VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
INFORMATIKOS INSTITUTAS

Elixir proceso priežiūros įtaka išskirstytų algoritmų teisingumui

Impact of Elixir process Supervision on the correctness of distributed algorithms

Magistro darbo planas

Atliko: Matas Savickis (parašas)

Darbo vadovas: Karolis Petrauskas, Doc., Dr. (parašas)

Recenzentas: (parašas)

Vilnius – 2023

TURINYS

Įvadas

Šiais laikais kai kurios programų sistemos yra išskirstytos [Smi18]. Tokios sistemos, kaip sufleruoja pavadinimas, yra kuriamos išskirstant skaičiavimo mazgus į atskiras, savarankiškas dalis [CDK05]. Ne kaip monolitinės sistemos, išskirstytos sistemos gali veikti skirtingose serverinėse, kurios gali būti įvairiose geografinėse vietose [Shi06]. Toks sistemos išskirstymas pasižymi šiomis savybėmis:

1. Pasiekiamumas (angl. *Availability*) – vartotojas gali pasiekti sistemą bet kuriuo metu [GLA+13].

2. Patvarumas (angl. *Durability*) – išskirstytos sistemos užtikrina duomenų išlaikymą ir pastovų veikimą net jeigu ir vienas iš paskirstytos sistemos mazgų nustotų veikti dėl sistemos sutrikimų, sukeltų programos klaidų arba gamtos katastrofų, tokių kaip: gaisrai, potvyniai ir panašios nelaimės. Ši savybė taip pat užtikrina sistemos gebėjimą atsistatyti ir neprarasti duomenų po minėtų įvykių [RP10].

3. Plečiamumas (angl. *Scalability*) – didėjant vartotojų skaičiui bei programų sistemos kompleksiškumui išskirstytos sistemos užtikriną vertikalų (padidinti mazgo techninės įrangos galingumą) bei horizontalų (padidinti mazgų skaičių sistemoje) plečiamumą [JW00].

4. Našumas (angl. *Efficiency*) – sistemos vartotojų skaičius dažniausiai būna nepastovus, jis kinta dienos metu arba atitinkamais metų periodais. Išskirstytos sistemos padeda užtikrinti našų įrangos resursų naudojimą sumažinant įrangos galingumą (kai vartotojų skaičius yra nedidelis) bei padidinant galingumą (kai sistemos apkrova padidėja).

Išskirstytas sistemas galima kurti naudojant bet kokią programavimo kalbą(ActiveMQ [SBD11] naudoja Java programavimo kalbą, Apache Spark [Spa18] naudoja Scala programavimo kalbą). Viena populiaresnių programavimo kalbų naudojamų išskirstytų sistemų kūrime yra Elixir. Elixir yra dinaminė, funkcinė programavimo kalba skirta kurti išskirstytoms sistemoms. Elixir kalba veikia naudodama Erlang BEAM VM virtualią mašiną kurios pagalba galima kurti mažo delsimo, išskirstytas, trigdžiams atsparias sistemas.

Norint užtikrinti kūriamos sistemos kokybę dažnai yra rašomi testai. Testai padeda atskleisti programos klaidas arba pasakyti ar naujas kodas nepaveikė seniau parašyto funkcionalumo [Whi00]. Tačiau net ir laikantis geryjų testavimo praktikų nepavyksta išvengti programos klaidų. Net ir paskyrus daugiau resursų testavimui sudėtinguose sistemose, pilnas sistemos testavimas yra neįmanomas [SYC+04]. Norint rasti subtilesnius sutrikimus pačioje sistemos architektūroje, tokius kaip dalinis mazgų neveikimas, lygiagrečių algoritmų klaidos naudojant keletą procesų, gedimų atsparumo ir atsistatymo po gedimo algoritmų klaidos bei kitiems kraštutiniams veikimo scenarijams [NRZ+14] rasti ir išspręsti turime ieškoti kitų būdų. Vienas iš jų formalios specifikacijos.

Formalios specifikacijos yra matematinės technikos skirtos apibūdinti sistemų elgseną ir padėti kuriant jas naudojant griežtas ir veiksmingas priemones [HP95]. Turint sistemos formalią specifikaciją galima ja pasinaudoti vykdant formalų verifikavimą ir parodant, kad algoritmas yra

adekvatus pagal sukurtą specifikaciją. Sudarinėti formalią sistemos specifikaciją galima ir nepradėjus įgyvendinti sistemos, turint tik jos architektūrą. Formaliai verifikuota specifikacija suteikia informacijos apie architektūros korektiškumą ir įgalina objektyviai koreguoti sistemos architektūrą dar prieš pradedant ją įgyvendinti. Formalios specifikacijos sudaromos pasinaudojant tam tikromis kalbomis arba įrankiais. Viena iš tokių formalaus specifikavimo kalbų yra TLA$^+$ [Lam02].

TLA$^+$ yra formalios specifikacijos kalba, kurią sukūrė Leslie Lamport [Lam02]. Leslie Lamport 1980 metais sukūrė laiko veiksmų logiką (angl. *Temporal Logic of Actions*) [Lam94] pasinaudodamas Amir Pnueli 1977 metais sukurta laiko logika (angl. *Temporal Logic*) [Pnu77]. 1999 metais Leslie Lamport naudodamasis laiko veiksmų logika sukūrė formalaus specifikavimo kalbą TLA$^+$ [Lam02].

TLA$^+$ kalba yra skirta kurti konkurencinių ir išskirstytų sistemų formalias specifikacijas ir jas verifikuoti. Naudojant TLA$^+$ galima specifikuoti šias išskirstytų sistemų savybes [Lam19]:

1. Gyvumas – geri dalykai įvyksta programos vykdymo metu. Sistema galiausiai atliks jai paskirtą užduotį arba pateks į norimą būseną.

2. Saugumas – blogi dalykai neatsitiks programos vykdymo metu. Sistema nesustos veikti dėl netikėtai iškilusios klaidos.

Kadangi TLA$^+$ specifikacijos yra rašomos formalia kalba, tai leidžia patikrinti sukurtos specifikacijos saugumo ir gyvumo savybes.

Šias savybes mes galime patikrinti naudodamiesi TLC Model Checker (modelio tikrintoju). TLC yra išreikštinės būsenos (explicit-state) modelio tikrintojas, kurio paskirtis yra palaipsniui pasiekti visas galimas sistemos būsenas pagal nurodytą formalią specifikaciją [YML99]. Tačiau kartais pagal sukurtą formalią specifikaciją susidaro labai daug būsenų, kurias sistema gali pasiekti, todėl tampa nepraktiška naudoti TLC. Tokiu atveju galime naudotis TLA$^+$ specifikacijos įrodymo sistema TLAPS [CDL$^+$12]. TLAPS yra įrodymų sistema skirta patikrinti TLA$^+$ įrodymus. Šios sistemos paskirtis yra patikrinti pateiktus teoremų įrodymus. Įrodžius teoremą laikoma, kad TLA$^+$ specifikacija yra korektiška.

Yra ir kitų formalaus specifikavimo kalbų kurias galėtume naudoti šiame darbe. Viena iš jų Z formalaus specifikavimo kalba [ORe17], kuri sėkmingai buvo naudota specifikuoti UNIX failų sistemai [Bow96], bei Oxfordo universiteto paskirstytų skaičiavimų projekte [Bow96]. Dar viena formalaus specifikavimo kalba yra VDA [BC$^+$78], kuria buvo specifikuoti bendros atminties sinchronizavimo algoritmai [SVH98]. Tačiau šiam darbui buvo pasirinkta TLA$^+$ kalba dėl jos pritaikymo išskirstytoms sistemoms naudojant būsenų mašiną [Lam02], esamų sėkmingo pritaikymo pavyzdžių specifikuojant išskirstytas sistemas [18; Gus04; JHS20; NRZ$^+$14] bei gausaus TLA$^+$ įrankių pasirinkimo.

Temos aktualumas bei naujumas

Darbo tikslas

Sukurti metodą kuris mappina Elixir supervizijos medį yra TLA+ specifikaciją

Uždaviniai

1. Sukurti taisyklių rinkinį kuris išskirtų TLA+ specifikaciją iš Elixir supervizijos medžio kodo.
2. Pagal sudarytas taisykles įgyvendinti įrankį kuris Elixir kodą verčia į TLA+ specifikaciją.
3. Įvertinti sugeneruotos specifikacijos teisingumą.
4. Surasti atviro kodo sistemų naudojančių Elixir supervizijos medį ir patikrinti to kodo teisingumą sugeneruojant TLA+ speicifikaciją.

Laukiami rezultatai

1. Elixir supervizijos medžio kodo pavertimas į TLA+ specifikaciją
2. Įrodymas apie Elixir kodo pavertimo į TLA+ specifikaciją adekvatumas
3. Elixir kodo ir TLA+ specifikacijos sutapimo įvertinimas.
4. Praėjusiu Elixir -> TLA+ generavimo projekto papildymas

Hipotezė

- H0 (Nulinė hipotezė) – mappinimas tarp Elixir supervizijos medžio kodo ir TLA+ specifikacijos nėra įmanomas.
- H1 (Alternatyvi hipotezė) – egzistuoja metodas, kaip mappinti Elixir supervizijos medžio kodą į TLA+ specifikaciją.

Literatūra

[18] Raft formal specification with tla+, 2018. URL: https://github.com/ongardie/raft.tla/blob/master/raft.tla.

[BC+78] Dines Bjorner, JONES CB ir k.t. The vienna development method: the meta-language. 1978.

[Bow96] Jonathan Peter Bowen. *Formal specification and documentation using Z: A case study approach*, tom. 66. International Thomson Computer Press London, 1996.

[CDK05] George F Coulouris, Jean Dollimore ir Tim Kindberg. *Distributed systems: concepts and design*. pearson education, 2005.

[CDL+12] Denis Cousineau, Damien Doligez, Leslie Lamport, Stephan Merz, Daniel Ricketts ir Hernán Vanzetto. Tla+ proofs. *International Symposium on Formal Methods*, p. 147–154. Springer, 2012.

[GLA+13] Trinabh Gupta, Joshua B. Leners, Marcos K. Aguilera ir Michael Walfish. Improving availability in distributed systems with failure informers. *10th USENIX Symposium on Networked Systems Design and Implementation (NSDI 13)*, p. 427–441, Lombard, IL. USENIX Association, 2013-04. ISBN: 978-1-931971-00-3. URL: https://www.usenix.org/conference/nsdi13/technical-sessions/presentation/leners.

[Gus04] Jason Gustafson. Hardening kafka replication. https://kafka-summit.org/sessions/hardening-kafka-replication, 2004. Pristatymas konferencijoje.

[HP95] Gerard J Holzmann ir Doron Peled. An improvement in formal verification. *Formal Description Techniques VII*, p. 197–211. Springer, 1995.

[YML99] Yuan Yu, Panagiotis Manolios ir Leslie Lamport. Model checking tla+ specifications. *Advanced Research Working Conference on Correct Hardware Design and Verification Methods*, p. 54–66. Springer, 1999.

[JHS20] A Jesse Jiryu Davis, Max Hirschhorn ir Judah Schvimer. Extreme modelling in practice. *arXiv e-prints*:arXiv–2006, 2020.

[JW00] P. Jogalekar ir M. Woodside. Evaluating the scalability of distributed systems. *IEEE Transactions on Parallel and Distributed Systems*, 11(6):589–603, 2000. DOI: 10.1109/71.862209.

[Lam02] Leslie Lamport. *Specifying systems*, tom. 388. Addison-Wesley Boston, 2002.

[Lam19] Leslie Lamport. Safety, liveness, and fairness, 2019.

[Lam94] Leslie Lamport. The temporal logic of actions. *ACM Trans. Program. Lang. Syst.*, 16(3):872–923, 1994-05. ISSN: 0164-0925. DOI: 10.1145/177492.177726. URL: https://doi.org/10.1145/177492.177726.

[NRZ+14] Chris Newcombe, Tim Rath, Fan Zhang, Bogdan Munteanu, Marc Brooker ir Michael Deardeuff. Use of formal methods at amazon web services, 2014. URL: http://research.%20microsoft.com/en-us/um/people/lamport/tla/formal-methods-amazon.pdf.

[ORe17] Gerard O'Regan. *Z formal specification language*. *Concise Guide to Formal Methods: Theory, Fundamentals and Industry Applications*. Springer International Publishing, Cham, 2017, p. 155–171. ISBN: 978-3-319-64021-1. DOI: 10.1007/978-3-319-64021-1_8. URL: https://doi.org/10.1007/978-3-319-64021-1_8.

[Pnu77] A. Pnueli. The temporal logic of programs. *18th Annual Symposium on Foundations of Computer Science (sfcs 1977)*, p. 46–57, 1977. DOI: 10.1109/SFCS.1977.32.

[RP10] S. Ramabhadran ir J. Pasquale. Analysis of durability in replicated distributed storage systems. *2010 IEEE International Symposium on Parallel Distributed Processing (IPDPS)*, p. 1–12, 2010. DOI: 10.1109/IPDPS.2010.5470366.

[SBD11] Bruce Snyder, Dejan Bosnanac ir Rob Davies. *ActiveMQ in action*, tom. 47. Manning Greenwich Conn., 2011.

[Shi06] Kenneth W Shirriff. Method and system for establishing a quorum for a geographically distributed cluster of computers, 2006-3 21. US Patent 7,016,946.

[SYC+04] Kevin Sullivan, Jinlin Yang, David Coppit, Sarfraz Khurshid ir Daniel Jackson. Software assurance by bounded exhaustive testing. *Proceedings of the 2004 ACM SIGSOFT international symposium on Software testing and analysis*, p. 133–142, 2004.

[Smi18] Tom Smith. New research shows 63% of enterprises are adopting microservices architectures, 2018. URL: https://www.globenewswire.com/news-release/2018/09/20/1573625/0/en/New-Research-Shows-63-Percent-of-Enterprises-Are-Adopting-Microservices-Architectures-Yet-50-Percent-Are-Unaware-of-the-Impact-on-Revenue-Generating-Business-Processes.html.

[Spa18] Apache Spark. Apache spark. *Retrieved January*, 17:2018, 2018.

[SVH98] Noemie Slaats, Bart Van Assche ir Albert Hoogewijs. *Shared memory synchronization*. *Proof in VDM: Case Studies*. J. C. Bicarregui, redaktorius. Springer London, London, 1998, p. 123–156. ISBN: 978-1-4471-1532-8. DOI: 10.1007/978-1-4471-1532-8_5. URL: https://doi.org/10.1007/978-1-4471-1532-8_5.

[Whi00] J. A. Whittaker. What is software testing? and why is it so hard? *IEEE Software*, 17(1):70–79, 2000. DOI: 10.1109/52.819971.