Rendomizirani vizantijski dogovor

Postoji neki poverljiv procesor q
koji u svakoj rundi baca na slučaj novčić
(coin) i informiše sve druge procesore

coin = heads (verovatnoća $\frac{1}{2}$)

coin = tail (verovatnoća $\frac{1}{2}$)

Svaki procesor p_i ima prioritetnu vred. v_i

Na početku,
prioritetna vred se postavlja na početnu vred

Predpostavimo da je početna vred. binarna

$$v_i \in \{0,1\}$$

Ovaj algoritam toleriše $f < \frac{n}{8}$ vizantijskih procesora

Postoje tri praga vrednosti:

$$L = \frac{5n}{8} + 1 \qquad H = \frac{6n}{8} + 1 \qquad G = \frac{7n}{8} + 1$$

U svakoj rundi, procesor p_i izvršava:

Šalji svima v_i;

Primi vrednosti od svih procesora;

$maj_i \leftarrow$ većinska vrednost;

$tally_i \leftarrow$ broj pojava od maj;

If coin=heads then $threshold \leftarrow L = \frac{5n}{8} + 1$

else $threshold \leftarrow H = \frac{6n}{8} + 1$

If $tally_i \geq theshold$ then $v_i \leftarrow maj_i$

else $v_i \leftarrow 0$

If $tally_i \geq G = \frac{7n}{8} + 1$ then došlo se do odluke

Analiza: Ispitajmo slučajeve u rundi

Završetak: Postoji neki procesor p_i sa $tally_i \geq G = \frac{7n}{8} + 1$

Drugi slučajevi:

Sluč. 1: Dva procesora p_i i p_k imaju različite $maj_i \neq maj_k$

Sluč. 2: Svi procesori imaju isti maj_i

Završetak: Postoji neki procesor p_i

sa $tally_i \geq G = \frac{7n}{8} + 1$

Pošto procesora u otkazu ima najviše $f < \frac{n}{8}$

procesor p_i prima bar

$$tally_i - f \geq \frac{6n}{8} + 1$$

glasova za maj_i od dobrih procesora

Zbog toga, svaki procesor p_k

će imati $maj_i = maj_k$

sa $tally_k \geq H = \frac{6n}{8} + 1$

Sledstveno, na kraju runde
svi dobri procesori će imati istu
prioritetnu vrednost:

$$v_k = maj_k = maj_i$$

Opažanje:

Ako na početku runde svi dobri procesori imaju istu prioritetnu vrednost onda se algoritam završava u toj rundi

Ovo važi jer će za svaki procesor p_i uslov završetka $tally_i \geq G = \frac{7n}{8} + 1$ biti zadovoljen u toj rundi

Zbog toga, ako je usloz završetka zadovoljen za jedan procesor u nekoj rundi, onda, će uslov završetka biti zadovoljen za sve procesore u sledećoj rundi.

Sluč. 1: Dva procesora p_i i p_k imaju različite $maj_i \neq maj_k$

Mora biti da je $tally_i < L = \frac{5n}{8} + 1$

i da je $tally_k < L = \frac{5n}{8} + 1$

I zbog toga je $v_i = v_k = 0$

Zato, svaki procesor bira 0,
i algoritam se završava u sledećoj rundi

Predpost. (radi kontradikcije) da je

$$tally_i \geq L = \frac{5n}{8} + 1$$

Onda je bar

$$tally_i - f \geq \frac{4n}{8} + 1 = \frac{n}{2} + 1$$

dobrih procesora glasalo maj_i

Sledstveno, $maj_i = maj_j$

Kontradikcija!

Sluč. 2: Svi procesori imaju isti maj_i

Onda za bilo koja dva procesora p_i i p_k važi da je $|tally_i - tally_k| \leq f$

jer bi inače, broj procesora u otkazu bio veći od f

Neka je p_{min} procesor sa

$$tally_{min} = \min_i \{tally_i\}$$

Pod-sluč. 1: $tally_{\min} < L = \frac{5n}{8} + 1$

Ako je $threshold = H = \frac{6n}{8} + 1$

(ovo se dešava sa verovatnoćom $\frac{1}{2}$)

onda, za bilo koji procesor p_k važi da je

$$tally_k \le tally_{\min} + f < L + f = \frac{6n}{8} + 1 = H$$

I zbog toga je $v_i = v_k = 0$

Dakle, svaki procesor izabira 0,
i algoritam se završava u sledećoj rundi

(ovo se dešava sa verovatnoćom $\frac{1}{2}$)

Pod-sluč. 2: $tally_{\min} \geq L = \frac{5n}{8} + 1$

Ako je $threshold = L = \frac{5n}{8} + 1$

(ovo se dešava sa verovatnoćom $\frac{1}{2}$)

onda, za bilo koji procesor p_k važi da je

$$tally_k \geq tally_{\min} \geq L$$

I zbog toga je $v_k = v_{min}$

Dakle, svaki procesor izabira v_{min} ,
i algoritam se završava u sledećoj rundi

(ovo se dešava sa verovatnoćom $\frac{1}{2}$)