Simultaneous Byzantine Agreement

Suppose there are $n$ generals, $t$ of them are traitors, the rest are loyal. But initially, nobody knows who the traitors are. There are no broadcast actions, only message passing. Every general has a preference about whether to attack.

Can we design a protocol so that

1. At some point, all the loyal generals either attack, or they all retreat.
2. If all the generals prefer to attack, then the agreement is to attack.

Even though the traitors may misbehave (e.g., tell one general they want to attack, and another that they want to retreat.)

Motivation: fault-tolerant protocols
Slide 5

Notation:

\(deciding_i(y)\) for \(\neg decided_i(y) \land \Box decided_i(y)\)

At a point \((r, m)\), let \(N(r, m)\) be the set of nonfaulty agents (for which the environment has not yet performed \(fail_i\)).

\((I, r, m) \vDash deciding_N(y)\) if \((I, r, m) \vDash deciding_i(y)\) for all \(i \in N(r, m)\)

Slide 6

Specification for SBA

A system \(I\) satisfies the SBA specification if for every run \(r\):

1. **Decision**: Every process that is nonfaulty in \(r\) performs exactly one \(decide_i(y)\) action in \(r\).

2. **Agreement**: If \(i\) is nonfaulty at \((r, m)\) and is about to decide \(y\) at \((r, m)\) and \(j\) is nonfaulty at \((r, m')\) and is about to decide \(y'\) at \((r, m)\) then \(y = y'\).

3. **Validity**: If all the processes have the same initial preference \(x\) then all the nonfaulty processes decide \(x\).

4. **Simultaneity**: the nonfaulty processes decide simultaneously, i.e., if \(i\) and \(j\) are nonfaulty at \((r, m)\) and \(i\) is about to decide at \((r, m)\), then so is \(j\).

Slide 7

Failure Modes

The following are possible failure modes:

1. **Crash Failures**: A faulty process follows its protocol up to the time when it fails (sending a subset of messages) after which it sends no messages.

2. **Omission Failures**: A faulty process follows its protocol, but in any round the set of messages it sends or receives is a subset of what it should be.

3. **Byzantine Failures**: Faulty processes may deviate from the protocol in any way: send a subset of messages, send false messages, collude with other faulty processes to deceive the non-faulty processes, etc.

Slide 8

Knowledge of preferences is not enough (\(n=3, t=1\))

\[
\begin{array}{c|c|c|c}
\hline
\text{1} & \text{2} & \text{3} \\
\hline
x_1 & 0 & 0 & 0 \\
\hline
x_2 & 0 & 0 & 0 \\
\hline
x_3 & 0 & 0 & 0 \\
\hline
\end{array}
\quad
\begin{array}{c|c|c|c}
\hline
\text{1} & \text{2} & \text{3} \\
\hline
x_1 & 0 & X & 0 \\
\hline
x_2 & 0 & X & \ast \\
\hline
x_3 & 0 & X & 0 \\
\hline
\end{array}
\quad
\begin{array}{c|c|c|c}
\hline
\text{1} & \text{2} & \text{3} \\
\hline
x_1 & 0 & X & 0 \\
\hline
x_2 & 1 & X & \ast \\
\hline
x_3 & 0 & X & 0 \\
\hline
\end{array}
\]

\[
\begin{array}{c|c|c|c}
\hline
\text{1} & \text{2} & \text{3} \\
\hline
\sim_1 x_1 & 0 & 0 & 0 \\
\hline
\sim_2 x_2 & 1 & 1 & 1 \\
\hline
\sim_3 x_3 & 0 & 0 & 0 \\
\hline
\sim_{\{1,2,3\}} x_1 & 1 & 1 & 1 \\
\hline
\sim_{\{1,2,3\}} x_2 & 1 & 1 & 1 \\
\hline
\sim_{\{1,2,3\}} x_3 & 1 & 1 & 1 \\
\hline
\end{array}
\]
Non-rigid sets of agents

We have defined common knowledge $C_G \phi$, and distributed knowledge $D_G \phi$ with respect to a fixed set $G$ of agents.

In SBA, we need to consider sets of agents that depend on the point.
In particular $\mathcal{N}(r,m)$, the set of agents that have not failed at point $(r,m)$.

An attempt to define non-rigid group knowledge

Let $S : \text{Points}(I) \rightarrow \text{Agents}$ be a non-rigid set of agents.

$E_S \phi = \bigwedge_{i \in S} K_i \phi$

$C_S \phi = E_S \phi \land E_S E_S \phi \land \ldots$

Problem: In general, we can have $(I,r,m) \models i \in S \land \neg K_i(i \in S)$

A definition that works better

Define

$B^S_i \phi$ as $K_i(i \in S \Rightarrow \phi)$

$E_S \phi$ as $\bigwedge_{i \in S} B^S_i \phi$

$C_S \phi = E_S \phi \land E_S E_S \phi \land \ldots$

$(I,r,m) \models D_S \phi$ if $(I,r,m) \models D_G(G \subseteq S \Rightarrow \phi)$ for $G = S(r,m)$

Remark: these definitions make the following valid:

$i \in S \Rightarrow B^S_i(C_S(i \in S))$

Relating $C_S$ to reachability

Define $(r',m')$ to be $S$-reachable from $(r,m)$ if there exists a sequence of points $(r_0,m_0) \ldots (r_k,m_k)$ such that

1. $(r,m) = (r_0,m_0)$ and $(r',m') = (r_k,m_k)$ and

2. for all $l = 0 \ldots k - 1$, there exists $i \in S(r_l,m_l) \cap S(r_{l+1},m_{l+1})$
   such that $(r_l,m_l) \sim_i (r_{l+1},m_{l+1})$

Lemma: $(I,r,m) \models C_S \phi$ iff $(I,r',m') \models \phi$ for all $(r',m')$ that are $S$-reachable from $(r,m)$. 
A Property of Byzantine Agreement Solutions

**Theorem:** Let \((\gamma, \pi)\) be a ba-compatible interpreted context and let \(P\) be a deterministic protocol. If \(I = I^{rep}(P, \gamma, \pi)\) satisfies the SBA specification, then

\[ I \models deciding_N(y) \Rightarrow B^N_i(C_N(\exists y)) \]

**Corollary:** Let \((\gamma, \pi)\) be a ba-compatible interpreted context and let \(P\) be a deterministic protocol. If \(I = I^{rep}(P, \gamma, \pi)\) satisfies the SBA specification, then

\[ I \models deciding_N(y) \Rightarrow B^N_i(C_N(\exists y)) \]

Assumptions on the faulty processes

Let
1. \(n\) be the number of processes
2. \(t\) be the maximum number of faulty processes in any run \((t \leq n)\)
3. \(\gamma^{cr}\) be the ba-context for crash failures (only)
4. \(\gamma^{som}\) be the ba-context for sending omission failures
5. \(\gamma^{gom}\) be the ba-context for general (send and receive) omission failures
6. \(\Gamma^{SBA} = \{\gamma^{cr}, \gamma^{som}, \gamma^{gom}\}\)

Solvability with up to \(t\) failures

**Theorem:** There are deterministic protocols that attain SBA in \(t + 1\) rounds in each of the contexts in \(\Gamma^{SBA}\).

**Theorem:** If \(P\) is a deterministic protocol that satisfies the SBA specification in a context \(\gamma \in \Gamma^{SBA}\), \(r\) is a failure free run in \(R^{rep}(P, \gamma)\) and \(P\) attains SBA in \(t'\) rounds in run \(r\), then \(t' \geq t + 1\).
Comparing the rate at which different protocols reach agreement

Let $P$ and $P'$ be two protocols for a context $\gamma \in \Gamma^{SBA}$.
Say that runs $r \in \mathcal{R}^{rep}(P, \gamma)$ and $r' \in \mathcal{R}^{rep}(P', \gamma)$ are corresponding if
1. $r(0) = r'(0)$
2. for all rounds $m$, the environment performs the same actions
   (e.g. fail a process, block delivery/transmission of a message) in round $m$ of $r$ as in round $m$ of $r'$.

$P$ dominates $P'$ if for every run $r \in \mathcal{R}^{rep}(P, \gamma)$ and corresponding run $r' \in \mathcal{R}^{rep}(P', \gamma)$, if the nonfaulty processes decide in round $m$ of $r$ then the nonfaulty processes decide in round $m$ or later in $r'$.

$P$ strictly dominates $P'$ if $P$ dominates $P'$ and there exists a run of $P$ where the nonfaulty processes decide strictly earlier than in the corresponding run of $P'$.

$P$ is optimal for SBA in context $\gamma$ if it is not strictly dominated by any other protocol for SBA in this context.

$P$ is optimum for SBA in context $\gamma$ if it dominates all protocols for SBA in this context.

The full-information protocol

The full-information protocol $FIP$ is the joint protocol $(FIP_1, \ldots, FIP_n)$ defined by the following rule:

In round $m$, $FIP_i$ sends a message containing all of agent $i$'s local state to all other agents.

Basic formulas

Say that a formula $\phi$ is determined by the initial state in a system $I$ if for every point $(r, m)$ of $I$, we have $(I, r, m) \models \phi$ iff $(I, r, 0) \models \phi$.

A formula is basic if it is of the form $K_i \psi, D_N \psi, C_N \psi$ or $B_N^{i} \psi$ where $\psi$ is determined by the initial state.
FIP is an optimum protocol

Theorem: Assume that $\gamma \in \Gamma^{SBA}$ and that $\phi$ is a basic formula. Also assume that $P$ is a deterministic protocol, $I = I^{rep}(P, \gamma, \pi^{sba})$ and $I^{FIP} = I^{rep}(FIP, \gamma, \pi^{sba})$. Let $r \in R^{rep}(P, \gamma)$ and corresponding run $r^{FIP} \in R^{rep}(FIP, \gamma)$ be corresponding runs. Then for all $m \geq 0$, if $(I, r, m) \models \phi$ then $(I^{FIP}, r^{FIP}, m) \models \phi$.

Corollary: If $\gamma \in \Gamma^{SBA}$ and $I^{FIP} = I^{rep}(FIP, \gamma, \pi^{sba})$ then for all runs $r$ of $I^{FIP}$, there is a time $m \leq t + 1$ such that $(I^{FIP}, r, m) \models C_N(\exists 0) \lor C_N(\exists 1)$.

Clean Rounds
Consider $\gamma^{cr}$ (Crash failures) and the full information protocol $FIP$.

When does initial information become common knowledge?
Define the proposition $faulty(i)$, for $i$ an agent, to hold at $(r, m)$ if $i$ has failed in some round $m' \leq m$ in $r$.

Say that round $m$ is clean if for every process $i$, if $(I, r, m) \models D_N(faulty(i))$ then $(I, r, m - 1) \models D_N(faulty(i))$.
(i.e., no new faults discovered by nonfaulty processes)
Define proposition clean to hold at $(r, m)$ if some round $m' \leq m$ is clean.

let $I^{cr} = I(FIP, \gamma^{cr}, \pi^{sba})$

Theorem: If $\phi$ is determined by the initial state, then $I(FIP, \gamma^{cr}, \pi^{sba}) \models C_N(\当事人\exists 0) \land D_N\phi \Rightarrow C_N\phi$.

If there are at most $t$ failures then one of the first $t + 1$ rounds of every run must be clean, and at all points $D_N(\exists 0)$ or $D_N(\exists 1)$, so

Corollary: Let $r$ be a run of $I^{cr}$. Then $(I^{cr}, r, t + 1) \models C_N(\exists 0) \lor C_N(\exists 1)$.
So the condition for making a decision is always attained by time $t + 1$. 
Exact timing of decision point

Let

$\text{#Failed}$ be the number of processes that have failed

$\text{KnownFailed}(r, m) = \max\{k \mid (I^{cr}, r, m) \models D_N(\text{#Failed} \geq k)\}$

$\text{diff}(r, m) = \#\text{KnownFailed}(r, m) - m$

$\mathcal{W}(r) = \max_{m \geq 0} \text{diff}(r, m)$

Then

**Theorem:** Let $r$ be a run of $I^{cr}$ and let $T = \min(t, n - 2)$. If $\phi$ is determined by the initial state, then

$(I^{cr}, r, T + 1 - \mathcal{W}(r)) \models D_N(\phi) \Rightarrow C_N(\phi)$. 

**Theorem:** Let $r$ be a run of $I^{cr}$ and let $T = \min(t, n - 2)$. If $\phi$ is determined by the initial state, and $m < T + 1 - \mathcal{W}(r)$, then

$(I^{cr}, r, m) \models D_N(\phi) \Rightarrow C_N(\phi)$ if $(I^{cr}, r, 0) \models D_N(\phi) \Rightarrow C_N(\phi)$.

Since $\exists 0/\exists 1$ are not initially common knowledge, whichever is true in $r$ becomes common knowledge to nonfaulty processes in $r$ after $k$ rounds if the waste is $t + 1 - k$.

---

Optimizing the Full-Information Protocol

The full-information protocol is wasteful in the amount of information it sends.

Suppose initial states consist of one bit and all messages are delivered. Then the size $\text{size}(k)$ of local states of the agents after round $k$ is defined by

$s(0) = 1$

$s(k + 1) = s(k) + (n - 1) \cdot s(k - 1)$

So $s(k) \leq (n - 1)^{k-1}$.

Local states grow exponentially in size.

We can represent a run of the full-information protocol up to a point $(r, m)$ by a labelled graph $G(r, m)$:

1. vertices are pairs $(i, k)$ with $i$ an agent and $0 \leq k \leq m$
2. $(i, 0)$ is labelled with agent $i$’s initial state
3. there is an edge from $(i, k)$ to $(j, k + 1)$ labelled $+$ if the message from $i$ to $j$ in round $k + 1$ was delivered
4. there is an edge from $(i, k)$ to $(j, k + 1)$ labelled $-$ if the message from $i$ to $j$ in round $k + 1$ was delivered
We can represent agent \( i \)'s state of information at \((r, m)\) as a subgraph \( G(r_i(m)) \) of \( G(r, m) \) in which

1. some edges are missing (if \( i \) does not know whether a message was delivered)
2. some initial states are

\( G(r, m) \) has size \( O(mn^2) \), so for the first \( n \) rounds, size \( O(n^3) \).

Let \( FIP' \) be the protocol in which, instead of sending its complete local state, agent \( i \) sends \( G(r_i(m)) \).

Then the first \( n \) rounds, the local states of \( i \) have size \( O(n \cdot n \cdot n^3) = O(n^5) \).

\textbf{Theorem:} Assume that \( \gamma \in \Gamma^{sba} \), and let \( \phi \) be a basic formula. Let \( r \) and \( r' \) be corresponding runs of \( I = I^{rep}(FIP, \gamma, \pi^{sba}) \) and \( I' = I'^{rep}(FIP', \gamma, \pi^{sba}) \), respectively. Then \( (I, r, m) \models \phi \) iff \( (I', r', m) \models \phi \).

\textbf{Theorem:} There is an algorithm that, given input \( r_i(m) \), with \( m < n \), decides in time polynomial in \( n \) whether 

\( (I^{rep}(FIP', \gamma, \pi^{sba}), r, m) \models B_i C_N(\exists y) \), when \( \gamma \) is the ba-context for either crash-failures or sending omission failures.

For General Omission failures, the problem is NP-hard (hence not in polynomial time).

\textbf{An efficient knowledge-based program for SBA}

\textbf{SBA=}

\textbf{Case of}

\begin{verbatim}
if \neg decided_i \land B_i^N C_N(\exists 0)  do decide_i(0);
if \neg decided_i \land \neg B_i^N C_N(\exists 0) \land B_i^N C_N(\exists 1)  do decide_i(1);
if \neg decided_i \land B_i^N C_N(\exists 0) \land \neg B_i^N C_N(\exists 1)
do send_i(G(local state))
end case
\end{verbatim}
This ensures satisfaction of SBA...

**Theorem:** If $(\gamma, \pi)$ is a ba-compatible interpreted context, $\mathcal{I}$ is consistent with the knowledge-based program SBA in $(\gamma, \pi)$, and $CN(\exists 0) \lor CN(\exists 1)$ is attained in every run of $\mathcal{I}$, then $\mathcal{I}$ satisfies the SBA specification. Moreover, the processes decide in a run $r$ if $\mathcal{I}$ at the round following the first time that $CN(\exists 0) \lor CN(\exists 1)$ is attained.

**Theorem:** for $\gamma \in \Gamma^\text{sba}$, there is a unique interpreted system representing SBA in $(\gamma, \pi^\text{sba})$. Moreover, the corresponding protocol is an optimum protocol for SBA in $\gamma$.

**Corollary:** There are polynomial time optimum protocols for SBA in the crash failure and sending omission failure contexts.

(If $P \neq NP$ then no polynomial-time protocol can be optimum for SBA in the general omission failure model.)