Research Statement

Amrita Suresh

Abstract

Asynchronous distributed processes communicating using First In First Out (FIFO) channels are widely used for distributed and concurrent programming. However, since they can simulate Turing machines, most verification properties are undecidable for them [BZ83]. Hence, there is a need to analyze subclasses which are powerful yet have decidable properties. The half-duplex restriction, introduced in [CF05], has been well-studied for the binary case, but there are a large number of open problems in the case of multiparty systems. Moreover, studying these systems in the ideal setting naturally leads to the question of their behaviour in unreliable settings. There are also various gaps in the existing literature regarding different notions of communication architecture. This proposal highlights some of the open problems that try to complete this picture.

Background

Communication with asynchronous message passing is widely used in concurrent and distributed programs implementing various types of systems such as communication protocols [vB75], hardware design, designing and verifying session types [LY19], web contracts, choreographies, concurrent programs, Erlang, Rust, etc. An asynchronous message passing system is built as a set of processes running in parallel, communicating asynchronously by sending messages to each other via channels or message buffers. Messages sent to a given process are stored in its entry channel, waiting for the moment they will be received by the process. In general, sending messages is not blocking for the sender process, which means that the message channels are supposed to be of unbounded size. Moreover, asynchrony introduces a tremendous amount of new possible interleavings, which makes them difficult to analyse. In particular, when the channels are FIFO ordered, the verification of reachability queries is undecidable even when each of the processes is finite-state [BZ83]. This gives rise to the interest of studying underapproximations, which restrict the behavior of general FIFO systems in turn having decidable verification properties.

During the course of my PhD, I have analysed various such underapproximations. Firstly, we studied systems restricted to input-bounded runs (i.e. the sequence of messages sent through a particular channel belongs to a given bounded language). We show that there are various verification problems, most notably rational-reachability, which are decidable for such systems [BFS22a]. Secondly, inspired by the notions of synchronizability in [BEJQ18, GLL20, BB11], we study synchronizable systems (i.e. whether every execution can be rescheduled so that it meets certain criteria, e.g., a channel bound). For such systems, we provide a framework, that unifies existing definitions, and allows one to easily derive decidability results for synchronizability [BGF$^+$21]. We also extend some notions for other communication architectures (peer-to-peer and mailbox). More recently, we also specifically studied the notion of synchronizable systems as in [BB11], and show that both, the problem of deciding inclusion to this class, as well as reachability problem, is undecidable for this class of systems. Finally, we also study an extension of well structured transition systems, originally studied in [Fin90], and show that boundedness and termination is decidable for this class of systems [BFS22b].

Research proposal

I would like to focus my research in the near-future in the cusp of communicating (and communicating session) automata, choreography realisability, synchronizability, and verification in the presence of unreliability. The following excerpts summarize some of the main problems.

Half-duplex multiparty communication. In [LV11], the authors show that for channel contracts, which are naturally modelled as communication automata, the question of reliability is best described using the idea of half-duplex communication. However, they do not extend their notion to multiparty automata, but instead only study binary half-duplex systems. One of the problems to be studied in the immediate future would be using extensions of half-duplex behaviour, for example as in [GGL21], and extend the define of reliable contracts for the multiparty case. This will also be a relevant problem in the area of session types as communication contracts are often based on multiparty session types.

Inclusion of k-MC into the synchronisability framework. In [LY19], the authors define the notion of k-multiparty compatibility (k-MC) in order verify communicating session automata. This notion is of immense practical importance as it can be used to represent session types and interactions. Moreover, the notion of k-MC can be seen as comparable to some notions of syncrhonizability, and hence, it would be of interest to see if it can be expressed in the unifying framework defined in [BGF$^+$21]. Furthermore, the notion of k-MC in the presence of unreliability is also an interesting open question.

Practical implementation of verification of communicating systems. The authors provide in [LY19] a tool that takes a system of communicating automata and a bound, and verifies if the system validates the k-MC property. This tool not only helps in k-MC checking, but also gives a practical procedure to check existential k-boundedness. In the larger context, there is a huge gap for tools which can be used to analyse communicating automata. Hence, a mid-term objective would be to add more capability to the k-MC checking tool in order to capture more properties to be verified. Moreover, it would be interesting to study if the notions of k-MC can be extended beyond session automata to communicating automata at large.

Conclusion and long term objectives

The problem of verifying communicating automata is a difficult problem. Hence, the study of models to make their verification easier is ever-evolving. Very recent works [GGL21, SZ22] have built on existing models in order to capture more subclasses of systems. It would be interesting to see if other known restrictions can be extended to communicating automata (e.g. reversal boundedness, ordering between channels, etc). Another open field of study would be regarding safety properties on these classes of systems, in particular properties studied in approaches based on session types [HYC16, DY12, SY19]. Moreover, due to the complexity of representing and analysing communicating automata, there has been a dearth of practical tools to verify them. On the other hand, their correspondence with multiparty session types is the foundation for various tools on session types. A worthwhile long-term goal would be to investigate if some ideas from the field of session types can be adapted to communicating automata in general. It would also be interesting to see how the graphical notions of Message Sequence Charts (MSCs) and High Level MSCs (HMSCs) can be exploited to gain more understanding of subclasses of communicating automata.

References

[BB11] Samik Basu and Tevfik Bultan. Choreography conformance via synchronizability. In Sadagopan Srinivasan, Krithi Ramamritham, Arun Kumar, M. P. Ravindra, Elisa Bertino, and Ravi Kumar, editors, *Proceedings of the 20th International Conference on World Wide Web, WWW 2011, Hyderabad, India, March 28 - April 1, 2011*, pages 795–804. ACM, 2011.

[BEJQ18] Ahmed Bouajjani, Constantin Enea, Kailiang Ji, and Shaz Qadeer. On the completeness of verifying message passing programs under bounded asynchrony. In Hana Chockler and Georg Weissenbacher, editors, *Computer Aided Verification - 30th International Conference, CAV 2018, Held as Part of the Federated Logic Conference, FloC 2018, Oxford, UK, July 14-17, 2018, Proceedings, Part II*, volume 10982 of *Lecture Notes in Computer Science*, pages 372–391. Springer, 2018.

[BFS22a] Benedikt Bollig, Alain Finkel, and Amrita Suresh. Bounded reachability problems are decidable in FIFO machines. *Log. Methods Comput. Sci.*, 18(1), 2022.

[BFS22b] Benedikt Bollig, Alain Finkel, and Amrita Suresh. Branch-well-structured transition systems and extensions. In Mohammad Reza Mousavi and Anna Philippou, editors, *Formal Techniques for Distributed Objects, Components, and Systems - 42nd IFIP WG 6.1 International Conference, FORTE 2022, Held as Part of the 17th International Federated Conference on Distributed Computing Techniques, DisCoTec 2022, Lucca, Italy, June 13-17, 2022, Proceedings*, volume 13273 of *Lecture Notes in Computer Science*, pages 50–66. Springer, 2022.

[BGF$^+$21] Benedikt Bollig, Cinzia Di Giusto, Alain Finkel, Laetitia Laversa, Étienne Lozes, and Amrita Suresh. A unifying framework for deciding synchronizability. In Serge Haddad and Daniele Varacca, editors, *32nd International Conference on Concurrency Theory, CONCUR 2021,* *August 24-27, 2021, Virtual Conference*, volume 203 of *LIPIcs*, pages 14:1–14:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

[BZ83] Daniel Brand and Pitro Zafiropulo. On communicating finite-state machines. *J. ACM*, 30(2):323–342, apr 1983.

[CF05] Gérard Cécé and Alain Finkel. Verification of programs with half-duplex communication. *Information and Computation*, 202(2):166–190, 2005.

[DY12] Pierre-Malo Deniélou and Nobuko Yoshida. Multiparty session types meet communicating automata. In Helmut Seidl, editor, *Programming Languages and Systems - 21st European Symposium on Programming, ESOP 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012. Proceedings*, volume 7211 of *Lecture Notes in Computer Science*, pages 194–213. Springer, 2012.

[Fin90] Alain Finkel. Reduction and covering of infinite reachability trees. *Inf. Comput.*, 89(2):144–179, 1990.

[GGL21] Cinzia Di Giusto, Loïc Germerie Guizouarn, and Étienne Lozes. Towards generalised half-duplex systems. In Julien Lange, Anastasia Mavridou, Larisa Safina, and Alceste Scalas, editors, *Proceedings 14th Interaction and Concurrency Experience, ICE 2021, Online, 18th June 2021*, volume 347 of *EPTCS*, pages 22–37, 2021.

[GLL20] Cinzia Di Giusto, Laetitia Laversa, and Étienne Lozes. On the k-synchronizability of systems. In Jean Goubault-Larrecq and Barbara König, editors, *Foundations of Software Science and Computation Structures - 23rd International Conference, FOSSACS 2020, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2020, Dublin, Ireland, April 25-30, 2020, Proceedings*, volume 12077 of *Lecture Notes in Computer Science*, pages 157–176. Springer, 2020.

[HYC16] Kohei Honda, Nobuko Yoshida, and Marco Carbone. Multiparty asynchronous session types. *J. ACM*, 63(1):9:1–9:67, 2016.

[LV11] Étienne Lozes and Jules Villard. Reliable contracts for unreliable half-duplex communications. In Marco Carbone and Jean-Marc Petit, editors, *Web Services and Formal Methods - 8th International Workshop, WS-FM 2011, Clermont-Ferrand, France, September 1-2, 2011, Revised Selected Papers*, volume 7176 of *Lecture Notes in Computer Science*, pages 2–16. Springer, 2011.

[LY19] Julien Lange and Nobuko Yoshida. Verifying asynchronous interactions via communicating session automata. In Isil Dillig and Serdar Tasiran, editors, *Computer Aided Verification*, pages 97–117, Cham, 2019. Springer International Publishing.

[SY19] Alceste Scalas and Nobuko Yoshida. Less is more: multiparty session types revisited. *Proc. ACM Program. Lang.*, 3(POPL):30:1–30:29, 2019.

[SZ22] Felix Stutz and Damien Zufferey. Comparing channel restrictions of communicating state machines, high-level message sequence charts, and multiparty session types. *CoRR*, abs/2208.05559, 2022.

[vB75] Gregor von Bochmann. Communication protocols and error recovery procedures. In *SIGCOMM / SIGOPS Workshop on Interprocess Communications*, 1975.