

# Byzantine Agreement with Optimal Early Stopping, Optimal Resilience and Polynomial Complexity

Ittai Abraham\*  
 VMware Research  
 Palo Alto, CA, USA  
 iabraham@vmware.com

Danny Dolev†  
 Hebrew University of Jerusalem  
 Jerusalem, Israel  
 dolev@cs.huji.ac.il

April 16, 2015

## Abstract

We provide the first protocol that solves Byzantine agreement with optimal early stopping ( $\min\{f + 2, t + 1\}$  rounds) and optimal resilience ( $n > 3t$ ) using polynomial message size and computation.

All previous approaches obtained sub-optimal results and used resolve rules that looked only at the immediate children in the EIG (*Exponential Information Gathering*) tree. At the heart of our solution are new resolve rules that look at multiple layers of the EIG tree.

## 1 Introduction

In 1980 Pease, Shostak and Lamport [PSL80, LSP82] introduced the problem of Byzantine agreement, a fundamental problem in fault-tolerant distributed computing. In this problem  $n$  processes each have some initial value and the goal is to have all correct processes decide on some common value. The network is reliable and synchronous. If all correct processes start with the same initial value then this must be the common decision value, and otherwise the value should either be an initial value of one of the correct processes or some pre-defined default value.<sup>1</sup> This should be done in spite of at most  $t$  corrupt processes that can behave arbitrarily (called Byzantine processes). Byzantine agreement abstracts one of the core difficulties in distributed computing and secure multi-party computation — that of coordinating a joint decision. Pease et al. [PSL80] prove that Byzantine agreement cannot be solved for  $n \leq 3t$ . Therefore we say that a protocol that solves Byzantine agreement for  $n > 3t$  has *optimal resilience*. Fisher and Lynch [FL82] prove that any protocol that solves Byzantine agreement must have an execution that runs for  $t + 1$  rounds. Dolev et al. [DRS90] prove that any protocol must have executions that run for  $\min\{f + 2, t + 1\}$  rounds, where  $f$  is the actual number of corrupt processes. Therefore we say that a protocol that solves Byzantine agreement with  $\min\{f + 2, t + 1\}$  rounds has *optimal early stopping*.

The protocol of [PSL80] has optimal resilience and optimal worst case  $t + 1$  rounds. However the message complexity of their protocol is exponential. Following this result, many have studied the question of obtaining a protocol with optimal resilience and optimal worst case rounds that uses only polynomial-sized messages (and computation).

Dolev and Strong [DS82] obtained the first polynomial protocol with optimal resilience. The problem of obtaining a protocol with optimal resilience, optimal worst case rounds and polynomial-sized messages turned out to be

---

\*Part of the work was done at Microsoft Research Silicon Valley.

†Part of the work was done while the author visited Microsoft Research Silicon Valley. Danny Dolev is Incumbent of the Berthold Badler Chair in Computer Science. This research project was supported in part by The Israeli Centers of Research Excellence (I-CORE) program, (Center No. 4/11), and by grant 3/9778 of the Israeli Ministry of Science and Technology.

<sup>1</sup>Other versions of the problem may not restrict to a value on one of the correct processes, if not all initial values are the same, or require agreement on a leader's initial value, which can be reduced to the version we defined.

surprisingly challenging. Building on a long sequence of results, Berman and Garay [BG93] presented a protocol with optimal worst case rounds and polynomial-sized messages for  $n > 4t$ . In an exceptional tour de force, Garay and Moses [GM93, GM98], presented a protocol for binary-valued Byzantine agreement obtaining optimal resilience, polynomial-sized messages and  $\min\{f + 5, t + 1\}$  rounds. We refer the reader to [GM98] for a detailed and full account of the related work. Recently Kowalski and Mostéfaoui [KM13] improved the message complexity to  $\tilde{O}(n^3)$  but their solution does not provide early stopping and requires exponential computation.

Worst case running of  $t + 1$  rounds is the best possible if the protocol is to be resilient to an adversary that controls  $t$  processes. However, in executions where the adversary controls only  $f < t$  processes, the optimal worst case can be improved to  $f + 2$  rounds. Berman et al. [BGP92] were the first to obtain optimal resilience and optimal early stopping (i.e.  $\min\{f + 2, t + 1\}$  rounds) using exponential size messages. Early stopping is an extremely desirable property in real world replication systems. In fact, agreement in a small number of rounds when  $f = 0$  is a core advantage of several practical state machine replication protocols (for example [CL99] and [KAD<sup>+</sup>07] focus on optimizing early stopping in the fault free case).

Somewhat surprisingly, after more than 30 years of research on Byzantine Agreement, the problem of obtaining the best of all worlds is still open. There is no protocol with optimal resilience, optimal early stopping and polynomial-sized message. The conference version of [GM98] claimed to have solved this problem but the journal version only proves a  $\min\{f + 5, t + 1\}$  round protocol, then says it is *possible* to obtain a  $\min\{f + 3, t + 1\}$  round protocol and finally the authors say they *believe* it should be possible to obtain a  $\min\{f + 2, t + 1\}$  round protocol. We could not see how to directly extend the approach of [GM98] to obtain optimal early stopping. The main contribution of this paper is solving this long standing open question and providing the optimal  $\min\{f + 2, t + 1\}$  rounds with optimal resilience and polynomial complexity. Moreover, our result applies directly for arbitrary initial values and not only to binary initial values, as some of the previous results.

Our Byzantine agreement protocol obtains a stronger notion of *multi-valued validity*. If  $v \neq \perp$  is the decision value then at least  $t + 1$  correct processes started with value  $v$ . The multi-valued validity property is crucial in our solution for early stopping with monitors. This property is also more suitable in proving that Byzantine agreement implements an ideal world centralized decider that uses the majority value. We note that several previous solutions (in particular [GM98]) are inherently binary and their extension to multi-valued agreement does not have the stronger multi-valued validity property.

**Theorem 1.** *Given  $n$  processes, there exists a protocol that solves Byzantine agreement. The protocol is resilient to any Byzantine adversary of size  $t < n/3$ . For any such adversary, the total number of bits sent by any correct process is polynomial in  $n$  and the number of rounds is  $\min\{f + 2, t + 1\}$  where  $f$  is the actual size of the adversary.*

**Overview of our solution.** At a high level we follow the framework set by Berman and Garay [BG93]. In this framework, if at a given round all processes seem to behave correctly then the protocol stops quickly thereafter. So if the adversary wants to cause the protocol to continue for many rounds it must have at least one corrupt process behave in a faulty manner in each round. However, behaving in a faulty manner will expose the process and in a few rounds the mis-behaving process will become publicly exposed as corrupt.

This puts the adversary between a rock and a hard place: if too few corrupt processes are publicly exposed then the protocol reaches agreement quickly, if too many corrupt process are exposed then a “monitor” framework (also called “cloture votes”) that runs in the background causes the protocol to reach agreement in a few rounds. So the only path the adversary can take in order to generate a long execution is to publicly expose exactly one corrupt process each round. In the  $t < n/4$  case, this type of adversary behavior keeps the communication polynomial.

For  $t < n/3$  a central challenge is that a corrupt process can cause communication to grow in round  $i$  but will be publicly exposed only in round  $i + 2$ . Naively, such a corrupt process may also cause communication to grow both in round  $i$  and  $i + 1$  and this may cause exponential communication blowup. Garay and Moses [GM98] overcome this challenge by providing a protocol such that, if there are at most two new corrupt processes in round  $i$  and no new corrupt process in round  $i + 1$  then even though they are publicly exposed in round  $i + 2$  they cannot increase communication in round  $i + 1$  (also known as preventing “cross corruption”).

At the core of the binary-valued protocol of Garay and Moses is the property that one value can only be decided on even rounds and the other only on odd rounds. This property seems to raise several unsolved challenges for obtaining

optimal early stopping. We could not see how to overcome these challenges and obtain optimal early stopping using this property. Our approach allows values to be fixed in a way that is indifferent to the parity of the round number (and is not restricted to binary values).

Two key properties of our protocol that makes it quite different from all previous protocols. First, the value of a node is determined by the values of its children and grandchildren in the EIG tree ([BNDDS92]). Second, if agreement is reached on a node then the value of all its children is changed to be the value of the node. This second property is crucial because otherwise even though a node is fixed there could be disagreement about the value of its child. Since the value of the parent of the fixed node depends on its children and grandchildren, the disagreement on the grandchild may cause disagreement on the parent and this disagreement could propagate to the root.

The decision to change the value of the children when their parent is fixed is non-trivial. Consider the following scenario with a node  $\sigma$ , child  $\sigma p$  and grandchild  $\sigma pq$ : some correct reach agreement that the value of  $\sigma pq$  is  $d$ , then some correct reach agreement that the value of  $\sigma p$  is  $d' \neq d$  and hence the value of  $\sigma pq$  is changed (colored) to  $d'$ . So it may happen that some correct decide the value of  $\sigma$  based on  $\sigma pq$  being fixed on  $d$  and some other correct decide the value of  $\sigma$  based on  $\sigma pq$  being colored to  $d'$ . Making sure that agreement is reached in all such scenarios requires us to have a relatively complex set of complementary agreement rules.

To bound the size of the tree by a polynomial size we prove that the adversary is still between a rock and a hard place: roughly speaking there are three cases. If just one new process is publicly exposed in a given round then the tree grows mildly (remains polynomial). If three or more new processes are exposed in the same round then this increases the size of the tree but can happen at most a constant number of times before a monitor process will cause the protocol to stop quickly.

The remaining case is when exactly two new processes are exposed, then a sequence of (possibly zero) rounds where just one new process is exposed in each round, followed by a round where no new process is exposed. This is a generalized version of the “cross corruption” case of [GM98] where the adversary does not face increased risk of being caught by the monitor process. We prove that in these cases the tree essentially grows mildly (remains polynomial).

In order to deal with this generalized “cross corruption” we introduce a special resolve rule (SPECIAL-BOT RULE) tailored to this scenario. In particular, in some cases we fix the value of a node  $\sigma$  to  $\perp$  (a special default value) if we detect enough support. This solves the generalized “cross corruption” problem but adds significant complications. Recall that when we fix a value to a node then we also fix (color) the children of this node with the same value.

Suppose a process fixes a node  $\sigma$  to  $\perp$ . The risk is that some correct processes may have used a child  $\sigma p$  with value  $d$  but some other correct process will see  $\perp$  for  $\sigma p$  (because when  $\sigma$  is fixed to  $\perp$  we color all its children to  $\perp$ ). Roughly speaking, we overcome this difficulty by having two resolve rule thresholds. The base is the  $n - t$  threshold (RESOLVE RULE, IT-TO-RT RULE) and the other is with a  $n - t - 1$  threshold (RELAXED RULE). In essence this  $n - t - 1$  rule is resilient to disagreement on one child node (that may occur due to coloring). We then make sure that the SPECIAL-BOT RULE can indeed change only one child value. This delicate interplay between the resolve rules is at the core of our new approach.

**The adversary.** Given  $n > 3t$  and  $\phi \leq t$ , as in [GM98], we will consider a  $(t, \phi)$ -adversary - an adversary that can control up to  $\phi$  corrupt processes that behave arbitrarily and at most  $t - \phi$  corrupt processes that are always silent (send some default value  $\perp$  to all processes every round). The  $(t, \phi)$ -adversary will be useful to model executions in which all correct processes have detected beforehand some common set of at least  $t - \phi$  corrupt processes and hence ignore them throughout the protocol. Note that the standard  $t$ -adversary is just a  $(t, t)$ -adversary.

## 2 The EIG structure and rules

In this section we define the EIG structure and rules.

Let  $N$  be the set of processes,  $n = |N|$  and assume that  $n > 3t$ . Let  $D$  be a set of possible decision values. We assume some decision  $\perp \in D$  is the designated default decision.

Let  $\Sigma_r$  be the set of all sequences of length  $r$  of elements of  $N$  without repetition. Let  $\Sigma_0 = \epsilon$ , the empty sequence. Let  $\Sigma = \bigcup_{0 \leq j \leq t+1} \Sigma_j$ . An *Exponential Information Gathering* tree (EIG in short) is a tree whose nodes are elements in  $\Sigma$  and whose edges connect each node to the node representing its longest proper prefix. Thus, node  $\epsilon$  has  $n$  children,

and a node from  $\Sigma_k$  has exactly  $n - k$  children.

We will typically use the Greek letter  $\sigma$  to denote a sequence (possibly empty) of labels corresponding to a node in an EIG tree. We use the notation  $\sigma q$  to denote the node in the EIG tree that corresponds to the child of node  $\sigma$  that corresponds to the sequence  $\sigma$  concatenated with  $q \in N$ . We denote by  $\bar{\epsilon}$  the root node of the tree that corresponds to the empty sequence. Given two sequences  $\sigma, \sigma' \in \Sigma$ , let  $\sigma' \sqsubset \sigma$  denote that  $\sigma'$  is a proper prefix of  $\sigma$  and  $\sigma' \sqsubseteq \sigma$  denote that  $\sigma'$  is a prefix of  $\sigma$  (potentially  $\sigma' = \sigma$ ).

In the EIG consensus protocol each process maintains a dynamic tree data structure  $\mathcal{IT}$ . This data structure maps a set of nodes in  $\sigma$  to values in  $D$ . Intuitively, this tree contains all the information the process has heard so far. Each process  $z$  also maintains two global dynamic sets  $\mathcal{F}, \mathcal{FA}$ . The set  $\mathcal{F}$  contains processes that  $z$  detected as faulty, and  $\mathcal{FA}$  contains processes that  $z$  knows are detected by all correct processes. The protocol for updating  $\mathcal{F}, \mathcal{FA}$  is straightforward:

- In each round the processes exchange their  $\mathcal{F}$  lists and update their  $\mathcal{F}$  and  $\mathcal{FA}$  sets once a faulty process appears in  $t + 1$  or  $2t + 1$  lists, respectively.
- When a process is detected as faulty every correct process masks its future messages to  $\perp$ .

The basic EIG protocol will be invoked repeatedly, and several copies of the EIG protocol may be running concurrently. The accumulated set of faulty processes will be used across all copies (the rest of the variables and data structures are local to each EIG invocation). Therefore, we assume that when the protocol is invoked the following property holds:

**Property 1.** *When the protocol is invoked, no correct process appears in the faulty sets of any other correct process. Moreover,  $\mathcal{FA}_p \subseteq \mathcal{F}_q$  and  $\mathcal{FA}_q \subseteq \mathcal{F}_p$  for any two correct processes  $p$  and  $q$ ,*

Each invocation of the EIG protocol is tagged with a parameter  $\phi$ , known to all processes. An EIG protocol with parameter  $\phi$ , will run for at most  $\phi + 1$  rounds. At the beginning of the agreement protocol the faulty sets are empty at all correct processes and the EIG protocol with parameter  $\phi = t$  is executed. Each additional invocation of the EIG protocol is with a smaller value of  $\phi$ . In the non-trivial case, when the EIG protocol with parameter  $\phi$  is invoked then  $|\bigcap_i \mathcal{FA}_i| \geq t - \phi$ . There will be one exception to this assumption, and it is handled in [Lemma 1](#). Thus, other than in that specific case, it is assumed that we have a  $(t, \phi)$ -adversary during the execution of the EIG protocol with parameter  $\phi$ .

The basic EIG protocol for a correct process  $z$  with initial value  $d_z \in D$  is very simple:

1. **Init:** Set  $\mathcal{IT}(\bar{\epsilon}) := d_z$ , so  $\mathcal{IT}(\bar{\epsilon})$  is set to be the initial value.
2. **Send:** in each round  $r$ ,  $1 \leq r \leq \phi + 1$ , for every  $\sigma \in \mathcal{IT} \cap \Sigma_{r-1}$ , such that  $z \notin \sigma$ , send the message  $\langle \sigma, z, \mathcal{IT}(\sigma) \rangle$  to every process.
3. **Receive set:** in each round  $r$ , let  $\mathcal{S}_r := \{\sigma x \in \Sigma_r\}$ .
4. **Receive rule:** in each round  $r$ , for all  $\sigma x \in \mathcal{S}_r$  set

$$\mathcal{IT}(\sigma x) := \begin{cases} \perp & \text{if } x \in \mathcal{F} \\ d & \text{if } x \notin \mathcal{F} \text{ sent } \langle \sigma, x, d \rangle \text{ and } d \in D; \\ \mathcal{IT}(\sigma) & \text{otherwise.} \end{cases}$$

*Note:* assigning of  $\mathcal{IT}(\sigma x) := \mathcal{IT}(\sigma)$  when  $x \notin \mathcal{F}$  is crucial for the case where  $x$  is correct and has halted in the previous round. Thus, if a process is silent but is not detected (possibly because it has halted due to early stopping)  $z$  assigns it the value it heard in the previous round.

We use a second dynamic EIG tree data structure  $\mathcal{RT}$ . Intuitively, if a process puts a value in a node of this tree then, essentially, all correct processes will put the same value in the same node in at most 2 more rounds. Processes use several rules to close branches of the  $\mathcal{IT}$  tree whose value in  $\mathcal{RT}$  is already determined by all. We present later the rules for closing branches of the  $\mathcal{IT}$  tree. To handle this, we modify lines 2 and 3 as described below (and keep lines 1 and 4 as above).

2. **Send:** in each round  $r$ ,  $1 \leq r \leq \phi + 1$ , for every  $\sigma \in \mathcal{IT} \cap \Sigma_{r-1}$ , such that  $z \notin \sigma$ , and the branch  $\sigma$  is not closed send the message  $\langle \sigma, z, \mathcal{IT}(\sigma) \rangle$  to every process.

3. **Receive set:** in each round  $r$ , let  $\mathcal{S}_r = \{\sigma x \in \Sigma_r \mid \text{branch } \sigma x \text{ is not closed}\}$ .

Informally,  $\mathcal{IT}_z(\sigma p) = d$  (where  $\mathcal{IT}_z$  denotes the  $\mathcal{IT}$  tree at process  $z$ ) indicates that process  $z$  received a message from process  $p$  that said that his value for  $\sigma$  was  $d$ .  $\mathcal{RT}_z(\sigma p) = d$  indicates, essentially, that process  $z$  knows that every correct process  $x$  will agree and have  $d \in \mathcal{RT}_x(\sigma p)$  in at most two more rounds.

Observe that we record in the EIG tree only information from sequences of nodes that do not contain repetition, therefore, not every message a process receives will be recorded.

At the end of each round, we apply the rules below to determine whether to assign values to nodes in  $\mathcal{RT}$ , assigning that value in  $\mathcal{RT}$  is called *resolving* the node.

## 2.1 The Resolve Rules

A key feature of our algorithm is that whenever we put a value into  $\mathcal{RT}(\sigma)$  we also color (assign) all the descendants of  $\sigma$  in  $\mathcal{RT}$  with the same value. Observe that this means we may color a node  $\sigma w$  in  $\mathcal{RT}$  to  $d$  even if  $w$  is correct and sent  $d' \neq d$  to all other correct processes.

**Rules for IT-to-RT resolve:** The following definitions and rules cause a node to be resolved based on information in  $\mathcal{IT}$ .

1. If  $\mathcal{IT}(\sigma w) = d$  **then** we say: (1)  $w$  is a voter of  $(\sigma, w, d)$ ; (2)  $w$  is confirmed on  $(\sigma, w, d)$ ; (3) For all  $v \in N \setminus \{\sigma\}$ ,  $w$  is a supporter of  $v$  on  $(\sigma, w, d)$ .

*Note:* the reason that we count  $w$  as a voter, as confirmed and as a supporter for all its echoers is that due to the EIG structure  $w$  does not appear in the subtree of  $\sigma w$ .

2. If  $\mathcal{IT}(\sigma w v) = d$ , **then** we say that  $v$  is a supporter of  $v$  for  $(\sigma, w, d)$ .

*Note:* again we need  $v$  to be a supporter of itself because of the EIG structure.

3. If  $\mathcal{IT}(\sigma w v u) = d$  **then** we say that  $u$  is a supporter of  $v$  for  $(\sigma, w, d)$ .

4. If there is a set  $|U| = n - t$ , such that for each  $u' \in U$ ,  $u'$  is a supporter of  $v$  on  $(\sigma, w, d)$  **then** we say that  $v$  is confirmed on  $(\sigma, w, d)$ .

*Note:* if  $\sigma$  contains no correct and  $w$  is correct, then any correct child  $v$  (of  $\sigma w$ ) will indeed have  $n - t$  supporters for  $\sigma w$  and hence will be confirmed. Note that one supporter is  $w$ , the other is  $v$  and the remaining are all the  $n - t - 2$  correct children of  $\sigma w v$ . Also note that  $w$  is confirmed, so all  $n - t$  correct will be confirmed on  $(\sigma, w, d)$ .

5. If  $u \neq w$  has a set  $|V| = n - t$ , such that for each  $v' \in V$ ,  $u$  is a supporter of  $v'$  on  $(\sigma, w, d)$  and  $v'$  is confirmed on  $(\sigma, w, d)$  **then**  $u$  is a voter of  $(\sigma, w, d)$ .

*Note:* this is somewhat similar to the notion of a Voter in grade-cast ([FM97, FM88]). But there is a crucial difference: all the  $n - t$  echoers need to be *confirmed*. Also note that  $w$  is a voter for itself.

6. IT-TO-RT RULE: If  $w$  has a set  $|U| = n - t$ , such that for each  $u' \in U$ ,  $u'$  is a voter of  $(\sigma, w, d)$  **then** if  $\sigma w \notin \mathcal{RT}$ , then put  $\mathcal{RT}(\sigma w) := d$  and color descendants of  $\sigma w$  with  $d$  as well.

*Note:* this is somewhat similar to the notion of a grade 2 in grade-cast. A crucial difference is that the  $n - t$  voters needed are defined with respect to *supported* echoers. This is a non-trivial change that breaks the standard grade-cast properties. Also note that we not only put a value in  $\sigma w$  but also color all the descendants.

7. ROUND  $\phi + 1$  RULE: if  $\mathcal{IT}(\sigma w) = d$  and  $\sigma \in \Sigma_t$  **then** if  $\sigma w \notin \mathcal{RT}$ , then put  $\mathcal{RT}(\sigma w) := d$ .

*Note:* this is a standard rule to deal with the last round.

**Rules for  $\mathcal{RT}$  tree resolve:** The following definitions and rules cause a node to be resolved based only on information in  $\mathcal{RT}$  (these rules do not look at  $\mathcal{IT}$ ).

1. If there is a set  $|U| = t + 1$ , such that for each  $u' \in U$ ,  $\mathcal{RT}(\sigma w v u') = d$  **then** we say  $v$  is  $\mathcal{RT}$ -confirmed on  $(\sigma, w, d)$ .

*Note:* if any correct sees a node as confirmed then it has  $n - t$  that echo its value. At least  $t + 1$  of them are correct and they all cause all correct to see the node as  $\mathcal{RT}$ -confirmed. Of course a node may become  $\mathcal{RT}$ -confirmed even if it was never confirmed by any correct. Observe that if  $\mathcal{RT}(\sigma w u) = d$  then, by coloring,  $u$  is  $\mathcal{RT}$ -confirmed on  $(\sigma, w, d)$ .

2. If  $u \neq w$  has a set  $|V| = n - t$ , such that each  $v' \in V$  is  $\mathcal{RT}$ -confirmed on  $(\sigma, w, d)$  and for each  $v' \in V \setminus \{u\}$ ,  $\mathcal{RT}(\sigma w v' u) = d$  and if  $u \in V$  then also  $\mathcal{RT}(\sigma w u) = d$ , **then**  $u$  is  $\mathcal{RT}$ -voter of  $(\sigma, w, d)$ .

*Note:* if any correct process sees a node as a voter then it has  $n - t$  echoers that are confirmed. So each of these  $n - t$  echoers will be  $\mathcal{RT}$ -confirmed. So all correct processes will see this node as  $\mathcal{RT}$ -voter. Of course a node can become  $\mathcal{RT}$ -voter even if it was never a voter at any correct process.

3. RESOLVE RULE: If  $w$  has a set  $|U| = t + 1$ , such that for each  $u' \in U$ ,  $u'$  is a  $\mathcal{RT}$ -voter of  $(\sigma, w, d)$  **then** if  $\sigma w \notin \mathcal{RT}$ , then put  $\mathcal{RT}(\sigma w) := d$ , and color descendants of  $\sigma w$  with  $d$  as well. The rule applies also for node  $\sigma w = \bar{\epsilon}$ .

*Note:* if any correct process does IT-TO-RT RULE then this rule tries to guarantee that all correct processes will also put this node in  $\mathcal{RT}$ . The problem is that SPECIAL-BOT RULE (see below) may be applied to one of the echoers and this may cause some of the  $\mathcal{RT}$ -voters to lose their required support. The following rule fixes this situation. It reduces the threshold to  $n - t - 1$  but requires that all children nodes are fixed.

4. RELAXED RULE: If all the children of  $\sigma w$  are in  $\mathcal{RT}$  (i.e.,  $\forall \sigma w v \in \Sigma: \sigma w v \in \mathcal{RT}$ ) and exists a set  $|V| = n - t - 1$ , such that for each  $v' \in V$ ,  $\mathcal{RT}(\sigma w v') = d$ , **then** if  $\sigma w \notin \mathcal{RT}$ , then put  $\mathcal{RT}(\sigma w) := d$ , and color descendants of  $\sigma w$  with  $d$  as well. The rule applies only for nodes  $|\sigma w| \geq 1$ .

*Note:* as mentioned above, the RELAXED RULE requires a threshold of  $n - t - 1$  so that it can take into account the possibility of one value changing to  $\perp$  due to the following rule:

5. SPECIAL-BOT RULE: If there is a set  $|V| = t + 2 - |\sigma w u|$  such that for all  $v \in V$ ,  $\mathcal{RT}(\sigma w u v) = \perp$  and for all  $u' \neq u$  such that  $\sigma w u' \in \Sigma$ ,  $\sigma w u' \in \mathcal{RT}$  **then** if  $\sigma w u \notin \mathcal{RT}$ , then put  $\mathcal{RT}(\sigma w u) := \perp$ , and color descendants of  $\sigma w u$  with  $\perp$  as well. The rule applies only for  $|\sigma w u| \geq 2$ .

*Note:* This rule can be applied to at most one child.

6. SPECIAL-ROOT-BOT RULE: If exists a set  $|U| = t + 1$  such that for each  $u \in U$ ,  $\mathcal{RT}(u) = \perp$  then if  $\bar{\epsilon} \notin \mathcal{RT}$ , then put  $\mathcal{RT}(\bar{\epsilon}) := \perp$ , and color descendants of  $\bar{\epsilon}$  with  $\perp$  as well.

*Note:* this rule is important in order to stop quickly if  $t + 1$  correct processes start with the value  $\perp$ .

To prevent the data structures from expanding too much processes close branches of the tree, and from that point on they do not send messages related to the closed branches. We use the notation  $\{\sigma \in \mathcal{RT}[r]\}$  to denote an indicator variable that equals true if  $\mathcal{RT}(\sigma)$  was assigned some value by the end of round  $r$ , and false otherwise.

**Branch Closing and Early Resolve rules:** There are three rules to close a branch in  $\mathcal{IT}$  two of them also trigger an early resolve. By the end of round  $r$ ,  $r \leq \phi$ ,

1. DECAY RULE: if  $\exists \sigma' \sqsubseteq \sigma$  such that  $\sigma' \in \mathcal{RT}[r - 1]$ , then close the branch  $\sigma \in \mathcal{IT}$ .

*Note:* this is the simple case: if a process already fixed the value of  $\sigma'$  in  $\mathcal{RT}$  in round  $r - 1$  then it stops in the end of round  $r$ , since by the end of round  $r + 1$  all correct processes will put  $\sigma'$  in  $\mathcal{RT}$  (and will interpret this process's silence in the right way during round  $r + 1$ ). There is no need to continue. Coloring will fix all the values of this subtree.

2. EARLY-IT-TO-RT RULE: if  $\sigma \in \Sigma_{r-1}$  and exists  $U \subseteq N$ ,  $U \cap \{u' \mid u' \in \sigma\} = \emptyset$ ,  $|U| = n - r$ , such that for every  $u, v \in U \setminus \mathcal{F}$ ,  $\mathcal{IT}(\sigma u) = \mathcal{IT}(\sigma v)$ , then if  $\sigma \notin \mathcal{RT}$ , then put  $\mathcal{RT}(\sigma) := \mathcal{IT}(\sigma)$  and close the branch  $\sigma \in \mathcal{IT}$ .

*Note:* this is a case where the process can forecast that all correct processes will put  $\sigma$  in  $\mathcal{RT}$  in the next round (because the process sees that all children nodes agree). So the process can fix  $\sigma$  in this round and stop now, because all correct processes will fix  $\sigma$  in  $\mathcal{RT}$  next round (and will interpret this process's silence in the right way).

3. **STRONG\_IT-TO-RT RULE:** if  $\sigma \in \Sigma_{r-2}$  and exists  $U \subseteq N$ ,  $U \cap \{u' \mid u' \in \sigma\} = \emptyset$ ,  $|U| = n - r + 1$  such that for every  $u, v \in U \setminus \mathcal{F}$ , where  $v \neq u$ ,  $\mathcal{IT}(\sigma uv) = \mathcal{IT}(\sigma vu)$  then, if  $\sigma \notin \mathcal{RT}$ , then put  $\mathcal{RT}(\sigma) := \mathcal{IT}(\sigma)$  and close the branch  $\sigma \in \mathcal{IT}$ .

*Note:* in this case all the correct children of  $\sigma$  except for at most one will be fixed in the next round to the same value, so the **RELAXED RULE** will be applied to  $\sigma$  in the next round. So we can fix  $\sigma$  in this round and stop now.

In each round all the above rules are applied repeatedly until none holds any more.

The rules above imply that there are two ways to give a value to a node in  $\mathcal{RT}$ . One is assigning it a value using the various rules, and the other is coloring it as a result of assigning a value to one of its predecessors. We will use the term *color* for the second one and the term *put* for the first one.

**Rules for fault detection and masking:** The following definitions and rules are used to detect faulty processes, put them into  $\mathcal{F}$  and hence mask them (all messages from  $\mathcal{F}$  are masked to  $\perp$ ). The last rule also defines an additional masking. The process first updates its  $\mathcal{F}$  and  $\mathcal{FA}$  sets using the sets received from the other processes during the current round. A process is added to  $\mathcal{F}$  or  $\mathcal{FA}$  once it appears in  $t + 1$  or  $2t + 1$  sets, respectively. Next the process applies the following fault detection rules. The fault detection is executed before applying any of the resolve rules above. When a new process is added to  $\mathcal{F}$ , the new masking is applied and the fault detection is repeated until no new process can be added. Only then the resolve rules above are applied.

At process  $z$  by the end of round  $r$ :

1. **Not Voter:** If  $\exists \sigma w \in \Sigma_{r-1}$  and  $w \neq z$  and  $\exists \sigma' \sqsubseteq \sigma w$  such that  $\sigma' \in \mathcal{RT}$  and it is not the case that there exists a set  $|U| = n - t - 1$  such that for each  $u' \in U$ ,  $\mathcal{IT}(\sigma w u') = \mathcal{IT}(\sigma w)$  **then** add  $w$  to  $\mathcal{F}$ .

*Note:* this is the standard detection rule after one round - if anything looks suspicious then detect.

2. **Not IT-to-RT:** If  $\exists \sigma w \in \Sigma_{r-2}$  for which  $w$  does not have a set  $|U| = n - t$ , such that for each  $u' \in U$ ,  $u'$  is a voter of  $(\sigma, w, d)$ , and  $\exists \sigma' \sqsubseteq \sigma$  such that  $\sigma' \in \mathcal{RT}$  **then** add  $w$  to  $\mathcal{F}$ .

*Note:* this is the standard detection rule after two rounds - if anything looks suspicious then detect.

3. If  $u, u \neq w$ , has a set  $|V| = n - t$ , such that for each  $v' \in V$ ,  $u$  is a supporter of  $v'$  on  $(\sigma, w, d)$  **then** we say that  $u$  is an *unconfirmed voter* of  $(\sigma, w, d)$ .

*Note:* the notion of an *unconfirmed voter* is exactly that of a voter in the standard grade-cast protocol.

4. If  $w$  has a set  $|U| = t + 1$ , such that for each  $u' \in U$ ,  $u'$  is an unconfirmed voter of  $(\sigma, w, d)$  **then** we say that  $\sigma w$  is *leaning towards*  $d$ .

*Note:* the notion of *leaning towards* is exactly that of getting grade  $\geq 1$  in the standard grade-cast protocol.

5. **Not Masking:** If  $\sigma w \in \Sigma_{r-3}$  is leaning towards  $d$  and there exists  $u$ ,  $|V| = t + 1$ , and  $d' \neq d$  such that for each  $v' \in V$ ,  $\mathcal{IT}(\sigma w v') = d'$  and there exists  $|\sigma''| > |\sigma|$  such that  $\mathcal{IT}(\sigma'' w u) \neq \perp$  then

(a)  $\mathcal{IT}(\sigma'' w u) = \perp$ ;

(b) if by the end of the round  $\exists \sigma' \sqsubseteq \sigma'' w$  such that  $\sigma' \in \mathcal{RT}$  **then** add  $u$  to  $\mathcal{F}$ .

*Note:* If  $\sigma w$  is leaning towards  $d$  then  $u$  must have heard at least  $t + 1$  say  $d$  on  $\sigma w$ . If  $t + 1$  say  $u$  said  $d'$  then  $u$  must have said  $d'$  to some correct. So  $u$  must have received  $d'$  from  $\sigma w$  but in the next round  $u$  hears  $t + 1$  say  $\sigma w$  said  $d$ . So  $u$  must conclude that  $w$  is faulty and  $u$  must mask him from the next round. If  $u$  did not mask some  $\sigma'' w u$  then the **Not Masking** rule will detect  $u$  as faulty and mask all such  $\sigma'' w u$  for you and also mark you as faulty. The reason we wait until the end of the round to add that node to  $\mathcal{F}$  is that it might be a node of

a correct process that stopped in the previous round and hence did not send any messages in the current round, and therefore did not send masking. In such a case we mask its virtual sending, but do not add it to  $\mathcal{F}$ .

**Finalized Output:** By the end of each round (after applying all the resolve rules), the process checks whether there is a frontier in  $\mathcal{RT}$ . A *frontier* (also called a cut) is said to exist if for all  $\sigma \in \Sigma_{\phi+1}$  there exists some sub-sequence  $\sigma' \sqsubseteq \sigma$  such that  $\sigma' \in \mathcal{RT}$ .

1. **Early Output rule:** By the end of a round, if  $\bar{e} \in \mathcal{RT}$ , **output**  $\mathcal{RT}(\bar{e})$ .
2. **Final Output rule:** Otherwise, if there is a frontier, **output**  $\perp$ .

Observe that the existence of a frontier can be tested from the current  $IT$  in  $O(|IT|)$  time.

**Stopping rule:** If all branches of  $IT$  are closed, stop the protocol.

### 3 The Consensus Protocol Analysis

The EIG protocol implicitly presented in the previous section is a consensus protocol  $\mathcal{D}_\phi$ , where  $\phi$ ,  $1 \leq \phi \leq t$  is a parameter. Protocol  $\mathcal{D}_\phi$  runs for at most  $\phi + 1$  rounds and solves Byzantine agreement against a  $(t, \phi)$ -adversary. Denote by  $G$  the set of correct processes,  $|G| \geq n - t$ , where  $n = |N|$ , and by  $S$ ,  $S = \bigcap_{q \in G} \mathcal{F}_q$ , the set of processes that are masked to  $\perp$  by all correct processes. Let  $s := |S|$ .

Our solution invokes several copies of the EIG protocol. For each invoked protocol,  $\mathcal{D}_\phi$ , there are two cases: either  $s \geq t - \phi$ , or we are guaranteed that the input of all correct processes that start the protocol is the same (in particular, it may be that some correct processes have halted and do not start the protocol). The following lemma deals with this latter case.

**Lemma 1.** [Validity and Fast Termination] For any  $(t, t)$ -adversary, and  $n \geq 3t + 1$ ,

1. if every correct process that starts the protocol holds the same input value  $d$  then  $d$  is the output value of all correct processes that start the protocol, by the end of round 2, and all of them complete the protocol by the end of round 3.
2. if all correct processes start the protocol and  $t + 1$  correct processes start with  $\perp$  then all correct processes output  $\perp$  by the end of round 3 and stop the protocol by the end of round 4.
3. For  $p, q \in G$ , no  $p$  will add  $q$  to  $\mathcal{F}_p$  in either of the above cases.

*Proof.* To prove the first item, let us follow the protocol. Let  $G_1$  be the set of correct processes that start the protocol and let  $G_2 = G \setminus G_1$ , be the remaining correct processes that remain silent throughout the protocol.

Initially, for every  $z \in G_1$ ,  $IT_z(\bar{e}) = d_z$ .

In the 1st round every correct process  $z \in G_1$  sends  $\langle \bar{e}, z, d_z \rangle$  to every process. By the end of the 1st round, every correct process applies the receive rule for all the other processes. Thus, every correct process  $z \in G_1$  has  $IT_z(x) := d_x$ , for every  $x \in G$ , since it completes the missing values from correct processes in  $G_2$  to be its own input value. Thus, the receive rule assigns at each  $z \in G_1$ ,  $IT_z(\sigma x) := IT_z(\sigma)$  for a missing value by  $x \in G_2$  for  $\sigma$ . EARLY\_IT-TO-RT RULE, may be applied by some correct processes at the end of the first round, and as a result will put  $\mathcal{RT}(\bar{e}) = d$  and will output  $d$ .

Since  $IT_z(x) = d$  for all  $x \in G$ , by the end of the 1st round, every  $z \in G_1$  sees every  $x \in G$  as supporter of  $x$  for  $(\bar{e}, \bar{e}, d)$ .

In the 2nd round, every correct process  $z \in G_1$  that did not apply EARLY\_IT-TO-RT RULE by the end of the 1st round, sends  $\langle x, z, d \rangle$  for every process  $x \in G$  to every process. Again, if any correct process did not send a message, its missing value for any  $x \in G$  will be assigned the same value at all correct processes. Notice that some additional correct processes may not send in the second round.

By the end of the 2nd round, after applying the receive rule, at each  $z \in G_1$  that did not apply EARLY\_IT-TO-RT RULE by the end of the 1st round,  $IT_z(xy) = d$  for every  $x, y \in G$ . Thus, for every such  $x$ , every  $y \in G \setminus \{x\}$ , is a supporter of  $x$  for  $(\bar{e}, \bar{e}, d)$ . As a result, for the set  $|G| = n - t$ , for each  $u' \in G$ ,  $u'$  is a supporter of  $v$  for  $(\bar{e}, \bar{e}, d)$ , for

every  $v \in G$ . Therefore, every  $v \in G$  is confirmed on  $(\bar{\epsilon}, \epsilon, d)$ . Therefore, every process  $z \in G_1$ , that did not apply EARLY\_IT-TO-RT RULE by the end of the 1st round, sees every process  $x \in G$  as a voter of  $(\bar{\epsilon}, \bar{\epsilon}, d)$ . This implies that it can apply the IT-TO-RT RULE and will put  $\mathcal{RT}(\bar{\epsilon}) = d$ , will output  $d$ , and will stop the protocol by the end of round 3.

For the second claim: by the end of the 1st round, every correct process  $z$  has  $\mathcal{IT}_z(x) := \perp$ , for at least  $t + 1$  processes  $x \in G$ . Let  $A = \{x \mid x \in G \ \& \ d_x = \perp\}$ . If  $\perp$  was the input value to all correct processes, we are done by the previous claim. Otherwise, no correct process will apply EARLY\_IT-TO-RT RULE to a value that is not  $\perp$ .

In the 2nd round, every correct process  $z$  sends  $\langle x, z, d_x \rangle$  for every process  $x \in G$  to every process. By the end of the 2nd round, after applying the receive rule, at each  $z \in G$ ,  $\mathcal{IT}_z(xy) = d_x$ , for every  $x, y \in G$ . Thus, every process  $z \in G$  sees each process  $v \in A$  both as supporter of  $v$  for  $(\bar{\epsilon}, v, \perp)$ , and also as supporter of  $u$  for  $(\bar{\epsilon}, v, \perp)$  for every  $u \in G$ .

In the 3rd round, every correct process  $z$  sends  $\langle vx, z, \perp \rangle$  for every process  $v \in A$  and  $x \in G$  to every process. If any correct process applied EARLY\_IT-TO-RT RULE in the previous round, then its missing value regarding other correct processes will be identical at all correct processes. By the end of the 3rd round, after applying the receive rule, at each  $z \in G$ ,  $\mathcal{IT}_z(vxy) = \perp$ , for every  $v \in A$ , and  $x, y \in G$ . Thus, every process  $z \in G$  sees every process  $u \in G \setminus \{v\}$  as a supporter of  $u'$  for  $(\bar{\epsilon}, v, \perp)$ , for every  $u' \in G \setminus \{v\}$  and  $v \in A$ . For every such  $v$  and  $u'$ ,  $v$  is also a supporter of  $u'$  for  $(\bar{\epsilon}, v, \perp)$ . Thus, every such  $u'$  is confirmed on  $(\bar{\epsilon}, v, \perp)$ , for every  $v \in A$ . Moreover, by definition, every such  $v$  is also confirmed on  $(\bar{\epsilon}, v, \perp)$ .

As a result, every process  $z \in G$  sees every process  $u \in G$  as a voter to  $(\bar{\epsilon}, v, \perp)$ , for every  $v \in A$ . Thus,  $v \in \mathcal{RT}_z$  for every  $v \in A$ . Thus, it can apply the SPECIAL-ROOT-BOT RULE and will put  $\mathcal{RT}(\bar{\epsilon}) = \perp$  by the end of round 3, and will stop by the end of round 4.

To prove the 3rd claim, observe that the fault detection rules can be applied only in rounds 2 or 3. If a correct process did not send any message in round 2, it is because of applying EARLY\_IT-TO-RT RULE, and it's missing values will not cause any other correct process to be suspected as a faulty process, neither the correct process that did not send. By the end of the 2nd round  $\bar{\epsilon}$  will be in  $\mathcal{RT}_q$  for every  $q \in G$ , and no one will apply any fault detection rules anymore.

If all correct processes participated in round 2, then Not-Voter will not apply to any correct process. If any correct process did not send any message in round 3, it's missing values will not harm any correct process or itself and all correct processes will be in  $\mathcal{RT}$  by the end of the round. For similar reasons, the Not-Masking rule will not cause any correct process to be added to  $\mathcal{F}$ .  $\square$

The only case in which not all correct processes invoke a  $\mathcal{D}_\phi$  protocol is when some of the background running monitors are being invoked by some of the correct processes, while others may have already stopped. This special case is guaranteed to be when the inputs of all participating correct processes is  $\perp$ , and consensus can be still be achieved. [Lemma 1](#) implies the following:

**Corollary 1.** *For any  $(t, t)$ -adversary, and  $n \geq 3t + 1$ , if every correct process that invokes the protocol start with input  $\perp$ , then  $\perp$  is the output value at each participating correct process by the end of round 2, and each participating correct process completes the protocol by the end of round 3. Moreover, for  $p, q \in G$ , no  $p$  will add  $q$  to  $\mathcal{F}_p$ .*

The gossip exchange among correct processes about identified faults ensures the following:

**Lemma 2.** *For a  $(t, \phi)$ -adversary and protocol  $\mathcal{D}_\phi$ ,  $n \geq 3t + 1$ , assuming [Property 1](#), for any  $k$ ,  $1 \leq k \leq \phi + 1$ , by the end of round  $k$ , for every two correct processes  $p, q$ ,  $\mathcal{FA}_p \subseteq \mathcal{F}_q$  and  $\mathcal{FA}_p[k - 1] \subseteq \mathcal{FA}_p[k]$ .*

*Proof.* Prior to invocation the claim holds by [Property 1](#). In each round processes exchange their  $\mathcal{F}$  sets. If a process finds out that some process  $b$  appears in the lists of at least  $t + 1$  processes it adds  $b$  to  $\mathcal{F}$ , and if it appears in  $2t + 1$  lists it adds it to both  $\mathcal{F}$  and  $\mathcal{FA}$ . The  $\mathcal{F}$  and  $\mathcal{FA}$  sets are never decreased, and  $\mathcal{FA}$  is updated only through gossiping. Therefore, it is easy to see that by the end of each round the claim holds.  $\square$

A node may initially assign a value using one of the “put” rules and later it may color it to a different value. In the arguments below we sometimes need to refer to the value that was put to a node rather than the value it might be

colored to. Once a node has a value it is not assigned a value using any put rule any more. Thus, the value assigned using a put rule is an initial value that may be assigned to a node before it is colored, or that node may never have a value put to it. To focus on these put operations, we will add, for proof purposes, that whenever a node  $p$  uses a put rule for some  $\sigma$ , except ROUND  $\phi + 1$  RULE, it also puts  $\sigma$  in  $\mathcal{PT}_p$  (The ‘‘Put-Tree’’) and as a result at that moment,  $\mathcal{PT}_p(\sigma) = \mathcal{RT}_p(\sigma)$ . We do not color nodes in  $\mathcal{PT}_p$ , thus for  $\sigma$  that is colored, but was not assigned a value prior to that,  $\mathcal{PT}_p(\sigma)$  is undefined. We exclude ROUND  $\phi + 1$  RULE from  $\mathcal{PT}$  on purpose.

The following is the core statement of the technical properties of the protocol. The only way we found to prove all these is via an induction argument that proves all properties together. The theorem contains four items.

The detection part proves that correct processes are never suspected as faulty. The challenge is that the various rules instruct processes when to stop sending messages, and that might cause other correct processes to be suspected as faulty.

The validity part proves that if a correct process sends a value, it will reach the  $\mathcal{RT}$  of every other correct process within two rounds. It also proves that if a correct process decides not to send a value (thus, closed a branch), the appropriate node will be in  $\mathcal{RT}$  of every correct process. The third claim in the validity part is that if a process appears in  $\mathcal{FA}$ , then it appears in  $\mathcal{RT}$  of every correct process within two rounds.

The safety part intends to prove consistency in the  $\mathcal{RT}$ . The challenge is that coloring may cause the trees of correct processes to defer. Therefore the careful statements looks at  $\mathcal{PT}$ , and which rule was used in order to assign the value to it. The  $\perp$  value is a default value, therefore there is a special consideration of whether the value the process puts is  $\perp$  or not. The end result is that if a node appears in  $\mathcal{PT}$  of two correct processes, it carries the same value.

The liveness part shows that if a node appears in  $\mathcal{RT}$  of a correct process, it will appear in  $\mathcal{RT}$  of any other correct process within two rounds.

**Theorem 2.** *For a  $(t, \phi)$ -adversary and protocol  $\mathcal{D}_\phi$ ,  $n \geq 3t + 1$ , assuming [Property 1](#) and that all correct processes participate in the protocol, then for any  $1 \leq k \leq \phi + 1$ :*

1. **No False Detection:** *For  $p, q \in G$ , no  $q$  will add  $p$  to  $\mathcal{F}_q$  in round  $k$ .*
2. **Validity:**
  - (a) *For  $\sigma \in \Sigma_{k-3}$  if  $p \in G$ , sends  $\langle \sigma, p, d_p \rangle$ , then at the end of round  $k$ , at every correct process  $x$ , either  $\mathcal{RT}_x(\sigma p) = d_p$  or  $\exists \sigma' \sqsubset \sigma$  such that  $\sigma' \in \mathcal{RT}_x$ . For  $k = \phi + 1$ , the property holds also for any  $\sigma \in \Sigma_{k-2}$  and for any  $\sigma \in \Sigma_{k-1}$ .*
  - (b) *If  $z \in \mathcal{FA}$  in the beginning of round  $k - 2$ , then by the end of round  $k$ , at every correct process, either  $\mathcal{RT}(\sigma z) = \perp$  or  $\exists \sigma' \sqsubset \sigma$  such that  $\sigma' \in \mathcal{RT}$ . For  $k = \phi + 1$ , the property holds for  $z \in \mathcal{FA}$  in the beginning of rounds  $k - 1$  or  $k$ .*
  - (c) *For  $\sigma \in \Sigma_{k-1}$ , if  $p \in G$ , does not send  $\langle \sigma, p, d \rangle$  for any  $d \in D$ , then at the end of round  $k$ , at every correct process  $x$ ,  $\exists \sigma' \sqsubset \sigma$  such that  $\sigma' \in \mathcal{RT}_x$ .*
3. **Safety:** *For  $p, q \in G$ ,  $x \in N$ ,  $|\sigma x| \leq \phi$ ,  $\sigma x \in \mathcal{PT}_p[k]$ , then*
  - (a) *if  $p$  applies RESOLVE RULE to put  $\mathcal{PT}_p(\sigma x) = d$ ,  $d \neq \perp$ , and  $v$  is one of the  $\mathcal{RT}$ -confirmed nodes on  $(\sigma, x, d)$  in  $\mathcal{RT}_p$  used in applying this rule in  $\mathcal{RT}_p$ , and in addition  $\mathcal{PT}_q(\sigma xv) = \perp$ , then  $q$  applied SPECIAL-BOT RULE to put  $\sigma xv$ ;*
  - (b) *if  $|\sigma x| \geq 1$  and  $\mathcal{PT}_p(\sigma x) = d$ ,  $d \neq \perp$ , then, by the end of round  $k$ ,  $|V_q| \leq t$ , where  $V_q = \{u \mid \mathcal{PT}_q(\sigma xu) = \perp\}$ ;*
  - (c) *if  $|\sigma x| \geq 1$  and  $\mathcal{PT}_p(\sigma x) = \perp$  and it wasn't put using SPECIAL-BOT RULE, then, by the end of round  $k$ ,  $|V_q| \leq t$ , where  $V_q = \{u \mid \mathcal{PT}_q(\sigma xu) \neq \perp\}$ ;*
  - (d) *if  $\sigma x \in \mathcal{PT}_q[k]$ , then  $\mathcal{PT}_p(\sigma x) = \mathcal{PT}_q(\sigma x)$ .*
4. **Liveness:** *For  $p, q \in G$ , if  $\sigma \in \mathcal{RT}_p[k - 2]$  then  $\sigma \in \mathcal{RT}_q[k]$ . For  $k = \phi + 1$ , if  $\sigma \in \mathcal{RT}_p$  then  $\sigma \in \mathcal{RT}_q$ .*

*Proof of Theorem 2.* We prove the theorem by induction on  $k$ . We first prove the theorem assuming  $\phi > 1$  and will conclude by proving the theorem for the case  $\phi = 1$ .

As the proof is quite complex, we split it into three ranges,  $k = 1$ ,  $k \leq \phi - 1$ , and  $k \leq \phi + 1$ . We will prove the following claims, where each handles the appropriate range:

**Claim 1.** *Theorem 2* holds for  $k = 1$ .

The general case. This is where most of the technical challenge lies:

**Claim 2.** *Theorem 2* holds for  $1 < k \leq \phi - 1$ .

The final two rounds, when the resolve rules are slightly different:

**Claim 3.** *Theorem 2* holds for  $\phi - 1 < k \leq \phi + 1$ .

*Proof of Claim 1.* We will prove each of the four items separately.

*Proof of Item 1 for Claim 1.* (Detection) By the end of round 1, a process may add another to  $\mathcal{F}$  only through gossiping. [Property 1](#) implies that no correct process will suspect any other correct process. The rest of the fault detection rules are not applicable in the first round.  $\square$

*Proof of Item 2 for Claim 1.* (Validity) For  $k = 1$ , [Statement 2c](#) and [Statement 2b](#) vacuously hold, since there was no such round. For proving [Statement 2a](#) observe that in the first round only EARLY\_IT-TO-RT RULE is applicable. Assume that a correct process  $p \in G$  applies EARLY\_IT-TO-RT RULE by the end of round 1, thus node  $\sigma$  is  $\bar{\epsilon}$ , since  $\sigma = \epsilon$ . This implies that for every  $x \in N \setminus \mathcal{F}_p$ ,  $\mathcal{IT}_p(x) = d$ . Since  $G \cap \mathcal{F}_p = \emptyset$ , we conclude that for every correct process  $q$ ,  $d_q = d$ , and by the end of the 2nd round, by [Lemma 1](#), all correct processes will have  $\mathcal{RT}(\bar{\epsilon}) = d = d_p$  and we are done.  $\square$

*Proof of Item 3 for Claim 1.* (Safety) Only [Statement 3d](#) is applicable for  $k = 1$ . Notice that the only case in which  $\sigma x \in \mathcal{PT}_p[1]$  is when  $p$  applies EARLY\_IT-TO-RT RULE in the end of the 1st round and as a result puts some value  $d$  to the root node in its  $\mathcal{RT}_p$ . In such a case, it is clear that if  $\sigma \in \mathcal{PT}_q[1]$  then  $\mathcal{PT}_p(\sigma) = \mathcal{PT}_q(\sigma)$ .  $\square$

*Proof of Item 4 for Claim 1.* (Liveness) This item vacuously holds.  $\square$

This completes the proof of [Claim 1](#).  $\square$

Now we move to proving the main part of the theorem.

*Proof of Claim 2.* The proof is by induction. The base case is [Claim 1](#). Assume correctness for any  $k''$ ,  $1 \leq k'' < k$ , and we will prove the claim for  $k$ ,  $k \leq \phi - 1$ .

*Proof of Item 1 for Claim 2.* (Detection) The fault detection takes place in every round before any resolve rule is applied. By induction we know that a correct process will not add another correct process to  $\mathcal{F}$  using gossiping from other processes. The three rules to add a process to  $\mathcal{F}$  are based on the messages accumulated in  $\mathcal{IT}$ . The induction on  $k - 1$  allows us to determine what messages correct processes will be sending in round  $k$ .

Let round  $k$  be the first round at which a process  $p$  is not sending messages related to the branch of  $\sigma$ . There are three cases in which a correct process,  $p$ , stops sending, by using DECAY RULE, EARLY\_IT-TO-RT RULE and STRONG\_IT-TO-RT RULE. If  $p$  closes the branch of  $\sigma$  at the end of round  $k - 1$  and is not sending messages related to it in round  $k$ , the receive rule instructs correct processes what values to add to their  $\mathcal{IT}$ .

Let's consider the three fault detection rules. Not-Voter is not applicable, since in the previous round  $p$  sent its messages appropriately. Since  $p$  is correct every correct process that sends messages echo's the message it sent, and whenever a correct process applies the receiving rule to assign messages to processes that did not send messages in the current round it adds the message  $p$  originally sent. For the similar reason Not-IT-to-RT is not applicable.

The last fault detection rule is Not-Masking. Assume that a correct process  $q$  is expecting process  $p$  to mask away some process  $w$ . The Not-Masking rule allows  $q$  to mask the non-sending by  $\perp$ , but  $q$  will not add  $p$  to  $\mathcal{F}$  if by the end of the round  $q$  will have  $\exists \sigma' \sqsubseteq \sigma'' w$  such that  $\sigma' \in \mathcal{RT}$ . Thus,  $p$  will not be in  $\mathcal{F}$  during the processing of all the rules below. [Statement 2c](#) that is proved next guarantees that also by the end of the round a correct process  $p$  will not be added to  $\mathcal{F}$ .  $\square$

*Proof of Item 2 for Claim 2.* (Validity)

For Statement 2a, the case of  $k = \phi + 1$  is excluded for now. Assume that  $p$  sends  $\langle \sigma, p, d_p \rangle$  in round  $k - 2$ . If any correct process  $x$  is not sending a message  $\langle \sigma, x, d_x \rangle$ , then by the protocol it should have set either  $\sigma' \in \mathcal{PT}_x[k - 4]$  (if used DECAY RULE) or  $\sigma' \in \mathcal{PT}_x[k - 3]$  (if used EARLY\_IT-TO-RT RULE or STRONG\_IT-TO-RT RULE) for some  $\sigma' \sqsubset \sigma$ , and we are done by induction (Statement 3d). If there is a correct node  $x \in \sigma$ , then the claim holds by induction (Statement 2a). So we are left with the case that no correct node appears in  $\sigma$  and all correct processes are participating in round  $k - 2$ . By the end of round  $k - 2$  every correct process  $x$  will apply the receiving rule and will have  $\mathcal{IT}_x(\sigma p) = d_p$ .

If any correct,  $x$  ( $x \neq p$ ), doesn't send a message  $\langle \sigma p, x, d_p \rangle$  then we are done by induction, using similar argument as above. Therefore, by the end of round  $k - 1$ , every correct process will apply the receiving rule and will have  $n - t - 1$  children nodes for  $p$  in its  $\mathcal{IT}$ . Thus, by the end of round  $k - 1$ , for every  $x \in G$ , at every  $y \in G$ ,  $x$  is a supporter of  $x$  for  $(\sigma, p, d_p)$ . And for every  $x, y \in G$ , where  $x \neq y \neq v$ ,  $\mathcal{IT}_x(\sigma p y) = d_p$ . In round  $k$  some correct process (including  $p$ ) may not send messages and all the rest will send identical value  $d_p$  messages. The above implies that the receiving rule will assign to each correct process that does not send messages the identical value  $d$  at every correct process that still process messages for this branch.

As we argued before, since  $p$  itself is confirmed on each node it echoes, every correct process will be a voter and therefore, by the end of round  $k$ , at every correct process  $x \in G$ , that still process messages for this branch either  $\mathcal{RT}_x(\sigma p) = d_p$ , or  $\exists \sigma' \sqsubset \sigma p$  such that  $\sigma' \in \mathcal{RT}_x$ .

The proof of Statement 2b is identical to the above, as if it is the case of a correct process sending  $\perp$ .

Proving Statement 2c: Let  $\sigma \in \Sigma_{k-1}$  and  $p \in G$ . If  $p$  does not send any message  $\langle \sigma, p, d \rangle$  for any  $d \in D$  in round  $k$ , then either the branch was closed earlier and we are done by induction, or this is the first round any correct process doesn't send a message on this branch. Thus,  $p$  applied DECAY RULE, EARLY\_IT-TO-RT RULE or STRONG\_IT-TO-RT RULE by the end of round  $k - 1$ .

We will cover each of the closing rules separately.

Proving the claim in case  $p \in G$  uses DECAY RULE: by definition  $\exists \sigma' \sqsubset \sigma$  such that  $\sigma' \in \mathcal{RT}_p[k - 2]$ , which results in closing the branch by the end of round  $k - 1$  and not sending in round  $k$ . If  $\exists \sigma'' \sqsubset \sigma$ ,  $\sigma'' \in \mathcal{RT}_p[k - 3]$ , then we are done by induction. Otherwise, it must be because of messages received in round  $k - 2$ . All such messages are reflected in  $\mathcal{IT}_p$ . To influence a  $\sigma' \in \mathcal{RT}_p$ , it should be as a result of applying IT-TO-RT RULE, ROUND  $\phi + 1$  RULE, EARLY\_IT-TO-RT RULE, or STRONG\_IT-TO-RT RULE. Since  $k - 2 \neq \phi + 1$ , we conclude that it is not a result of applying ROUND  $\phi + 1$  RULE. If it is a result of  $p$  applying EARLY\_IT-TO-RT RULE, or STRONG\_IT-TO-RT RULE in round  $k - 2$  then this branch would be closed already by the end of round  $k - 1$  and we are done by induction. Similarly, if any other correct process closed the branch by the end of round  $k - 2$ , we are done by induction.

Assume now the case that it is a result of  $p$ 's using IT-TO-RT RULE. Thus, there should be some  $\bar{\sigma} w$ , such that  $\sigma' \sqsubseteq \bar{\sigma}$ ,  $\bar{\sigma} w \in \Sigma_{k-4}$  and  $p$  applied IT-TO-RT RULE in round  $k - 2$  to put it in  $\mathcal{RT}_p$  (and  $\mathcal{PT}_p$ , for proof purposes). Let  $d$  be the value assigned by  $p$  to  $\mathcal{PT}_p(\bar{\sigma} w)$  as a result of processing  $\mathcal{IT}_p$  by the end of round  $k - 2$ . If there is a correct node in  $\bar{\sigma} w$ , we are done by induction. Since this is not the case, then when  $p$  applied IT-TO-RT RULE it observed a set  $U$  of  $n - t$  processes in  $\mathcal{IT}_p$  that are voters of  $(\bar{\sigma}, w, d)$ , of which at least  $t + 1$  are correct processes. Let  $\bar{U}$  be the set of correct voters in  $U$ .

For each voter  $v \in \bar{U}$  there is a set of  $W_v$  of  $n - t$  processes that are confirmed on  $(\bar{\sigma}, w, d)$ , where  $v$  is a supporter to each  $u \in W_v$  on  $(\bar{\sigma}, w, d)$ . Since we assume that there is no correct nodes in  $\bar{\sigma} w$ ,  $v \neq w$ .

By definition, for each  $u \in W_v \setminus \{w, v\}$ ,  $\mathcal{IT}_p(\bar{\sigma} w u v) = d$ , and since  $v \in G$  and no correct process closed the branch or stopped sending yet, then by the end of round  $k - 2$ , for every  $x \in G \setminus \{u, v\}$ ,  $\mathcal{IT}_x(\bar{\sigma} w u v) = d$ . If  $v \in W_v$ , then all will also have  $\mathcal{IT}_x(\bar{\sigma} w v) = d$ .

For  $u \in G$ , since  $\bar{\sigma} w \in \Sigma_{k-4}$ , by induction,  $\mathcal{RT}_x(\bar{\sigma} w u v) = d$ , or  $\exists \sigma' \sqsubset \bar{\sigma} w u v$  such that  $\sigma' \in \mathcal{RT}_x$ , at every  $x \in G$ .

For  $u \notin G$ , by the end of round  $k - 1$ , for every  $x \in G$ , at every  $y \in G$ ,  $x$  is a supporter of  $x$  for  $(\bar{\sigma} w u, v, d)$ . And for every  $x, y \in G$ , where  $x \neq y \neq v$ ,  $\mathcal{IT}_x(\bar{\sigma} w u v y) = d$ . In round  $k$  some correct process (including  $p$ ) may not send messages and all the rest will send identical value  $d$  messages. The above implies that the receiving rule will assign to each correct process that does not send messages the identical value  $d$  at every correct process that still process

messages for this branch.

As we argued before, since  $v$  itself is confirmed on each node it echoes, every correct node will be a voters and therefore, by the end of round  $k$ , at every correct process  $x \in G$ , that still process messages for this branch, and for every  $u \in W_v$ , either  $\mathcal{RT}_x(\bar{\sigma}wuv) = d$ , or  $\exists \sigma' \sqsubset \bar{\sigma}wuv$  such that  $\sigma' \in \mathcal{RT}_x$ .

Now observe that each  $u \in W_v$ , being confirmed on  $(\bar{\sigma}, w, d)$ , has a set  $U_u$  of  $n - t$  of supporters in  $\mathcal{IT}_p$  of  $u$  for  $(\bar{\sigma}, w, d)$  (one of which is  $u$  itself). Let  $\bar{U}_u$  be the set of correct processes in  $U_u$ . By definition, for each  $u \in W_v$ ,  $\mathcal{IT}_p(\bar{\sigma}wu) = d$  and for each  $u' \in \bar{U}_u \setminus \{u\}$ ,  $\mathcal{IT}_p(\bar{\sigma}wu'u') = d$ . Since no correct process closed the brach or stopped sending, at every  $x \in G$ ,  $\mathcal{IT}_x(\bar{\sigma}wu'u') = d$ , and if  $u \in G$ , then  $\mathcal{IT}_x(\bar{\sigma}wu) = d$ . Thus, by the end of round  $k$ , at every correct process  $x \in G \setminus \{u, u'\}$ , that still process messages for this branch,  $\mathcal{PT}_x(\bar{\sigma}wu'u') = d$ , where  $u \in W_v$ , and  $u' \in \bar{U}_u \setminus \{u\}$ . Thus, each  $u \in W_v$ , is  $\mathcal{RT}$ -confirmed on  $(\bar{\sigma}, w, d)$  and each  $v \in \bar{U}$  is  $\mathcal{RT}$ -voter on  $(\bar{\sigma}, w, d)$ . The same holds, by definition, for  $u$  and  $u'$  if they did not closed the branch earlier. This implies that such  $x$  will apply RESOLVE RULE to assign  $\mathcal{PT}_x(\bar{\sigma}w) = d$  (or would observe by that time  $\exists \sigma' \sqsubset \bar{\sigma}w$  such that  $\sigma' \in \mathcal{RT}_x$ ), which completes the proof for this case.

Proving the claim in case  $p \in G$  uses EARLY\_IT-TO-RT RULE: Assume that a correct process  $p \in G$  applies EARLY\_IT-TO-RT RULE by the end of round  $k - 1$ . Let  $\sigma \in \Sigma_{k-2}$  and denote  $\sigma = \tau u$ . The assumption of  $p$ 's closing the branch implies, among other things, that for every  $x, y \in N \setminus \mathcal{F}_p$ , such that  $\tau ux, \tau uy \in \Sigma_k$ ,  $\mathcal{IT}_p(\tau ux) = \mathcal{IT}_p(\tau uy) = d$ , for some  $d \in D$ , and thus  $\mathcal{PT}_p(\tau u) = d$ . This also implies that every correct process  $x$  that applies the receiving rule in round  $k$  will assign  $\mathcal{IT}_x(\sigma p) = \mathcal{IT}_x(\sigma) = d$ . If there is any correct process in  $\tau$ , we are done by induction (Statement 2a on  $k - 1$ , since the correct processes sent in  $k - 3$  or earlier). If this is not the case, whether  $u$  is correct or not, we conclude that by the end of round  $k - 1$  every correct process  $x \in G$  will have  $\mathcal{IT}_x(\tau uy) = d$  for every  $y \in G \setminus \{u, x\}$ , and if  $u \in G$  then also  $\mathcal{IT}_x(\tau u) = d$ . This is true since by Lemma 2, and Item 1,  $G \cap \mathcal{F}_q = \emptyset$ . Thus, by the end of round  $k$  every correct process  $x$  that did not close the branch will use IT-TO-RT RULE to obtain  $\mathcal{RT}_x(\tau u) = d$  (or would observe by that time  $\exists \sigma' \sqsubset \tau u$  such that  $\sigma' \in \mathcal{RT}_x$ ), and we are done.

Proving the claim in case  $p \in G$  uses STRONG\_IT-TO-RT RULE: Assume that  $p$  applies STRONG\_IT-TO-RT RULE by the end of round  $k - 1$ . If there is a correct process in  $\sigma$ , we are done by induction. If  $\exists \sigma' \sqsubseteq \sigma$  such that  $\sigma' \in \mathcal{RT}_q[k - 1]$  for any correct  $q$ , we are also done. Otherwise, let  $\sigma \in \Sigma_{k-3}$ . By definition there exists  $U, U \cap \sigma = \emptyset, |U| = n - r + 2$  such that for every  $u, v \in U \setminus \mathcal{F}$ , where  $v \neq u$ ,  $\mathcal{IT}_p(\sigma uv) = \mathcal{IT}_p(\sigma vu)$ . Let  $x$  be the node such that  $\sigma x \in \Sigma$ , but  $x \notin U \cup \mathcal{F}$ . Since we assume that there is no correct process in  $\sigma$ ,  $G \subseteq U \cup \{x\}$ . Assume first that  $x$  is not correct. If this is the case, then the assumption on  $U$  implies that all members of  $U$  are supporters and voters and by the end of round  $k - 1$ ,  $\sigma$  would be in  $\mathcal{RT}$  of every correct process. If this is not the case, we are left with the option that  $x$  is correct but doesn't agree with some of the values all members of  $U$  sent. Denote by  $\bar{U}$  the correct member of  $U$ , and it is clear that  $|\bar{U}| = n - t - 1$  and  $|U| \geq n - t$ . The definition of the set  $U$  implies that by the end of round  $k - 1$ , either  $p$  puts  $\sigma$  in  $\mathcal{PT}_p$ , or  $\exists \sigma' \sqsubset \sigma$  such that  $\sigma' \in \mathcal{RT}_p$ . Moreover, by induction, for every member  $u$  of  $\bar{U}$ ,  $\sigma u \in \mathcal{RT}_q$  of every correct process  $q$  by the end of round  $k$ . Thus, by the end of round  $k$  every correct process  $q$  that doesn't already have  $\sigma \in \mathcal{RT}_q$  will be able to apply RELAXED RULE to put  $\bar{\sigma} \in \mathcal{RT}_q$ , and we are done.  $\square$

*Proof of Item 3 for Claim 2.* (Safety) Notice that when a process  $p$  puts a value to a node  $\sigma x$ , say in round  $k$ , then at that point in time  $\not\exists \sigma' \sqsubset \sigma$ , such that  $\sigma' \in \mathcal{RT}_p[k]$ .

Observe that if both  $p$  and  $q$  put values to  $\sigma x$  prior to round  $k$ , then the claims hold by induction on  $k$ . Therefore we limit ourselves to nodes which value  $q$  puts in its  $\mathcal{PT}$  in round  $k$  and  $p$  had put a value to that node in its  $\mathcal{PT}$  in some round  $k' \leq k$ . Moreover, we limit ourselves to the case where no correct process had put a value to that node in its  $\mathcal{PT}$  in any round  $k'' < k'$ .

We prove Item 3 by backward induction on the length  $\ell = |\sigma x|$  from  $\ell = k$  to 1. For each  $\ell$  we will go through all the put rules  $p$  could have applied in setting the value to  $\sigma x$  in round  $k$  or earlier, and for each rule we consider the relevant rules  $q$  could have apply, and we will prove that the four statements hold in each case.

The rules to put a value to a node in  $\mathcal{RT}$  (and  $\mathcal{PT}$ ) are: 1) IT-TO-RT RULE, 2) RESOLVE RULE, 3) RELAXED RULE, 4) SPECIAL-BOT RULE, 5) SPECIAL-ROOT-BOT RULE, 6) EARLY\_IT-TO-RT RULE, 7) STRONG\_IT-TO-RT RULE and 8) ROUND  $\phi + 1$  RULE.

The case  $\ell = k$ : A node of level  $k$ , where  $k \leq \phi$ , cannot be put in  $\mathcal{PT}$  by the end of round  $k$ .

The case  $1 \leq \ell < k$ : let  $|\sigma x| = \ell$  and assume correctness for every  $\ell' > \ell$ . Since  $k < \phi$ , ROUND  $\phi + 1$  RULE is

not applicable.

If there is a correct predecessor in  $\sigma$ , we are done by Item 2, since by the end of round  $\ell + 1$  process  $q$  will have  $\sigma x \in \mathcal{RT}_q$  (due to coloring), hence no node  $\sigma x u$  will be in  $\mathcal{PT}_q$  and all four statements clearly hold.

Otherwise, if process  $x$  is correct, by Item 2, by the end of round  $\ell + 2$  process  $q$  will have  $\sigma x \in \mathcal{RT}_q$ . A node  $\sigma x u$  can be in  $\mathcal{PT}_q$  only if  $q$  applied EARLY\_IT-TO-RT RULE, or STRONG\_IT-TO-RT RULE in that round, so any such node will also be set to the value of  $\sigma x$ , which is the same at both  $p$  and  $q$ , thus all four statements hold.

Otherwise, there is no correct process in  $\sigma x$ . Thus, node  $x$  has  $n - \ell$  children nodes, out of which at least  $n - t$  are correct and out of the  $t - \ell$  others, at most  $\phi - \ell$  are actively faulty and at least  $t - \phi$  are silent.

We start by proving the first three statements and after that we will prove the fourth statement.

► Consider the case that  $p$  used RESOLVE RULE to put  $\sigma x$ : RESOLVE RULE implies that there are  $t + 1$   $\mathcal{RT}$ -voters. Each  $\mathcal{RT}$ -voter has a set of  $n - t$  children nodes  $\mathcal{RT}$ -confirmed for  $(\sigma, x, d')$ . Define, in such a case, by  $V_p$  the set of children nodes of  $\sigma x$  that are  $\mathcal{RT}$ -confirmed to  $d'$  in  $\mathcal{PT}_p$ . By definition, each confirmed node in  $V_p$  has  $t + 1$  children nodes in  $\mathcal{RT}_p$  with the same value  $d'$ .

*Proof of Statement 3a of Item 3 for Claim 2.* By definition, confirmed is defined for  $\ell + 2 \leq k < \phi + 1$ . For node  $v$  being  $\mathcal{RT}$ -confirmed implies that there is a set  $V_d$ , such that for each  $v' \in V_d$ ,  $\mathcal{RT}_p(\sigma x v v') = d$ , where  $|V_d| = t + 1$ . If  $\sigma x v \in \mathcal{RT}_p$  when  $p$  puts  $\sigma x$ , then also  $\sigma x v \in \mathcal{PT}_p$ , otherwise  $\sigma x$  should be in  $\mathcal{RT}_p$  already. Moreover, if  $\sigma x v \in \mathcal{RT}_p$ , it should be that  $\mathcal{RT}_p(\sigma x v) = d$ , otherwise, by coloring,  $\mathcal{RT}_p(\sigma x v v')$  would also not be equal  $d$ . By induction, level  $\ell + 1$ , Statement 3d, we conclude that  $q$  can't put  $\sigma x v$  to  $\perp$ . Therefore, it should be the case that when  $p$  puts  $\sigma x$  to  $\mathcal{PT}_p$ ,  $\sigma x v \notin \mathcal{PT}_p$ . In such a case, all children nodes of  $\sigma x v$  that are in  $\mathcal{RT}_p$  are in  $\mathcal{PT}_p$ . Specifically, every  $v' \in V_d$  is in  $\mathcal{PT}_p$ . This also implies that  $v \notin G$ . By induction, on level  $\ell + 2$ , Statement 3d, we conclude that for every  $v' \in V_d$ , if  $\sigma x v v' \in \mathcal{RT}_q$  then  $\mathcal{PT}_p(\sigma x v v') = \mathcal{PT}_q(\sigma x v v') = d$ .

Node  $v$  has exactly  $n - \ell - 1$  children nodes. When  $q$  puts a value to node  $\sigma x v$ , all children nodes of node  $\sigma x v$  are not colored. There are at most  $n - \ell - 1 - (t + 1) < n - t$  children nodes of  $\sigma x v$  in  $\mathcal{PT}_q$  that are not in  $V_d$ .

Look at the rules  $q$  may use in order to put  $\sigma x v$  to  $\perp$ .

— Consider the case that  $q$  used IT-TO-RT RULE to put  $\sigma x v$  to  $\perp$ : If  $q$  applies IT-TO-RT RULE, then it should have for each voter  $e$  a set  $U_e$  of  $n - t$  processes confirmed on  $(\sigma x, v, \perp)$  in  $\mathcal{IT}_q$ . There is at least one process in the intersection of  $U_e$  and  $V_d$ . Denote it by  $u$ ,  $u \in U_e \cap V_d$ . Observe that the definition of  $V_d$  implies that  $u \neq v$ . Being confirmed implies that  $u$  has a set of at least  $t + 1$  correct processes  $U_u$  such that  $\mathcal{IT}_q(\sigma x v u u') = \perp$  for every  $u' \in U_u$ . For any such  $u'$  that sends messages in this round,  $\mathcal{IT}_p(\sigma x v u u') = \perp$ . If there is  $u'$  that closed the branch using DECAY RULE, then it did so before round  $k - 2$ , and we are done by induction. Otherwise it used EARLY\_IT-TO-RT RULE and both  $q$  and  $p$  would assign it the same value, and therefore we also conclude that  $\mathcal{IT}_p(\sigma x v u u') = \perp$ . If it used STRONG\_IT-TO-RT RULE, then there is a set  $U'$  of at least  $t + 1$  correct processes such that  $\mathcal{IT}_p(\sigma x v u u') = \mathcal{IT}_q(\sigma x v u u') = \perp$ , since all but one send the same value, and  $q$  saw  $n - t$  of them.

We now argue that if  $p$  has such a set of children node, it implies that if  $\sigma x v u \in \mathcal{PT}_p$ , then  $\mathcal{PT}_p(\sigma x v u) = \perp$ .

Consider the various put rules  $p$  can use to put a value to  $\mathcal{PT}_p(\sigma x v u)$ . Thus, if  $p$  uses EARLY\_IT-TO-RT RULE in round  $\ell + 3$  it should be to the value  $\mathcal{IT}_p(\sigma x v u) = \perp$ . If  $p$  applies IT-TO-RT RULE in round  $\ell + 4$  it should be the case that  $\mathcal{IT}_p(\sigma x v u) = \perp$ . By the end of round  $\ell + 5$ , all the correct children nodes in  $U_u$  (or  $U'$ ), by Item 2, will be in  $\mathcal{PT}_p$  with value  $\perp$  and will color their subtrees in  $\mathcal{RT}_p$  to  $\perp$ . Therefore, if  $p$  applies any rule to put the value of  $\sigma x v u$ , it will be to  $\perp$ . This contradicts the fact that  $u \in V_d$ .

— Consider the case that  $q$  used RESOLVE RULE to put  $\sigma x v$  to  $\perp$ : If  $q$  applies RESOLVE RULE, then it should have a set  $U_e$  of  $\mathcal{RT}$ -confirmed on  $(\sigma x, v, \perp)$  in  $\mathcal{PT}_q$ . Each  $u$  in  $U_e$  has a set  $W_u$  of size  $t + 1$  such that for each  $u' \in W_u$   $\mathcal{PT}_q(\sigma x v u u') = \perp$ . Since, at least one of the nodes in  $U_e$  is in  $V_d$ , there is a contradiction to the induction on Statement 3b.

— Consider the case that  $q$  used RELAXED RULE to put  $\sigma x v$  to  $\perp$ : Contradiction, to Statement 3d.

Thus, we are left with the option of  $q$  applying SPECIAL-BOT RULE put  $\sigma x v$  to  $\perp$ , proving the statement.  $\square$

*Proof of Statement 3b of Item 3 for Claim 2.* In this case, potentially some nodes from  $V_p$  (though at most one) may resolve to  $\perp$ . Observe that node  $\sigma x$  in  $\mathcal{RT}_q$  has at most  $n - \ell - (n - t) = t - \ell$  children nodes outside  $V_p$ . Since  $\ell \geq 1$ ,

for the claim not to hold there should be at least 2 nodes from  $V_p$  that resolve to  $\perp$ . Statement 3a and the definition of SPECIAL-BOT RULE imply that at most one node can be resolved using SPECIAL-BOT RULE. We are done since  $t - \ell + 1 < t + 1$ .  $\square$

*Proof of Statement 3c of Item 3 for Claim 2.* The observation above implies that every node in  $V_p$  that is put in  $\mathcal{RT}_q$  should be with value  $\perp$ . Thus, proving this case.  $\square$

► Consider the case that  $p$  used IT-TO-RT RULE to put  $\sigma x$ :  
Statement 3a is not applicable in this case, and the rest of the cases we discuss next.

*Proof of Statement 3b of Item 3 for Claim 2.* The IT-TO-RT RULE implies that in  $\mathcal{IT}_p$  there is a set  $V$  of  $n - t$  voters of  $(\sigma, x, d)$ , where  $d \neq \perp$ . Each  $v \in V$  has a set  $W_v$  of  $n - t$  processes that are confirmed on  $(\sigma, x, d)$ , where  $v$  is a supporter to each  $u \in W_v$  on  $(\sigma, x, d)$ . Each such  $u$ , being confirmed on  $(\sigma, x, d)$ , has a set  $U_u$  of  $n - t$  supporters in  $\mathcal{IT}_p$  to  $u$  on  $(\sigma, x, d)$ . Each of these sets of size  $n - t$  contains at least  $t + 1$  correct nodes. Let  $U_\perp$  be the set of children nodes, where each one has at most  $t$  correct supporters to  $(\sigma, x, d)$  in  $\mathcal{IT}_p$ . The above implies that  $|U_\perp| \leq t - \ell$  (notice that  $U_\perp \subseteq N \setminus W_v$ ).

Assume by contradiction that  $q$  has  $|V_q| > t$  children nodes of  $\sigma x$  in  $\mathcal{PT}_q$  such that  $\mathcal{PT}_q(\sigma x u) = \perp$  for each  $u \in V_q$ . Therefore, there must exist two nodes,  $y_1, y_2 \in V_q$  that are not from the set  $U_\perp$  (because  $\ell \geq 1$  so  $|U_\perp| \leq t - \ell \leq t - 1$ ).

We now go through the put rules  $q$  can apply to put values to the children nodes of  $\sigma x$ . We will also study the minimal round at which  $q$  can apply these put rules. Since  $\mathcal{RT}_q(\sigma x)$  can't have a value when the put rule is applied by  $q$  to the children nodes of  $\sigma x$ , the earliest round at which  $q$  can use any other rule to put its value, if at all, is the end of  $\ell + 2$ .

For round  $\ell + 2$  : If  $\ell + 2 \leq k$ , then by the end of round  $\ell + 2$ , it can't be that all echoing processes to  $y_1$  or  $y_2$  have sent the value  $\perp$ . Thus, by the end of round  $\ell + 2$ ,  $q$  cannot have either  $y_1$  or  $y_2$  in  $\mathcal{RT}_q$  with value  $\perp$ , and the claim holds.

For round  $\ell + 3$  : If  $\ell + 3 \leq k$ , then by the end of round  $\ell + 3$ , each  $y \in \{y_1, y_2\}$  has  $t + 1$  correct children that are supporters for  $d$  in  $\mathcal{IT}_q$  and therefore  $y$  can't be in  $\mathcal{PT}_q(\sigma x y)$  for value  $\perp$ . Thus, by the end of round  $\ell + 3$ ,  $q$  can have at most  $t - \ell$  children nodes of  $\sigma x$  in  $\mathcal{RT}_q$  with value  $\perp$ , and the claim holds.

If  $\ell + 4 \leq k$ , then by the end of round  $\ell + 4$ , by Item 2, the value of all correct nodes in all sets  $V$ ,  $W_v$  and  $U_u$  above are already in  $\mathcal{RT}_q$ . This implies that  $y_1$  and  $y_2$  each has at least  $t + 1$  children nodes in  $\mathcal{RT}_q$  with value  $d$ . The value of neither  $y_1$  nor  $y_2$  can be put to  $\perp$  using rules RESOLVE RULE, or RELAXED RULE, and clearly not SPECIAL-ROOT-BOT RULE. We already excluded EARLY\_IT-TO-RT RULE, STRONG\_IT-TO-RT RULE, and IT-TO-RT RULE, so the only rule that may be applied is SPECIAL-BOT RULE. But SPECIAL-BOT RULE can be applied only when all other sibling nodes are already in  $\mathcal{RT}_q$ , so it can be applied to either  $y_1$  or  $y_2$  but not to both. A contradiction. This completes the proof of Statement 3b for this case, assuming  $p$  used IT-TO-RT RULE to put the value of  $\mathcal{RT}_p(\sigma x)$ .  $\square$

*Proof of Statement 3c of Item 3 for Claim 2.* The proof is identical to the proof of Statement 3b with a small change, except that SPECIAL-BOT RULE does not produce a value that is different than  $\perp$ .  $\square$

► Consider the case that  $p$  used EARLY\_IT-TO-RT RULE in order to put  $\sigma x$ .

*Proof of Statement 3b of Item 3 for Claim 2.* The EARLY\_IT-TO-RT RULE implies that in  $\mathcal{IT}_p$  there is a set  $U, U \cap \{u' \mid u' \in \sigma x\} = \emptyset, |U| = n - \ell$ , such that for every  $u, v \in U \setminus \mathcal{F}, \mathcal{IT}(\sigma x u) = \mathcal{IT}(\sigma x v)$ . Assume first that no correct process closes the branch by the end of round  $\ell + 1$ . This implies that  $q$  will also see all correct processes sending the same value. Therefore, it can't apply any rule on its  $\mathcal{IT}_q$  to put any child of  $\sigma x$   $\mathcal{PT}_q$  with a value of  $\perp$ . By the end of round  $\ell + 3$ , by Item 2, the value of all correct nodes in  $U$  are already in  $\mathcal{RT}_q$ . This implies that  $q$  can't have a set  $V_q$  of more than size  $t$  for any different value.

Now, if there is  $u \in U$  that closed the branch and did not send in round  $\ell + 1$ , then by the end of round  $\ell + 1$ , by Statement 2c, at every correct process  $q, \exists \sigma' \sqsubset \sigma x$  such that  $\sigma' \in \mathcal{RT}_q$ , which implies that by the end of  $\ell + 1$ ,  $\sigma x \in \mathcal{RT}_q$ , contradicting our assumption.  $\square$

*Proof of Statement 3c of Item 3 for Claim 2.* The proof is identical to the proof of Statement 3b with a small change, except that SPECIAL-BOT RULE does not produce a value that is different than  $\perp$ .  $\square$

► Consider the case that  $p$  used STRONG\_IT-TO-RT RULE in order to put  $\sigma x$ .

*Proof of Statement 3b of Item 3 for Claim 2.* Assume for contradiction that  $\exists V_q$  such that  $|V_q| = t + 1$ , where  $V_q = \{u \mid \mathcal{PT}_q(\sigma x u) = \perp\}$ . The STRONG\_IT-TO-RT RULE implies that in  $\mathcal{IT}_p$ , by the end of round  $\ell + 2$ , there is a set  $U$ ,  $U \cap \{u' \mid u' \in \sigma\} = \emptyset$ ,  $|U| = n - \ell + 1$  such that for every  $u, v \in U \setminus \mathcal{F}$ , where  $v \neq u$ ,  $\mathcal{IT}_p(\sigma x u v) = \mathcal{IT}_p(\sigma x v u) = d$ .

Assume first that no correct process closes the branch by the end of round  $\ell + 2$ . This implies that  $\mathcal{IT}_q$  will include all values above appearing in  $\mathcal{IT}_p$  for correct processes. We assume that there is no correct process in  $\sigma x$ , and that  $|\sigma x| \geq 1$ . Therefore  $|\mathcal{F}_q \setminus \{u' \mid u' \in \sigma x\}| < t$ . Moreover, also  $|\mathcal{F}_p \cup \mathcal{F}_q \setminus \{u' \mid u' \in \sigma x\}| < t$ . Therefore, there should be at least two processes in  $V_q$  that are not in  $\mathcal{F}_q$ . Therefore, there should be  $y \in V_q$  such that  $y \in U \setminus (\mathcal{F}_p \cup \mathcal{F}_q)$ . By the definition of  $U$ , there is a set  $U_q$  of  $n - t - 1$  correct processes such that  $\mathcal{IT}_q(\sigma x y u) = d$ , for  $u \in U_q$ . Therefore, by the end of round  $\ell + 3$   $q$  can't have  $\mathcal{PT}_q(\sigma x y) = \perp$ .

Since  $p$  applied STRONG\_IT-TO-RT RULE by the end of round  $\ell + 2$ , by the end of  $\ell + 3$ , by Statement 2c,  $\sigma x \in \mathcal{RT}_q$ , so  $\mathcal{PT}_q(\sigma x y)$  will never be set to  $\perp$ . A contradiction.  $\square$

*Proof of Statement 3c of Item 3 for Claim 2.* The proof is identical to the proof of Statement 3b with a small change, except that SPECIAL-BOT RULE does not produce a value that is different than  $\perp$ .  $\square$

► Consider the case that  $p$  used RELAXED RULE to put  $\sigma x$ : In this case when  $p$  applies the rule, all its children nodes are in  $\mathcal{PT}_p$ . By induction (Statement 3d), none of these children nodes will appear with a conflicting value in  $\mathcal{PT}_q$ . Since  $n - t - 1$  of them are with the same value  $d'$ , then at most  $n - \ell - (n - t - 1) = t - \ell + 1$  are with a different value. RELAXED RULE is applied only when  $\ell \geq 1$ . This immediately implies that Statement 3b and Statement 3c hold.

We completed the proof of the first 3 statements. We now prove the last one.

*Proof of Statement 3d of Item 3 for Claim 2.* If  $|\sigma x| \geq 1$ , then Statement 3b and Statement 3c clearly prove that Statement 3d holds, unless  $p$  uses SPECIAL-BOT RULE to put  $\sigma x$ . The proof above covers the case that  $q$  uses any rule other than SPECIAL-BOT RULE, by symmetry between  $p$  and  $q$  in this statement. Thus, we are left with the case that both are using SPECIAL-BOT RULE, and clearly both put  $\perp$ .

We are left to consider the case  $|\sigma x| = 0$ , thus  $\sigma x = \bar{\epsilon}$ . For that we need to consider all put rules that  $p$  and  $q$  may have applied. There are 3 applicable rules, IT-TO-RT RULE, RESOLVE RULE, and SPECIAL-ROOT-BOT RULE, to put a value to  $\bar{\epsilon}$ . Notice that SPECIAL-BOT RULE and RELAXED RULE are not applicable and EARLY\_IT-TO-RT RULE, or STRONG\_IT-TO-RT RULE were covered in Statement 2c.

Node  $\bar{\epsilon}$  has  $n$  children nodes, out of which at least  $n - t$  are correct and out of the  $t$  others, at most  $\phi$  are actively faulty and at least  $t - \phi$  are silent. Notice that for  $\bar{\epsilon}$ , every child node that is in  $\mathcal{RT}_p$  is also in  $\mathcal{PT}_p$ , since once we assign a value to  $\bar{\epsilon}$  we do not process any other node.

► Consider the case that  $p$  used EARLY\_IT-TO-RT RULE or STRONG\_IT-TO-RT RULE to put a value to  $\bar{\epsilon}$ : Both rules imply that  $p$  sees a unanimous echoing by all  $n$  processes, with the exception of at most one process. Since we assume that all correct processes participate, there is no way that  $q$  will put a different value to  $\bar{\epsilon}$ .

► Consider the case that  $p$  used IT-TO-RT RULE to put  $\bar{\epsilon}$  and that  $\mathcal{RT}_p(\bar{\epsilon}) = \perp$ : The basic arguments are the same as in the case  $\ell \geq 1$ , but the set of put rules that  $q$  may apply differ. If  $q$  also uses IT-TO-RT RULE, then the claim clearly holds. If  $q$  uses SPECIAL-ROOT-BOT RULE, then it obtains the same value. So we are left with the case of  $q$  using RESOLVE RULE. The arguments are the same as in the case  $\ell \geq 1$ , which exclude the possibility that  $q$  puts any value other than  $\perp$  to  $\bar{\epsilon}$ , completing the proof of this case.

► Consider the case that  $p$  used IT-TO-RT RULE to put  $\bar{\epsilon}$  and that  $\mathcal{RT}_p(\bar{\epsilon}) = d$ ,  $d \neq \perp$ : We now need to consider the possibility of  $q$  using IT-TO-RT RULE, RESOLVE RULE and SPECIAL-ROOT-BOT RULE. The arguments for the first two are the same as above and are left out.

For using SPECIAL-ROOT-BOT RULE node  $q$  should have a set  $V_q$ ,  $|V_q| = t + 1$ , such that for each  $v \in V_q$ ,  $\mathcal{RT}_q(v) = \perp$ . Notice that also here there is no difference between  $\mathcal{RT}_q(v)$  and  $\mathcal{PT}_q(v)$ .

The IT-TO-RT RULE implies that in  $\mathcal{IT}_p$  there is a set  $V_p$  of  $n - t$  voters of  $(\bar{\epsilon}, \epsilon, d)$ . Each  $v \in V_p$  has a set of  $W_v$  of  $n - t$  children nodes such that  $v$  is a supporter to each  $u \in W_v$  on  $(\bar{\epsilon}, \epsilon, d)$ , and each such  $u$  has a set  $U_u$  of  $n - t$  supporters in  $\mathcal{IT}_p$  to  $(\bar{\epsilon}, \epsilon, d)$ . Each of these sets of size  $n - t$  contains at least  $t + 1$  correct nodes. Thus, there is a set  $U_\perp$  of size at most  $t$  that does not have at least  $t + 1$  correct supporters to  $(\bar{\epsilon}, \epsilon, d)$ .

Thus, there should be a process  $x \in V_q$  that has a set  $U_x$  of  $n - t$  supporters in  $\mathcal{IT}_p$  to  $(\bar{\epsilon}, \epsilon, d)$ . The set contains a set  $\bar{U}_x$  of at least  $t + 1$  correct processes that are also supporters in  $\mathcal{IT}_q$  to  $(\bar{\epsilon}, \epsilon, d)$ . Consider the various rules  $q$  can apply to put a value  $\perp$  to  $\mathcal{RT}_q(x)$ . By the end of the 2nd round it can apply EARLY\_IT-TO-RT RULE to set a  $\perp$  to it, because all processes in  $\bar{U}_x$  send a different value. For that reason it can't apply IT-TO-RT RULE in the end of round 3 to put value  $\perp$  to  $\mathcal{RT}_q(x)$ . By the end of round 4 for every process  $y \in \bar{U}_x$   $\mathcal{PT}_q(xy) = d$ . Process  $q$  can't apply SPECIAL-BOT RULE to put a value  $\perp$  to  $x$ , since that rule is not applicable for  $|x| = 1$ . RESOLVE RULE, RELAXED RULE or STRONG\_IT-TO-RT RULE, can't be used to put  $\perp$ . Since we assume that  $k < \phi$ , the case  $\phi = 1$  is not relevant, Therefore also ROUND  $\phi + 1$  RULE can't be applied either - and we are done.

► Consider the case that  $p$  used RESOLVE RULE to put  $\bar{\epsilon}$ : If  $q$  uses IT-TO-RT RULE, by symmetry we are done. If  $q$  also uses RESOLVE RULE, by definition both obtain the same value. We are left with the case that  $q$  uses SPECIAL-ROOT-BOT RULE. The interesting case is that  $\mathcal{RT}_p(\bar{\epsilon}) = d, d \neq \perp$ . Observe that we cannot use the induction on  $k = 1$  since the set of applicable rules differ. The arguments for proving the case are similar to the previous case, the case of IT-TO-RT RULE, since  $q$  can't apply SPECIAL-BOT RULE to any node in level 1.

► Consider the case that  $p$  used SPECIAL-ROOT-BOT RULE to put  $\bar{\epsilon}$ : If  $q$  also uses it the claim holds. Otherwise it falls into the other rules discussed above.

This completes the proof of Statement 3d. □

This completes the proof of Item 3 (Safety) for Claim 2. □

*Proof of Item 4 for Claim 2.* (Liveness) It is enough to prove that if  $p \in G$  puts  $\sigma x \in \mathcal{PT}_p$  in some round  $r \leq k$ , then by the end of round  $\max(r + 2, \phi + 1)$   $\sigma x \in \mathcal{RT}_q$ , for every  $q \in G$ .

We prove the lemma by backward induction on  $\ell = |\sigma x|$ , from  $\ell = k$  to  $\ell = 1$ . As in the proof of Item 3, the claim clearly holds for  $\ell = k$ , since no node of level  $k, k < \phi + 1$  can be added to  $\mathcal{PT}$  by the end of round  $k$ . The case  $\ell = k - 1$  is applicable only to EARLY\_IT-TO-RT RULE, and is covered by the proof of Statement 2c.

Assume the induction for any  $k \geq \ell' > \ell$  and we will prove for  $\ell, \ell \leq \phi - 1$ . If  $\sigma x$  contains a correct node then by induction on Item 2 we are done. So assume that there is no correct process in  $\sigma x$ . Let  $p$  be the first to put  $\sigma x$ , where  $\sigma x \in \mathcal{PT}_p$ , and let  $r$  be the round at which it did that. Consider the various possible put rules.

► Case  $p$  applied EARLY\_IT-TO-RT RULE, or STRONG\_IT-TO-RT RULE Statement 2c implies the proof.

► Case  $p$  applied IT-TO-RT RULE: By definition, this can happen only in round  $r = \ell + 2$ . The IT-TO-RT RULE implies that there are  $t + 1$  correct voters of  $(\sigma, x, d)$  in  $\mathcal{IT}_p$ , each having  $n - t$  nodes, each of which is confirmed on  $(\sigma, x, d)$  in  $\mathcal{IT}_p$ . Let  $U_x$  be the set of the confirmed nodes on  $(\sigma, x, d)$  in  $\mathcal{IT}_p$  and  $V_e$  the set of correct voters. Observe that  $U_x$  contains at least  $t + 1$  correct processes.

If by round  $r + 1$   $\sigma x \in \mathcal{RT}_q$  we are done. If not, then if for any  $u \in U_x$   $\sigma x u \in \mathcal{RT}_q$ , it should be in  $\mathcal{PT}_q$ , and it should be with a value  $d$ , because of using either IT-TO-RT RULE, EARLY\_IT-TO-RT RULE, or STRONG\_IT-TO-RT RULE by  $q$ , and it can't obtain a different value, because of the correct processes in  $U_x$  and  $V_e$ .

If by round  $r + 2$   $\sigma x \in \mathcal{RT}_q$  we are done. If not, Item 2 implies that by  $\max(r + 2, k)$  all voters in  $V_e$  will appear in  $\mathcal{RT}_q$  as  $\mathcal{RT}$ -voters on  $(\sigma, x, d)$ , since the nodes in  $U_x$  will be confirmed to  $(\sigma, x, d)$ . These arguments and Item 3 imply that if any of them is colored, it should be colored to  $d$ . Therefore,  $q$  can apply RESOLVE RULE to add  $\sigma x$  to  $\mathcal{PT}_q$  and we are done.

► Case  $p$  applied RESOLVE RULE: By definition, assuming that no branch closing took place, this can happen only in some round  $r \geq \ell + 4$ . Assume first that  $\ell \geq 1$ , we later deal with smaller values of  $\ell$ . If by the end of round  $r + 2$  process  $q$  puts a value to  $\sigma x$  or to a predecessor of  $\sigma x$ , we are done. Otherwise, by the induction hypothesis, by  $r + 2$ , each node involved in applying RESOLVE RULE by  $p$  to  $\sigma x$  in  $\mathcal{PT}_p$  is either colored or its value put by  $q$  in  $\mathcal{RT}_q$ . We will show that by  $r + 2$  process  $q$  can apply one of the rules to put a value to  $\sigma x$  in  $\mathcal{PT}_q$ .

Let  $V_p$  be that set of children nodes of  $\sigma x$  that are  $\mathcal{RT}$ -confirmed to  $d'$  in  $\mathcal{RT}_p$ . By Statement 3d, for every  $v \in V_p$ , if  $\sigma x v \in \mathcal{PT}_p$  and  $\sigma x v \in \mathcal{PT}_q$ , then  $\mathcal{PT}_p(\sigma x v) = \mathcal{PT}_q(\sigma x v)$ .

None of the nodes in  $V_p$  can be confirmed to a different value than  $d'$  in  $\mathcal{RT}_q$ , unless it was put by  $q$  to a different value. If  $d' \neq \perp$  this can happen to the value of  $\perp$  and by Statement 3a, this can happen only using SPECIAL-BOT RULE. Thus, there can be at most one such node  $z \in V_p$  that was set to  $\perp$  by  $q$ .

If none was set using SPECIAL-BOT RULE, then by  $r + 2$  process  $q$  should see the same set of voters that  $p$  did and is able to apply RESOLVE RULE. Otherwise, it should have applied the SPECIAL-BOT RULE to one of the nodes in  $V_p$ . Before it can apply SPECIAL-BOT RULE, all other children nodes of  $\sigma x$  should be put to a value. After applying SPECIAL-BOT RULE to node  $\sigma x z$  all the children nodes of  $\sigma x$  have a value in  $\mathcal{RT}_q$ . For every  $y \in V_p$  the value is  $d'$ , so  $q$ , by that time, would have at least  $n - t - 1$  children nodes set to  $d'$ . Thus,  $q$  can apply RELAXED RULE to put a value to  $\sigma x$  and the claim holds.

In the case of  $\ell = 1$ , by definition  $q$  can't apply SPECIAL-BOT RULE to set a value to  $z$ . And therefore it should have been able to use RESOLVE RULE to set a value to  $\sigma x$ . The case of  $\ell = 0$  is similar to the case of  $\ell = 1$ .

► Case  $p$  applied RELAXED RULE: since  $p$  applies this rule, all the children nodes of  $\sigma x$  are put to a value in  $\mathcal{PT}_p$  and by induction by  $r + 2$  also at  $q$ . If  $\sigma x \in \mathcal{RT}_q$ , we are done. Otherwise, by Statement 3d their value is the same as for  $p$  and process  $q$  can also apply RELAXED RULE.

► Case  $p$  applied SPECIAL-BOT RULE or SPECIAL-ROOT-BOT RULE: exactly as in the previous case.

This completes the proof of Item 4 (Liveness) for Claim 2. □

This completes the proof of Claim 2. □

We can now complete the proof of the Theorem by covering the case of  $k \in \{\phi, \phi + 1\}$

*Proof of Claim 3.* We cover both cases for each item.

*Proof of Item 1 for Claim 3.* (Detection) There is no special issues that surface in the last two round regarding detection, and the proof for the case  $k < \phi$  holds. □

*Proof of Item 2 for Claim 3.* (Liveness)

► Consider the case  $k = \phi$ : There is no difference between the arguments for this case and those of  $k < \phi$ .

► Consider the case  $k = \phi + 1$ : If  $|\sigma x| = \phi$  and if any correct process is not sending in this round it is because of applying the  $\mathcal{RT}[r - 3]$  limitation, and by induction we are done. Otherwise, if  $z$  sends, then ROUND  $\phi + 1$  RULE completes the proof. The case  $|\sigma x| < \phi$  is identical to that of  $k < \phi$ .

The proof of Statement 2b is similar to the case in which a correct process sends  $\perp$  in the first round (Statement 2a). □

*Proof of Item 3 for Claim 3.* (Safety) Item 3 is not applicable in case  $k = \phi + 1$ .

Consider the case  $k = \phi$ . The case  $|\sigma x| = \phi$ : A value to a node at this level can't be put at any round  $\leq \phi$ . Observe that two correct processes may put conflicting values in their  $\mathcal{RT}$  to a node  $\sigma xy$  at level  $\phi + 1$  that is associated with a faulty process, since they may have conflicting values in their  $\mathcal{IT}$  for that node. This may happen only if there wasn't any correct predecessor of  $x$  in  $\sigma$ , since Item 2 implies that before assigning  $y$  a value it would already be colored. By Property 1, there is no conflict on all the  $t - \phi$  faulty nodes that are initially in  $\mathcal{FA}$ . Thus, there can be at most one faulty node in level  $\phi + 1$ . Item 2 also implies that during round  $\phi + 1$  node  $\sigma x$  will be assigned a value by all correct processes, and therefore so will node  $\sigma xy$ .

Statement 3a is not applicable in the case of  $|\sigma x| = \phi$ .

*Proof of Statement 3c for Claim 3.* Node  $\sigma x$  was put to  $\perp$  by process  $p$ . By the assumption of Statement 3c, SPECIAL-BOT RULE wasn't applied. ROUND  $\phi + 1$  RULE is not applicable, since we are in level  $\phi$ . IT-TO-RT RULE and RESOLVE RULE are not relevant, since there is only a single level of nodes in  $\mathcal{IT}$  or  $\mathcal{RT}$ . SPECIAL-ROOT-BOT RULE is relevant only for the case of  $\sigma x = \bar{e}$ , which can't happen for  $|\sigma x| = \phi$ . If process  $p$  uses EARLY\_IT-TO-RT RULE, or STRONG\_IT-TO-RT RULE, then similar arguments to those used in the proof of Statement 2c can be used.

We are left with RELAXED RULE. Node  $\sigma x$  has  $n - t - 1$  children nodes in  $\mathcal{RT}_p$  all having the value  $\perp$  and all but one are clearly correct nodes. Since there are exactly  $n - \phi - 1$  nodes in level  $\phi + 1$ , and there can be at most

$n - \phi - 1 - (n - t - 2) = t - \phi + 1$  nodes holding a non  $\perp$  value. Thus, node  $q$  can't have  $t + 1$  or more children nodes with a value not  $\perp$  when it applies it's put operation; Completing the arguments for Statement 3c.  $\square$

*Proof of Statement 3b for Claim 3.* Node  $\sigma x$  was put to  $d$ ,  $d \neq \perp$  by process  $p$ . Thus, SPECIAL-BOT RULE is not applicable and, as in Statement 3c, we are left with RELAXED RULE. Node  $\sigma x$  has  $n - t - 1$  children nodes in  $\mathcal{RT}_q$  all having the value  $d$  and all but one are clearly correct nodes. Since there are exactly  $n - \phi - 1$  nodes in level  $\phi + 1$ , and there can be at most  $n - \phi - 1 - (n - t - 2) = t - \phi + 1$  nodes holding a non  $d$  value. Thus, node  $q$  can't have  $t + 1$  or more children nodes with a value not  $d$  when it applies it's put operation; completing the arguments for Statement 3b.  $\square$

*Proof of Statement 3d for Claim 3.* Case  $d = \perp$ , if  $\sigma x \in \mathcal{PT}_q$ , then by Statement 3c, the only applicable rules for  $q$  are RELAXED RULE, or SPECIAL-BOT RULE. Both will result in validating the claim. Case  $d = \not\perp$ , if  $\sigma x \in \mathcal{PT}_q$ , then by Statement 3b it is clear that the only possible rule to be applied is RELAXED RULE, which results in validating the claim for Statement 3d.  $\square$

For node  $|\sigma x| < \phi - 1$  identical arguments to those used in the proof of Claim 2 complete the proof of Item 3 (Safety) for Claim 3.  $\square$

*Proof of Item 4 for Claim 3.* (Liveness) The arguments for this item are the same for  $k = \phi$  and  $k = \phi + 1$ . As we mentioned before, it is enough to prove that if  $p \in G$  puts  $\sigma x \in \mathcal{PT}_p$  in some round  $r$ , then by the end of  $\max(r + 2, \phi + 1)$   $\sigma x \in \mathcal{RT}_q$ , for every  $q \in G$ . The proof is by backward induction on  $\ell = |\sigma x|$ .

Case  $\ell = \phi + 1$ . The only round at which a process can put a value to a node in level  $\phi + 1$  in it's  $\mathcal{RT}$  is during round  $\phi + 1$ . At that round, every correct process that doesn't have  $\sigma x$  in its  $\mathcal{RT}$  as a colored node, will insert it to its  $\mathcal{RT}$  using ROUND  $\phi + 1$  RULE.

Case  $\ell = \phi$ . Either  $p$  used EARLY\_IT-TO-RT RULE, or STRONG\_IT-TO-RT RULE or it set the value in round  $\phi + 1$ . If it used EARLY\_IT-TO-RT RULE, or STRONG\_IT-TO-RT RULE, then Statement 2c completes the proof. Now we need to consider the various potential put rules  $p$  applied in round  $\phi + 1$  in order to put the value for  $\sigma x$ . IT-TO-RT RULE and RESOLVE RULE are not applicable in this case.

► Case  $p$  applied RELAXED RULE: If exists a correct process in  $\sigma$  then by Item 2 we are done. If  $x \notin G$  then all children nodes of  $\sigma x$  are either correct or silent, and if  $p$  applies the rule, every correct process can apply the same rule. If  $x \in G$ , then there are  $n - t - 1$  correct children nodes of  $\sigma x$ , all of which will send the same value, and all will apply the RELAXED RULE, completing the proof of this case.

► Case  $p$  applied SPECIAL-BOT RULE: using similar arguments as above, this case is applicable only if  $x \notin G$ , and as the arguments above show, if any correct process applies this rule, all will.

For node  $|\sigma| < \phi - 1$  identical arguments to those used in the proof of Claim 2 complete the proof of this case.  $\square$

This completes the proof of Claim 3.  $\square$

We now prove the theorem for the case of  $\phi = 1$ .

By assumption there is at most one faulty process, say  $b$ , that doesn't appear in  $\mathcal{FA}$  of any correct process. There are at most two rounds of information exchange.

In the first round every process sends its input value. By the end of the first round, at every  $z$ ,  $\mathcal{IT}_z(\bar{e}) = d_z$ ,  $\mathcal{IT}_z(z) = d_z$ , and for every  $x \in N \setminus \mathcal{F}_z$ ,  $\mathcal{IT}_z = d_x$ , where  $d_x$  is the value received from  $x$ , and for every  $y \in \mathcal{F}_z$ ,  $\mathcal{IT}_z = \perp$ . The only rule that may be applied by a correct process by the end of this round is the EARLY\_IT-TO-RT RULE.

Assume that  $z$  applies the EARLY\_IT-TO-RT RULE by the end of round 1. This can happen only when all inputs are  $\perp$  or when  $\mathcal{F}_z = \emptyset$  and all input values are identical. If this happen,  $z$  sets  $\mathcal{RT}_z(\bar{e}) = \mathcal{IT}_z(\bar{e}) = d_z$ .  $z$  does not send any message in round 2. Following that, every correct process  $p$  that doesn't stop sends to every process the set of values it entered to  $\mathcal{IT}_p(x)$  for every  $x \in N$ . If a correct process  $z$  stops, all these values are identical, other than the values associated with  $b$ . Moreover, for  $z$  and any other correct process that did not send a message, all correct processes add to their  $\mathcal{IT}$  the same value for it. By the end of round 2, every correct process,  $p$ , that did not stop

applies ROUND  $\phi + 1$  RULE to copy  $\mathcal{IT}_p(\sigma)$ , for  $\sigma \in \Sigma_2$  to  $\mathcal{RT}_p(\sigma)$ . By the previous discussion it is clear that all will have identical values regarding all node, other than maybe the nodes on  $\sigma$  that include  $b$ . Therefore, every correct process  $p$  will be able to apply RELAXED RULE and will put the same value to  $\bar{e}$ .

This discussion shows, implicitly that all the items of the theorem hold for this case.

Now consider the case that no correct  $z$  stopped at the end of round 1. In the second round every correct process sends to every process the set of values it entered to  $\mathcal{IT}_p(x)$  for every  $x \in N$ . By the end of round 2 every correct process,  $p$ , applies ROUND  $\phi + 1$  RULE to copy  $\mathcal{IT}_p(\sigma)$ , for  $\sigma \in \Sigma_2$  to  $\mathcal{RT}_p(\sigma)$ . By the end of the second round, for every  $p, q, z$  correct processes  $\mathcal{RT}_p(zp) = \mathcal{RT}_p(zq) = \mathcal{RT}_q(zp)$ .

Since  $b$  is the only potentially faulty process we conclude that for every  $p, q, z \in N \setminus \{b\}$ ,  $\mathcal{RT}_p(bz) = \mathcal{RT}_q(bz)$ .

We now show that the theorem holds in this case.

To prove that Item 2 (Validity) holds, let's look at its three statements. Statement 2c vacuously holds. Statement 2a holds, since for every correct process that sends in the last round there is consensus. For every  $p$  in  $G$  that sends in the first round, as we mentioned before, all processes, but  $b$ , sent the same value  $d_p$  that  $p$  sent in the first round, and by applying RELAXED RULE, which can be applied to node  $p$ , all reach consensus. For every  $p \in \mathcal{FA}$ , the same arguments hold.

To prove that Item 3 holds, let's look at its four statements.

*Proof of Statement 3a when  $\phi = 1$ .* By definition, node  $p, p \in G$ , can apply RESOLVE RULE only on node  $\bar{e}$ . Assume it resolved to  $d, d \neq \perp$ . By definition  $p$  observed at least 2 processes as voters to  $d$ , and it identified  $n-t$   $\mathcal{RT}$ -confirmed nodes. All correct processes among them will never resolve to  $\perp$ . The only possibility that another correct process  $q$  can resolve any to  $\perp$  is node  $b$ . If node  $b$  is  $\mathcal{RT}$ -confirmed, it has at least 2 children nodes  $x, y$  such that  $\mathcal{RT}_p(bx) = \mathcal{RT}_p(by) = \perp$ . Since both  $x$  and  $y$  are necessarily correct processes, we conclude that  $\mathcal{RT}_q(bx) = \mathcal{RT}_q(by) = \perp$ . Moreover, for all  $\mathcal{RT}$ -confirmed nodes  $z$  in  $\mathcal{RT}_p$ , except of node  $b$ ,  $\mathcal{RT}_p(z) = \mathcal{RT}_q(z) = d$ , since all are correct. The only rule  $q$  may be able to apply to resolve  $b$  to  $\perp$  is SPECIAL-BOT RULE. But SPECIAL-BOT RULE is not applicable to nodes of level 1.  $\square$

*Proof of Statement 3b and Statement 3c when  $\phi = 1$ .* These statements clearly hold since  $\mathcal{PT}_p$  is defined only for nodes in level 1, and  $\mathcal{PT}_q$  is not defined for level  $\phi + 1$ .  $\square$

*Proof of Statement 3d when  $\phi = 1$ .* Consider three cases, if  $x \in G$ , then by Item 2 we conclude equality. Consider the case that  $x = b$ . In this case, as we wrote above, for every  $p, q, z \in N \setminus \{b\}$ ,  $\mathcal{RT}_p(bz) = \mathcal{RT}_q(bz)$ . Therefore, if  $p$  applied a rule to conclude  $b \in \mathcal{PT}_p$ , so will  $q$ . We are left with the case of  $x = \bar{e}$ . As we just proved, on every node of level 1,  $p$  and  $q$  agrees. All but one of them are nodes associated with correct processes. The only node on level 2 on which  $p$  and  $q$  differ is node  $xb$ . But because of coloring, both color node  $xb$  by the value of  $x$ . Therefore, on every node  $\sigma, |\sigma| \geq 1$  if  $\sigma \in \mathcal{RT}_p$ , then  $\sigma \in \mathcal{RT}_q$ . Therefore, every rule  $p$  applies holds also for  $q$ . This completes the proof of Statement 3d.  $\square$

To prove that Item 4 holds consider the 3 possible levels. ROUND  $\phi + 1$  RULE implies that it holds for level  $\phi + 1$ . Statement 3d proves the rest of the cases.

To prove that Item 1 holds observe that by Property 1, it holds initially. In the first round, no detection takes place. In the 2nd round, no correct process suspects any other correct process.

This completes the proof of Theorem 2.  $\square$

The following Theorem summarizes the properties needed from our protocol.

**Theorem 3.** For a  $(t, \phi)$ -adversary and protocol  $\mathcal{D}_\phi$  and  $n \geq 3t+1$  and assuming that all correct processes participate in the protocol:

1. Every correct process outputs the same value.
2. If the input values of all correct processes are the same, this is the output value. Every correct process outputs it by round 2 and stops by round 3.

3. If  $t + 1$  of the correct processes hold an input value of  $\perp$ , then all correct processes output  $\perp$  by the end of round 3 and stop by the end of round 4.
4. If the actual number of faults is  $f_\phi < \phi$ , then all correct processes complete the protocol by the end of round  $f_\phi + 2$ .
5. If the actual number of faults is  $f_\phi = 0$ , and all correct processes start with the same initial value, then all correct processes complete the protocol by the end of round 1.
6. If the actual number of faults is  $f_\phi = 1$ , and all correct processes start with the same initial value, then all correct processes complete the protocol by the end of round 2.
7. If a correct process outputs in round  $k$ , it stops by the end of round  $k + 1$ .
8. If a correct process stops in the end of round  $k$ , all correct processes output by round  $k + 1$  and stop by round  $k + 2$ .

*Proof of Theorem 3.*

**Proof of Statement 1:** By definition a correct process outputs a value once it identifies a frontier. It is clear that by the end of round  $\phi + 1$  there is a frontier for every correct process. Define the front of  $\mathcal{RT}$  to be:  $\sigma x$  is in the front of  $\mathcal{RT}$  if exists  $p \in G$  such that  $\sigma x \in \mathcal{RT}_p$  and for every  $q \in G$ ,  $\sigma \notin \mathcal{RT}_q$ . [Theorem 2](#) implies that if  $\sigma$  is in the front of process  $p$ , within two rounds it will be in the front of any other correct process. Since all correct processes shares the front, then if  $\bar{\epsilon} \in \mathcal{RT}_p$ , it will be at every other correct process and vice versa. Since a process does not stop for two rounds after it holds a frontier the first claim holds.

**Proof of Statement 2:** [Lemma 1](#) proves the second claim.

**Proof of Statement 3:** The proof of [Theorem 2](#) implies that SPECIAL-ROOT-BOT RULE can be applied by the end of round 3 if there are  $t + 1$  correct processes that start with input  $\perp$ . Thus, the third claim holds.

**Proof of Statement 4:** Observe that if the actual number of faults is  $f_\phi$  and  $f_\phi < \phi$ , then for every  $\sigma \in \Sigma_{\phi+1}$  there is a prefix of length  $k$ ,  $k \leq f_\phi + 1$  in which a correct process appears as the last node. If  $k \leq \phi - 1$  then by [Theorem 2](#), by  $k + 2$  every correct process will have that prefix in its  $\mathcal{RT}$  and will be able to apply DECAY RULE to close the branch by the end of round  $\phi + 2$ .

Consider a prefix  $\tau p$  of length  $\phi + 1$ . By assumption  $\tau$  contains all faulty processes. Therefore, by the end of round  $\phi + 2$ , every correct process will be able to apply EARLY\_IT-TO-RT RULE to add  $\tau p$  to  $\mathcal{RT}$  and will close the branch. Observe that sometimes more than one rule can be applied, but since we go down from the later rounds to the earlier ones, we happen to close the branch earlier.

We are left with the case of  $\tau p$  of length  $\phi$ . There is at most one corrupt node, say  $x$ , that can send values relating to  $\tau p$  that will be added to the  $\mathcal{IT}$  of correct processes in rounds  $\phi + 1$  and round  $\phi + 2$ . In round  $\phi + 1$  all correct processes becomes children nodes and by the end of round  $\phi + 2$  all will add  $\tau p$  to their  $\mathcal{PT}$  and would be able to apply STRONG\_IT-TO-RT RULE to close the branch.

Thus, in all cases, by the end of round  $\phi + 2$  all correct processes will close all branches and can output a value.

**Proof of Statement 5:** since there are no faults, all correct processes apply EARLY\_IT-TO-RT RULE by the end of the first round to set a value to  $\bar{\epsilon}$ .

**Proof of Statement 6:** since there is a single fault, all correct processes apply STRONG\_IT-TO-RT RULE by the end of the 2nd round to set a value to  $\bar{\epsilon}$ .

**Proof of Statement 7:** The branch closing rules immediately imply that there can be at most one round between adding the final value to  $\mathcal{RT}$  that produces the frontier, thus providing output, and closing of all branches that imply stopping the protocol.

**Proof of Statement 8:** The first part of the statement holds, since if  $p$  stops by the end of round  $k$ , it doesn't send anything in round  $k + 1$ . [Theorem 2](#) (Statement 2c) imply that by the end of that round every correct process will output a value, and by the previous statement all will stop by the end of  $k + 2$ .  $\square$

## 4 Monitors

We follow the approach of [[BG93](#), [GM93](#), [GM98](#)] with some modifications for guaranteeing early stopping.

In round  $r = 1$  we run  $\mathcal{D}_t$  using the initial values. For each integer  $k$ , in round  $1 < r = 1 + 4k < t - 1$  we invoke protocol  $\mathcal{D}_{t-1-4k}$  whose initial values is either  $\perp$  (meaning everything is OK) or BAD (meaning that too many corrupt processes were detected). We call this sequence of protocols the *basic monitor sequence*. We will actually run 4 such sequences.

## 4.1 The Basic Monitor Protocol

Each process  $z$  stores two variables:  $v \in D$ , the current value, and *early*, a boolean value. Initially  $v$  equals the initial input of process  $z$  and *early* := *false*. Later, *early* = *true* will be an indicator that the next decision protocol must decide  $\perp$  (because there is not enough support for BAD). Each process remembers the last value of *early* <sub>$q$</sub>  it received from every other process  $q$ , even if  $q$  did not send one recently.

Throughout this section we use the notation:  $\bar{r} \equiv r \pmod{4}$ .

---

### Algorithm 1: The Basic Monitor protocol (at process $z$ )

---

```

1: if  $\bar{r} = 1$ :
2:   if  $r < t - 1$  then invoke protocol  $\mathcal{D}_{t+1-r}$  with initial value  $v_z$ ;
3: if  $\bar{r} = 2$ :
4:   at the end of the round:
5:     if  $|\mathcal{FA}| \geq r + 3$  then set  $v_z := \text{BAD}$ 
6:     otherwise set  $v_z := \perp$ ;
7: if  $\bar{r} = 3$ :
8:   send  $v_z$  to all;
9:   at the end of the round:
10:    if  $|\{q \mid v_q = \text{BAD}\}| \leq t$  then set  $\text{early}_z := \text{true}$ 
11:    otherwise set  $\text{early}_z := \text{false}$ ;
12: if  $\bar{r} = 0$ :
13:   send  $\text{early}_z$  to all;
14:   at the end of the round:
15:     if  $|\{q \mid \text{early}_q = \text{true}\}| \geq t + 1$  then set  $v_z := \perp$ ;
16:     if every previously invoked protocol produced an output then set  $v_z := \perp$ .

```

---

The monitor protocol runs in the background until the process halts. The monitor protocol invokes a new  $\mathcal{D}_\phi$  protocol every 4 rounds. In each round, the monitor's lines of code are executed before running all the other protocols, and its end of round lines of code are executed before ending the current round in all currently running protocols. This is important, since it needs to detect, for example, whether all currently running protocols produced outputs for determining its variable for the next round. At the end of each round the monitor protocol applies the `monitor_halt` and `monitor_decision` rules below to determine whether to halt all the running protocols at once, or only to commit to the final decision value.

When a process is instructed to apply a `monitor_decision` it applies the following definition. If it is instructed to halt (`monitor_halt`), then if it did not previously apply the `monitor_decision`, it applies `monitor_decision` first and then halts all currently running protocols that were invoked by the monitor at once.

**Definition 1** (`monitor_decision`). *A process that did not previously decide, **decides** BAD, if any previously invoked protocol outputs BAD. Otherwise, it decides on the output of  $\mathcal{D}_t$ .*

When a process is instructed to decide without halting, it may need to continue running all protocols for few more rounds to help others to decide. We define “halt by  $r + x$ ” to mean continue to run all active protocols until the end of round  $\min\{r + x, t + 1\}$ , unless an halt is issued earlier.

## 4.2 Monitor Halting and Decision Conditions

Given that different processes may end various invocations of the protocols in different rounds we need a rule to make sure that all running protocols end by the end of round  $f + 2$ . The challenge in stopping all protocols by the end

of  $f + 2$  is the fact that individual protocols may end at round  $f + 2$  and we do not have a room to exchange extra messages among the processes. This also implies that we need to have a halting rule at every round of the monitor protocol, since  $f + 2$  may occur at any round.

Each halting rule implies how other rules need to be enforced in later rounds, since any process may be the first to apply a `monitor_halting` at a given round and we need to ensure that for every extension of the protocols, until everyone decides, all will reach the same decision despite the fact that those that have halted are not participating any more. The conditions take into account processes that may have halted. A process considers another one as halted if it doesn't receive any message from it in any of the concurrently running set of invoked protocols, monitors and the gossiping of  $\mathcal{F}$ .

To achieve that we add the following set of rules.

**Monitor Halting Rules:**

- $H_{\text{BAD}}$ . Apply `monitor_halting` if any monitor stops with output BAD. Otherwise if any monitor outputs BAD, apply `monitor_decision` now and `monitor_halting` by  $r + 2$ .
- $H_1$ . Case  $\bar{r} = 1$ :
- (a) If all previously invoked protocols stopped, apply `monitor_halting`.
  - (b) Otherwise, if only the latest invoked protocol did not stop and  $|\{q \mid \text{early}_q = \text{true or } q \text{ halted}\}| \geq n - t$ , then apply `monitor_halting`.
  - (c) Otherwise, if only the latest invoked protocol did not stop and  $|\{q \mid \text{early}_q = \text{true or } q \text{ halted}\}| \geq t + 1$ , then apply `monitor_decision` now and `monitor_halting` by  $r + 2$ .
- $H_2$ . Case  $\bar{r} = 2$ :
- (a) If all previously invoked protocols stopped, apply `monitor_halting`.
  - (b) Otherwise, if only the latest invoked protocol did not stop and  $|\{q \mid \text{early}_q = \text{true or } q \text{ halted}\}| \geq n - t$  was true in the previous round, then apply `monitor_halting`.
  - (c) Otherwise, if only the latest invoked protocol did not stop and  $|\{q \mid \text{early}_q = \text{true or } q \text{ halted}\}| \geq t + 1$  was true in the previous round, then apply `monitor_decision` and now and `monitor_halting` by  $r + 1$ .
- $H_3$ . Case  $\bar{r} = 3$ : If all previously invoked protocols stopped, apply `monitor_halting`.
- $H_4$ . Case  $\bar{r} = 0$ : If all previously invoked protocols stopped and  $|\{q \mid \text{early}_q = \text{true or } q \text{ halted}\}| \geq n - t$  then apply `monitor_halting`.

**Lemma 3.** *If  $n > 3t$  and there are  $f$ ,  $f \leq t$ , corrupt processes then all correct processes apply `monitor_halting` by the end of round  $\min(t + 1, f + 2)$ .*

*Proof.* We need to show that all previously invoked protocols halt by the end of round  $\min(t + 1, f + 2)$ . Observe that **Theorem 3** (Statement 4), implies that  $\mathcal{D}_t$  itself is stopped by  $\min(t + 1, f + 2)$ .

By definition, protocol  $\mathcal{D}_\phi$  is invoked in round  $r_\phi$ , where  $\phi = t + 1 - r_\phi$ . By **Theorem 3** (Statement 4),  $\mathcal{D}_\phi$  is stopped by  $\min(\phi + 1, t_\phi + 2)$ , if the upper bound on the number of faults (that were not detected by all correct processes before invoking the protocol) is  $t_\phi$ . Note that if the number of faults that are not detected by all is higher than  $t_\phi$  the protocol may not stop by  $\phi + 1$ .

Let's study the number of faults that are not detected by all correct processes when  $\mathcal{D}_\phi$  is invoked. **Figure 1** Line 3 indicates that if any correct  $p$  sets  $v_p := \text{BAD}$  in round  $r_\phi - 3$ , then, by **Lemma 2**, the number of faults that are not detected by all correct processes when  $\mathcal{D}_\phi$  is invoked is at most  $t - r_\phi$ . In such a case, by **Theorem 3**,  $\mathcal{D}_\phi$  will be stopped by round  $\min(\phi + 1, t_\phi + 2)$ , where  $t_\phi \leq t - r_\phi$ . Let us call these  $\mathcal{D}_\phi$  regular-protocols.

If no correct  $p$  sets  $v_p := \text{BAD}$ , then all correct processes invoke  $\mathcal{D}_\phi$  with  $v = \perp$ , therefore no matter how many faults are present (as long as not more than  $t$ ), **Lemma 1** guarantees that  $\mathcal{D}_\phi$  is stopped within 3 rounds, and all outputs are obtained within 2 rounds. Let us call these  $\mathcal{D}_\phi$  fast protocols.

For regular-protocols we need to prove that the extra conditions hold. In addition, for fast-protocols we need also to prove that the protocol that was invoked recently will also stop in time.

Let us consider the  $r \pmod 4$  round at which  $\min(t + 1, f + 2)$  falls.

**Case  $\min(t + 1, f + 2) \pmod 4 = 0$ :** By  $H_4$  we need to show that all previously invoked protocols will be stopped and that  $|\{q \mid \text{early}_q = \text{true or } q \text{ halted}\}| \geq n - t$ , at every correct process.

For regular-protocols, since all are stopped by round  $\min(t + 1, f + 2)$  then when correct processes executed Line 3, just before stopping, none would set  $v := \text{BAD}$ . Therefore, all will set  $v$  to  $\perp$  and later *early* to *true*. Thus, the extra property for  $H_4$  holds, and all will halt.

For fast-protocols, since no process sets  $v$  to  $\text{BAD}$ , every previously invoked protocol stops within at most 3 rounds (Theorem 3, Statement 2). The latest protocol was invoked 3 rounds ago, and we are done. The arguments for the extra condition in  $H_4$  are the same as for the regular-protocols.

**Case**  $\min(t + 1, f + 2) \pmod{4} = 3$ : By  $H_3$  we need to show that all previously invoked protocols will be stopped.

The arguments for regular-protocols and for fast protocols are the same, the latest invocation was two rounds ago, and therefore, by Theorem 3 (Statement 2), by the end of the current round all will be stopped.

**Case**  $\min(t + 1, f + 2) \pmod{4} = 2$ : By  $H_2$  we need to show that either all previously invoked protocols have stopped by the end of the current round, or all but the last one and the extra condition holds.

If  $\min(t + 1, f + 2) = t + 1$ , then no protocol was invoked in the previous round, by definition. All previous regular or fast protocols will be stopped by the end of the current round.

If  $\min(t + 1, f + 2) = f + 2$ , by Theorem 3 (Statement 4), using similar arguments as above, all previous protocols will be stopped by the end of the current round, except, maybe the last protocol that was invoked in the previous round. Observe that correct processes set up their  $v$  four rounds ago. Since the current round is  $f + 2$ , then the round at which the processes executed Line 3 in Figure 1 is  $f - 2$  and therefore no process could have more than  $f$  faults, and would have set  $v := \perp$ . Therefore, every correct process that haven't halt yet would send *early* = *true* two rounds ago, and therefore the extra condition for  $H_2$  holds.

**Case**  $\min(t + 1, f + 2) \pmod{4} = 1$ : By  $H_1$  we need to show that either all previously invoked protocols have stopped by the end of the current round, or all but the last one and the extra condition holds.

If  $\min(t + 1, f + 2) = t + 1$ , then no protocol was invoked in the current round, by definition. All previous regular or fast protocols will be stopped by the end of the current round.

If  $\min(t + 1, f + 2) = f + 2$ , by Theorem 3 (Statement 4) using similar arguments as above, all previous protocols will be stopped by the end of the current round, except, maybe the last protocol that was invoked in the previous round. Observe that correct processes set up their  $v$  three rounds ago. Since the current round is  $f + 2$ , then the round at which the processes executed Line 3 in Figure 1 is  $f - 1$  and therefore no process could have more than  $f$  faults, and would have set  $v := \perp$ . Therefore, every correct process that haven't halt yet would send *early* = *true* two rounds ago, and therefore the extra condition for  $H_1$  holds.  $\square$

**Lemma 4.** *If the first process applies monitor\_halt in round  $r$  on  $d$  then every correct process applies monitor\_decision by round  $\min\{r + 4, f + 2, t + 1\}$ , applies monitor\_halt by round  $\min\{r + 5, f + 2, t + 1\}$ , and obtains the same decision value,  $d$ .*

*Proof.* Let  $p$  be a correct process applying monitor\_halt in the earliest round that any correct process applies it.

Observe that in some of the halting rules a process decides before the last invoked protocol outputs a value. There may be cases that one process halts and other processes continue to run and even invoke an additional protocol after the halting. We later prove that whenever these cases happen, the decision value is the same and it not  $\text{BAD}$ . We show that any protocol whose output is not taken into account by any correct process must output  $\perp$ .

Consider first the case that  $p$  halts with output  $\text{BAD}$ . By Theorem 3 (Statement 1 and Statement 8), if  $p$  halts with output  $\text{BAD}$  and if the output of that protocol is not ignored by any correct process then all correct processes will output  $\text{BAD}$  by next round and will halt within two rounds. This will lead to unanimous decision.

So pending on the fact that we later prove that any protocol whose output is not taken into account by any correct process will output  $\perp$ , we are left to consider the case that  $p$  does not output  $\text{BAD}$ .

If  $r = \min(t + 1, f + 2)$ , we are done by Lemma 3 (and Theorem 3, Statement 1). Since every correct process considers the outputs of the same set of protocols, the decision value is the same at every correct process.

Consider the various halting rules used by  $p$  to apply monitor\_halt, and let  $r$  be the round at which it was applied.

**Case**  $p$  uses  $H_1$ : There are three possibilities, one in which  $p$  noticed that all previously invoked protocols stopped. In this case, Theorem 3 (Statement 8) implies that all correct processes will observe that all previously invoked protocols

reported output by the end of  $r + 1$  and will observe that all previously invoked protocols have stopped by the end of round  $r + 2$  and will use rule  $H_3$  to apply `monitor_halt`. All correct obtain the same decision value, since all will consider the same set of protocols and, by [Theorem 3](#) (Statement 1) and the decision rule, will decide the same.

Otherwise, when  $p$  executed round  $r$  it noticed that by the end of that round all previous protocols stopped and only the one that started at the beginning of round  $r$  did not stop yet and the values of `early` that  $p$  received in round  $r - 1$  imply that  $|\{q \mid \text{early}_q = \text{true or } q \text{ halted}\}| \geq n - t$ . Since no process halted earlier, in round  $r - 1$  every correct process sets  $v := \perp$ . By [Lemma 1](#), the protocol that started in round  $r$  will produce output of  $\perp$  in round  $r + 1$  at all correct processes that did not stop earlier, and will stop by round  $r + 2$ . Thus, every correct process will apply either  $H_2$  or  $H_3$  and will reach the same decision.

Otherwise, when  $p$  executed round  $r - 2$  it noticed that by the end of that round all previous protocols stopped and only the one that started at the beginning of round  $r - 2$  did not stop yet. Moreover,  $p$  received at the beginning of round  $r - 3$ ,  $|\{q \mid \text{early}_q = \text{true or } q \text{ halted}\}| \geq t + 1$ . Since no correct halted earlier, the instruction to set the value for `early` implies that there was a correct process  $q$  that set its `earlyq` to `true` in round  $r - 4$ . Thus,  $q$  received less than  $t$  BAD. This implies that there are  $t + 1$  correct processes with  $v = \perp$ . [Lemma 1](#), implies that the last protocol starting in the beginning of round  $r - 2$  will output value  $\perp$  by the end of round  $r$  and stop by the end of round  $r + 1$ . By the end of round  $r$  all correct processes will observe the outputs of all previously invoked protocols. Therefore, by the end of round  $r + 1$  all correct processes that did not apply `monitor_halt` already, will either be able to apply `monitor_halt` by the end of that round, or will set  $v := \perp$ , since all previously invoked protocols produced output and even stopped. Since the latest invoked protocol is guarantee to produce an output of  $\perp$ , those that have halted will reach the same decision. Notice that those processes that do not halt will start another protocol in which every correct process that invoked it has input  $\perp$  and the rest are not participating. By [Corollary 1](#), by the end of round  $r + 3$  they will decide the same decision value and will halt by the end of round  $r + 4$ .

**Case  $p$  uses  $H_2$ :** As in the previous case, there are three possibilities, one in which  $p$  noticed that all previously invoked protocols stopped. In this case, [Lemma 1](#) implies that all correct processes will observe that all previously invoked protocols reported output by the end of  $r + 1$  and have stopped by the end of round  $r + 2$ . Some may use rule  $H_3$  or rule  $H_4$  to apply `monitor_halt` and decide the same, and some will invoke the next protocol with input  $\perp$  and will reach the same decision by round  $r + 4$  and will halt by the end of round  $r + 5$ .

Otherwise, when  $p$  executed round  $r$  it noticed that by the end of that round all previous protocols stopped and only the one that started at the beginning of round  $r - 1$  did not stop yet and the values of `early` that  $p$  received in round  $r - 2$  imply that  $|\{q \mid \text{early}_q = \text{true or } q \text{ halted}\}| \geq n - t$ . Since no correct process halted earlier, in round  $r - 2$  every correct process sets  $v := \perp$ . The protocol that started in round  $r - 1$  will produce output of  $\perp$  in round  $r$  and stop by round  $r + 1$ . Thus, every correct process will reach the same decision and will use rule  $H_3$  to halt by the end of round  $r + 1$ .

Otherwise, when  $p$  executed round  $r - 1$  it noticed that by the end of that round all previous protocols stopped and only the one that started at the beginning of round  $r - 2$  did not stop yet. Moreover,  $p$  received in round  $r - 3$ ,  $|\{q \mid \text{early}_q = \text{true or } q \text{ halted}\}| \geq t + 1$ . And since no correct process halted earlier, as in the case for halting rule  $H_1$ , we are done.

**Case  $p$  uses  $H_3$ :** Here we need to consider the case were all previously invoked protocols were stopped. In this case every other correct process that did not apply `monitor_halt` in round  $r$  will notice currently running protocols producing outputs by the end of round  $r + 1$  ([Theorem 3](#), Statement 8) and stopping by the end of round  $r + 2$ . Therefore, by the end of in round  $r + 1$  every correct process that will not halt by the end of round  $r + 1$  will set  $v := \perp$ . Thus, all correct processes participating in the new protocol in round  $r + 2$  will have an input  $\perp$ , and every correct process not participating will assume to have an input  $\perp$ . Thus, ([Corollary 1](#)) by the end of round  $r + 3$  that protocol produces an output, and all decides the same decision value and halt by the end of round  $r + 4$ .

**Case  $p$  uses  $H_4$ :** Here we need to consider the case where all previously invoked protocols were stopped, and, in addition,  $p$  observes  $|\{q \mid \text{early}_q = \text{true or } q \text{ halted}\}| \geq n - t$ , which leads to halting by the end of round  $r$ . In this case, every other correct process that did not apply `monitor_halt` in round  $r$  will notice all previously invoked protocols producing outputs by the end of round  $r + 1$  and stopping by the end of round  $r + 2$  ([Theorem 3](#), Statement 8). The property  $|\{q \mid \text{early}_q = \text{true or } q \text{ halted}\}| \geq n - t$  implies that by the end of round  $r + 1$  or  $r + 2$  every correct process will notice  $|\{q \mid \text{early}_q = \text{true or } q \text{ halted}\}| \geq t + 1$ . By the end of round  $r + 1$  all correct processes that

did not halt in round  $r$ , but noticed that all previously invoked protocols stopped by the end of round  $r + 1$  will apply `monitor_halt` in that round. Those that will notice that all previously invoked protocols, except the one starting in round  $r + 1$ , have stopped, will apply `monitor_halt`. The same arguments as for the case of using rule  $H_3$ , the decision value is identical at all correct processes.

By the end of round  $r + 2$ , all other correct processes, that did not already apply `monitor_halt`, will either observe that all previously invoked protocols have stopped and will apply `monitor_halt`, or will observe that all previously invoked protocols except the one starting in round  $r + 1$  have stopped and will have the condition that  $|\{q \mid \text{early}_q = \text{true} \text{ or } q \text{ halted}\}| \geq t + 1$  and will apply `monitor_decision` by the end of round  $r + 2$  and will halt by the end of round  $r + 3$ , thus potentially ignoring the output of the last protocol. Again, using previous arguments, all decision values are the same.  $\square$

Lemma 3 and 4 complete the correctness part of Theorem 1. To simplify the polynomial considerations we look at a pipeline of monitors.

### 4.3 Monitors Pipeline

The basic monitor protocol runs a sequence of monitors and tests the number of faults' threshold every 4 rounds (Line 5). This allows the adversary to expose more faults in the following round, and be able to further expand the tree before the threshold is noticed the next time the processes execute Line 5. To circumvent this we will run a pipeline of 3 additional sequences of monitors on top of the basic one appearing above. Doing this we obtain that in every round  $r$  one of the 4 monitor sequences will be testing the threshold on the number of faults

Monitor sequence  $i$ , for  $1 \leq i \leq 4$  begins in round  $i$  and invokes protocols every 4 rounds, in every round  $r$ ,  $1 < r = i + 4k < t - 1$ , it invokes protocol  $\mathcal{D}_{t-i-4k}$ . Monitor sequence 1 is the basic monitor sequence defined in the previous subsection. Each monitor sequence independently runs the basic monitor protocol (Figure 1) every 4 rounds. In the monitor protocol, the test  $\bar{r} = j$ , which stands for  $\bar{r} \equiv r \pmod{4}$  in the basic monitor sequence, is replaced with  $\bar{r}_i = j$ , which stands for  $\bar{r}_i \equiv r + 1 - i \pmod{4} = j$  (naturally only for  $r + 1 - i > 0$ ). Each of the four monitor sequences decides and halts separately, as in the previous section above.

Notice that protocol  $\mathcal{D}_t$  is invoked only by the basic sequence (Sequence 1). For each of the three other monitor sequences, the decision rule is: decide BAD, if any invoked protocol (in this sequence) outputs BAD, and  $\perp$  otherwise. Observe that Lemma 3 and 4 hold for each individual sequence.

We now state the global decision and global halting rules:

**Definition 2** (Global Halting). *If any monitor sequence halts with BAD, or all 4 monitor sequences halt, the process halts.*

**Definition 3.** *The global\_decision is the output of  $\mathcal{D}_t$ , unless any monitor sequence returns BAD, in which case the decision is BAD.*

The following are immediate consequences of Lemma 3 and 4 and the above definitions.

**Corollary 2.** *If  $n > 3t$  and there are  $f$ ,  $f \leq t$ , corrupt processes then all correct processes halt by the end of round  $\min(t + 1, f + 2)$ .*

**Corollary 3.** *If the first correct process halts in round  $r$  on  $d$  then every correct process applies global\_decision by round  $\min\{r + 4, f + 2, t + 1\}$ , halts by round  $\min\{r + 5, f + 2, t + 1\}$ , and obtains the same decision value.*

## 5 Bounding the size of the tree

Following the approach in [GM98], we make the following definitions:

**Definition 4.** *A node  $\sigma z \in \Sigma$  is fully corrupt if there does not exist  $p \in G$  and  $\sigma' \sqsupseteq \sigma z$  such that  $\sigma' \in \mathcal{RT}_p[|\sigma z| + 2]$ .*

**Definition 5.** A process  $z$  is becomes fully corrupt at  $i$  if exists a node  $\sigma z \in \Sigma$  that is fully corrupt,  $|\sigma z| = i$  and for every previous node  $|\sigma' z| < i$ , node  $\sigma' z$  is not fully corrupt.

The following is immediate from the definitions above.

**Claim 4.** If process  $z$  becomes fully corrupt at  $i$  then of all the nodes of  $\Sigma$  that end with  $z$  only nodes of round  $i$  and  $i + 1$  can be fully corrupt.

*Proof.* By definition of fully corrupt, all correct processes will have  $z \in \mathcal{F}$  in round  $i + 2$ . So in that round and later all nodes will put  $\perp$  in  $\mathcal{RT}$  for  $z$ .  $\square$

Let  $\mathcal{CT}$ , the *corrupt tree*, be a dynamic tree structure.  $\mathcal{CT}$  is the tree of all fully corrupt nodes (note that due to coloring, the set of fully corrupt nodes is indeed a tree). We denote by  $\mathcal{CT}[i]$  the state of  $\mathcal{CT}$  at the end of round  $i$ . By the definition of fully corrupt, at round  $i$  we add nodes of length  $i - 2$  to  $\mathcal{CT}$ .

We label the nodes in  $\mathcal{CT}$  as follows: a node  $\sigma z \in \mathcal{CT}$  is a *regular* node if process  $z$  becomes fully corrupt at  $|\sigma z|$  and  $\sigma z \in \mathcal{CT}$  is a *special* node if process  $z$  becomes fully corrupt at  $|\sigma z| - 1$ .

Let  $\alpha_i$  denote the distinct number of processes that become fully corrupt at round  $i$ . For convenience, define  $\alpha_0 = 0$  (this technicality is useful in Lemma 7). Let  $A = \alpha_0, \alpha_1, \dots$  be the sequence of counts of process that become fully corrupt in a given execution.

Following the approach of [GM98], we define  $waste_i = (\sum_{j \leq i} \alpha_j) - i$ . So  $waste_i$  is the number of processes that became fully corrupt till round  $i$  minus  $i$  (the round number). The following claim connects  $waste_i$  to  $\cap_{p \in G} \mathcal{FA}[i+3]_p$  the set of fully detected corrupt processes at round  $i + 3$ .

**Claim 5.** For any round  $4 \leq r \leq t + 1$ , and any correct process we have  $|\mathcal{FA}[r]| \geq \sum_{j \leq r-3} \alpha_j$ .

*Proof.* By the definition of  $z$  becoming fully corrupt at  $i$ , all correct processes will have  $z \in \mathcal{F}$  in round  $i + 2$ . Due to the gossiping of  $\mathcal{F}$ , all correct processes will have  $z \in \mathcal{FA}$  in round  $i + 3$ .  $\square$

So if  $waste_i \geq 6$  then in round  $r = i + 3$  we will have  $(\sum_{j \leq i} \alpha_j) - i \geq 6$  so by Lemma 5 for each correct process we have  $|\mathcal{FA}[r]| \geq r + 3$ . In this case all correct processes will start in the associated monitor sequence the next protocol with initial value BAD and the protocol and monitor sequence and global protocol will reach agreement and halt on BAD by round  $i + 6$  (by Lemma 1).

We will now show that if the adversary maintains a small waste (less than 6 by the argument above, but this will work for any constant) then the  $\mathcal{CT}$  tree must remain polynomial sized.

The following key lemma shows that the adversary cannot increase the number of leaves by “cross contamination”. In more detail, if the adversary causes two fully corrupt processes at round  $i_1$  followed by a sequence of rounds with exactly one fully corrupt process at each round followed by a round with no fully corrupt process at that round then this action essentially keeps the tree  $\mathcal{CT}$  growing at a slow (polynomial) rate. We note that the focus on “cross contamination” follows the approach of [GM98]. But they only verify the case of two fully corrupt followed by a round with no fully corrupt. We have identified a larger family of adversary behavior that does not increase the waste (in the long run). Our proof covers this larger set of behaviors and this requires additional work.

**Lemma 5.** Assume  $0 < i_1 < i_2$  such that  $\alpha_{i_1} = 2$ ,  $\alpha_{i_2} = 0$  and for all  $i_1 < i < i_2$ ,  $\alpha_i = 1$  then for any  $\sigma \in \Sigma_{i_1-1} \cap \mathcal{CT}$  it is not the case that there exists  $\sigma p \tau \in \Sigma_{i_2+1} \cap \mathcal{CT}$  and there exists  $\sigma q \tau \in \Sigma_{i_2+1} \cap \mathcal{CT}$  (so there is at most one extension). Moreover the size of the subtree starting from  $\sigma p$  or  $\sigma q$  and ending in length  $i_2 + 1$  is bounded by  $O((i_2 - i_1)^2)$ .

See the additional analysis in Section 5.1.

To bound the size of  $\mathcal{CT}$ , we partition the sequence  $A = \alpha_0, \alpha_1, \dots$  by iteratively marking subsequences using the following procedure. For each subsequence we mark, we prove that it either causes the tree to grow in a controllable manner (so the ending tree is polynomial), or it causes the tree to grow considerably (by a factor of  $O(n)$ ) but at the price of increasing the waste by some positive constant. Since the waste is bounded by a constant, the result follows.

1. By [Lemma 7](#) we know that if  $A$  contains a  $0(1)^*0$  (a sequence starting with 0 then some 1's then 0) then it contains it just once as a suffix of  $A$ . Moreover, this suffix does not increase the size of the tree by more than  $O(n)$ . Let  $A_1$  be the resulting unmarked sequence after marking such a suffix (if it exists).
2. Mark all subsequences in  $A_1$  of the form  $2(1)^*0$  (a sequence starting with 2 then some 1's then 0). By [Lemma 5](#) each such occurrence will not increase the number of leafs in  $\mathcal{CT}$  (but may add branches that will close whose total size is at most  $n^2$  over all such sequences). Let  $A_2$  be the remaining unmarked subsequences.
3. Mark all subsequences in  $A_2$  of the form  $X(1)^*0$  where  $X \in \{3, \dots, t\}$  (a sequence starting with 3 or a larger number followed by some 1's then 0). By [Lemma 8](#) each occurrence of such a sequence may increase the size of the tree multiplicatively by  $O(n)$  leafs and  $O(n^2)$  non-leaf nodes, but this also increases the *waste* by  $c - 1 > 1$  (where  $c$  is the first element of the subsequence). Observe that the remaining unmarked subsequences do not contain any element that equals 0. Let  $A_3$  be the remaining unmarked subsequences.
4. Mark all subsequences of the form  $Y(1)^*$  where  $Y \in \{2, \dots, t\}$  (a sequence whose first element is 2 or a larger number followed by some 1's but no zero at the end). Again, by [Lemma 8](#) each such occurrence may increase the size of the tree by  $O(n)$  leafs and  $O(n^2)$  non-leafs, but this also increases the *waste* by  $c > 1$ . Let  $A_4$  be the remaining unmarked.
5. Since  $A_3$  contains no element that equals zero and we removed all subsequences that have element of value 2 or larger as the first element then  $A_4$  must either be empty or  $A_4$  is a prefix of  $A$  of the form  $(1)^*$  (a series of 1's). Since it is a prefix of  $A$  then a sequence of 1's keeps at most one leaf. So the tree remains small.

Thus, the size of  $\mathcal{CT}$  is polynomial, which by [Lemma 6](#) bounds the size of  $\mathcal{IT}$ . This completes the proof of [Theorem 1](#).

## 5.1 Additional Analysis

The following lemma bounds the size of  $\mathcal{IT}$  as a function of the size of  $\mathcal{CT}$  times  $O(n^7)$ .

**Lemma 6.** *If  $\sigma \in \mathcal{IT}$  and  $|\sigma| > 7$  then there exists  $\sigma' \sqsubset \sigma$  with  $|\sigma'| \geq |\sigma| - 7$  such that  $\sigma' \in \mathcal{CT}$ .*

*Proof.* Seeking a contradiction let  $\sigma = \sigma'\tau$  be of minimal length such that  $\sigma \in \mathcal{IT}$ ,  $|\sigma| > 7$ ,  $|\tau| = 7$  and there does not exist  $\sigma'\tau' \in \mathcal{CT}$  such that  $\tau' \sqsubseteq \tau$ .

Let  $w$  be the first element in  $\tau$  so  $\sigma'w \sqsubseteq \sigma'\tau$  then since  $\sigma'w \notin \mathcal{CT}$  then by definition, some correct process will have  $\sigma'w \in \mathcal{RT}[|\sigma'w|+2]$ . By [Theorem 2](#) statement 4 all correct processes will have  $\sigma'w \in \mathcal{RT}[|\sigma'|+5]$  and will close the branch  $\sigma'w$  by round  $|\sigma'| + 6$  (see DECAY RULE) a contradiction to the assumption that  $\sigma \in \mathcal{IT}$  and  $|\tau| = 7$ .  $\square$

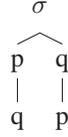
The following lemma shows that the protocol stops early if the adversary causes two rounds with no new fully corrupt and only one fully corrupt per round between them.

**Lemma 7.** *If exists  $0 \leq i_1 < i_2$  such that  $\alpha_{i_1} = 0$ ,  $\alpha_{i_2} = 0$  and for all  $i_1 < i < i_2$ ,  $\alpha_i = 1$  then all processes will halt by the end of round  $i_2 + 5$ .*

*Proof.* The only fully corrupt process that can appear in round  $i_1 + 1$  is the new one from  $\alpha_{i_1+1} = 1$  (because  $\alpha_{i_1} = 0$  and a process can be as a node in  $\mathcal{CT}$  for only two rounds starting from the first round it is fully corrupt). A simple induction shows that at round  $i_1 + j$  only the new fully corrupt node of round  $i_1 + j$  can appear. Once we reach round  $i_2$  then no node can be fully corrupt so all branches will close and all processes will halt by the end of round  $i_2 + 5$ .  $\square$

We now prove the main technical result of this section [Lemma 5](#). It shows that having two fully corrupt then a series of one fully corrupt then a round with no fully corrupt does not increase the number of leafs in the tree. This can add some non-leaf nodes to the tree, but the overall addition of such nodes is bounded by a multiplicative factor of  $O(n^2)$  over all such sequences.

*Proof of Lemma 5.* Let processes  $p, q$  be the two that become fully corrupt at  $i_1$ . We begin with the case that  $i_2 = i_1 + 1$  such that there is no process that becomes fully corrupt at  $i_2$ . Consider any  $\sigma \in \mathcal{CT}$  where  $|\sigma| = i_1 - 1$ . The following is the subtree of  $\sigma \in \mathcal{CT}$  that we will analyze:



The following analysis for process  $p$  shows that either  $\sigma p$  or  $\sigma q$  or  $\sigma qp$  will quickly be in  $\mathcal{RT}$ . Note that this implies that  $p, q$  can extend any node  $\sigma \in \mathcal{CT}$  into at most one node of length  $i_2$  in  $\mathcal{CT}$ .

Let *correctDetector* be the set of correct processes that detect  $\sigma p$  via the **Not Voter** detection rule in round  $|\sigma p| + 1$ . Let *correctVoter* be the remaining correct processes (that are not in *correctDetector*). Note that by definition of **Not Voter**, the value of all those in *correctVoter* must be the same. Let  $d$  be this value.

For each  $\sigma pu \in \Sigma$  with  $u \neq q$  we have that  $\sigma pu \notin \mathcal{CT}$  (because  $\alpha_{i_1} = 0$ ). So  $\sigma pu \in \mathcal{RT}[|\sigma pu| + 2]$  for some correct processes and hence their value is fixed (otherwise  $\sigma p \in \mathcal{RT}$  and we are done) and all correct processes will have  $\sigma pu \in \mathcal{RT}[|\sigma p| + 5]$ . Let *faultyEcho* be the set of corrupt children of  $\sigma p$  whose value is fixed to  $d$ . Let *faultyEchoOther* be the remaining corrupt process that are children of  $\sigma p$  whose value is fixed to  $\neq d$ . Note that  $\sigma p$  has  $n - |\sigma p|$  children of which all but child  $\sigma pq$  must be fixed. Hence  $|faultyEcho| + |faultyEchoOther| \geq n - |\sigma p| - 1$ .

There are three cases to consider:

**Case 1:** If  $|correctVoter| + |faultyEcho| \geq n - t - 1$  then  $\sigma p \in \mathcal{RT}[|\sigma p| + 5]$  for all correct processes since all these  $n - t - 1$  children of  $\sigma p$  will appear in  $\mathcal{RT}[|\sigma p| + 5]$  and so  $\sigma p \in \mathcal{RT}[|\sigma p| + 5]$  using the RELAXED RULE.

Otherwise,  $|correctVoter| + |faultyEcho| \leq n - t - 2$  so it must be that  $|correctDetector| + |faultyEchoOther| \geq t + 1 - |\sigma p| = t + 2 - |\sigma pq|$ . This is because  $\sigma p$  has  $n - |\sigma p|$  children and each one of them except of child  $q$  must fix their value in  $\mathcal{RT}[|\sigma p| + 3]$ .

**Case 2:** If  $|correctDetector| \geq t + 2 - |\sigma pq|$  then SPECIAL-BOT RULE will fire on the level  $i_1 + 1$  node  $\sigma qp$ . This will occur because all other children of  $\sigma q$  are not fully corrupt - hence will appear in  $\mathcal{RT}[|\sigma q| + 5]$ . The only case in which SPECIAL-BOT RULE may not fire is if in the meantime  $\sigma q \in \mathcal{RT}$  in which case we are done.

**Case 3:** It must be that  $correctDetector \leq t$ , hence  $correctVoter \geq t + 1$  on value  $d$  (because  $\sigma$  contains no correct process). Since  $correctVoter \geq t + 1$  then all correct processes will see that  $\sigma p$  is *leaning towards*  $d$  (see definitions 3. and 4. in the fault detection rules).

For any  $w \in faultyEchoOther$ , since  $w$  does not become fully corrupt at  $i_1$  or  $i_1 + 1$  it must be that are at least  $t + 1$  correct processes that are children of  $\sigma pw$  that hear from  $\sigma pw$  a value  $d'$ ,  $d' \neq d$ . So the conditions of **Not Masking** for  $\sigma pw$  hold.

This implies that  $w$  is 'forced' to send  $\perp$  for  $\sigma qp w$  to all correct processes. For if  $w$  sends  $d' \neq \perp$  to any correct processes for  $\sigma qp w$  then by **Not Masking** rule at round  $|\sigma pw| + 2 = |\sigma qp w| + 1$  these correct processes will detect  $w$  as corrupt and in the same round mask  $\sigma qp w$  to  $\perp$ .

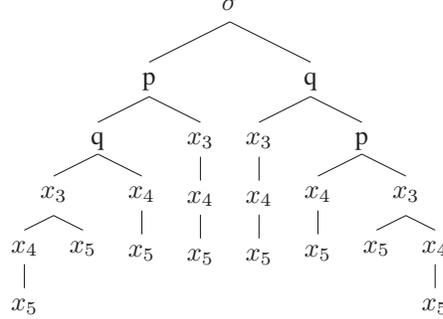
Therefore there will be  $|correctDetector| + |faultyEchoOther| \geq t + 2 - |\sigma qp|$  children of  $\sigma qp$  that will appear in  $\mathcal{IT}$  with value  $\perp$  and since there is no process that becomes fully corrupt at  $i_1 + 1 = i_2$  then all other children of  $\sigma q$  must appear in  $\mathcal{RT}[|\sigma q| + 5]$ . So the SPECIAL-BOT RULE will fire on the level  $i_1 + 1$  node  $\sigma qp$ . This completes the proof for the case  $i_1 - i_2 = 1$ .

We can now consider the case where  $i_1 - i_2 > 1$ . The key observation is that the above argument required two properties for a process  $z$  that becomes fully corrupt at round  $i$ . The first is that all the level  $i$  nodes of the form  $\sigma z$  have all their children (except one) fixed to some value. The second is that the level  $i + 1$  nodes of the form  $\sigma' z$  have the property that all other children of  $\sigma'$  are fixed.

Intuitively, if a child  $\sigma zu$  is fixed to the majority value of  $\sigma z$  then  $\sigma zu$  will help fix  $\sigma z$  using the relaxed rule. Otherwise,  $\sigma zu$  is fixed to some  $d'$ , which implies that at least  $t + 1$  correct processes received  $d'$  from  $\sigma zu$ . Hence  $\sigma zu$  must be a masker for the round  $i + 1$  node  $\sigma' z$ .

Next we observe the structure of  $\mathcal{CT}$  given a sequence with  $i_1 - i_2 > 1$ . Let  $p, q$  be the two processes in  $i_1$ , let  $\ell = i_2 - i_1 + 1$  and denote by  $x_3, \dots, x_\ell$  the remaining fully corrupt by order of appearance. Using an inductive argument one can show that any  $\mathcal{CT}$  graph will be a subgraph of the following: for every node  $\sigma \in \mathcal{CT}$  of length  $i_1 - 1$  there will be two branches that we call *special branches*. These branches will be  $\sigma pq x_3 \dots x_\ell$  and  $\sigma qp x_3 \dots x_\ell$ . Observe that these branches contain only special nodes. In addition, there will be regular branches as follows:  $\sigma p x_3 \dots x_\ell$ ,

$\sigma qx_3 \dots x_\ell, \sigma pqx_4 \dots x_\ell, \sigma qpx_4 \dots x_\ell, \dots, \sigma pqx_3 \dots x_i x_{i+2} \dots x_\ell, \sigma qpx_3 \dots x_i x_{i+1} \dots x_\ell, \dots, \sigma pqx_3 \dots x_{\ell-2} x_\ell, \sigma qpx_3 \dots x_{\ell-2}, x_\ell$ . Observe that all these regular branches contain regular nodes and that all their children will be fixed due to round  $i_2$  having no fully corrupt process. The number of regular branches is  $O(i_2 - i_1)$  and the length of each branch is bounded by  $O(i_2 - i_1)$ .



The above tree is an example for  $i_2 - i_1 = 4$ . The two special branches are the rightmost and leftmost paths. All other leafs are the endpoints of all the regular branches. Observe that given one more fully corrupt, each special branch is split into two branches, one extends the original special branch and the other is a new regular branch that continues as a path. Also observe that one more fully corrupt will simply extend the path of each regular branch by one.

As all the regular branches will have all their children fixed, they cannot be used as leafs to extend the tree. Since there are  $O(i_2 - i_1)$  regular branches and each of them is of length at most  $O(i_2 - i_1)$  then the total amount of nodes added in this process is  $O((i_2 - i_1)^2)$  per each leaf in  $\mathcal{CT}$  of length  $i_1 - 2$ . So if the size of the tree without this subtree is  $x$  then the total number of non-tree nodes added by these types of sequences is at most  $O(xn^2)$  (this is a crude bound that can be improved).

We now need to show that at least one of the special branches gets fixed. Since all the regular branches cannot expand, our goal is to prove that it cannot be the case that both special branches are not fixed (in the  $i_1 - i_2 = 1$  the analogue is that either  $\sigma pq$  or  $\sigma qp$  is fixed). Given the key observation and the structure statement we can now apply a similar argument as we did for  $p$  in the  $i_1 - i_2 = 1$  case. We start with  $x_\ell$  and going towards  $p, q$ . We will show that in each iteration on level  $i$  we either fix one of the special branches (and we are done) or we have sufficient conditions to use main argument on level  $i - 1$ .

For the base case, consider  $x_\ell$ . Because  $i_2 = 0$  then all the level  $i_1 + \ell - 2$  nodes of the form  $\sigma' x_\ell$  (for any  $\sigma'$ ) have all their children fixed. So we can apply the main argument: if all these level  $i_1 + \ell - 2$  nodes get fixed using the RELAXED RULE then all the regular branches ending with  $x_{\ell-1}$  have all their children fixed and the two special branches ending  $x_{\ell-1}$  each have their parent with  $x_{\ell-1}$  as a only child. Therefore we continue by induction. Otherwise, by the argument above, all the level  $i_1 + \ell - 2 + 1$  nodes of the form  $\sigma' x_\ell$  (for any  $\sigma'$ ) will be fixed SPECIAL-BOT RULE. In particular this includes the special branch. So we are done.

For the general case, we assume that all level  $i_1 + j - 2$  nodes of the form  $\sigma' x_j$  (for any  $\sigma'$ ) have all their children fixed and that for the two special branches, the parents of  $x_j$  have  $x_j$  as their only child. Again we can apply the  $i_i - i_2 = 1$  arguments: If all these level  $i_1 + j - 2$  node get fixed using the RELAXED RULE then we continue by induction to  $j - 1$ . Otherwise, by the argument above, all the level  $i_1 + j - 2 + 1$  nodes of the form  $\sigma' x_\ell$  (for any  $\sigma'$ ) will be fixed by the SPECIAL-BOT RULE. In particular this includes the special branch. So we are done since the special branch is fixed  $\square$

The following lemma shows that having a large number (3 or more) of processes becoming fully corrupt at a given round, followed by a sequence of 1's and then maybe followed by 0 does increase the number of leafs considerably. Note that if  $\alpha_{i_1-1} + \alpha_{i_1} \geq 6$  then the monitor process will cause the protocol to reach agreement and stop in a constant number of rounds. So we only look at the case that  $\alpha_{i_1-1} + \alpha_{i_1} < 6$ .

**Lemma 8.** *If  $2 < \alpha_{i_1}, \alpha_{i_1-1} + \alpha_{i_1} < 6, \alpha_{i_2} \in \{0, 1\}$  and for all  $i_1 < i < i_2, \alpha_i = 1$  then for any  $\sigma \in \Sigma_{i_1-1} \cap \mathcal{CT}$  there are at most  $O(i_2 - i_1)$  nodes of the form  $\sigma\tau \in \Sigma_{i_2+1} \cap \mathcal{CT}$ . Moreover the size of the subtree starting from  $\sigma$  and ending in length  $i_2 + 1$  is bounded by  $O((i_2 - i_1)^2)$ .*

*Proof.* Using an overly pessimistic argument, every node  $\sigma \in \Sigma_{i_1-1} \cap \mathcal{CT}$  can have at most  $\alpha_{i_1-1} \cdot \alpha_{i_1} \leq 16 = O(1)$  nodes of length  $i_1 + 2$  in  $\mathcal{CT}$ . Even if each such node is a special node then after  $O(i_2 - i_1)$  rounds of just one fully corrupt each round, each such node of length  $i_1 + 2$  will generate at most  $O(i_2 - i_1)$  regular branches, each is a path with at most  $O(i_2 - i_1)$  nodes. □

## 6 Conclusion

In this paper we resolve the problem of the existence of a protocol with polynomial complexity and optimal early stopping and resilience. The main remaining open question is reducing the complexity of such protocols to a low degree polynomial. Another interesting open problem is obtaining unbeatable protocols [CGM14] (which is a stronger notion than early stopping).

We would like to thank Yoram Moses and Juan Garay for insightful discussions and comments.

## References

- [BG93] Piotr Berman and Juan A. Garay. Cloture votes:  $n/4$ -resilient distributed consensus in  $t+1$  rounds. *Mathematical Systems Theory*, 26(1):3–19, 1993.
- [BGP92] Piotr Berman, Juan A. Garay, and Kenneth J. Perry. Optimal early stopping in distributed consensus. In Adrian Segall and Shmuel Zaks, editors, *Distributed Algorithms*, volume 647 of *Lecture Notes in Computer Science*, pages 221–237. Springer Berlin Heidelberg, 1992.
- [BNDDS92] Amotz Bar-Noy, Danny Dolev, Cynthia Dwork, and H. Raymond Strong. Shifting gears: changing algorithms on the fly to expedite byzantine agreement. *Inf. Comput.*, 97:205–233, April 1992.
- [CGM14] Armando Castañeda, Yannai A. Gonczarowski, and Yoram Moses. Unbeatable consensus. In Fabian Kuhn, editor, *Distributed Computing - 28th International Symposium, DISC 2014, Austin, TX, USA, October 12-15, 2014. Proceedings*, volume 8784 of *Lecture Notes in Computer Science*, pages 91–106. Springer, 2014.
- [CL99] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *Proceedings of the third symposium on Operating systems design and implementation, OSDI '99*, pages 173–186, Berkeley, CA, USA, 1999. USENIX Association.
- [DRS90] Danny Dolev, Ruediger Reischuk, and H. Raymond Strong. Early stopping in byzantine agreement. *J. ACM*, 37:720–741, October 1990.
- [DS82] Danny Dolev and H. Raymond Strong. Polynomial algorithms for multiple processor agreement. In *ACM Symposium on Theory of Computing*, pages 401–407, New York, NY, USA, 1982. ACM.
- [FL82] Michael J. Fischer and Nancy A. Lynch. A lower bound for the time to assure interactive consistency. *Inf. Process. Lett.*, 14(4):183–186, 1982.
- [FM88] Paul Feldman and Silvio Micali. Optimal algorithms for byzantine agreement. In *ACM Symposium on Theory of Computing*, pages 148–161, 1988.
- [FM97] Peaseh Feldman and Silvio Micali. An optimal probabilistic protocol for synchronous byzantine agreement. *SIAM J. Comput.*, 26(4):873–933, 1997.
- [GM93] Juan A. Garay and Yoram Moses. Fully polynomial byzantine agreement in  $t + 1$  rounds. In *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing, STOC '93*, pages 31–41, New York, NY, USA, 1993. ACM.

- [GM98] Juan A. Garay and Yoram Moses. Fully polynomial byzantine agreement for processors in rounds. *SIAM J. Comput.*, 27:247–290, February 1998.
- [KAD<sup>+</sup>07] Ramakrishna Kotla, Lorenzo Alvisi, Mike Dahlin, Allen Clement, and Edmund Wong. Zyzzyva: speculative byzantine fault tolerance. In *Proceedings of twenty-first ACM SIGOPS symposium on Operating systems principles*, SOSP '07, pages 45–58, New York, NY, USA, 2007. ACM.
- [KM13] Dariusz R. Kowalski and Achour Mostéfaoui. Synchronous byzantine agreement with nearly a cubic number of communication bits: Synchronous byzantine agreement with nearly a cubic number of communication bits. In *Proceedings of the 2013 ACM Symposium on Principles of Distributed Computing*, PODC '13, pages 84–91, New York, NY, USA, 2013. ACM.
- [LSP82] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4:382–401, July 1982.
- [PSL80] Marshall Pease, Robert Shostak, and Leslie Lamport. Reaching agreement in the presence of faults. *J. ACM*, 27(2):228–234, 1980.