Reference frame agreement in quantum networks

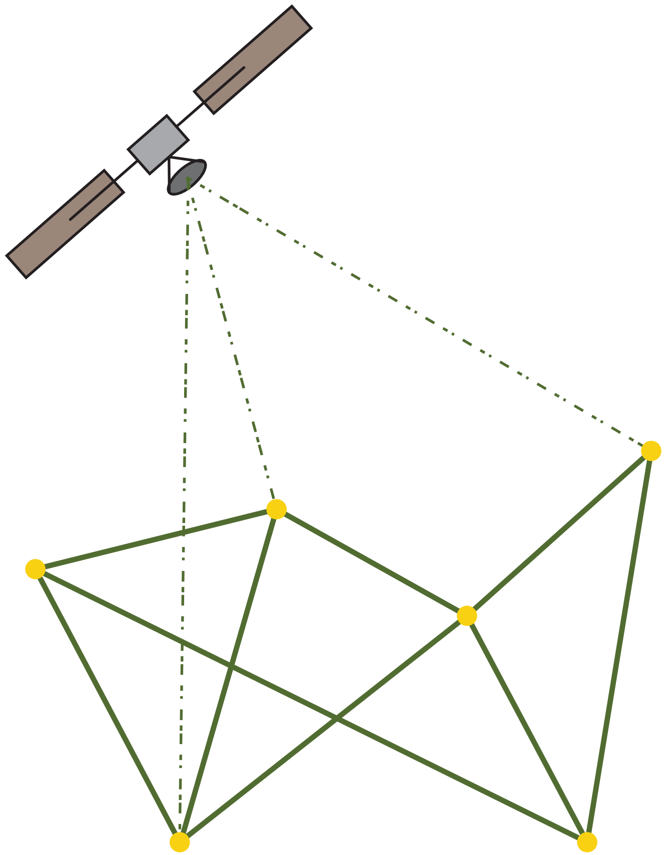
Tanvirul Islam, Loïck Magnin, Brandon Sorg, and Stephanie Wehner

arXiv:1306.5295

Centre for Quantum Technologies

National University of Singapore

Quantum Networks



- Distributed quantum computing

  Beals et al. Proc. R. Soc. A 469 (2013)

- Quantum Cloud computing

  Barz et al. Science 335, 303 (2012)

- QKD networks

  C. Elliott, New J. Phys. 4, 46 (2002)

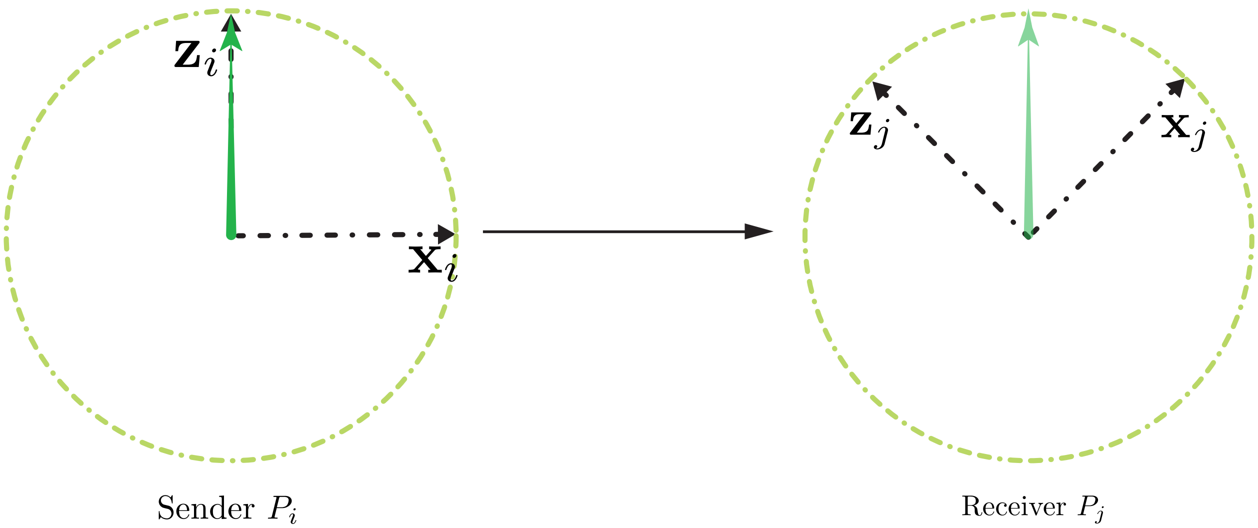
- Satellite QKD

  Bonato et al. New J. Phys. 11, 045017 (2009)

Reference Frame

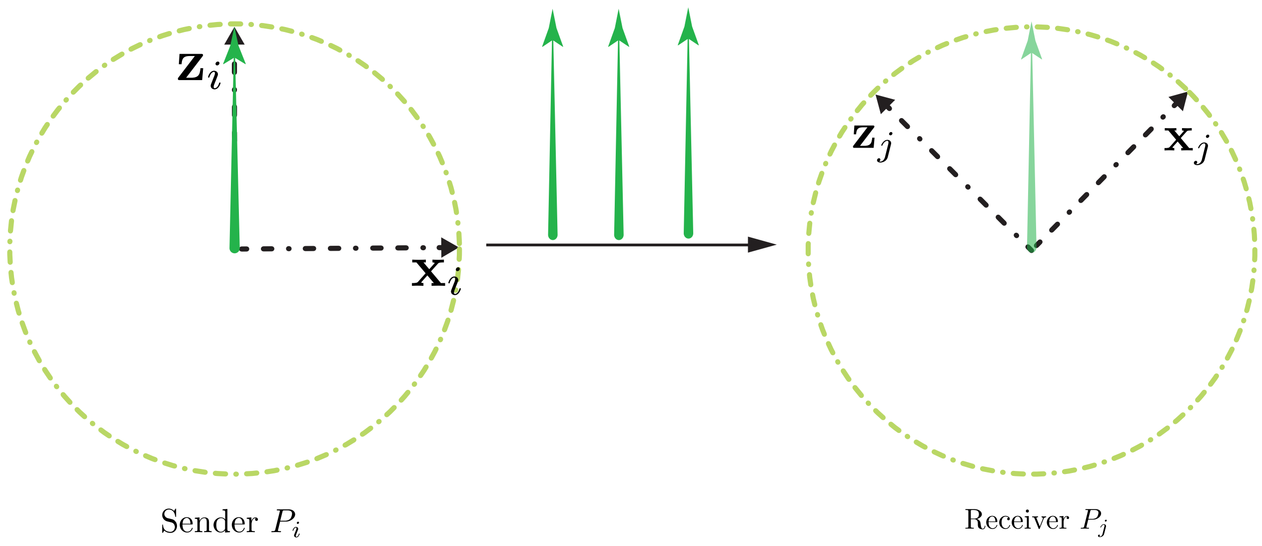
- Quantum info. are encoded with respect to some Reference Frame
  - Photon polarization → Cartesian frame
  - Phase
- Clock

2-party reference frame



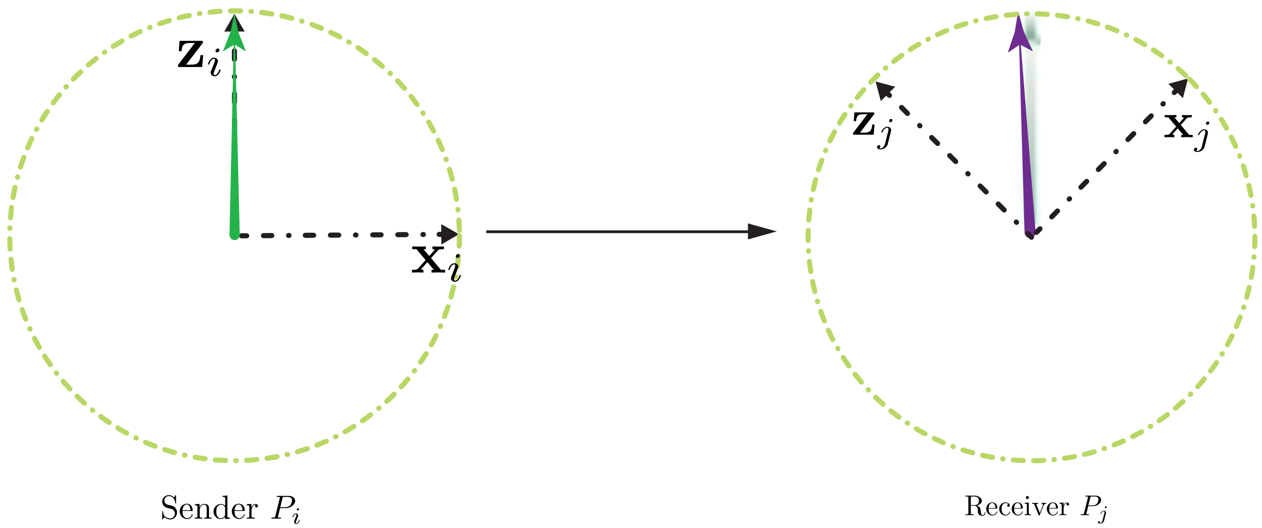
- One cannot agree on directions classically

Example of protocol: 2ED



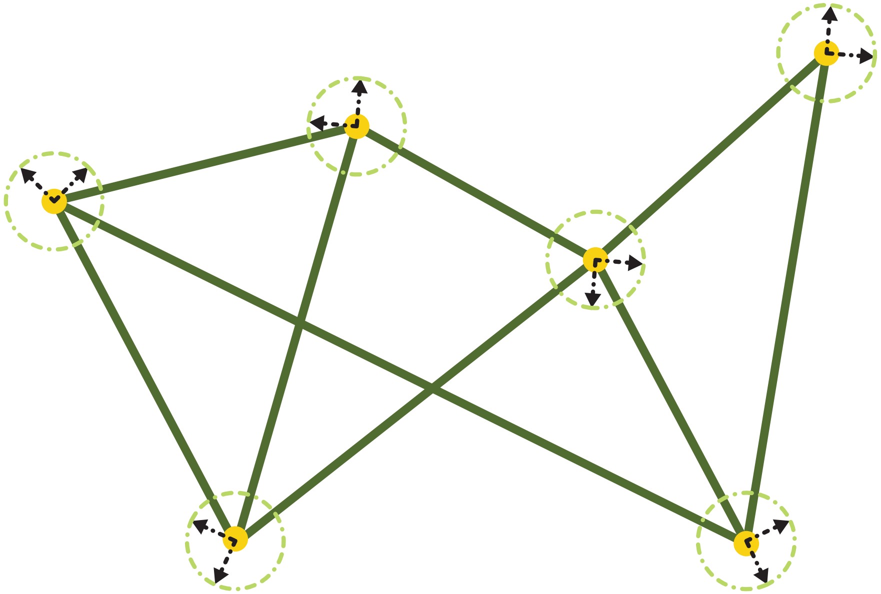
- Possible using qubits

Example: 2ED



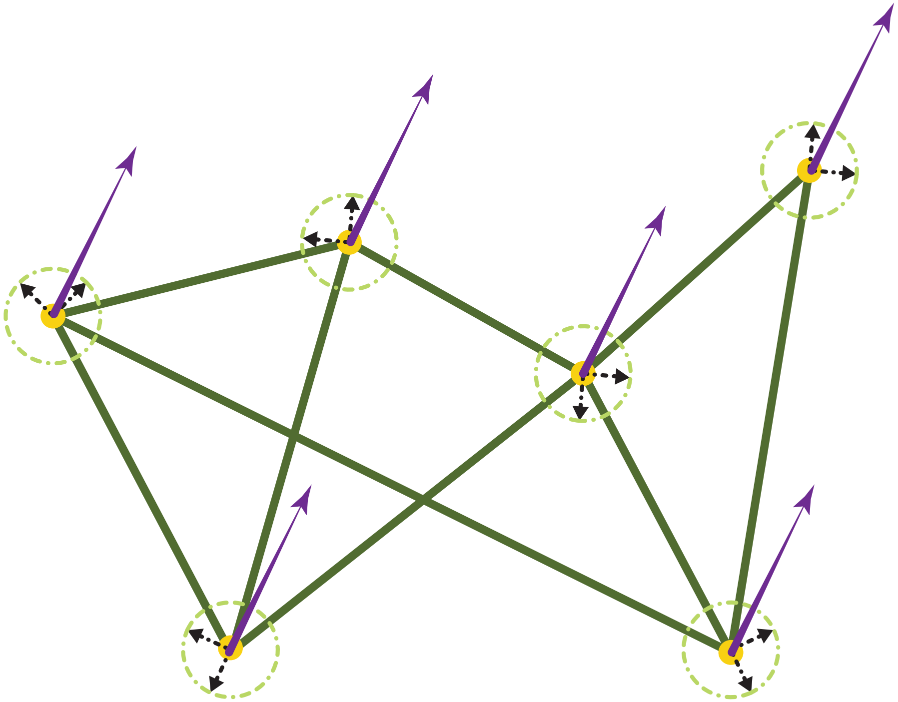
- Protocol characterized by two parameters:
  - Accuracy delta: $d(v_i, v_j) \leq \delta$
  - Probability of success q_{succ}: $q_{\text{succ}} \geq 1 - e^{\Omega(-n\delta^2)}$

The problem



- *m* players
- At most *t* of them are dishonest

The problem



- Must satisfy:
  - **Consistency:** Correct nodes P_i and P_j must ouput $d(v_i,v_j) \leq \eta$ for $\eta > 0$.

Adversary

- Faulty nodes (dishonest players)
  - Non-responding
  - Wrong message
  - Correlated errors
  - Controlled by an adversary

Communication model

- Complete graph
  - Direct link between each pair of players
- Public
  - Allows more powerful adversary
- Authenticated
  - Origin cannot be faked
  - Message cannot be altered
- Synchronous
  - Message transmissions are timed

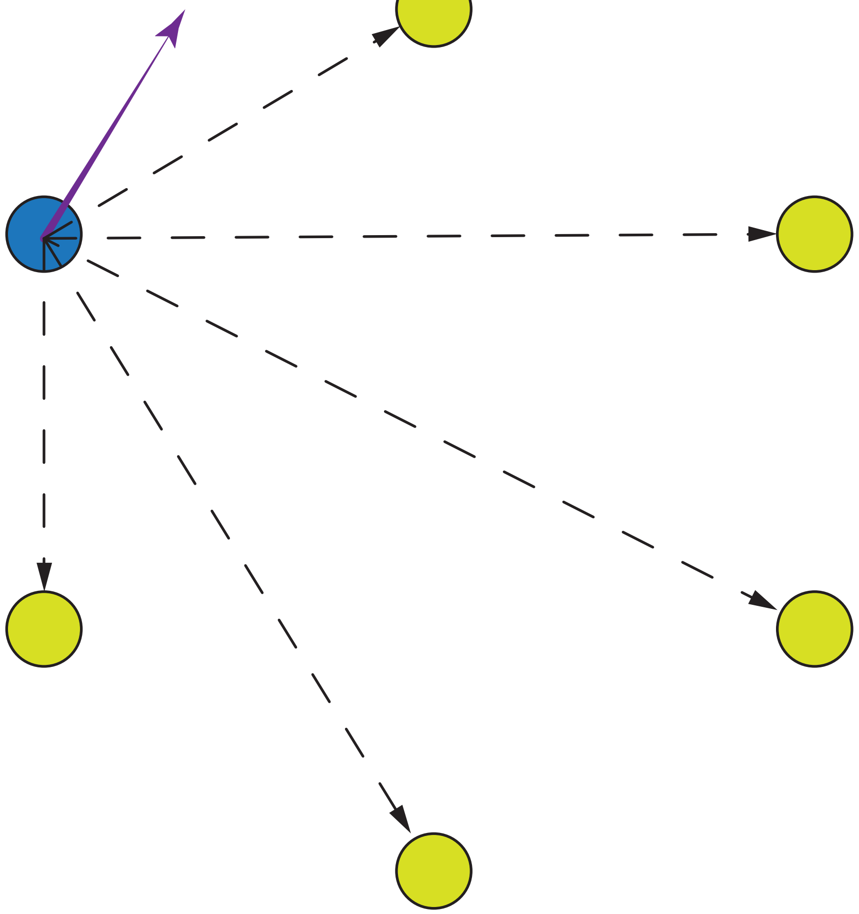
Result

- Our Protocol RF-Consensus
  - **Takes:** any 2-party $(\delta, q_{\text{succ}})$ protocol
  - **Gives:** m-party $(30\delta, q_{\text{succ}}^{m^2})$ reference frame agreement
  - **Tolerates:** dishonest $t < m/3$
- **Example**: using the simple 2ED
  - $q_{\text{succ}}^{m^2} \geq 1 - e^{-\Omega(n\delta^2 - \log m)}$
- Uses ideas from Classical protocol by Fitzi and Maurer

Fitzi and Maurer in Proc. ACM STOC'00 (2000)

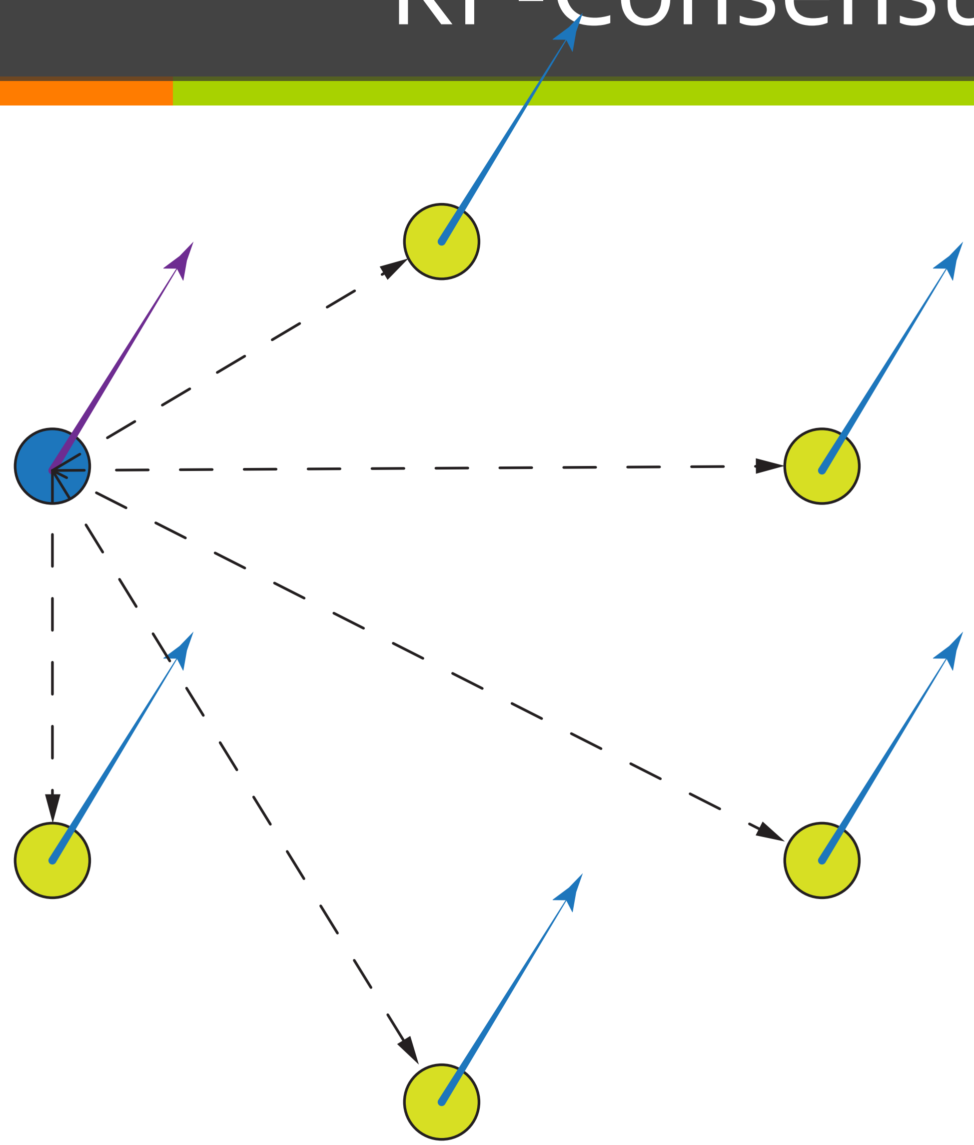
RF-Consensus

- An arbitrarily nominated player fixes a direction



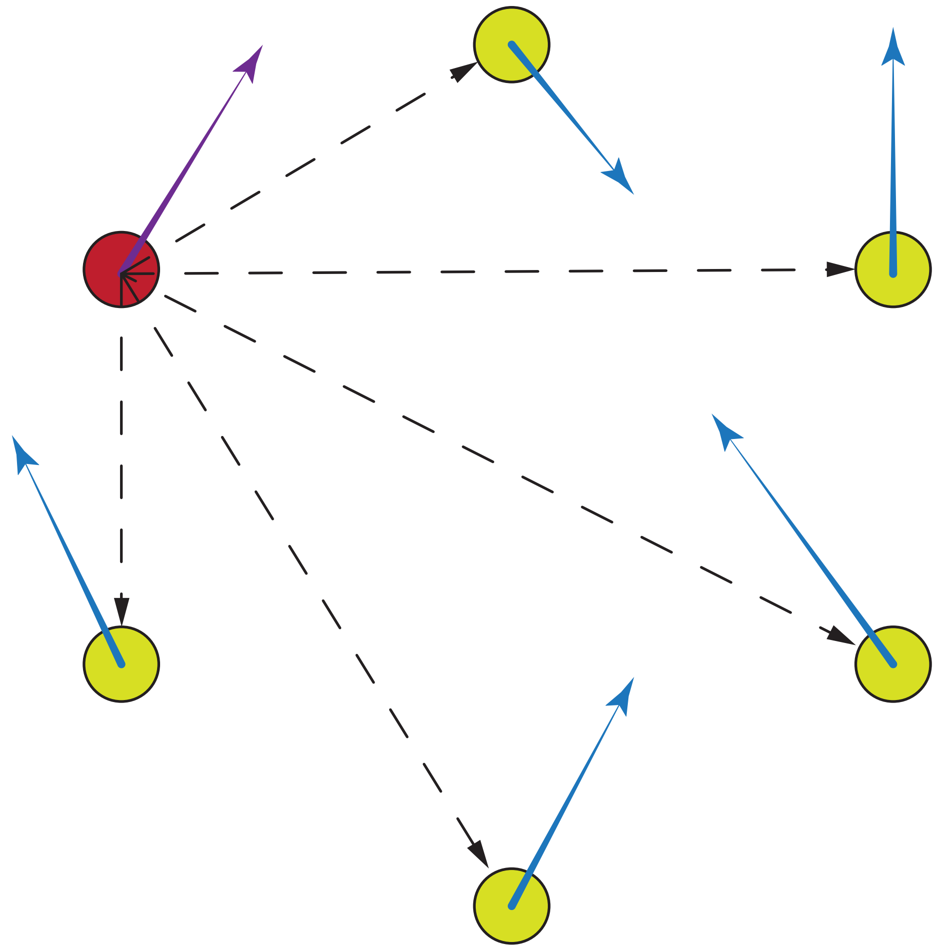
RF-Consensus

- Sends the direction to all the others using 2ED



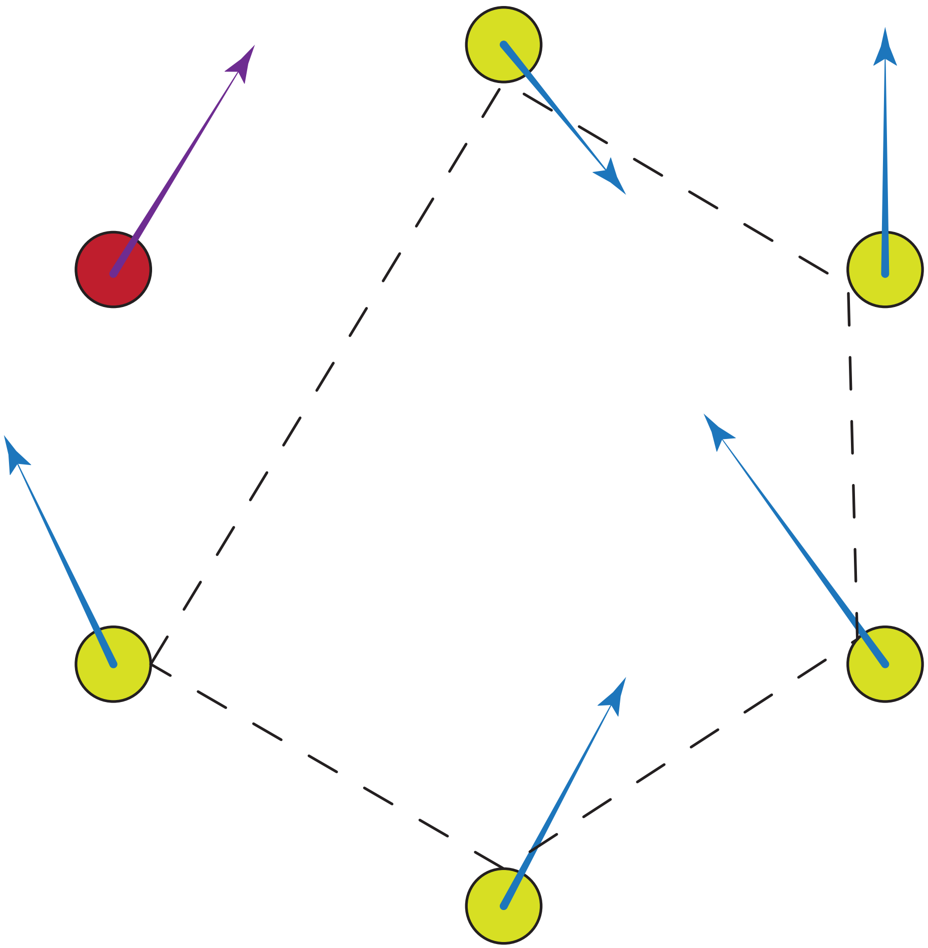
RF-Consensus

- But the chosen one could be dishonest



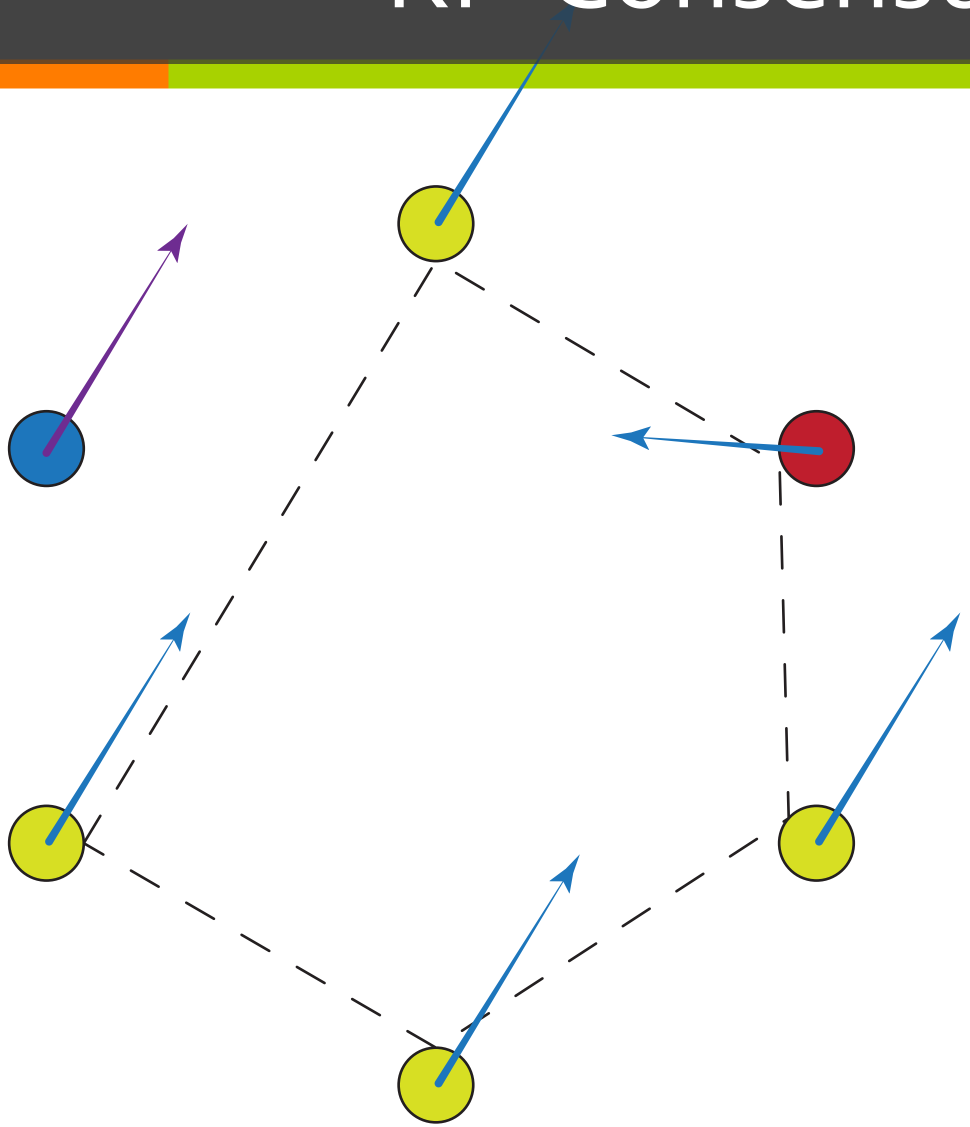
RF-Consensus

- So, verification needed.



RF-Consensus

- But some of the receivers might be dishonest



RF-Consensus

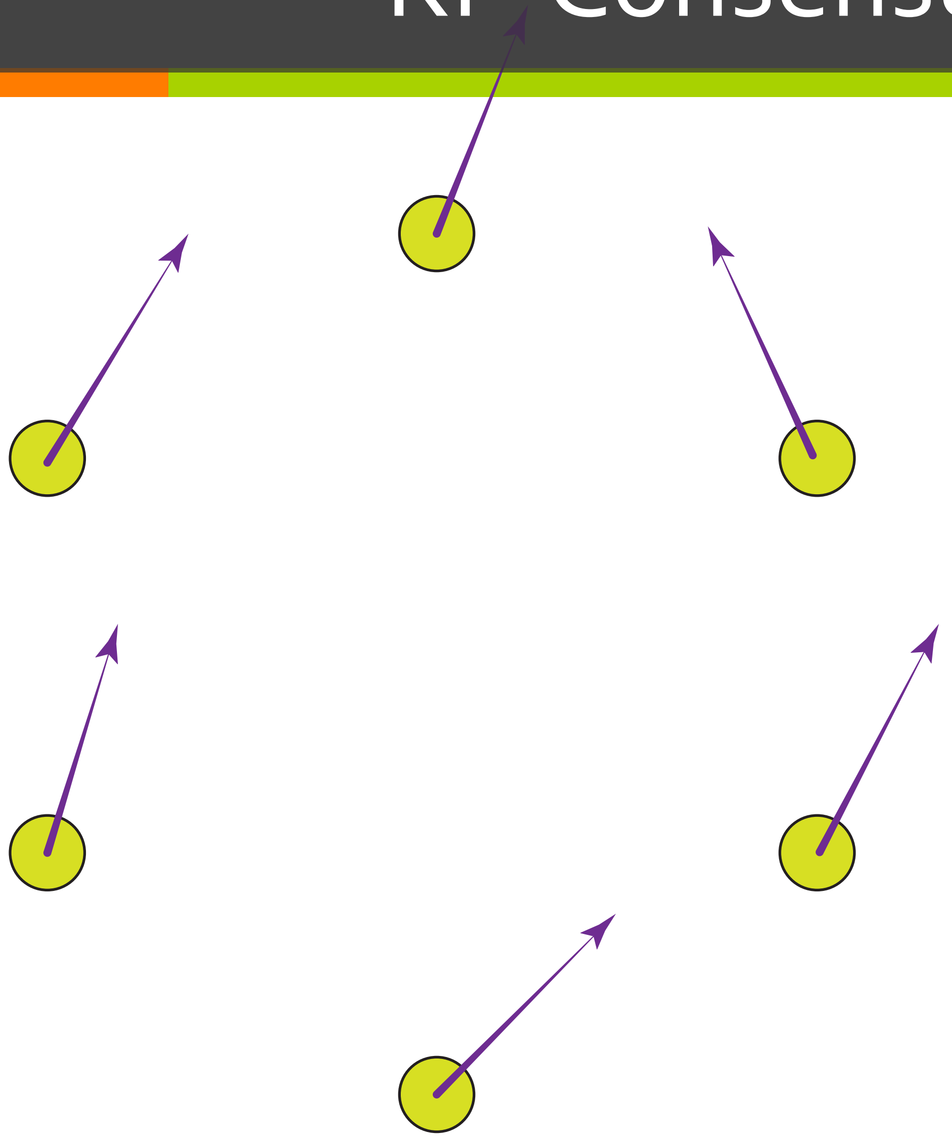
- **Persistency: (**honest king**)**
  - If there exists w_k such that $d(w_i, w_k) \leq \delta$
  - Then $d(v_i, w_k) \leq \delta$
- **Consistency: (**dishonest king**)**
  - Either, **all** honest P_i, P_k output $d(v_i, v_j) \leq \eta$
  - Or, they **all** output $\perp$

RF-Consensus

- **Persistency: (**honest king**)**
  - If there exists w_k such that $d(w_i, w_k) \leq \delta$
  - Then $d(v_i, w_k) \leq \delta$
- **Consensus: (**dishonest king**)**
  - Either, **all** honest P_i, P_k output $d(v_i, v_j) \leq \eta$
  - Or, they **all** output $\perp$
- **Weak consistency:**
  - If honest P_i and P_j output direction $v_i \neq \perp$ and $v_i \neq \perp$,
  - Then, $d(v_i, v_j) \leq \eta$

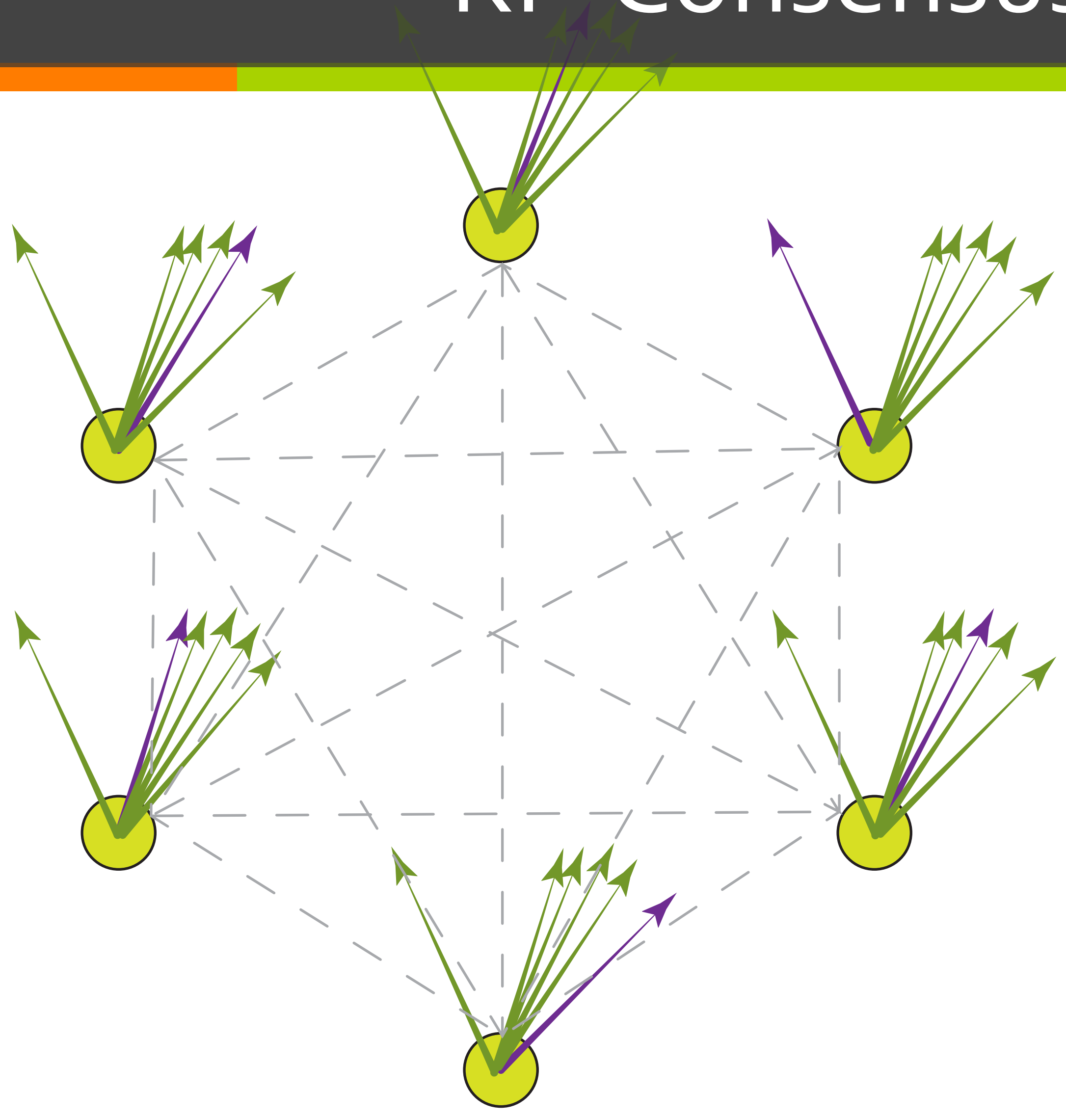
RF-Consensus

- Everyone starts with an arbitrary direction
- Which they might have received from a king

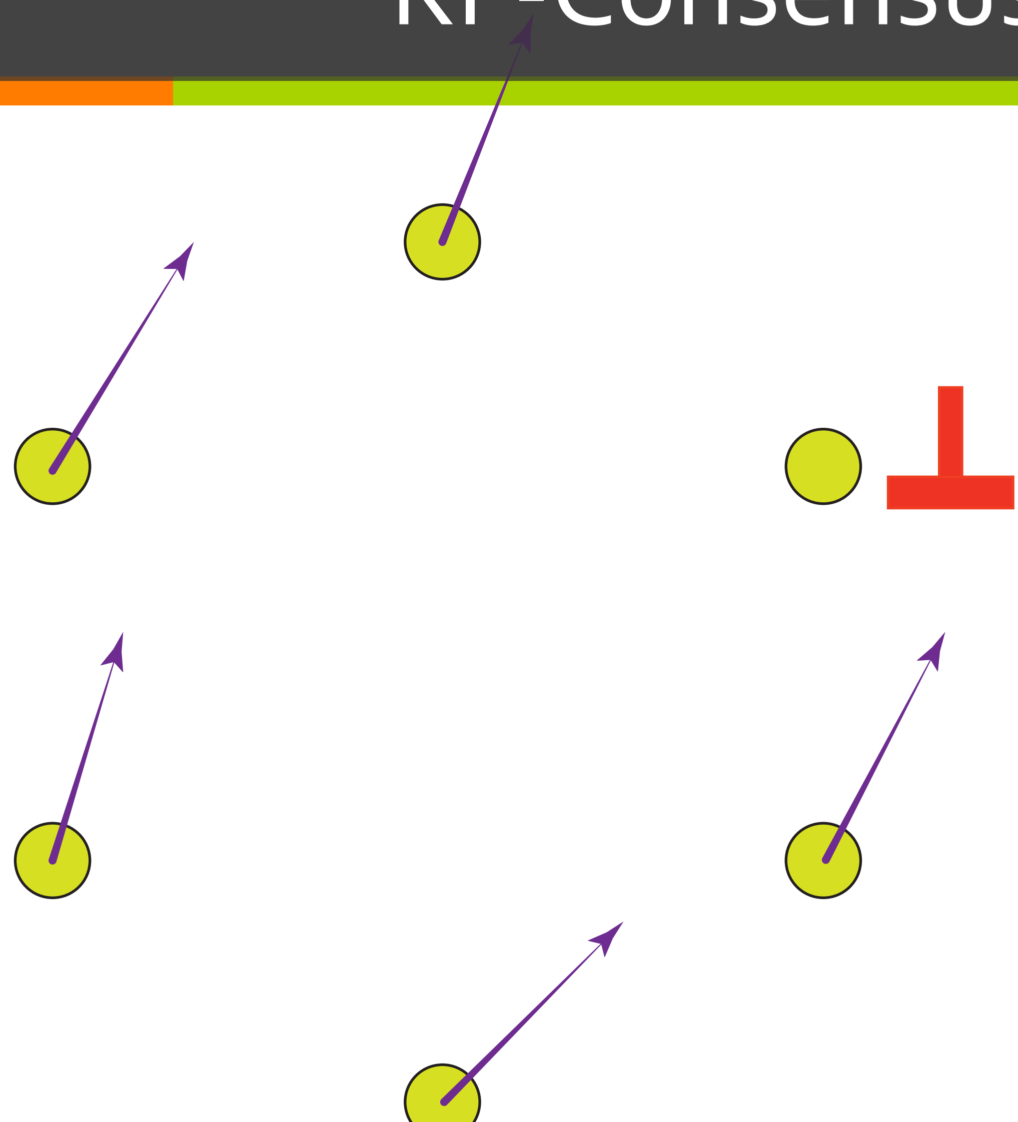


RF-Consensus

- Every one sends their direction to every one using 2ED

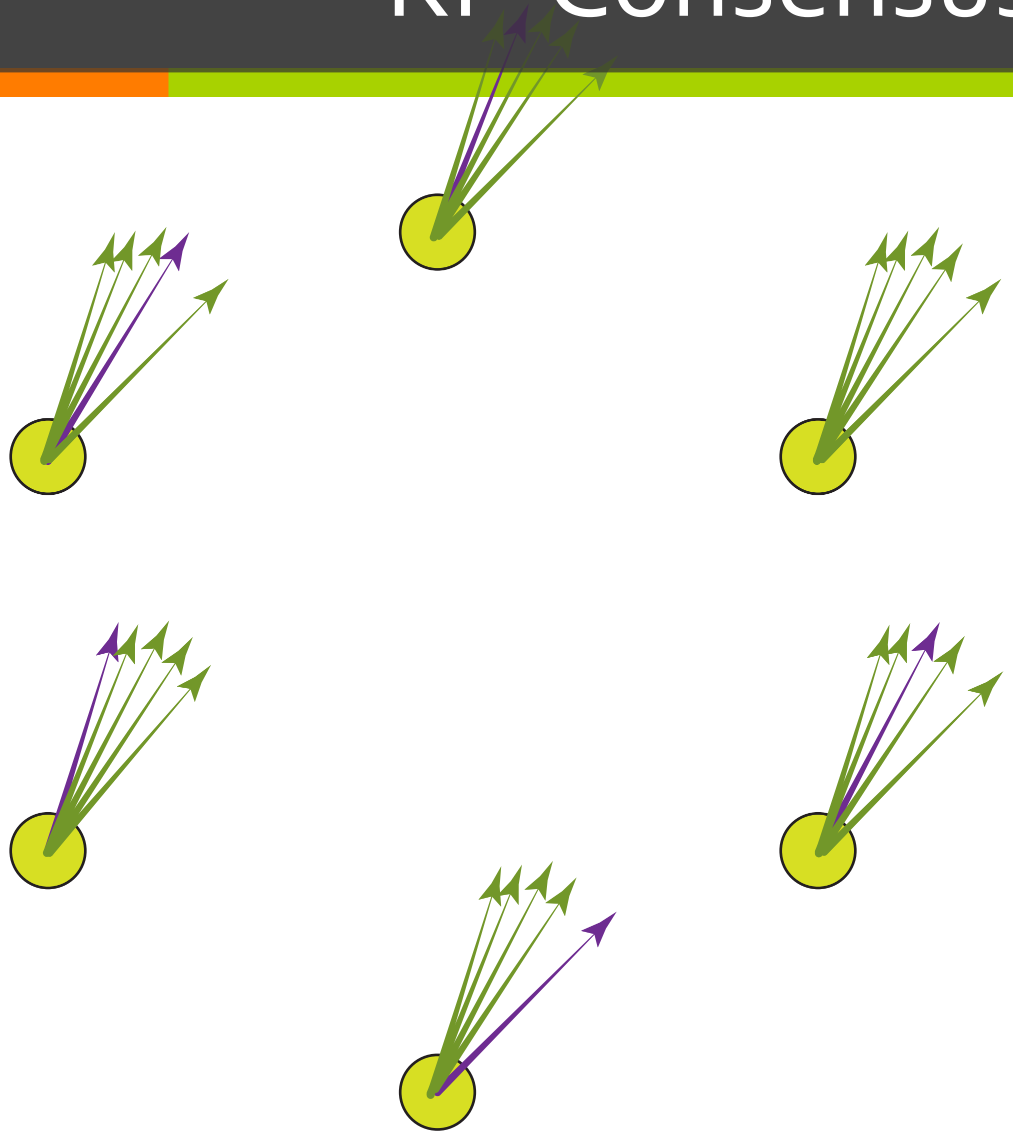


RF-Consensus



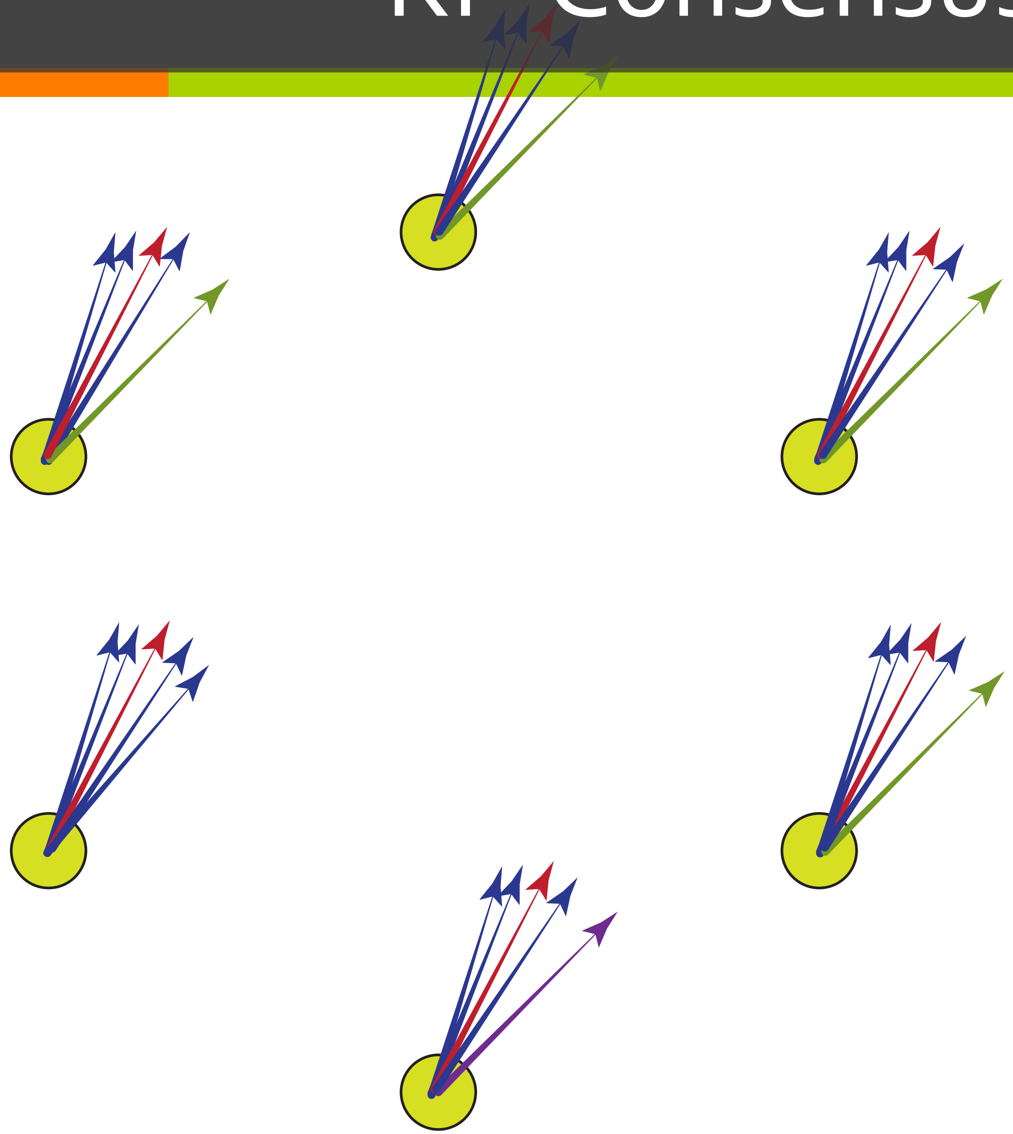
- If more than *2m/3* are close, keeps their own direction
- Else, announces ⊥
- This satisfies *8δ* weak consistency

RF-Consensus



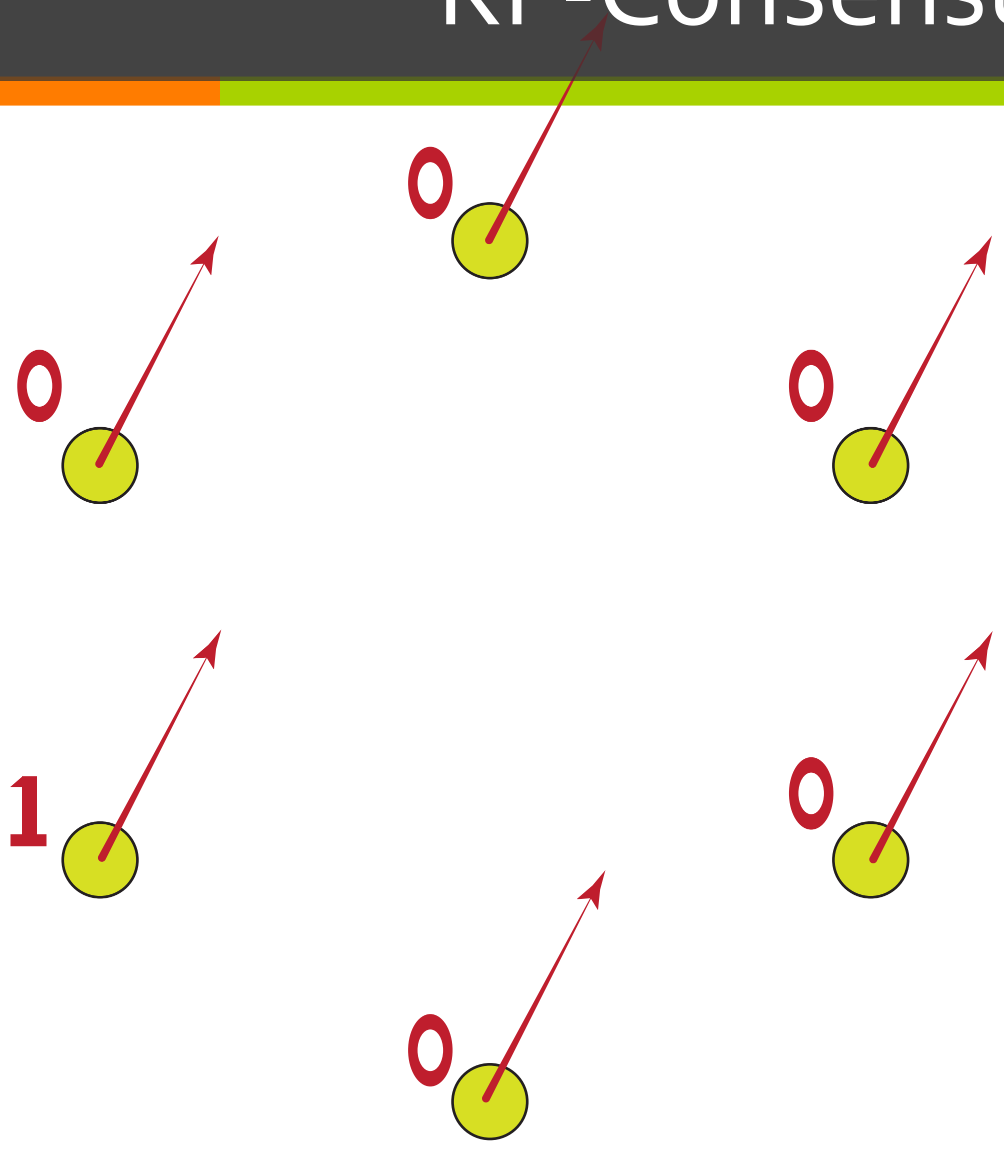
- Everyone removes the unfit
- And finds the largest cluster among the rest

RF-Consensus



- Outputs the cluster center
- Also outputs a grade bit

RF-Consensus

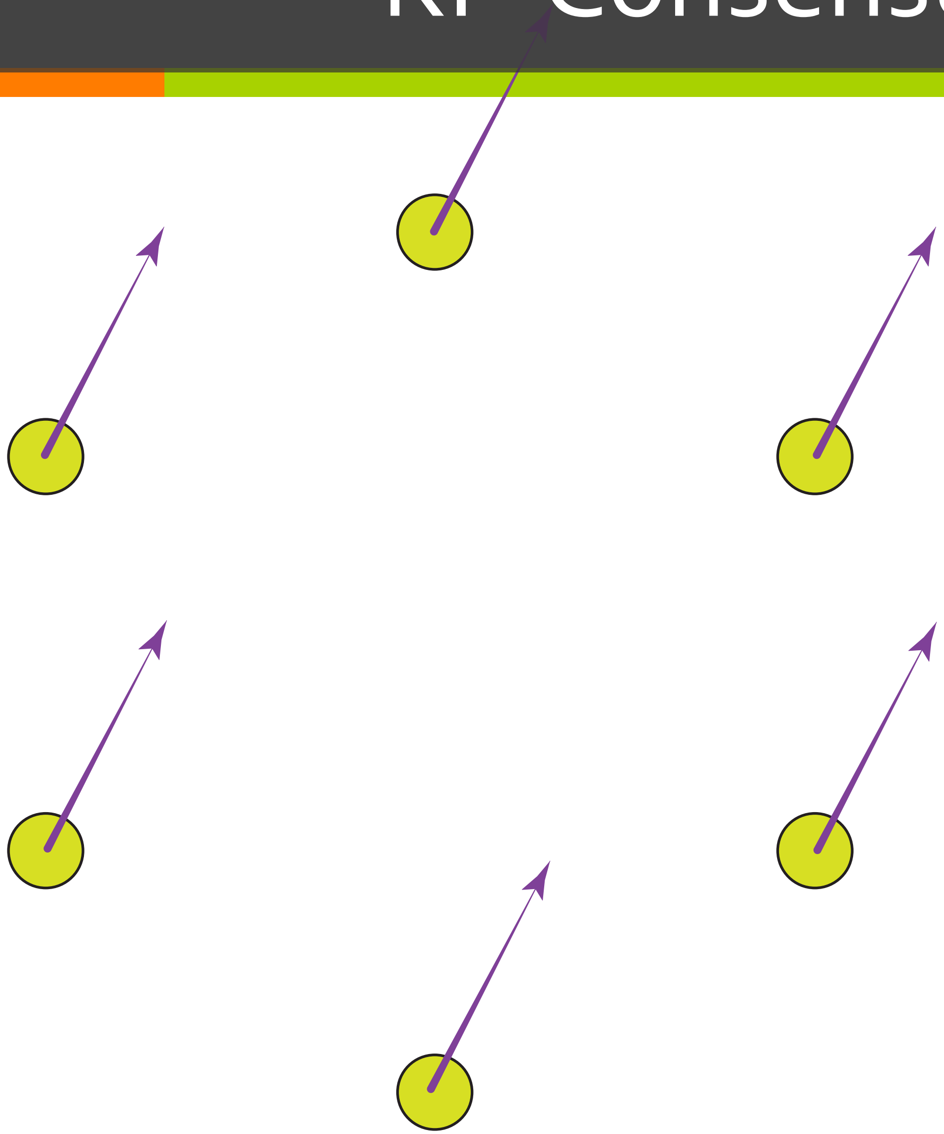


- If the cluster size more than 2m/3, grade = 1.
- They run A **classical consensus** with the grade bit as input

RF-Consensus

- **Graded consistency:**
  - If any honest P_i outputs grade $g_i = 1$
  - Then for all honest P_j and P_k, $d(v_j, v_k) \leq \eta = 30\delta$

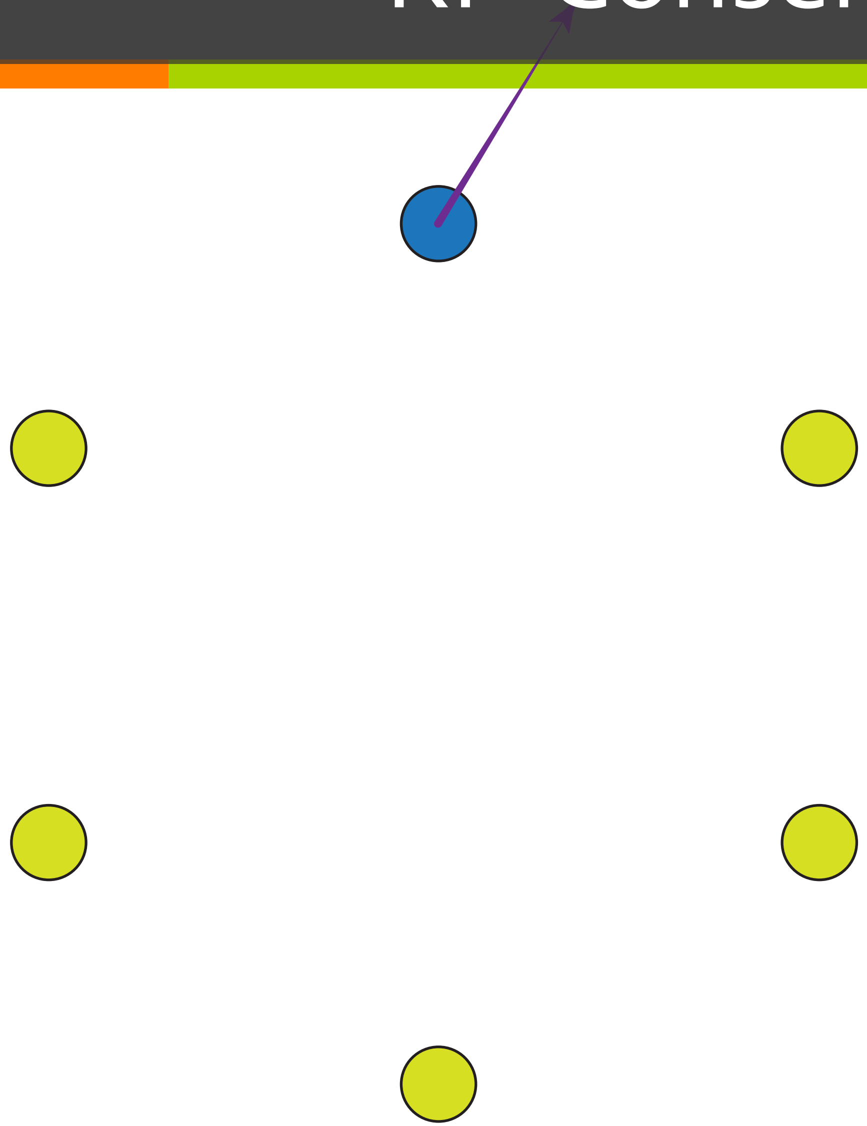
RF-Consensus



- If the **classical consensus** outputs 1
- Then a reference frame consensus is reached.

RF-Consensus

- If no consensus reached
- The game repeats with a new king



Future directions

- Improvement of the protocol
  - Can we do better than dishonest $t < m/3$?
    - $t < m/3$ would be optimal if qsucc = 1.
    - For constant error $t<m/2$ might be achievable [Yao']
  - Are there simpler protocol?
    - Can entanglement help?
- More realistic model
  - Asynchronous case
  - Different network topology

arXiv:1306.5295

Thank you!

This work is funded by the Ministry of Education (MOE) and National Research Foundation Singapore, as well as MOE Tier 3 Grant MOE2012-T3-1- 009.

Weak Persistency

Input: direction $w_{i,}$ **output**: direction u_i or $\perp$

1. *Send w_i to all other nodes*
2. *Receive $a_i[j]$ from node P_j*
3. *Create set S_i with nodes P_j for which $d(w_i, a_i[j]) \leq 3\delta$*
4. *If, $|S_i| > 2m/3$ then, output $u_i = w_{i,}$ else output $\perp$*

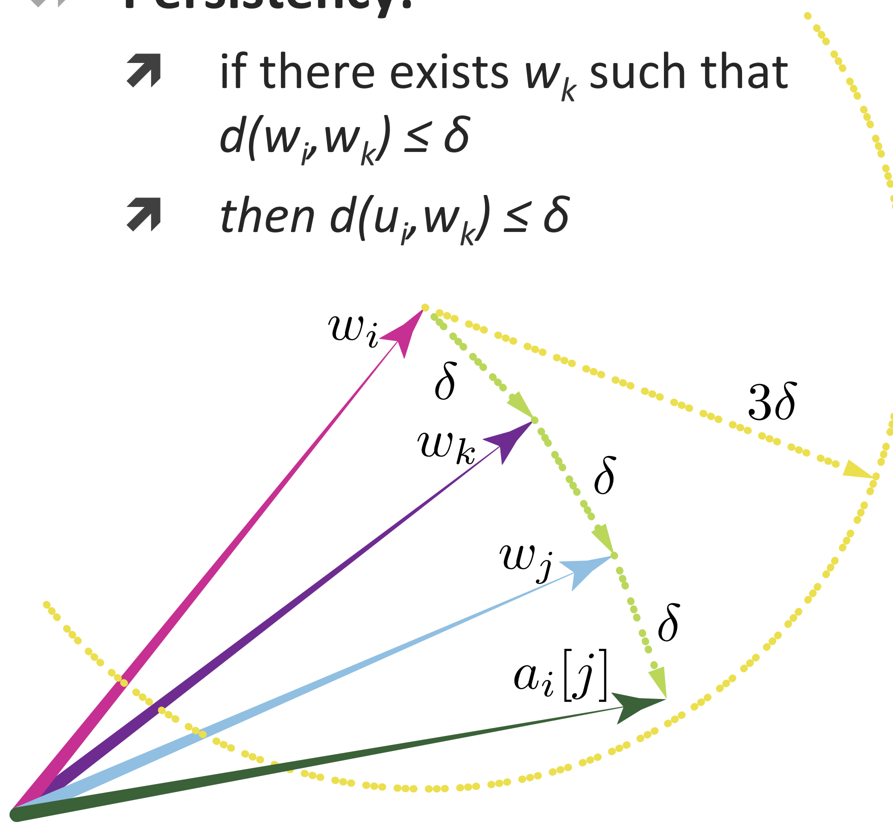
- **Weak persistency:**
  - if there exists w_k such that $d(w_i, w_k) \leq \delta$
  - then $d(u_i, w_k) \leq \delta$

Weak Persistency

Input: direction w_i, **output**: direction u_i or $\perp$

1. *Send w_i to all other nodes*
2. *Receive $a_i[j]$ from node P_j*
3. *Create set S_i with nodes P_j for which $d(w_i, a_i[j]) \leq 3\delta$*
4. *If, $|S_i| > 2m/3$ then, output $u_i = w_i$, else output $\perp$*

- **Persistency:**
  - if there exists w_k such that *$d(w_i, w_k) \leq \delta$*
  - *then $d(u_i, w_k) \leq \delta$*



Weak Consistency

Input: direction $w_{i,}$ **output**: direction u_i or $\perp$

1. *Send w_i to all other nodes*
2. *Receive $a_i[j]$ from node P_j*
3. *Create set S_i with nodes P_j for which $d(w_i, a_i[j]) \leq 3\delta$*
4. *If, $|S_i| > 2m/3$ then, output $u_i = w_{i,}$ else output $\perp$*

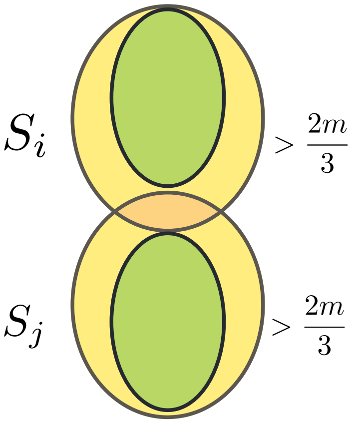
- **Weak consistency:**
  - If P_i and P_j output direction $u_i \neq \perp$ and $u_i \neq \perp$,
  - Then, $d(u_i, u_j) \leq \eta = 8\delta$

Weak Consistency

Input: direction w_i, **output**: direction u_i or $\perp$

1. *Send w_i to all other nodes*
2. *Receive $a_i[j]$ from node P_j*
3. *Create set S_i with nodes P_j for which $d(w_i, a_i[j]) \leq 3\delta$*
4. *If, $|S_i| > 2m/3$ then, output $u_i = w_i$, else output $\perp$*

- **Weak consistency:**
  - If P_i and P_j output direction $u_i \neq \perp$ and $u_j \neq \perp$,
  - Then, $d(u_i, u_j) \leq \eta = 8\delta$

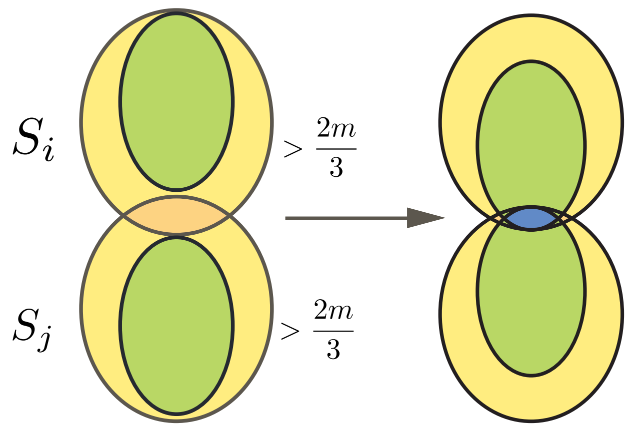


Weak Consistency

Input: direction $w_{i,}$ **output**: direction u_i or $\perp$

1. *Send w_i to all other nodes*
2. *Receive $a_i[j]$ from node P_j*
3. *Create set S_i with nodes P_j for which $d(w_i,a_i[j]) \leq 3\delta$*
4. *If, $|S_i| > 2m/3$ then, output $u_i = w_{i,}$ else output $\perp$*

- **Weak consistency:**
  - If P_i and P_j output direction $u_i \neq \perp$ and $u_i \neq \perp$,
  - Then, $d(u_i,u_j) \leq \eta = 8\delta$

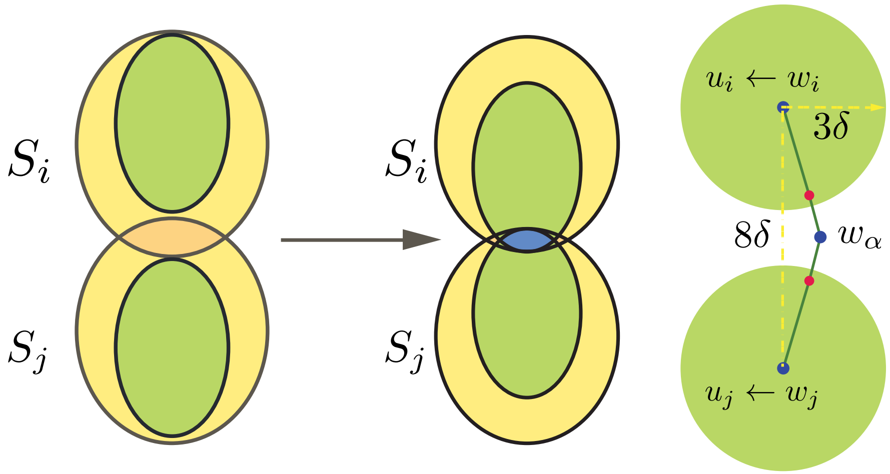


Weak Consistency

Input: direction $w_{i,}$ **output**: direction u_i or $\perp$

1. *Send w_i to all other nodes*
2. *Receive $a_i[j]$ from node P_j*
3. *Create set S_i with nodes P_j for which $d(w_i, a_i[j]) \leq 3\delta$*
4. *If, $|S_i| > 2m/3$ then, output $u_i = w_{i,}$ else output $\perp$*

- **Weak consistency:**
  - If P_i and P_j output direction $u_i \neq \perp$ and $u_j \neq \perp$,
  - Then, $d(u_i, u_j) \leq \eta = 8\delta$



Graded Consensus

Input: direction $w_{i,}$ **output:** direction $v_{i,}$ grade $g_i \in \{0, 1\}$

1. *Run Weak-Consensus(w_i)*
2. *For all the nodes $P_{j,}$ P_k which output non-$\perp$ create set $T_i[j] = \{P_k$: $d(a_i[j],a_i[k]) \leq 10\delta\}$*
3. *Assign $l_i = \arg\max\{|T_i[j]|\}$*
4. *Assign $v_i = a_i[l_i]$*
5. *If $|T_i[l_i]| \geq 2m/3$ then assign g_i=1, else g_i=0*
6. *Output ($v_{i,}g_i$)*

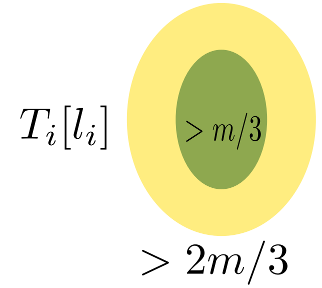
- **Graded consistency:**
  - If any honest P_i outputs grade g_i=1
  - Then for all honest P_j and P_k, $d(v_j,v_k) \leq \eta = 30\delta$

Graded Consensus

Input: direction $w_{i,}$ **output:** direction $v_{i,}$ grade $g_i \in \{0, 1\}$

1. *Run Weak-Consensus(w_i)*
2. *For all the nodes $P_{j,}$ P_k which output non-⊥ create set $T_i[j] = \{P_k$: $d(a_i[j],a_i[k]) \leq 10\delta\}$*
3. *Assign $l_i = \arg\max\{|T_i[j]|\}$*
4. *Assign $v_i = a_i[l_i]$*
5. *If $|T_i[l_i]| \geq 2m/3$ then assign g_i=1, else g_i=0*
6. *Output ($v_{i,}g_i$)*

- **Graded consistency:**
  - If any honest P_i outputs grade g_i=1
  - Then for all honest P_j and P_k, $d(v_j, v_k) \leq \eta = 30\delta$

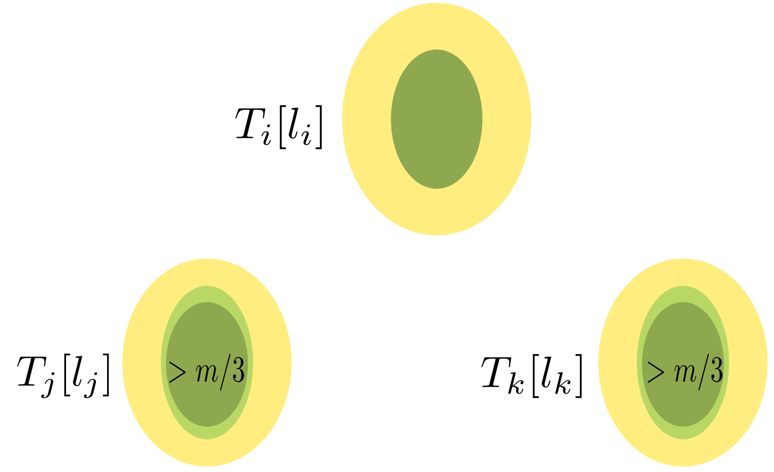


Graded Consensus

Input: direction w_i, **output:** direction v_i, grade $g_i \in \{0, 1\}$

1. *Run Weak-Consensus(w_i)*
2. *For all the nodes P_j, P_k which output non-$\perp$ create set $T_i[j] = \{P_k: d(a_i[j], a_i[k]) \leq 10\delta\}$*
3. *Assign $l_i = \arg\max\{|T_i[j]|\}$*
4. *Assign $v_i = a_i[l_i]$*
5. *If $|T_i[l_i]| \geq m - t$ then assign g_i=1, else g_i=0*
6. *Output (v_i,g_i)*

- **Graded consistency:**
  - If any honest P_i outputs grade g_i=1
  - Then for all honest P_j and P_k, $d(v_j, v_k) \leq \eta = 30\delta$

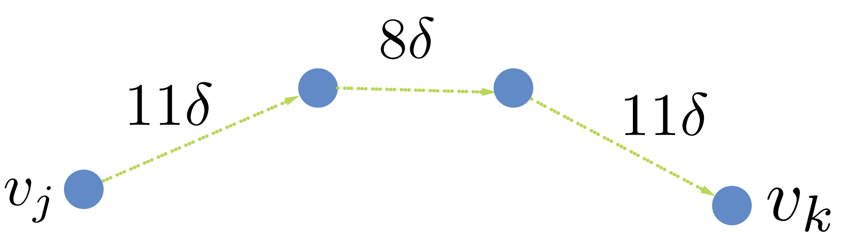


Graded Consensus

Input: direction $w_{i,}$ **output:** direction $v_{i,}$ grade $g_i \in \{0, 1\}$

1. *Run Weak-Consensus(w_i)*
2. *f*
3. *For all the nodes $P_{j,}$ P_k which output non-⊥ create set $T_i[j] = \{P_k: d(a_i[j],a_i[k]) \leq 10\delta\}$*
4. *Assign l_i = arg max$\{|T_i[j]|\}$*
5. *Assign $v_i = a_i[l_i]$*
6. *If $|T_i[l_i]| > 2m/3$ then assign g_i=1, else g_i=0*
7. *Output (v_i,g_i)*

- **Graded consistency:**
  - If any honest P_i outputs grade g_i=1
  - Then for all honest P_j and P_k, $d(v_j,v_k) \leq \eta = 30\delta$



Classical Consensus

- A protocol between *m* parties, in which each node starts with an input bit g_i and outputs a bit y_i.
- **Agreement:** All correct nodes should output the same bit;
- **Validity:** If all correct nodes start with the same input $g_i = b$, they should all output this value, that is $y_i = b$.
- Tolerant to $t < m/3$ faulty nodes