We assign to each operation $op$ a tag $tag_{op} = \langle ts_{op}, cid_{op} \rangle$

write: $ts_{op}$ is the timestamp created in TS phase.

read: $ts_{op}|cid_{op}$ equals value of maxts/maxcid received by reader.

### 0.1 Validity condition

We want to show that the value returned by each read is the value of the last preceding write in $\prec$.

Suppose not. Then, suppose $w \prec_w w' \prec r$, and $r$ reads the value written by $w$ (for simplicity we can assume that every write is unique).

Example: $4 \ 3 \ 5 \ 4 \ r$ then read returns 4 (the last one).

Therefore, we have $w(v_1)$ and then $r(v_1)$. If not, then there was a write in between with $v_1$.

We argue that there can’t be the case that $w(v_1) \prec \sigma w'(v_2) \prec \sigma r(v_1)$

$tag_w \prec \sigma \prec tag_{w'} \prec tag_r$

Since $tag_w \prec tag_{w'}$, the maxts computed in TS phase by write $w$ is less than that of write $w'$. Let $Q_w$ and $Q_{w'}$ be the write quorums for $w$ and $w'$ that $w$ and $w'$ write to in their write phases.

Let $Q_r$ be the read quorum that read $r$ receives from in the read phase.

$Q_r \cap Q_w \neq \emptyset$, and $Q_r \cap Q_{w'} \neq \emptyset$. The maxts received by read $r$ should be $\geq (ts_w, ts_{w'})$.

Since $ts_{w'} \succ ts_w$, read $r$ cannot return value written by $w$.

### 1 Byzantine Quorum Systems

Simple non-empty intersections between quorums are not sufficient to guarantee consistency. In particular, if the intersection between two quorums contains a single process that is byzantine, then there is a problem.

Byzantine quorum systems are specified not only with respect to a set of processors $S$, but also assuming specific set system over $S$ called a monotone adversary.
**Definition 1 (Adversary)** Given a set $S$, a set system $\mathcal{B}$ is an adversary for $S$ iff $B \in \mathcal{B} \land B' \subseteq B \Rightarrow B' \in \mathcal{B}$.

Note: the adversary is defined to capture all possible combinations of simultaneously Byzantine processes.

We assume that an adversary for $S$ contains as its elements all possible subsets of $S$ whose elements can be simultaneously Byzantine in any given execution.

### 1.1 Threshold Adversary

We denote by $\mathcal{B}_t$ a threshold adversary that contains all subsets of $S$ of cardinality at most $t$, i.e.

$$\mathcal{B}_t = \{Q \subseteq S : |Q| \leq t\}.$$

We define a kind of Byzantine Quorum Systems called Dissemination Quorum Systems (DQS) [Malkhi, Reiter, '98].

**Definition 2 (Dissemination Quorum Systems)** Given a set $S$ and an adversary $\mathcal{B}$ for $S$, a quorum system DQS is a dissemination quorum system over $S$ iff

$$(\forall Q_1, Q_2 \in \text{DQS}) (\forall B \in \mathcal{B}) Q_1 \cap Q_2 \not\subseteq B.$$

assuming "authenticated Byzantine model".

**Theorem 1** Let $\text{BQS}$ be a coterie over set $S$ and let $\mathcal{B}$ be an adversary for $S$. Then, if there exists an asynchronous implementation of the SWSR storage based on $\text{BQS}$, then $\text{BQS}$ is a dissemination quorum system.