

Contents

1	Introduction	1
1.1	Motivation	1
1.2	Objectives	5
1.3	Outline	5
1.4	Remarks on Notation	8
2	Modelling Fault-Tolerant Distributed Systems	9
2.1	Interprocess Communication	10
2.2	States, Traces, Properties	12
2.3	Temporal Logic of Actions	19
2.4	Fault Model	25
2.5	Fault Tolerance	29
2.6	Timing Model	31
2.7	Summary	37
3	Modelling Fault Assumptions with Structural Failure Models	39
3.1	Related Work	40
3.2	Functional Failure Models	42
3.3	Structural Failure Models	47
3.4	Component Failure Models	50
3.5	Set-Based Structural Failure Models	60
3.6	Sequence-Based Structural Failure Models	89
3.7	Stochastics, Sets, and Sequences	92
3.8	Summary	94
4	Constructing Coteries	97
4.1	Related Work	99
4.2	Introduction to Quorums	101
4.3	Highly Available Static Coteries	109
4.4	Highly Available Dynamic Coteries	118
4.5	Reducing Probe Complexity	126
4.6	Summary	137

5	Reaching Consensus	139
5.1	Related Work	141
5.2	Introduction to Consensus	143
5.3	Consensus in Asynchronous Systems with Unreliable Failure Detectors	154
5.4	Consensus in Partially Synchronous Systems	169
5.5	Consensus in Synchronous Systems	174
5.6	Summary	186
6	Conclusion and Future Work	189
	Bibliography	195
	Index	213