contrasty metrics.

Case	$\lvert\mathcal{B}\rvert$	$\lvert\mathcal{B}_g\rvert$	$\lvert\mathcal{B}_c\rvert$	#suc.
RP1	37.1	3.2	**1.2**	10
RP2	35.1	2.6	**1.2**	10
Ele	28	3.2	**2.6**	10
TCP	53.9	2.1	**1.5**	10
AAP	50.3	3.7	**1.8**	10
MP	40.7	4.5	**1.4**	10
ATM	64.4	3.4	**1.2**	10
RRCS	27.9	3	**1**	10
Tel	36.5	3	**1**	2
LAS	N/A	N/A	N/A	N/A
PA	N/A	N/A	N/A	N/A
RRA	40.571	3.14	**1**	7
SA	N/A	N/A	N/A	N/A
LB	N/A	N/A	N/A	N/A
LC	N/A	N/A	N/A	N/A
AMBA	N/A	N/A	N/A	N/A

Evaluation of Contrasty

Results

- Our method can solve all the cases that can be solved by `GA` to identify BCs.
- `GA` can return a large number of BCs.

Table 2: The number of BC recommended by different metrics, where $\mathcal{B}$ indicates the number of BC computed by BC solver, $\mathcal{B}_g$ indicates the generality metrics, and $\mathcal{B}_c$ indicates the contrasty metrics.

Case	$\|\mathcal{B}\|$	$\|\mathcal{B}_g\|$	$\|\mathcal{B}_c\|$	#suc.
RP1	37.1	3.2	**1.2**	10
RP2	35.1	2.6	**1.2**	10
Ele	28	3.2	**2.6**	10
TCP	53.9	2.1	**1.5**	10
AAP	50.3	3.7	**1.8**	10
MP	40.7	4.5	**1.4**	10
ATM	64.4	3.4	**1.2**	10
RRCS	27.9	3	**1**	10
Tel	36.5	3	**1**	2
LAS	N/A	N/A	N/A	N/A
PA	N/A	N/A	N/A	N/A
RRA	40.571	3.14	**1**	7
SA	N/A	N/A	N/A	N/A
LB	N/A	N/A	N/A	N/A
LC	N/A	N/A	N/A	N/A
AMBA	N/A	N/A	N/A	N/A

Evaluation of Contrasty

Results

- Our method can solve all the cases that can be solved by GA to identify BCs.
- GA can return a large number of BCs.
- Lots of BCs identified by GA are redundant in most cases, which cause a huge burden in the assessment stage and the resolution stage.

Table 2: The number of BC recommended by different metrics, where $\mathcal{B}$ indicates the number of BC computed by BC solver, $\mathcal{B}_g$ indicates the generality metrics, and $\mathcal{B}_c$ indicates the contrasty metrics.

Case	$\lvert\mathcal{B}\rvert$	$\lvert\mathcal{B}_g\rvert$	$\lvert\mathcal{B}_c\rvert$	#suc.
RP1	37.1	3.2	**1.2**	10
RP2	35.1	2.6	**1.2**	10
Ele	28	3.2	**2.6**	10
TCP	53.9	2.1	**1.5**	10
AAP	50.3	3.7	**1.8**	10
MP	40.7	4.5	**1.4**	10
ATM	64.4	3.4	**1.2**	10
RRCS	27.9	3	**1**	10
Tel	36.5	3	**1**	2
LAS	N/A	N/A	N/A	N/A
PA	N/A	N/A	N/A	N/A
RRA	40.571	3.14	**1**	7
SA	N/A	N/A	N/A	N/A
LB	N/A	N/A	N/A	N/A
LC	N/A	N/A	N/A	N/A
AMBA	N/A	N/A	N/A	N/A

Evaluation of Contrasty

Results

- Our method can solve all the cases that can be solved by `GA` to identify BCs.
- `GA` can return a large number of BCs.
- Lots of BCs identified by `GA` are redundant in most cases, which cause a huge burden in the assessment stage and the resolution stage.
- Compared with the generality metric, the contrasty metric can considerably reduce the number of BCs.

Table 2: The number of BC recommended by different metrics, where $\mathcal{B}$ indicates the number of BC computed by BC solver, $\mathcal{B}_g$ indicates the generality metrics, and $\mathcal{B}_c$ indicates the contrasty metrics.

Case	$\|\mathcal{B}\|$	$\|\mathcal{B}_g\|$	$\|\mathcal{B}_c\|$	#suc.
RP1	37.1	3.2	**1.2**	10
RP2	35.1	2.6	**1.2**	10
Ele	28	3.2	**2.6**	10
TCP	53.9	2.1	**1.5**	10
AAP	50.3	3.7	**1.8**	10
MP	40.7	4.5	**1.4**	10
ATM	64.4	3.4	**1.2**	10
RRCS	27.9	3	**1**	10
Tel	36.5	3	**1**	2
LAS	N/A	N/A	N/A	N/A
PA	N/A	N/A	N/A	N/A
RRA	40.571	3.14	**1**	7
SA	N/A	N/A	N/A	N/A
LB	N/A	N/A	N/A	N/A
LC	N/A	N/A	N/A	N/A
AMBA	N/A	N/A	N/A	N/A

Evaluation of Contrasty

Table 3: The BCs produced by different metrics

Case	generality metric[4] + likelihood[5]		contrasty metric + likelihood[5]		
	Rank	BC	Rank	BC	Witness
RP1	1	$\Diamond(((p \wedge (\Box(\neg q))) \,\mathcal{U}(\Diamond(q \wedge (\neg p)))) \vee (\Box(p \wedge (\Box(\neg q)))))$	1	$(p \wedge (\Box(\neg q))) \vee (\Diamond(q \wedge (\neg p)))$	1,2,3,4
	2	$\bigcirc((p \wedge (\Box(\neg q))) \vee (\Diamond(q \wedge (\neg p))))$			
	3	$((\neg q \,\mathcal{U}(q \wedge \neg p)) \,\mathcal{U}(\Diamond(p \wedge (\Box(\neg q))))) \vee (\Box(\neg q \,\mathcal{U}(q \wedge \neg p)))$			
	4	$(p \wedge (\Box(\neg q))) \vee (\Diamond(q \wedge \neg p))$			
...	...	...	...	...	...
Ele	1	$\bigcirc(\Diamond(call \wedge (\Box(\neg open))))$	1	$\bigcirc(\Diamond(call \wedge (\Box\neg open)))$	1,3
	2	$((\Diamond(\neg atfloor \wedge (\bigcirc open))) \,\mathcal{U}(call \wedge (\Box(\neg open)))) \vee (\Box(\Diamond(\neg atfloor \wedge (\bigcirc open))))$	2	$open \,\mathcal{U}(call \wedge (\Box\neg open))$	2,4
	3	$\Box(\neg atfloor \wedge (\bigcirc call))$	3	$(call \wedge (\Box(\neg open))) \vee (\bigcirc(\Box(call \wedge (\Box\neg open))))$	2,3,5
	4	$open \,\mathcal{U}(call \wedge (\Box\neg open))$			
	5	$(call \wedge (\Box(\neg open))) \vee (\bigcirc(\Box(call \wedge (\Box(\neg open)))))$			
...	...	...	...	...	...
RRCS	1	$\Diamond((\Diamond(cc \wedge tc)) \vee (\bigcirc(go \wedge ta)))$	1	$(cc \wedge tc) \vee (\Diamond(go \wedge ta))$	1,2,3,4
	2	$(\Diamond(cc \wedge tc)) \vee (go \wedge ta)$			
	3	$(cc \wedge tc) \vee (\Diamond(go \wedge ta))$			
	4	$(\Diamond(cc \wedge tc)) \vee (\Box(go \wedge tc))$			
...	...	...	...	...	...

Results

Evaluation of Contrasty

Table 3: The BCs produced by different metrics

Case	generality metric[4] + likelihood[5]		contrasty metric + likelihood[5]		
	Rank	BC	Rank	BC	Witness
RP1	1 2 3 4	$\Diamond(((p \wedge (\Box(\neg q)))\,\mathcal{U}(\Diamond(q \wedge (\neg p)))) \vee (\Box(p \wedge (\Box(\neg q)))))$ $\bigcirc((p \wedge (\Box(\neg q))) \vee (\Diamond(q \wedge (\neg p))))$ $((\neg q\,\mathcal{U}(q \wedge \neg p))\,\mathcal{U}(\Diamond(p \wedge (\Box(\neg q))))) \vee (\Box(\neg q\,\mathcal{U}(q \wedge \neg p)))$ $(p \wedge (\Box(\neg q))) \vee (\Diamond(q \wedge \neg p))$	1	$(p \wedge (\Box(\neg q))) \vee (\Diamond(q \wedge (\neg p)))$	1,2,3,4
...	...	...	...	...	...
Ele	1 2 3 4 5	$\bigcirc(\Diamond(call \wedge (\Box(\neg open))))$ $((\Diamond(\neg atfloor \wedge (\bigcirc open)))\,\mathcal{U}(call \wedge (\Box(\neg open)))) \vee (\Box(\Diamond(\neg atfloor \wedge (\bigcirc open))))$ $\Box(\neg atfloor \wedge (\bigcirc call))$ $open\,\mathcal{U}(call \wedge (\Box\neg open))$ $(call \wedge (\Box(\neg open))) \vee (\bigcirc(\Box(call \wedge (\Box(\neg open)))))$	1 2 3	$\bigcirc(\Diamond(call \wedge (\Box\neg open)))$ $open\,\mathcal{U}(call \wedge (\Box\neg open))$ $(call \wedge (\Box(\neg open))) \vee (\bigcirc(\Box(call \wedge (\Box\neg open))))$	1,3 2,4 2,3,5
...	...	...	...	...	...
RRCS	1 2 3 4	$\Diamond((\Diamond(cc \wedge tc)) \vee (\bigcirc(go \wedge ta)))$ $(\Diamond(cc \wedge tc)) \vee (go \wedge ta)$ $(cc \wedge tc) \vee (\Diamond(go \wedge ta))$ $(\Diamond(cc \wedge tc)) \vee (\Box(go \wedge tc))$	1	$(cc \wedge tc) \vee (\Diamond(go \wedge ta))$	1,2,3,4
...	...	...	...	...	...

Results

- A set of general BCs still retains the BCs that represent the same divergence.

Evaluation of Contrasty

Table 3: The BCs produced by different metrics

Case	generality metric[4] + likelihood[5]		contrasty metric + likelihood[5]		
	Rank	BC	Rank	BC	Witness
RP1	1	$\Diamond(((p \wedge (\Box(\neg q)))\ \mathcal{U}(\Diamond(q \wedge (\neg p)))) \vee (\Box(p \wedge (\Box(\neg q)))))$	1	$(p \wedge (\Box(\neg q))) \vee (\Diamond(q \wedge (\neg p)))$	1,2,3,4
	2	$\bigcirc((p \wedge (\Box(\neg q))) \vee (\Diamond(q \wedge (\neg p))))$			
	3	$((\neg q\ \mathcal{U}(q \wedge \neg p))\ \mathcal{U}(\Diamond(p \wedge (\Box(\neg q))))) \vee (\Box(\neg q\ \mathcal{U}(q \wedge \neg p)))$			
	4	$(p \wedge (\Box(\neg q))) \vee (\Diamond(q \wedge \neg p))$			
...	...	...	...	...	...
Ele	1	$\bigcirc(\Diamond(call \wedge (\Box(\neg open))))$	1	$\bigcirc(\Diamond(call \wedge (\Box \neg open)))$	1,3
	2	$((\Diamond(\neg atfloor \wedge (\bigcirc open)))\ \mathcal{U}(call \wedge (\Box(\neg open)))) \vee (\Box(\Diamond(\neg atfloor \wedge (\bigcirc open))))$	2	$open\ \mathcal{U}(call \wedge (\Box \neg open))$	2,4
	3	$\Box(\neg atfloor \wedge (\bigcirc call))$	3	$(call \wedge (\Box(\neg open))) \vee (\bigcirc(\Box(call \wedge (\Box \neg open))))$	2,3,5
	4	$open\ \mathcal{U}(call \wedge (\Box \neg open))$			
	5	$(call \wedge (\Box(\neg open))) \vee (\bigcirc(\Box(call \wedge (\Box(\neg open)))))$			
...	...	...	...	...	...
RRCS	1	$\Diamond((\Diamond(cc \wedge tc)) \vee (\bigcirc(go \wedge ta)))$	1	$(cc \wedge tc) \vee (\Diamond(go \wedge ta))$	1,2,3,4
	2	$(\Diamond(cc \wedge tc)) \vee (go \wedge ta)$			
	3	$(cc \wedge tc) \vee (\Diamond(go \wedge ta))$			
	4	$(\Diamond(cc \wedge tc)) \vee (\Box(go \wedge tc))$			
...	...	...	...	...	...

Results

- A set of general BCs still retains the BCs that represent the same divergence.
- The BCs in the general BC set will lead to mistakes of likelihood.

Evaluation of Contrasty

Summary

1. The generality metric cannot capture the difference between BCs.
2. Surprisingly, lots of BCs identified by the state-of-the-art BC solver are redundant in most cases which put an expensive burden on assessing and resolving divergences.
3. The contrasty metric is more finer-grained and meaningful to filter out redundant BCs.
4. A set of contrastive BCs is a better recommendation for engineers to saving the costs of assessing and resolving divergences.

Content

1 Motivation

2 Contrasty Metric

3 Joint Framework

4 Conclusion

Joint Framework

Theorem 1 (BC termination condition)

Let Dom be domain properties and G goals. If $\exists 1 \leq i \leq |G|, Dom \wedge G_{-i} \wedge \neg G_i \models \bot$, then there does not exist a BC under Dom and G.

Joint Framework

Theorem 1 (BC termination condition)

Let Dom be domain properties and G goals. If $\exists 1 \leq i \leq |G|, Dom \wedge G_{-i} \wedge \neg G_i \models \bot$, then there does not exist a BC under Dom and G.

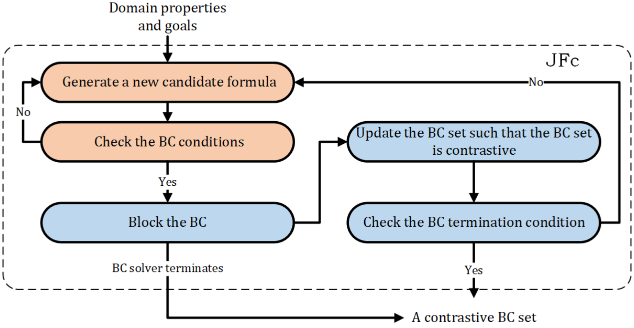

Figure 2: The joint framework to interleave filtering based on the contrasty metric with identifying BCs (JFc). JFc takes the domain properties Dom and goals G as inputs. Its output is a set of contrastive BCs $\mathcal{B}_c$.

Evaluation of JFc

RQ2. What is the performance of JFc for producing a contrastive BC set compared with PPFc?

Evaluation of JFc

RQ2. What is the performance of JFc for producing a contrastive BC set compared with PPFc?

Results

Table 4: The overall performance of PPFc and JFc

Case	PPFc					JFc				
	$\lvert\mathcal{B}\rvert$	$\lvert\mathcal{B}_c\rvert$	GA t. (s)	t. (s)	#suc.	$\lvert\mathcal{B}\rvert$	$\lvert\mathcal{B}_c\rvert$	#T	t. (s)	#suc.
RP1	37.1	1.2	157.4	224.53	10	**1**	**1**	10	**29.5**	10
RP2	35.1	1.2	130.2	206	10	**1.1**	**1.1**	10	**78.9**	10
Ele	28	2.6	45.8	88.01	10	**2.1**	**2.1**	10	**43.4**	10
TCP	53.9	1.5	225.1	**308.26**	10	**1.4**	**1.4**	0	801.6	10
AAP	50.3	1.8	65.3	208.64	10	**1**	**1**	10	**41.3**	10
MP	40.7	1.4	59.3	146.02	10	**1**	**1**	10	**60.8**	10
ATM	64.4	1.2	102.2	259.19	10	**1**	**1**	10	**25.2**	10
RRCS	27.9	1	68.3	91.87	10	**1**	1	10	**15**	10
Tel	36.5	1	35.3	46.53	2	**1**	1	10	**27**	**10**
...	...	...	...	...	...	...	...	...	...	...
RRA	40.571	1	696.43	878.7	7	**1**	1	10	**255.1**	**10**
...	...	...	...	...	...	...	...	...	...	...

Evaluation of JFc

RQ2. What is the performance of JFc for producing a contrastive BC set compared with PPFc?

Results

- For PPFc, the cost of producing a set of contrastive BCs is proportional to the number of BCs identified by a BC solver.

Table 4: The overall performance of PPFc and JFc

Case	PPFc					JFc				
	$\lvert\mathcal{B}\rvert$	$\lvert\mathcal{B}_c\rvert$	GA t. (s)	t. (s)	#suc.	$\lvert\mathcal{B}\rvert$	$\lvert\mathcal{B}_c\rvert$	#T	t. (s)	#suc.
RP1	37.1	1.2	157.4	224.53	10	**1**	**1**	10	**29.5**	10
RP2	35.1	1.2	130.2	206	10	**1.1**	**1.1**	10	**78.9**	10
Ele	28	2.6	45.8	88.01	10	**2.1**	**2.1**	10	**43.4**	10
TCP	53.9	1.5	225.1	**308.26**	10	**1.4**	**1.4**	0	801.6	10
AAP	50.3	1.8	65.3	208.64	10	**1**	**1**	10	**41.3**	10
MP	40.7	1.4	59.3	146.02	10	**1**	**1**	10	**60.8**	10
ATM	64.4	1.2	102.2	259.19	10	**1**	**1**	10	**25.2**	10
RRCS	27.9	1	68.3	91.87	10	**1**	1	10	**15**	10
Tel	36.5	1	35.3	46.53	2	**1**	1	10	**27**	**10**
...	...	...	...	...	...	...	...	...	...	...
RRA	40.571	1	696.43	878.7	7	**1**	1	10	**255.1**	**10**
...	...	...	...	...	...	...	...	...	...	...

Evaluation of JFc

RQ2. What is the performance of JFc for producing a contrastive BC set compared with PPFc?

Results

- For PPFc, the cost of producing a set of contrastive BCs is proportional to the number of BCs identified by a BC solver.
- JFc produces a strong search bias towards the contrastive BCs, thereby avoiding searching for the redundant BCs.

Table 4: The overall performance of PPFc and JFc

Case	PPFc					JFc				
	$\lvert\mathcal{B}\rvert$	$\lvert\mathcal{B}_c\rvert$	GA t. (s)	t. (s)	#suc.	$\lvert\mathcal{B}\rvert$	$\lvert\mathcal{B}_c\rvert$	#T	t. (s)	#suc.
RP1	37.1	1.2	157.4	224.53	10	**1**	**1**	10	**29.5**	10
RP2	35.1	1.2	130.2	206	10	**1.1**	**1.1**	10	**78.9**	10
Ele	28	2.6	45.8	88.01	10	**2.1**	**2.1**	10	**43.4**	10
TCP	53.9	1.5	225.1	**308.26**	10	**1.4**	**1.4**	0	801.6	10
AAP	50.3	1.8	65.3	208.64	10	**1**	**1**	10	**41.3**	10
MP	40.7	1.4	59.3	146.02	10	**1**	**1**	10	**60.8**	10
ATM	64.4	1.2	102.2	259.19	10	**1**	**1**	10	**25.2**	10
RRCS	27.9	1	68.3	91.87	10	**1**	1	10	**15**	10
Tel	36.5	1	35.3	46.53	2	**1**	1	10	**27**	**10**
...	...	...	...	...	...	...	...	...	...	...
RRA	40.571	1	696.43	878.7	7	**1**	1	10	**255.1**	**10**
...	...	...	...	...	...	...	...	...	...	...

Content

1 Motivation

2 Contrasty Metric

3 Joint Framework

4 Conclusion

Conclusion

1. Discover the drawbacks of existing work in providing a reasonable set of BCs for assessing and resolving divergences.
2. Propose a new metric, contrasty, which mainly distinguishes the difference between BCs from the point of resolving divergences.
3. Experimental results have shown the contrasty metric filters out the BCs capturing the same divergence and helps to avoid costly reworks.
4. Design a joint framework to improve the performance of the post-processing framework.

References I

[1] J. Kramer, J. Magee, M. Sloman, and A. Lister, "Conic: an integrated approach to distributed computer control systems," *IET Computers & Digital Techniques*, vol. 130, no. 1, pp. 1–10, 1983.

[2] A. Van Lamsweerde, R. Darimont, and E. Letier, "Managing conflicts in goal-driven requirements engineering," *IEEE Trans. Software Eng.*, vol. 24, no. 11, pp. 908–926, 1998.

[3] R. Degiovanni, N. Ricci, D. Alrajeh, P. Castro, and N. Aguirre, "Goal-conflict detection based on temporal satisfiability checking," in *ASE*, 2016, pp. 507–518.

[4] R. Degiovanni, F. Molina, G. Regis, and N. Aguirre, "A genetic algorithm for goal-conflict identification," in *ASE*, 2018, pp. 520–531.

[5] R. Degiovanni, P. Castro, M. Arroyo, M. Ruiz, N. Aguirre, and M. Frias, "Goal-conflict likelihood assessment based on model counting," in *ICSE*, 2018, pp. 1125–1135.

[6] J. Li, S. Zhu, G. Pu, and M. Y. Vardi, "Sat-based explicit ltl reasoning," in *HVC*, 2015, pp. 209–224.

[7] A. Cailliau and A. Van Lamsweerde, "A probabilistic framework for goal-oriented risk analysis," in *RE*, 2012, pp. 201–210.

Thank you for your listening!

Divergence and Boundary Condition

Definition 6 (Divergence and Boundary Condition[3])

Let $G = \{g_1, \ldots, g_n\}$ be a set of goals and Dom a set of domain properties. A *divergence* occurs within Dom iff there exists a *boundary condition (BC)* φ under Dom and G such that the following conditions hold:

$$Dom \land G \land \varphi \models \bot \qquad \text{(logical inconsistency)}$$

$$Dom \land G_{-i} \land \varphi \not\models \bot, \text{ for each } 1 \leq i \leq n \qquad \text{(minimality)}$$

$$\neg G \not\equiv \varphi \qquad \text{(non-triviality)}$$

where $G = \bigwedge_{1 \leq i \leq n} g_i$ and $G_{-i} = \bigwedge_{j \neq i} g_j$.

Divergence and Boundary Condition

Definition 6 (Divergence and Boundary Condition [3])

Let $G = \{g_1, \ldots, g_n\}$ be a set of goals and Dom a set of domain properties. A *divergence* occurs within Dom iff there exists a *boundary condition (BC)* φ under Dom and G such that the following conditions hold:

$$Dom \wedge G \wedge \varphi \models \perp \qquad \text{(logical inconsistency)}$$

$$Dom \wedge G_{-i} \wedge \varphi \not\models \perp, \text{ for each } 1 \leq i \leq n \qquad \text{(minimality)}$$

$$\neg G \not\equiv \varphi \qquad \text{(non-triviality)}$$

where $G = \bigwedge_{1 \leq i \leq n} g_i$ and $G_{-i} = \bigwedge_{j \neq i} g_j$.

Divergence:

- the goals of the requirement cannot be satisfied as a whole
- captured by boundary condition (BC)

Goal-Conflict Analysis

Identification of BCs:

- pattern-based approach [2]
- tableaux-based approach [3]
- genetic algorithm [4]

Goal-Conflict Analysis

Identification of BCs:

- pattern-based approach [2]
- tableaux-based approach [3]
- genetic algorithm [4]

Assessment of BCs:

- framework with extra probabilistic information [7]
- model counting-based method [5]

Goal-Conflict Analysis

Identification of BCs:

- pattern-based approach [2]
- tableaux-based approach [3]
- genetic algorithm [4]

Assessment of BCs:

- framework with extra probabilistic information [7]
- model counting-based method [5]

Resolution of Divergences:

- open problem [2]

Goal-Conflict Analysis

Identification of BCs:

- pattern-based approach [2]
- tableaux-based approach [3]
- genetic algorithm [4]

Assessment of BCs:

- framework with extra probabilistic information [7]
- model counting-based method [5]

Resolution of Divergences:

- open problem [2]

Issue: Large number of identified BCs make assessing and resolving divergences expensive.

- more than 100 BCs in the case named London Ambulance Service [4]

Filtering out Redundant BCs

Definition 7 (Generality[4])

Let S be a set of BCs. A BC $\varphi_i \in S$ is *more general* than another BC $\varphi_j \in S$ if φ_j implies φ_i.

Example 4 (Example 1 cont.)

$\varphi_1 = \Diamond(h \wedge m)$ and $\varphi_2 = h \wedge m$ are BCs. Considering the generality metric, we filter out φ_2 because φ_1 is more general than φ_2.

Definition 8 (General BC Set[4])

Let $\mathcal{B}_g$ be a set of BCs. $\mathcal{B}_g$ is general, iff $\forall \phi, \varphi \in \mathcal{B}_g \wedge \phi \neq \varphi$, $\phi \rightarrow \varphi$ and $\varphi \rightarrow \phi$ do not hold.

Filtering out Redundant BCs

Definition 7 (Generality[4])

Let S be a set of BCs. A BC $\varphi_i \in S$ is *more general* than another BC $\varphi_j \in S$ if φ_j implies φ_i.

Example 4 (Example 1 cont.)

$\varphi_1 = \Diamond(h \wedge m)$ and $\varphi_2 = h \wedge m$ are BCs. Considering the generality metric, we filter out φ_2 because φ_1 is more general than φ_2.

Definition 8 (General BC Set[4])

Let $\mathcal{B}_g$ be a set of BCs. $\mathcal{B}_g$ is general, iff $\forall \phi, \varphi \in \mathcal{B}_g \wedge \phi \neq \varphi$, $\phi \rightarrow \varphi$ and $\varphi \rightarrow \phi$ do not hold.

Unfortunately, we observe that a set of general BCs still retains a large number of redundant BCs.

Witness

Definition 9 (Witness)

Let f be an LTL formula and φ a BC. f is a *witness* of φ iff $\varphi \wedge \neg f$ is not a BC.

- The witness f of a BC φ indicates why φ is a BC.
- If f is a BC, it means that the divergence captured by φ is also captured by f.

Witness

Definition 9 (Witness)

Let f be an LTL formula and φ a BC. f is a *witness* of φ iff $\varphi \wedge \neg f$ is not a BC.

- The witness f of a BC φ indicates why φ is a BC.
- If f is a BC, it means that the divergence captured by φ is also captured by f.

Example 5 (Example 1 cont.)

$\varphi_1 = \Diamond(h \wedge m)$ and $\varphi_3 = \Diamond(h \wedge \neg m \wedge p \wedge \bigcirc(\neg h \wedge \neg p \vee h \wedge (m \vee \neg p)))$.

- Because $\varphi_1 \wedge \neg\varphi_3$ is also a BC, φ_3 is not a witness of φ_1.
- φ_1 is a witness of φ_3 since $\varphi_3 \wedge \neg\varphi_1$ does not satisfy the minimality constraint of BC, *i.e.*, $d_1 \wedge g_1 \wedge (\varphi_3 \wedge \neg\varphi_1)$ is unsatisfiable.

Contrasty

Definition 10 (Contrasty)

Let ϕ and φ be BCs. ϕ and φ are *contrastive*, iff ϕ is not a witness of φ and φ is not a witness of ϕ.

Definition 11 (Contrastive BC Set)

Let $\mathcal{B}_c$ be a set of BCs. $\mathcal{B}_c$ is contrastive, iff $\forall \phi, \varphi \in \mathcal{B}_c \wedge \phi \neq \varphi$, ϕ and φ is contrastive.

Contrasty

Definition 10 (Contrasty)

Let ϕ and φ be BCs. ϕ and φ are *contrastive*, iff ϕ is not a witness of φ and φ is not a witness of ϕ.

Definition 11 (Contrastive BC Set)

Let $\mathcal{B}_c$ be a set of BCs. $\mathcal{B}_c$ is contrastive, iff $\forall \phi, \varphi \in \mathcal{B}_c \wedge \phi \neq \varphi$, ϕ and φ is contrastive.

Example 6 (Example 1 cont.)

$\varphi_1 = \Diamond(h \wedge m)$, $\varphi_2 = h \wedge m$, and $\varphi_3 = \Diamond(h \wedge \neg m \wedge p \wedge \bigcirc(\neg h \wedge \neg p \vee h \wedge (m \vee \neg p)))$.

- φ_1 and φ_3 are not contrastive.
- φ_1 and φ_2 are not contrastive.
- φ_2 and φ_3 are contrastive.

Finer-grained Metric

Lemma 1

Let ϕ and φ be BCs. If $\phi \to \varphi$, then φ is a witness of ϕ.

Theorem 2

Let $\mathcal{B}_c$ be a set of contrastive BCs. $\forall \phi, \varphi \in \mathcal{B}_c \wedge \phi \neq \varphi$, $\phi \not\to \varphi \wedge \varphi \not\to \phi$.

A more finer-grained metric than generality metric

- There is not a general relation between any two BCs in a contrastive BC set.
- There can be a witness relation between some two BCs in a general BC set.
- Contrasty metric can filter out more redundant BCs than the generality metric.

Meaningful Metric

Property 1

Let ϕ and φ be BCs. If ϕ is a witness of φ and φ is not a witness of ϕ, then resolving the divergence captured by ϕ leads to resolving the divergence captured by φ.

Theorem 3

Let ϕ and φ be BCs. If ϕ and φ are contrastive, then ϕ and φ capture different divergences.

A meaningful metric to filter out redundant BCs

- It is reasonable that engineers prioritize the BC, a witness of others, to resolve.
- Contrastive BCs capture different divergences.

A set of contrastive BCs should be recommended to engineers, rather than a set of general BCs.

Characterization of JFc

Theorem 4

Let Dom be domain properties, G goals, and $\mathcal{B}$ a set of BCs that has been identified. A LTL formula ϕ is a BC under Dom and G, if ϕ is a BC under $Dom \cup \{\neg\varphi | \varphi \in \mathcal{B}\}$ and G.

The results of JFc are still BCs under the original domain properties and goals.

Theorem 5

In JFc, $\nexists \varphi \in \mathcal{B}_c$ *s.t.* φ is a witness of ϕ, where $\mathcal{B}_c$ is a contrastive BC set and ϕ is a new BC.

JFc can produce a search bias towards the BCs that capture different divergences.

Theorem 6

In JFc, the BCs in the final $\mathcal{B}_c$ are not witnesses with each other.

JFc can return a set of contrastive BCs.