Consensus with Three Options

"Stabilizing Consensus with Many Opinions" — Becchetti et al.

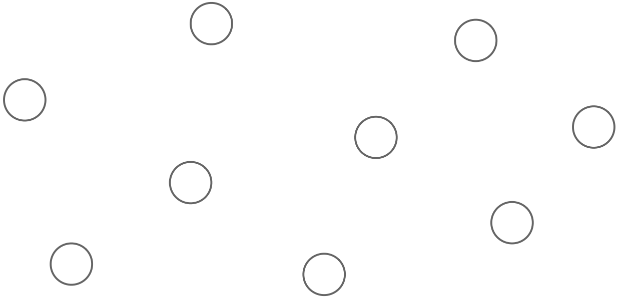
"Fast Plurality Consensus in Regular Expanders" — Cooper et al.

Laurent Chuat

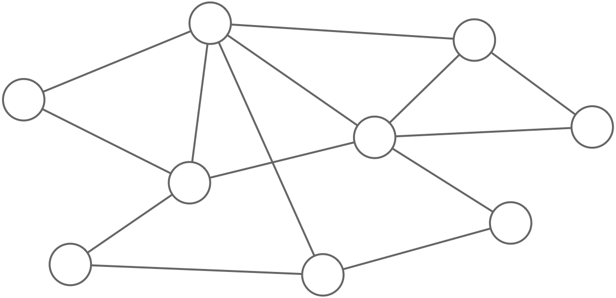
February 27, 2018

Network Security Group, ETH Zurich

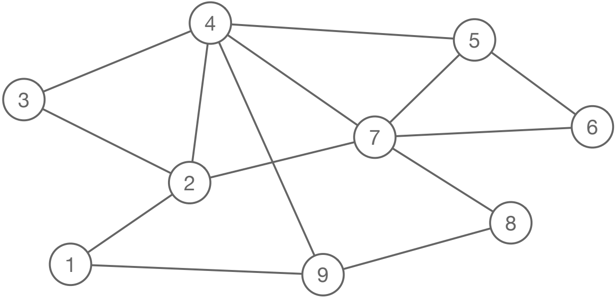
The Consensus Problem



The Consensus Problem

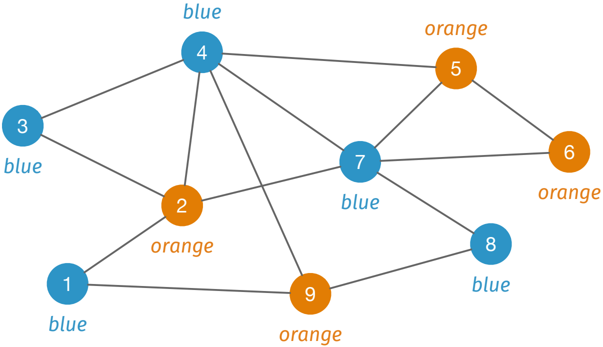


The Consensus Problem



$n = 9$

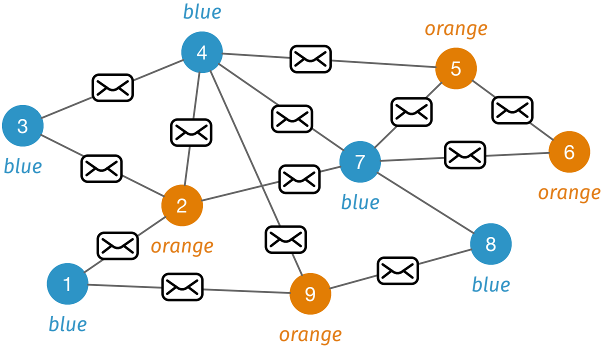
The Consensus Problem



$$n = 9$$

$$\Sigma = \{\text{“blue”}, \text{“orange”}\}$$

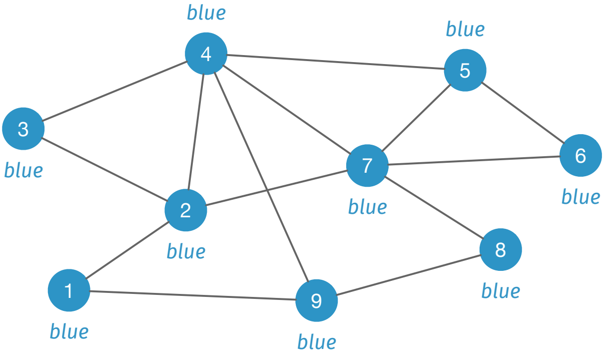
The Consensus Problem



$$n = 9$$

$$\Sigma = \{\text{“blue”}, \text{“orange”}\}$$

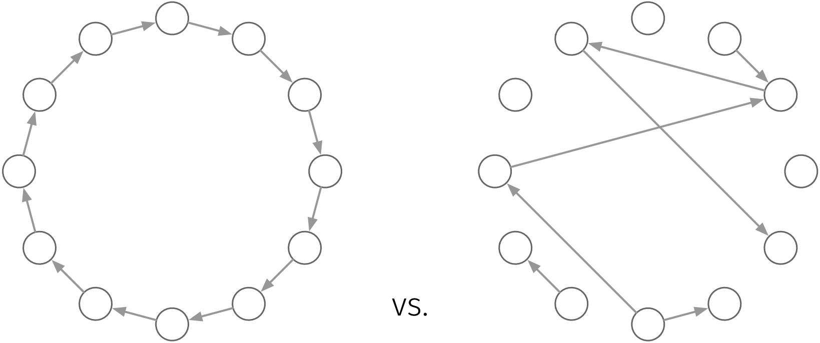
The Consensus Problem



$$n = 9$$

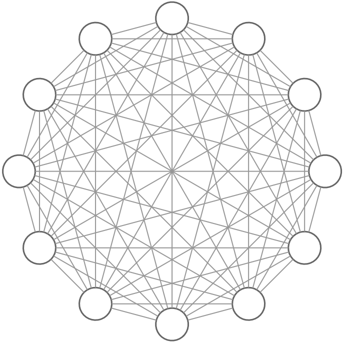
$$\Sigma = \{\text{“blue”}, \text{“orange”}\}$$

Variants of Consensus



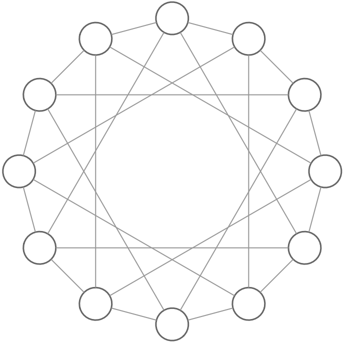
Synchronous vs. Asynchronous

Variants of Consensus



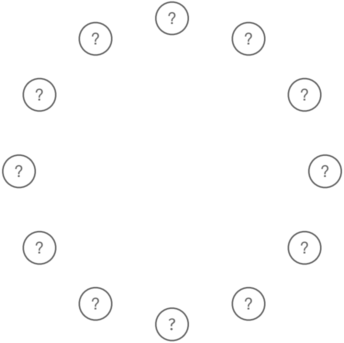
Complete Network

VS.



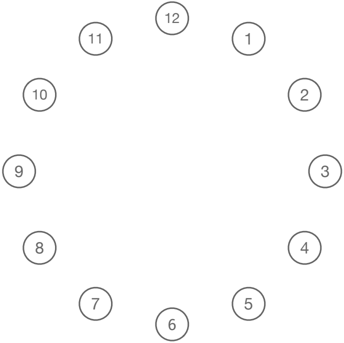
Incomplete Network

Variants of Consensus



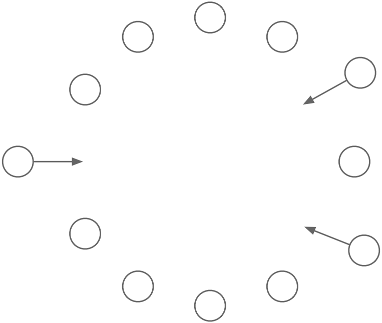
Anonymous Nodes

VS.



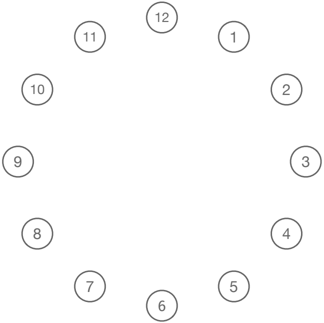
Identified Nodes

Variants of Consensus



Permissionless System

VS.



Permissioned System

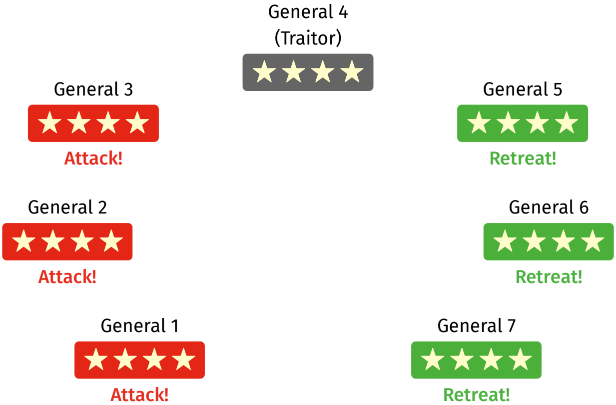
Consensus in the Age of Blockchains

Nakamoto Consensus

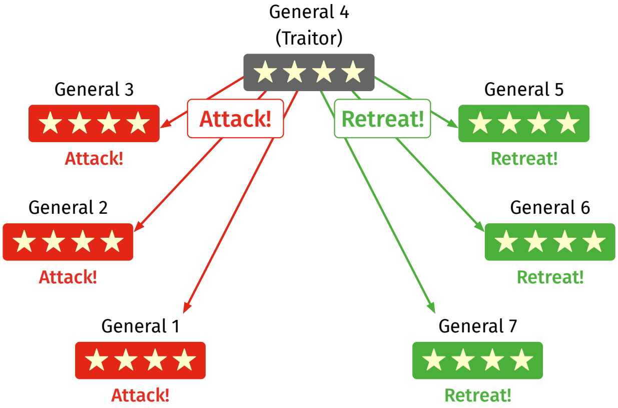
- **Objective:** consensus on the set and order of transactions
- **How:** proof of work
- **Why:** prevent censorship and multiple spending

Byzantine Adversaries

Byzantine Adversaries

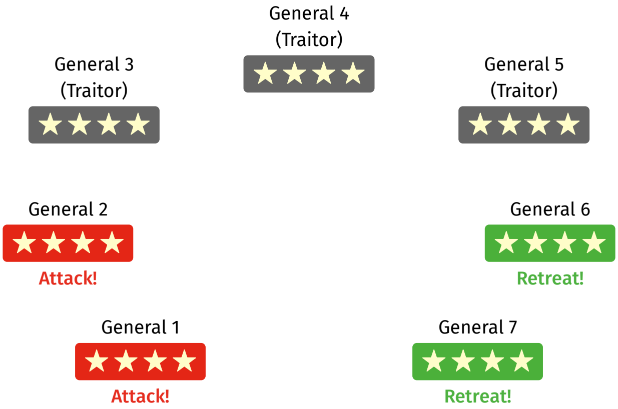


Byzantine Adversaries



Byzantine Adversaries

Byzantine Adversaries



[1] “The Byzantine Generals Problem”, Leslie Lamport, Robert Shostak, and Marshal Pease, 1982.

Objective

The goal of *Byzantine agreement* is to bring the system into a configuration that meets the following conditions:

1. Agreement
2. Validity
3. Termination

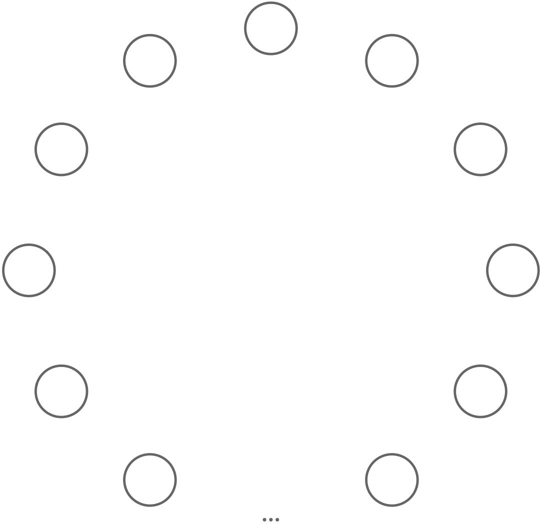
Stabilizing Consensus with Many Opinions

Luca Becchetti[1], Andrea Clementi[2], Emanuele Natale[1], Francesco Pasquale[2], and Luca Trevisan[3]

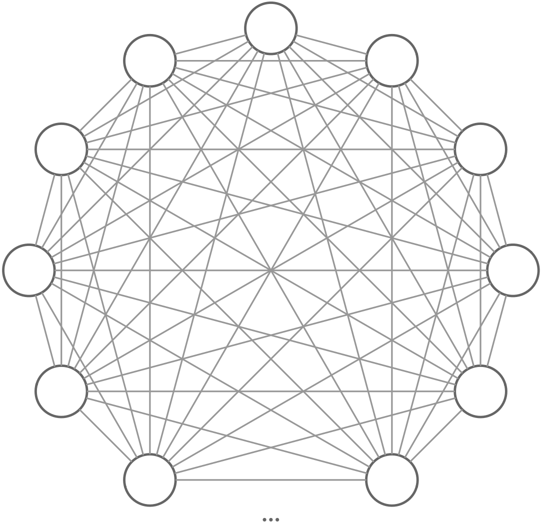
[1] *Sapienza Università di Roma*
[2] *Università Tor Vergata di Roma*
[3] *U.C. Berkley*

August 28, 2015

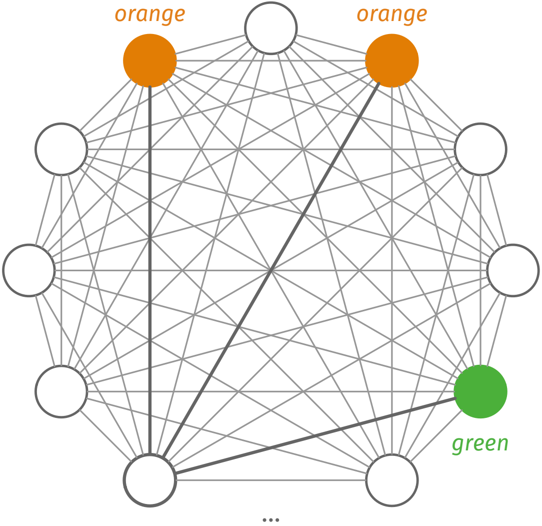
Setting



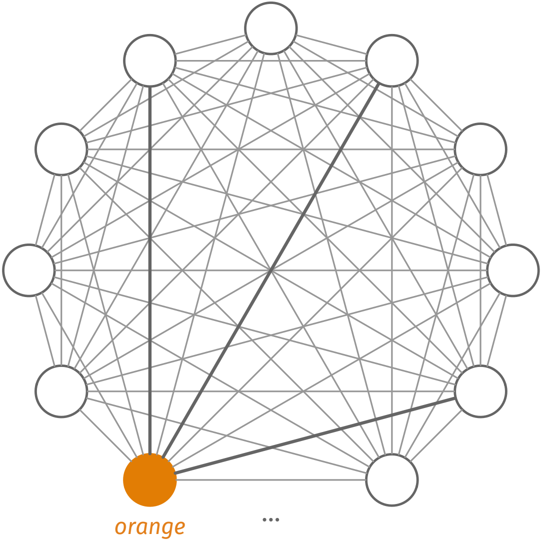
Setting



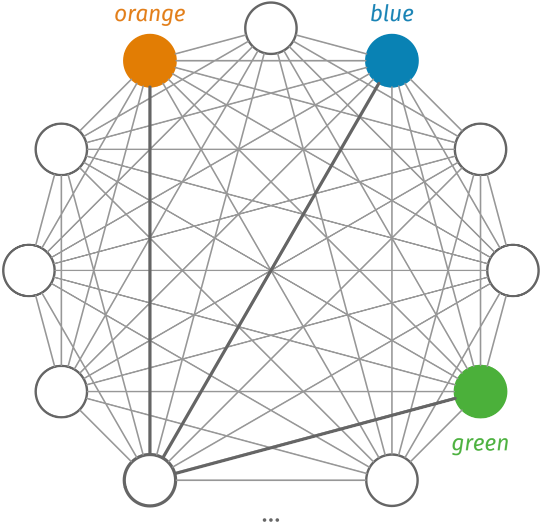
3-Majority Dynamics



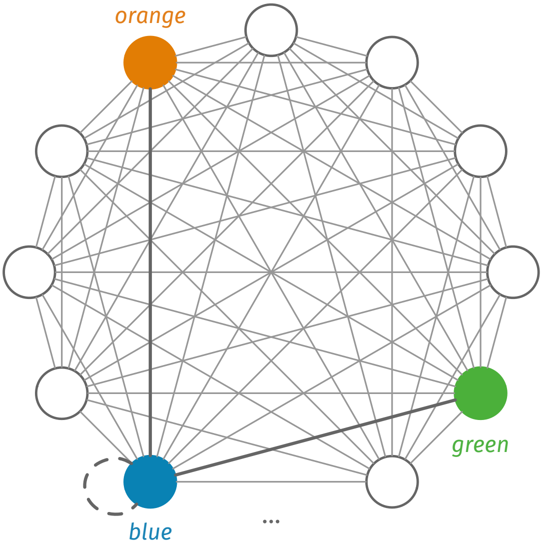
3-Majority Dynamics



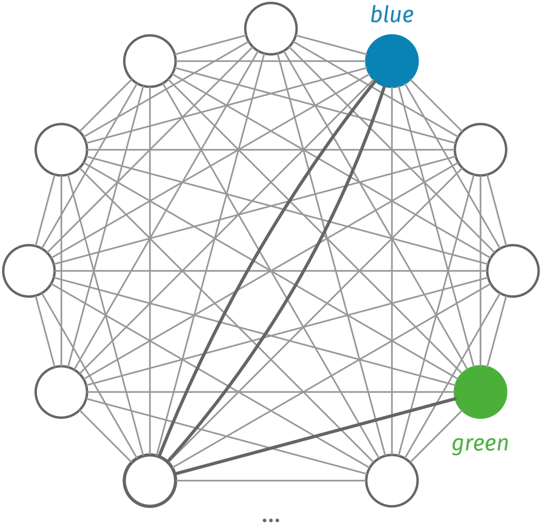
3-Sampling: Tie Breaking



3-Sampling: Including the Node Itself



3-Sampling: With Repetitions



Objective

1. *Almost* Agreement: The system must reach a regime of configurations where all but a negligible subset (i.e., having size $\mathcal{O}(n^\gamma)$ for a constant $\gamma < 1$) of the nodes support the same opinion.

Objective

2. *Almost* Validity: Converge w.h.p. to an almost agreement where all but a negligible subset keep the same valid opinion.

3. *Non* Termination: Nodes are not necessarily able to detect any global property.

Objective

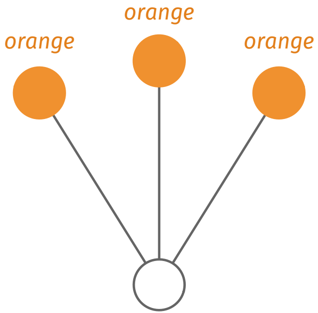
4. *Stability:* Convergence is only guaranteed to hold *with high probability* (in short, w.h.p.) and over a long period (i.e., polynomial number of rounds).

Notation

n	number of nodes
Σ	set of opinions
$W \subseteq \Sigma$	set of active opinions
$\mathbf{c} := (c_1, \ldots, c_{\lvert\Sigma\rvert})$	configuration
$\mathbf{C}^{(t)}$	configuration at time t
c_i	support of opinion i
$X_{i,u}^{(t)}$	node u gets opinion i at time t

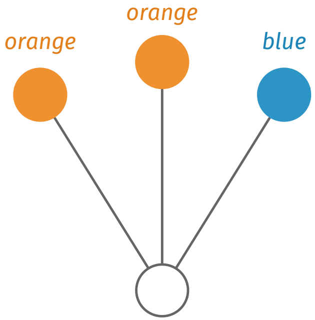
Drift of Below-Average Opinions

$$\mathsf{P}\left(X_{i,u}^{(t+1)} = 1 \mid \mathbf{C}^{(t)} = \mathbf{c}\right) = \left(\frac{c_i}{n}\right)^3 + \ldots$$



Drift of Below-Average Opinions

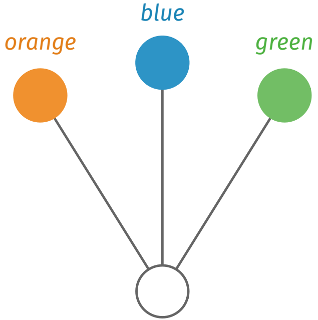
$$\mathsf{P}\left(X_{i,u}^{(t+1)} = 1 \mid \mathbf{C}^{(t)} = \mathbf{c}\right) = \ldots + 3\left(\frac{c_i}{n}\right)^2\left(\frac{n-c_i}{n}\right) + \ldots$$



Drift of Below-Average Opinions

$$\mathbf{P}\left(X_{i,u}^{(t+1)} = 1 \mid \mathbf{C}^{(t)} = \mathbf{c}\right) = \dots$$

$$+ \left(\frac{c_i}{n}\right)\left[1 - \left(\frac{\sum_{l \in S}^{k} c_l^2}{n^2} + 2\left(\frac{c_i}{n}\right)\left(\frac{n - c_i}{n}\right)\right)\right]$$



Drift of Below-Average Opinions

Lemma 2.1

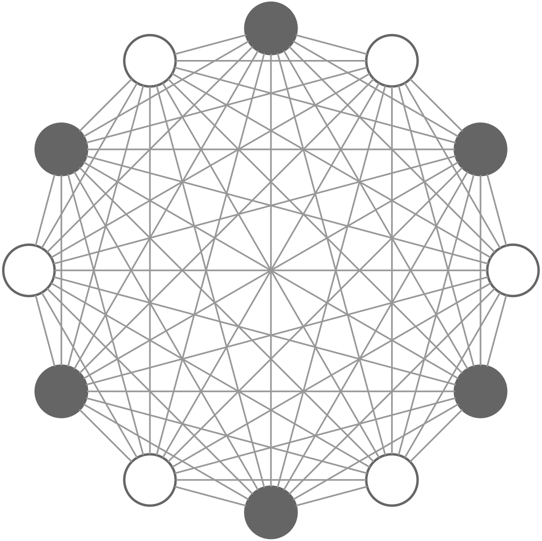
$$\mathrm{E}\left[C_i^{(t+1)} \mid \mathbf{C}^{(t)} = \mathbf{c}\right] = c_i \left(1 + \frac{c_i}{n} - \frac{\sum_{j \in W} c_j^2}{n^2}\right) \leq c_i \left(1 + \frac{c_i}{n} - \frac{1}{|W|}\right)$$

Drift of Below-Average Opinions

If $c_i = n/|W|$, then

$$\mathrm{E}\left[C_i^{(t+1)} \mid \mathbf{C}^{(t)} = \mathbf{c}\right] \le c_i$$

Symmetry-Breaking



Lemma 3.3. Let c be any configuration with $|W|$ active opinions. Within $t = \mathcal{O}(|W|^2 \log^{1/2} n)$ rounds, it holds that

$$\mathrm{P}_{\mathsf{c}}(\exists\ i \text{ such that } C_i^{(t)} \leq n/|W| - \sqrt{|W| n \log n}) \geq \frac{1}{2}$$

Dropping Stage 1

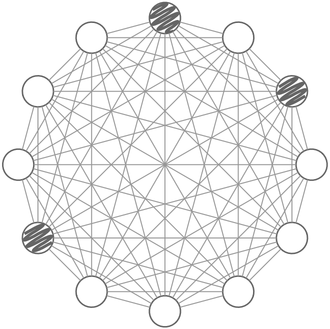
Lemma 3.4. Let **c** be any configuration with $|W| \leq n^{1/3-\epsilon}$ active opinions, where $\epsilon > 0$ is an arbitrarily small positive constant, and such that an opinion i exists with $c_i \leq n/|W| - \sqrt{|W| n \log n}$. Within $t = \mathcal{O}(|W| \log n)$ rounds, opinion i becomes $\mathcal{O}(|W|^2 \log n)$ with high probability.

Dropping Stage 2

Lemma 3.5. Let $\mathbf{c}$ be any configuration with $|W| \leq n^{1/3-\epsilon}$ active opinions, where $\epsilon > 0$ is an arbitrarily small positive constant, and such that an opinion i exists with $c_i \leq n/(2|W|)$. Within $t = \mathcal{O}(|W| \log n)$ rounds, opinion i disappears with probability at least 1/2.

The F-Static Adversary

At the end of the first round, once every node has fixed his own initial opinion, the adversary looks at the configuration and arbitrarily replaces the opinion of at most F nodes with an arbitrary opinion.

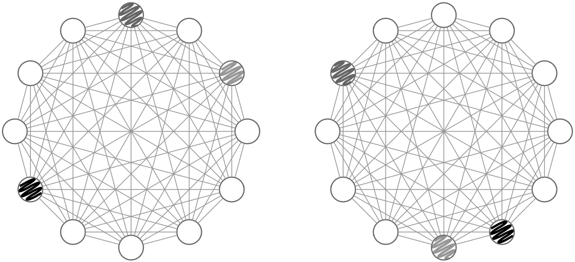


$F = 3$

Corollary 4.1. Let $k \leq n^{\alpha}$ for some constant $\alpha < 1$ and $F = n/k - \sqrt{kn \log n}$. Starting from any initial configuration having k opinions, the 3-majority protocol reaches a stabilizing almost-consensus in presence of any F-static adversary, w.h.p.

The F-Dynamic Adversary

At the end of every round t, after nodes have updated their opinions, the adversary looks at the current configuration and replaces the opinion of up to F nodes with any opinion.



$F = 3$

Final result

Theorem 4.2. Let $k \leq n^{\alpha}$ for some constant $\alpha < 1$ and $F = \beta\sqrt{n}/(k^{5/2}\log n)$ for some constant $\beta > 0$. Starting from any initial configuration having k opinions, the 3-majority reaches a valid stabilizing almost-consensus in presence of any F-dynamic adversary within a bounded number of rounds, with high probability.

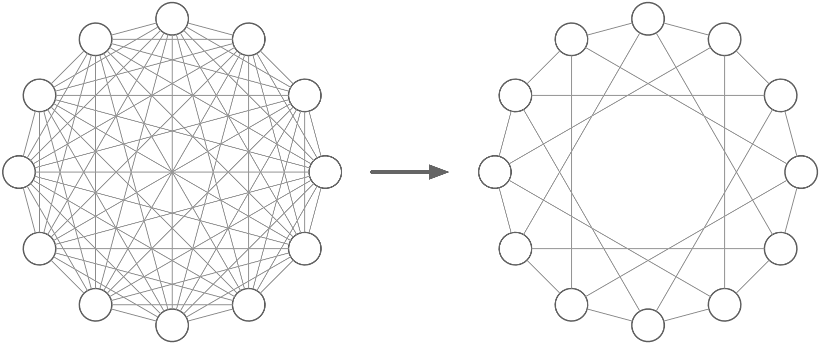
Fast Plurality Consensus in Regular Expanders

Colin Cooper[1], Tomasz Radzik[1], Nicolás Rivera[1], Takeharu Shiraga[2]

[1] King's College London
[2] Kyushu University

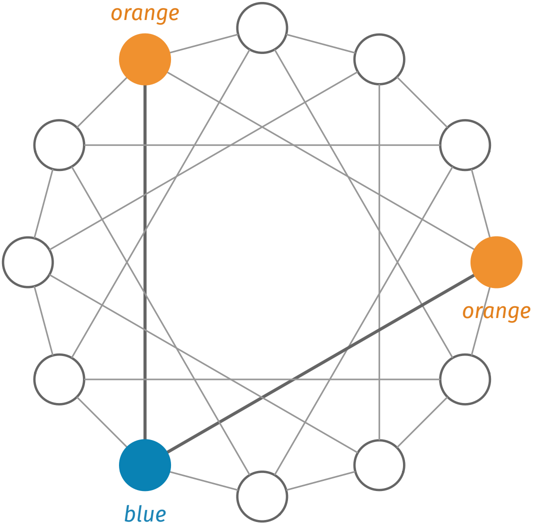
April 14, 2017

A graph is *regular* if every vertex has the same degree (i.e., the number of edges at that vertex).

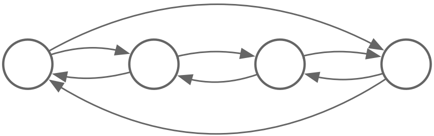


On the left: complete graph, **On the right:** 4-regular graph

Two-sample voting



Random Walk as a Markov Chain



A random walk on the graph defines a Markov chain.

Theorem 1. Let G be a regular n-vertex graph and let the initial sizes of the opinions be $C_1, C_2, \ldots, C_k$ in non-increasing order. Assume that $C_1 - C_2$ is sufficiently large.

With probability at least $1 - 1/n$, after a bounded number of rounds, the two-sample voting completes and the final opinion is the largest initial opinion.

Questions?