# CoT共识协议容错能力证明

## CoT共识协议容错能力证明

**定理 (容错下限)**
在一个部分同步的网络中，若一个确定性共识协议需要容忍 `f` 个拜占庭节点，并同时保证**安全性**（即一致性）与**活性**（即最终性），则全网参与共识的节点总数 `N` 必须满足：

$$N \geq 3f + 1$$

### 1. 定义与前提

1. **拜占庭节点 (Byzantine Node)**: 可能表现出任意行为的故障节点，包括不响应、发送错误信息、欺骗、合谋等。
2. **安全性 (Safety)**: 所有诚实节点对最终状态达成一致，绝不会在同一个位置提交不同的值。（即**不会出现分叉**）。
3. **活性 (Liveness)**: 客户端提交的合法请求最终会被系统处理并记录。（即**共识最终能够达成**）。
4. **网络模型**: 我们假设一个**部分同步网络**。即存在一个未知的全局稳定时间点，在此之后，网络消息的传输延迟存在一个已知的上限 `Δ`。这是PBFT及其衍生协议（如CoT）的标准网络假设。
5. **确定性协议**: 在相同输入和状态下，诚实节点的行为是确定的。

### 2. 反证法证明

我们采用反证法，假设存在一个协议 `P`，在 `N ≤ 3f` 的情况下，依然能保证安全性和活性。我们将展示这会导致矛盾。

#### 2.1 情景构造

将全网 `N` 个节点划分为三个互不相交的集合 `G1`，`G2`，`G3`，其大小满足：

$$|G1| = |G2| = f, \quad |G3| = N - 2f$$

根据我们的假设 `N ≤ 3f`，可得：

$$|G3| = N - 2f \leq 3f - 2f = f$$

现在，我们考虑三个不同的执行场景（`Execution 1`，`Execution 2`，`Execution 3`）。在每个场景中，集合 `G3` 的节点行为是相同的，但网络分区和恶意节点的行为不同。

- **Execution 1 ($E_1$):**
  - `G2` 和 `G3` 中的节点是**拜占庭节点**（总数 `|G2| + |G3| ≤ f + f = 2f`）。
  - `G1` 中的节点是诚实的。
  - 客户端提议了一个值 `v1`。由于拜占庭节点可以合谋，它们对 `G1` 隐藏了 `G3` 的存在。在 `G1` 的视角里，网络中只有 `G1` (f个) 和 `G2` (f个) 两个群体。由于 `|G1| = f`，`|G2| = f`，且 `G2` 是恶意的，诚实节点 `G1` 无法独立达成共识（因为无法获得 `2f+1` 的多数票）。然而，为了满足**活性**，协议 `P` 必须最终达成共识。拜占庭节点 `G2` 和 `G3` 配合 `G1` 的请求，让 `G1` 最终在值 `v1` 上达成共识。
- **Execution 2 ($E_2$):**
  - 此场景与 $E_1$ 对称。
  - `G1` 和 `G3` 中的节点是**拜占庭节点**（总数 `≤ 2f`）。
  - `G2` 中的节点是诚实的。
  - 客户端提议了一个值 `v2` (且 `v2 ≠ v1`)。同样，拜占庭节点对 `G2` 隐藏了 `G3`。`G2` 在不知情的情况下，为了满足**活性**，最终在值 `v2` 上达成共识。
- **Execution 3 ($E_3$):**
  - `G3` 中的节点是**拜占庭节点**（总数 `|G3| ≤ f`）。
  - `G1` 和 `G2` 中的节点是诚实的。
  - 网络发生**分区**。`G1` 和 `G2` 之间无法通信。
  - 在 `G1` 的分区中，情况与 $E_1$ 完全一样：`G1` 只能看到自己（诚实）和 `G2`（由于网络分区，`G2` 不响应，其行为与恶意节点无异）。为了满足活性，`G1` 必须在某个值上达成共识。根据 $E_1$ 的经验，`G1` 最终会提交 `v1`。
  - 在 `G2` 的分区中，情况与 $E_2$ 完全一样。根据 $E_2$ 的经验，`G2` 最终会提交 `v2`。

### 2.2 推导矛盾

1. 在 $E_1$ 中，诚实集合 `G1` 提交了 `v1`。
2. 在 $E_2$ 中，诚实集合 `G2` 提交了 `v2`。
3. 在 $E_3$ 中:
   - 对于诚实集合 `G1`，其本地视图与 $E_1$ 是不可区分的。所有收到的消息来源（来自 `G2` 和拜占庭集合 `G3` 的消息）在 $E_1$ 和 $E_3$ 中对于 `G1` 来说是完全相同的（都是沉默或看似恶意）。由于协议是确定性的，`G1` 在 $E_3$ 中必然做出与 $E_1$ 中相同的决定，即**提交** `v1`。
   - 同理，对于诚实集合 `G2`，其本地视图与 $E_2$ 是不可区分的。因此，`G2` 在 $E_3$ 中必然提交 `v2`。

由此，我们得出在 $E_3$ 这个执行场景中，诚实节点集合 `G1` 提交了 `v1`，而另一个诚实节点集合 `G2` 提交了 `v2`，且 `v1 ≠ v2`。

这**直接违反了安全性**（一致性）的定义。两个诚实的群体最终对共识结果产生了分歧，导致了状态分叉。

### 2.3 结论

因此，我们最初的假设 `N ≤ 3f` 是错误的。一个能够同时保证安全性和活性的确定性拜占庭容错共识协议，其节点总数必须满足:

$$N \geq 3f + 1$$

### 3. 补充说明

- `3f+1` **的最优性**: 上述证明表明 `N ≥ 3f+1` 是一个**必要条件**。事实上，PBFT 等协议已经证明了 `N = 3f+1` 是**充分条件**。因此，`3f+1` 是此类问题的**紧确界**。
- **与投票配额的关系**: 在协议的具体实现中（如CoT的第4步），通常要求收到 `2f+1` 个相同响应后才能进入下一阶段。这是因为在 `N = 3f+1` 的情况下，`2f+1` 是**绝对多数**。任何两个 `2f+1` 的集合之间必然存在至少一个**公共的诚实节点**，这个公共的诚实节点保证了不同视图下的一致性，从而奠定了安全性的基础。
  - 设两个法定人数集合为 `Q1` 和 `Q2`，`|Q1| = |Q2| = 2f+1`。
  - 则 `|Q1 ∩ Q2| = |Q1| + |Q2| - |Q1 ∪ Q2| ≥ (2f+1) + (2f+1) - (3f+1) = f+1`。
  - 这 `f+1` 个公共节点中至少有一个是诚实的（因为恶意节点最多只有 `f` 个）。这个诚实的公共节点确保了 `Q1` 和 `Q2` 就同一件事达成一致。