非同期システムのビザンチン定足数が $2f+1$ になる理由

清家大嗣

平成 34 年 3 月 20 日

1 $n = 3f+1$ とした場合に, 定足数が $2f+1$ になる理由について

n を全ノード数, f をフォルティノード数, $n-f$ を誠実なノード数, q をビザンチン定足数 (Byzantine quorum) とする. ここで, 誠実なノード集団が 2 つに分割され, フォルティノードがそれぞれの集団に異なった投票を実行するケースを考える. この場合, 非同期システムであるが故に, ディジタル署名を用いても, この不正行為を検知する前に合意形成を実行してしまう可能性がある. 従って, このような状態でも一つの結果について合意するためには, 以下の不等式が成立する必要がある.

$$\frac{n-f}{2} + f < q. \tag{1}$$

これがビザンチン投票における, 安全性 (Safety) 条件である. また, ビザンチン定足数 q を大きくすれば安全性が確保される一方で, システムが合意形成に至るまでの時間が長くなることが予想される. 特に, 誠実なノード数 $n-f$ を超える定足数 q を設定した場合, システムが永遠に合意形成をしないという状況も考えられる. このような状況を防ぐため, 以下の不等式が成立する必要がある.

$$q \leq n-f. \tag{2}$$

これがビザンチン投票における, 生存性 (Liveness) 条件である. (1, 2) の不等式から, (3) の不等式が得られる.

$$\frac{n+f}{2} < q \leq n-f. \tag{3}$$

特に $n = 3f+1$ とした場合に, 次の不等式が成立する.

$$2f + \frac{1}{2} < q \leq 2f+1. \tag{4}$$

この不等式を満たす q は $2f+1$ しか存在しない. これより, 以下の定理が得られる.

Th. 1. 全ノード数 $n = 3f+1$, フォルティノード数 f とした場合, この非同期システムにおいてビザンチン合意を得るためのビザンチン定足数 q は $2f+1$ しか存在しない.

2 $n = kf$ とした場合のビザンチン定足数の挙動

(3) の不等式に $k = f/n$ を代入することで, (5) の不等式が得られる.

$$\frac{1}{2} \cdot (1 + \frac{1}{k}) \cdot n < q \leq (1 - \frac{1}{k}) \cdot n. \tag{5}$$

ここで, ビザンチン定足数 q が存在する条件は, 以下である.

$$\frac{1}{2} \cdot (1 + \frac{1}{k}) < (1 - \frac{1}{k}).$$

$$\therefore\ 3 < k. \tag{6}$$

また, $k \to \infty$ とすると, (5) の不等式は以下のようになる.

$$\frac{n}{2} < q \leq n. \tag{7}$$

つまり, 誠実なノードの割合がフォルティノードに対して十分に大きくなれば, 多数決の原理によって安全性が保証される. また, 全会一致となる定足数 q に対してあっても, 生存性が保証される (いつかは合意に至る).

参考文献

[1] LayerX Research 「Why Byzantine quorum is $2f + 1$?」`https://scrapbox.io/layerx/Byzantine_quorum`.