Verlässliche Systeme

8. Kapitel
Behandlung Byzantinischer Fehler

Prof. Matthias Werner
Professur Betriebssysteme

8.1 Agreementprobleme

Konsens

Konsens

Konsens erlaubt einer Menge von fehlerfeien Verarbeitungseinheiten den korrekten Wert eines Teils des Systemzustandes zu erfahren und gleichzeitig zu wissen, dass jede andere korrekte Verarbeitungseinheit das selbe Ergebnis erhält, unabhängig von den Aktionen der fehlerhaften Einheiten.

- Bereits betrachtete „Systemdiagnose“ kann bereits als Konsens aufgefasst werden
- Andere Konsensansätze sind z.B.:
  - Mehrheitsabstimmung
  - Gruppenmitgliedschaft
  - Uhrensynchronisation
- Wir betrachten hier **Byzantinische** Konsens-Probleme ➡ arbeiten auch bei Byzantinischen Fehlern (vgl. Kapitel 4)

Problem des Byzantinischen Agreements

- Byzantinisches Agreement nach LAMPORT
  - Die Armee von Byzanz will mit mehreren Divisionen eine Stadt erobern
  - Jede Division wird von einem General befehligt, ein General ist der kommandierende General (*Commander*), die anderen Generalleutnants (*Lieutenant Generals*)
  - Generäle kommunizieren ausschließlich durch Boten
  - Unter den Generälen können sich Verräter befinden
  - Eroberung ist nur bei konsistentem Verhalten (der loyalen Generäle) erfolgreich
- **Problem:** Gesucht ist ein Verfahren (Algorithmus), das folgendes garantiert:
  - Alle (loyalen) Generäle befolgen die gleiche Anweisung
  - Ist der kommandierende General loyal, befolgen die (loyalen) Generäle seine Anweisung

Varianten

Es gibt eine Reihe ähnlicher Probleme, die sich aber ineinander überführen lassen:

- **Generalsproblem (Byzantinisches Agreement)**
  - Ein General gibt Befehl; alle loyalen Generäle sollen gleichen Befehl ausführen; wenn der kommandierender General loyal ist, wird sein Befehl ausgeführt
- **Konsens**
  - Alle Generäle haben eine private Meinung; alle loyalen Generäle sollen sich auf eine Meinung einigen
- **Interaktive Konsistenz**
  - Alle Generäle haben eine private Meinung; alle loyalen Generäle haben am Ende den gleichen Werte-Vektor, wobei sie Meinungen der loyalen Generäle im Werte-Vektor korrekt sind

Achtung: Benennung ist in der Literatur unterschiedlich zu finden.

Formale Definition am Beispiel Konsens

Eine etwas formalere Definition:

- Eine Menge von n Knoten v_i (Prozessoren, Rechnern, ...) sind durch ein (fehlerfreies) Netzwerk miteinander verbunden
- Jeder Knoten besitzt einen zunächst privaten Wert δ_i aus einer Menge Δ möglicher Werte
- Ziel ist es, dass jeder Knoten für einen Wert aus Δ entscheidet, wobei drei Bedingungen erfüllt werden sollen:
  - **Agreementbedingung**
    Keine zwei (fehlerfreien) Knoten entscheiden sich für unterschiedliche Werte
  - **Validierungsbedingung** auch: (Integritätsbedingung)Wenn alle fehlerfreien Knoten mit dem gleichen privaten Wert $\delta \in \Delta$ beginnen, dann muss dies auch der Ergebniswert sein
  - **Terminierungsbedingung**
    Alle fehlerfreien Knoten entscheiden sich nach endlicher Zeit

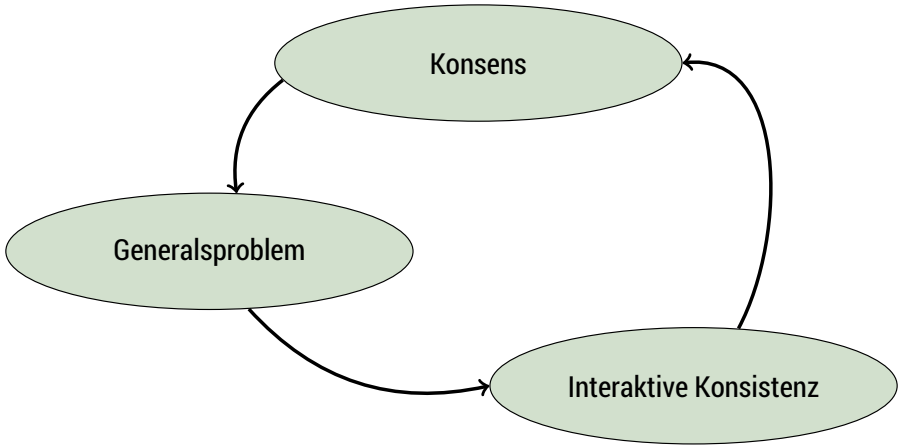
Vergleich

	Generalsproblem	Konsens	Int. Konsistenz
Startwert(e)	Wert des Kommandants	private Werte	private Werte
Einigung auf	gemeinsamer Wert	gemeinsamer Wert	Wertevektor
Validität (Resultat)	loyaler Kommandant ➡ Wert des Kommandants	$\forall$ korrekte Teilnehmer mit gleichen Wert v ➡ v	korrekter Teilnehmer ➡ korrektes Vektorelement

- Terminierungbedingung ist immer gleich

Äquivalenz

- Jedes Problem kann auf ein anderes zurückgeführt werden



- Daher gelten die meisten Aussage für **alle** Probleme

8.2 Unmöglichkeit von Byzantinischen Agreement

Anzahl der „Verräter“

Theorem 8.1

Wenn f die maximale Anzahl fehlerhafter Knoten in einem System S von n Knoten ist, gibt es keinen Algorithmus, der das Problem des Byzantinischen Agreements löst, solange $n \leq 3f$ gilt

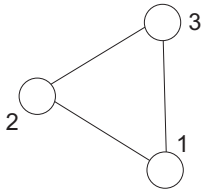
Beweis für Theorem 8.1

- Für $n = 2$: offensichtlich.
- Für $n > 2$: Beweisen zunächst einfacheres Lemma 8.1

Lemma 8.1

Das Byzantinische Agreement ist nicht lösbar, wenn $n = 3$ gilt und mindestens ein Fehler möglich ist.

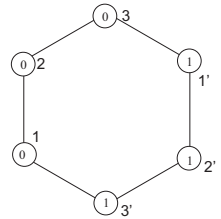
Betrachten System $\mathcal{S}$ mit 3 Knoten:

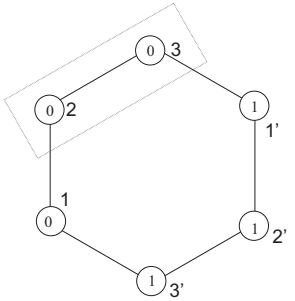


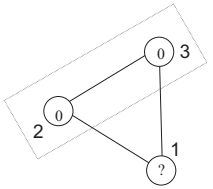
- **Widerspruchsbeweis**
- **Annahme**: In $\mathcal{S}$ lasse sich das Byzantinische Agreement lösen

Beweis für Lemma 8.1

- Konstruieren System $\mathcal{S}'$ aus zwei $\mathcal{S}$:
- O.B.d.A.: Die eine Hälfte startet mit 0, die andere mit 1
- Für jedes Paar korrekter Knoten ist (lokal) kein Unterschied zwischen $\mathcal{S}'$ und $\mathcal{S}$ mit einem defektem Knoten erkennbar

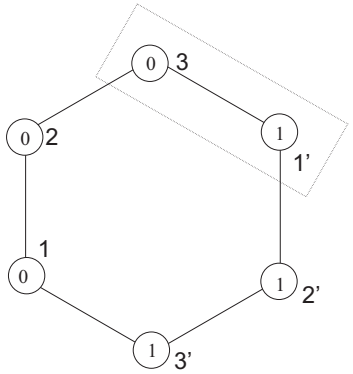






Beweis für Lemma 8.1 (Forts.)

- Wir wissen wenig über $\mathcal{S}'$, insbesondere nicht, ob es zum Konsens kommt
- Wir wissen aber, dass **benachbarte** Knoten zu einem Konsens kommen (folgt aus Annahme über $\mathcal{S}$)
- Betrachtung jeweils zweier anderer Knoten führt zum Widerspruch



Beweis für Lemma 8.1 (Forts.)

- Für $n \leq 3f$: Annahme des Gegenteils, sei $\mathcal{A}$ ein System mit n Knoten, von denen f fehlerhaft sind
- $\mathcal{A}$ löse das Agreementproblem
- Partitioniere $\mathcal{A}$ in drei nichtleere Teilmengen I_1, I_2 und I_3 mit $|I_i| \leq f$
- OBdA: Alle fehlerhaften Knoten von $\mathcal{A}$ sind entweder in I_1, I_2 oder I_3

Beweis für Lemma 8.1 (Forts.)

- Betrachten System $\mathcal{B}$, das durch $\mathcal{A}$ simuliert wird.
- $\mathcal{B}$ bestehe aus N_1, N_2 und N_3 (entsprechend I_1, I_2 und I_3)
- $\mathcal{A}$ kann $\mathcal{B}$ durch folgenden Spielregeln simulieren:
  - Alle Knoten in jedem I_i haben den gleichen Startwert v_i
  - Wenn alle Knoten in I_i sich für einen Endwert entscheidet, dann hat sich I_i (d.h. N_i) entschieden; falls unterschiedliche Werte in I_i entschieden werden, wird einer davon genommen.
- Wenn $\mathcal{A}$ das Agreement löst, wird das Agreement auch für $\mathcal{B}$ gelöst ➡ Widerspruch zu Lemma 8.1

□

Kommunikation zwischen den Generälen

Theorem 8.2

In einem System S mit n Knoten, von denen maximal f fehlerhaft sind, gibt es keinen Algorithmus, der das Problem des Byzantinischen Agreements löst, wenn die Konnektivität des Kommunikationsgraphen $k = \gamma(S) \leq 2f$ ist.

- Der Beweis von Theorem 8.2 wird hier nicht geführt ➡ Übung

Lösbarkeit Byzantinischer Probleme

- Es gibt ziemlich viel Unmöglichkeitsbeweise für das Byzantinische Agreement u.ä. Probleme
- DOLEV ET AL. haben fünf Systemcharakteristika genannt, die eine Rolle spielen:
  - **Ausführung auf den Knoten:** synchron vs. asynchron
  - **Kommunikation:** synchron vs. asynchron
  - **Nachrichtenreihenfolge:** geordnet vs. ungeordnet
  - **Übertragungsmechanismus:** broadcast vs. Punkt-zu-Punkt
  - **Senden/Empfangen-Atomarität:** atomar vs. nicht atomar

Lösbarkeit Byzantinischer Probleme (Forts.)

Es konnten genau vier Fälle identifiziert werden, bei denen es Byzantinisches Agreement mit $f > 1$ fehlerhaften Knoten geben kann:

- Synchrone Knoten und synchrone Kommunikation
- Synchrone Knoten und geordnete Nachrichtenreihenfolge
- Broadcast-Übertragung und geordnete Nachrichtenreihenfolge
- Synchrone Kommunikation, Broadcast-Übertragung, atomares Senden/Empfangen

Für $f = 1$ gibt es noch einen weiteren Fall:

- Asynchrone Knoten, synchrone Kommunikation, Punkt-zu-Punkt-Kommunikation und atomares Senden/Empfangen

8.3 Ein Algorithmus für Byzantinisches Agreement

- Oral-Messages-Algorithmus für Generalsproblem
- Annahmen:
  - Sei $|\Delta| = 2$ (z.B. $\Delta = \{a, b\}$)
  - Sei $n > 3 \cdot f$
  - Vollständig vernetzter Graph

Oral-Messages-Algorithmus

1. Kommandierender General sendet an alle Leutnants seinen Befehl
2. Alle senden ihre Sicht an alle anderen
3. Schritt 2 wird f-mal wiederholt
4. Jeder Leutnant führt einen **Baum-Mehrheits-Algorithmus** durch

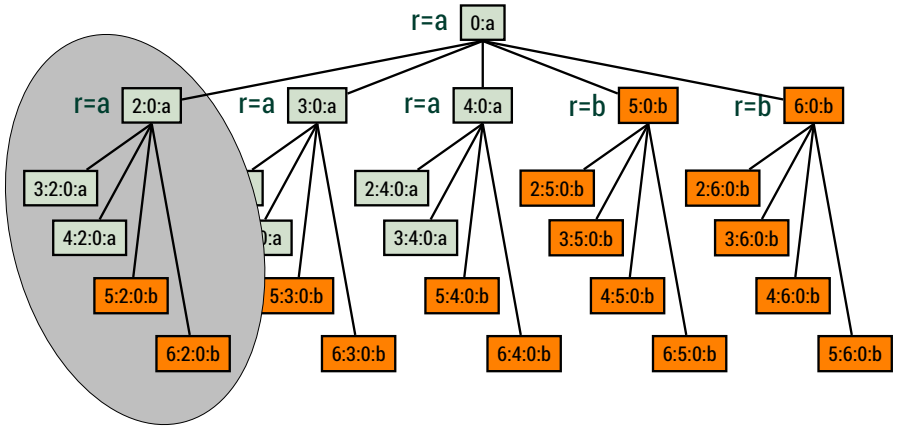
Baum-Mehrheit

Algorithmus

- Jeder Leutnant bildet einen Nachrichtenbaum
- Jede Hierachiestufe ist eine Indirektion der Sicht
- Alle Unterknoten eines Knotens zeigen die (behauptete) Sicht der anderen auf diesen Knoten
- Es wird rekursive die Mehrheit über die Subbäume (Knoten + Unterknoten) gebildet
- Fehlende Nachrichten werden beliebig ersetzt

Beispiel für Baum-Mehrheit, $n = 7$, $f = 2$

Sicht von Leutnant Nr. 1 (0 ist Kommandierender General):
Nachrichtenformat: Prefix gibt an, wessen Sicht es ist.



Gesamter Nachrichtenbaum

Effizienz

- **Minimalität**
  - Bewiesen: ein Byzantinisches Agreement braucht mindestens $3f + 1$ Prozessoren, $f + 1$ Runden und Nachrichten in der Größe von $\mathcal{O}(t^2)$ Bits
  - Bisher noch kein Algorithmus gefunden, bei dem alle Parameter minimal sind
- **Randomisierte Algorithmen**
  - Erlauben Synchronisationsforderungen aufzugeben
  - Keine Garantie, aber Wahrscheinlichkeit eines Agreements geht gegen 1
  - Im Mittel weniger Runden als deterministische Algorithmen

Diskussion

- Obwohl die Annahme Byzantinischer Fehler etwas paranoid wirkt, sind sie in der Realität relevant
  - Uhrensynchronisation ist bei Existenz inkorrekter Uhren **immer** byzantinisch
  - Mehrere Plattformen nutzen Byzantinisches Agreement:
    - SIFT (Software Implemented Fault Tolerance, NASA)
    - TTA
    - BitCoin
    - ...
- Schwächere Annahmen erlauben effizientere Protokolle
  - Authenticated Byzantine fault (oder noch schwächere Fehlermodelle)
  - Keine konsistentes Ergebnis (nur „nahezu“)
  - Keine garantiere Terminierung (probabilistisch)
  - ...

Referenzen

[Pra96] Dhiraj K. Pradhan, Hrsg. *Fault Tolerant Computer Systems*. Prentice Hall, 1996, Section 3.4 und Chapter 8

[Lyn96] Nancy A. Lynch. *Distributed Algorithms*. Morgan Kaufmann, 1996, Chapter 6

[LSP82] Leslie Lamport, Robert Shostak und Marshall Pease. „The Byzantine Generals Problem“. In: *ACM Transactions on Programming Languages and Systems* 4.3 (Juli 1982), S. 382–401

[BDM93] Michael Barborak, Anton Dahbura und Miroslaw Malek. „The consensus problem in fault-tolerant computing“. In: *ACM Computing Survey* 25.2 (Juni 1993), S. 171–220