Phase-King Algorithm

- LSP requires f + 1 rounds and can tolerate upto f <= floor ([n-1] / 3) traitors but requires an exponential number of messages
- Phase King algorithm by Berman and Garay solves the problem under the same model, requiring f + 1 phases and a polynomial number of messages but can tolerate only f < ceil (n/4) traitors

Phase-King

- Each phase has 2 rounds
  - Round 1:
    - Each process broadcasts its estimate of the consensus to all others and awaits the values broadcast by others
    - Counts the number of 1 votes and 0 votes
    - If either number > n/2, then it sets majority to that value and sets **mult** to the number of votes received for the majority value
    - If neither number of votes is greater than n/2, a default value is used fo rmajority value

Phase-King

- Round 2:
  - The phase king for phase k is P_k
  - P_k broadcasts its majority value which serves as a tie-breaker for those which have a mult value less than n/2 + f
  - When a process receives the tie-breaker from the king,
    - If mult > n/2 + f then it updates its estimate of the decision variable v to its majority value
    - Otherwise it updates its estimate of the decision variable v to the tie-breaker value

Phase King Algorithm

Code for each processor p_i:

pref := my input

<u>first round of phase k, $1 \le k \le f+1$:</u>

send pref to all

receive prefs of others

let maj be value that occurs > $n/2$ times (0 if none)

let mult be number of times maj occurs

<u>second round of phase k:</u>

if $i = k$ then send maj to all // I am the phase king

receive tie-breaker from p_k (0 if none)

if mult > $n/2 + f$

then pref := maj

else pref := tie-breaker

if $k = f + 1$ then decide pref

Unanimous Phase Lemma

Lemma (5.12): If all nonfaulty processors prefer *v* at start of phase *k*, then all do at end of phase *k*.

Proof:

- Each nonfaulty proc. receives at least $n - f$ preferences for *v* in first round of phase *k*
- Since $n > 4f$, it follows that $n - f > n/2 + f$
- So each nonfaulty proc. still prefers *v*.

Phase King Validity

Unanimous phase lemma implies validity:

- Suppose all procs have input *v.*
- Then at start of phase 1, all nf procs prefer *v.*
- So at end of phase 1, all nf procs prefer *v.*
- So at start of phase 2, all nf procs prefer *v.*
- So at end of phase 2, all nf procs prefer *v.*
- …
- At end of phase $f + 1$, all nf procs prefer *v* and decide *v.*

Nonfaulty King Lemma

Lemma (5.13): If king of phase k is nonfaulty, then all nonfaulty procs have same preference at end of phase k.

Proof: Let p_i and p_j be nonfaulty.

Case 1: p_i and p_j both use p_k 's tie-breaker. Since p_k is nonfaulty, they both have same preference.

Nonfaulty King Lemma

Case 2: p_i uses its majority value v and p_j uses king's tie-breaker.

- Then p_i receives more than $n/2 + f$ preferences for v
- So p_k receives more than $n/2$ preferences for v
- So p_k 's tie-breaker is v

Nonfaulty King Lemma

Case 3: p_i and p_j both use their own majority values.

- Suppose p_i *'s* majority value is v
- Then p_i receives more than $n/2 + f$ preferences for v
- So p_j receives more than $n/2$ preferences for v
- So p_j 's majority value is also v

Phase King Agreement

Use previous two lemmas to prove agreement:

- Since there are $f + 1$ phases, at least one has a nonfaulty king.
- Nonfaulty King Lemma implies at the end of that phase, all nonfaulty processors have same preference
- Unanimous Phase Lemma implies that from that phase onward, all nonfaulty processors have same preference
- Thus all nonfaulty decisions are same.

Complexities of Phase King

- number of processors $n > 4f$
- $2(f + 1)$ rounds
- $O(n^2 f)$ messages, each of size $\log|V|$