Exact Fault Tolerance Consensus with Voting Validity

Zhangchen Xu [1]**,** Yuetai Li [2], Chenglin Feng [2] and Lei Zhang [2]

[1] Department of Electrical and Computer Engineering, University of Washington
[2] James Watt School of Engineering, University of Glasgow

Outline

- Background: Distributed Consensus
- Motivation
- Existing Solutions
- Main Theoretical Results
- Consensus Protocol Design and Refinement
- Conclusion and Future Work

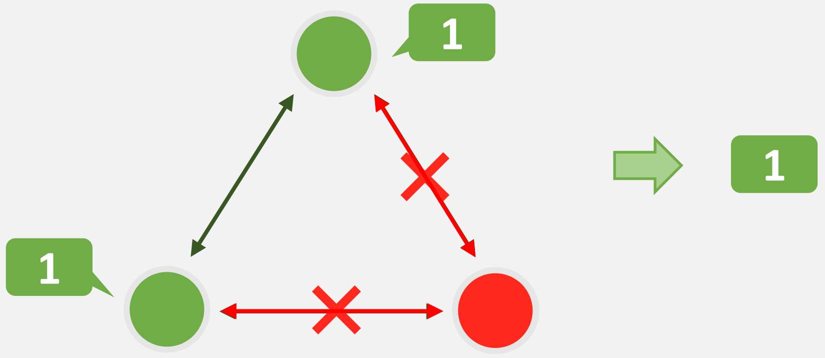
Background

Distributed Consensus

- Reaching an agreement among a group of nodes, despite the existence of faulty (i.e., **crash** or **Byzantine**) nodes.

Crash Fault Tolerance (CFT) $N > 2t$

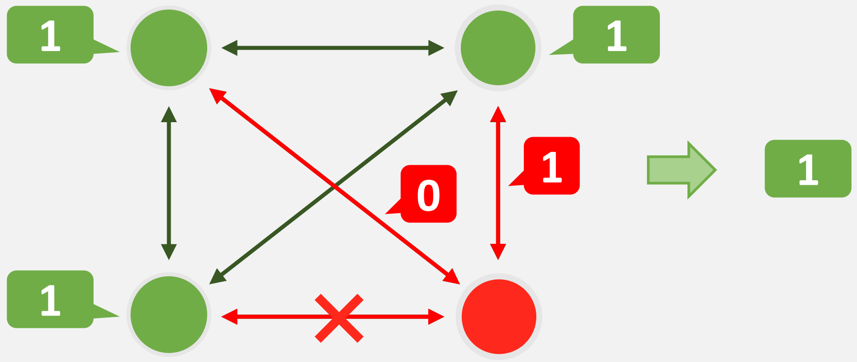
Min No. of votes: $N - t$



Crash Fault: stops working without resuming

Byzantine Fault Tolerance (BFT) $N > 3t$

Min No. of votes: $N - t$



Byzantine Fault: act arbitrarily

Background

Distributed Consensus

- [Classic Binary Consensus Definition] A distributed consensus algorithm must satisfy:
  - **Termination**: Every non-faulty node can decide a single output **value in finite time**
  - **Agreement**: The output value of non-faulty nodes are **identical**
  - **Validity**: If all non-faulty nodes **begin with the same input value**, they output that value

→ Can non-faulty nodes **begin with different input values** according to what they prefer, like a democratic election?

Motivation

Differences of "voting" in distributed consensus and social choice

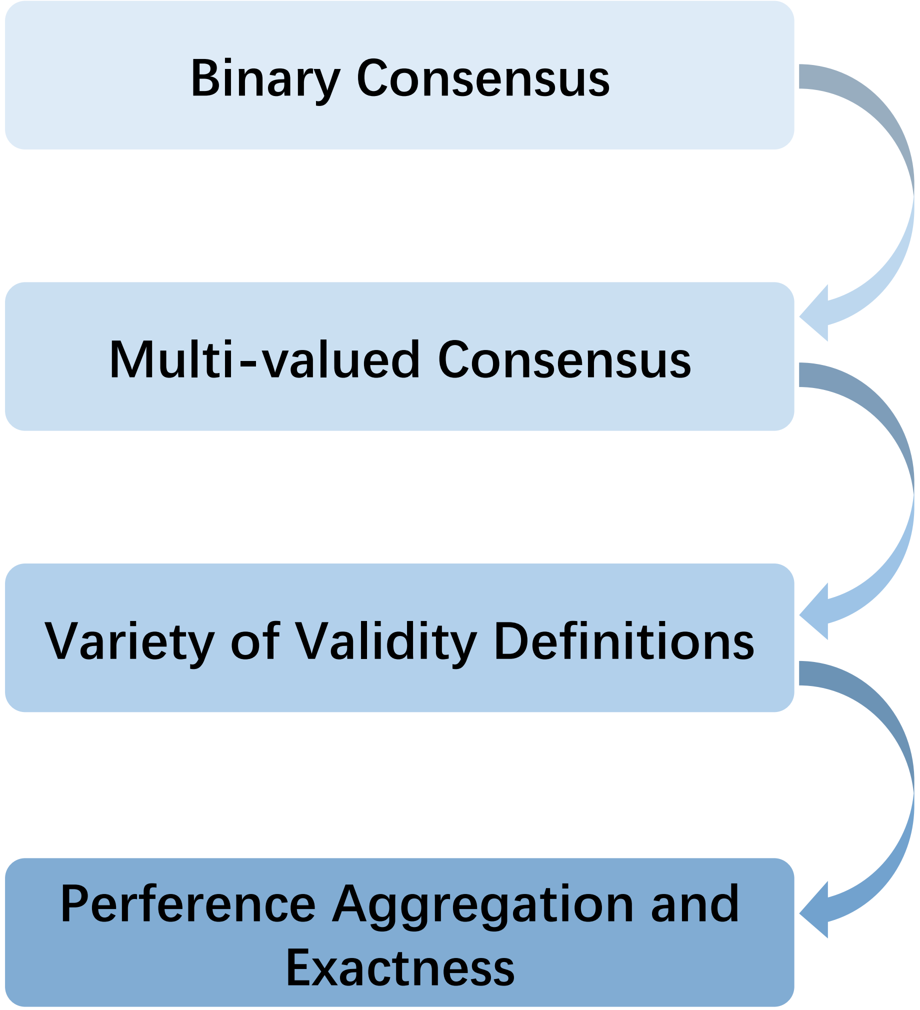
- Voting in Distributed Consensus: A mechanism that produces **agreement** among different nodes. Reach agreements > what agreements be made
- Voting in Social Choice: **Preference aggregation**. Participants have specific preferences for one option.

*Can we ensure not only **agreement** but also realize **preference aggregation** in consensus process?*

Potential applications

- Multi-agent coordination
- Majority voting in distributed systems
- Leader election in blockchain
- …

Existing Solutions


Binary Consensus
Multi-valued Consensus
Variety of Validity Definitions
Perference Aggregation and Exactness

Validity Definitions

Validity: If all non-faulty nodes begin with the same input value, they output that value.

Binary inputs to multi-valued inputs.

Strong Validity: The output value of each non-faulty node must be the input value of some non-faulty nodes.

Add more practical meaning.

Median Validity, Interval Validity, Approximate Average …

Map validity to perference aggregation.

Discrete Inputs --> Require exactness of the outputs.

[This Paper] Voting Validity: The output value of non-faulty nodes must be the **exact plurality** of the inputs of non-faulty nodes.

- Achieve Termination, Agreement and Voting Validity

Main Results

Options $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$, maximum fault tolerance $\boldsymbol{t}$, total number of nodes $\boldsymbol{N}$
$\boldsymbol{A_G} > \boldsymbol{B_G} > \boldsymbol{C_G}$: number of non-faulty nodes support $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$

With Prior voting knowledge:

- Impossibility of distributed consensus with voting validity if

$$N \leq \boldsymbol{max\{3t, 2t + 2B_G + C_G\}}$$

- Possibility of distributed consensus with voting validity if

$$N > \boldsymbol{max\{3t, 2t + 2B_G + C_G\}}$$

Our BFT Protocol

Main Results

Options $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$, maximum fault tolerance $\boldsymbol{t}$, total number of nodes $\boldsymbol{N}$
$\boldsymbol{A_G} > \boldsymbol{B_G} > \boldsymbol{C_G}$: number of **non-faulty nodes** support $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$

Without Prior voting knowledge:

- **Impossibility** of distributed consensus with voting validity without prior voting knowledge.
- **Possibility** of distributed consensus with voting validity without prior voting knowledge **if termination property is relaxed**.
  - Introduce Safety-critical Tolerance (SCT) and Safety-Guaranteed Protocol:

Termination Condition: $N > \boldsymbol{3t} + \boldsymbol{2B_G} + \boldsymbol{C_G}$

Our Safety-Guaranteed BFT Protocol

Protocol Design and Refinement

Highlights of Protocol Design:

- We proposed one-shot CFT, BFT and SCT consensus protocols with the proposed voting validity
- We proved the correctness of proposed protocols

Two Protocol Refinements:

- Incremental Threshold Protocol to realize **optimistic responsiveness.**
- Distributed consensus in **wireless broadcast networks**. The BFT distributed consensus protocol with voting validity can achieve if

$$N > \boldsymbol{2t} + \boldsymbol{2B_G} + \boldsymbol{C_G}$$

Conclusion and Future Work

- We proposed **voting validity**, a crossover between distributed consensus and social choice.
- We provide a comprehensive fault-tolerance analysis and give several **impossibility results**.
- We proposed CFT, BFT and SCT distributed consensus **protocols** and proved their correctness.

Future work:

- Different validity definitions and their application perspective
- Extending the voting validity to multi-dimensional agreement
- Developing State-Machine-Replication protocols for voting validity

Thank you

zxu9@uw.edu