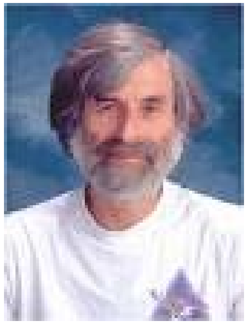
# Byzantine Agreement

## Deterministic, Randomized & Quantum Protocols

Michael Ben-Or

The Hebrew University



- 1970's - SRI to design a "fly by wire" fault tolerant system for the space shuttle.
- Reaching Agreement in the Presence of Faults [PSL 1977/8]
- Lamport coins the name "Byzantine Agreement" [PSL 1982]

- **$n$ processes or players, $P_1,\ldots P_n$, each with an input bit $b_i$**
- **Want all non faulty players to reach agreement on a a bit $b$ such that**
  - All non faulty players agree on the same $b$
  - If all $P_i$ start with the same $b_i$ then output $b=b_i$
- **Pairwise communication channels**
- **This talk mostly synchronous communication networks**

# Motivation

- Reaching agreement in the presence of faults is a natural and fundamental problem in distributed computation.
- Demonstrates remarkable differences between what is possible with deterministic, randomized and quantum protocols!

We model faults by a computationally unbounded Adversary

- Computer crash, no electricity – Fail-Stop fault model
- Software or undetected hardware errors, incoherent or wrong data, malicious players – Byzantine fault model

Assuming we have $n$ players and at most $t$ faults

Lower Bounds:

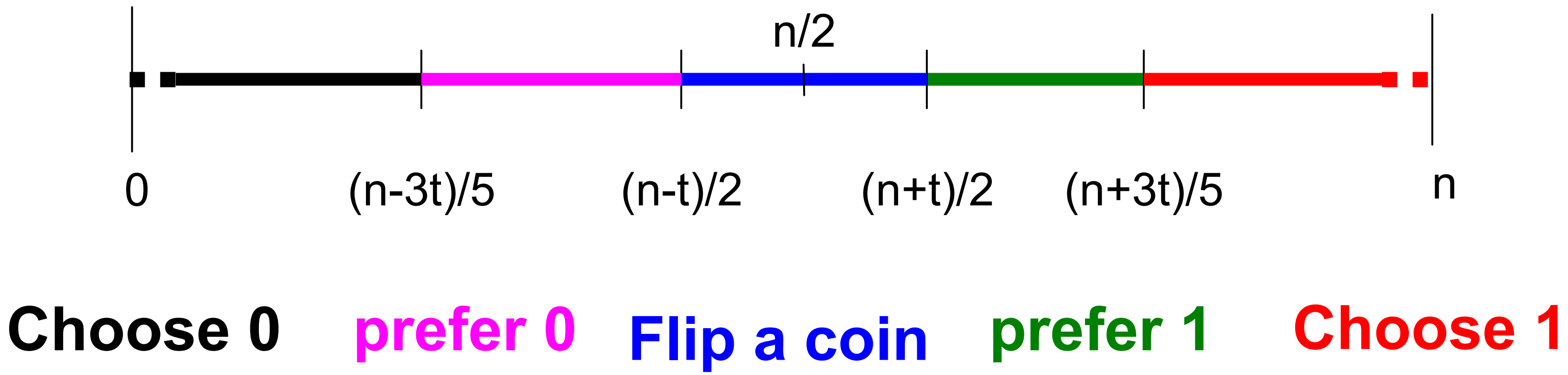
- A deterministic lower bound of $t+1$ rounds for fail stop faults
- For Byzantine faults $t<n/3$ [PSL78].
- No deterministic protocols even for $t=1$ in the asynchronous setting [FLP82].

Protocols:

- There are efficient deterministic $t+1$ rounds protocols tolerating $t<n/3$ Byzantine faults in the synchronous model [PSL77-78,GM93]

# Weak Global Coin

- We reduce agreement to weak global coin flipping
- Decide when there is a large majority of players suggesting the same value $b \in \{0,1\}$.




- If the coin flip succeeds with probability $p$ the expected number of round to reach agreement is $O(1/p)$.

## Adversary can react to players' random selections:

- static or adaptive failures
- private communication or full information about the system
- fail stop or Byzantine type faults

## Examples:

- Static, fail stop, full information adversary:

  Each player $P_i$ selects a random $r_i \in [0,n^3)$. Declare the player with the min as the **leader**. Leader flips an unbiased coin.

  ⇨ **O(1)** rounds protocol.

- Adaptive, Byzantine, full information (even asynchronous) adversary: Use majority voting on local random bits.

  ⇨ Exponential time, but just **O(1)** for $t < O(n^{1/2})$.

# Randomized Protocols – More Examples

- Adaptive, fail-stop, full information adversary:

  Majority gives for all $t < n$

  $$t / \sqrt{n \cdot \log\left(2 + t / \sqrt{n}\right)} \Rightarrow \sqrt{n / \log(n)}$$

  matching the lower bound [BB98].

- Static, Byzantine, full information adversary:

  First try: Use functions that minimize the influence of each variable.

  Given $f : \{0,1\}^n \to \{0,1\}$ the influence of $S \subset [n]$

  $$I_f(S) = Pr_x[\ \exists\ s_0, s_1 \in \{0,1\}^S \text{ s.t. } f(s_0,x) \neq f(s_1,x)\ ]$$

  $$I_f(k) = \max\{\ I_f(S) : |S| = k\ \}$$

  **[KKL]** If $Pr_x[\ f(x)=0\ ] \approx ½$ then $I_f(1) = \Omega(\ (\log n)/n\ )$

  and $\exists\ S,\ |S| \approx n/\log n$, such that $I_f(S) > 1 - \varepsilon$

[BKKKL] showed that $I_f(1)=\Omega((\log n)/n)$ for general balanced $f$

$$f: X_1 \times X_2 \times \quad \times X_n \rightarrow \{0,1\}$$

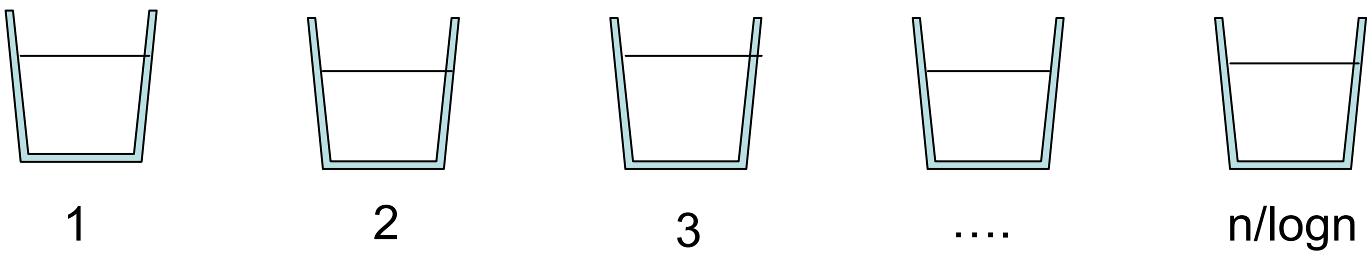
The question whether always a small subset can control the function remains open, leaving the possibility of an $O(1)$ round protocol open [for the static, Byzantine, full information adversary model].

More than one round coin flipping games:

- For $t \geqslant n/2$ there are always $t$ faulty players that can force either 0 or 1 (not true for quantum coin flipping!)
- There are games where the maximal bias by $t$ players is bounded by $O(t/n)$, and this is optimal.

# Feige's $\log_* n$ Leader Election Game

Each player selects a random bin.




The smallest bin is selected, and they continue recursively, until a single leader is elected [RZ98,F99].

Using just one round of Feige's trick [BPV06,GPV07 and KSSV06] achieve **O(log n)** time protocols for static, Byzantine, full information adversary.

## Coin Flipping with an Adaptive Adversary

Note: All known robust coin flipping games select an almost random leader, and then the leader flips a coin.

All this is useless in the adaptive setting.

Are there better games than the “Majority” game for adaptive adversaries?

- Adaptive, Byzantine, private comm. adversary:

  Each player $P_i$ selects a random $r_i \in [0,n^3)$. Declare the player with the min as the **leader**. Leader flips an unbiased coin.

  Problem: A bad player can choose 1 and get elected.

  First try:

  Independently for player **P**: Each $P_k$ , k=1…n, selects random $r_i \in [0,n^3)$, and set

$$r = \sum_{k=1}^{n} r_k \pmod{n^3}$$

  Problem: A bad player can select $r_k$ after other values are known and control **r**.

  **Idea:** Use Verifiable Secret Sharing **(VSS)**

  Problem: **VSS** requires Byzantine Agreement !?

  **Idea**:[FM88] A two round "weak agreement" protocol is good enough for here ⇨ O(1) time protocol.

- Adaptive, Byzantine, full information adversary:

Players have pairwise quantum channels

"full information" in the quantum setting: The adversary knows the description of the current pure state of the system.

**Toy Example**: Adaptive, fail-stop, full information adversary

Each player prepares

$$|\phi\rangle = \sum_{k=0}^{n^3-1} |k,k,\dots,k\rangle$$

and a GHZ state

$$|\psi\rangle = |0,0,\dots,0\rangle + |1,1,\dots,1\rangle$$

and distributes the pieces to all **n** players.

$$|\phi\rangle = \sum_{k=0}^{n^3-1} |k,k,\ldots,k\rangle$$

$$|\psi\rangle = |0,0,\ldots,0\rangle + |1,1,\ldots,1\rangle$$

At the next round all players measure all the pieces they have; a leader is selected according to the shared minimum; and the corresponding measured bit serves as the “global coin”.

**Cor:** We get an $O(1)$ expected round agreement protocol.

By delaying the measurements until all the quantum messages have arrived the adversary has to stop messages before the outcome is known, and so effectively the adaptive adversary isn’t stronger than the static one.

- Adaptive, Byzantine, full information adversary:

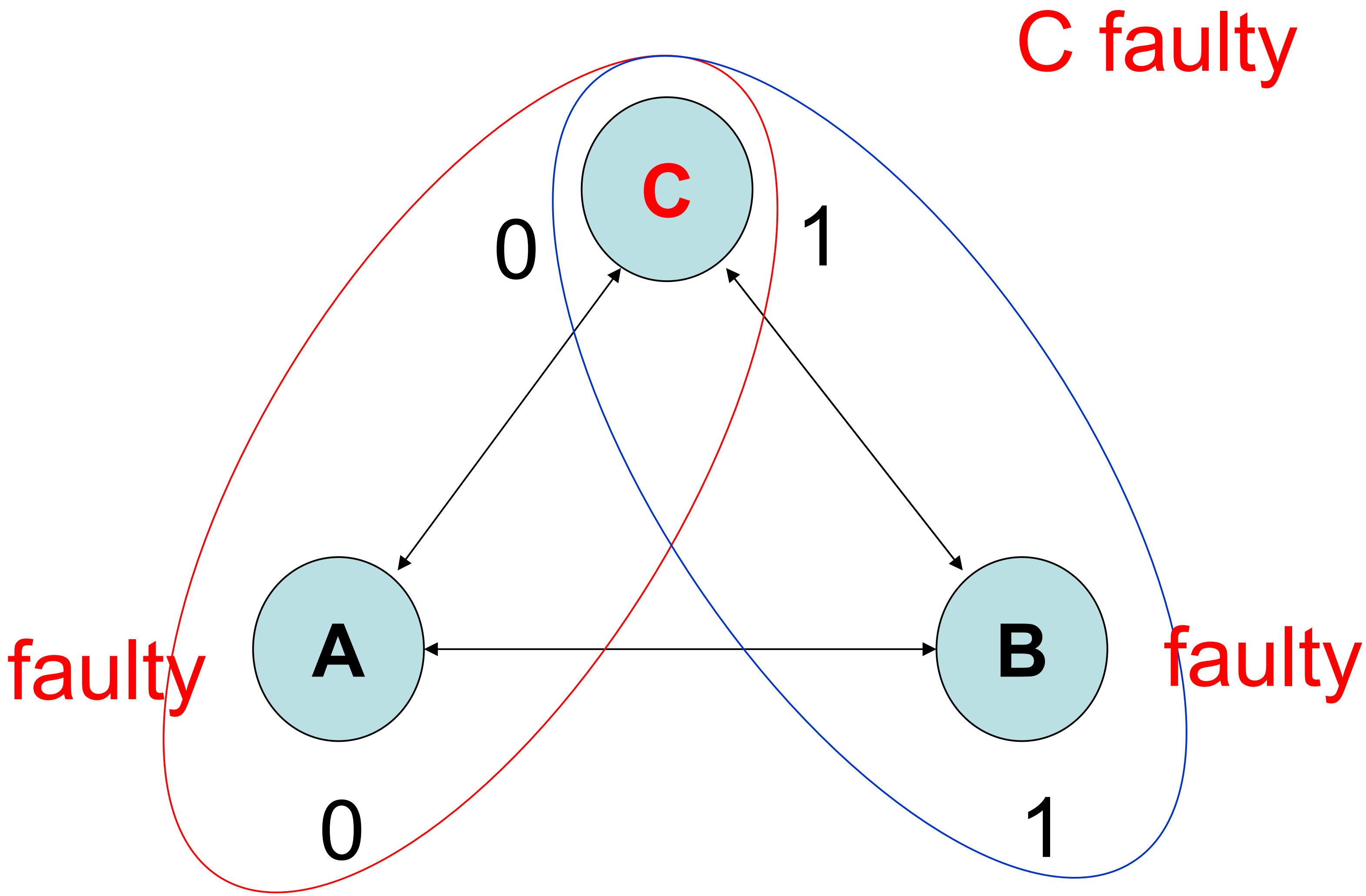
**Idea:** replace random shared secrets by a superposition on all possible $n^3$ secrets and all possible polynomials.

- This is just an encoding of the superposition of all secrets using a standard CSS quantum error correcting code.
- We can use the QVSS procedure of [CGS02] replacing Byzantine agreements with the “weak agreements” of [FF88]

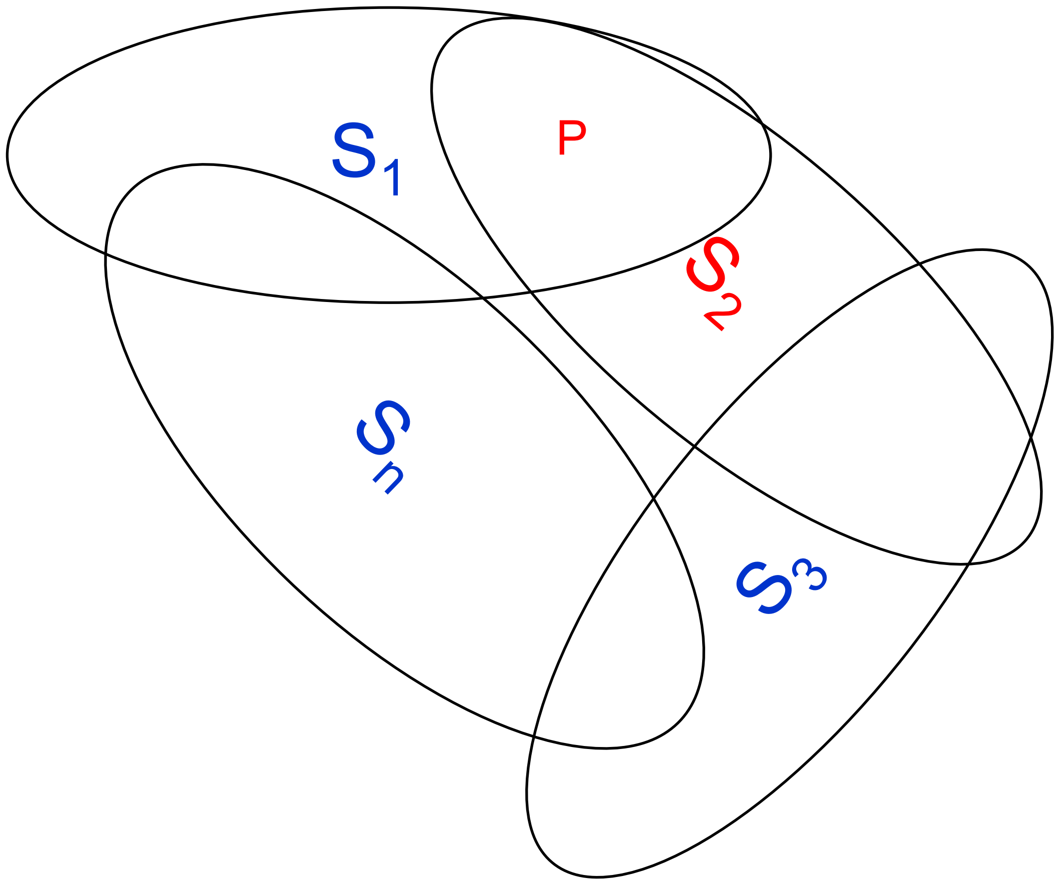
- We get an O(1) round quantum Byzantine agreement protocol in the adaptive, Byzantine, full information adversary model, tolerating an optimal $t<n/3$ faults.

# Open Problems

- In the asynchronous setting we can handle only $t<n/4$ faults, while BA is possible for $t<n/3$. The classical "private channel" solution of [CR93, see also BCGHS07] uses secret authentication codes and this can't work here.
- Is the majority coin flipping game asymptotically optimal with an adaptive adversary ?
- Extend KKL lower bound to general functions.
- Can we beat the $O(\log n)$ for the static, Byzantine, full information adversary ?
- Scalable large network protocols [see KSSV06].




A and B do not agree - contradiction




**$S_1$,…,$S_n$** are processes, each composed of a group of players. While the **S**'s are trying to reach agreement a bad player P in a good set can leak information to bad players in a bad set

A process is "good" is less than 1/3 of its players are faulty.