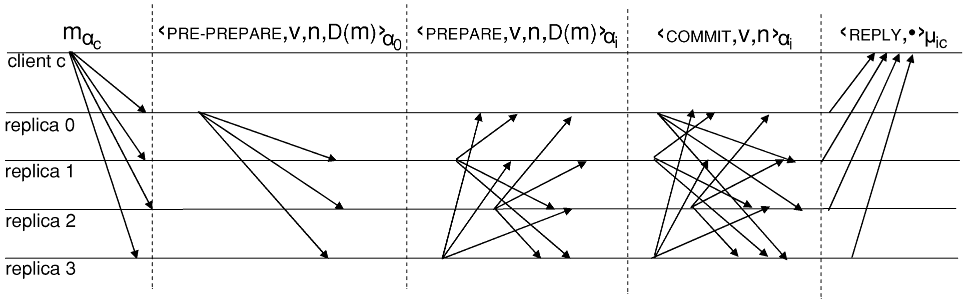
m_{α_c}
$\langle$PRE-PREPARE,v,n,D(m)$\rangle_{\alpha_0}$
$\langle$PREPARE,v,n,D(m)$\rangle_{\alpha_i}$
$\langle$COMMIT,v,n$\rangle_{\alpha_i}$
$\langle$REPLY,•$\rangle_{\mu_{ic}}$
client c
replica 0
replica 1
replica 2
replica 3

Fig. 1. Normal case operation: the primary (replica 0) assigns sequence number n to request m in its current view v and multicasts a PRE-PREPARE message with the assignment. If a backup agrees with the assignment, it multicasts a matching PREPARE message. When a replica receives messages that agree with the assignment from a quorum, it sends a COMMIT message. Replicas execute m after receiving COMMIT messages from a quorum.

Like PRE-PREPARES, the PREPARE and COMMIT messages sent in the other phases also contain n and v. A replica only accepts one of these messages provided that it is in view v; that it can verify the authenticity of the message; and that n is between a low water mark h and a high water mark H. The last condition is necessary to enable garbage collection and to prevent a faulty primary from exhausting the space of sequence numbers by selecting a very large one. We discuss how H and h advance in Section 4.4.

A backup i accepts the PRE-PREPARE message provided (in addition to the conditions above) it has not accepted a PRE-PREPARE for view v and sequence number n containing a different digest. If a backup i accepts the PRE-PREPARE and it has request m in its log, it enters the *prepare* phase by multicasting a $\langle\text{PREPARE}, v, n, D(m), i\rangle_{\alpha_i}$ message with m's digest to all other replicas; in addition, it adds both the PRE-PREPARE and PREPARE messages to its log. Otherwise, it does nothing. The PREPARE message signals that the backup agreed to assign sequence number n to m in view v. We say that a request is *pre-prepared* at a particular replica if the replica sent a PRE-PREPARE or PREPARE message for the request.

Then each replica collects messages until it has a quorum certificate with the PRE-PREPARE and $2f$ matching PREPARE messages for sequence number n, view v, and request m. We call this certificate the *prepared certificate* and we say that the replica *prepared* the request. This certificate proves that a quorum has agreed to assign number n to m in v. The protocol guarantees that it is not possible to obtain prepared certificates for the same view and sequence number and different requests.

It is interesting to reason why this is true because it illustrates one use of quorum certificates. Assume that it were false and there existed two distinct requests m and m' with prepared certificates for the same view v and sequence number n. Then the quorums for these certificates would have at least one nonfaulty replica in common. This replica would have sent PRE-PREPARE or PREPARE messages agreeing to assign the same sequence number to both m and m' in the same view. Therefore, m and m' would not be distinct, which contradicts our assumption.