# Spatial reference frame agreement in quantum networks



2014 New J. Phys. 16 063040

(http://iopscience.iop.org/1367-2630/16/6/063040)

New Journal of Physics
The open access journal at the forefront of physics
Deutsche Physikalische Gesellschaft DPG | IOP Institute of Physics

# Spatial reference frame agreement in quantum networks

**Tanvirul Islam**[1,2], **Loïck Magnin**[1], **Brandon Sorg**[1] **and Stephanie Wehner**[1,2]
[1] Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543 Singapore, Singapore
[2] School of Computing, National University of Singapore, 13 Computing Drive, 117417 Singapore, Singapore
E-mail: tanvir@locc.la, loick@locc.la and steph@locc.la

Received 17 February 2014, revised 13 April 2014
Accepted for publication 24 April 2014
Published 17 June 2014
*New Journal of Physics* **16** (2014) 063040
doi:10.1088/1367-2630/16/6/063040

**Abstract**
In order to communicate information in a quantum network effectively, all network nodes should share a common reference frame. Here, we propose to study how well $m$ nodes in a quantum network can establish a common spatial reference frame from scratch, even though $t$ of them may be arbitrarily faulty. We present a protocol that allows all correctly functioning nodes to agree on a common reference frame as long as they are fully connected and not more than $t < m/3$ nodes are faulty. Our protocol furthermore has the appealing property that it allows any existing two-node protocol for reference frame agreement to be lifted to a protocol for a quantum network.

Keywords: quantum networks, reference frame agreement, quantum communication

Quantum networks are gaining importance [1] for a variety of tasks such as quantum distributed computing [2], quantum cloud computing [3] and quantum key distribution (see e.g. [4–7]). From the current architecture of the internet one can assume that any such network will contain a large number of nodes that are distributed over widespread geographical locations on Earth or on satellites [8–12] and connected via quantum and classical communication channels [13]. Some of the many challenges in building a quantum network spanning long distances include

how to perform quantum error correction [14] and construct quantum repeaters (see e.g. [15]). Yet, before we can hope to implement even such basic building blocks effectively, we would like all nodes in the quantum network to agree on a common reference frame to enable easy quantum communication.

A significant research effort has been devoted to developing protocols for agreeing on a reference frame between just two nodes [16–23]. Such protocols demand quantum communication because in the absence of a pre-shared reference frame, a node cannot meaningfully share directional information with a distant node by exchanging only classical data. Instead, a quantum system must be sent, for example, a qubit with its Bloch vector pointing in the required direction. A simple two-node protocol is thus to send many copies of the same qubit such that the receiver can approximate the direction with a certain level of accuracy.

Here, our goal is to allow $m > 2$ number of nodes in a quantum network to agree on a common spatial reference frame, where in this first work we assume a fully connected network graph. That is, every node is connected to every other node using both classical and quantum communication channels. Why is this problem any more difficult than solving the problem for two nodes? Note that in an ideal case, where all the nodes are perfect and the channels connecting them are error-free, one node can send a reference frame to everyone else, and everyone can subsequently use that as their common frame of reference. But one can see that in a practical network, where some of the nodes can be arbitrarily faulty this simple method will not work because if the sending node is faulty, then it might send a different frame to different receivers and thus cause different nodes to output different reference frames. That is, it can prevent them from *agreeing* on a *common* frame. Dealing with faulty nodes in a quantum network is challenging because we do not know *a priori* which nodes are faulty, and to make things even worse, the faulty nodes might have correlated errors. This is quite realistic in a practical setting where for example their hardware might have the same manufacturing defects, they might be located at a geographical location which is going through some disaster, or they might even be hijacked by an adversary trying to disrupt the network. Such arbitrarily correlated errors can all be characterized by imagining a worst case scenario in which the $t$ faulty nodes in the network are indeed actively cooperating to thwart our efforts in trying to establish a common reference frame.

To state the requirements for our protocol for establishing a common Cartesian reference frame, let us first clarify what it means to (approximately) agree on a frame. Let $v_i = \left(\alpha_i, \beta_i, \gamma_i\right)$ be the classical representation of the vector $\alpha_i\vec{x}_i + \beta_i\vec{y}_i + \gamma_i\vec{z}_i$ held by the node $P_i$, expressed relative to its local Cartesian frame $\left(\vec{x}_i, \vec{y}_i, \vec{z}_i\right)$. We denote $d\left(v_i, v_j\right)$ the Euclidean distance between the two vectors[3], expressed with respect to the same reference frame. That is, when considering the distance between vectors $v_i$ held by node $P_i$ and $v_j$ held by node $P_j$, we translate them into one fixed frame which without loss of generality we take to be the frame of the first node $P_i$. Informally, $P_i$ and $P_j$ thus (approximately) $\eta$-agree on a reference frame if $d\left(v_i, v_j\right) \leqslant \eta$ where $\eta$ is ideally small. We are now ready to define our goal.

[3] For unit vectors, $d$ takes values between 0 and 2.

**Definition 1.** For $\eta > 0$, a $\eta$-reference frame consensus protocol among $m$ network nodes is a protocol such that

| | |
|---|---|
| Termination | Each correct node $P_i$ terminates the protocol, and outputs a reference frame $v_i$. |
| Consistency | For all pairs of correct nodes $P_i$ and $P_j$ we have $d\left(v_i, v_j\right) \leqslant \eta$. |

Note that consistency does not require that all the correct nodes share the same reference frame ($\eta = 0$), but that each node has an approximation of it ($\eta$ is small). This is important because already any two-node protocol using only a finite number of rounds of communication cannot allow the two nodes to share a frame exactly.

## Results

We introduce the first protocol to solve the reference frame agreement problem in a quantum network of $m$ nodes of which $t < m/3$ can be arbitrarily faulty. Our protocol has the appealing feature that it can use any two-node protocol as a black box. Such two-node protocols [22] are characterized by the accuracy $\delta$ (i.e., the two nodes $\delta$-agree) and the success probability $q_{\text{succ}}$ with which such an approximation guarantee is achieved.

**Theorem 1.** *Given any two-node protocol to estimate a direction with accuracy $\delta$ and success probability $q_{\text{succ}}$, the protocol* RF-consensus *is a $(30\delta)$-reference frame consensus protocol tolerant to $t < m/3$ faulty nodes. It succeeds with probability at least $q_{\text{succ}}^{m^2}$.*

Our protocol is *efficient* as we need only a linear (in the number of nodes $m$) number of rounds of quantum communication. As an example, we take the simplest two-node protocol in which the sender encodes the direction in the Bloch vector of a qubit and sends $n$ identical copies of it to the receiver. For accuracy $\delta > 0$, the success probability of this two-node protocol is $q_{\text{succ}} \geqslant 1 - \mathrm{e}^{\Omega\left(-n\delta^2\right)}$. From this, we get the overall success probability of our protocol to be $q_{\text{succ}}^{m^2} \geqslant 1 - \mathrm{e}^{-\Omega\left(n\delta^2 - \log m\right)}$. We also show that this setting is *robust* to noise on the channel connecting any two nodes. To give some examples of parameters, protocol RF-consensus achieves accuracy $30\delta = 0.02$ with success probability 99% in a network of $m = 10$ nodes with noiseless communication, if each node transmits $n \approx 3.1 \times 10^8$ qubits at each round.

Our protocol uses ideas of [24] which solves a simpler problem from classical distributed computing called Byzantine agreement [25]; in particular we use classical consensus as a subroutine. This problem has been extensively studied using synchronous [26, 27] and asynchronous [28–31] classical communication, as well as quantum communication [32], also in a fail-stop model in which the faulty nodes can prevent the protocol from ever terminating [33]. There, the correct nodes should perfectly agree on a single classical bit. Recall that we cannot send a direction classically without a shared reference frame, and hence we cannot use such protocols. In addition, we face two extra challenges: first, we are dealing with a continuous set of outcomes; and second, it is impossible to transmit a direction perfectly using a finite amount of communication, even on an otherwise perfect channel. In quantum networks,

furthermore, we also have errors on the communication channel, which are pretty much unavoidable in a regime where we cannot easily perform quantum error correction due to the lack of a common frame. In the Byzantine problem such errors would be attributed to faulty nodes, but in our setting this would mean that *all* nodes in the network are faulty and no protocol could ever hope to succeed. Here, we thus require a careful treatment of such approximation errors.

### Model of communication

We assume that all the communication channels are public (faulty nodes can adapt their strategy depending on the network traffic), authenticated (faulty nodes cannot tamper with the channel connecting correct nodes), and synchronous (correct nodes know when they are supposed to receive a message, and if none is received, e.g. due to communication error, the protocol continues which ensures that our protocol cannot stall indefinitely).

We only use quantum communications to send a direction between a sender and a receiver. As an example we use protocol 2ED, one of the simplest possible protocols as studied in [16]. Here a sender creates many identical qubits with their Bloch vector pointing in the intended direction and the receiver measures them with Pauli measurements. From the statistics of the measurement outcomes, the receiver then estimates the Bloch vector's direction closely with high success probability. We use this protocol since it has some experimental advantages for implementation: it does not require any quantum memory or creation of entangled states, and it succeeds even if the quantum channel has a depolarizing noise. But the downside of this choice is that our protocol is not optimal in the number of qubits sent to achieve a certain accuracy. Optimal protocols [34–36] can align frames in the so-called Heisenberg limit [21], they have a quadratic gain over the one we use here.

**Protocol 1:** 2ED

**input** : Sender, direction $u$
**output**: Receiver, direction $v$

**Sender: 2ED-Send**
- Prepare $3n$ qubits with direction $u$
- Send them to the receiver

**Receiver: 2ED-Receive**
- Receive $3n$ qubits from the sender
- Measure $n$ qubits with $\sigma_x$ and compute $p_x$, the frequency of getting outcome $+1$
- Similarly on the remaining qubits, compute $p_y$ and $p_z$ with measurements $\sigma_y$ and $\sigma_z$ on $n$ qubits each
- Assign $x \leftarrow 2p_x - 1$, $y \leftarrow 2p_y - 1$, $z \leftarrow 2p_z - 1$
  Assign $l \leftarrow \sqrt{x^2 + y^2 + z^2}$
- Output $v \leftarrow (x/l, y/l, z/l)$

We prove the following theorem in the appendix.

**Theorem 2.** *For all $\delta > 0$, using a depolarizing channel $\rho \mapsto (1-\varepsilon)\rho + \varepsilon\mathbb{1}/2$ between the sender and the receiver, protocol 2ED provides to the receiver a $(1-\varepsilon)\delta + \frac{5\varepsilon}{2}$ approximation of the sender's direction. It succeeds with probability $q_{\text{succ}} \geqslant 1 - e^{-\Omega(\delta^2 n)}$.*

## Protocols

In this section, we present a summary of our protocols and an outline of their proof of correctness. For further detail, we refer to the appendix.

Our protocol works in two phases: first, a node is elected as the *king* $P_k$. Second, the king chooses a direction $w_k$ and sends it to all the other nodes. We denote $w_i$ the direction received by the node $P_i$ in its own frame. If the king is not faulty, 2ED ensures that $d\left(w_i, w_k\right) \leqslant \delta$. Then the correct nodes should decide either all to accept this direction (they output $v_i \approx w_k$ in their respective own frame), or all to reject it (output $\perp$). This second phase is known as *king-consensus*. More formally, a king-consensus protocol should satisfy two properties: *$\delta$-persistency*: if the king is not faulty, all the correct nodes $P_i$, should output $v_i$ such that $d\left(v_i, w_k\right) \leqslant \delta$; and *$\eta$-consistency*: All the correct nodes reach a consensus, that is, they either all output $\perp$, or they all output directions that are $\eta$-close to each other, i.e., for all correct nodes $P_i$ and $P_j$, the distance $d\left(v_i, v_j\right) \leqslant \eta$.

We repeat those two phases with different kings as long as a consensus is not reached. In particular, the protocol will terminate after at most $t + 1$ rounds since there are at most $t$ faulty nodes.

**Protocol 2:** RF-Consensus

**Input** : None
**Output** : $\forall i$, $P_i$ outputs direction $v_i$

**for** $k = 1$ *to* $t + 1$ **do**
  $v_i$ = King-Consensus($P_k$)
  **if** $v_i \neq \perp$ **then**
    Output $v_i$

The rest of this paper is thus devoted to constructing a king-consensus protocol, which is done in three steps.

*Step 1: Weak-consensus* We first create a weaker protocol than king-consensus by relaxing the condition that the correct nodes either *all* output a direction, or *all* output $\perp$. In a weak-consensus, *some* nodes can output $\perp$ and the others a direction. However we keep the condition that if two correct nodes $P_i$ and $P_j$ output directions $u_i$ and $u_j$, they should be close to each other. Formally, we define a *weak-consensus* protocol as a protocol with the following two properties: *$\delta$-weak persistency*: if there exists a direction $w_k$ such that for every correct node $P_i$, $d\left(w_i, w_k\right) \leqslant \delta$, then $d\left(u_i, w_k\right) \leqslant \delta$; and *$\eta$-weak consistency*: For every pair of correct nodes $P_i$ and $P_j$ which output $u_i \neq \perp$ and $u_j \neq \perp$ respectively, we have $d\left(u_i, u_j\right) \leqslant \eta$.

**Protocol 3:** Weak-Consensus

**Input** : $\forall i$, $P_i$ inputs direction $w_i$
**Output** : $\forall i$, $P_i$ outputs direction $u_i$ or $\perp$

Send $w_i$ to all other nodes
Receive $a_i[j] \leftarrow$ direction received from $P_j$
Create the set $S_i \leftarrow \{P_j : d(w_i, a_i[j]) \leq 3\delta\}$
**if** $|S_i| \geq m - t$ **then**
  Assign $u_i \leftarrow w_i$
**else**
  Assign $u_i \leftarrow \perp$
Output $u_i$

Protocol weak-consensus achieves $\delta$-weak persistency and $(8\delta)$-weak consistency with probability at least $q_{\text{succ}}^{m^2-m}$ where $\delta$ is the accuracy achieved with probability $q_{\text{succ}}$ by the two-node protocol used to send directions.

Here, with probability at least $q_{\text{succ}}^{m^2-m}$, for every correct node $P_i$ and $P_j$, $d\left(a_i[j], w_j\right) \leqslant \delta$. It is easy to see that this protocol is $\delta$-weak persistent. We sketch the proof of the weak consistency. Consider the sets $S_i$ and $S_j$ of two correct nodes $P_i$ and $P_j$. If $u_i \neq \perp$ and $u_j \neq \perp$, then $S_i$ and $S_j$ contains at least one correct node in common, let us call it $P_\alpha$. Thus,

$$\begin{aligned} d\left(u_i, u_j\right) &\leqslant d\left(u_i, a_i[\alpha]\right) + d\left(a_i[\alpha], w_\alpha\right) + d\left(w_\alpha, a_j[\alpha]\right) + d\left(a_j[\alpha], u_j\right) \\ &\leqslant 3\delta + \delta + \delta + 3\delta \\ &= 8\delta. \end{aligned}$$

*Step 2: Graded-consensus.* In a king-consensus protocol, the correct nodes should have a 'global' behavior, as they should all either output a direction or $\perp$, whereas in the weak-consensus each node has a 'local' strategy. A *graded-consensus* protocol behaves intermediately. Alongside a direction $v_i \neq \perp$ the nodes also output a grade $g_i \in \{0, 1\}$ which carries a 'global' property, namely, *η-graded consistency*: If *any* correct node outputs a grade 1, then the directions between *all* the correct nodes should be $\eta$-close to each other, that is, for every pair $(P_i, P_j)$ of correct nodes, $d\left(v_i, v_j\right) \leqslant \eta$.

**Protocol 4:** Graded-Consensus

**Input** : $\forall i$, $P_i$ inputs direction $w_i$
**Output** : $\forall i$, $P_i$ outputs direction $v_i$ and grade $g_i \in \{0, 1\}$

Run Weak-Consensus($w_i$)
// This initialises the variables $u_i$ and $a_i[j]$'s
**if** $u_i = \perp$ **then**
  Send flag $f_i = 0$ to all other nodes
**else**
  Send flag $f_i = 1$ to all other nodes
**for all the** *nodes* $P_j$ **do**
  $f_i[j] \leftarrow$ Receive $f_j$
**for all the** *nodes* $P_j$ *with* $f_i[j] = 1$ **do**
  Create set $T_i[j] \leftarrow \{P_k : f_i[k] = 1$, and $d(a_i[j], a_i[k]) \leq 10\delta\}$
Assign $l_i \leftarrow \arg\max\{|T_i[j]|\}$
**if** $f_i = 1$ **then**
  Assign $v_i \leftarrow w_i$
**else**
  Assign $v_i \leftarrow a_i[l_i]$
**if** $|T_i[l_i]| > m - t$ **then**
  Assign $g_i \leftarrow 1$
**else**
  Assign $g_i \leftarrow 0$
Output $(v_i, g_i)$

Protocol graded-consensus achieves $(30\delta)$-graded consistency. It succeeds with probability at least $q_{\text{succ}}^{m^2-m}$.

The main idea of graded-consensus is that the nodes which output $\perp$ in the weak-consensus inform the other nodes (by sending the flags $f_i$). The first consequence is that for all

correct nodes $P_\alpha$ and $P_\beta$ with $f_\alpha = f_\beta = 1$, $d\left(u_\alpha, u_\beta\right) \leqslant 8\delta$. The second consequence is that if a correct node has grade 1, then for all correct nodes $P_i$ and $P_j$, the sets $T_i$ and $T_j$ each contain at least one correct node, let us denote them $P_\alpha$ and $P_\beta$. Thus, $d\left(v_i, u_\alpha\right) \leqslant d\left(v_i, a_i\left[\alpha\right]\right) + d\left(a_i\left[\alpha\right], u_\alpha\right) \leqslant 10\delta + \delta = 11\delta$. Finally, we get, $d\left(v_i, v_j\right) \leqslant d\left(v_i, u_k\right) + d\left(u_k, u_l\right) + d\left(u_l, v_j\right) \leqslant 11\delta + 8\delta + 11\delta = 30\delta$.

*Step 3: King-consensus.* We are ready to present the king-consensus protocol that achieves $\delta$-persistency and $\left(30\delta\right)$-consistency. Our protocol uses classical-consensus as a subroutine. It solves a problem which is closely related to Byzantine agreement. Here, every node $P_i$ starts with a bit $g_i$ and outputs a bit $y_i$. All the correct nodes agree on a bit $b$, that is if $P_i$ is correct, $y_i = b$ where at least one of the correct nodes, $P_j$ has input $g_j = b$. Classical-consensus can be reached if there are $t < m/3$ faulty nodes; for an example of such protocol, see e.g. [37].

**Protocol 5:** King-Consensus

**Input** : Id of the king $P_k$.
**Output** : $\forall i$, $P_i$ outputs direction $v_i$ or $\perp$

```
if I am the king then
    Fix an arbitrary direction w_k
    Send w_k to all other nodes
else
    Receive w_i ← direction received from the king
Assign (v_i, g_i) ← Graded-Consensus(w_i)
Assign y_i ← Classical-Consensus(g_i)
if y_i = 1 then
    Output v_i
else
    Output ⊥
```

If the king is not faulty, then all the correct nodes will have grade $g_i = 1$. Hence the classical-consensus will also be reached with value $y_i = 1$. So, all the correct nodes will accept the direction shared by the king. If the king is faulty and yet the correct nodes reach a consensus with $y_i = 1$, it means that at least one correct node had grade 1. In this case the $\left(30\delta\right)$-graded consistency implies that $d\left(v_i, v_j\right) \leqslant 30\delta$ for all the correct nodes $P_i$ and $P_j$. As a consequence, king consensus is $(30\delta)$-consistent, and so is RF-consensus.

## Discussion

We have presented the first protocol for reference frame agreement in a quantum network. Even in the classical setting, the algorithms to solve the Byzantine agreement problem are surprisingly complicated. We would be very keen to know if simpler and more efficient protocols could be designed for our setting, possibly by using entangled states. It is an interesting open question to construct protocols that also work in an asynchronous communication model. The latter is already challenging for the classical case [28–31], so we expect a similar behavior to hold here. Another interesting question is whether more faulty nodes than $t < m/3$ can be tolerated. If our protocol were to succeed with probability 1 and $\eta$ sufficiently small, we can prove that it is optimal in that sense by adapting the classical proof

[38] to our setting. However, for equationing reference frames, any protocol can only succeed with probability strictly less than 1. This problem has been partially studied in the classical case [39]. Even in the constant error scenario the optimal number of faulty nodes that can be tolerated is not known for the classical Byzantine agreement problem [40]. This leaves hope to find protocols that can tolerate $t < m/2$ faulty nodes when allowing constant success probability both for Byzantine and reference frame agreement.

## Acknowledgments

We thank Esther Hänggi and Jürg Wullschleger for useful discussions.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.

## Appendix A. Estimating directions

In this section, we analyze the protocol 2ED to exchange a direction between two nodes. Since this cannot be done perfectly, the receiver has to *estimate* the direction sent by the sender. This task is formally defined by:

**Definition 2.** A *$\delta$-estimate direction* protocol is a two-node protocol where one node (the sender) sends a direction $u$ to the other node (the receiver). Upon termination the receiver gets a $\delta$-approximation $v$ of $u$, that is, $d\left(u, v\right) \leqslant \delta$.

This simple protocol has several advantages: it does not require any quantum memory or the creation of entangled states, and it succeeds even if the quantum channel has a depolarizing noise. But the downside of this choice is that the protocol is not optimal in the number of qubits sent to achieve a certain accuracy. Any other protocol can be used here [22].

**Protocol 1:** 2ED

**input** : Sender, direction $u$
**output** : Receiver, direction $v$

**Sender: 2ED-Send**
- Prepare $3n$ qubits with direction $u$
- Send them to the receiver

**Receiver: 2ED-Receive**
- Receive $3n$ qubits from the sender
- Measure $n$ qubits with $\sigma_x$ and compute $p_x$, the frequency of getting outcome $+1$
- Similarly on the remaining qubits, compute $p_y$ and $p_z$ with measurements $\sigma_y$ and $\sigma_z$ on $n$ qubits each
- Assign $x \leftarrow 2p_x - 1$, $y \leftarrow 2p_y - 1$, $z \leftarrow 2p_z - 1$; Assign $l \leftarrow \sqrt{x^2 + y^2 + z^2}$
- Output $v \leftarrow (x/l, y/l, z/l)$

**Theorem 2.** *For all $\delta > 0$, using a depolarizing channel $\rho \mapsto \left(1 - \varepsilon\right)\rho + \varepsilon\mathbb{1}/2$ between the sender and the receiver, protocol 2ED provides to the receiver a $\left(1 - \varepsilon\right)\delta + \frac{5\varepsilon}{2}$ approximation of the sender's direction. It succeeds with probability $q_{\text{succ}} \geqslant \left(1 - 2e^{\left(-2n\delta^2/25\right)}\right)^3$.*

**Proof.** We will prove this theorem in two steps. First, we consider the case when the communication channel is noise free ($\varepsilon = 0$), and then, we see how depolarizing noise affects the approximation factor.

In the noise-free case, let us fix $\delta > 0$ and denote by $\theta_x$, $\theta_y$, and $\theta_z$ the angles between $u$ and the $x$-, $y$-, and $z$-axis of the local frame of the receiver. So, $\cos^2\frac{\theta_x}{2}$ is the probability of getting outcome $+1$ after the Pauli measurement $\sigma_x$ on a qubit. Similarly, $\cos^2\frac{\theta_y}{2}$ and $\cos^2\frac{\theta_z}{2}$ are the probabilities for outcome $+1$ on measurement $\sigma_y$ and $\sigma_z$ respectively.

Now, we will show that each of the following three conditions:

$$\left| p_x - \cos^2\frac{\theta_x}{2} \right| \leqslant \delta/5, \tag{A.1}$$

$$\left| p_y - \cos^2\frac{\theta_y}{2} \right| \leqslant \delta/5, \tag{A.2}$$

$$\left| p_z - \cos^2\frac{\theta_z}{2} \right| \leqslant \delta/5, \tag{A.3}$$

holds with probability at least $\left(1 - 2e^{-\frac{2}{25}n\delta^2}\right)$, and later show that equations (A.1), (A.2), and (A.3) imply that $d\left(u, v\right) \leqslant \delta$.

We know in the ideal case, when $n \to \infty$ the relative frequency $p_x \to \cos^2\frac{\theta_x}{2}$ but in 2ED $n$ is finite. So, using Hoeffding's inequality we get,

$$Pr\left( \left| p_x - \cos^2\frac{\theta_x}{2} \right| > \frac{\delta}{5} \right) \leqslant 2\exp\left( -\frac{2n^2\delta^2}{25n} \right), \tag{A.4}$$

hence conditions (A.1), (A.2), and (A.3) are all satisfied with probability at least $\left(1 - 2e^{\left(-2n\delta^2/25\right)}\right)^3$. Denoting the vector $u$ in the receiver's basis by $\left(x_u, y_u, z_u\right)$, we have

$$x_u = \cos\theta_x = 2\cos^2\frac{\theta_x}{2} - 1. \tag{A.5}$$

So,

$$\left|x - x_u\right| = \left| \left(2p_x - 1\right) - \left(2\cos^2\frac{\theta_x}{2} - 1\right) \right|, \tag{A.6}$$

$$= 2\left| \left(p_x - \cos^2\frac{\theta_x}{2}\right) \right|, \tag{A.7}$$

$$\leqslant 2\delta/5. \tag{A.8}$$

Here, inequality (A.8) follows from inequality (A.1). Similarly we have,

$$y - y_u \leqslant 2\delta/5 \quad \text{and} \quad z - z_u \leqslant 2\delta/5. \tag{A.9}$$

Using (A.8) and (A.9), we get,

$$d\left((x, y, z), u\right) = \sqrt{\left(x - x_u\right)^2 + \left(y - y_u\right)^2 + \left(z - z_u\right)^2},$$

$$\leqslant \sqrt{\left(2\delta/5\right)^2 + \left(2\delta/5\right)^2 + \left(2\delta/5\right)^2}, \tag{A.10}$$

$$= \frac{2\sqrt{3}\,\delta}{5}. \tag{A.11}$$

This means that $(x, y, z)$ is within a sphere of radius $\frac{2\sqrt{3}\,\delta}{5}$ centered in $u$, so its angle $\theta$ with $u$ is at most $\arcsin\left(2\sqrt{3}\,\delta/5\right)$. Since $v$ is the normalization of $(x, y, z)$, its angle with $u$ is also $\theta$ and from a simple trigonometric observation, we have,

$$d(u, v) = 2\sin\left(\theta/2\right) \leqslant 2\sin\left(\frac{1}{2}\arcsin\left(2\sqrt{3}\,\delta/5\right)\right). \tag{A.12}$$

Moreover, one can check that for all $\alpha \in [0, 1]$, $\sin\left(\frac{1}{2}\arcsin(\alpha)\right) \leqslant \frac{5}{4\sqrt{3}}\alpha$, thus,

$$d(u, v) \leqslant \delta. \tag{A.13}$$

So far we have considered only a noiseless channel, let us now turn to the case of a depolarizing channel: if the sender sends a pure state $|\psi\rangle$, the receiver gets the mixed state

$$\rho = (1 - \varepsilon)|\psi\rangle\langle\psi| + \varepsilon\frac{\mathbb{I}}{2}. \tag{A.14}$$

From equation (A.14) one can see that the effective relative frequency $p_x$ is given by

$$p_x = (1 - \varepsilon)p'_x + \frac{\varepsilon}{2}, \tag{A.15}$$

where $p'_x$ is the relative frequency that the receiver would have got if the channel was noise-free, meaning that $\left|p'_x - \cos^2\frac{\theta_x}{2}\right| \leqslant \delta/5$. Therefore,

$$\left|p_x - \cos^2\frac{\theta_x}{2}\right| = \left|(1 - \varepsilon)p'_x + \frac{\varepsilon}{2} - \cos^2\frac{\theta_x}{2}\right|, \tag{A.16}$$

$$\leqslant \left|(1 - \varepsilon)\frac{\delta}{5} + \frac{\varepsilon}{2} - \varepsilon\cos^2\frac{\theta_x}{2}\right|, \tag{A.17}$$

$$\leqslant \left|(1 - \varepsilon)\frac{\delta}{5} + \frac{\varepsilon}{2}\right|, \tag{A.18}$$

$$= (1 - \varepsilon)\frac{\delta}{5} + \frac{\varepsilon}{2}. \tag{A.19}$$

Here inequality (A.18) follows because $\varepsilon\cos^2\left(\theta_x/2\right)$ is positive.

The rest of the analysis remains the same as the noise-free case by replacing $\delta/5$ by $\arcsin\left(2\sqrt{3}\,\delta/5\right)$ in equation (A.1). □

## Appendix B. Step 1: Weak-consensus

Let us start by giving a more formal definition of a weak-consensus protocol.

**Definition 3.** A $(\delta, \eta)$-weak-consensus protocol is a $m$-node protocol, in which each node $P_i$ has an input direction $w_i$ and outputs either a direction $u_i$ or $\perp$, that satisfies the following two properties:

| | |
|---|---|
| $\delta$-weak persistency | If there exists a direction $s$ such that for every correct node $P_i$, $d(s, w_i) \leqslant \delta$, then every correct node $P_i$ outputs a direction $u_i$ with $d(s, u_i) \leqslant \delta$. |
| $\eta$-weak consistency | For every pair of correct nodes $P_i$ and $P_j$ who output $u_i \neq \perp$ and $u_j \neq \perp$ respectively, we have $d(u_i, u_j) \leqslant \eta$. |

**Protocol 3:** Weak-Consensus

**Input** : $\forall i$, $P_i$ inputs direction $w_i$
**Output** : $\forall i$, $P_i$ outputs direction $u_i$ or $\perp$

1 Send $w_i$ to all other nodes
2 Receive $a_i[j] \leftarrow$ direction received from $P_j$
3 Create the set $S_i \leftarrow \{P_j : d(w_i, a_i[j]) \leq 3\delta\}$
4 **if** $|S_i| \geq m - t$ **then**
5 Assign $u_i \leftarrow w_i$
6 **else**
7 Assign $u_i \leftarrow \perp$
8 Output $u_i$

**Theorem 3.** *Using a two-node $\delta$-estimate direction protocol that succeeds with probability $q_{\text{succ}}$, the protocol weak-consensus is a $(\delta, 8\delta)$-weak consensus protocol tolerant to $t < m/3$ faulty nodes that succeeds with probability at least $q_{\text{succ}}^{m^2-m}$.*

**Proof.** After line 2, the property

$$\forall \text{ correct nodes } P_i, P_j, \quad d(a_i[j], w_j) \leqslant \delta, \tag{B.1}$$

holds with probability at least $q_{\text{succ}}^{m^2-m}$ since each of the $m$ nodes uses 2ED $m - 1$ times. The rest of the proof shows that Property (B.1) implies $\delta$-weak persistency and $8\delta$-weak consistency. This means that weak-consensus succeeds with probability at least $q_{\text{succ}}^{m^2-m}$.

*Weak persistency.* We assume there exists a direction $s$ such that the input $w_i$ of every correct node $P_i$ satisfies $d(s, w_i) \leqslant \delta$. Let $P_i$ be a correct node. We now show that $d(s, u_i) \leqslant \delta$. The idea is to show that $|S_i| \geqslant m - t$, hence $d(s, u_i) = d(s, w_i) \leqslant \delta$. This is done by showing that every correct node is in the set $S_i$. Indeed, let us consider a correct node $P_j$, then by triangular inequality we get,

$$d(w_i, a_i[j]) \leqslant d(w_i, s) + d(s, w_j) + d(w_j, a_i[j]). \tag{B.2}$$

Each of the first two terms is at most $\delta$ by assumption, and the last one is also at most $\delta$ by property (B.1). Thus,

$$d\left(w_i, a_i[j]\right) \leqslant 3\delta. \tag{B.3}$$

Since there are at least $(m - t)$ non faulty nodes, $\left|S_i\right| \geqslant \left(m - t\right)$. This completes the proof of the $\delta$-weak persistency.

*Weak consistency.* Let us consider two correct nodes $P_i$ and $P_j$ which output $u_i \neq \perp$ and $u_j \neq \perp$ respectively. Now we show that $d\left(u_i, u_j\right) \leqslant 8\delta$. The idea is to show that there exists a direction $w_\alpha$ such that $d\left(u_i, w_\alpha\right) \leqslant 4\delta$ and $d\left(u_j, w_\alpha\right) \leqslant 4\delta$. This is done by first showing that there exists one correct node $P_\alpha$ in both sets $S_i$ and $S_j$. For that, let us define the sets $C_i$ and $C_j$ by,

$$C_i = \left\{P_l\text{: } P_l \in S_i \text{ and node } P_l \text{ is correct}\right\}, \tag{B.4}$$

$$C_j = \left\{P_l\text{: } P_l \in S_j \text{ and node } P_l \text{ is correct}\right\}. \tag{B.5}$$

We need to prove that $C_i \cap C_j \neq \varnothing$. We do it by contradiction: let us assume that

$$C_i \bigcap C_j = \varnothing. \tag{B.6}$$

Note that,

$$\left|S_j\right| \geqslant m - t \Rightarrow \left|S_j - C_j\right| + \left|C_j\right| \geqslant m - t, \tag{B.7}$$

$$\Rightarrow t + \left|C_j\right| \geqslant m - t, \tag{B.8}$$

$$\Rightarrow \left|C_j\right| \geqslant m - 2t, \tag{B.9}$$

$$\Rightarrow \left|C_j\right| > \frac{m}{3}. \tag{B.10}$$

Inequality (B.8) follows because there can be at most $t$ faulty nodes, and inequality (B.10) since $t < \frac{m}{3}$. Now,

$$\left|S_i \cup S_j\right| = \left|\left(S_i - C_i\right) \cup \left(S_j - C_j\right) \cup C_i \cup C_j\right|, \tag{B.11}$$

$$= \left|\left(S_i - C_i\right) \cup \left(S_j - C_j\right)\right| + \left|C_i\right| + \left|C_j\right|, \tag{B.12}$$

$$\geqslant \left|\left(S_i - C_i\right)\right| + \left|C_i\right| + \left|C_j\right|, \tag{B.13}$$

$$= \left|\left(S_i - C_i\right) \cup C_i\right| + \left|C_j\right|, \tag{B.14}$$

$$= \left|S_i\right| + \left|C_j\right|, \tag{B.15}$$

$$\geqslant \left(m - t\right) + \left|C_j\right|, \tag{B.16}$$

$$> m - \frac{m}{3} + \frac{m}{3}. \tag{B.17}$$

Here, equation (B.12) follows from equation (B.6), and inequality (B.17) from inequality (B.10). We just proved that $\left|S_i \cup S_j\right| > m$ which contradicts the fact that there are exactly $m$ nodes. So, we have $C_i \cap C_j \neq \varnothing$.

Consider a correct node $P_\alpha \in \left(C_i \cap C_j\right)$. We have:

$$d\left(u_i, w_\alpha\right) = d\left(w_i, w_\alpha\right), \tag{B.18}$$

$$\leqslant d\left(w_i, a_i[\alpha]\right) + d\left(a_i[\alpha], w_\alpha\right), \tag{B.19}$$

$$\leqslant 3\delta + \delta. \tag{B.20}$$

The factor $3\delta$ comes from the fact that $P_\alpha$ is in $S_i$ and the remaining $\delta$ since $P_\alpha$ is correct. We can do the same reasoning with the node $P_j$, hence we also have:

$$d\left(u_j, w_\alpha\right) \leqslant 4\delta. \tag{B.21}$$

By combining equations (B.20) and (B.21), we prove the $8\delta$-weak consistency:

$$d\left(u_i, u_j\right) \leqslant d\left(u_i, w_k\right) + d\left(w_k, u_j\right) \leqslant 4\delta + 4\delta = 8\delta. \tag{B.22}$$

□

## Appendix C. Step 2: Graded-consensus

Again, we shall start by giving a formal definition of a graded-consensus protocol.

**Definition 4.** A $(\delta, \eta)$-graded consensus protocol is an $m$-party protocol, in which each node $P_i$ has an input direction $w_i$ and outputs a direction $v_i$ as well as a grade $g_i \in \{0, 1\}$, that satisfies the following properties:

| | |
|---|---|
| $\delta$-graded persistency | If there exists a direction $s$ such that for every correct node $P_i$, $d\left(s, w_i\right) \leqslant \delta$, then every correct node $P_i$ outputs a direction $v_i$ such that $d\left(s, v_i\right) \leqslant \delta$ and $g_i = 1$. |
| $\eta$-graded consistency | If there exists a correct node $P_c$ which outputs grade $g_c = 1$, then for all pairs $(P_i, P_j)$ of correct nodes, $d\left(v_i, v_j\right) \leqslant \eta$. |

**Protocol 4:** Graded-Consensus

**Input** : $\forall i$, $P_i$ inputs direction $w_i$
**Output** : $\forall i$, $P_i$ outputs direction and grade $g_i \in \{0, 1\}$

Run Weak-Consensus($w_i$)
// This initialises the variables $u_i$ and $a_i[j]$'s
**if** $u_i = \perp$ **then**
  Send flag $f_i = 0$ to all other nodes
**else**
  Send flag $f_i = 1$ to all other nodes
**forall the** *nodes* $P_j$ **do**
  $f_i[j] \leftarrow$ Receive $f_j$
**forall the** *nodes* $P_j$ *with* $f_i[j] = 1$ **do**
  Create set $T_i[j] \leftarrow \{P_k : f_i[k] = 1$, and $d(a_i[j], a_i[k]) \leq 10\delta\}$
Assign $l_i \leftarrow \arg\max\{|T_i[j]|\}$
**if** $f_i = 1$ **then**
  Assign $v_i \leftarrow w_i$
**else**
  Assign $v_i \leftarrow a_i[l_i]$
**if** $|T_i[l_i]| > m - t$ **then**
  Assign $g_i \leftarrow 1$
**else**
  Assign $g_i \leftarrow 0$
Output $(v_i, g_i)$

From line 2 to line 7, the nodes send and receive classical bits, there is no approximation here. An important consequence is that $f_i[j] = f_j$ whenever the nodes $P_i$ and $P_j$ are correct.

**Theorem 4.** *Consider that weak-consensus uses a $\delta$-estimate direction protocol that succeeds with probability $q_{\text{succ}}$. Protocol graded-consensus is a $(\delta, 30\delta)$-graded-consensus protocol tolerant to $t < m/3$ faulty nodes that succeeds with probability at least $q_{\text{succ}}^{m^2-m}$.*

**Proof.** Similarly to the weak-consensus protocol, with probability at least $q_{\text{succ}}^{m^2-m}$, the following property holds:

$$\forall \text{ correct nodes } P_i, P_j, \quad d(a_i[j], w_j) \leqslant \delta. \tag{C.1}$$

*Graded persistency.* We assume there exists a direction $s$ such that, for each correct node $P_i$, $d(s, w_i) \leqslant \delta$. We first show that every correct node $P_i$ outputs grade $g_i = 1$, and then show their output $v_i$ satisfies $d(s, v_i) \leqslant \delta$.

Let us consider a correct node $P_i$. It outputs $g_i = 1$ if and only if $|T_i[l_i]| \geqslant m - t$. To show that the later condition holds, we first show that for each of the $(m - t)$ correct nodes $P_j$ we $|T_i[j]| \geqslant m - t$. Therefore, by definition of $l_i$, we have $|T_i[l_i]| \geqslant |T_i[j]| \geqslant m - t$. This is proved by showing that for every correct node $P_\alpha$, we have $d(a_i[j], a_i[\alpha]) \leqslant 4\delta$, that is, every correct node $P_\alpha \in T_i[j]$.

Since the nodes $P_j$ and $P_\alpha$ are both correct, and weak-consensus is $\delta$-weak persistent, we know that $u_j \neq \perp$, $u_\alpha \neq \perp$ with

$$d(s, u_j) \leqslant \delta \quad \text{and} \quad d(s, u_\alpha) \leqslant \delta. \tag{C.2}$$

As a consequence $f_i[j] = f_i[\alpha] = 1$. We also know that $a_i[j]$ and $a_i[\alpha]$ are $\delta$-approximations of $u_j$ and $u_\alpha$ respectively, that is,

$$d(a_i[j], u_j) \leqslant \delta \quad \text{and} \quad d(a_i[\alpha], u_\alpha) \leqslant \delta. \tag{C.3}$$

Using the triangular inequality again with the inequalities (C.2) and (C.3), we get,

$$\begin{aligned} d(a_i[j], a_i[\alpha]) &\leqslant d(a_i[j], u_j) + d(u_j, s) \\ &\quad + d(s, u_\alpha) + d(u_\alpha, a_i[\alpha]), \qquad \text{(C.4)} \\ &\leqslant 4\delta. \qquad \text{(C.5)} \end{aligned}$$

Since $f_i[j] = 1$, the set $T_i[j]$ exists, and since $f_i[\alpha] = 1$ and $d(a_i[j], a_i[\alpha]) \leqslant 4\delta \leqslant 10\delta$, $P_\alpha \in T_i[j]$. This proves that $g_i = 1$.

Now, let us show that $d(s, v_i) \leqslant \delta$. By $\delta$-weak persistency, we know that $u_i \neq \perp$, therefore, $f_i = 1$. In this case, line 12 assigns $v_i \leftarrow w_i$. As a direct consequence, we get, $d(s, v_i) = d(s, w_i) \leqslant \delta$. This concludes the proof of the $\delta$-graded persistency.

*Graded consistency.* Let us assume that there exists a correct node $P_c$ that outputs grade 1. In this case we show that for any two correct nodes $P_i$ and $P_j$, the distance $d(v_i, v_j) \leqslant 30\delta$.

This proof is in three steps. First, we will show that all the correct nodes that are in the sets created at line 9 are close to each other. More precisely, we will show that for all the correct nodes $P_\alpha$ and $P_\beta$ with $f_\alpha = f_\beta = 1$, we have $d\left(u_\alpha, u_\beta\right) \leqslant 8\delta$. The second step shows that $v_i$ and $v_j$ are $11\delta$-close to some $u_\alpha$ and $u_\beta$ respectively where $P_\alpha$ and $P_\beta$ are correct nodes with $f_\alpha = f_\beta = 1$. The last step combines these two facts to conclude the proof.

*Step (1)*: This first step is a consequence of the $8\delta$-weak consistency of the weak-consensus protocol used at line 1. Indeed, consider two correct nodes $P_\alpha$ and $P_\beta$ such that $f_\alpha = f_\beta = 1$. This means that $u_\alpha \neq \perp$ and $u_\beta \neq \perp$, hence they satisfy

$$d\left(u_\alpha, u_\beta\right) \leqslant 8\delta. \tag{C.6}$$

*Step (2)*: We now prove that there exists a correct node $P_\alpha$ such that $d\left(v_i, u_\alpha\right) \leqslant 11\delta$. There are two cases to consider here. First $f_i = 1$: in this case, the correct node $P_i$ outputs $v_i = u_i$, thus $d\left(v_i, u_i\right) = 0 \leqslant 11\delta$. The more interesting case is $f_i = 0$. We are going to show that in this case, there exists a correct node $P_\alpha \in T_i\left[l_i\right]$. This is done by showing that the number of nodes in the set $T_i\left[l_i\right]$ is more than the number of faulty nodes, that is, $\left|T_i\left[l_i\right]\right| > m/3$. In a similar way to the graded persistency, we will in fact prove that for every correct node $P_k$ with $f_k = 1$, $\left|T_i[k]\right| > m/3$, hence $\left|T_i\left[l_i\right]\right| \geqslant \left|T_i[k]\right| \geqslant m/3$.

Let us then consider a correct node $P_k$ with $f_k = 1$. By equation (C.6), we have $d\left(u_k, u_{k'}\right) \leqslant 8\delta$ for every correct node $P_{k'}$ with $f_{k'} = 1$. As a consequence, we also have

$$\begin{aligned} d\left(a_i[k], a_i\left[k'\right]\right) &\leqslant d\left(a_i[k], u_k\right) + d\left(u_k, u_{k'}\right) + d\left(u_{k'}, a_i\left[k'\right]\right), \\ &\leqslant \delta + 8\delta + \delta. \end{aligned} \tag{C.7}$$

This with line 9 implies that the set $T_i[k]$ contains every correct node $P_{k'}$ with $f_{k'} = 1$. Let us argue that there are more than $m/3$ such correct nodes. Recall that we have assumed that the correct node $P_c$ has outputted grade $g_c = 1$. We thus have $\left|T_c\left[l_c\right]\right| > \left(m - t\right)$. We also know that there are at most $t < \frac{m}{3}$ faulty nodes. So, there must be at least $m - 2t > \frac{m}{3}$ correct nodes in $T_c\left[l_c\right]$, that is, there are more than $m/3$ correct nodes $P_{k'}$ with $f_{k'} = 1$.

We just proved that there exists at least one correct node $P_\alpha$ in $T_i\left[l_i\right]$, therefore,

$$d\left(v_i, u_\alpha\right) = d\left(a_i\left[l_i\right], u_\alpha\right), \tag{C.8}$$

$$\leqslant d\left(a_i\left[l_i\right], a_i[\alpha]\right) + d\left(a_i[\alpha], u_\alpha\right), \tag{C.9}$$

$$\leqslant 10\delta + \delta. \tag{C.10}$$

Using similar arguments, there exists at least one correct node $P_\beta$ such that

$$d\left(v_j, u_\beta\right) \leqslant 11\delta. \tag{C.11}$$

*Step (3)*: Now using triangular inequality with inequalities (C.10), (C.6), and (C.11) we get,

$$d\left(v_i, v_j\right) \leqslant d\left(v_i, u_\alpha\right) + d\left(u_\alpha, u_\beta\right) + d\left(u_\beta, v_j\right), \tag{C.12}$$

$$\leqslant 11\delta + 8\delta + 11\delta. \tag{C.13}$$

This proves the $(30\delta)$-graded consistency of the protocol. □

## Appendix D. Step 3: King-consensus

**Definition 5.** A $(\delta, \eta)$-king-consensus protocol is an $m$-node protocol in which one node $P_k$, called the king, chooses a direction $w_k$ and each of the other nodes $P_i$ outputs either a direction $v_i$ or each of them outputs $\perp$, which satisfies the following two properties:

$\delta$-persistency If the king is correct, then all the correct nodes $P_i$ output $v_i \neq \perp$ with $d\left(w_k, v_i\right) \leqslant \delta$.

$\eta$-consistency All correct nodes reach a consensus, that is, they either all output $\perp$, or they all output directions that are $\eta$-close to each other, i.e., for all correct nodes $P_i$ and $P_j$, the distance $d\left(v_i, v_j\right) \leqslant \eta$.

Our protocol to solve the king-consensus problem uses graded-consensus and classical-consensus as subroutines. The latter is a protocol between $m$ nodes, in which each node starts with an input bit $g_i$ and outputs a bit $y_i$, that satisfies the following two properties:

*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 $y_i = b$.

Classical-consensus is tolerant to $t < m/3$ faulty nodes (for a protocol see, e.g., [37]).

**Protocol 5:** King-Consensus

```
Input  : Id of the king P_k.
Output : ∀i, P_i outputs direction v_i or ⊥
if I am the king then
    Fix an arbitrary direction w_k
    Send w_k to all other nodes
else
    Receive w_i ← direction received from the king
Assign (v_i, g_i) ← Graded-Consensus(w_i)
Assign y_i ← Classical-Consensus(g_i)
if y_i = 1 then
    Output v_i
else
    Output ⊥
```

**Theorem 5.** *Using a $\delta$-estimate direction protocol that succeeds with probability $q_{\text{succ}}$, king-consensus is a $(\delta, 30\delta)$-king-consensus protocol that succeeds with probability at least $q_{\text{succ}}^{m^2}$.*

**Proof.** *Persistency.* Let us assume that the king is correct. We want to show that every correct node $P_i$ outputs $v_i \neq \perp$ with $d\left(w_k, v_i\right) \leqslant \delta$. Since the king is non faulty, with probability at least $q_{\text{succ}}^{m}$, we have that for all correct players $P_i$, the distance $d\left(w_k, w_i\right) \leqslant \delta$.

From the $\delta$-graded persistency of graded-consensus used in line 6, we know that for all correct nodes $P_i$, $d\left(v_i, w_k\right) \leqslant \delta$ and $g_i = 1$ with success proability at least $q_{\text{succ}}^{m^2}$; and from the validity of classical-consensus, we have that $y_i = 1$ for all correct nodes $P_i$. Hence all the correct nodes output a $\delta$-approximation of $w_k$ with probability at least $q_{\text{succ}}^{m^2}$.

*Consistency.* To prove consistency we will show that all the correct nodes output $\perp$, or they all output a direction. In this case we also have to show that for every pair $\left(P_i, P_j\right)$ of correct nodes, $d\left(v_i, v_j\right) \leqslant 30\delta$.

Since the variables $y_i$ are outputs of classical-consensus, the agreement property ensures that there exists a bit $b$ such that for all the correct nodes $P_i$, $y_i = b$.

If $b = 0$, all the correct nodes output $\perp$.

If $b = 1$, by validity of classical-consensus, at least one of the correct nodes, let us denote it by $P_i$, has flag $g_i = 1$. Recall that the $(30\delta)$-graded consistency of graded-consensus says that we have in this case $d\left(v_i, v_j\right) \leqslant 30\delta$ for every correct node $P_i$ and $P_j$. □

## References


[1] Kimble H J 2008 *Nature* **453** 1023
[2] Beals R, Brierley S, Gray O, Harrow A W, Kutin S, Linden N, Shepherd D and Stather M 2013 *Proc. R. Soc.* A **469** 20120686
[3] Barz S, Kashefi E, Broadbent A, Fitzsimons J F, Zeilinger A and Walther P 2012 *Science* **335** 303
[4] Elliott C 2002 *New J. Phys.* **4** 46
[5] Poppe A, Peev M and Maurhart O 2008 *Int. J. Quantum Inf.* **06** 209
[6] Stucki D *et al* 2011 *New J. Phys.* **13** 123001
[7] Sasaki M *et al* 2011 *Opt. Express* **19** 10387
[8] Bonato C, Tomaello A, Deppo V D, Naletto G and Villoresi P 2009 *New J. Phys.* **11** 045017
[9] Peng C-Z *et al* 2005 *Phys. Rev. Lett.* **94** 150501
[10] Armengol J M P *et al* 2008 *Acta Astronaut.* **63** 165
[11] Bonato C, Aspelmeyer M, Jennewein T, Pernechele C, Villoresi P and Zeilinger A 2006 *Opt. Express* **14** 10050
[12] Aspelmeyer M, Jennewein T, Pfennigbauer M, Leeb W and Zeilinger A 2003 *IEEE J. Sel. Top. Quantum Electron.* **9** 1541
[13] Cirac J I, Zoller P, Kimble H J and Mabuchi H 1997 *Phys. Rev. Lett.* **78** 3221
[14] Shor P W 1995 *Phys. Rev.* A **52** 2493
[15] Sangouard N, Simon C, de Riedmatten H and Gisin N 2011 *Rev. Mod. Phys.* **83** 33
[16] Massar S and Popescu S 1995 *Phys. Rev. Lett.* **74** 1259
[17] Peres A and Scudo P F 2001 *Phys. Rev. Lett.* **87** 167901
[18] Bagan E, Baig M, Tapia R M and Rodriguez A 2004 *Phys. Rev.* A **69** 010304
[19] Chiribella G and DÁriano G M 2004 *J. Math. Phys.* **45** 4435

[20] Bagan E and Tapia R M 2006 *Int. J. Quantum Inf.* **4** 5
[21] Giovannetti V, Lloyd S and Maccone L 2006 *Phys. Rev. Lett.* **96** 010401
[22] Bartlett S D, Rudolph T and Spekkens R W 2007 *Rev. Mod. Phys.* **79** 555
[23] Skotiniotis M and Gour G 2012 *New J. Phys.* **14** 073022
[24] Fitzi M and Maurer U 2000 *Proc. ACM STOC'00* pp 494–503
[25] Lamport L, Shostak R and Pease M 1982 *ACM T. Prog. Lang. Syst.* **4** 382
[26] Feldman P and Micali S 1997 *SIAM J. Comput.* **26** 873
[27] Ben-Or M, Pavlov E and Vaikuntanathan V 2006 *Proc. ACM STOC'06* pp 179–86
[28] Abraham I, Aguilera M K and Malkhi D 2010 *Proc. DISC'10* pp 4–19
[29] Abraham I, Dolev D and Halpern J Y 2008 *Proc. ACM PODC'08* (ACM) pp 405–14
[30] Bracha G 1984 *Proc. ACM PODC'84* pp 154–62
[31] Canetti R and Rabin T 1993 *Proc. ACM STOC'93* (ACM) pp 42–51 0-89791-591-7
[32] Ben-Or M and Hassidim A 2005 *Proc. ACM STOC'05* (ACM) pp 481–5
[33] Fitzi M, Gisin N and Maurer U 2001 *Phys. Rev. Lett.* **87** 217901
[34] Chiribella G, Giovannetti V, Maccone L and Perinotti P 2012 *Phys. Rev.* A **86** 010304
[35] Bagan E, Baig M and Tapia R M 2004 *Phys. Rev.* A **70** 030301
[36] Chiribella G, D'Ariano G M and Sacchi M F 2005 *Phys. Rev.* A **72** 042338
[37] Pease M, Shostak R and Lamport L 1980 *J. ACM* **27** 228
[38] Fischer M J, Lynch N A and Merritt M 1985 *Proc. ACM PODC'85* pp 59–70
[39] Graham R L and Yao A C 1989 *Proc. ACM STOC'89* pp 467–78
[40] Fitzi M, Wolf S and Wullschleger J 2006 *Proc. IEEE ISIT'06* pp 504–5