

Fehlersuche und Visualisierung der Belegung von Synchronisationsmitteln in nebenläufigen Systemen

Marcel Sobottka

30. April 2020

Erstgutachter: Prof. Dr.-Ing. habil. Herwig Unger
Zweitgutachter: Dipl.-Inform. (Univ.) Marcel Schaible

Inhaltsverzeichnis

	Seite
Inhaltsverzeichnis	III
Abbildungsverzeichnis	IV
Tabellenverzeichnis	V
Quellcodeverzeichnis	VI
1 Motivation	7
2 Analyse	9
2.1 Deadlockerkennung allgemein	9
2.2 PEARL	10
2.3 MagicLock	11
3 Design	13
3.1 Erzeugung der Trace-Datei	13
3.2 Analysieren der Trace-Datei	14
3.3 Erweiterung: Potenzielle Deadlocks	14
4 Implementierung	15
4.1 Trace Funktion	15
4.2 Analyse Programm	15
4.3 Visualisierung von potenziellen Deadlocks	15
5 Validierung	16
5.1 Trace Funktion	16
5.2 Analyse Programm	16
5.3 Visualisierung von potenziellen Deadlocks	16
6 Ausblick	17
6.1 Offene Punkte	17
6.2 Weiterentwicklung	17
Literatur	18

Abbildungsverzeichnis

Tabellenverzeichnis

Quellcodeverzeichnis

Beispiel einer OpenPEARL Anwendung mit einem potenziellen Deadlock . 12

1 Motivation

Bei der parallelen Programmierung ist Nebenläufigkeit ein bewusst genutztes Mittel. Die Ausführung von solchen Programmen ist nicht deterministisch. Dies führt dazu, dass Zugriffe auf gemeinsam genutzte Ressourcen synchronisiert werden müssen. Bei der Synchronisierung können zur Laufzeit Deadlocks auftreten. Diese werden in Abschnitt 2.1 beschrieben. Für Entwickler stellen potenzielle Deadlocks ein großes Problem dar, da sie oft erst zur Laufzeit auffallen. Während der Entwicklung kann ein Entwickler Nebenläufigkeitsprobleme die zu Deadlocks führen können nur sehr schwer erkennen. Gerade in komplexen Anwendungen in denen viele parallele Aufgaben ausgeführt werden, ist es für den Entwickler nicht mehr möglich potenzielle Deadlocks zu erkennen. Automatisierte Tests können das Erkennen solcher Probleme zwar verbessern, durch die nicht deterministische Ausführung bleiben jedoch viele Probleme unerkannt. Für die Echtzeit-Programmiersprache PEARL gibt es derzeit keine Unterstützung für den Entwickler um solche Probleme effektiv zu erkennen. Um den Entwickler besser unterstützen zu können wird ein Verfahren vorgestellt und für PEARL implementiert, welches die chronologische Abfolge von verwendeten Synchronisationsmitteln darstellen und potenzielle Deadlocks erkennen kann.

In Abschnitt 2.1 wird das grundlegende Verfahren zur Identifizierung von potenziellen Deadlocks vorgestellt. Es wird dargestellt was ein Deadlock ist und wie dynamische Verfahren zur Erkennung von Deadlocks funktionieren. In Abschnitt 2.2 wird die Echtzeit-Programmiersprache PEARL [2] beschrieben. Es wird gezeigt welche Synchronisationsmittel in PEARL existieren und wie diese benutzt werden. Anschließend wird ein Algorithmus zur Erkennung von potenziellen Deadlocks in Abschnitt 2.3 beschrieben. Anhand eines Quellcode Beispiels in PEARL wird der Algorithmus Schritt für Schritt durchlaufen und erläutert.

Das Design zur Implementierung des Algorithmus wird in Kapitel 3 beschrieben. In Abschnitt 3.2 wird der in PEARL umzusetzende Anteil definiert, um die benötigten Informationen für den Algorithmus in einer Trace-Datei zusammenzustellen. Zusätzlich werden die Anforderungen bezüglich der Performanz festgelegt. In Abschnitt 3.2 wird das Design des Programms zur Visualisierung der chronologischen Belegung der Synchronisationsmittel basierend auf den Informationen der erstellten Trace-Datei definiert. In Abschnitt 3.3 wird eine Erweiterung des Analyse-Programms vorgestellt. Zusätzlich zu der chronologischen Belegung der Synchronisationsmittel werden potenzielle Deadlocks erkannt. Es wird beschrieben wie die Visualisierung aussehen und wie der in Abschnitt 2.3 vorgestellte Algorithmus umgesetzt werden soll.

In Abschnitt 4.1 wird die Implementierung zur Erstellung der Trace-Datei in PEARL beschrieben. Anschließend werden die Implementierungen des Programms zur Analyse und Visualisierung der Trace-Datei in Abschnitt 4.2 und Abschnitt 4.3 vorgestellt.

Die Validierung der in Kapitel 4 erstellten Programme und Funktionen wird in Kapitel 5

beschrieben. Dabei werden vor allem die definierten Performanz Anforderungen validiert. Abschließend werden in Kapitel 6 offene Punkte und mögliche Weiterentwicklung beschrieben.

2 Analyse

	Seite
2.1 Deadlockerkennung allgemein	9
2.2 PEARL	10
2.3 MagicLock	11

2.1 Deadlockerkennung allgemein

Im Gegensatz zu Single-Threaded-Applikationen sind Multi-Threaded-Anwendungen nicht deterministisch. Dies kann zu *race conditions* führen. Eine *race condition* tritt zum Beispiel dann auf, wenn zwei Threads einen Zähler jeweils um eins erhöhen wollen. Angenommen der Zähler hat zu Beginn den Wert drei. Beide Threads wollen jetzt nahezu gleichzeitig den Zähler um eins erhöhen. Dazu lesen beide Threads den aktuellen Wert des Zählers, in diesem Fall drei, aus. Anschließend addieren beide eins hinzu und schreiben den neuen Wert, in diesem Fall vier, in den Zähler. Erwartet wurde jedoch der Wert fünf, da beide Threads den Zähler um jeweils eins erhöhen sollten. Um solche *race conditions* zu verhindern werden Synchronisierungsmechanismen benötigt.

Eine Möglichkeit um den Zugriff auf eine gemeinsame Ressource zu synchronisieren sind Locks. Ein Lock ist ein exklusiver Zugriff auf ein Objekt, ein sogenanntes Lockobjekt. Das bedeutet, dass während ein Thread einen Lock auf ein Objekt besitzt, andere Threads, welche auf dasselbe Objekt zugreifen wollen, warten müssen bis es freigegeben wurde.

Betrachtet man das Beispiel mit dem Zähler erneut, dieses Mal mit Locks als Synchronisationsmittel, kann es zu folgender Ausführung kommen. Der Zähler hat zu Beginn wieder den Wert drei. Die Threads $T1$ und $T2$ wollen erneut den Zähler nahezu gleichzeitig erhöhen. Dieses Mal versuchen beide das Lockobjekt $L1$ in Besitz zu nehmen. Der Thread $T2$ nimmt $L1$ zuerst in Besitz, daraus folgt $T1$ muss warten. $T2$ liest den aktuellen Wert des Zählers aus, erhöht diesen um eins und schreibt den neuen Wert vier in den Zähler. Anschließend gibt $T2$ das Lockobjekt $L1$ frei. Jetzt erhält der Thread $T1$ den Zugriff auf $L1$ und liest ebenfalls den Zähler, jetzt vier, aus, erhöht diesen und schreibt den neuen Wert fünf in den Zähler. Anschließend gibt $T1$ das Lockobjekt $L1$ frei.

Die Verwendung von Locks kann in Verbindung mit der nicht deterministischen Ausführung von Multi-Threaded-Anwendungen zu Problemen führen. Angenommen es existieren zwei Threads $T1$ und $T2$ und zwei Lockobjekte $L1$ und $L2$. Angenommen $T1$ besitzt $L1$ und zu gleichen Zeit erlangt $T2$ das Lockobjekt $L2$. Wenn jetzt der Thread $T1$ das Lockobjekt $L2$ anfordert und der Thread $T2$ das Lockobjekt $L1$, kommt es zu einem *Deadlock*. Die Ausführung des Programms terminiert nicht, da beide Threads auf den jeweils anderen Thread warten und sich gegenseitig blockieren.

Solche potenziellen Deadlocks zu erkennen ist die Aufgabe von statischen und dynamischen Methoden zur Deadlockerkennung. Die statische Deadlockerkennung analysiert den Quellcode und wird hier nicht näher betrachtet. Die dynamische Deadlockerkennung analysiert eine Anwendung zur Laufzeit und läuft in folgenden drei Schritten ab:

1. Erstellung einer Trace-Datei
2. Erstellung eines Graphen basierend auf den Informationen aus der Trace-Datei
3. Auffinden von potenziellen Deadlocks durch die Identifizierung von Zyklen innerhalb des Graphen

Eine Trace-Datei enthält einen *execution trace* des ausführenden Programms. Ein *execution trace* ist eine Abfolge von Events. Ein Event e_i wird durch eine der folgenden Methoden definiert: starten eines Threads, Inbesitznahme eines Lockobjekts und Freigabe eines Lockobjekts. Das Starten eines neuen Threads ist definiert durch:

$s(\text{Programmstelle}, \text{ausführender Thread}, \text{Name des neuen Threads})$

Zum Beispiel bedeutet $s(2, \text{main}, T1)$, dass an der Programmstelle 2 der Thread *main* den Thread *T1* gestartet hat. Die Inbesitznahme eines Lockobjekts ist definiert durch:

$l(\text{Programmstelle}, \text{ausführender Thread}, \text{Name des Lockobjekts})$

Zum Beispiel bedeutet $l(24, T1, L3)$, dass an der Programmstelle 24 der Thread *T1* das Lockobjekt *L3* in Besitz genommen. Die Freigabe eines Lockobjekts ist definiert durch:

$u(\text{Programmstelle}, \text{ausführender Thread}, \text{Name des Lockobjekts})$

Zum Beispiel bedeutet $u(30, T1, L3)$, dass an der Programmstelle 30 der Thread *T1* das Lockobjekt *L3* freigegeben hat.

Die Abfolge aller während der Laufzeit des Programms aufgetretenen Events definieren einen möglichen *execution trace* des Programms. Programme welche mit mehreren Threads arbeiten, liefern keine deterministische Abfolge. Jede Ausführung eines solchen Programms kann zu unterschiedlichen *execution traces* führen.

Im zweiten Schritt wird aus dem vorher erzeugten *execution trace* ein Lockgraph erstellt. Ein Lockgraph ist definiert durch:

$$LG = (L, R)$$

L ist die Menge aller Lockobjekte im *execution trace* und R die Menge aller Lockpaare. Ein Lockpaar ist definiert durch das Tupel $(L1, L2)$ für das gilt: Es existiert ein Thread, welcher das Lockobjekt *L1* besitzt, während er den Lock *L2* anfordert.

2.2 PEARL

- Kurze Beschreibung der Programmiersprache PEARL
- Aufzeigen der Möglichkeiten von Synchronisationsmitteln in PEARL

In Quellcode 2.1 ist ein Beispielprogramm in der Programmiersprache PEARL dargestellt. Das Programm startet zwei parallele Aufgaben welche beide eine Zeichenfolge auf der Standardausgabe ausgeben. Der Zugriff auf die Standardausgabe muss dabei synchronisiert erfolgen.

In den Zeilen 1 bis 11 werden Variablen definiert, wie zum Beispiel die Ausgabe über die Standardausgabe und die zwei *SEMA* Variablen *L1* und *L2* in den Zeilen 9 und 10. Ein *SEMA* Objekt ist ein Semaphore und dient als Synchronisationsmittel. Es kann als Wert nicht negative ganze Zahlen besitzen, wobei null den Zustand „gesperrt“ und positive Zahlen den Zustand „frei“ bedeuten [2, S. 9–17]. Eine *SEMA* Variable hat zu Beginn den Wert null und den Zustand „gesperrt“. In den Zeilen 12 bis 17 ist ein *TASK* definiert. Durch die Kennzeichnung *MAIN* wird der *TASK* direkt beim Start des Programms ausgeführt. Die Befehle *RELEASE* in den Zeilen 13 und 14 erhöhen den Wert der jeweiligen *SEMA* Variable um eins, wodurch der Zustand von „gesperrt“ auf „frei“ gesetzt wird. Anschließend werden in den Zeilen 15 und 16 die *TASKS* *T2* und *T3* gestartet.

Die *TASKS* *T2* und *T3* geben in den Zeilen 22 bis 24 und in den Zeilen 32 bis 34 die Zeichenfolge „Hello World T2“ bzw. „Hello World T3“ auf der Standardausgabe aus. Die Synchronisierung des Zugriffs auf die Standardausgabe erfolgt mittels den *SEMA* Variablen *L1* und *L2*. Mit dem *REQUEST* Befehl wird der Wert einer *SEMA* Variable um eins verringert. Ist der Wert einer *SEMA* Variable null wird der *TASK* angehalten und in eine Warteschlange eingereiht. Sobald die Variable über den Befehl *RELEASE* wieder freigeben wird, wird der nächste *TASK* in der Warteschlange gemäß seiner Priorität fortgeführt. Beide *TASKS* versuchen beide *SEMA* Variablen in Besitz zu nehmen. *T2* versucht in den Zeilen 20 und 21 zuerst *L1* und dann *L2* in Besitz zu nehmen. *T3* versucht in den Zeilen 30 und 31 zuerst *L2* und dann *L1* in Besitz zu nehmen. Da beide *TASKS* parallel laufen, kann es passieren, dass *T2* *L1* in Zeile 20 in Besitz nimmt und gleichzeitig *T3* in Zeile 30 *L2* in Besitz nimmt. Beide *SEMA* Variablen haben jetzt den Wert null und den Zustand „gesperrt“. Der *TASK* *T2* wartet jetzt darauf, dass *L2* freigegeben wird und *T3* wartet darauf, dass *L1* freigegeben wird. Beide *TASKS* warten auf den jeweils anderen. Diese Situation wird als Deadlock bezeichnet.

2.3 MagicLock

- Beschreibung des MagicLock[1] Algorithmus

```
1  MODULE(test);
2
3  SYSTEM;
4      stdout: StdOut;
5
6  PROBLEM;
7      SPC stdout DATION OUT SYSTEM ALPHIC GLOBAL;
8      DCL termout DATION OUT ALPHIC DIM(*,80) FORWARD STREAM CREATED(stdout);
9      DCL L1 SEMA;
10     DCL L2 SEMA;
11
12 T1: TASK MAIN;
13     RELEASE L1;
14     RELEASE L2;
15     ACTIVATE T2;
16     ACTIVATE T3;
17 END;
18
19 T2: TASK;
20     REQUEST L1;
21     REQUEST L2;
22     OPEN termout;
23     PUT 'Hello World T2' TO termout BY A, SKIP;
24     CLOSE termout;
25     RELEASE L2;
26     RELEASE L1;
27 END;
28
29 T3: TASK;
30     REQUEST L2;
31     REQUEST L1;
32     OPEN termout;
33     PUT 'Hello World T3' TO termout BY A, SKIP;
34     CLOSE termout;
35     RELEASE L1;
36     RELEASE L2;
37 END;
38
39 MODEND;
```

Quellcode 2.1: Beispiel einer OpenPEARL Anwendung mit einem potenziellen Deadlock

3 Design

	Seite
3.1 Erzeugung der Trace-Datei	13
3.2 Analysieren der Trace-Datei	14
3.3 Erweiterung: Potenzielle Deadlocks	14

3.1 Erzeugung der Trace-Datei

- Definition der notwendigen Informationen der Trace-Datei
- Aufzeigen der Herausforderungen in Bezug auf Performance und Speicherauslastung
- Anforderungen definieren:
 - Laufzeit des Programms soll sich um maximal $x\%$ erhöhen
 - Speicherauslastung des Programms soll sich um maximal $y\%$ erhöhen
- Aktuelle Idee: Das Erstellen der Trace-Datei wird in eine eigenes Modul ausgelagert. Das Modul enthält einen Task der durch einen Interrupt aktiviert wird. Bei Aktivierung werden die benötigten Informationen für den Trace-Logeintrag übergeben/zur Verfügung gestellt. Diese Informationen werden in eine Warteschlange eingereiht. Die Warteschlange wird über eine einfach verkettete Liste realisiert. Das Einfügen in eine einfach verkettete Liste ist konstant und geschieht daher in $O(1)$. Bei jeder x -ten Aktivierung, wobei x die maximale Größe der Warteschlange ist, wird über einen zusätzlichen Interrupt ein zweiter Task aktiviert. Der zweite Task liest alle vorhanden Einträge aus der Warteschlange aus und schreibt diese in die Trace-Datei. Das Entfernen des ersten Eintrags aus der Warteschlange (einfach verkettete Liste) ist wieder konstant und daher $O(1)$. Die Liste wird für jeden Eintrag einmal durchlaufen. Die Laufzeit beträgt daher $O(x)$. Das Öffnen und Schließen der Trace-Datei hat die Laufzeit y . Das Schreiben eines Logeintrags, also eine Zeile in die Trace-Datei, hat die Laufzeit z . Damit hat jeder x -te Interrupt die Laufzeit $O(y + x \cdot z)$. Somit hat jeder Interrupt die Laufzeit $O(\frac{y+x \cdot z}{x})$.

Zusätzlich zu jedem x -ten Interrupt muss der zweite Task, welcher die Einträge aus der Warteschlange in die Trace-Datei schreibt, auch zeitlich angestoßen werden. Zum Beispiel sollte der Task alle 60 Sekunden oder nach x Interrupts aktiviert werden. Nach einer Aktivierung des Tasks muss der Timer wieder zurückgesetzt werden. Bedeutet wenn nach 50 Sekunden der x -te Interrupt kommt, muss der Timer wieder von vorne beginnen, damit die Trace-Datei nicht nach 10 Sekunden erneut beschrieben wird.

Der zusätzliche Speicherbedarf beträgt $x \cdot i$, wobei i die Größe der Information eines Logeintrags entspricht. Ein Logeintrag benötigt die Informationen:

1. Aktion (REQUEST oder RELEASE) \Rightarrow 1 Bit
2. Programmstelle \Rightarrow 64-Bit Ganzzahl (muss eventuell noch genauer definiert werden)
3. ID des Threads \Rightarrow 16-Bit Ganzzahl (maximale Thread Id für Linux beträgt 32768) theoretisch über 15 Bit abbildbar, da immer positiv
4. Name des Lockobjekts \Rightarrow 11 Bit Ganzzahl (maximal Variablennamenslänge für C++ beträgt 2048)

Mindestgröße für i beträgt $1 + 64 + 16 + 11 = 92$ Bit. Die Größe eines Zeigers in C++ beträgt auf einem 64 Bit System 64 Bit. Ein Eintrag in der Warteschlange benötigt somit $92 \text{ Bit} + 64 \text{ Bit} = 156 \text{ Bit}$ Speicher. Die Warteschlange benötigt maximal daher $156 \text{ Bit} \cdot x$ zusätzlichen Speicher.

3.2 Analysieren der Trace-Datei

- Externes Programm geschrieben in Java
- Anforderungen definieren:
 - Darstellung der Trace-Datei (welcher Thread hat welches Synchronisationsmittel wann genommen und wieder freigegeben)

3.3 Erweiterung: Potenzielle Deadlocks

- Programm aus Abschnitt 3.2 wird erweitert
- Es sollen potenzielle Deadlocks mit Hilfe des aus Abschnitt 2.3 beschriebenen Verfahrens bestimmt werden
- Potenzielle Deadlocks sollen als gerichtete Graphen visualisiert werden

4 Implementierung

	Seite
4.1 Trace Funktion	15
4.2 Analyse Programm	15
4.3 Visualisierung von potenziellen Deadlocks	15

4.1 Trace Funktion

- Vorstellung der Implementierung der Trace Funktionalität in PEARL

4.2 Analyse Programm

- Vorstellung der Implementierung des Analyse Programms in Java
- Grafiken/Screenshots mit Analyse Beispielen

4.3 Visualisierung von potenziellen Deadlocks

- Vorstellung der Implementierung des Algorithmus zur Erkennung von potenziellen Deadlocks
- Grafiken/Screenshots mit Analyse Beispielen

5 Validierung

	Seite
5.1 Trace Funktion	16
5.2 Analyse Programm	16
5.3 Visualisierung von potenziellen Deadlocks	16

5.1 Trace Funktion

- Beispielprogramme in PEARL definieren
- Anforderungen validieren:
 - Laufzeiten der einzelnen Programme mit und ohne Trace Funktionalität bestimmen und vergleichen
 - Speicherauslastung der einzelnen Programme mit und ohne Trace Funktionalität bestimmen und vergleichen

5.2 Analyse Programm

- Die aus Abschnitt 5.1 erstellten Trace-Dateien mit dem erstellten Analyse Programm auswerten

5.3 Visualisierung von potenziellen Deadlocks

- Die aus Abschnitt 5.1 erstellten Trace-Dateien auswerten und die potenziellen Deadlocks visuell als gerichtete Graphen aufzeigen

6 Ausblick

	Seite
6.1 Offene Punkte	17
6.2 Weiterentwicklung	17

6.1 Offene Punkte

- Aufzeigen was nicht gemacht wurde und warum (eventuell welche Synchronisationsmittel nicht erkannt werden (nur Sema keine Bolt Variablen))

6.2 Weiterentwicklung

- Alle möglichen Synchronisationsmittel erkennen
- Trace Funktionalität in den OpenPEARL Compiler integrieren, so dass es mittels compiler flag an und ausgeschaltet werden kann

Literatur

- [1] Yan Cai und W. K. Chan. „Magiclock: Scalable Detection of Potential Deadlocks in Large-Scale Multithreaded Programs“. In: *IEEE Transactions on Software Engineering (TSE)* (2014) (siehe S. 11).
- [2] PEARL’ GI-Fachgruppe 4.4.2 ’Echtzeitprogrammierung. *PEARL 90 Sprachreport*. 1. Jan. 1995. URL: <https://www.real-time.de/misc/PEARL90-Sprachreport-V2.0-GI-1995-de.pdf> (besucht am 13. Nov. 2019) (siehe S. 7, 11).