Back to the Coordinated Attack Problem

The Power of Topology Tools

E. Godard E. Perdereau

LIS – AMU

Journées ANR Descartes 09/10
A Kind of Folklore Problem (Gray 78)

Two generals have gathered forces on top of two facing hills. In between, in the valley, their common enemy is entrenched. This enemy can only be defeated if both armies attack. Every day each general sends a messenger to the other through the valley. However this is risky as the enemy may capture them. Now they need to get the last piece of information: are they both ready to attack?

It is also stated as the *Two Generals Problem*. 
This is the **Consensus Problem** for **two** processes that communicate by **synchronous message-passing** with possible **omission faults**.

**The Consensus Problem**

Each process is given an initial value. Each process has to decide a value such that

- **Agreement** At most 1 value can be decided,
- **Validity** The decided value is included in the set of initial values,
- **Termination** Any *non-faulty* process eventually decides.
A Key Impossibility Result

one of the first distributed computability result

J. Gray prove it was a problem impossible to solve deterministically. The proof is basically that, if the two generals want to communicate, they will be in an infinite sequence of mutual acknowledgements...
An Interesting Case?

- Consensus is a well known problem
- Simple (minimal!) instance
- Faults, but benign ones

Maybe too simple and obvious?...
History

Our Result

A Topological Technique

An Interesting Case?

- Consensus is a well known problem
- Simple (minimal!) instance
- Faults, but benign ones

Maybe too simple and obvious?... Actually, yes!!
Because it is possible to lose every message, it is obvious the task is impossible.
In [Gray78], such a dramatic scenario is not explicitly ruled out...

In textbooks:

- Santoro’s *Design and Analysis of Distributed Algorithms*: the zero-message scenario is explicitly excluded.
- Lynch’s *Distributed Algorithms*: the problem statement is weakened such that it is not obviously impossible.

**Interesting Question**

What are the impossible cases?
Describing Scenarios: Message Adversaries

Let $\Sigma = \{\circ \leftrightarrow \bullet, \circ \leftarrow \bullet, \circ \rightarrow \bullet, \circ \rightarrow \circ\}$, and $\Gamma = \{\circ \leftrightarrow \bullet, \circ \leftarrow \bullet, \circ \rightarrow \bullet\}$. The interpretation is that:

- $\circ \leftrightarrow \bullet$, no process loses messages
- $\circ \leftarrow \bullet$, the message of process $\circ$ is not transmitted
- $\circ \rightarrow \bullet$, the message of process $\bullet$ is not transmitted
- $\circ \rightarrow \circ$, both messages are not transmitted.

**Definition**

A *message adversary* is a set of infinite sequences of elements of $\Sigma$. 

Emmanuel Godard (LIS – AMU)
With the infinite word notation

- at each round, up to 2 messages can be lost: $\Sigma^\omega$.
- at each round, only one message can be lost: $\Gamma^\omega$.
- at most one of the processes can lose messages: $S_1 = \{\circ\leftrightarrow\bullet, \circ\leftarrow\bullet\}^\omega \cup \{\circ\leftrightarrow\bullet, \circ\rightarrow\bullet\}^\omega$.
- at most one of the processes can crash:
  $C_1 = \{\circ\leftrightarrow\bullet\}^\omega \cup \{\circ\leftrightarrow\bullet\}^* (\{\circ\rightarrow\bullet\}^\omega + \{\circ\rightarrow\bullet\}^\omega)$.
- The communication system is fair:
  $Fair = \Sigma^\omega \setminus \Sigma^* (\{\bullet\rightarrow\circ, \bullet\leftarrow\circ\}^\omega \cup \{\bullet\rightarrow\circ, \circ\rightarrow\bullet\}^\omega)$. 

Emmanuel Godard (LIS – AMU)
Finally and classically,

**Definition**

A algorithm $\mathcal{A}$ solves the Coordinated Attacked Problem for the message adversary $L$ if for any condition $w \in L$, there exists $u \in \text{Pref}(w)$ such that the states of the two processes $(s^\circ(u)$ and $s^\bullet(u))$ satisfy the three conditions of Consensus.

**Definition**

A message adversary $L$ is said to be *solvable* if there exists an algorithm that solves the Coordinated Attacked Problem for $L$. It is said to be an *obstruction* otherwise.
Obstructions

Restating the Initial Problem

What are the obstructions for the Coordinated Attack Problem?
Which are minimal?
Minimal obstruction

- $\Gamma^\omega$ is an obstruction set.
- (almost) all subset of $\Gamma^\omega$ are not solvable.

- 2011: purely combinatorial proof
- this talk: topological proof
Index of a Scenario

\[ \delta(\circ \rightarrow \bullet) = -1, \]
\[ \delta(\circ \leftrightarrow \bullet) = 0, \]
\[ \delta(\circ \leftarrow \bullet) = 1. \]

Definition

Let \( w \in \Gamma^* \). We define \( \text{ind}(\varepsilon) = 0 \). If \( |w| \geq 1 \), then we have \( w = ua \) where \( u \in \Gamma^* \) and \( a \in \Gamma \). In this case, we define

\[ \text{ind}(w) := 3\text{ind}(u) + (-1)^{\text{ind}(u)} \delta(a) + 1. \]
## Examples

<table>
<thead>
<tr>
<th>word of length &quot;1&quot;</th>
<th>0 → •</th>
<th>0 ↔ •</th>
<th>0 ← •</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>
Examples

<table>
<thead>
<tr>
<th>Word of length &quot;1&quot;</th>
<th>( \circ \to \bullet )</th>
<th>( \circ \leftrightarrow \bullet )</th>
<th>( \circ \leftrightarrow \bullet )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Word of length &quot;2&quot;</th>
<th>( \circ \to \bullet \circ \to \bullet )</th>
<th>( \circ \to \bullet \circ \leftrightarrow \bullet )</th>
<th>( \circ \to \bullet \circ \leftarrow \bullet )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Word of length &quot;2&quot;</th>
<th>( \circ \leftrightarrow \bullet \circ \to \bullet )</th>
<th>( \circ \leftrightarrow \bullet \circ \leftrightarrow \bullet )</th>
<th>( \circ \leftrightarrow \bullet \circ \leftarrow \bullet )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>5</td>
<td>4</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Word of length &quot;2&quot;</th>
<th>( \circ \leftrightarrow \bullet \circ \to \bullet )</th>
<th>( \circ \leftrightarrow \bullet \circ \leftrightarrow \bullet )</th>
<th>( \circ \leftrightarrow \bullet \circ \leftarrow \bullet )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>
Distributed Computability

**Theorem (Fevat, G. 2011)**

Let $L \subset \Gamma^\omega$, then Consensus is solvable for message adversary $L$ if and only if one of the following holds

- $\exists f \in \text{Fair}, f \notin L$,
- $\exists (u, u') \in \text{SPair}, u, u' \notin L$,
- $\circ \rightarrow \omega \notin L$,
- $\circ \leftarrow \omega \notin L$.

where we define *special pairs* to be

$$\text{SPair} = \{(w, w') \in \Gamma^\omega \times \Gamma^\omega \mid w \neq w', \forall r \in \mathbb{N} | \text{ind}(w|_r) - \text{ind}(w'|_r)| \leq 1\}.$$
Classical Proof Technique

Necessary Condition
It is a classical proof by \textit{bivalency}.

Sufficient Condition
A new index-based Consensus Algorithm.
A Consensus Algorithm $A_w$

\begin{algorithmic}
  \State $r=0$; $\text{initother}=\text{null}$;
  \If{ "$\bigcirc = \bigcirc$" } \State $\text{ind}=0$; \EndIf
  \Else \State $\text{ind}=1$; \EndElse
  \While{ "$|\text{ind} - \text{ind}(w|r)| \leq 1$" } \Do
    \State $\text{msg} = (\text{init},\text{ind})$;
    \State $\text{send}(\text{msg})$; $\text{msg} = \text{receive()}$;
    \If{ $\text{msg} == \text{null}$ } \Then \State "$\text{ind} = 3 \times \text{ind}$"; \EndIf
    \Else \State "$\text{ind} = 2 \times \text{msg}.\text{ind} + \text{ind}$"; \EndElse
    \State $\text{initother} = \text{msg}.\text{init}$;
    \State $r=r+1$;
  \EndDo
\end{algorithmic}
A Consensus Algorithm $A_w$ (cont.)

```plaintext
if "⊙ = o" then
  if "ind ≤ ind(w|r)" then
    Output: init
  else
    Output: initother
else
  if "ind ≥ ind(w|r)" then
    Output: init
  else
    Output: initother
```
Fundamental Invariant

**Proposition**

For any round $r$ of an execution of Algorithm $A_w$ under scenario $v \in \Gamma^r$, such that no process has already halted,

$$\begin{cases} |\text{ind}_r^\bullet - \text{ind}_r^\circ| = 1, \\ \text{sign}(\text{ind}_r^\bullet - \text{ind}_r^\circ) = (-1)^{\text{ind}(v)}, \\ \text{ind}(v) = \min\{\text{ind}_r^\circ, \text{ind}_r^\bullet\}. \end{cases}$$
Simplicial Complexes

The real ones

Definition

\[ \sigma = \{ v_0, \ldots, v_n \} \subset \mathbb{R}^N \] is a simplex of dimension \( n \) if the vector space generated by \( \{ v_1 - v_0, \ldots, v_n - v_0 \} \) is of dimension \( n \).

Definition

A simplicial complex is a collection \( C \) of simplices

- If \( \sigma \in C \) and \( \sigma' \subseteq \sigma \), then \( \sigma' \in C \),
- If \( \sigma, \tau \in C \) and \( |\sigma| \cap |\tau| \neq \emptyset \) then there exists \( \sigma' \in C \) such that \( |\sigma| \cap |\tau| = |\sigma'| \).

Abstract simplicial complexes are an equivalent presentation when the collection is finite.
|\sigma| \text{ is the convex hull of } \sigma.

It is the geometric realization of \sigma.
Given a set $P$, a chromatic simplex is $(\sigma, c)$ where $c : \sigma \rightarrow P$ is injective.
Encoding the Global State of a Distributed System

\( P \) is the set of processes (here \( P = (\circ, \bullet) \)), \( \text{state}^{\circ} \) is the state of \( \circ \).

- \( (\circ, \text{state}^{\circ}) \Rightarrow \text{local state} \) of \( \circ \)
- the simplex \( \{(\circ, \text{state}^{\circ}), (\bullet, \text{state}^{\bullet})\} \Rightarrow \text{global state} \)
Encoding the Binary Consensus Problem

In_{2gen}

Out_{2gen}
Encoding the Binary Consensus Problem

In\text{2gen} \quad \Delta\text{2gen} \quad \text{Out}\text{2gen}
Chromatic Subdivision

It is a complex operator \( \text{Chr} \) such that

\[
\begin{align*}
0 & \quad \frac{1}{3} & \quad \frac{2}{3} & \quad 1 \\
0 & \quad \frac{1}{9} & \quad \frac{2}{9} & \quad 1 \\
0 & \quad \frac{1}{27} & \quad \frac{2}{27} & \quad \frac{23}{27} & \quad \frac{24}{27} & \quad 1
\end{align*}
\]
Chromatic Subdivision

It is a complex operator \( \text{Chr} \) such that

\[
\begin{array}{c}
0 \quad 0 \quad 0 \\
\frac{1}{3} \quad \frac{2}{3} \\
\frac{1}{9} \quad \frac{2}{9} \\
\frac{1}{27} \quad \frac{2}{27} \\
\end{array}
\]

\[
\begin{array}{c}
\sigma \\
\text{Chr} \sigma \\
\text{Chr}^2 \sigma \\
\text{Chr}^3 \sigma \\
\end{array}
\]

Encoding Partial Executions

Let \( w \in \Gamma^* \), the simplex \( \left\{ \frac{\text{ind}(w)}{3\|w\|}, \frac{\text{ind}(w)+1}{3\|w\|} \right\} \) is associated to \( w \).

\[
\left[ \frac{23}{27}, \frac{8}{9} \right] \Rightarrow \text{corresponds to } \quad \circ \leftarrow \bullet \circ \leftarrow \bullet \circ \rightarrow \bullet .
\]
Iterated Protocol Complex

$PC^L(r)$ is the protocol complex for $L$ at round $r$.

Uncertainty appears as adjacent simplices.
Encoding Full Executions

- $\forall n \in \mathbb{N}, \forall w \in \Gamma^n \quad ind_n(w) = \frac{ind(w)}{3^n}$
- $\forall w \in \Gamma^\omega \quad \overline{ind}(w) = \lim_{n \to +\infty} ind_n(w|_{n})$
Encoding Full Executions

- \( \forall n \in \mathbb{N}, \forall w \in \Gamma^n \), \( \text{ind}_n(w) = \frac{\text{ind}(w)}{3^n} \)

- \( \forall w \in \Gamma^\omega \), \( \overline{\text{ind}}(w) = \lim_{n \to +\infty} \text{ind}_n(w|_n) \)

With \( L \subset \Gamma^\omega \), we associate a subspace of \([0, 1]\) to \( L \).

Special Pairs

\( \{w, w'\} \) is a special pair iff \( \overline{\text{ind}}(w) = \overline{\text{ind}}(w') \)
First Impossibility Proof

For $\Gamma^\omega$, remark that the image of $\Gamma$ by $\overline{\text{ind}}$ is $[0, 1]$

If an algorithm exists, then we have a morphism from a connected space onto a disconnected one.
Terminating Subdivision

(inspired by Gafni, Kuznetsov Manolescu 2014)

**Definition**

Let $C$ be a chromatic complex. A *terminating subdivision* $TS$ of $C$ is a (possibly infinite) sequence of chromatic complexes $(\Sigma_k)_{k \in \mathbb{N}}$ such that

- $\Sigma_0 = \emptyset$,
- for all $k \geq 1$ $\Sigma_k \subset \text{Chr}^k C$,
- $\bigcup_{i \leq k} \Sigma_i$ is a simplicial complex.

$K(TS) = \bigcup_{i \leq 0} \Sigma_i$ is the terminating complex (could be infinite).
Terminating Subdivision

\[ \Sigma_0 = \emptyset \]
\[ \Sigma_1 \equiv \{ \circ \leftrightarrow \bullet \} \]
\[ \Sigma_2 \equiv \{ \circ \leftrightarrow \bullet \circ \leftrightarrow \bullet, \circ \rightarrow \bullet \circ \leftrightarrow \bullet \} \]
\[ \Sigma_3 \text{ is all remaining simplices} \]
Admissible Terminating Subdivisions

Definition

A terminating subdivision $TS$ is *admissible* for $L$ if for any scenario $\rho \in L$ the corresponding sequence of edges $\sigma_0, \sigma_1, \ldots$ is such that there exists $r > 0$ and a simplex $\tau \in K(TS)$ such that $|\sigma_r| \subseteq |\tau|$. 
Theorem (G., Perdereau 2019)

Consensus is solvable in \( L \subseteq \Gamma^\omega \) if and only if there exist a terminating subdivision \( \Phi \) of \( \text{ln}_{2\text{gen}} \) and a simplicial function \( \delta : K(\Phi) \rightarrow \{0, 1\} \) such that:

- \( \Phi \) is admissible for \( L \);
- For all simplex \( \sigma \in \text{ln}_{2\text{gen}} \), if \( \tau \in K(\Phi) \) is such that \( |\tau| \subset |\sigma| \), then \( \delta(\tau) \in \Delta'_{2\text{gen}}(\sigma) \);
- \( |\delta| \) is continuous.
Necessary Condition

Suppose we have an algorithm \( A \) for \( L \).

\[
\Sigma_r = \{ \{ x, y \} \in PC^L(r) \mid x \text{ and } y \text{ have both decided and at least one has just decided in round } r \} \]

\[
\delta(x) = \text{decision}(x) \quad \forall x \in V(\Sigma_r), \text{piecewise}
\]
Necessary Condition

Suppose we have an algorithm $A$ for $L$.

$$
\Sigma_r = \{\{x, y\} \in PC^L(r) \mid x \text{ and } y \text{ have both decided and at least one has just decided in round } r\}
$$

$$
\delta(x) = \text{decision}(x) \quad \forall x \in V(\Sigma_r), \text{piecewise}
$$

- $\Phi = (\Sigma_r)$ is admissible for $L$
- to prove $|\delta|$ continuous, we show that $\forall x \in |K(\Phi)|$

$$
\exists \eta_x > 0 \quad \forall y \in |K(\Phi)| \quad |x - y| \leq \eta_x \Rightarrow |\delta|(x) = |\delta|(y)
$$

with $\eta_x = \min\{ \frac{1}{3r+1} \mid \exists r \in \mathbb{N}, \exists y, \{x, y\} \in V(\Sigma_r)\}$
Since $|\delta|$ is continuous, there exists $\eta(x)$ such that for all $y$, 
$||x - y|| < \eta(x) \Rightarrow \delta(x) = \delta(y)$.

**Data:** function $\eta$

**Input:** $init \in \{0, 1\}$

$t = 1;$

**if** $\bigcirc = \bullet$ **then**

  ind = 1;
  initw = null;
  initb = init;

**else**

  ind = 0;
  initw = init;
  initb = null;
Algorithm

while

geo(ind/t, initw, initb) \notin |K(\Phi)| \lor \eta(geo(ind/t, initw, initb)) < t

do

msg = (init, ind); send(msg); msg = receive();
if msg == null then // message was lost
  ind = 3 * ind;
else
  ind = 2 * msg.ind + ind;
if \bigcirc = \bullet then
  initw = msg.init;
else
  initb = msg.init;

\[ t = t/3; \]

Output: \[ |\delta|(ind/t) \]
The combinatorial description is better explained by connectivity

**Combinatorial Theorem**

Let $L \subset \Gamma^\omega$, then Consensus is solvable for message adversary $L$ if and only if one of the following holds:

- $\exists f \in Fair, f \notin L$,  
- $\exists (u, u') \in SPair, u, u' \notin L$,  
- $\circ\rightarrow\bullet \omega \notin L$,  
- $\circ\leftarrow\bullet \omega \notin L$.  

Why special pairs are tricky

Consider $L = \Gamma^\omega \setminus \{\circ \rightarrow \bullet \leftarrow \bullet \omega\}$

\[
\begin{array}{ccccccccc}
\circ & \bullet & \circ & \bullet & \circ & \bullet & \circ & \bullet & \bullet \\
\Sigma_1 & \Sigma_2 & \Sigma_3 & \ldots
\end{array}
\]
Conclusion

- Consensus is not solvable for $\Gamma^\omega$: bivalency $\iff$ connectivity
- Computability for arbitrary message adversaries
- Topology tools are powerful, but beware of definition of simplicial complexes
- Extension to $n > 2$: presented at PODC 2019 by Nowak, Schmid, and Winkler
Questions?

Thanks for your attention.