ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Prof. F. Mattern
Übung Verteilte Systeme
D-INFK
HS 2009

Verteilte Systeme

Theoretische Übungen

Bemerkungen

Diese Übungen dienen zur Vorbereitung auf die schriftliche Prüfung. Sie sind freiwillig und werden nicht korrigiert. Wenn Sie Fragen oder Bemerkungen zu den schriftlichen Übungen haben, wenden Sie sich bitte an einen der verantwortlichen Assistenten.

Matthias Kovatsch (kovatsch@inf.ethz.ch)
Iulia Ion (iion@inf.ethz.ch)

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Prof. F. Mattern
Übung Verteilte Systeme
D-INFK
HS 2009

1 Topologien und Pfadlängen

1. Gegeben sei ein 16×16-Gitter mit 256 Netzknoten. Wie gross ist die maximale Pfadlänge?
2. Wenn die 256 Knoten in einem Hypercube angeordnet werden, wie gross ist dann die maximale Pfadlänge?
3. Aus diesem Hypercube wird nun ein Cube Connected Cycle (CCC) erzeugt, indem wie in der Vorlesung angegeben die Ecken durch Ringe ersetzt werden.
   a) Wieviele Knoten enthält der CCC?
   b) Wie gross ist bei diesem CCC die maximale Pfadlänge?

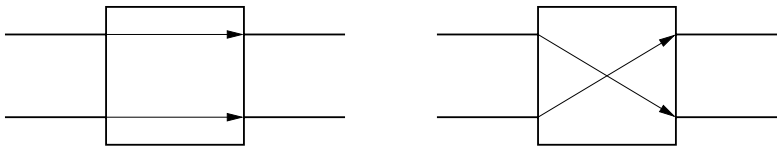
Anmerkung: Die *maximale Pfadlänge* bezeichnet die Länge des längsten Pfades aus der Menge aller kürzesten Pfade (keine Umwege).

2 Pfade im Hypercube

1. Welchen Abstand haben die beiden Knoten $a = (0, 1, 1, 0, 1, 0)$ und $b = (1, 1, 0, 0, 1, 1)$ eines 6-dimensionalen Hypercubes?
2. Wieviele Pfade gibt es zwischen zwei Knoten im Abstand k $(1 \leq k \leq d)$ eines Hypercubes der Dimension d?
3. Wieviele dieser Pfade sind knotendisjunkt (d.h. sie haben keine gemeinsamen Knoten ausser dem Anfangs- und Endknoten)? Beweis?

3 Permutationsnetze

1. In den Vorlesungsunterlagen ist ein Permutationsnetz mit $\log n$ Stufen mit jeweils $n/2$ Schaltern abgebildet (ein Ω-Netz). Die Anzahl der Eingänge (und Ausgänge) ist dabei mit n bezeichnet. Begründen Sie, warum $\log n$ Stufen (mit jeweils $n/2$ Schaltern) notwendig sind, um alle Verbindungen herstellen zu können.
2. Typischerweise gibt es in Permutationsnetzen diese beiden Schaltelemente:



   Lässt sich damit ein Broadcast implementieren? Falls nicht, mit welchen Schaltelementen wäre das möglich?

4 Fehlermodelle

Im Abschnitt "Kommunikation" der Vorlesung werden verschiedene Fehlermodelle beschrieben (fehlerhaftes Senden, Empfangen, Übertragen, Crash, Fail-Stop, Zeitfehler, Byzantinische Fehler).

Durch welche Fehlermodelle werden die folgenden Anwendungsfälle am besten charakterisiert? Geben Sie auch jeweils an, wen oder was Sie unter einer Nachricht und dem Empfänger bzw. Sender einer Nachricht verstehen.

1. Bei der Anfrage an einen Webserver wird ein Dokument (HTML-Seite) nicht gefunden.
2. Die Batterie eines GSM-Telefons ist leer.
3. Auf einem Rechner, der an einem Peer-to-Peer-Netz teilnimmt, hat sich ein spezialisierter Virus eingenistet, der den P2P-Verkehr beobachtet und bestimmte Zugriffe sperrt.
4. Die WLAN-Verbindung eines Laptops ist instabil und bricht immer wieder für kurze Zeit ab.
5. Wegen Überlastung eines Mailservers kommen wichtige E-Mails verspätet beim Empfänger an.
6. Der Spam-Filter eines E-Mail-Clients verschiebt wichtige E-Mails in einen Spam-Ordner, wo sie der Benutzer übersieht.
7. Ein Drucker druckt den Text von Postscript-Dateien aus, statt den Postscript-Code zu interpretieren.

5 Kommunikation

1. Wie kann es bei synchroner Kommunikation zwischen zwei Prozessen zu einem Deadlock kommen?

2. Bei welchem Kommunikationsmechanismus besteht nur eine geringe Gefahr für Deadlocks? Begründen Sie Ihre Antwort.

3. Warum bevorzugen Programmierer trotzdem RPC?

4. Was ist der Unterschied zwischen synchroner, mitteilungsbasierter und synchroner, auftragsorientierter Kommunikation ohne Rückgabewert?

6 RPC

1. Ist es möglich, bei RPC-Aufrufen einen Zeiger als Eingabeparameter zu verwenden ("call by reference")? Als Ausgabeparameter? Begründung!

2. Wenn ein Client zu seiner Anfrage nach einem gewissen Timeout keine Bestätigung erhält, wird er die Anfrage wiederholen. Es könnte aber nur die Bestätigungsnachricht verlorengegangen sein, obwohl der Server die Anfrage bearbeitet hat. Welche Gefahr besteht hierbei und wie könnte man ihr begegnen?

3. Mit welcher RPC-Fehlersemantik-Klasse würden Sie das Verhalten eines Paares Websurfer/Webserver beschreiben, wenn der Websurfer eine GET-Anfrage (Lesen einer Webseite) stellt und, wenn nichts angezeigt wird, den "Reload"-Knopf des Browsers drückt, bis die gewünschte HTML-Seite erscheint?

7 Broadcast

In Abbildung 1 sind zwei Broadcast-Fälle dargestellt.

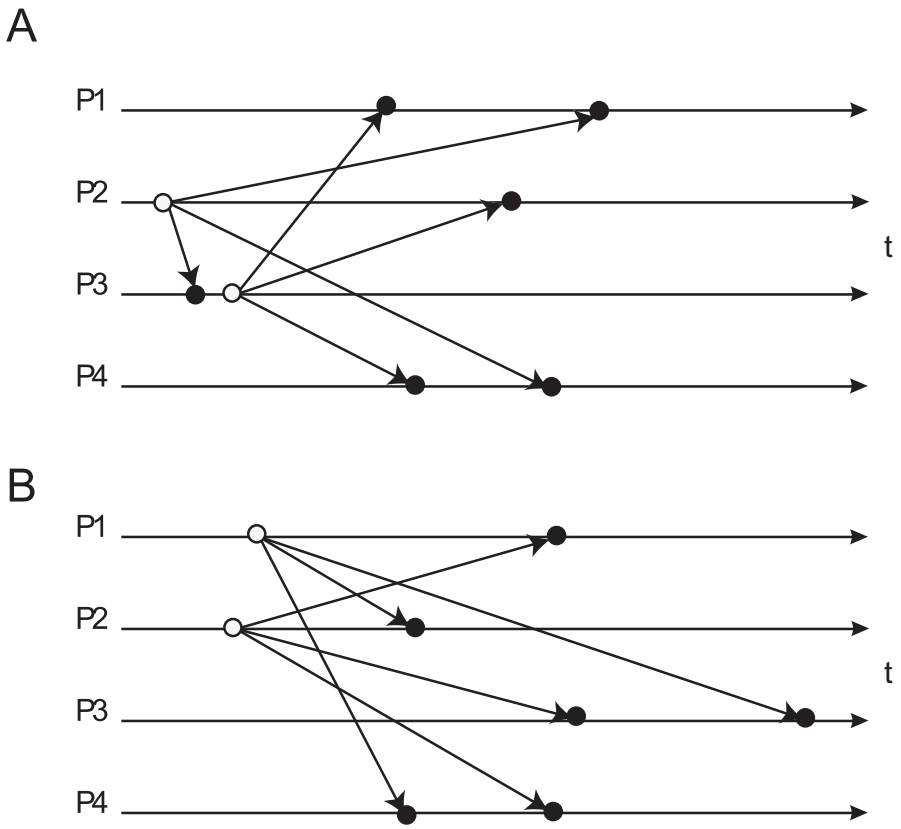


Abbildung 1: Broadcast

1. Welcher der beiden Fälle ist “atomar”?
2. Welchen Vorteil haben atomare Broadcasts gegenüber nicht-atomaren?
3. Besteht eine kausale Abhängigkeit zwischen den Broadcasts von P2 und P3 im Fall A? Zwischen den Broadcasts von P1 und P2 im Fall B?
4. Sind Broadcasts, die über einen zentralen “Sequencer” gesendet werden, notwendigerweise total geordnet? Welche Voraussetzung muss dazu erfüllt sein?

8 Lamport-Zeit

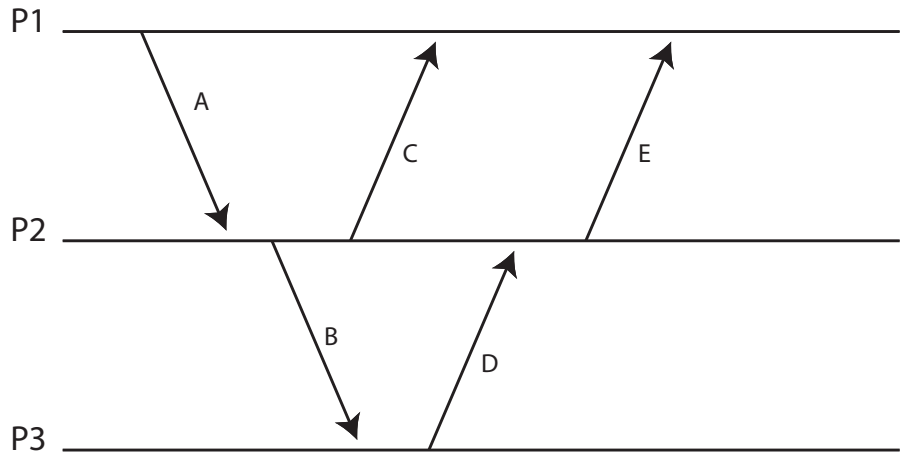


Abbildung 2: Zeitdiagramm

Im folgenden bezeichnet $\prec$ die Kausalrelation auf Ereignissen ("happened before"), C ist die Abbildung von Ereignissen auf Zeitstempel (die durch natürliche Zahlen repräsentiert werden).

1. Geben Sie ein Paar von Ereignissen aus Abb. 2 an, über deren kausale Abhängigkeit keine Aussage getroffen werden kann.

2. Fügen Sie in Abb. 2 eine Nachricht N ein, für die gilt

$$\text{A.receive} \prec \text{N.send} \ \wedge C(\text{N.receive}) < C(\text{E.send})$$

   wobei Sie Absender und Empfänger der Nachricht (die unterschiedlich sein sollen) frei wählen können, sofern die Bedingung erfüllt ist.

3. Fügen Sie auf ähnliche Art eine Nachricht M ein, für die gilt

$$\text{M.send} \prec \text{C.send} \ \wedge C(\text{B.receive}) < C(\text{M.receive})$$

   und die von P1 gesendet und von P2 empfangen wird.

Bemerkung: Die Notation X.send bzw. X.receive bezeichnet das send- bzw. receive-Ereignis der Nachricht X.

9 Lamport-Zeit – Wechselseitiger Ausschluss

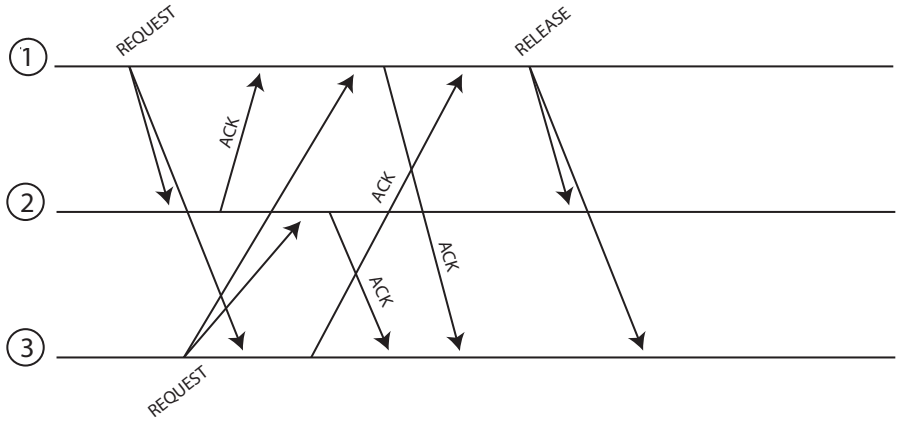


Abbildung 3: Wechselseitiger Ausschluss mit Lamport-Zeit

In Abb. 3 ist ein Zeitdiagramm dargestellt mit Nachrichten von drei Prozessen. Prozesse 1 und 3 bewerben sich um den exklusiven Zugriff auf eine gemeinsame Ressource. Die Prozesse wenden das aus der Vorlesung bekannte Verfahren zum wechselseitigen Ausschluss an, das Lamport-Zeit und verteilte Warteschlangen benutzt.

1. Geben Sie die Sende- und Empfangszeitstempel für jedes Ereignis an.
2. Geben Sie für die Prozesse 1 und 3 an, wie die Warteschlange des jeweiligen Prozesses nach jedem Sende- bzw. Empfangsereignis aussieht.
3. Sind beim Einreihen in die Warteschlange die Sende- oder die Empfangszeitstempel zu verwenden? Warum?
4. Welche Bedingung muss erfüllt sein, damit Prozess 1 auf die Ressource zugreifen kann?
5. Markieren Sie den Zeitpunkt im Zeitdiagramm, zu dem Prozess 1 bzw. Prozess 3 auf die Ressource zugreifen kann.

10 Namen

1. Was versteht man unter dem Binden und dem Auflösen von Namen? Nennen Sie ein Beispiel für einen Dienst, der diese Operationen zur Verfügung stellt.

2. Was ist der Unterschied zwischen iterativer und rekursiver Namensauflösung?

3. Warum bietet es sich an Caching bei der Auflösung von Namen einzusetzen und was wird dadurch erreicht?

4. Nehmen Sie an, die Abbildung von Namen auf Objektadressen wird in einem lokalen Cache eines Clients gespeichert. Ein bereits gebundener und im Cache aufgrund einer früheren Anfrage enthaltener Name wird nun an eine andere Adresse gebunden, das alte Objekt bleibt aber weiterhin aktiv.
   a) Welches Problem tritt nun beim Client auf? Kann der Client dieses Problem erkennen?
   b) Tritt das Problem auch bei solchen Clients auf, die statt der Adresse den zuständigen Nameserver im Cache halten?

5. Zur Erhöhung von Effizienz und Fehlertoleranz werden Nameserver repliziert. Für welche Nameserver ist dies besonders relevant? Begründen Sie Ihre Antwort.

11 Client-/Server

1. Bei Web-basierten Diensten wird oft ein Bezeichner in Links codiert ("URL rewriting"), um die aktuelle Transaktion zu identifizieren. Wie könnte ein Unbefugter eine laufende Transaktion "übernehmen" und was kann man gegen diese Gefahr tun?

2. Welches Problem entsteht bei einem zustandsbehafteten Server, wenn viele Clients abstürzen, bevor sie ihre Transaktionen beendet haben?

3. Erläutern Sie kurz ein paar Vorteile von zustandslosen gegenüber zustandsbehafteten Client/Server-Protokollen und umgekehrt.

12 Middleware

1. Wie werden in CORBA verschiedene Programmiersprachen zur Implementierung der Anwendung unterstützt? Welchen Vorteil hat die Unterstützung mehrerer Sprachen?
2. Welche Funktionen übernimmt ein Stub in CORBA?
3. Was ist der ORB? Wo wird er ausgeführt?
4. Warum wird CORBA heutzutage nicht mehr weiterentwickelt?
5. Was versteht man unter Objekt-Serialisierung? Für was wird sie benötigt? Nennen Sie ebenfalls Beispiele, wie die Serialisierung in Middlewaresystemen realisiert wird?

13 Jini

1. Erläutern Sie kurz die Funktion von Leases.
2. Eine Besonderheit von Jini ist das Ausnutzen der Mobilität von Java-Code. Welche Code-Teile werden übertragen und welche Möglichkeiten ergeben sich dadurch?

14 Sicherheit

1. Auf welche Herausforderungen trifft man bei der Schlüsselverteilung in verteilten Systemen?

2. Beschreiben Sie zwei möglichen Lösungsansätze zur Schlüsselverteilung.

3. In der Vorlesung wurde der Diffie-Hellman-Algorithmus besprochen.
   a) Für was wird er verwendet?
   b) Beschreiben Sie kurz das Verfahren.
   c) Was ist ein möglicher Angriff und wie könnte man sich dagegen verteidigen?

4. Wie funktioniert zertifikatsbasierte Authentifizierung? Von welchem weitverbreiteten System wird sie verwendet?

5. Wenn One-Time-Pads ein perfektes Verschlüsselungssystem darstellen, warum werden diese dann heutzutage nicht global eingesetzt?

6. Mit Einwegfunktionen lassen sich Einmalpasswörter erzeugen und leicht überprüfen. f sei eine Einwegfunktion und x_1 ein initiales Passwort, aus dem eine Passwortkette erzeugt wird:
$$x_1 \rightarrow^f x_2 \rightarrow^f \ldots \rightarrow^f x_{n-1} \rightarrow^f x_n$$
   a) Um die Passwörter zur Authentisierung nutzen zu können, muss x_n zunächst zum Server S übertragen werden. Welche der folgenden Anforderungen müssen erfüllt sein:
      i. Ein Angreifer darf nichts über x_n erfahren, die Übertragung muss also geheimnisbewahrend erfolgen.
      ii. Es muss sichergestellt sein, dass x_n bei der Übertragung nicht verändert wird.
   b) Wir nehmen an, es sei $n = 100$. Dem Server S wird x_{100} bekanntgemacht. Ein Client C schreibt die Werte $x_1, x_2, \ldots, x_{99}$ in eine Liste. Bei der ersten Anmeldung an S verwendet er x_{99} und streicht diesen Wert von der Liste. Beim zweiten Mal verwendet C aus Versehen x_{89} (statt x_{98}). Welche Gefahr besteht, wenn dieser Wert von einem Angreifer abgehört wird und S den Anmeldeversuch einfach ignoriert, weil $f(x_{89}) \neq x_{99}$?

7. Im Kerberos-Protokoll erhält ein Client vom KDC (Key Distribution Center) ein verschlüsseltes TGT (Ticket Granting Ticket). Kann dieses TGT von einem anderen Client verwendet werden, um vom TGS (Ticket Granting Service) ein ST (Service Ticket) anzufordern? Begründung!

8. Nennen Sie zwei Gründe, warum in Kerberos KDC und TGS getrennt sind.