On Byzantine Agreement over (2, 3)-Uniform Hypergraphs

D.V.S. Ravikant, V. Muthuramakrishnan, V. Srikanth, K. Srinathan*, and C. Pandu Rangan

Department of Computer Science and Engineering,
Indian Institute of Technology, Madras, Chennai 600036, India
{muthu,ravidvs,srikanth,ksrinath}@meenakshi.cs.iitm.ernet.in,
rangan@iitm.ernet.in

Abstract. In a *Byzantine agreement* protocol, a synchronous network of n interconnected processes of which t may be faulty, starts with an initial binary value associated with each process; after exchanging messages, all correct processes must agree on one of the initial values of the non-faulty processes.

If the network consists of only unicast channels (i.e. a 2-uniform hypergraph), then Byzantine agreement is possible if and only if $n \geq 3t + 1$ (Pease *et. al.* [11]). However, Fitzi and Maurer ([7]) show that if, in addition to all unicast channels, there exists local broadcast among every three processes in the network (i.e. a complete $(2, 3)$-uniform hypergraph), $n \geq 2t + 1$ is necessary and sufficient for Byzantine agreement.

In this paper, we show that optimum tolerance of $n \geq 2t + 1$ can be achieved even if a substantial fraction of the local broadcast channels are *not* available. Specifically, we model the network as a $(2, 3)$-uniform hypergraph $H = (P, E)$, where P denotes the set of n processes and E is a set of 2-tuples and/or 3-tuples of processes (edges or 3-hyperedges), wherein each 3-hyperedge represents a local broadcast among the three processes; we obtain a characterization of the hypergraphs on which Byzantine agreement is possible. Using this characterization, we show that for $n = 2t + 1$, $\left(\frac{2}{3}t^3 + \Theta(t^2)\right)$ 3-hyperedges are necessary and sufficient to enable Byzantine agreement. This settles an open problem raised by Fitzi and Maurer in [7]. An efficient protocol is also given whenever Byzantine agreement is possible.

1 Introduction

The problem of Byzantine agreement is a classic problem in distributed computing introduced by Lamport et al. in [12]. In many practical situations, it is necessary for a group of processes in a distributed system to agree on some issue, despite the presence of some faulty processes. More precisely, a protocol among a group of n processes (t of which may be faulty), each having a value, is said to achieve Byzantine agreement, if, at the end of the protocol, all honest processes

* Financial support from Infosys Technologies Limited, India, is acknowledged.

R. Guerraoui (Ed.): DISC 2004, LNCS 3274, pp. 450–464, 2004.

agree on a value and the following conditions hold: (1) *Agreement:* All honest processes agree on the same value; (2) *Validity:* If all honest processes start with the value $v \in \{0, 1\}$, then all honest processes agree on v; (3) *Termination:* All honest processes eventually agree.

In this paper, we shall use the simple and standard model of a synchronous network wherein any communication protocol evolves as a series of *rounds*, during which the players send messages, receive them and perform (polynomial time) local computations according to the protocol.

The processes' mutual distrust in the network is typically modeled via a (fictitious) centralized adversary that is assumed to control/corrupt the faulty processes. In the threshold adversary model, a fixed upper bound t is set for the number of faulty processes.

Over a complete graph (of point-to-point authenticated channels), it was proved [11] that, Byzantine agreement is achievable on a set of n processes with t (Byzantine) faults if and only if $t < \frac{n}{3}$. Subsequently, there have been (successful) attempts on "improving" the above bound.

One approach has been to study the problem in a non-threshold adversary model like in [8, 6, 1]. In this model the adversary is characterized by an *adversary structure* which is a monotone set of subsets of processes from which processes in any one of the subsets may be corrupted; it was proved [6] that Byzantine agreement is possible if and only if the adversary structure $\mathcal{A}_{adv}$ satisfies $\mathcal{Q}^{(3)}$, i.e., no three sets in $\mathcal{A}_{adv}$ cover the full set of processes.

A second approach is to assume (stronger) communication primitives in addition to the point-to-point authenticated links. For example in [7], a broadcast among three processes was assumed to be available among every set of three processes and the bound was improved to $t < \frac{n}{2}$.

In another line of research, Dolev *et. al.* in [5] study the possibility of Byzantine agreement over incomplete graphs. If $n > 3t$, they prove that Byzantine agreement is achievable if and only if the underlying graph is at least $(2t + 1)$-connected. Generalizing this result using the first approach, Kumar *et. al.* [9] show that if the adversary structure $\mathcal{A}$ satisfies $\mathcal{Q}^{(3)}$, Byzantine agreement is achievable if and only if the underlying graph is $\mathcal{A}^{(2)}$-connected, that is, the union of no two sets in the adversary structure is a vertex cut-set of the graph.

With this as the state-of-the-art, the following question (mentioned as an open problem in [7]) arises: *what is a necessary and sufficient condition for achieving Byzantine agreement over incomplete* $(2, 3)$*-uniform hypergraphs?* In this paper, we provide a concise characterization that generalizes the results of [5] (which uses the 1-cast model) to the $(2, 3)$-uniform hypergraph model.

2 Motivation and Contributions

In practice one finds local broadcast channels in various networks in the form of LAN (Local Area Network) like an Ethernet or Token ring system. Another example is wireless communication, which is inherently broadcast in nature. A particular case when there is a local broadcast among every three players, that

is, a complete $(2,3)$-uniform hypergraph, has been studied in [7]. We investigate the strength of arbitrary $(2,3)$-uniform hypergraphs in the context of achieving Byzantine agreement. Recall that even over *complete* $(2,3)$-uniform hypergraphs on n processes of which up to t may be Byzantine faulty, Byzantine agreement is achievable if and only if $n > 2t$ [7]. We characterize the (im)possibility of Byzantine agreement on an arbitrary network.

Definition 1. *A hypergraph H is said to be (α, β)-hyper-γ-connected if on removal of any $(\gamma - 1)$ vertices, for any partition of the remaining vertices into α sets of maximum size β, there exists a hyperedge which has non-empty intersection with every set of the partition.*

In Section 4 we prove that Byzantine agreement among $n > 2t$ processes connected via a $(2,3)$-uniform hypergraph H is possible if and only if H satisfies the following three conditions: (i) if $n = 2t+1$, then H is 2-hyperedge complete; (ii) if $n > 2t+1$, then H is $(2,n)$-hyper-$(2t+1)$-connected, and (iii) if $2t < n \leq 3t$, then H is $(3,t)$-hyper-$(3t-n+1)$-connected.

Implicit in the characterization are the principles for fault-tolerant network design using $(2,3)$-hyperedges. Nevertheless, we provide explicit constructions of minimally connected optimally tolerant 3-uniform hypergraphs (in Section 5).

The impact of our results can be seen from the following implications:

Implication 1 *For any $n > 3t$, addition of (any number of) 3-hyperedges does not reduce the $(2t+1)$-connectivity requirement.*

Remark: Note that any hypergraph H is $(2,n)$-hyper-$(2t+1)$-connected if and only if its underlying graph is $(2t+1)$-connected. By underlying graph, we mean the graph obtained by replacing each 3-hyperedge by its corresponding three edges.

Implication 2 *The optimum of $n = (2t+1)$ can be achieved even if a considerable fraction of the 3-hyperedges are absent. Furthermore, the minimum number of 3-hyperedges necessary to facilitate agreement reduces as (n/t) increases.*

Remark: We will present in Section 5, the design of networks that allow Byzantine agreement with at most $\frac{1}{2}(3t-k-1)(t+k+1)(k+1)$ 3-hyperedges, where $n = 3t-k$, for $0 \leq k < t$.

Implication 3 *There are several scenarios (networks) for which no known protocol can achieve Byzantine agreement while our protocol succeeds.*

Remark: For example, consider the network $H(P,E)$ on five nodes two of which may be faulty and contains eight 3-hyperedges, $P = \{p_1, p_2, p_3, p_4, p_5\}$ and $E_{basis} = \{\{p_1,p_2,p_3\}, \{p_1,p_2,p_4\}, \{p_2,p_3,p_4\}, \{p_3,p_4,p_5\}, \{p_4,p_5,p_1\}, \{p_1,p_2,p_5\}, \{p_2,p_3,p_5\}, \{p_1,p_3,p_5\}\}$. Note that H satisfies the conditions[1] of Theorem 1; hence our protocol of Section 4 achieves agreement while all the extant protocols fail.

[1] For any hypergraph on five nodes tolerating two faults, it can in fact be shown that it is impossible to satisfy the conditions of Theorem 1 using any set of seven (or less) 3-hyperedges. Thus, our example is tight.

3 Definitions and the Model

Definition 2. *A hypergraph H is defined as the ordered pair (P, E) where P is a set of vertices and $E \subseteq 2^P$ is a monotone[2] set of hyperedges. A set $e \in E$ is called a $|e|$-hyperedge. The maximal basis of E is $\{e \in E|$ no proper superset of e is in $E\}$.*

We model the network as a hypergraph $H(P, E)$ where $P = \{p_1, p_2, \ldots, p_n\}$ is the set of processes and $\{p_1, p_2, ..., p_k\} \in E$ if and only if $p_1, p_2, ..., p_k$ are connected by a local broadcast.

Definition 3. *A 3-uniform hypergraph is a hypergraph $H(P, E)$ in which all hyperedges in the maximal basis of E are 3-hyperedges. A $(2, 3)$-uniform hypergraph is a hypergraph $H(P, E)$ in which every hyperedge in the maximal basis of E is either a 2-hyperedge or a 3-hyperedge.*

In this paper, we work with networks that are modeled by a $(2, 3)$-uniform hypergraph.

Definition 4. *If $P_1, P_2, \ldots, P_m$ are mutually disjoint non empty sets of size $\leq t$ such that $P_1 \cup P_2 \cup \ldots \cup P_m = P$, then we say $(P_1, P_2, \ldots, P_m)$ forms a (m, t)-partition of P. Formally, $(P_1, P_2, \ldots, P_m)$ forms a (m, t)-partition of P if $1 \leq |P_i| \leq t$ for all i, $1 \leq i \leq m$, $(P_i \cap P_j) = \emptyset$ for all i, j, $1 \leq i < j \leq m$ and $P_1 \cup P_2 \cup \ldots \cup P_m = P$. A hypergraph $H(P, E)$ is said to be (m, t)-hyperconnected if for every (m, t)-partition $(P_1, P_2, \ldots P_m)$ of P, $\exists e \in E$ such that $(e \cap P_i) \neq \emptyset$ for $1 \leq i \leq m$. A hypergraph H is (m, t)-hyper-k-connected if on removal of any $(k-1)$ vertices, the hypergraph remains (m, t)-hyperconnected.*

Remark: A k-(vertex)connected graph on n nodes is a $(2, n)$-hyper-k-connected hypergraph.

A hypergraph is said to be 2-hyperedge complete if it contains all 2-hyperedges (2-hyperedges among every 2 vertices).

Definition 5. *An adversary structure, $\mathcal{A}_{adv}$, is a monotone[3] set of subsets of the process set P. We abuse the notation $\mathcal{A}_{adv}$ to also denote the maximal basis. Any adversary characterized by $\mathcal{A}_{adv}$ can corrupt the processes in any one set of his choice from $\mathcal{A}_{adv}$. The adversary structure $\mathcal{A}_{adv}$ is said to satisfy $\mathcal{Q}^{(k)}$ if the union of no k sets in $\mathcal{A}_{adv}$ equals P.*

4 Characterization of Byzantine Agreement

Theorem 1. *Let $H(P, E), |P| = n$ be a $(2, 3)$-uniform hypergraph. There exists a deterministic protocol for Byzantine agreement on H tolerating t faults if and only if all the following hold:*

1. *If $n = 2t + 1$, then H should have all 2-hyperedges.*
2. *If $n > 2t + 1$, then H is $(2, n)$-hyper-$(2t + 1)$-connected.*[4]
3. *If $2t < n \leq 3t$, then H is $(3, t)$-hyper-$(3t - n + 1)$-connected.*

[2] If $S \in E$ and $S' \subseteq S$ then $S' \in E$.

[3] If $S \in \mathcal{A}_{adv}$ then $S' \in \mathcal{A}_{adv}$ for every $S' \subset S$

[4] This condition implies that we still need $(2t + 1)$-edge connectivity with respect to 2-hyperedges.

Proof (Necessity of conditions 1 and 2): The proof is similar to the proof for $(2t+1)$-connectivity on normal graphs in [10]. The main idea of the proof is illustrated in the Lemma 1.

The key idea behind Lemma 1 is to design a distributed system with contradicting behavior assuming the existence of a protocol satisfying the conditions stated in the lemma. Note that the newly constructed system need not solve the Byzantine agreement problem. The processors in the new system behave exactly as specified in the (assumed) protocol.

Lemma 1. *Byzantine agreement is not achievable on a four node hypergraph H tolerating one fault if the hypergraph is not $(2,4)$-hyper-3-connected.*

Proof: Suppose, for the sake of contradiction, that there is a protocol A that achieves agreement among the four players p_1, p_2, p_3 and p_4 connected by a hypergraph H which is not $(2,4)$-hyper-3-connected.

Assume without loss of generality that $\{p_2, p_4\}$ disconnects H. The maximal hypergraph H_1 that is not $(2,4)$-hyper-3-connected which has $\{p_2, p_4\}$ as a cut-set is as shown in Figure 1. The only two 3-hyperedges possible in H_1 are $\{p_1, p_2, p_4\}$ and $\{p_2, p_3, p_4\}$. Since H is a subgraph of H_1, the protocol also works on H_1. Without loss of generality assume that all communication is through the two 3-hyperedges $\{p_1, p_2, p_4\}$ and $\{p_2, p_3, p_4\}$[5].

Let $\pi_1, \pi_2, \pi_3, \pi_4$ denote the local programs of p_1, p_2, p_3, p_4 respectively.[6] For each $i \in \{0, \ldots, 3\}$ let p'_i be an identical copy of player p_i.

We construct a new system S of eight players (the original ones along with their copies) connected by the hypergraph H'_1 as shown in the Figure 1. The 3-hyperedges in H'_1 are $\{\{p_1, p_2, p'_4\}, \{p_2, p_3, p_4\}, \{p'_1, p'_2, p_4\}, \{p'_2, p'_3, p'_4\}\}$. In S, both p_i and its copy p'_i run the same local program π_i. Notice that some hyperedges to which p_i was connected in the original network H_1 are substituted by other hyperdeges in the new network H'_1. For each player p_i, we specify a mapping $M_{p_i} : E(H_1) - > E(H'_1)$ such that if p_i communicates along $e \in H_1$ in A then it communicates along $M_{p_i}(e)$ in the new system.
$M_{p_1}(\{p_1, p_2, p_4\}) = \{p_1, p_2, p'_4\}, M_{p_3}(\{p_2, p_3, p_4\}) = \{p_2, p_3, p_4\}$,
$M_{p_2}(\{p_1, p_2, p_4\}) = \{p_1, p_2, p'_4\}, M_{p_2}(\{p_2, p_3, p_4\}) = \{p_2, p_3, p_4\}$,
$M_{p_4}(\{p_1, p_2, p_4\}) = \{p'_1, p'_2, p_4\}, M_{p_4}(\{p_2, p_3, p_4\}) = \{p_2, p_3, p_4\}$
The mapping for p'_i is obtained by substituting p'_j for p_j and vice versa in the mapping for p_i. The mapping becomes clear from Figure 1.

The rest of the proof follows as in the proof of Theorem [6.39] of [10]. □

Observe that in the proof, we only used the corruptibility of the processes p_2 and p_4. Thus we have the following

[5] If p_1 wants to send some message to p_2 along $\{p_1, p_2\}$, he sends it along $\{p_1, p_2, p_4\}$ and addresses it to p_2. If p_2 wants to send a message to p_4 he sends it along $\{p_1, p_2, p_4\}$ and $\{p_2, p_3, p_4\}$ and addresses them to p_4.

[6] By 'local program' we mean the version of the protocol as run at a particular player. An execution of a local program is dependent only on his input value and on the messages he receives during the course of the protocol.

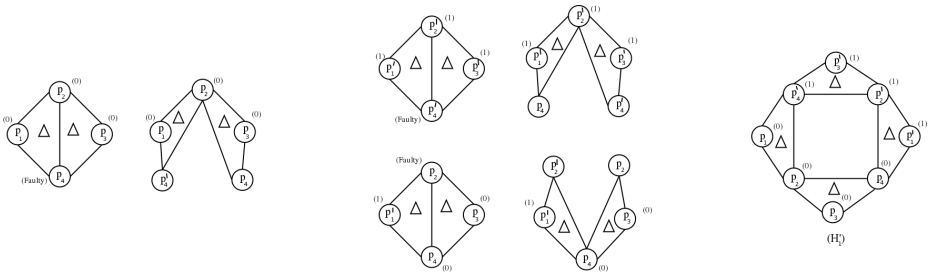


Fig. 1. Views: $\{p_1, p_2, p_3\}$,$\{p'_1, p'_2, p'_3\}$ & $\{p'_1, p_4, p_3\}$.

Observation 1 *Byzantine agreement is not achievable on four node hypergraph H tolerating the adversary $\mathcal{A}$ characterized by the adversary structure $\mathcal{A}_{adv} = \{\{p_2\}, \{p_4\}\}$ if $\{p_2, p_4\}$ disconnects the hypergraph.*

We shall now continue with the proof of the necessity of conditions 1 and 2 of Theorem 1. Specifically we prove that Byzantine agreement is not achievable among n processes tolerating t faults if the hypergraph is not $(2, n)$-hyper-$(2t + 1)$-connected.

On the contrary, assume a protocol Π exists for Byzantine agreement on some hypergraph $H(P, E)$ that is not $(2, n)$-hyper-$(2t+1)$-connected. The main idea of the proof is to construct a protocol Π' that achieves Byzantine agreement on a four node hypergraph H' tolerating the adversary $\mathcal{A}$ characterized by the adversary structure $\mathcal{A}_{adv} = \{\{p_2\}, \{p_4\}\}$ where $\{p_2, p_4\}$ disconnects the hypergraph H'. This leads to a contradiction since existence of such Π' violates Observation 1.

Let $n > (2t+1)$, assume that $H(P, E)$ is not $(2, n)$-hyper-$(2t+1)$-connected. That is there exist a set of $2t$ processes that disconnect H. Partition this set into two sets of t processes each, say P_2 and P_4. On removal of the $2t$ processes, the hypergraph disconnects into at least two components, let the processes in one component be P_1 and the processes in the remaining components be P_3. Processes in P_1 and P_3 are disconnected from each other. Thus there does not exist a hyperedge in E which has non empty intersection with both P_1 and P_3.

Construct a hypergraph $H'(P', E')$ on four processes where $P' = \{p_1, p_2, p_3, p_4\}$, $\{p_i, p_j\} \in E'$ if P_i and P_j are connected in H (there is a hyperedge $e \in E$ that has non empty intersection with each of P_i, P_j) and $\{p_i, p_j, p_k\} \in E'$ if P_i, P_j and P_k are connected in H (there is a hyperedge $e \in E$ that has non empty intersection with each of P_i, P_j, P_k). It follows from the earlier argument that $\{p_1, p_3\} \notin E'$ and hence $\{p_2, p_4\}$ disconnects H'.

Using the protocol Π, construct a protocol Π' for Byzantine agreement among the processes in P' connected by the hypergraph H' by allowing p_i simulate the behavior of processes in P_i for $i = 1, 2, 3, 4$. Processes p_i simulate the behavior of processes in P_i as follows: (a) Set the inputs of all players in P_i as the input of p_i, (b) In each round, messages sent among $p \in P_i$ and $q \in P_j$ using the hyperedge $\{p, q\} \in E$ are sent using the hyperedge $\{i, j\} \in E'$ ($\{i, j\} \in E'$

by the definition of E') and messages sent among $p \in P_i$, $q \in P_j$ and $r \in P_k$ using the hyperedge $\{p, q, r\} \in E$ are sent using the hyperedge $\{i, j, k\} \in E'$ ($\{i, j, k\} \in E'$ by the definition of E') and (c) At the end of simulation of Π, p_i accepts the value of a process in P_i.

Observe that if Π tolerates t faults, specifically if Π tolerates the adversary characterized by the adversary structure $\{P_2, P_4\}$ where $P_2 \cup P_4$ disconnects H then Π' tolerates the adversary characterized by the adversary structure $\{\{p_2\}, \{p_4\}\}$ where $\{p_2, p_4\}$ disconnects H'. This leads to a contradiction to Corollary 1.

To prove the case for $n = (2t+1)$, assume the contrary i.e., there is a protocol that achieves Byzantine agreement on a $(2t+1)$-node hypergraph that is not 2-hyperedge complete. Consider the set of P' of $(2t-1)$ processes that disconnect H. Partition P' into two sets P_2 and P_4 of sizes t and $(t-1)$ respectively and continue as in the above case. This completes the proof of the necessity of conditions 1 and 2 of Theorem 1 □

We shall now turn to the proof of the necessity of condition 3 of Theorem 1. It is crucial to understand connectivity of hypergraphs from a set theoretic view at this point.

Lemma 2. *Let* $|\mathcal{P}| = n$, $2t < n \leq 3t$, $P_1, P_2, P_3 \subset \mathcal{P}$ *and* $|P_1| = |P_2| = |P_3| = t$. *If* $(P_1 \cup P_2 \cup P_3) = \mathcal{P}$ *then* $|P_1 - (P_2 \cup P_3)| + |P_2 - (P_1 \cup P_3)| + |P_3 - (P_2 \cup P_1)| \geq (2n - 3t)$.

Proof:
$|P_1 - (P_2 \cup P_3)| + |P_2 - (P_1 \cup P_3)| + |P_3 - (P_2 \cup P_1)|$
$= n - |(P_1 \cap P_2) - P_3| - |(P_2 \cap P_3) - P_1| - |(P_1 \cap P_3) - P_2| - |P_1 \cap P_2 \cap P_3|$
$= n - |P_1 \cap P_2| - |P_2 \cap P_3| - |P_3 \cap P_1| + 2|P_1 \cap P_2 \cap P_3|$
$= n - (3t - n + |P_1 \cap P_2 \cap P_3|) + 2|P_1 \cap P_2 \cap P_3|$
$= 2n - 3t + |P_1 \cap P_2 \cap P_3| \geq 2n - 3t.$ □

Lemma 3. *Let* $|P| = n$, $2t < n \leq 3t$. *Hypergraph* $H(P, E)$ *is* $(3, t)$*-hyper-*$(3t - n+1)$*-connected if and only if for every* $P_1 \cup P_2 \cup P_3 = P$ *and* $|P_1| = |P_2| = |P_3| = t$, *there exists a* 3*-hyperedge across* $P_1 - (P_2 \cup P_3), P_2 - (P_1 \cup P_3), P_3 - (P_2 \cup P_1)$ *i.e.,* $\exists i \in P_1 - (P_2 \cup P_3)$, $j \in P_2 - (P_1 \cup P_3)$, $k \in P_3 - (P_2 \cup P_1)$ *such that* $\{i, j, k\} \in E$.

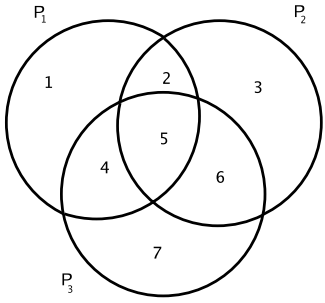
Proof: ($\Longrightarrow$) Let $H(P, E)$ be $(3, t)$-hyper-$(3t - n + 1)$-connected. $|(P_1 \cap P_2) - P_3| + |(P_2 \cap P_3) - P_1| + |(P_1 \cap P_3) - P_2| + |P_1 \cap P_2 \cap P_3| \leq 3t - n$ from proof of Lemma 2. Further each of the sets $P_1 - (P_2 \cup P_3), P_2 - (P_1 \cup P_3)$ and $P_3 - (P_2 \cup P_1)$ are non empty since $|P_i \cup P_j| \leq 2t < n$. Since H is $(3, t)$-hyper-$(3t - n + 1)$-connected, there is a 3-hyperedge across the sets $P_1 - (P_2 \cup P_3), P_2 - (P_1 \cup P_3)$ and $P_3 - (P_2 \cup P_1)$.
($\Longleftarrow$) Assume the contrary, i.e. there exists a hypergraph $H(P, E)$ such that for some t $(2t < n \leq 3t)$ H is not $(3, t)$-hyper-$(3t - n + 1)$-connected but there exists a 3-hyperedge across $P_1 - (P_2 \cup P_3), P_2 - (P_1 \cup P_3), P_3 - (P_2 \cup P_1)$ whenever $P_1 \cup P_2 \cup P_3 = \mathcal{P}$ and $|P_1| = |P_2| = |P_3| = t$. Since H is not $(3, t)$-hyper-$(3t - n + 1)$, there exists a set C of $(3t - n)$ nodes and a partition of $P - C$ into 3 sets S_1, S_2, S_3 with $1 \leq |S_i| \leq t$, such that there is no 3-hyperedge across S_1, S_2, S_3.

Partition C into 3 sets C_1, C_2, C_3 such that $|C_i| = 2t + |S_i| - n$. Construct P_1, P_2, P_3 such that $P_1 = S_1 \cup C_2 \cup C_3$, $P_2 = S_2 \cup C_1 \cup C_3$ and $P_3 = S_3 \cup C_1 \cup C_2$. Observe that $P_1 \cup P_2 \cup P_3 = S_1 \cup S_2 \cup S_3 \cup C = P$. Further $|P_1| = |S_1| + |C_2| + |C_3| = |S_1| + |C| - |C_1| = |S_1| + 3t - n - 2t - |S_i| + n = t$. Similarly, $|P_2| = |P_3| = t$. So there exists a 3-hyperedge across S_1, S_2, S_3. This is a contradiction. Hence H is $(3, t)$-hyper-$(3t - n + 1)$-connected. □

Proof (Necessity of the condition 3): Assume the contrary, i.e., $H(P, E)$ is not $(3, t)$-hyper-$(3t-n+1)$-connected. Then, from Lemma 3 it follows that there exist $P_1, P_2, P_3 \in \mathcal{A}_{adv}$ such that $|P_1| = |P_2| = |P_3| = t$, $P_1 \cup P_2 \cup P_3 = P$ with no 3-hyperedge across $P_1 - (P_2 \cup P_3), P_2 - (P_1 \cup P_3), P_3 - (P_2 \cup P_1)$. Let Π be the protocol for Byzantine agreement tolerating the adversary $\mathcal{B}$ characterized by the adversary structure $\mathcal{A}_{adv}$, the protocol also tolerates the adversary $\mathcal{B}'$ characterized by the adversary structure $\mathcal{A}'_{adv} = \{P_1, P_2, P_3\}$. We show that there cannot exist a protocol for Byzantine agreement among the processes of $P_1 \cup P_2 \cup P_3$ tolerating the adversary $\mathcal{B}'$ when $P_1 - (P_2 \cup P_3), P_2 - (P_1 \cup P_3), P_3 - (P_2 \cup P_1)$ are not connected by a 3-hyperedge.

Assume that the protocol runs for r rounds. Informally, the proof aims to construct three *scenarios* of protocol execution by defining the process inputs and behavior in each case such that the requirements of Byzantine agreement in these three scenarios imply a contradiction. The proof is similar to the proof of Theorem 3.1 in [1].

Before proceeding to the proof, we first introduce some notation. We denote the messages sent from process x to process y in round r as $M^r{}_{xy}(\delta)$ where δ is the scenario under consideration. We also let $\mathcal{M}^r_x(\delta)$ denote the ordered list of all the messages sent to the process x through rounds $1, 2, ..., r$. We define two scenarios X and Y to be *indistinguishable* with respect to process x after r rounds if $\mathcal{M}^r_x(X) = \mathcal{M}^r_x(Y)$ and the process x's input in X and Y is the same. We now describe three scenarios, α, β and γ of protocol execution and show



scenario	1	2	3	4	5	6	7
alpha	h0	h0	h0	c0	s	c1	c
beta	h0	c0	c	h0	s	c1	h1
gamma	c	c0	h1	c0	s	h1	h1

c - corrupt, h - honest, s - stop
initial value 1 or 0

Fig. 2. Scenarios α, β and γ.

that the requirements of Byzantine agreement in these three scenarios imply a contradiction to the existence of a protocol. For each scenario we specify the behavior of players belonging to each adversary set.

- **Scenario α:** In this scenario, the adversary corrupts processes belonging to the set P_3. Processes in $(P_1 \cup P_2) - P_3$ are all honest and start with input 0.
- **Scenario β:** The adversary corrupts processes belonging to the set P_2. Processes in $P_3 - (P_1 \cup P_2)$ have input 1 while processes in $P_1 - P_2$ have input 0.
- **Scenario γ:** The adversary corrupts processes belonging to the set P_1. Processes in $(P_3 \cup P_2) - P_1$ are honest and start with input 1.

We now describe the adversary strategy for each of the scenarios.

- In scenario α, the faulty processes imitate their behavior in scenario β. Formally, $M^r_{zx}(\alpha) = M^r_{zx}(\beta)\ \forall r, z \in P_3$,(i.e. In the first round every one acts honestly in all three scenarios. From the next round every player in P_3 in scenario α would behave as how they would behave in scenario β in that round.)
- In scenario γ, the faulty processes imitate their behavior in scenario β. Formally, $M^r_{zx}(\gamma) = M^r_{zx}(\beta)\ \forall r, z \in P_1$.
- In scenario β, the adversary corrupts processes belonging to the adversary set P_2. In their communication with processes in $P_1 - (P_2 \cup P_3)$ the faulty processes send the same messages that were sent by them in scenario α. And in their communication with players in $P_3 - (P_2 \cup P_1)$ the faulty processes send the same messages that were sent by them in scenario γ[7].
- Processes belonging to more than one adversary set send the same messages as in the scenario in which they are honest. Therefore, they send the same messages in all the three scenarios.

We complete the proof by separately proving the following statement: No protocol can achieve agreement in all three scenarios (see Lemma 6). Evidently the above statement completes the contradiction to the assumption that Byzantine agreement is possible if the hypergraph is not $(3, t)$-hyper-$(3t-n+1)$-connected.

Lemma 4. *The two scenarios, α and β are indistinguishable to any process belonging to $P_1 - (P_2 \cup P_3)$.*

Proof: Processes belonging to $P_1 - (P_2 \cup P_3)$ start with the same inputs in both the scenarios α and β. Hence they behave similarly in the first round of both the scenarios. By the specified adversarial strategy, processes belonging to P_2 and P_3 send the same message to processes in $P_1 - (P_2 \cup P_3)$ in both the scenarios. By induction on the number of rounds, it follows that processes in $P_1 - (P_2 \cup P_3)$ receive the same messages in both the scenarios, i.e., $\forall r\ \mathcal{M}^r_x(\alpha) = \mathcal{M}^r_x(\beta)$, $x \in P_1 - (P_2 \cup P_3)$. □

Lemma 5. *The two scenarios, β and γ are indistinguishable to any process belonging to $P_3 - (P_1 \cup P_2)$.*

[7] Had there been a 3-hyperedge across $P_2 - (P_1 \cup P_3)$, $P_1 - (P_2 \cup P_3)$ and $P_3 - (P_2 \cup P_1)$, the protocol would have forced the players in $P_2 - (P_1 \cup P_3)$ to use the 3-hyperedges whenever they have to send messages to $P_1 - (P_2 \cup P_3)$ or $P_3 - (P_2 \cup P_1)$. This would have prevented the double dealing of the processes that is being described here.

Proof: Similar to the proof of Lemma 4. □

Lemma 6. *No protocol can achieve agreement in all three scenarios.*

Proof: Suppose there exists a protocol which achieves agreement in all the three scenarios. From the validity condition for agreement, it follows that the honest processes must agree on the value 0 in scenario α, and the value 1 in the scenario γ. Processes in $P_1 - (P_2 \cup P_3)$, who behave honestly in both the scenarios, α and β perceive both these scenarios to be indistinguishable (Lemma 4), hence decide on the same value in both the scenarios, viz, 0. Similarly, the processes in $P_3 - (P_1 \cup P_2)$ decide on the same value in scenarios β and γ, namely 1. This contradicts the agreement condition for Byzantine agreement in scenario β. □
This completes the proof of necessity of all the conditions for Theorem 1. We shall now prove the sufficiency of the three conditions stated in Theorem 1.

Proof Sufficiency: [4] gives a protocol for achieving consensus tolerating Byzantine faults whenever $n > 3t$ and the conditions of Theorem 1 are satisfied. When $n \leq 3t$, we give a protocol (Figure 3) that achieves consensus tolerating Byzantine faults whenever a hypergraph $H(P, E)$ satisfies the conditions of Theorem 1. We only use the 3-hyperedges of H.

In a hypergraph $H(P, E)$, every 3-hyperedge $e \in E$ can locally agree on a single value by a triple majority voting protocol (MVP)[8] [7]. Thus the set e can act as a virtual process P_e, as exploited by [1]. We denote the set of virtual processes $\{P_e | e \in E \text{ and } |e| = 3\}$ as $\mathcal{VP}$.

Observe that the value of a virtual process $P_{\{p,q,r\}}$ can be successfully reconstructed by a honest process whenever two or more processes of $\{p, q, r\}$ are honest. We say that a set A_i in the adversary structure $\mathcal{A}_{adv}$ *dominates* a virtual process $e = \{p, q, r\} \in E$ if $|e \cap A_i| \geq 2$. The value of a virtual process p_e that is dominated by A_i might not be uniquely re-constructable by all honest processes when A_i dominates p_e, so p_e can behave "dishonestly" when A_i is corrupted. The combined adversary set over real and virtual processes ${\mathcal{A}^{\mathcal{P}\cup\mathcal{VP}}}_{adv}$ is given by $\{B(A_i) | A_i \in \mathcal{A}\}$ where $B(A_i) = \bigcup_j \{e_j \text{ where } e_j \in E, \text{ and } A_i \text{ dominates } e_j\} \cup A_i$.

From Lemma 3 it follows that for every three (adversary) sets from ${\mathcal{A}^{(\mathcal{P}\cup\mathcal{VP})}}_{adv}$ we have a virtual player $\{i, j, k\}$ such that no two of $\{i, j, k\}$ belongs to a single adversary set (among the three). This means that none of the three adversary sets can corrupt this virtual player. Thus the adversary structure satisfies $\mathcal{Q}^{(3)}$. Hence a simple extension of the Phase King protocol as described in [2, 3] achieves Byzantine agreement. □

Complexity of the protocol: Real players can exchange values reliably since the hypergraph is (2,n)-hyper-$(2t + 1)$-connected. A universal exchange among the virtual players can be simulated by a universal exchange among the real players, followed by a local computation of all the virtual players values. The reconstruction is successful if the virtual player is honest. This reduces the complexity of universal exchange in each phase from $O(|\mathcal{VP}|^2)$ to $O(|\mathcal{P}|.|\mathcal{VP}|)$. As in

[8] In a MVP every process broadcasts its value and agrees via a local majority

```
for k = 1 to |P| do                    (* Set of kings *)
begin                                  (* Start of a phase *)
    send(value)[a]                     (*Universal Exchange 1*)
    receive(V)
    V^i = {r ∈ P ∪ VP, r sent i}, i = 0, 1
    if V^0 ⊂ of some adversary set in A^(P∪VP)_adv
        send(1)
    else
        send(0)                        (*Universal Exchange 2*)
    receive(R)
    R^i = {r ∈ P ∪ VP, r sent i }, i = 0, 1
    if R^1 ⊄ of any adversary set in A^(P∪VP)_adv
        value = 1
    else
        value = 0
    (for the king p_k only)
        send(value)                    (* King's Broadcast *)
    receive(king's value)
    if R^0 ⊂ of some adversary set in A^(P∪VP)_adv
        value =1
    if R^1 ⊂ of some adversary set in A^(P∪VP)_adv
        value =0
    else   value = king's value
end                                    (* End of the phase *)
```

[a] By send(x) we mean sending x reliably to all processes (if required) using a sub-protocol like that of [5].

Fig. 3. Description of the Phase King protocol for a process in $\mathcal{P} \cup \mathcal{VP}$.

[5, 10], O(t) communication is required for reliably communicating 1 bit between v_i, v_j if $\{v_i, v_j\} \notin E$. Further since $|\mathcal{VP}| = \mathrm{O}(t^3)$, the complexity of each phase is O(nt^4) and hence the above protocol has an overall bit complexity of O(nt^5).

5 Network Design

For $n > 3t$, Byzantine agreement is possible if and only if the graph is $(2t + 1)$-connected [4, 10]. Therefore the graph with the minimal number of edges on which Byzantine agreement is possible is a graph on n nodes that is $(2t + 1)$-connected and has the minimal number of edges. The problem of finding the minimal edge graph on n nodes that is k-connected is a well studied problem in graph theory.

In this section we ask a similar question, for $2t < n \leq 3t$, what is the "minimal" $(2, 3)$-hypergraph on which Byzantine agreement is possible. We assume that the hypergraph is 2-hyperedge complete and give a placement of (nearly) as few 3-hyperedges as possible satisfying the conditions of Theorem 1. In other words, for $n = (3t-k)$, $0 \leq k < t$, we give a $(3, t)$-hyper-$(3t-n+1)$-connected hypergraph that has $O(kt^2)$ 3-hyperedges. For $n = 3t$ this implies that an addition of $O(t^2)$ 3-hyperedges makes Byzantine agreement possible among $3t$ players. Furthermore, for $n = (2t + 1)$ we give a construction that provably uses an asymptotically optimum (ratio bound $1 + o(1)$) number of 3-hyperedges.

5.1 Design for $n = (3t - k)$

Definition 6 (Edge Graph). *Given a 3-uniform hypergraph $H(P, E)$, the* edge graph *of a node $v \in P$ is defined as $G_v(P_v, E_v)$ where $P_v = P - \{v\}$ and $E_v = \{\{i, j\} | \{i, j, v\} \in E\}$.*

For constructing a (3,t)-hyper-$(3t - n + 1)$-connected hypergraph $H(P, E)$ on $n = (3t - k)$ nodes, we consider $P' = \{v_0, v_1, v_2, \ldots, v_k\} \subset P$ and place 3-hyperedges such that for each i, $0 \leq i \leq k$, v_i's edge graph is $(t + k)$-connected. The edge graph is isomorphic to $G(V, E)$ where $V = \{1, 2, \ldots, n-1\}$ and $\{i, j\} \in E$ whenever $(i - j) \bmod (n - 1) \leq \lceil \frac{t+k}{2} \rceil$. Clearly $G(V, E)$ is $(t + k)$-connected.

Claim. $H(P, E)$ is (3,t)-hyper-$(3t - n + 1)$-connected.

Proof: Consider a partition of P into P_1, P_2, P_3 each of size t. It is enough to show that there exists a hyperedge across $P_1 - (P_2 \cup P_3), P_2 - (P_1 \cup P_3), P_3 - (P_2 \cup P_1)$ (Lemma 3). Let us call these sets P'_1, P'_2 and P'_3 respectively. These sets are disjoint and of size $\leq t$ by definition and from Lemma 2, $|P'_1 \cup P'_2 \cup P'_3| = |P'_1| + |P'_2| + |P'_3| \geq (2n - 3t) = (3t - 2k)$. Hence $|P - (P'_1 \cup P'_2 \cup P'_3)| \leq k$.

Since $|P'| = (k + 1)$, there exists a $v \in P'$ such that $v \in P'_1 \cup P'_2 \cup P'_3$. Without loss of generality let $v \in P'_1$. Let G be the subgraph induced by $P'_2 \cup P'_3$ on G_v. Note that G is obtained from G_v by removing $\leq t + k - 1$ nodes from P_v ($|P_v| = 3t - k - 1$ and $|P'_2 \cup P'_3| \geq 2t - 2k$). Since G_v is $(t + k)$ connected, G is 1-connected. This means there exists a pair (i, j) with $i \in P'_2$ and $j \in P'_3$ such that the edge $\{i, j\} \in E_v$, i.e. $\{i, j, v\} \in E$. Therefore the required 3-hyperedge across P'_1, P'_2 and P'_3 is $\{i, j, v\}$. □

In H each of the $(k+1)$ nodes of P' are part of $O(k+t)n = O(t^2)$ hyperedges. Therefore the total number of 3-hyperedges in our construction $= O(kt^2)$.

5.2 Lower Bound for $n = (2t + 1)$

Claim. Consider any hypergraph $H(P, E)$ on $|P| = (2t + 1)$ nodes such that Byzantine Agreement is possible between the nodes (processes) in P tolerating t faults. Every pair of nodes in $H(P, E)$ is part of at least t 3-hyperedges.

Proof: On the contrary, suppose there exist nodes p_1 and p_2 such that they form less than t 3-hyperedges i.e. $|P' = \{p | \{p, p_1, p_2\} \in E\}| < t$. Consider the partition of a $(t + 2)$ subset of $P - P'$ into 3 sets P_1, P_2, P_3, such that $P_1 = \{p_1\}, P_2 = \{p_2\}$. Since Byzantine Agreement is possible among the nodes in P tolerating t faults, from Theorem 1, H must be $(3, t)$-hyper-t-connected, i.e. there exists a 3-hyperedge $\{p_1, p_2, p_3\} \in E$ such that $p_1 \in P_1, p_2 \in P_2, p_3 \in P_3$. But $P_3 \cap P' = \emptyset$; this is a contradiction. □

Observation 2 *From the above claim we find that the total number of 3-hyperedges is at least* $\frac{\binom{2t+1}{2} \times t}{3} = \frac{(2t+1)t^2}{3}$

5.3 Design for $n = (2t + 1)$

We give an inductive construction which yields an asymptotically optimum number of 3-hyperedges.

Basis: The base case starts with $t = 1$ ($n = 3$). Since there are only 3 nodes, one 3-hyperedge is necessary and sufficient.

Induction: Given a hypergraph $H(P, E)$ on $n = (2t + 1)$ nodes ($t \geq 1$) which is $(3, t)$-hyper-t-connected, we give a construction of a hypergraph $H'(P', E')$ on $n = (2t + 3)$ nodes that is $(3, t + 1)$-hyper-$(t + 1)$-connected. We construct $H'(P', E')$ by extending $H(P, E)$ i.e., $P \subset P', E \subset E'$. Let the two additional nodes be x and y i.e. $P' = P \cup \{x, y\}$.

Consider the complete 2-uniform hypergraph on the vertex set P; it can be decomposed into t vertex disjoint Hamilton cycles $C_1, C_2, C_3, \ldots, C_t$. Define

$$\left.\begin{array}{l} C_x = C_1 \cup C_2 \cup \ldots \cup C_{\frac{t}{2}} \\ C_y = C_{\frac{t}{2}+1} \cup C_{\frac{t}{2}+2} \cup \ldots \cup C_t \end{array}\right\} \text{ t even} \qquad \left.\begin{array}{l} C_x = C_1 \cup C_2 \cup \ldots \cup C_{\frac{t+1}{2}} \\ C_y = C_{\frac{t+1}{2}} \cup C_{\frac{t+1}{2}+1} \cup \ldots \cup C_t \end{array}\right\} \text{ t odd}$$

Let the subgraphs induced by C_x and C_y be $G_x(P, C_x)$ and $G_y(P, C_y)$ respectively. Note that G_x and G_y are (2,n)-hyper-t-connected and their union is the complete 2-uniform hypergraph. The additional 3-hyperedges added are: $E_x = \{\{x\} \cup e | e \in C_x\}, E_y = \{\{y\} \cup e | e \in C_y\}, E_{xy} = \{\{x, y, v\} | v \in P\}, E' = E \cup E_x \cup E_y \cup E_{xy}$

Lemma 7. *The hypergraph $H'(P', E')$ is $(3, t + 1)$-hyper-$(t + 1)$-connected.*

Proof: We need to show that for every partition of any $(t + 3)$ subset S of P' into 3 sets S_1, S_2, and S_3, there is a 3-hyperedge that has non empty intersection with each of S_1, S_2, S_3. We consider the different cases of partitions that arise for the $(t + 3)$ set.

Case $S \subset P$: By induction hypothesis we know that for every 3 partition of any $(t + 2)$ subset of P the condition is satisfied and hence will be satisfied for any 3 partition of a $(t + 3)$ subset also.

Case $S - \{x\} \subset P$ and $x \in P_1$: Two cases arise depending on the size of the partition P_1.

If $|P_1| > 1$, consider the $(t+2)$ set $S' = S - \{x\}$ (subset of P). By induction hypothesis, the result is true on S' with the partition $P_1 - \{x\}, P_2$,and P_3.

In the case $|P_1| = 1$ i.e., $P_1 = \{x\}$. The pair of nodes in P which forms 3-hyperedges with x are precisely the edges in C_x. We need one of those edges to be across P_2 and P_3 for the condition to be valid. This means that the subgraph induced by $P_2 \cup P_3$ on G_x must be (2,n)-hyperconnected. Now $|P_2 \cup P_3| = (t+2)$ implying that G_x must be (2,n)-hyper-t-connected.

Case $\{x, y\} \subset S$: Two cases arise depending on whether x and y occur in the same partition or in different partitions.

If they occur in the same partition say P_1, then by virtue of the fact that every pair of nodes in P forms a 3-hyperedge with either x or y since $G_x \cup G_y$ is the complete 2-uniform hypergraph on $2t + 1$ nodes we get that for any $u \in P_2$ and $v \in P_3$ the 2-hyperedge $\{u, v\}$ must form a triangle with either x or y.

If they occur in different partitions, $x \in P_1$ and $y \in P_2$, then for any $v \in P_3$ we have the hyperedge $\{x, y, v\} \in E_{xy} \subset E'$. □

Let $N(k)$ denote the number of 3-hyperedges in the above construction for $n = (2k + 1)$ then $N(k)$ is given by:

$$N(k+1) = N(k) + |E_x(k)| + |E_y(k)| + |E_{xy}(k)| = \begin{cases} N(k) + 2k^2 + 3k + 1 \text{ (t even)} \\ N(k) + 2k^2 + 5k + 2 \text{ (t odd)} \end{cases}$$

Solving the recursion we find $N(k) = \frac{2}{3}t^3 + \Theta(t^2)$. Since the lower bound on the minimum number of 3-hyperedges required is $\frac{(2t+1)t^2}{3}$, the above construction is asymptotically optimum with ratio bound $1 + o(1)$.

6 Conclusion

In this paper, we generalized the following well-known theorem in the literature: *Theorem([5, 10]):* Byzantine agreement in a graph (or 2-uniform hypergraph) of n processes of which up to t may be faulty is possible if and only if $n > 3t$ and the graph is $(2t + 1)$-connected.
Our Generalization: See Theorem 1.

Using this generalization, we solve an open problem of [7], viz., *for* $n = (2t + 1)$*, what is the minimum number of* 3*-hyperedges required to enable Byzantine agreement?* We show that $\left(\frac{2}{3}t^3 + \Theta(t^2)\right)$ 3-hyperedges are necessary and sufficient.

Whenever $n > 2t$ and the minimal connectivity requirements (or more) are satisfied, we presented efficient protocols for Byzantine agreement over $(2, 3)$-hypergraphs.

There are many interesting open questions in a wide variety of directions. We list four natural directions that could be explored.

First, one could consider the complexity issues regarding Byzantine agreement protocols over hypergraphs. For instance, on a complete 2-uniform hypergraph, $t+1$ rounds are necessary and sufficient for agreement; what is the round complexity for the case of hypergraphs?(See [13] for some results).

Next, the lower bounds on the minimum number of hyperedges to achieve agreement seem to be interestingly connected to extremal hypergraph theory. For instance, when $n = 3t$ computing the lower bound in the case of 3-hyperedges becomes the problem of computing a specific *Hypergraph Turan number.*[9]

A third interesting line of research is about the complexity of the following decision problem: *given the required fault-tolerance, is Byzantine agreement possible on the given hypergraph?* For instance, in the case of 2-uniform hypergraphs, verifying $2t + 1$-connectivity is easy (polynomial time algorithms exist); however, for 3-uniform hypergraphs, the status is unknown; nevertheless, there exist very interesting connections to algorithmic hypergraph theory.

Finally, one could extend our results to the non-threshold adversarial model. A straightforward application of the ideas of this paper would result in the following characterization.

[9] The *Turan number* for a hypergraph H denoted as $ex(n, H)$ is the maximum number of hyperedges on a n vertex hypergraph which (up to an isomorphism) does not contain H as its subgraph.

Theorem 2. *Byzantine agreement on a* $(2,3)$*-uniform hypergraph* $H(P,E)$ *tolerating any adversary characterized by the adversary structure* $\mathcal{A}_{adv}$ *that satisfies* $\mathcal{Q}^{(2)}$ *is possible if and only if*

1. *For every node* v *such that there exist two sets* A *and* B *in* $\mathcal{A}_{adv}$ *with* $P - (A \cup B) = \{v\}$*, the edge* $\{v, w\}$ *belongs to* E *for every* $w \in P$ *where* $w \neq v$*.*
2. *If for all* A *and* B *in* $\mathcal{A}_{adv}$*,* $|A \cup B| < (n-1)$*, then the underlying graph of* $H(P,E)$ *is* $\mathcal{A}^{(2)}$*-connected.*
3. *If* $\mathcal{A}_{adv}$ *does not satisfy* $Q^{(3)}$*, then for every three sets* S_1, S_2 *and* S_3 *in* $\mathcal{A}_{adv}$ *such that* $(S_1 \cup S_2 \cup S_3) = P$*, there exists* $e \in E$ *such that* e *has non empty intersection with the sets* $S_1 - (S_2 \cup S_3), S_2 - (S_1 \cup S_3)$ *and* $S_3 - (S_1 \cup S_2)$*.*

However, complexity and placement issues for the non-threshold model are still to be looked into.

References

1. S. Amitanand, I. Sanketh, K. Srinathan, V. Vinod, and C. Pandu Rangan. Distributed consensus in the presence of sectional faults. In *22nd ACM PODC*, pages 202–210, July 2003.
2. P. Berman and J. A. Garay. Asymptotically optimal distributed consensus. In *ICALP*, volume 372 of *LNCS*, pages 80–94, 1989.
3. P. Berman, J.A. Garay, and K.J. Perry. Towards optimal distributed consensus. In *21st IEEE FOCS*, pages 410–415, 1989.
4. D. Dolev. The byzantine generals strike again. *Jl. of Algorithms*, 3(1):14–30, 1982.
5. D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly secure message transmission. *JACM*, 40(1):17–47, 1993.
6. M. Fitzi and U. Maurer. Efficient byzantine agreement secure against general adversaries. In *DISC*, volume 1499 of *LNCS*, pages 134–148, Springer-Verlag, 1998.
7. M. Fitzi and U. Maurer. From partial consistency to global broadcast. In *32nd ACM STOC*, pages 494–503, 2000.
8. M. Hirt and U. Maurer. Complete characterization of adversaries tolerable in secure multiparty computation. In *16th ACM PODC*, pages 25–34, 1997.
9. M.V.N. Ashwin Kumar, P.R. Goundan, K. Srinathan, and C. Pandu Rangan. On perfectly secure communication over arbitrary networks. In *21st ACM PODC*, pages 193-202, 2002.
10. N. Lynch. *Distributed Algorithms*. Morgan Kaufmann, 1997.
11. M. Pease, R. Shostak, and L. Lamport. Reaching agreement in the presence of faults. *Journal of ACM*, 27:228–234, April 1980.
12. M. Pease, R. Shostak, and L. Lamport. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, July 1982.
13. D.V.S. Ravikant, V. Muthuramakrishnan, V. Srikanth, K. Srinathan, and C. Pandu Rangan. Brief Announcement: On the round complexity of distributed consensus over synchronous networks. In *23rd ACM PODC*, 2004. To appear.