How to Identify Boundary Conditions with Contrasty Metric?

罗炜麟
合作者：万海、宋晓彤、杨滨好、钟洪桢、陈寅
published in ICSE 2021

中山大学 计算机学院

Content

Content

About Me

Research Interest

- Representing and learning of formal languages, eg, linear temporal logic
  - published in IEEE Trans. Reliab. 2021, ICCAD 2021, and AAAI 2022
- Solving hard computational problems (NPC, NP-hard, PSPACE, etc.)
  - published in AAAI 2022
- Generalization and interpretability of artificial intelligence

About Me

Research Interest

- Representing and learning of formal languages, eg, linear temporal logic
  - published in IEEE Trans. Reliab. 2021, ICCAD 2021, and AAAI 2022
- Solving hard computational problems (NPC, NP-hard, PSPACE, etc.)
  - published in AAAI 2022
- Generalization and interpretability of artificial intelligence

Sharing

- interest
- curiosity
- cooperate
- insist

Content

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 *boundary conditions (BCs)* is $\varphi_1 = \Diamond(h \wedge m)$.

Content

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

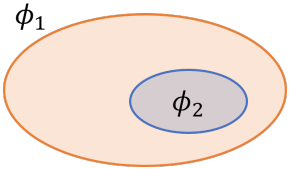
Identification of BCs:

- 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]

Generality Metric:



Filtering out Redundant BCs

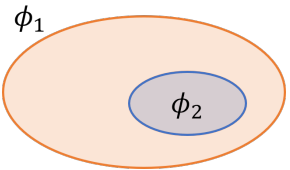
Identification of BCs:

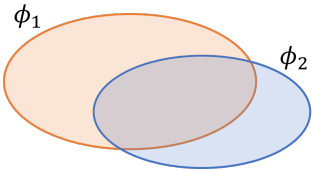
- pattern-based approach [2]
- tableaux-based approach [3]
- genetic algorithm [4]

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

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

Generality Metric:





Filtering out Redundant BCs

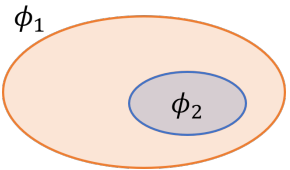
Identification of BCs:

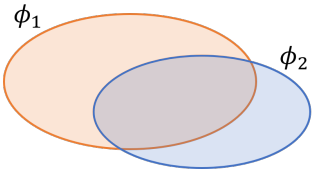
- pattern-based approach [2]
- tableaux-based approach [3]
- genetic algorithm [4]

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

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

Generality Metric:





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

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

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): $\square(h \rightarrow \bigcirc(p))$. 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

Witness and Contrasty

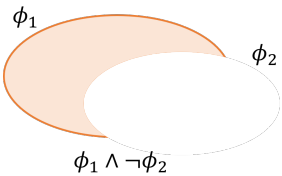
Definition 1 (Witness)

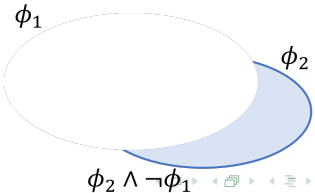
Let f be an LTL formula and φ a BC. f is a *witness* of φ iff $\varphi \wedge \neg f$ is not a BC.

- 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 2 (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.





Evaluation of Contrasty

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

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

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

Content

Conclusion and Future Work

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. Future work includes to automatically resolve divergences.

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.

Q & A

Thank you for your listening!

Divergence and Boundary Condition

Definition 3 (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:

$$Dom \wedge G \wedge \varphi \models \bot \qquad \text{(logical inconsistency)}$$
$$Dom \wedge G_{-i} \wedge \varphi \not\models \bot, \text{ for each } 1 \leq i \leq n \qquad \text{(minimality)}$$
$$\neg G \not\equiv \varphi \qquad \text{(non-triviality)}$$

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

Divergence and Boundary Condition

Definition 3 (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:

$$Dom \wedge G \wedge \varphi \models \bot \qquad \text{(logical inconsistency)}$$
$$Dom \wedge G_{-i} \wedge \varphi \not\models \bot, \text{ for each } 1 \leq i \leq n \qquad \text{(minimality)}$$
$$\neg G \not\equiv \varphi \qquad \text{(non-triviality)}$$

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

Divergence:

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

Witness

Definition 4 (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 4 (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 4 (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 5 (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 6 (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 5 (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 6 (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 5 (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.

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.