Aufgabe 14: Einigungsprotokolle - Dolev und Burns/Neiger

Literatur:

[1] Singhal, M.; Shivaratri, N. G.
Advanced Concepts in Operating Systems
McGraw-Hill, Inc: New York et al. 1994

[2] Dolev, D.; Fischer, M.J.; Fowler, R.; Lynch, N.; Strong, H.R.:
An Efficient Algorithm for Byzantine Agreement without Authentication
Information and Control, 52 (1982), pp257-274

[3] J.E. Burns, G. Neiger:
Fast and simple Consensus
Distributed Computing Vol. 8, Number 2, Springer International 1994

Oral-Message-Algorithmus nach Dolev

a) Was bedeuten die Mengen LOW und HIGH bezüglich der Lösbarkeit des Einigungsprotokolls?

b) Veranschaulichen Sie, welche Phasen durchlaufen werden, wenn der Initiator die Nachricht “Rückzug” verbreiten will. Unter den 4 Teilnehmern befindet sich 1 Verräter. Skizzieren Sie die Nachrichtenmengen aus Sicht des Knotens 2, Knoten 4 ist defekt.

c) Was kann der Verräter maximal anrichten (welche Nachrichten kann er in Umlauf bringen)?

Oral-Message-Algorithmus nach Burns/Neiger

d) Zeigen Sie, daß bei 5 intakten und einem defekten Knoten sich alle intakten Knoten auf einen Wert einigen - auch wenn die erste Gruppe mit unterschiedlichen Werten beginnt.

Lösungsvorschlag Aufgabe 14: Einigungsprotokolle (Teil 2)

a) Was bedeuten die Mengen HIGH und LOW?

LOW = m + 1
Mindestens ein korrekter Knoten ist in der Menge. Daraus folgt:
Wenn man von LOW-vielen Knoten die gleiche Meinung erhält, hat mindestens ein korrekter Knoten diese Meinung vertreten. Als Folgerung kann man diese Meinung auch unterstützen.

HIGH = 2m + 1
Die Mehrzahl der Knoten in der Menge sind korrekt. Daraus folgt:
Die korrekten Knoten einer solchen Menge können alle fehlerhaften Knoten immer überstimmen. Um sich auf einen Wert festzulegen, muß man also von mindestens HIGH Knoten eine gleiche Meinung erhalten. (Der Algorithmus muß dabei gewährleisten, daß sich diese Meinung auch durchsetzen wird.)

b) Veranschaulichen Sie, welche Phasen durchlaufen werden, wenn der Initiator die Nachricht “Rückzug” verbreiten will. Unter den 4 Teilnehmern befindet sich 1 Verräter.Skizzieren Sie die Nachrichtenmengen aus Sicht des Knotens 2, Knoten 4 ist defekt. (siehe nächste Seite).

c) Was kann der Verräter maximal anrichten (welche Nachrichten kann er in Umlauf bringen)?

Der Verräter kann maximal folgende Nachrichten an alle aussenden:

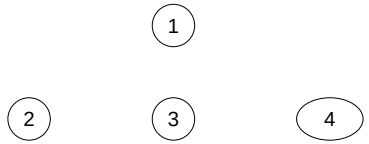
*, 1, 2, 3, 4

Danach sind alle von ihm ausgehenden Nachrichten wirkungslos, da die W-Mengen der jeweiligen Knoten nicht mehr erweitert werden. Da jedoch seine falschen Aussagen von keinen weiteren Knoten bestätigt werden - insbesondere nicht von mindestens LOW-1 vielen, haben seine Nachrichten keinen weiteren Effekt.

Algorithmus **OralMessage nach Dolev**

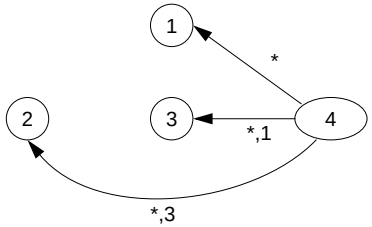
Konstanten: m=1, n=3m+1=4, LOW=m+1=2, HIGH=2m+1=3
Anzahl der Runden: 2m+3 = 5

	1	2	3	4
W*				
W1				
W2				
W3				
W4				



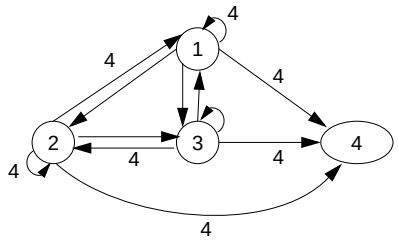
In der ersten Runde verteilt der Knoten 1 keine Nachrichten, da er für den Wert 0 plädiert.

	1	2	3	4
W*	4	4	4	
W1			4	
W2				
W3		4		
W4				



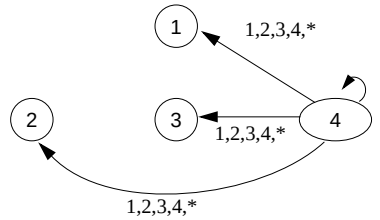
In der zweiten Runde verschickt der fehlerhafte Knoten 3 *-Nachrichten und zwei j-Nachrichten an seine Nachbarn. Diese tragen die Nachrichten in ihren W-Mengen ein. Durch die erhaltenen *-Nachrichten unterstützen alle Knoten in der 3. Runde den Knoten 4 direkt, und schicken j-Nachrichten mit dem Inhalt 4 an alle anderen Knoten:

	1	2	3	4
W*	4	4	4	
W1			4	
W2				
W3		4		
W4	123	123	123	123
C	4	4	4	4



Die 3. Runde bewirkt, daß in den W4-Mengen aller Knoten 1,2,und 3 steht - was bedeutet, daß diese drei Knoten Zeugen dafür sind, daß Knoten 4 eine Stern-Nachricht geschickt hat. Dies bedeutet wiederum, daß die Knoten 1,2 und 3 davon überzeugt sind (W4 >= HIGH), daß 4 eine *-Nachricht geschickt hat, und nehmen Knoten 4 in ihre C-Menge auf. Nachdem bei jedem Knoten dadurch auch W4 >= LOW ist, unterstützt desweiteren jeder Knoten 4 indirekt. Da die Knoten jedoch bereits Nachrichten durch die direkte Unterstützung geschickt haben, schicken sie keine weiteren Nachrichten.

	1	2	3	4
W*	4	4	4	4
W1	4	4	4	4
W2	4	4	4	4
W3	4	4	4	4
W4	1234	1234	1234	1234
C	4	4	4	4

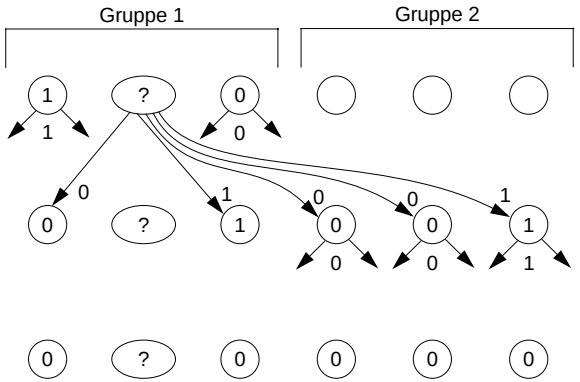


Dafür schickt Knoten 4 in Runde 4 an alle Knoten alle möglichen Nachrichtentypen: *,1,2,3,4. Dies bewirkt, daß jeder Knoten den Knoten 4 in jeder W-Menge aufnimmt. Da jedoch dadurch keine der Mengen eine Kardinalität von mindestens LOW aufweisen kann, haben diese Nachrichten keinen weiteren Effekt.

In Runde 5 terminiert der Algorithmus. Da in den C-Mengen der Knoten lediglich Knoten 4 existiert (und damit nicht mindestens HIGH Knoten), ist keiner der Knoten überzeugt - und alle einigen sich darauf, daß der Anführer den Wert 0 vorgab.

d) Oral-Message-Algorithmus nach Burns/Neiger

Zeigen Sie, daß bei 5 intakten und einem defekten Knoten sich alle intakten Knoten auf einen Wert einigen - auch wenn die erste Gruppe mit unterschiedlichen Werten beginnt.



Alle Knoten starten mit eigenen Anfangswerten. Diese könnten z.B. durch einen Initiator am Anfang (vor Runde 1) verteilt worden sein. Die Abbildung zeigt dann den Fall, daß dieser Initiator und ein weiterer Knoten defekt sind. Da in Runde 1 noch keine vollständige Einigung erzielt wird - es kommt nicht von allen Knoten aus Gruppe 1 der gleiche Vorschlag - muß eine weitere Runde durchgeführt werden. In Runde 2 kommt zwar auch nicht von allen Knoten der gleiche Wert, jedoch einigen sich alle Knoten auf die Mehrheit (in diesem Fall 0), da es die letzte mögliche Runde des Algorithmus ist. (m=1 daher kann es maximal 2 Runden geben.)

