VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
DEPARTMENT OF INTELLIGENT SYSTEMS

ROZŠÍRENIE NÁSTROJA ANACONDA PRE DYNAMICKÚ ANALÝZU PARALELNÝCH PROGRAMOV

AN EXTENSION OF THE ANACONDA TOOL

FOR DYNAMIC ANALYSIS OF CONCURRENT PROGRAMS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE **MICHAL HORŇÁK**
AUTHOR

VEDOUCÍ PRÁCE **Prof. Ing. TOMÁŠ VOJNAR, Ph.D.**
SUPERVISOR

BRNO 2017

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav inteligentních systémů Akademický rok 2016/2017

Zadání bakalářské práce

Řešitel: **Horňák Michal**
Obor: Informační technologie
Téma: **Rozšíření nástroje ANaConDa pro dynamickou analýzu paralelních programů**
An Extension of the ANaConDa Tool for Dynamic Analysis of Concurrent Programs
Kategorie: Analýza a testování softwaru

Pokyny:

1. Seznamte se s problematikou testování a dynamické analýzy paralelních programů s využitím vkládání šumu a extrapolující analýzy.
2. Seznamte s nástrojem ANaConDa pro dynamickou analýzu C/C++ programů na binární úrovni.
3. Navrhněte rozšíření možností nástroje ANaConDa o vhodně zvolené extrapolující analýzy a/nebo mechanismy vkládání šumu, které dosud nejsou v tomto nástroji podporovány.
4. Implementujte navržená rozšíření a otestujte je na testovacích případech nástroje ANaConDa, případně doplňte další vhodné testovací případy.
5. Shrňte a diskutujte dosažené výsledky a možnosti jejich dalšího rozšíření v budoucnu.

Literatura:

- Fiedor, J., Hrubá, V., Křena, B., Letko, Z., Ur, S., Vojnar, T.: Advances in Noise-based Testing of Concurrent Software, In: STVR, 25(3), Elsevier, 2015.
- Fiedor, J., Vojnar, T.: ANaConDA: A Framework for Analysing Multi-threaded C/C++ Programs on the Binary Level, In: Proc. of RV'12, LNCS 7687, Springer, 2012.
- Flanagan, C., Freund, S.N.: FastTrack: Efficient and Precise Dynamic Race Detection, In: Proc. of PLDI'09, ACM, 2009.
- Savage, S., Burrows, M., Nelson, G., Sobalvarro, P., Anderson, T.: Eraser: A Dynamic Data Race Detector for Multi-threaded Programs, In: Proc. of SOSP'97, ACM, 1997.

Pro udělení zápočtu za první semestr je požadováno:

- První dva body zadání a alespoň začátek práce na bodě třetím.

Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Vojnar Tomáš, prof. Ing., Ph.D.**, UITS FIT VUT
Konzultant: Fiedor Jan, Ing., UITS FIT VUT
Datum zadání: 1. listopadu 2016
Datum odevzdání: 17. května 2017

L.S.

doc. Dr. Ing. Petr Hanáček
vedoucí ústavu

Abstrakt

Cieľom tejto práce bolo implementácia algoritmu FastTrack pre dynamickú analízu viac-vláknových programov v jazyku C/C++. Ide o algoritmus detekujúci chyby typu data race. Je založený na relácii happens-before zakódovanej do tzv. vektor-klokov. Tie umožňujú extrapolovať beh programu a odhaľovať tak potenciálne chyby, ktoré sa v aktuálnom behu nevyskytli, ale v iných exekúciách by sa mohli vyskytnúť. Algoritmus je implementovaný v prostredí ANaConDA. Jedná sa o nástroj slúžiaci pre jednoduchšie implementovanie dynamických analizátorov monitorujúcich paralelné programy na binárnej úrovni. ANaConDA poskytuje analyzátorom potrebné informácie o behu programu, ktoré detektory následne využívaju k odhaľovaniu chýb.

Abstract

The main goal of this thesis is to implement algorithm FastTrack for dynamic analysis of multi-threaded programs in C/C++. FastTrack is algorithm which detects data race errors. It is based on happens-before relation encoded into the vector-clocks. Vector-clocks allows extrapolation of the execution which improves detection of potential errors, which were not seen in the actual run of the program however in other executions they could cause problems. Algorithm is implemented into the framework ANaConDA. ANaConDA is a tool for implementation of dynamic analyzers of parallel programs on binary level. It provides neccessary run time program informations for detectors use to discover concurency errors.

Kľúčové slová

dynamická analýza, FastTrack, ANaConDA, C, C++, data race, viac-vláknové programovanie, paralelné programy, vektor-klok, Djit+

Keywords

dnamic analysis, FastTrack, ANaConDA, C, C++, data race, multithreading, parallel programs, vector-clock, Djit+

Citácia

HORŇÁK, Michal. *Rozšírenie nástroja ANaConDA pre dynamickú analýzu paralelných programov*. Brno, 2017. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Prof. Ing. Tomáš Vojnar, Ph.D.

Rozšírenie nástroja ANaConDA pre dynamickú analýzu paralelných programov

Prehlásenie

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne pod vedením pána prof. ing. Tomáša Vojnara, Ph.D. a odborného konzultanta Ing. Jana Fiedora. Uviedol som všetky literárne pramene, zdroje a publikácie, z ktorých som čerpal.

.....
Michal Horňák
28. júla 2017

Poďakovanie

Rád by som sa poďakoval prof. ing. Tomášovi Vojnarovi, Ph.D., za poskytnutie možnosti pracovať na vývoji nástroja ANaConDA a Ing. Janu Fiedorovi za poskytnutú pomoc, čas a trpezlivosť ktorú mi venoval pri konzultáciách.

Obsah

Kapitola 1

Úvod

V súčastnosti sú viac-jadrové procesory výpočetným centrom každedého osobného počítača. Rozvoj takýchto procesorov priniesol viacero techník pracujúcich na báze súbežných výpočtov, ako je viac-procesorové programovanie (multi-processing) alebo viac-vláknové programovanie (multi-threading), ktoré umožňujú využívanie novo-vzniknutých výpočetných zdrojov. Takéto paradigma zvyšuje rýchlosť, s akou sa jednotlivé operácie v počitači vykonávajú vďaka paralelizácii, ktorá umožňuje množstvu činností prebiehať súčastne. Pochopitelne, so zvyšujúcim sa počtom operácií prebiehajúcich súbežne, musia aj vlákna, ktoré sprostredkovávajú tieto činnosti, zdieľať určité dáta s ostatnými vláknami. S takýmto nárastom komplexnosti prichádza aj značná množina rizík vznikajúcich:

- pri komunikácii s ostatnými vláknami počas prístupu ku zdieľaným dátam (data race) [2]
- pri prerušení vykonávania operácie vláknom a zmene kontextu v nepravý čas (atomicity violations) [10]
- pri prístupe k dátam, kedy vznikne kruhová zavislosť medzi vláknami čakajúcimi na uvoľnenie zdrojov, a tak žiadne z nich nie je schopné sa k dátam dostať (deadlock) [2]

K odhaľovaniu vyššie zmienených chýb boli vyvinuté techniky popísané v ďalších častiach tejto práce.

1.1 Téma práce

Táto práca sa zaoberá problémom chýb vznikajúcich v paralelných programoch, prevažne ich detekciou pomocou dynamickej analýzy [3], ktorá monitoruje program počas jeho exekúcie.

Cieľom je implementácia algoritmu pre dynamickú analýzu C/C++ programov nazývaného FastTrack [5], v prostredí ANaConDA [4]. ANaConDA je nástroj slúžiaci pre jednoduchšie implementovanie a využívanie dynamických analyzátorov k analyzovaniu bežiacich programov na binárnej úrovni. Toto prostredie zabezpečuje komunikáciu a poskytuje zdroje a informácie o analyzovanom programe pre daný dynamický algoritmus.

1.2 Motivácia

Motiváciou tejto práce je nedostatok nástrojov pre dynamickú analýzu C/C++ programov na binárnej úrovni. RoadRunner [6] už obsahuje implementáciu algoritmu FastTrack, no slúži len na analýzu java programov. V tejto práci ide o implementáciu tohto algoritmu pre C/C++ programy, naprogramovanom rovnako v jazyku C/C++.

Jedným z vyššie spomínaných nástrojov je ANaConDA. Problémom dynanickej analýzy je závisloť na konkrétnej exekúcii, kedy sa chyba prejaví len v malom počte z veľkého množstva behov programu. FastTrack umožňuje rýchlu detekciu data race chýb pomocou extrapolácie tzn., že dochádza k odvodeniu z jednej exekúcie množstvo podobných, a vo všetkých naraz hľadá chyby.

Implementačný jazyk

Hlavným motívom využívania jazykov ako sú C alebo C++, je dosiahnutie čo najvyššieho výkonu programu. Nástrojov na analýzu takýchto C/C++ programov je však málo a často krát nie sú určené pre analyzovanie skutočných programov z praxe. Nástroj ANaConDA predstavuje prostredie pre dynamickú analýzu práve programov implementovaných v jazykoch C a C++. Repertoár algoritmov, ktoré implementuje ANaConDA nezahŕňa niektoré významné analyzátori, čo bolo jednou z motivácií tejto práce.

Vlastnosti analyzátorov

Ďalšou motiváciou pre výber práve algoritmu FastTrack je jeho presnosť a rýchlosť. Existujú analyzátory ako napríklad Djit+ [14], ktorý sítce predstavuje presnú detekciu konkurentných chýb, no vytvára veľkú pamäťovú a výpočtovú záťaž. Na druhej strane je algoritmus AtomRace [10], ktorý detekuje chyby rýchlo, avšak len tie, ktoré v exekúcii nastali.
FastTrack kombinuje odľahčenú verziu Djit+ algoritmu čím redukuje záťaž a presnosť detekcie konkurentných chýb. Jeho implementácia v rozhraní ANaConDA umožňuje rýchlu analýzu programu a odhaľovanie chyby na každej zdieľanej položke.

Kapitola 2

Verifikácia viacvláknových programov

Táto kapitola sa zaoberá princípmi komunikácie a synchronizácie v konkurentných programoch, typmi chýb, ktoré môžu v takýchto programoch nastať/vyskytujú sa, a základnými prístupmi pre detekciu konkurentných chýb.

2.1 Viacvláknové programy

Schopnosť spúšťať viac ako jeden proces v rovnaký čas sa nazýva multi-processing. Proces pozostáva z vykonávaného programu a vlastného vyhradeného pamäťového priestoru. Vlákna sú odľahčená verzaia procesov, predstavujúca najmenšiu jednotku inštrukcií manažovatelných plánovačom, kde v jednom procese existuje viacero vlákien, ktoré delia záťaž do oddelených častí a umožňujú vykonávanie jednotlivých inštrukcií paralelne. Vlákna, ako odľahčená modifikácia procesov ponúkajú menšiu flexibilitu, no umožňujú rýchlejšiu inicializáciu a rýchlejšie prepínanie kontextu. V rovnakom procese zdieľajú spoločný pamäťový priestor (heap), ale každému vláknu je zároveň priradený aj vlastný vyhradený priestor (tvz. thread-local storage) resp. zásobník, ktorý je individuálny pre každé vlákno. Moderné objektovo-orientované programovacie jazyky dovoľujú programátorom vytvárať viac-vláknové programy, ktoré však výrazne zvyšujú šancu vzniku chýb v kóde. Konkurentné chyby sú jednoduché na vytváranie, no na druhej strane náročné na odhaľovanie.

Príkladom môže byť triviálny program, ktorý inkrementuje hodnotu zdieľanej premennej x prostredníctvom vlákien $t1$ a $t2$. Obe vlákna vykonávajú príkaz $x = x + 1$. Táto operácia však môže pozostávať z viacerých, dielčích inštrukcií. Ak nie sú prístupy do pamäte synchronizované, môže nastať situácia, kedy si obe vlákna načítajú súčastne inicializačnú hodnotu premennej nezávisle na sebe a následne ju inkrementujú. Na spoločnom výstupe bude mať x hodnotu 1, z dôvodu súbežného prístupu k premennej bez dodatočnej synchronizácie. Dochádza teda k chybe nazývanej porušenie atomicity (sekcia 2.2.2). Riešením takéhoto problému je, aby jednotlivé vlákna pristupovali ku premenným jednotlivo alebo aby operácie čítanie a zápis boli atomickými.

2.1.1 Komunikácia a synchronizovanie v konkurentných programoch

Jednou z možností ako zabezpečiť program pred konkurentnými prístupmi v zdieľanej pamäti je požadovať, aby každé vlákno najskôr zabralo synchronizačný zámok chrániaci prístup ku premennej a následne ku nej pristupovalo. Takýto spôsob však vytvára zbytočnú

výpočtovú záťaž. Lepší spôsob je zohľadňovať ďalšie synchronizačné primitíva a špecifické situácie, pri ktorých nie je potrebné uskutočňovať synchronizáciu a vytvárať výlučný prístup len v prípadoch, kedy to je nutné.

Pri exkluzívnom prístupe vlákna k premennej sú ostatné vlákna blokované a nemôžu k zdieľanému zdroju pristupovať. Vlákno musí najskôr zabrať zdieľanú položku pre seba, a tým blokovať ostatné prístupy. Blokovanie zabezpečujú rôzne typy synchronizačných primitív vymenovaných nižšie. Ak je položka zamknutá, musí vlákno počkať, kým sa zdroj odomkne a následne ho môže zabrať. Takáto situácia, kedy viacero uchádzačov bojuje o rovnaké zdroje, negatívne vplíva na výkon viac-vláknových programov, lebo dochádza ku sekvenčnému prístupu, a tým zároveň ku serializácii výpočtu a degradácii výkonu. Sekcia, ktorá je vykonávaná mezdi dvoma prvkami zabezpečujúcimi výlučný prístup sa nazýva kritická sekcia.

Na to, aby vlákna mohli komunikovať, potrebujú synchronizovať svoje operácie, a tým zdieľať informácie s okolím. Vlákna alebo procesy spolu môžu komunikovať cez správy odosielané cez spoločný kanál alebo si môžu vymieňať údaje cez zdieľanú pamäť. Komunikácia pomocou správ je zvyčajne rozšírená v synchronizácii medzi viacerými procesmi (zvyčajne v distribuovaných systémoch [9]). Zdieľaná pameť je preferovaná u vlákien, kde v jednom procese umožňuje vláknam komunikovať medzi sebou.

Operačný systém poskytuje nízko-úrovňové synchronizačné mechanizmi:

- spinlock
- semafór
- zámok
- barriéra
- podmienené premenné (condition variables) atď.

Programovacie jazyky ďalej vytvárajú pokročilejšiu synchronizáciu ako nadstavbu nad funkciami OS. V C/C++ jazykoch je sychnronizácia vykonávaná prostredníctvom volaní synchronizačných funkcií. Preto analyzátory, ktoré analyzujú C/C++ programy musia stopovať a monitorovať volania funkcií a hodnoty ich parametrov, ktoré reprezentujú synchronizačné primitíva, aby dokázali odhaliť, kedy nastáva synchronizácia a nad akým synchronizačným objektom. Takéto stopovanie je náročné na implementáciu, preto sú analyzátory integrované do prostredí, ktoré takéto problémy riešia globálne pre všetky detektory, ako je tomu aj v nástroji ANaConDA [4].

Existuje viacero metód ako v programe vytvárať synchronizáciu:

- globálne zámky
- jemné zamykanie (fine-grained locking)
- transakčná pamäť [7]

Globálne zámky sú využívané globálne naprieč procesom. Jedno vlákno zamkne globálne prístup do zdieľanej pamäte a ostatné vlákna musia počkať na jej odblokovanie. Takýto prístup je jednoduchý na použitie, no s ním aj degraduje výkon aplikácie kvôli serializácii prístupov.

Ďalším spôsobom je jemné zamykanie, predstavujúce snahu o zamykanie prístupov pre každú zdieľanú položku zvlášť a len na miestach, kde je to nutné. Určiť nutnosť existencie

zámku v danej situácii však nie je jednoduché, preto je tento prístup náchylný na množstvo chýb. Pri zlom poradí zamykania môže vzniknúť deadlock alebo pri zlom zámku nemusí vzniknúť žiadna synchronizácia, z čoho vznikajú data race chyby (2.2.1). Oproti globálnym zámkom však pri správnej synchronizácii predstavuje výrazný nárast výkonu.

Tretím spôsobom je využitie transakčnej pamäte. Tá monitoruje sekvencie inštrukcií načítania (load) a uloženia (store) do pamäte, ktoré sú vykonané atomicky. Ak dôjdeku porušeniu atomicity, je výsledok všetkých operácií anulovaný a hodnoty v pamäti sú navrátené do stavu pred vykonaním celej sekvencie. Transakčná pamäť predstavuje alternatívu ku synchronizácii pomocou zámkov. Je kombináciou jednoduchého používania a následného dobrého výkonu programu, no nevylučuje existenciu chýb.

2.2 Chyby vo viac-vláknových programoch

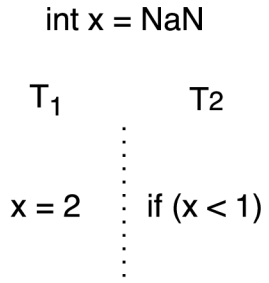
Viac-vláknové programy vytvorili možnosť pre príchod nepravidelných, konkurentných chýb [2], ktoré sú veľmi ťažko detekovatelné pomocou bežných testovacích metód. Hlavným problémom je, že viac-vláknové programy môžu byť vykonané rozlišne pri násobnom spustení aplikácie s rovnakou inicializáciou, ale nedeterministickým usporiadaním vlákien.

2.2.1 Data race

Časovo závislá chyba nad dátami (data race) [8], je jednou z najčastejšie sa vyskytujúcich chýb v konkurentných programoch. K identifikácii výskytu data race chyby v behu konkurentného programu, je nevyhnutné určiť (1) ktoré premenné sú zdieľané pre akúkoľvek dvojicu vlákien (2) či akákoľvek dvojica prístupov k danej premennej je synchronizovaná.

Definícia 1 *V programe sa nachádza data race, ak dve predom nesynchronizované vlákna pristupujú ku zdieľanej premennej súčastne a minimálne jedna operácia je zápis.*

Nasledujúci obrázok 2.1 zobrazuje situáciu, kedy za určitých okolností môže dôjsť ku chybe v súbežnom prístupe do pamäte. Jedna z možností ako by sa program mohol správať je, že by sa operácia porovnania vo vlákne T_2 vykonala ako prvá, ktorá nepredstavuje číselnú hodnotu a zostáva na programovacom jazyku ako sa k tejto situácii zachová. Druhou možnosťou je priebeh v poradí priradenie nasledované podmienkou. V tomto prípade by potenciálna chyba zostala nepovšimnutá. Poslednou možnosťou je problém atomických operácií vysvetlovaných už na príklade v sekcii 2.1. Ako sa detekujú takéto chyby pomocou dynamickej analýzy je podrobnejšie vysvetlené v sekcii 3.1.



Obr. 2.1: Obrázok zobrazuje pseudokód programu, v ktorom sa vyskytuje potenciálna data race chyba.

2.2.2 Porušenie atomicity

Atomická operácie predstavuje vykonanie jednotného príkazu a to tak, že systém rozpoznáva len 2 stavy: stav pred a stav po vykonaní atomickej operácie a nevidí žiaden medzistav. Porušenie atomicity je často spájané a nekorektne označované ako data race chyba. Navonok jednotné a atomicky pôsobiace operácie môžu pozostávať z viacerých inštrukcií, ktoré sa vykonávajú samostatne, sériovo. Ak sú takéto neatomické operácie vykonávané paralelne, môže dôjsť ku nesynchronným prístupom do pamäte počas vykonávania nezosynchronizovaných atomických operácií tvoriacich jednotný, zdanlivo atomický príkaz.

Definícia 2 *Beh programu porušuje atomicitu, ak nie je možné nájsť ekvivalentný beh v ktorom všetky atomické sekcie sú vykonané sériovo.*

2.2.3 Ostatné chyby

Nasledujúce chyby [2] v konkurentných programoch predstavujú nemenej významné problémy, no z hľadiska tejto práce sú okrajové.

Uviaznutie (deadlock) - uviazdnutie predstavuje situáciu, v ktorej dva a viac procesov (v našom prípade vlákien) čaká na podmienky, ktoré nemôžu nastať. Dve vlákna sa nachádzajú v stave uviaznutia, ak prvé vlákno je blokované a čaká na udalosť, ktorá by ho odblokovala, ale táto udalosť je vykonaná druhým vláknom, ktoré rovnako čaká v blokovanom stave na udalosť sprostredkovanú prvým vláknom - cyklická závyslosť medzi prvým a druhým vláknom.

Nesprávne poradie - k takejto chybe dochádza v prípade, kedy nastáva porušenie určitých požiadaviek na poradie vykonávaných operácií (napr. súbor musí byť otvorený skôr ako používaný) a tieto akcie nenastanú v očakávanom poradí.

Zmeškaný signál - zmeškaný signál predstavuje správu, ktorá mala byť doručená určitému vláknu, no doručenie nenastalo. Buď bola správa odoslaná inému vláknu, alebo skôr ako na ňu správne vlákno začalo čakať.

Blokované vlákno - blokované vlákno čaká na udalosť v programe, ktorá by ho odblokovala, no v behu programu takáto udalosť nikdy nenastane.

Uviaznutie s aktívnym čakaním (livelock) - rozdiel medzi livelock a deadlock je, že pri livelock sa vykonáva naviac (napríklad cyklus), teda niečo robia, ale vlákna nie sú označené ako blokované a aktívne čakajú na odblokovanie.

2.3 Metódy pre analýzu programov

2.3.1 Programové testovanie

Jedným z najbežnejších prístupov k vyhľadávaniu chýb v software je programové testovanie. Účelom testovanie je odhalenie chýb, ktoré vedú ku neočakávanému správaniu programu. Bežným postupom pri testovaní je systematické spúšťanie testovacích prípadov, ktoré tvoria jednotlivé testy a ich vstupy a výstupy. Výstupom testovacieho procesu je odpoveď áno / nie, či program alebo programová časť funguje správne/nesprávne. Avšak nájsť testovacie prípady, ktoré overia dostatočnú časť správania sa programu nie je jednoduché.

Problém odhaľovania chýb v súbežných programoch pomocou testovania je vo všeobecnosti obtiažny, z dôvodu veľkého množstva preložení vlákien a prirodzenému nedeterminizmu v plánovaní poradia vykonávania operácií vláknami počas exekúcie programu. Teda viacero exekúcií totožného programu s rovnakými parametrami môže viesť k rôznym výsledkom. Preto jediné spustenie a otestovanie programu nie je dostačujúce pre evaluovanie korektnosti aplikácie.

2.3.2 Dynamická analýza

Dynamickú analýzu [15] [14] je možné využívať aj bez znalosí zdrojového kódu, ktorý je naopak potrebný pri statickej analýze, a tak nie sú potrebné pre analýzu implementačné detaily monitorovanej aplikácie. Ide o metódu založenú na stopovaní priebehu programu (program tracing), ktorá zbiera informácie o aktuálne spustenej instancii programu, a tie sú analyzované za účelom odhalenia chýb. Navzdory tomu, že analýza pracuje s informáciami pochádzádzajúcimi len z jediného behu, často krát dokáže odhaliť chyby, ktoré nie sú priamo vykonávané v spustenom programe vďaka extrapolácii. Nevýhodou dynamického monitorovania kódu je problém prehliadnutia kritických scenárov aplikácie, pretože analýza sleduje len aktuálny beh, ale nemonitoruje behy, ktoré by mohli nastať zmenou použitia programu a najmä zmenou preloženia vlákien a tým spôsobenou zmenou vykonávania operácií. Výhodou pozorovania len jednoho behu programu za jeho exekúcie je dobrá škálovateľnosť, čím zvládne pomerne rozsiahle programy a umožňuje prácu s presnými informáciami.

- – Analýza jednoho behu
- \+ Dobrá škálovateľnosť
- \+ Presné informácie o behu

2.3.3 Statická analýza

Statická analýza [1] je prístup k overovaniu programov z oblasti formálnej verifikácie. Je založená na princípe získavania informácií zo zdrojového kódu bez toho, aby bol program spustený. Oproti predchádzajúcim metódam verifikácie software, nie je statická analýza závislá na jednom spustení programu, čo jej umožňuje v teórii preskúmať aj cesty programu, ktoré by boli veľmi ťažko dostuné pri bežnom testovaní. Táto skutočnosť však znamená, že je potrebné preskúmať exponenciálny počet možných preložení a usporiadavaní vykonávania udalostí, čo však v praxi nie je príliš reálne. Statická analýza vychádza z kódu analyzovanej aplikácie, k čomu však nevyžaduje prostredie programu (knižnice, vstupy, výstupy atď.), tým prispieva k vysokej miere možnej automatizácie. Keďže táto technika neprebieha počas behu programu (pracuje offline), znamená to tiež, že využíva na analýzu len zdroje poskytované z kódu programu, čo v praxi znamená stratu špecifických informácií o programe (ako napríklad konkurentné informácie o vstupoch a výstupoch, s ktorými môže program pracovať) a následne možný vznik falošných alarmov. Falošné alarmy predstavujú chyby, ktoré sa v programe vôbec nevyskytujú, lebo statická analýza overuje aj behy so vstupmi a výstupmi, ktoré nikdy nenastanú.

\+ Analýza všetkých možných exekúcií

\– Slabá škálovateľnosť pri analýze

\– Minimálne informácie o behu

2.3.4 Model checking

Model checking [13] je ďalšou, plne automatizovanou technikou formálnej verifikácie na odhaľovanie chýb vo viac-vláknových programoch. Táto metóda je založená na princípe zjednodujšeného modelu zdrojového kódu a postupnom priechode všetkými jeho stavmi. Problémom tejto metódy overovania software je množstvo stavov, v ktorých sa systém môže nachádzať, a ktoré treba monitorovať, čo vytvára výraznú časovú a pamäťovú náročnosť.

Kapitola 3

Dynamická analýza

Dynamická analýza spomínaná už v 2.3.2, predstavuje populárnu metódu verifikácie konkurentného software, najmä z hľadiska relatívne jednoduchého nasadzovania (spustím a sledujem) a dobrej škálovatelnosti umožnujúcej analyzovať aj komplexné programy. Okrem sledovania výstupov behu programu, je možné takpovediac vstúpiť do programu, preskúmať a zozbierať určité informácie na základe ktorých je možné určiť či v programe existuje potenciálne miesto vzniku chyby. Táto technika vkladania dodatočného kódu do programu na konkrétne miesta sa volá inštrumentácia kódu [4]. Odhalenie potenciálneho miesta chyby práve preto, lebo dynamická analýza dokáže rozšíriť princíp testovania takým spôsobom, že extrapoluje a vyhodnocuje nie len udalosti v konkrétnom behu programu, ale zároveň aj množstvo ďalších exekúcií odvodených od inicializačného behu. Avšak pri veľkej abstrakcii (odvodení ďalších behov) nie všetky hlásenia sú hlásenia o chybe v programe, ale typicky ide o chyby v abstrakcii, čo predstavuje falošné alarmy.

3.1 Detekovanie konkurentných chýb

Dynamická analýza sa využíva na detekovanie najbežnejších konkurentných chýb spomenutých v sekcii 2.2. Táto práca sa zaoberá odhaľovaním data race chýb pomocou FastTrack algoritmu, a preto sa aj aktuálna sekcia primárne sústreďuje na bližšie definovanie data race stavov a ich odhaľovanie v paralélnom software.

3.1.1 Data Race chyby

Jedným z najznámejších problémov konkurentných programov sú chyby v súbežnosti (chyby typu data race). Jedná sa o chybu simultánneho prístupu vlákien do zdieľanej pamäte. Pretože tieto chyby spôsobujú nepredvídatelné správanie programu, ich odhaľovanie je veľmi dôležité pri testovaní software. Techniky pre detekovanie data race chýb sú založené, buď na princípe locksetov alebo happens-before relácie.

Lockset analyzátory

Lockset algoritmy sú založené na princípe synchronizácie pomocou zámkov. Podmienkou je, aby každá zdieľaná pamäťová položka mala definovaný výlučný prístup, takže nemôže dôjsť k súbežnému prístupu dvoch konkurentných vlákien, a teda nemôže nastať data race chyba. V základe Lockset algoritmus kontroluje zamykanie premenných tak, aby dochádzalo len ku výlučným prístupom. Porušenie takejto logiky však nemusí znamenať data race

chybu, z čoho vzniká problém hlásenia veľkého množstva nevyžiadaných falošných chýb, ktoré skrívajú reálne data race chyby. Princíp algoritmu Lockset je využívaný v analyzátore Eraser [15], ktorý vykazuje veľmi dobré výsledky.

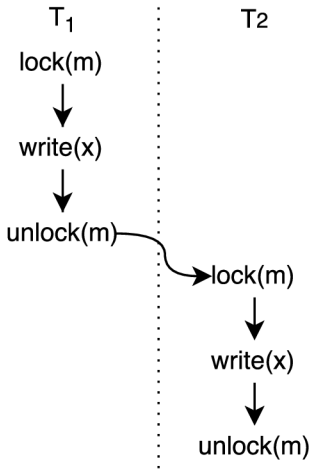
Happens-before (H-B) analyzátory

Happens-before relácia sa využíva pre určenie čiastočného zoradenia udalostí v paralelných programoch, bez využitia fyzických hodín. Happens-before relácia na princípe distribuovaných systémov je popísana v [9] nasledovne. Uvažujeme systém pozostávajúci z procesov obsahujúcich kolekciu sekvencie udalostí. Jeden proces je definovaný ako sada udalostí s úplnym usporiadaním, teda udalosti sa vykonávajú postupne v poradí za sebou (a *happens before* b). Predpokladáme, že zaslanie alebo prijatie správy je jedna udalosť v procese, potom môžme definovať "happenes before"reláciu, zapísanú ako " $\rightarrow$ " takto:

Definícia 3 (H-B) *Relácia* $\rightarrow$ *medzi skupinou udalostí viacerých procesov je najmenšia relácia spĺňujúca tieto tri podmienky:*

- *ak* a *a* b *sú udalosti v rovnakom procese a* a *predchádzalo* b*, potom platí* $a \rightarrow b$ *(program order)*
- *ak* a *je odosielateľ a* b *je adresát rovnakej správy (udalosti) ale v inom procese, potom* $a \rightarrow b$
- *ak* $a \rightarrow b$ a $b \rightarrow c$ *potom* $a \rightarrow c$ *(tranzitivita)*

Dve nezhodujúce sa udalosti a *a* b *sú považované za konkurentné ak* $a \nrightarrow b$ a $b \nrightarrow a$



Obr. 3.1: Lamportova H-B relácia

V prostredí paralelných (viac-vláknových) programov sa jedná o podobný princíp. V každom vlákne sú udalosti usporiadané sekvenčne za sebou. Medzi vláknami sú udalosti zoradené na základe toho, ako dochádzalu ku synchronizovaniu medzi vláknami, a aké synchronizačné primitíva boli využité. Ak jedno vlákno pristupuje ku synchronizačnému objektu a ďalší prístup prichádza z iného vlákna, potom je prvý aj druhý prístup synchronizovaný a definovaný ako H-B relácia medzi prvým a druhým vláknom. Ku príkladu, na obrázku 3.1 je znázornený úsek synchronizácie dvoch vlákien. Treba zdôrazniť, že uzamknutie objektu

v poradí ako je na obrázku je len jedna z možných variant. V inom prípade by vlákno T_2 mohlo zabrať zámok m ako prvé. Všetky tri operácie vo vlákne T_1 sú zoradené podľa happens-before relácie, lebo sú spúšťané sekvenčne v rámci jednoho vlákna. Udalosť $lock(m)$ vlákna T_2 dodržiava happens-before reláciu s operáciou $unlock(m)$ vlákna T_1, lebo zámok m môže byť vlastnený maximálne jedným vláknom a nemôže byť zabratý pred tým, ako ho uvolní aktuálny vlastník. Nakoniec tri operácie odohrávajúce sa vo vlákne T_2 sú rovnako zoraden ako v prípade T_1.

Ak dve vlákna pristupujú k rovnakej premennej a prístupy nie sú zoradené podľa happens-before relácie, potom v ďalších behoch programu môže dôjsť k zmene rýchlosti vykonávania operácií vlákanmi a vzniká riziko simultánneho prístupu, čo pri určitých prípadoch, kedy je aspoň jeden prístup zápis, môže nastať až data race chyba. Algoritmy založené na takomto princípe využívajú zakódovanie happens-before relácie v podobe vektorových hodín podrobnejšie vysvetlených v 5.1.

3.2 Vkladanie Šumu

Vkladanie šumu [3] je technika využívaná v prostredí testovania a dynamickej analýzy, pre zvyšovanie šance na odhalenie chýb ovplivňovaním plánovania vlákien programu. V princípe ide o to, vo vhodný okamžik pozastaviť alebo spomaliť vlákno pomocou šumu a umožniť ostatným vláknam postupovať ďalej vo vykonávaní ich kódu. Tým pádom dochádza ku zmene poradia vykonávaných operácií programu a zvyšuje sa tak šanca pozorovať scenáre, ktoré by mohli viesť ku chybám, ale nenastali by za bežných podmienok prostredia.

Šum sa vkladá do programu pomocou takzvanej inštrumentácie bližšie vysvetlenej v sekcii 4.1. Ide o vloženie kódu generujúceho šum do sledovaného programu, a tým pádom táto metóda nevyžaduje žiadnu modifikáciu originálnych testov a prostredia, v ktorom sa program spúšťa.

Pri vkladaní je potrebné riešiť dva problémy: (1) Kedy vytvárať šum a (2) akým spôsobom ovplivniť program (aký typ šumu vložiť). Pri vyberaní miesta inštrumentácie šumu je dôležité zvážiť či na danom mieste bude mať efekt. Vkladať šum na miesta v kóde, ktoré neovplivňujú synchronizáciu alebo komunikáciu medzi vláknami je bezpredmetné. Z tohto dôvodu je vhodné vyberať miesta ovplivňujúce konkurentné správanie ako je spúšťanie udalostí pôsobiacich na synchronizáciu a prístupy do zdieľanej pamäte. Pri vložení monitorovacieho kódu pred každú inštrukciu môže vznikať problém vyrušenia šumu, kedy sa jednotlivé inštrumentované rutiny vyrušia a dochádza v súčte len ku veľkému spomaleniu. Existujú rôzne heuristické metódy na určenie miest pre inštrumentovanie šumu. Jednoduchým a lacným riešením je využiť pseudo-náhodného generátoru a pomocou neho vkladať šum náhodne. Do programu sa vkladajú rôzne typy šumu:

- Zastavenie vlákna na určitú dobu alebo do určitej udalosti (sleep/wait)
- Opakované volanie inštrukcie pre uvolnenie procesoru (yield)
- Vykonávanie nadbytočného kódu (busy-wait)

Úspešnosť analýzy závisí na behu, ktorý algoritmus videl. V kombinácii šumu, ktorý umožňuje vidieť aj iné scenáre ako tie za bežného testovania s rovnakým prostredím a dynamickou analýzu, ktorá to obalí do abstrakcie umožňujúcej monitorovať aj okolité scenáre, rastie šanca na odhalenie chyby.

Kapitola 4

ANaConDA

ANaConDA - "adaptable native-code concurrency-focused dynamic analysis"[4], je platforma pre vytváranie dynamických analyzátorov, postavená nad nástrojom PIN [11]. Umožňuje monitorovanie paralelných C/C++ programov na binárnej úrovni, za účelom odhalenia konkurentných chýb vo viac-vláknových aplikáciách (sekcia 2.2). Cieľom nástroja je zjednodušenie vytvárania dynamických analyzátorov pre analyzovanie viac-vláknových C/C++ programov. Analyzátorom poskytuje monitorovaciu vrstvu, ktorá zbiera informácie o bežiacom programe a interpretuje oznámenia o dôležitých udalostiach ako sú synchronizácia alebo prístupy do pamäte, čím do seba zabaľuje laicky "bonzovaciu"vrstvu a dovoľuje ju využívať analyzátrom, a tým zjednodušuje vývoj ďalších analyzátrov. ANaConDA zároveň poskytuje injektovanie šumu (sekcia 3.2) do programu, vďaka čomu umožňuje analyzátorom zlepšiť pokrytie možných situácií medzi vláknami, a tým udhaliť viacej chýb.

Sondy Sondy slúžia k získaniu konkrétneho typu informácií o behu testovaného objektu. ANaConDA má možnosť sledovať množstvo informácií:

- Prístupy do pamäte
- Synchronizovanie vlákien
- Spúštanie a ukončenie behu vlákien
- Postupnosti volaní
- Volané funkcie a ich parametre

Implementované analyzátory ANaConDA v súčastnosti podporuje radu analyzátorov:

- AtomRace [10] - analyzátor na odhaľovanie chýb typu data race
- Contract-validator - detektor porušenia kontraktov[1] pre súbežnosť
- Data-validator
- Goodlock - detektor uviaznutí

[1]Kontrakty umožňujú popísať ako volať funkcie v paralelnom programe, aby nedošlo ku chybám ako je porušenie atomicity, nesprávne poradie a zmeškaný signál

- Hldr-detector - detektor High-level data race (podmnožina chýb typu porušenie atomicity)
- Tx-monitor - analyzátor práce s transakčnou pamäťou [2]

4.1 Inštrumentácia kódu

Inštrumnetácia [4] je technika pre vkladanie dodatočného kódu do aplikácie, ktorý umožňuje monitorovanie či modifikovanie behu programu.

Inštrumentačné nástroje ako Pin alebo Valgrind [12], sa vo veľkej miere používajú pre zbieranie informácií o exekúcii programu. Tieto dáta môžu byť efektívne využívané pri odchytávaní chýb programov, optimalizáciách alebo verifikácii bezpečnosti.

Existujú tri možnosti kam monitorovací kód umiestniť: do zdrojového kódu, medzikódu alebo do binárneho kódu. Inštrumentácia na binárnej úrovni poskytuje značné výhody oproti ostatným vrstvám. Pri analyzovaní programu, od ktorého užívateľ nemá zdrojové kódy, môže byť veľký problém najmä pri práci s knižnicami. Tie však analyzátor, ktorý pracuje pomocou inštrumentácie na binárnej úrovni nepotrebuje. Ďalšou výhodou je lepšia presnosť vkladania kódu, keďže sa pohybujeme na strojovej úrovni inštrumentačný nástroj môže vkladať kód presne na potrebné miesto a nedochádza ani k nechceným optimalizáciám kódu prekladačom, ktorý by mohol monitorovací kód rôznym spôsobom modifikovať. Inštrumentácia zdrojových kódov je značne závislá na implementačnom jazyku, čo pri binárnej neplatí. Existujú dva prístupy k binárnej inštrumentácii.

Statická binárna inštrumentácia vkladá kód do programu pred jeho spustením, a tým trvalo modifikuje obsah jeho binárnych súborov. Tento prístup môže byť výhodnejší, lebo pri modifikovaní testovaného programu vkladá kód pred spustením, čím odpadá záťaž, ktorú vytvára dynamická inštrumentácia. Statická inštrumentácia však nie je schopná inštruovať zdieľané knižnice pokial nie sú inštruované oddelene od originálnych, ktoré využívajú aj iné programy a pri ich modifikovaní by dochádzalo ku chybám. Taktiež umožňuje menšiu flexibilitu, keďže inštrumentačný kód zotrváva v programe počas celej doby exekúcie.

Dynamická binárna inštrumentácia na druhej strane vkladá inštrumentačný kód až počas exekúcie programu bez toho, aby došlo k permanentným modifikáciám akéhokoľvek kódu. Dokáže pracovať s dynamicky generovaným kódom, ktorý nie je známy pred spustením programu a pre statickú analýzu je prakticky nedosiahnuteľný. Tým, že dynamická inštrumentácia pracuje s kópiami binárnych zdrojov, dáva priestor pre analyzovanie knižníc využitých v testovanom programe a súbežne dovoľuje použitie rovnakých knižníc ostatným programom, čo v prípade statickej inštrumentácie nie je možné bez udržiavania dvoch separátnych verzií knižníc a ukazateľov (linkov) na ne. Nevýhodou je, už spomínaná opakovaná réžia pri každom spostení analýzy, čo môže predstavovať problém najmä pri časovo alebo priestorovo náročných programoch.

[2] Transakčná pamäť je nový spôsob synchronizácie vlákien kedy je kód vykonaný paralelne a pokial bola porušená jeho atomicita, je vlákno vykonávajúce tento kód vrátené do stavu perd jeho vykonaním (rollback)

4.2 Intel PIN

Pin [11] je inštrumentačný nástroj, ktorý vykonáva dynamickú (run-time) binárnu inštrumentáciu C/C++ programov. Dovoľuje nástrojom vkladať dodatočný kód (v jazykoch C/C++) na ľubovolné miesta v spustiteľnom kóde. Pin ponúka bohaté aplikačné rozhranie, ktoré abstrahuje vrstvu inštrukčnej sady a dovoľuje tak kontextovým informáciám, ako sú obsahy registrov a pamäte, aby mohli byť predané do injektovaného kódu ako parametre. Pin automaticky ukladá a obnovuje registre, ktoré boli prepísané vkladaným kódom, takže aplikácia naďalej pokračuje v činnosti. Ako nástroj dynamickej binárnej inštrumentácie vykonáva Pin inštrumentáciu počas behu preložených binárnych súborov, teda nevyžaduje rekompilovanie zdrojových kódov a podporuje inštrumnetáciu programov, ktoré dynamicky vytvárajú svoj vlastný kód. Dokáže sa dynamicky pripojiť ku bežiacemu procesu, inštrumentovať ho a odpojiť, čím redukuje výpočtové náklady najmä u veľkých systémov. Pin pracuje ako "just in time"(JIT) prekladač. Vstupom prekladača nie je bytekód ale spustiteľný súbor. Pin pozdrží vykonanie prvej inštrukcie programu a vygeneruje novú sekvenciu kódu, takmer identickú ku originálu, ale zabezpečuje, aby po vykonaní novovygenerovaného kódu opäť prevzal kontrolu a generoval ďalši kód. V JIT móde je vykonávaný len novo-vygenerovaný kód, zdrojové dáta sú využívané len ako referencie. Práve pri generovaní nového kódu Pin umožňuje užívateľovi vložiť (inštrumentovať) dnu svoj vlastný kód. Nástroj ANaConDA využíva Pin z viacerých dôvodov:

- podporuje dynamickú binárnu inštrumentáciu
- neobmedzuje viac-vláknové programy (neserializuje ich exekúciu)
- dokáže sprostredkovať inštrumentáciu zdieľaných knižníc
- zvláda seba-modifikujúci kód
- umožňuje inštrumentáciu v prostredí Windows, Linux, MacOS

4.3 Vkladanie šumu v prostredí ANaConDA

AKo bolo už spomínané v sekcii 3.2, vkladanie šumu sa zameriava na zvýšenie počtu pozorovaných usporiadaní vlákien narúšaním plánovania vlákien programu. Toto je dosiahnuté pomocou vloženia špecifického kódu do programu na niektoré miesta a cieľom je prinútit testovaný program ku prepnutiu vykonávaného vlákna na iné.

Nástroj ANaConDa implementuje vkladanie viacerých typov šumu, primárne využívané sú hlavne yield a sleep, ktoré vykazujú úspešné výsledky aj v ďalších analyzátoroch pre dynamickú analýzu [4].

- **Yield** umožňuje vláknu vzdať sa procesoru, čo dovoľuje ostatným vláknam prebrať iniciatívu a pokračovať vo vykonávaní svojej činnosti.
- **Sleep** sa vzdá procesoru a na určitú dobu sa uspí, čím zamedzí spätnému prepnutie vlákien na určitú dobu.

Pri vkladaní treba odhadnúť rozumnú mieru sily šumu. Pri vkladaní yield, sa jedná o počet volaní tejto funkcie. Pri vkladaní sleep zas treba určiť, na ako dlho sa má dané vlákno uspať.

4.4 Princíp analýzy programu

V princípe ide o komunikáciu medzi analyzátorom a ANaConD-ou nasledovne. Analyzátor by vyžadoval sledovanie určitých udalostí v programe. Zaujíma sa hlavne o to, čo sa deje vo vnútri.

- interné dátové štruktúry
- volania pri danej operácii
- synchronizácia (zámky)
- volania podprogramov

ANaConDA pomocou vlastných sónd riadi zber týchto informácií a predávanie ich analyzátorom. Analyzátor musí byť vo forme zdieľaného objektu (pre Linux) alebo dynamickej knižnice (pre Windows), ktoré obsahujú špecificky pre každý algoritmus implementované funkcie, a ktoré sú následne volané pri požadovaných udalostiach (synchronizácia, prístup do pamäte atď.). Analyzátor musí zaregistrovať spätné volania funkcií pre udalosti, o ktoré má záujem.

Pin využíva ANaConD-u ako zásuvný modul, pomocou ktorého registruje spätné volania kdekoľvek je potrebné vložiť nový kód. Inštrumentačný komponent predstavuje vkladanie týchto spätných volaní na funkcie, ktoré neskôr monitorujú stav systému v mieste vloženého volania, a tým analyzujú bežiaci program. ANaConDA spolu s Pinom umožňuje vkladanie kódu pred a po operáciách zaujmavých pre analyzátory paralelných programov, ako sú synchronizácie a prístupy do pamäte alebo vytváranie a zanikanie vlákien počas exekúcie programu. Napríklad, ak Pin narazí na pamäťové operácie *read* alebo *write*, ANaConDA umožňuje analyzátorom registrovanie spätných volaní napríklad $ACCESS\_beforeMemoryRead$ alebo $ACCESS\_beforeMemoryWrite$. Na tieto volania si už analyzátor naviaže vlastné rutiny, ktoré bude pri spätnom volaní vykonávať.

Kapitola 5

Odhaľovanie data race chýb

Data race chyby (viz. sekcia 2.2.1), sú veľmi nepríjemnou súčasťou vývoja konkurentných programov. Táto kapitola sa bližšie zaoberá vyhľadávaním chýb typu data race pomocou dynamickej analýzy, detekcia chýb pomocou techniky vektorových hodín a ich využitie v analyzátore Djit+ [14], z ktorého vychádza aj analyzátor FastTrack [5] , ktorý je predmetom tejto bakalárskej práce.

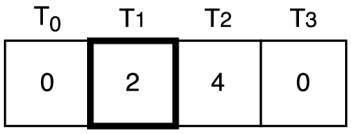
Dynamické data race detektory Vo všeobecnosti spadajú takéto analyzátory do dvoch skupín, tie ktoré ohlasujú len reálne chyby a analyzátory, ktoré spolu s korektnými výstupmi hlásia aj falošné hlásenia. Vznik falošných hlásení často kotví v pomerne veľkej abstrakcii analýzy. Presné race detektory zvyčajne využívajú myšlienku happens-before relácie na monitorovanie priebehu programu, zakódovanú pomocou tzv. vektorových hodín (sekcia 5.1).

Lamportove hodiny Pri detekovaní data-race chýb v konkurentných programoch vzniká problém, ako monitorovať poradie pristupovania vlákien (procesov) ku zdieľanému pamäťovému priestoru a následne určiť či môže nastať situácia, kedy by pristupovalo viac vlákien ku zdieľanej premennej zároveň. Každé vlákno má informácie len o svojich vlastných udalostiach a nemá žiadne poznatky o svojom okolí. Lamportove logické hodiny [9] sa zakladajú na veľmi jednoduchej myšlienke. Všetky vlákna majú svoje vlastné lokálne hodiny vytvárajúce ku každej udalosti (ktorá nastane v danom vlákne) časové razítko. Najbežnejším prevedením takýchto hodím je jednoduché počítadlo, ktoré sa inkrementuje pri každej udalosti daného vlákna, a tak vytvára inkrementujúce sa časové známky unikátne pre postupne prichádajúce udalosti. Predchádzajúca udalosť má časové razítko menšie ako nasledujúca. Táto podmienka platí pre udalosti spracované v totožnom vlákne. V konkurentných programoch existujú aj prípady, pri ktorých dochádza ku medzi vláknovej komunikácii cez synchronizačné objekty. Takéto správy predstavujú čiastočné zosynchronizovanie sa medzi participujúcimi vláknami a pomocou synchronizačnej operácie si spravia obraz o okolitých vláknach v akom stave (aké hodnoty počítadla) sa nachádzajú. Happens-before relácia 3.1.1 využíva práve lamportove logické hodiny pri vyjadrovaní informácií o synchronizácii vlákien.

5.1 Kódovanie H-B relácie pomocou vektorových hodín

Vektorové hodiny sú vektory logických (Lamportových) hodín, teda rozšírenie logických hodín pre paralelné programy. Pomocou H-B relácie, ktorú kódujú, dokážu bezpečne extrapolovať beh programu, a tak vedia overiť exekúcie podobné behu, ktorý sme videli, a nájsť v ňom chyby. Pretože ide o bezpečnú extrapoláciu, potom všetky extrapolované behy by mali byť reálne a tým aj chyby v nich.

Myšlienka za monitorovaním medzivláknovej komunikácie a synchronizácie v podobe vektorových hodín je nasledujúca. Každé vlákno je identifikované vlastným unikátnym identifikačným číslo t a vlastní svoj lokálny vektor hodín T_{vc}. Pozícia vo vektore o hodnote t predstavuje vlastné hodiny (logické lamportove hodiny) daného vlákna t. Čiže t značí identifikačné číslo vlákna a táto hodnota je zároveň pozícia hodín daného vlákna vo vektror-kloku. Ostatné hodnoty v T_{vc} predstavujú logické hodiny okolitých vlákien a značia poslednú udalosť, ktorá sa stala v inom vlákne a platí pre ňu happens-before relácia (sekcia 3.1.1) vzhľadom ku aktuálnej operácii vlákna t.



Obr. 5.1: Vektorové hodiny vlákna T_1

Vektorové hodiny sú čiastočne zoradené $\sqsubseteq$ v jendotnom smere, teda pri porovnaní musia byť rovnako usporiadané. Ku spojeniu dochádza pomocou operácie $\sqcup$, ktorá vyberie maximálne hodnoty z každého elementu vektoru, definujú minimálny element $\bot_V$ a k inkrementácii využívajú funkciu *inc*. Formálny zápis operácií popísaných vyššie kde V značí vektor hodín a t,u značia identifinkačné číslo vlákna:

$$V_1 \sqsubseteq V_2 \Leftrightarrow \forall t.\ V_1(t) \leq V_2(t) \tag{5.1}$$

$$V_1 \sqcup V_2 = \lambda t.\ max(V_1(t), V_2(t)) \tag{5.2}$$

$$\bot_v = \lambda t.\ 0 \tag{5.3}$$

$$inc_t(V) = \lambda u.\ if\ u = t\ then\ V(u) + 1\ else\ V(u) \tag{5.4}$$

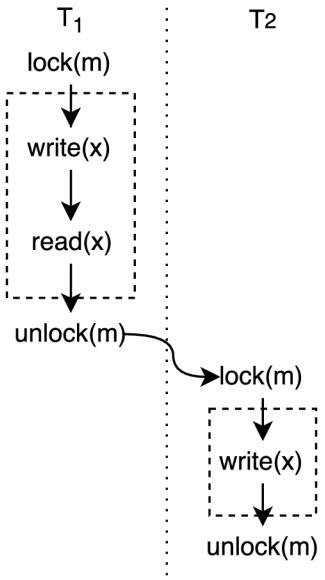
Inicializácia a inkrementácia hodín je riešená na úrovni implementácie, každý algoritmus môže myšlienku vektorových hodín reprezentovať trochu inak. Vo všeobecnosti sú si však operácie podobné. Na začiatku dochádza ku inicializácii, kedy sú hodnoty hodín vo vektoroch nastavené rovnako, a pri každej ne-synchronizačnej operácii dochádza ku inkrementácii logických hodín na indexe t vlákna, ktoré danú operáciu vykonalo. Pri synchronizácii s okolitými vláknami nastáva kontrola happens-before relácie pomocou $\sqsubseteq$ porovnania a následnému spojeniu $\sqcup$ vektorových hodín medzi ktorými prebehla synchronizácia. Vektorové hodiny bývajú implementované v rôznych podobách a dochádza ku rôznym optimalizáciám, no základný princíp rozšírených Lamportových hodín pre paralelné programy v podobe vektorových hodín zostáva rovnaký.

5.2 Djit+

Pred tým, ako si dopodrobna vysvetlíme algoritmus FastTrack (kapitola 6), je podstatné zmieniť princíp analyzátora Djit+ [14], na ktorého základe je postavený FastTrack. Djit+ využíva tzv. vektorové rámce, čo sú rámce založené na vektorových razítkach, ktoré slúžia na detekovanie data race chýb. Algoritmus pracuje s logovacím mechanizmom, ktorý je schopný dynamicky zaznamenávať prístupy k položkám v zdieľanej pamäti. Cieľom algoritmu je sledovanie prístupov do zdieľaných zdrojov a monitorovanie či všetky operácie splňujú happens-before reláciu. Djit+ je renomovaná verzia Djit algoritmu, u ktorého vylepšuje hlavne nedostatok detekcie viacerých chýb (Djit umožňuje detekovať len prvú data race chybu v behu).

5.2.1 Vektorové hodiny v Djit+

Oproti klasickej implementácii vektorových hodín, Djit+ pracuje s upravenou verziou, kde miesto toho, aby pri každej udalosti inkrementoval hodnotu lokálnych hodín, mení ich hodnotu len v určitej situácii. Priebeh exekúcie vlákna si je možné predstaviť ako sekvenciu časových rámcov. Ide o optimalizovanie monotónnej inkrementácie lokálnych hodín, ktorá sa deje len v čase synchronizačnej operácie, kedy dochádza ku zosynchronizovaniu vlákna s okolím. Vektorove rámce využívajúce vektorové razítka sú v princípe to isté ako pojmy vektorové hodiny rozširujúce logické hodiny využívané napríklad u FastTrack-u.



Obr. 5.2: Vektorové rámce, čiarkovane sú vyznačené úseky, počas ktorých nedochádza k inkrementácii lokálneho čítača(razítka), ale až po ukončení bloku (rámca)

5.2.2 implementácia vektorových hodín v Djit+

Definícia operácií a konvencí zápisov

Program pozostáva z viacerých konkurentných vlákien s jedinečným identifikátorom $t \in Tid$, kde Tid je množina všetkých identifikátorov vlákien. Každé vlákno t si drží vektok logických hodín o veľkosti maximálneho počtu vlákien $\mid T \mid$ zapísaný ako C_t. Hodnota $C_t(t)$

predstavuje vlastné lokálne logické hodiny a $C_t(u)$,kde u je iné vlákno, značí logické hodiny vlákna u . $C_t(u)$ teda predstavuje synchronizačný vzťah - ako vlákno t vidí vlákno u v daný okamih. Ďalej vlákna manipulujú so zdieľanými položkami $x \in Var$, kde Var predstavuje množinu všetkých zdieľaných premenných a ďalej využívajú zámky $m \in Lock$, kde $Lock$ je množina všetkých poskytovaných zámkov. Operácie, ktoré vlákno t môže vykonať zahŕňa:

- $rd(t, x)$, $wr(t, x)$ predstavujúce čitanie (read), zápis (write) z premennej x vláknom t
- $acq(t, m)$, $rel(t, m)$ značiace zabratie (acquire), uvolnenie (release) zámku m vláknom t
- $fork(t, u)$ je vytvorenie nového vlákna u vláknom t
- $join(t, u)$ je zpojenie vlákna u do vlákna t

5.2.3 Komunikačný protokol Djit+

K tomu, aby mohli byť implementované pravidlá správania sa vektorových hodín pri synchronizačných operáciách, musí byť priradený vektor hodín ku každému vláknu C_t, ku každému synchronizačnému objektu L_m a každá zdielaná premenná musí naviac ukladať svoju tzv. históriu prístupov. História predstavuje rámec posledného prístupu k danej položke zaznamenaný pre každé vlákno zvlášť ako W_x a R_x operácie zápis a čitanie z premennej x. Potom Djit+ definuje nasledujúce operácie:

Inicializácia
Každé vlákno t si inkrementuje svoju vlastné časové razítko:

$$C_t(t) \leftarrow 1$$
$$\forall i : C_t(i) \leftarrow 0$$

História prístupov ku každej premennej x je vynulovaná:

$$\forall i : R_x(i) \leftarrow 0, W_x(i) \leftarrow 0$$

Synchronizačné zámky m sú taktiež vynulované:

$$\forall i : L_m(i) \leftarrow 0$$

Uvolnenie zámku (*release*)
Pri *release* vlákno t prechádza do nového rámca:

$$C_t(t) \leftarrow C_t(t) + 1$$

Každá položka zámku m je aktualizovaná na maximálnu hodnotu zjednotenia vektoru vlákna t a vektoru hodín m:

$$\forall i : L_m(i) \sqcup max(C_t(i), L_m(i))$$

Získanie zámku (*acquire*)
Pri *acquire* je vlákno t aktualizovaná na maximálnu hodnotu zjednotenia vektoru hodín t a vektoru hodín zámku m:

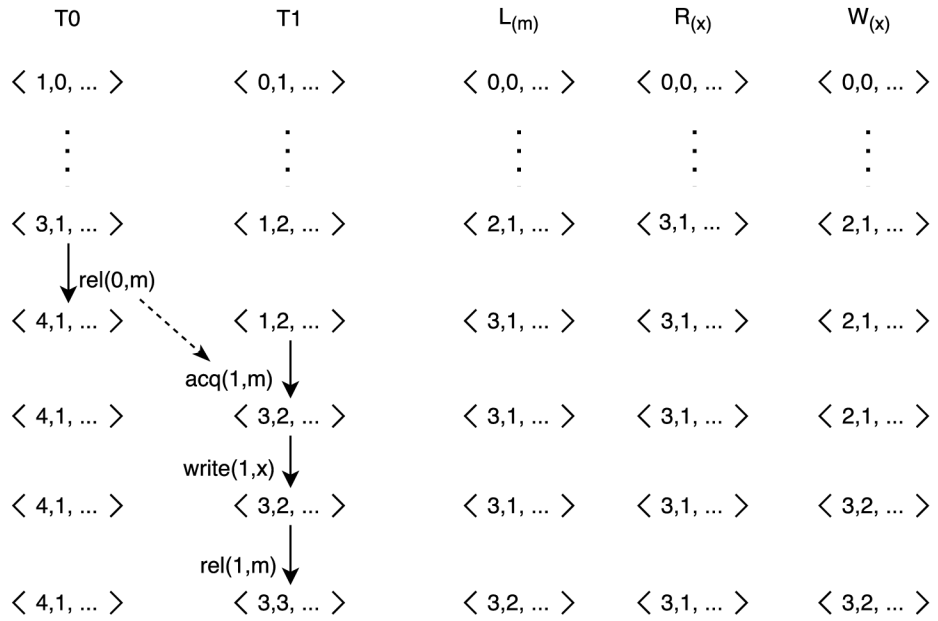
$$\forall i : C_t(i) \sqcup max(C_t(i), L_m(i))$$

R/W operácie
Počas prístupových operácií sa aktualizuje hodnota hodín na pozícii t vlákna t, ktoré pristupuje k položke x:

$$R_x(t) \leftarrow C_t(t) \text{ alebo}$$
$$W_x(t) \leftarrow C_t(t)$$

Pred tým, ako nastane priradenie je nutné vykonať overenie relácie happens-before pre odchytenie potenciálnych chýb typu data race

$$\text{pre read: } W_x(t) \sqsubseteq C_t(t)$$
$$\text{pre write: } W_x(t) \sqsubseteq C_t(t), R_x(t) \sqsubseteq C_t(t)$$



Obr. 5.3: Úsek programu monitorovaný vektorovými hodinami využívanými v Djit+. Na prvom riadku je znázornená inicializácia vektorových hodín. Následne zobrazený úsek priebehu analýzy programu. Medzi inicializáciou a týmto úsokem došlo v poradí, ku zabratiu zamku m vláknom T_0, v tejto kritickej sekcii došlo ku čítaniu aj zápisu z premennej x. Následne zabratie toho istého zámku vláknom T_1 (po jeho uvolnení), kde došlo tak isto k obom pamäťovým operáciám. Nakoniec došlo k opakovanému zabratiu tohto zámku vláknom T_0. Tu však došlo už len ku čítaniu premennej x.

5.2.4 Detekovanie data-race stavov

Na odhaľovanie chýb typu data race sa využíva happens-before relácia (sekcia 3.1.1) zakódovaná do podoby vektorových hodín. H-B relácia platí, ak napríklad operácie a, b vytvárajúce taký vzťah, že a sa udialo pred b a platí minimálne jedna podmienka:

- Operácie sú vykonané rovnakým vláknom
- Obe operácie využívajú totožný zámok
- Jedna z operácií je $fork(t, u)$ alebo $join(t, u)$ a druhá je vykonaná vláknom u

Ak dve operácie nie sú v relácii happens-before, potom sú považované za konkurentné.

Na detekovanie data race stavov, Djit+ uchováva históriu prístupov R_x a W_x pre každú zdieľanú premennú x. Každé vlákno t, ktoré sa pokúša pristupovať k danej premennej $R_x(t)$ a $W_x(t)$ uchováva hodiny posledného zápisu respektíve čítania. Operácia čítania z premennej x vláknom u neobsahuje data race chybu ak platí, že sa udiala po zápise každého vlákna ako posledná operácia, $W_x \sqsubseteq C_t$, kde C_t je vektor hodín pri vykonávaní operácie čítanie. Pri zápise je potrebné určiť či k operácii vláknom u došlo po všetkých predchádzajúcich prístupoch k premennej, $W_x \sqsubseteq C_t, R_x \sqsubseteq C_t$, kde C_t je vektor hodín pri vykonávaní operácie zápis.
Počas operácie porovnania dvoch vektorových rámcov $\sqsubseteq$, dochádza k porovnaniu všetkých položiek oboch vektorov, čo vo výsledku predstavuje výpočtovú záťaž až $O(n)$ pre jedno vlákno. Týmto problémom sa neskôr zaoberá algoritmus FastTrack rozoberaný v nasledujúcej kapitole 6. Každý vektor zaberá pamäť o veľkosti 1 až maximálny počet vlákien $\mid T \mid$. V preklade ide opäť o náročnú pamäťovú záťaž $O(n)$, ktorú sa FastTrack opäť snaží optimalizovať.

Kapitola 6

FastTrack

Pri analyzovaní veľkých programov s množstvom vlákien alebo časovo limitovaných programov je rýchlosť analýzy značne dôležitá. Vysoká pamäťová náročnosť môže v niektorých systémoch znamenať nemalé problémy. Tieto často krát vysoké náklady je možné zredukovať. Detekovanie data race chýb v paralelných programoch je náročné a preto zaznamenanie, čo i len prvého výskytu takejto chyby v reťazci naväzujúcich chýb prináša mnoho prínosu. FastTrack [5] je optimalizovná verzia Djit+ algoritmu (sekcia 5.2) pracujúceho s myšlienkou, kde sa snaží zredukovať náklady na analýzu na minimum a pritom garantovať presné detekovanie apoň jednoho výskytu každej reálnej chyby.

6.1 Problémy využívania vektorových hodín

Extrapolácia

Počas monitorovania programu môžu vznikať hlásenia, ktoré nepredstavujú chyby v programe, ale chyby v abstrakcii využitej techniky na monitorovanie synchronizácie a konkurentných prístupov do zdieľaného priestoru. Ako bolo vysvetlené v sekcii o vektorových hodinách (sekcia 5.1), ide o bezpečnú extrapoláciu, teda extrapolujú sa reálne behy programu. Toto tvrdenie však nemusí vždy platiť. Jedná sa o bezpečnú extrapoláciu vzhľadom ku happens-before relácii (sekcia 3.1.1). To znamená, že ak H-B relácia bude správna, potom aj extrapolované behy budú správne (reálne). Ak by sa v behu programu objavila synchronizácia, ktorú sme nepremietli do H-B relácie, potom extrapolované behy nemusia byť reálne vykonatelné a analyzátor môže detekovať falošné (false) alarmy. Jedná sa teda o prehliadnutie synchronizačných objektov pomocou vektorových hodín (H-B relácie). Ak by boli definované vlastné synchronizačné prvky v programe, potom by ich analyzátor nedokázal detekovať a vytvoril by tak nepresné extrapolácie behu.

Záťaž na systém

Druhý problém spočíva v prevedení, akým vektorové hodiny reprezentujú (ukladajú) dáta, pomocou ktorých je vykonávaná detekcia chýb. Vektorové hodiny predstavujú pole počítadiel o veľkosti maximálneho počtu využitých vlákien v programe. Z toho vyplíva, že vektor môže dynamicky narásť do veľkých rozmerov, čo je často-krát pravidlom pri viac-vláknových programoch. Takto vzniká značná záťaž na pamäť uchovávajúca tieto vektory, formálne sa jedná o pamäťovú náročnosť $O(n)$ pre jedno vlákno, kde n je maximálny počet vzniknutých vlákien za konkrétnej exekúcie.

Súčastne je problémom aj spôsob, akým dochádza k overovaniu H-B relácie. V prípade vektorových hodín operáciou $\sqsubseteq$. Jedná sa takisto o náročnosť $O(n)$ ako pri pamäťových nárokoch, čo predstavuje opeť veľké výpočetné nároky na analýzu.

6.1.1 Epochy

Využívanie vektorových hodín (sekica 5.1) je veľmi výhodné z pohladu presnosti detekcie, no na druhej strane podstatne nákladné. Vo večšine monitorovaných prípadov však nie je nutné uchovávať históriu prístupov pre káždé vlákno, ale stačí využívať len klúčové informácie pre dosiahnutie plného pokrytia chybových stavov a presnosti detekcie. Za predpokladu, že nedošlo ku detekovaniu data race chyby pri prístupe ku zdieľanej premennej x, môžme považovať všetky zápisy do tejto premennej za zoradené podľa H-B relácie. Z tohto pozorovania plynie skutočnosť, že nie je nutné uchovávať históriu prístupov k premennej jednotlivých vlákien, ale len poslednú operáciu zápisu a čítania. Spolu s identifikáciou vlákna t je možné bezpečne určiť či pri pamäťových operáciách nedošlo k data race chybe. S takto redukovanými hodnotami vektorových hodín je možné garantovať len prvý výskyt chyby vzhľadom na spomínanú stratu údajov o predchádzajúcich pamäťových operáciách nad danou premennou ostanými vláknami. Dvojica logikcé hodiny c a identifikačné číslo vlákna t sa nazýva epocha, formálne zapísaná ako $c@t$.
Porovnanie na korektnosť H-B relácie medzi epochou $c@t$ a vektorom hodín V vyjadruje vzťah:

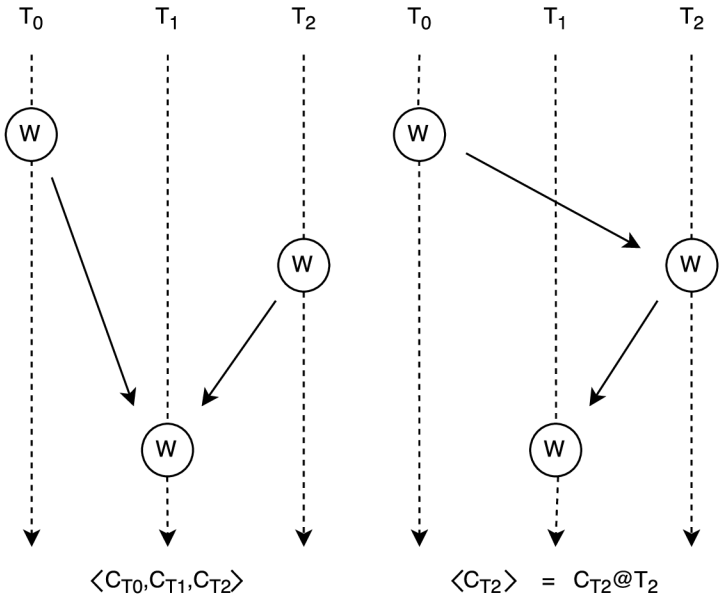
$$c@t \preceq V \Leftrightarrow c \leq V(t) \tag{6.1}$$

Ide teda o operáciu porovnania $\preceq$ s konštantnou zložitosťou $O(1)$, narozdiel od operácie $\sqsubseteq$, u porovnávaní dvoch vektorových hodín, ktorá vykazuje zložitosť $O(n)$. Epocha ako dvojica je nenáročná aj na pamäťový priestor a vykazuje tak len konštantnú pamäťovú náročnosť $O(1)$, naproti vektorovým hodinám, pri ktorých už bolo viac krát spomínaná pamäťová záťaž $O(n)$.

Epochy teda predstavujú optimalizované riešenie vektorových hodín. K ich využívaniu dochádza pri zaznamenávaní histórie posledných prístupov k premennej pre zápis aj čitanie. V určitých situáciách však nie je možné pripustiť stratu informácií o histórii. Tu prichádza na radu dynamické prepínanie medzi epochami a vektorovými hodinami popísané ďalej v tejto kapitole (6.3).

6.2 Detekovanie chýb typu data race

Optimalizácia vychádza z pozorovania, že značná väčšina operácií v konkurentných programoch sú zápis a čítanie zo zdieľanej pamäte, pri ktorých nie je nutné zaznamenávať celú vektorovú reprezentáciu, ale len odľahčenú verziu v podobe epoch. Na druhej strane synchronizačné operácie (fork, join, lock, release atď.), na monitorovanie ktorých treba využívať celé vektorové hodiny, tvoria len malú časť operácií vyskytujúcich sa v programe. Vo výsledku len pri malom počte operácií je potrebné využívať vektorové hodiny. Keďže všetky operácie sú zoradené podľa H-B relácie (pokiaľ nenastala chyba), detekovanie chýb v súbežnosti predstavuje dvojicu operácií, z ktorých je aspoň jedna operácia zápisu.



Obr. 6.1: Vektorové hodiny a epocha. Pri využívaní vektorových hodín sa so všetkými operáciami porovnáva H-B relácia. Naproti epochy predpokladajú, že sú všetky operácie zoradené, a tak porovnávajú len posledný prístup s tým aktuálnym.

6.2.1 zápis-zápis

Detekovanie data race chyby dvoch konkurentných zápisov v sebe naplno uplatňuje optimalizácie, ktoré FastTrack prináša. Ak nedošlo doposiaľ k žiadnej detekcii data-race chyby algoritmus uplatňuje pozorovanie, že v tomto prípade sú všetky zápisy do zdieľanej premennej úplne zoradené podľa H-B relácie. Preto jediné kritické informácie sú obsiahnuté v epochách.

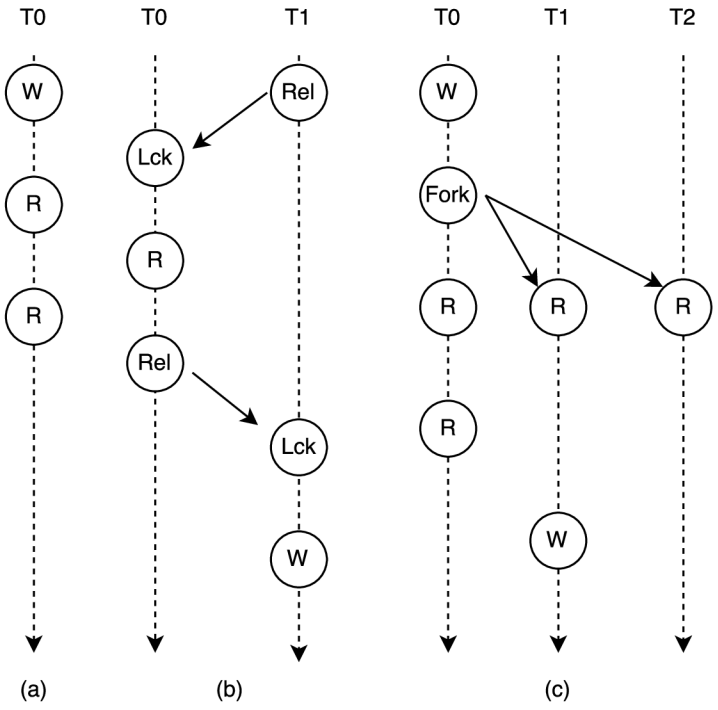
6.2.2 zápis-čítanie

Pri detekcii kombinácie zápis a čitanie sa využíva rovnaký princíp ako pri predchádzajúcom prípade. Algoritmus sleduje či sa posledné čitanie z premennej x udialo po predchádzajúcom zápise pomocou $\preceq$ operácie v konštantnom čase $O(1)$.

6.2.3 čítanie-zápis

Kombinácia čítanie a zápis už predstavuje zložitejší prípad monitorovania ako v predchádzajúcich dvoch prípadoch, kde sme mali garantované zoradenie operácií na základe relácie happens-before v prípade, že nedošlo k žiadnemu výskytu chyby. Operácie čítania nemusia byť podla tohto zvťahu zoradené ani v programoch, ktoré sú tzv. *data race free*, teda neobsahujú žiadne konkurentné chyby. Posledný zápis môže potenciale kolidovať nielen s posledným čítaním, ale aj s ktorým koľvek iným čítaním v ostatných vláknach. Z tohto dôvodu FastTrack prechádza na dočasné monitorovanie pomocou plnohodnotných vektorových hodín, avšak v množstve situácií je možné predísť využívaniu vektorových hodín. FastTrack rieši nasledujúce situácie:

- **Thread-local dáta** - dáta využívané len jedným vláknom, a teda všetky prístupy sú zoradené a vykonávané sekvenčne, preto sa naďalej využívajú epochy pre uloženie histórie.
- **Lock-protected dáta** - pamäťové položky chránené vlasnými výlučným zámkom pre každú položku osobytný. V týchto prípadoch sú operácie čítania zoradené a je možné využívanie epoch na monitorovanie histórie prístupov.
- **Read-shared dáta** - dáta, pri ktorých ide o situáciu, kedy je zdieľaná položka najskôr inicializovaná jedným vláknom a následne nazdieľaná medzi ďalšie vlákna. Tu za použitia epoch môže dôjsť k prehliadnutiu data race chyby, a preto je potrebný prechod na celé vektory.

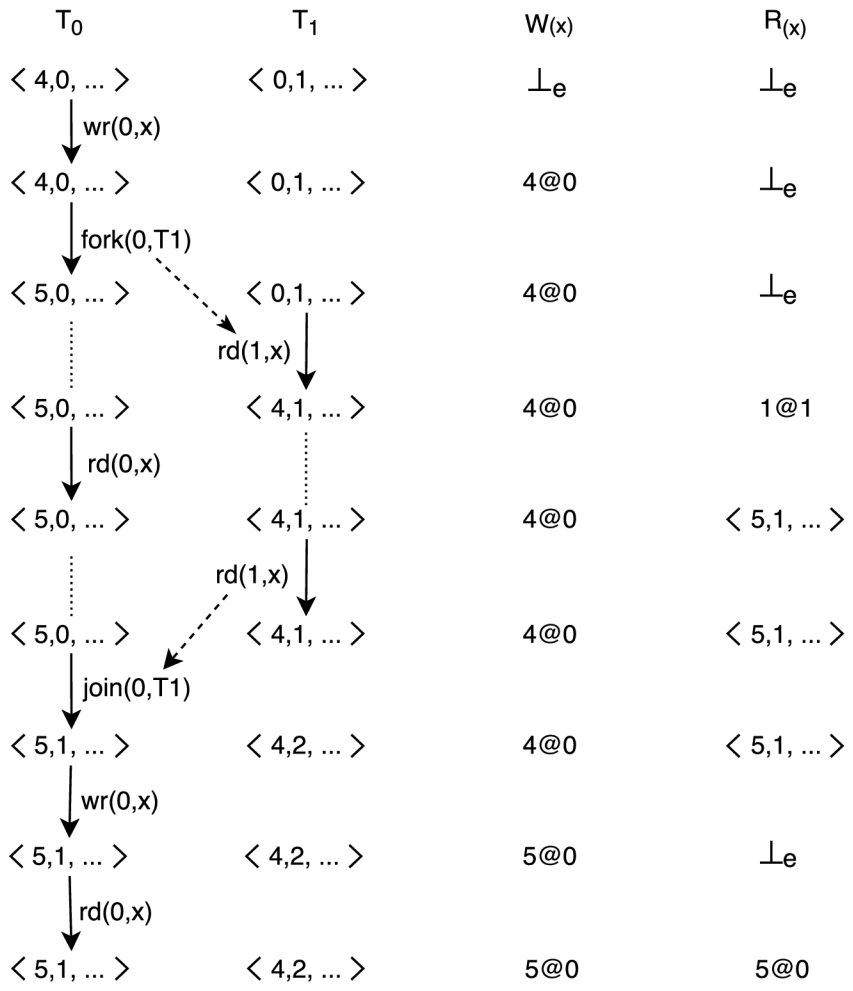


Obr. 6.2: Read-Write scenáre v programe. (a) thread-local dáta, (b) lock-protected dáta, (c) read-shared dáta

6.3 Adaptívne správanie FastTracku

FastTrack využíva adaptívnu reprezentáciu histórie zápisov, čo mu umožňuje jednak značnú redukciu potrebných výpočtových a pamäťových prostriedkov v podobe epoch, a zároveň mu poskytuje v prípade potreby plnú silu obsiahnutú vo vektorových hodinách. Pri situáciách kedy sa k dátam pristupuje len z jednoho vlákna (t*hread-local*), alebo kedy sú pristupované dáta zabezpečené pred súbežným prístupom pomocou synchronizačných objektov (*lock-protected*), FastTrack potrebuje zaznamenať len epochu, keďže ku premmým je zaručený výlučný prístup. Pri raritných prípadoch, kedy sú dáta zdieľané medzi viacero vlákien (*read-shared*), algoritmus musí uchovávať celý vektor hodín. Avšak aj tu detekcia W-R a R-W

data race chýb prebieha v konštantnom čase, pretože sa vektorove hodiny porovnávajú s epochami operácií zápisu v konštantnom čase pomocou $\preceq$ operácie.



Obr. 6.3: Úsek komunikácie dvoch vlákien, vlákno T_1 nazdieľalo vláknu T_2 položku x, pri zaznamenávaní histórie zápisov muselo dôjsť ku prechodu na vektorové hodiny, pretože medzi týmito vláknami môže nastať data race chyba. Všetky tri čítania predstavujú konkurentný prístup ku zdieľanej premennej, no nenastáva data race chyba. Ak by v zdieľanej časti bola vykonaná operácia zápisu, tak by už nastala chyba. Vzhľadom na to, že data race nemusí nastať medzi dvoma psoledným prístupmi, treba prejsť na vektorovú reprezentáciu. Po spojení vlákien algoritmus prechádza späť k využívaniu epoch.

6.4 Algoritmus

Algoritmus počas behu udržuje stav σ, v prípade, ak analyzátor vykoná operáciu a, dôjde k aktualizovaniu stavu analýzy pomocou relácie $\sigma \Rightarrow^a \sigma'$. Inštrumentačný stav σ pozostáva zo štyroch komponent (C, L, R, W) :

- C_t identifikuje súčastný stav vektorových hodín vlákna t.
- L_m identifikuje súčastný stav vektorových hodín posledného uvoľnenia zámku m.
- R_x identifikuje súčastný stav epochy (alebo vektorových hodín) posledného čítania z premennej x.
- W_x identifikuje epochu posledného zápisu do premennej x.

Počiatočným stavom analýzy je:

$$\sigma_0 = (\lambda t.inc_t(\bot_v),\ \lambda m\ .\ \bot_v,\ \lambda x\ .\ \bot_e,\ \lambda x\ .\ \bot_e)$$

V ďalších sekciách sú popísané klúčové detaily ako FastTrack spracúva a monitoruje čítanie (read), zápis (write) a synchronizačné operácie, v ktorych sú využívané konvencie zapísané (v 5.2.2).

6.4.1 Operácia čítanie (read)

Analyzovanie $read(t, x)$ operácie môžu byť realizované v štyroch rôznych situáciách (*same epoch*, *read shared*, *exclusive*, *read share*) a sú zoradené podľa pravdepodobnosti, s akou sa prevažne v programoch vyskytujú [5].

Pravidlo *Same epoch* predstavuje optimalizáciu situácie, kedy sa operácie čítania $rd(t, x)$ odohrávajú v tom istom vlákne, teda nie je potrebná kontrola happens-before, keďže operácie v rovnakom vlákne su vykonávané sekvenčne. Pravidlo predstavuje prevažnú časť všetkých situácií operácie čítania. $E(t)$ obsahuje aktuálnu epochu $c@t$, kde platí $c = C_t(t)$.

[Same epoch]

$$\frac{R_x\ =\ E(t)}{(C, L, R, W)\ \Rightarrow^{rd(t,x)}\ (C, L, R, W)}$$

V prípade *Read shared* (sekica 6.2.3) algoritmus už pracuje s plnohodnotnými vektorovými hodinami v histórii čítaní z premennej. Overovanie H-B relácie so zápisom je však stále uskutočnené pomocou operácie $\preceq$. Ak je história R_x vektor hodín, potom sa pri čítaní len aktualizuje potrebná položka vo vektorových hodinách R_x na pozícii t vlákna, ktoré k nej pristupuje.

[Read shared]

$$\frac{\begin{array}{c} R_x\ \in\ VC \\ W_x \preceq C_t \\ R'\ =\ R[x\ :=\ R_x[t\ :=\ C_t(t)]] \end{array}}{(C, L, R, W)\ \Rightarrow^{rd(t,x)}\ (C, L, R', W)}$$

Pravidlo *exclusive* predstavuje situáciu, kedy vlákno pristupuje ku položke, ku ktorej predchádzajúce operácie pristupovali za využitia medzivláknovej synchronizácie. V tomto prípade sú všetky operácie optimalizované epochami, história R_x je aktualizovaná priradením epochy pristupujúceho vlákna t.

[Exclusive]

$$\frac{R_x \in Epoch \quad R_x \preceq C_t \quad W_x \preceq C_t \quad R' = R[x := E(t)]}{(C, L, R, W) \Rightarrow^{rd(t,x)} (C, L, R', W)}$$

Pravidlo *read share* určuje situáciu, kedy dochádza ku nazdieľaniu premennej, a tým musí dôjsť k prechodu zo systému využívajúceho epochy v histórii čítaní, na vektor hodín. Táto situácia nastáva v malom počte prípadov, no je spomedzi všetkých najdrahšie, keďže dochádza ku vytváraniu nového vektoru hodín.

[Read share]

$$\frac{R_x = c@u \quad W_x \preceq C_t \quad V = \bot_v\,[t := C_t(t), u := c] \quad R' = R[x := V]}{(C, L, R, W) \Rightarrow^{rd(t,x)} (C, L, R', W)}$$

6.4.2 operácia zápis (write)

Ďalšie tri situácie (*same epoch*, *write shared*, *exclusive*) predstavujú možné scenáre monitorovanie zápisov $wr(t, x)$.

Pravidlo *Same epoch* opäť optimalizuje situáciu, kedy už nastal zápis $wr(t, x)$ do rovnakej premennej x, v rovnakom vlákne t.

[Same epoch]

$$\frac{W_x = E(t)}{(C, L, R, W) \Rightarrow^{wr(t,x)} (C, L, R, W)}$$

Pravidlo *Exclusive* kotroluje, že všetky predchádzajúce operácie pristupujúce ku danej premennej x sa odohrali skôr ako aktuálny zápis $wr(t, x)$. V tomto prípade je história čítaní R_x v stave epochy.

[Exclusive]

$$\frac{\begin{array}{c} R_x \in Epoch \\ R_x \preceq C_t \\ W_x \preceq C_t \\ W' = W[x := E(t)] \end{array}}{(C, L, R, W) \Rightarrow^{wr(t,x)} (C, L, R, W')}$$

Ak história R_x je reprezentovaná vektorovými hodinami, nastáva situácia *write shared*, čo je zápis do takto definovanej pamäte a je potrebné využiť proovnanie medzi dvoma vektormi $\sqsubseteq$. K tejto situácii však dochádza v malom počte operácií.

[Write Shared]

$$\frac{\begin{array}{c} R_x \in VC \\ R_x \sqsubseteq C_t \\ W_x \preceq C_t \\ W' = W[x := E(t)] \\ R' = R[x :=\bot_e] \end{array}}{(C, L, R, W) \Rightarrow^{wr(t,x)} (C, L, R', W')}$$

6.4.3 Synchronizačné operácie

Ostatné operácie $acquire(), release(), fork(), join()$ sú v porovnaní s $read()$ a $write()$ veľmi ojedinelé. Využitie úplnych vektorových hodín je v týchto prípadoch potrebné, no v kombinácii s raritou akou sa vyskytujú pri monitorovaní, sa nejedná o veľkú záťaž na rýchlosť analýzy.

[**Acquire**]

$$\frac{C' \;=\; C[t := (C_t \sqcup L_m)]}{(C, L, R, W) \;\Rightarrow^{acq(t,m)}\; (C', L, R, W)}$$

[**Release**]

$$\frac{\begin{array}{c} L' \;=\; L[m := C_t] \\ C' \;=\; C[t := inc_t(C_t)] \end{array}}{(C, L, R, W) \;\Rightarrow^{rel(t,m)}\; (C', L', R, W)}$$

[**Fork**]

$$\frac{C' \;=\; C[u := C_u \sqcup C_t, t := inc_t(C_t)]}{(C, L, R, W) \;\Rightarrow^{fork(t,u)}\; (C', L, R, W)}$$

[**Join**]

$$\frac{C' \;=\; C[t := C_t \sqcup C_u, u \;:= inc_u(C_u)]}{(C, L, R, W) \;\Rightarrow^{join(t,u)}\; (C', L, R, W)}$$

Kapitola 7

Implementácia

Táto kapitola sa zaoberá časťami implementácie, ktoré sú z môjho pohľadu zaujímavé a venuje sa odlišnostiam v implementácii od teórie.

7.1 Detaily implementácie

Implementácia FastTrack-u priraďuje ku každému vláknu jeden objekt `ThreadState`. Ten predstavuje lokálne dáta jednoho vlákna - lokálny vektor hodín (5.1) `currentClock`, identifikátor vlákna `ts_tid` a referenciu na zoznam `ThreadStateList` ostatných `ThreadState` objektov, reprezentujúcich lokálne dáta ostatných vlákien. Tento odkaz na lokálne dáta ostatných vlákien narušuje podstatu súkromných informácií jednotlivých vlákien. Prehrešok lokality je vysvetlený a zdôvodnený v sekcii 7.3.1. Objekt `LockState` je priradený ku každému zámku, ktorý je využívaný v analyzovanom programe a následne je uložený v zdieľanej mape `CurrentLockMap`. Táto mapa je spoločná naprieč všetkými vláknami a zjednocuje všetky zámky (resp. `LockState` objekty). `LockState` obsahuje jediný vektor hodín `lockClock`, zaznamenávajúci históriu prístupov ku zámku. Jednotlivé premnné, na ktorých prebieha monitorovanie, a následne prípadná detekcia data race chýb, sú reprezentované `VarState` objektami. Ku každej premennej je priradený jeden `VarState` objekt, ktorý je tak isto ako pri zámkoch, uložený v zdieľanej mape `CurrentAccessMap`. Obsahom všetkých `VarState` objektov sú dve položky (dvoje vektorové hodiny), jedna `W` pre zápis do premennej a druhá `R` pre čítanie z premennej. Obe sú v počiatku inicializované ako epochy a ich prechod na vektory popisuje sekcia o implementácii epoch (7.2.1).

7.2 Kódovanie H-B relácie

Kódovanie happens-before relácie 3.1.1 do podoby vektorových hodín v teórii znie jednoducho. V praxi však pri implementácii treba riešiť viacero otázok. Jedným z problémov je počet vlákien. V teórii je možné jednoducho počítať s pevne daným počtom vlákien, no v praxi ide o dynamický počet, ktoré môžu rôzne vznikať a zanikať, a tým aj o dynamyckú veľkosť vektorových hodín. Z tohto poznatku vyplíva, že nie je možné dopredu určiť počet vlákien a je nutné využiť dynamicky sa alokujúcu štruktúru. V tejto implementácii je využívaný vektor zo štandardnej c++ knižnice, ktorý si automaticky alokuje potrebnú pamäť pri nadobudnutí maximálnej veľkosti. Ďalší problém nastáva v oblasti operácií nad vektorovými hodinami, konkrétne pri ich porovnávaní a spájaní. Často nastávajú situácie, kedy jeden vektor je kratší alebo dlhší ako druhý. V takýchto prípadoch je nutné tento

poznatok brať v potaz a zabezpečiť operáciu pred týmito situáciami. Do tretice bolo treba vyriešiť, ako bude dochádzať ku prechodu z epochy na vektor hodín a naspäť. Nakoľko dochádza ku prechodu z jedno-prvkového vektoru na viac-prvkový a opačne, treba zabezpečiť, aby informácie potrebné pre analýzu neboli pri vytváraní celého vektoru zahodené, ale prenesené do nového vektoru, respektíve pri opačnej operácii, aby došlo k vynulovaniu prvkov a reštartu na jednoprvkový vektor. Všetky tieto otázky/problémy a ich riešenia sú popísané v tejto sekcii.

7.2.1 Implementácia epoch

Myšlienka epoch (6.1.1), predstavuje základný pilier algoritmu FastTrack. Pri implementácii bolo potrebné rozšíriť resp. zjednodušiť vektorové hodiny implementované ako trieda `VectorClock` tak, aby ich bolo možné použiť aj v podobe epoch. Cieľom bolo zjednotiť obe formy do jednotnej triedy tak, aby si epochy zachovali svoju nízku pamäťovú náročnosť a udržali si rýchlosť pri porovnávaní vektorových hodín pomocou operácie $\preceq$. Zároveň však zjednotenie oboch prevedení do jedného malo predstavovať rýchlu a jednoduchú možnosť, ako zaručiť adaptívne správanie vektorových hodín vo FastTrack-u (kapitola 6).

Vektorove hodiny sú implementované ako kontajner `vc`, reprezentujúci vektor nezáporných celočíselných hodnôt. Ku každému vektoru je definovaná aj signalizačná premenná (flag) `epochID` nesúca dva druhy informácií. Záporná hodnota indikuje, že objekt je aktuálne v stave plnohodnotného vektoru hodín. Ak je `epochID` nezáporné, jedná sa o epochu definovanú ako $c@t$. Potom `epochID` značí identifikačné číslo vlákna t a jeho hodnota c je uložená ako prvá požka vektoru (položka na indexe 0), aby nedochádzalo ku plytvaniu pamäťovým priestorom. Preklopenie medzi epochou a vektorom je realizované pomocou metódy `switchToVC`, ktorá realizuje tento prevod inicializovaním všetkých potrebných položiek vektoru na hodnotu 0 pomocou metódy `initL`. Prednostne je však potrebné si uchovať aktuálnu hodnotu epochy, ktorá nesie aktuálny stav prístupu na premennej, a je potrebné ju brať v potaz resp. zobraziť do vektoru hodín pre nasledujúce monitorovanie premennej. Následne je teda vložená na požadované miesto (`epochID`) v novovzniknutom vektore. Nakoniec dochádza ku prepnutiu signalizačnej premennej `epochID` na hodnotu -1. Podľa tejto hodnoty sa riadi aj v každej funkcii mechanizmus výberu, teda aká funkcionalita nastane podľa toho či ide o vektorové hodiny (`epochID` je rovné -1) alebo epochu (`epochID` je väčšie alebo rovné 0).

7.2.2 Veľkosť vektorových hodín a operácie nad nimi

Problém spomínaný už v úvode kapitoly, kedy algoritmus musí pracovať s premenlivým počtom vlákien, a teda veľkosť vektorových hodín sa musí meniť spolu s počtom vlákien v monitorovanom programe je v implementácii riešený nasledovne. Ide o implementovanie pomocou dynamického vektoru, ktorý automaticky zväčšuje svoju veľkosť na základe požadovaného miesta resp. počtu vlákien, ktoré treba zaznamenávať. Pomocou operácie `assign` je pri inicializácii vektoru hodín vytvorené potrebné miesto pre všetky jeho položky a inicializované na 0. Počet položiek pri inicializácii je hodnota $tid + 1$ (identifikátory vlákien začínajú od nuly), teda pre vlákno s $tid = 0$, má vektor veľkosť 1. V operácii `join` je ďalej podľa potreby vektor zväčšovaný, ak dochádza ku spájaniu rôzne veľkých vektorov. Táto situácia nastáva pochopiteľne v prípadoch vytvárania vlákien (`fork`). Rodičovské vlákno (parent) si ponechá aktuálnu veľkosť, no potomok (child) má veľkosť o jedna väčšiu. Zjednotenie dvoch rôzne veľkých vektorov nastáva napríklad pri prvom zabraní synchronizačného objektu jednotlivými vláknami (viz. 6.4).

Porovnávanie

Hlavnými operáciami nad vektorovými hodinami sú už zmieňované spájanie dvoch vektorov `join` a porovnanie, či nedošlo k porušeniu happens-before reláacie, `hb`. Vždy sa jedná o dvojicu vektorov, nad ktorými je prevedená daná operácia. Pri vykonávaní operácie porovnania, teda pri kontrole či nenastala medzi prístupmi k premmnej data race chyba (sekcia 2.2.1), volajúci objekt reprezentuje aktuálne pristupujúce vlákno (v relácii happens-before operáciu, ktorá sa udiala ako posledná) a parameter `history` tejto metódy reprezentuje históriu prístupov (nastáva porovnanie vlákna voči hostórii). Kôli premenlivosti počtu vlákien dochádza aj k porovnávaniu rôzne dlhých vektorových hodín operáciou $\sqsubseteq$. Dynamicky sa meniaci počet vlákien nemá vplyv na využívanie epoch, no pri vektorových hodinách je to problém, preto nie je možné využívať statickej štruktúry. Pri porovnávaní je potrebné najskôr zistiť, či je *tid* vlákna menšie ako veľkosť vektoru histórie. Ak by *tid* bolo väčšie (prípadne rovné), indikovalo by to, že nedošlo k predchádzajúcemu zosynchronizovaniu, a dochádza tak ku data race chybe. Vďaka tomuto porovnaniu, nemusia byť porovnané celé vektory, ale len dve hodnoty. Inak dochádza ku porovnaniu oboch vektorov. V prípade epochy sa porovnávajú len dve hodnoty.

Spájanie

Pri spájaní dvoch vektorových hodín operáciou join $\sqcup$ (zjednotenie maximálnych hodnôt oboch vektorov) implementovanou v rovnomennej metóde `join`, môže dôjsť tak isto ku situácii, kedy sa spájajú dva vektory s rozdielnými dĺžkami. Prvotne je nutné určiť, ktorý z dvojice vektorových hodín je väčší, a ktorý je menší. Následne prebieha spájanie preiterovaním spoločnej časti a vyberaním maxima z jednoho alebo druhého vektoru. Objekt volajúci metódu spájania reprezentuje výsledný vektor. V prípade, ak je výsledný vektor menší ako druhý z dvojice, dochádza ku priradeniu zvyšných položiek na koniec výsledného vektoru pomocou funkcie `push_back`.

7.3 Úložisko dát

Informácie využívané pri monitorovaní bežiaceho programu sú rozdelené podľa lokality na lokálne, špecifické len pre danú entitu, ktorej patrí, v našom prípade pre jedno vlákno, a globálne úložisko, ktoré je otvorené prístupom zo všetkých vlákien. Tieto dáta sú spoločné pre všetky vlákna a môžu k ním pristupovať, z čoho vyplýva potreba zabezpečiť prístupy ku zdieľaným štruktúram aj vo vnútri analyzátora.

7.3.1 Lokálny priestor vlákien

Lokálny priestor pre jednotlivé vlákna (thread local storage – TLS) zapúzdruje informácie špecifické pre jednotlivé vlákna samostatne. Spolu s hodnotou vektorových hodín si udržiava aj identifikačné číslo *tid* a referenciu na zoznam ostatných súkromných priestorov ostatných vlákien. Týmto však porušuje súkromie informácií špecifických pre jednotlivé vlákna, čím čiastočne neguje lokálnosť dát. Takáto niance je však potrebná pri spracovávaní synchronizačných operácií algoritmom. Operícia `join` pracuje s lokálnymi vektorovými hodinami nie len vlastného vlákna, ale aj okolitých. Implementácia rieši tento problém nasledovne. Lokálny priestor každého vlákna `ThreadLocal` disponuje už vyššie spomínanými položkami, vektorom hodín vlákna `currentVector` a identifikačným číslom `ts_rid` reprezentujúcimi

informáciami o vlákne, a zoznamom všetkých TLS `m_threadStates`. Z tohto plynie, že k lokálnym údajom je možné pristupovať aj z ostatných vlákien. Týmto spôsobom porušujeme princíp lokálneho úložiska. Pri operácii spojenia vlákien *join* je nutné mať informácie o druhom, pripojovanom vlákne, keďže tu dochádza ku synchronizácii dvoch vlákien bez nejakého sprostredkovateľa ako napríklad zámku.

7.3.2 Globálne úložisko

Algoritmus analyzátoru FastTrack pre svoju činnosť vyžaduje spolu s lokálnym úložiskom jednotlivých vlákien aj globálne zdieľané dáta naprieč všetkými vláknami. Bez zdieľania informácii medzi jednotlivými vláknami by analyzátor nemal zmysel, keďže by nedokázal zistiť vzťah medzi prístupmi ku premennej od rozlišných vlákien. `LockState`, ako objekt reprezentujúci zámok, je jedným zo zdieľaných entít a obsauje jedinú položku v podobe vektorových hodín `lockClock`, ktorý ukladá históriu využívania daného zámku jednotlivými vláknami. Tieto objekty reprezentujúce zámky sú ukladané do mapy `CurrentLockMap`. Jednotlivé zámky sú od seba odlišované identifikátorom `lock`.

Druhou zdieľanou entitou globálneho priestoru je `VarState`. Reprezentuje objekt asociovaný ku každej premennej monitorovaného programu a umožňuje tak sledovať vzťahy respektíve postupnosti operácií čitania a zápisu nad nimi vykonavané jednotlivými vláknami. Obsahuje dva vektory hodín, jeden pre čitanie `R` a druhý pre zápis `W`. Oba sú inicializované ako epochy, vektor hodín `W` je počas celej analýzy v podobe epochy. Ku prechodu na plnohodnotné vektorové hodiny dochádza iba v ojedinelých prípadoch na `R`. `VarState` objekty sú ukladané v zdieľanej mape `CurrentAccessMap` a jednotlivé premenné su rozlišované na základe adries `ADDRINT`.

Zamykanie globálneho priestoru

Keďže sa jedná o zdieľané entity, môžu nastať konkurentné chyby aj v štruktúrach analyzátora, a preto je potrebné zabrániť takýmto chybám pomocou výlučného prístupu. Globálne zdieľané zamky sú chránené pomocou `g_currentLockMapMutex` a premenné sú chranené pomocou `g_currentAccessMapMutex`. Oba tieto zámky sú takzvané read/write zámky a umožňujú úplne výlučný prístup v podobe `PIN_RWMutexWriteLock` alebo je prístup povolený viacerým vláknam ale len na čítanie `PIN_RWMutexReadLock`. V tejto implementácii sú využívané pri prístupe ku `CurrentAccessMap` ako aj ku `CurrentLockMap` výlučné prístupy, a to z dôvodu maximálnej bezpečnosti a jednoduchosti. V niektorých prípadoch by bolo možné prejsť aj na viac-vláknové čítanie, no v algoritme dochádza ku častým prepínaním medzi čítaním a zápisom, a dochádzalo by tak ku častým zamykaním/odomykaním, čo by mohlo spôsobiť spomalenie. Z tohto dôvodu som zvolil jednoduchší prístup, aj keď môže dochádzať ku poklesu výkonu analyzátora.

7.4 Proces odhaľovania data race chyby

Odhaľovanie data race chýb je primárnym cieľom analyzátoru. Implementácia sa drží konceptu popísaného v [5]. Na začiatku každej monitorovanej operácie či už sa jedná o zápis, čitanie alebo synchronizáciu je potrebné zistiť, či sa daný monitorovaný objekt (premenná alebo zámok) nachádzajú v zdieľaných mapách, a ak nie, tak ich tam treba vložiť. Potom analýza prechádza niektorou z možných etáp. Pri operácii čitania (read) môže dôjsť ku trom situáciám. Po prvé je využívaný poznatok, že prevažná časť operácií za sebou sa vykonáva

v rovnakom vlákne a tak dochádza ku rýchlemu porovnaniu na túto skutočnosť medzi *tid* pristupujúceho vlákna a *epochID* resp. *tid* posledného prístupu k premennej. Ak táto podmienka nie je platná, potom nastáva overenie happens-before relácie, či nedošlo k jej porušeniu (W-R data race). Toto overovanie je až na druhom mieste, keďže v jednom vlákne sú operácie vykonávané sériovo. Ďalej môže nastať situácia, kedy prístup je chránený zámkom. V takomto prípade nemôže dôjsť ku chybe. Posledným prípadom je read-shared stav (sekcia 6.2). Do tohto stavu sa môže algoritmus dostať, ak nebola splnená happens-before relácia, čo pri zdieľanom čítaní neimplikuje chybu. Pri operácii zápisu (write) je situácia v úvode rovnaká. Ďalej však dochádza ku intenzívnemu overovaniu data race chýb (R-W a W-W), keďže podmienkou pre vznik takýchto chýb je minimálne jedna operácia zápisu. Ak je aktuálny prístup čistý, pristupuje sa ku zjednoteniu vektorových hodín (epoch) histórie premennej a vlákna. Algoritmus primárne generuje a modifikuje monitorovacie dáta (vektorové hodiny atď.) po zamknutí a pred odomknutím zámkov. Činnosť všetkých operácií je popísaná v kapitole o algoritme 6.4.

Kapitola 8

Dosiahnuté výsledky

V tejto kapitole sú popísané experimenty prevedené na rôznych typoch programov obsahujúcich data race chyby (sekcia 2.2.1) za účelom otestovania frekvencie odhaľovania chýb a porovnania týchto výsledkov s ďalším dynamickým analyzátorom. Experimenty boli vykonávané pomocou analyzátora FastTrack (kapitola 6) implementovaného v prostredí ANaConDA (kapitola 4) na programoch využívajúcich knižnicu pthreads, podporovanú práve prostredím ANaConDA na operačnom systéme Ubuntu (ver. 14.04.5). V úvode sú uvedené experimenty na dvoch jednoduchých programoch ilustrujúcich základný princíp data race chyby. Následne sú predložené experimenty nad pokročilejšími programmi, u ktorých sa data race chyby vyskytujú na rôznych miestach. Ide napríklad o chyby v nesprávnom zamykaní, kedy sa pracuje so zdieľanou premennou nie len v kritickej sekcii, ale operuje sa s ňou aj mimo zabezpečenú sekciu, alebo sa jedná o nesprávne inicializovanie zámkov priamo vo vláknach. Nakoniec sú výsledky porovnané s dynamickým analyzátorom AtomRace, ktorý je taktiež implementovaný v prostredí ANaConDA. FastTrack vykazuje značný nárast v počte varovaní úspešných detekcií chýb oproti analyzátoru AtomRace.

Tabuľka 8.1: Tabuľka zobrazujúca úspešnosť odhalenia data race chyby v programoch čítač a banka, zobrazuje v koľkých prípadoch bola detekovaná chyba z celkového počtu testovacích behov.

	AtomRace	FastTrack
čítač	4/30	30/30
banka	0/30	30/30

8.1 Jednoduché experimenty

Prvotné experimenty boli vykonané na dvoch triviálnych programoch `čítač` a `banka`. Oba tieto programy obsahujú jednoduchý príklad data race chyby. V prípade čítača nedochádza ku žiadnemu zosynchronizovaniu medzi dvoma vláknami, ktoré jednoducho inkrementujú spoločnú premennú, a tak vzniká data race chyba. V prípade programu banka sa pri prístupe ku zdieľanej premennej kombinuje prístup s alebo prístup bez synchronizácie, a tak vzniká

na tejto premennej data race. Tieto príklady predstavujú len ilustráciu ako data race chyby môžu v programe vznikať a ich odhaľovanie pomocou ostatných analyzátorov.

8.2 Experimenty s algoritmom s prístupovými lístkami

Nasledujúce, už zložitejšie programy boli vytvorené študentmi ako projekty do predmetu pokročilé operačné systémy. Všetky popisujú rovnaký algoritmus na tikety resp. prístup do kritickej sekcie. Cieľom je synchronizovať všetky vlákna programu pri vykonávaní nejakej vzájomne výlučnej činnosti v programe abstrahovanej ako funkcia `doWork()`. Ak sa vlákno pokúša vykonať túto prácu, je mu najskôr priradený lístok (tiket) s najnižším volným číslom funkciou `getticket()` a následne čaká na to, kým sa dostane na radu (lístok s najnižším číslom má prednosť). Premenná `next_ticket` si uchováva práve túto hodnotu s najnižším volným lístok a prístup ku nej je chránený zámkom. Prístup do miesta, kde je vykonávaná hlavná práca, je chránený monitorom. Vstupom je funkcia `await()` a výstupom z monitora funkcia `advance()`. Obe funkcie pracujú s premennou `curr_ticket`, ktorá určuje číslo tiketu pre vstup do monitoru. Funkica `await()` prečíta lístok vstupujúceho vlákna, a ak nie je na rade (číslo jeho lístku neodpovedá premennej `curr_ticket`), musí vlákno čakať. Fukcia `advance()` následne inkrementuje túto hodnotu dovolujúc ďalšiemu vláknu vstúpiť. Prístup k aktuálnemu tiketu je tiež chránený zámkom (odlišným od toho pri vytváraní lístkov).

Algoritmus 1 Ticket algoritmus

```
1: for each thread do
2:     while (ticket = getticket()) < M do
3:         sleep(random);
4:         await(ticket);
5:         doWork();
6:         advance();
7:         sleep(random);
8:     end while
9: end for
```

Data race chyby v experimentoch

Pri odhaľovaní data race chýb (sekcia 2.2.1), kedy dochádza ku dvom prístupom ku zdieľanej premmenj bez synchronizácie a minimálne jeden z prístupov je zápis, FastTrack využíva happens-before reláciu (sekcia 3.1.1) zakódovanú v podobe vektorových hodín (sekcia 5.1). Ak sa pri porovnávaní vektorových hodín vlákna aktuálne pristupujúceho k premennej a epochy (prípadne vektoru hodín) histórie prístupov k tejto premennej zistí, že neplatí porovnávacie pravidlo (sekcia 6.1), dochádza k detekovaniu data race chyby na danej premennej. Zvyčajne sa dva konkurentné prístupy do pamäte vyskytujú len vo veľmi malom počte behov, no vďaka extrapolácii FastTrack preveruje okrem aktuálneho aj množstvo ďalších behov, a tým značne zvyšuje šancu na odhalenie chyby. V uvažovaných programoch reprezentujúcich ticket algoritmus sa vyskytujú variácie rôznych data race chýb, ktoré sú popísané nižšie.

Bližší popis vyskytujúcich sa chýb

V testovanom programe `t01` sa vyskytuje data race chyba v lístkovacej funkcii `getticket()` pri vrátení nasledujúceho tiketu. S premennou sa pracuje vo vnútri kritickej sekcie, no čítané je z nej mimo túto sekciu. Ku chybe dochádza pomerne často keďže funkcia na vydávanie lístkov je často volaná. V ďalšom prípade `t02` sa jedná o modifikovanie úplne nechránenej premennej v hlavnej funkcii vlákna. V programe `t03` sa vyskytuje podobná chyba ako v prvom prípade. Tu je však vo funkcii `getticket()` využívaná statická pomocná premenná, ktorá však ako statická predstavuje zdieľanú premennú pre všetky vlákna a nie lokálnu, pre každé vlákno zvlášť. V ďalšom testovanom subjekte `t04` sa nachádza data race na štruktúre uchovávajúcej identifikátory vlákien a ich tikety. Pri vytváraní vlákien aj v hlavnej funkcii vlákien je využívaná rovnaká štruktúra (data race chyby sa prejavujú pri vytváraní vlákien). `t05` je prvý z dvojice prípadov, kedy dochádza ku detekcii chyby len v malom počte exekúcií. Jedná sa o veľmi ojedinelú chybu prejavujúcu sa na jednotlivých položkách pola (ktoré obsahuje identifikátory každého vlákna) v momente, kedy hlavné vlákno začne čakať na dokončenie činnosti jednotlivých vlákien. Vo vláknach je toto pole zabezpečené pred konkurentným prístupom, no hlavné vlákno k nemu pristupuje bez synchronizácie na konci programu, kedy v ojedinelých prípadoch dochádza ku simultánnemu prístupu. V nasledujúcich programoch `t06` a `t07` vzniká konkurentný prístup v hlavnej funkcii vlákna, na štruktúre uchovávajúcej veľkosť časovača, ako dlho má vlákna spať po a pred prechodom monitoru resp. pred vstupo `await()` a po odchode `advance()`. Táto pasáž sa vykonáva často, závisí však na počte prechodov (vykonaní práce `doWork()`) zadanom pri spúšťaní programu. V prípade programu `t07` je výpočet doby čakania uskutočňovaný v pomocnej funkcii, kde sa data race chyba prejavuje. Program `t08` obsahuje chybu na premennej, ktorá umožňuje vláknu prechod cez funkciu `await()`, v ktorom sa vlákno aktívne dotazuje na možnosť pokračovať v práci. Ide teda o hodnotu `curr_ticket`. V programe `t09` sa opäť nachádza chyba na štruktúre obsahujúcej náhodné čakanie vykonané pred vstupom do kritickej sekcie a po jeho výstupe, rovnako ako pri `t06` a `t07`. `t10` je druhým prípadom, kedy dochádza len k ojedinelému nálezu data race chyby obsiahnutej v tomto programe. Chyba sa vyskytuje na statickej premennej inicializovanej vo funkcii vydávajúcej lístky, kde sa následne v kritickej sekcii s touto premennou pracuje. Problémom nízkej úspešnosti detekovania chýb môže byť aj fakt, že mimo kritickej sekcie sa do premennej zapisuje len pri inicializácii. Nasledujúci program `t11` opäť zle zabezpečuje `curr_ticket` pri prístupe. Modifikácia prebieha v kritickej sekcii, no čítanie mimo nej. V programe `t12` nastáva zlé inicializovanie zámkov alebo lepšie povedané ich inicializácia nastáva v každom vlákne, čím reštartujú vlastníka zámku a ostatné jeho údaje. V poslednom prípade `t13` nastávajú data race chyby na zdieľanej premennej uchovávajúcej návratové hodnoty funkcií z knižnice pthread. Táto premenná je často aktualizovaná a tak sa chyby prejavujú relatívne často.

Chyby v nesprávnom využívaní zámkov

V testovacích programoch sa vyskytli aj prípady, kedy dochádzalo ku zlému využívaniu pthread knižnice, ako napríklad uvolnenie zámku viac krát po sebe. `t02` a `t12` inicializujú pthread zámok priamo v každom vytvorenom vlákne. Tým pádom reštartujú informácie daného zámku (informácie o vlastníkovi, stav zámku) vždy s novým štartom vlákna. Toto správanie umožňuje viacerým vláknam zabrať jeden zámok. Prvé vlákno zabere zámok, ktorý následne druhé, novovzniknuté vlákno reštartuje (jeho vlastníka). Takto môže dochádzať ku data race chybám, kedy viac ako jedno vlákno pristupuje do kritickej sekcie, ktorá by mala zabezpečovať výlučný prístup za bežných okolností. V týchto dvoch programoch

nastáva data race na začiatku, pri štarte vlákien. V programe `t14` sa zas jedná o problém kedy dochádza ku odomknutiu zámku dva krát za sebou (miesto zamknutia a uvolnenia) a tak sa do kritickej sekcie môže dostať ďalšie vlákno resp. zámok vlastní viac vlákien. FastTrack vďaka detekovaniu zamykacej logiky umožňuje detekovať takéto zlé zamykanie a ohlásiť možnú data race chybu v kritickej sekcii. Ak nastane podozrivé zamykanie (resp. ANaConDA zachytí takéto správanie) fasttrack detekuje na vektorových hodinách neaktualizované hodnoty a nahlási tak chybu v prístupoch ku premennej.

8.3 Vyhodnotenie experimentov

Programy, na ktorých boli prevádzané experimenty, dovoľujú zadať ako argumenty počet vlákien vytvorených a vykonávajúcich danú prácu a počet priechodov cez vytvorenú kritickú sekciu. Odskúšaných bolo viacero kombinácií týchto parametrov, no rozumným kompromisom pre overenie programu pri dostatočnom počte vlákien a prechodov bola kombinácia 9 vlákien a 100 prechodov.

Výsledky zhrnuté v tabuľke (8.2) ukazujú, že v 11 z 13 prípadov, FastTrack detekoval data race chyby s takmer ideálnou presnosťou. V prípade dvoch programov `t05` a `t10`, bola úspešnosť detekovania chyby značne nízka. Problémom detekcie v oboch programoch bol malý počet situácií, kedy by došlo ku data race chybe, a to v prípade `t05` dochádzalo len medzi hlavným vláknom a ostatnými vláknami, pri príchode hlavného ku koncu programu a v prípade `t10` to bolo pri inicializáii statickej premennej na začiatku funkcie vydávajúcej lístky. V prípade programov `t02`, `t12` a `t14` dokázal FastTrack odhaliť aj takzvané assertion chyby, teda chyby vzniknuté zlým využitím pthread knižnice. V prípadoch `t07`, `t08`, `t09` a `t10` dochádza k detekovaniu data race chýb v unwind systémovej knižnici, ktorá je taktiež monitorovaná analyzátorom.

Hodnoty uvedené v zátvorke v tabuľke 8.2 predstavujú namerané hodnoty odhaľovania data race chýb, s využitím menšieho počtu vlákien a prechodov pomocou za pomoci analyzátora FastTrack. Ide o programi, ktoré vykazujú istú špecifickosť (assertion chyby, ojedinelosť výskytu chyby v aktuálnom behu). V programe `t02` sa jedná len o výskyt data race chyby zapríčinenej zlým zamykaním (celkovo v programe sa vyskytuje aj ďalšia chyba mimo túto). V `t12` sa taktiež jedná o rovnaký problém. V prípade `t08` a `t11` ide o rovnakú chybu v oboch programoch, pri dotazovaní sa na aktuálny tiket.

8.3.1 FastTrack a AtomRace

Pri experimentovaní s predchádzajúcimi prípadmi bol využívaný aj analyzátor AtomRace, pomocou ktorého dochádzalo či už k overeniu správnosti detekovaných data race chýb, tak aj k porovnaniu presnosti detekcie. FastTrack s očakávaním v tejto oblasti výrazne vyniká oproti AtomRace. Keďže AtomRace detekuje len aktuálne videný výskyt data race chyby v danom behu narozdiel od FastTrack-u, ktorý zohladňuje aj ďalšie možné scenáre preloženia vlákien, a tým prechádza väčšie množstvo reálnych behov programu. Ako je vidieť z tabuľky 8.2, FastTrack predčil vo frekvencii vyhľadania chýb AtomRace v každom programe, samozrejme výsledky sú udávané bez využitia akéhokoľvek šumu. Reálny príklad rozdielu medzi týmito dvoma analyzátormi je zjavne viditelný na príklade banky (tabuľka 8.1), kde sa vyskytne data race chyba v aktuálnom behu len ojedine, takže AtomRace nič nezaznamená aj po veľkom množstve opakovaní, no FastTrack odhalí chybu okamžite.

Tabuľka 8.2: Tabuľka zobrazujúca úspešnosť odhalenia data race chyby v programoch t1 až t13, zobrazuje v koľkých prípadoch bola detekovaná chyba z celkového počtu testovacích behov.

	AtomRace	FastTrack
t1	3/30	30/30
t2	0/30	28/30 (17/30)
t3	2/30	30/30
t4	3/30	30/30
t5	0/30	2/30
t6	1/30	30/30
t7	19/30	30/30
t8	1/30	27/30 (26/30)
t9	2/30	30/30
t10	0/30	1/30
t11	4/30	27/30 (25/30)
t12	1/30	24/30 (20/30)
t13	21/30	30/30

8.4 Ďalšie experimenty

Ďalším smerom, ktorým by bolo vhodné sa uberať pri experimentovaní s analyzátorom, je využitie šumu, najmä v prípadoch `t05` a `t10`, kedy dochádzalo k slabým výsledkom. S tým je spojené aj experimentovanie a porovnávanie využitia šumu spolu s analyzátorom AtomRace, proti využitiu šumu s analyzátorom FastTrack. Vhodné by bolo porovnať ako sa odlišujú rôzne konfigurácie šumu pre oba analyzátory, či spôsobujú rovnaký efekt, alebo s rovnakou konfiguráciou vytvárajú rôzne výsledky medzi týmito analyzátormi. Bolo by však vhodné obmeniť programovú sadu smerom k programom podobným `t05` a `t10`, keďže v ostatných programoch extrapolácia FastTrack-u umožnila odhaliť data race chyby takmer vždy naproti AtomRace-u, kde bol výsledok opačný. Rýchlosť analýzy samozrejme taktiež hrá rolu pri verifikovaní software. Ďalšie porovnanie by bolo možné medzi rýchlosťou analyzovania programu pomocou FastTrack-u a iného analyzátora založeného na princípe vektro-klokov, ako napríklad Djit+. Implementácia v jazykoch Java a C/C++ by bolo ďalším možným porovnaním tohto analyzátora, nie len v rýchlosti analýzy ale aj v počte a frenkvencii odhaľovania chýb a taktiež využitie šumu v oboch prípadoch.

Kapitola 9

Záver

Chyby typu data race sú vo viac-vláknovom programovaní veľkým problémom a ich odhalovanie môže byť veľmi problematické najmä z pohladu nedeterministického plánovania vlákien. Jednou z techník, ktorá sa snaží takéto chyby detekovať je dynamická analýza (kapitola 3) založená na princípe monitorovania programu za jeho behu. Tým, že monitoruje len jeden beh umožňuje chybám, ktoré sa prejavia len v konkrétnych, často ojedinelých preložení, zostať nepovšimnuté, a tak vystaviť užívatela do mylnej predstavy bezchybného programu. Z tohto dôvodu sa dynamická analýza rozširuje o ďalšie techniky extrapolácie, ktoré umožňujú analyzátorom overiť aj ďalšie exekúcie podobné primárnemu behu a nájsť v nich chyby. Extrapolácia môže byť prevedená pomocou happens-before relácie (sekcia 3.1.1). Algoritmus pre odhaľovanie chýb typu data race (sekcia 2.2.1) pomocou dynamickej analýzy FastTrack (kapitola 6), implementuje túto reláciu v podobe vektorových hodín (sekcia 5.1). V porovnaní s ďalšími analyzátormi sa snaží optimalizovať náklady na analýzu. FastTrack prichádza s myšlienkou optimalizovaných vektorových hodín v podobe epoch(sekcia 6.1.1), ktoré tvoria dvojicu vlákno a hodnota hodín, na miestach kde je to bezpečné. FastTrack je implementovaný pre programy v jazyku Java. Cieľom tejto práce ho bolo implementovať pre C/C++ programy. Algoritmus je implementovaný v prostredí ANaConDA (kapitola 4), ktoré tvorí monitorovaciu vrstvu medzi analyzátorom a analyzovaným programom, čím zabezpečuje vyťahovanie zaujímavých informácií z bežiaceho programu a tým poskytuje analyzátoru potrebné informácie ku monitorovaniu aplikácie.

Možnosti rozšírenia

Odovzdaná implementácia algoritmu FastTrack umožňuje detekovanie viac data race chýb v programe, no jeho rozšírenie je možné vo viacerých smeroch. V provom rade by bolo možné optimalizovať epochy na maximum, implementovaním epoch v podobe jednej číselnej hodnoty, narozdiel od dvojice hodnota a identifikačné číslo vlákna. Jednalo by sa o číslo rozdelené na dve bitové časti reprezentujúce indentifikačné číslo vlákna a v druhej časti hodnotu hodín. Ďalšou z možností, ako rozšíriť algoritmus by bolo rozšírenie podpory pre viac synchronizačných objektov ako napríklad bariér alebo iných programátorom definovaných synchronizačných funkcií. Aktuálna verzia podporuje len základnú synchronizáciu v podobe zámkovej logiky `lockAcquire` a `lockRelease` a synchronizáciu pri vytváraní a zanikaní vlákien `fork` a `join`. Taktiež by sa dal vylepšiť výstup, ktorý podáva analyzátor. Pridať backtrace (alebo ukladať dáta) pre zistenia bližších informácii (zobrazovať na akom riadku v kóde došlo ku chybe) o predposlednom prístupe, teda prístupe s ktorým kolidoval ten posledný. Ako ďalší postup by bolo možné otestovať rýchlosť, s akou FastTrack analyzuje

programy oproti iným analyzátorom, ako napríklad už spomínaný AtomRace alebo Djit+. Do budúcna by bolo dobré otestovať FastTrack aj na komplexnejších programoch, kde by sa mala ukázať jeho prednosť v rýchlosti analýzy.

Literatúra

[1] Ferrara, P.: Static Analysis of the Determinism of Multithreaded Programs. In *2008 Sixth IEEE International Conference on Software Engineering and Formal Methods*, Nov 2008, ISSN 1551-0255, s. 41–50, doi:10.1109/SEFM.2008.14.

[2] Fiedor, J.; Křena, B.; Letko, Z.; aj.: *A Uniform Classification of Common Concurrency Errors*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, ISBN 978-3-642-27549-4, s. 519–526, doi:10.1007/978-3-642-27549-4_67.
URL http://dx.doi.org/10.1007/978-3-642-27549-4_67

[3] Fiedor, J.; Vojnar, T.: Noise-Based Testing and Analysis of Multi-threaded C/C++ Programs on the Binary Level. In *PADTAD'12*, ACM, 2012, s. 36–46.

[4] Fiedor, J.; Vojnar, T.: ANaConDA: A Framework for Analysing Multi-threaded C/C++ Programs on the Binary Level. In *Proc. of RV'13*, volume 7687 of LNCS, Springer-Verlag, 2013, s. 35–41.

[5] Flanagan, C.; Freund, S. N.: FastTrack: efficient and precise dynamic race detection. In *PLDI'09: Proceedings of the 2009 ACM SIGPLAN conference on Programming language design and implementation*, New York, NY, USA: ACM, 2009, ISBN 978-1-60558-392-1, s. 121–133, doi:http://doi.acm.org/10.1145/1542476.1542490.

[6] Flanagan, C.; Freund, S. N.: The RoadRunner Dynamic Analysis Framework for Concurrent Programs. In *Proceedings of the 9th ACM SIGPLAN-SIGSOFT Workshop on Program Analysis for Software Tools and Engineering*, PASTE '10, New York, NY, USA: ACM, 2010, ISBN 978-1-4503-0082-7, s. 1–8, doi:10.1145/1806672.1806674.
URL http://doi.acm.org/10.1145/1806672.1806674

[7] Guerraoui, R.; Kapalka, M.: *Principles of Transactional Memory*. Morgan and Claypool Publishers, 2010.

[8] Kasikci, B.; Zamfir, C.; Candea, G.: Data Races vs. Data Race Bugs: Telling the Difference with Portend. In *Proceedings of the Seventeenth International Conference on Architectural Support for Programming Languages and Operating Systems*, ASPLOS XVII, New York, NY, USA: ACM, 2012, ISBN 978-1-4503-0759-8, s. 185–198, doi:10.1145/2150976.2150997.
URL http://doi.acm.org/10.1145/2150976.2150997

[9] Lamport, L.: Time, Clocks, and the Ordering of Events in a Distributed System. *Commun. ACM*, ročník 21, č. 7, Červenec 1978: s. 558–565, ISSN 0001-0782, doi:10.1145/359545.359563.
URL http://doi.acm.org/10.1145/359545.359563

[10] Letko, Z.; Vojnar, T.; Křena, B.: AtomRace: data race and atomicity violation detector and healer. In *PADTAD'08*, New York, NY, USA: ACM, 2008, ISBN 978-1-60558-052-4, s. 1–10.

[11] Luk, C.-K.; Cohn, R.; Muth, R.; aj.: Pin: Building Customized Program Analysis Tools with Dynamic Instrumentation. In *Proceedings of the 2005 ACM SIGPLAN Conference on Programming Language Design and Implementation*, PLDI '05, New York, NY, USA: ACM, 2005, ISBN 1-59593-056-6, s. 190–200, doi:10.1145/1065010.1065034.
URL http://doi.acm.org/10.1145/1065010.1065034

[12] Nethercote, N.; Seward, J.: Valgrind: A Framework for Heavyweight Dynamic Binary Instrumentation. *SIGPLAN Not.*, ročník 42, č. 6, Červen 2007: s. 89–100, ISSN 0362-1340, doi:10.1145/1273442.1250746.
URL http://doi.acm.org/10.1145/1273442.1250746

[13] Parízek, P.; Lhoták, O.: Model Checking of Concurrent Programs with Static Analysis of Field Accesses. *Sci. Comput. Program.*, ročník 98, č. P4, Únor 2015: s. 735–763, ISSN 0167-6423, doi:10.1016/j.scico.2014.10.008.
URL http://dx.doi.org/10.1016/j.scico.2014.10.008

[14] Pozniansky, E.; Schuster, A.: Efficient On-the-fly Data Race Detection in Multithreaded C++ Programs. In *Proc. of PPoPP'03*, New York, NY, USA: ACM, 2003, ISBN 1-58113-588-2, s. 179–190, doi:http://doi.acm.org/10.1145/781498.781529.

[15] Savage, S.; Burrows, M.; Nelson, G.; aj.: Eraser: A Dynamic Data Race Detector for Multithreaded Programs. *ACM Trans. Comput. Syst.*, ročník 15, č. 4, Listopad 1997: s. 391–411, ISSN 0734-2071, doi:10.1145/265924.265927.
URL http://doi.acm.org/10.1145/265924.265927

Príloha A

Obsah CD

Priložené CD obsahuje nasledujúce súbory:

- BP_ elektronickaForma.pdf - elektronická forma bakalárskej práce
- BP_ listForma.pdf - forma pre tlač bakalárskej práce
- Manuál - manuál ku spusteniu analyzátora
- Anaconda - súbor obsahujúci framefork ANaConDA