

## 1. 绘图表示使用专用硬件所获得的总体加速比 (y 轴) 与 $e$ (x 轴) 之间的关系。

总体加速比 ( $S$ ) 由 Amdahl's Law 给出:

$$S = \frac{1}{(1-f) + \frac{f}{A}}$$

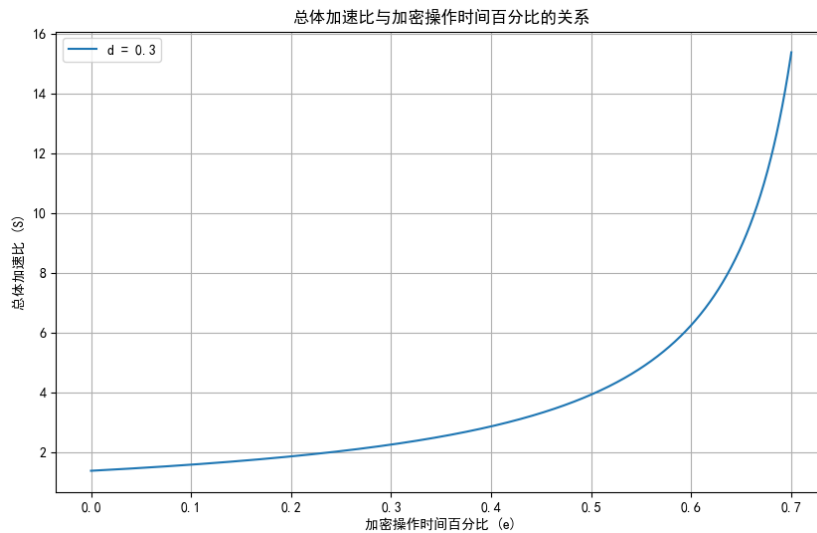
其中,  $f$  是可以加速的部分在总时间中所占的比例,  $A$  是加速比。

假设在普通硬件上, 处理时间中有  $e$  百分比花费在加密上,  $d$  百分比花费在解密上, 剩余  $1 - e - d$  的百分比花费在其他无法加速的操作上。

那么, 总体加速比  $S$  可以表示为:

$$S = \frac{1}{(1 - e - d) + \frac{e}{20} + \frac{d}{10}}$$

为绘制总体加速比  $S$  与加密操作时间百分比  $e$  之间的关系, 我们可以在固定  $d(d = 0.3)$  的前提下, 计算并绘制  $S$  随  $e$  变化的曲线。



## 2. 如果总体加速比为 2, 那么使用专门硬件后花费在解密操作上的时间百分比是多少?

我们已经知道总体加速比  $S$  由以下公式给出:

$$S = \frac{1}{(1 - e - d) + \frac{e}{20} + \frac{d}{10}}$$

代入总体加速比  $S = 2$ , 反解出解密操作时间百分比  $d$  与加密操作时间百分比  $e$  的关系。

$$2 = \frac{1}{(1 - e - d) + \frac{e}{20} + \frac{d}{10}}$$

简化得到:

$$d = \frac{0.5 - 0.95e}{0.9}$$

### 3. 我们能够得到的最大总体加速比是多少？哪种类型的工作会给我们带来这样的加速比？获得最大加速比时， $e$ 和 $d$ 分别是多少？

总体加速比  $S$  由以下公式给出：

$$S = \frac{1}{(1 - e - d) + \frac{e}{20} + \frac{d}{10}}$$

我们的目标是找到使  $S$  最大的  $e$  和  $d$  值。首先，我们需要分析在极端情况下的加速比：

当  $e = 1$  且  $d = 0$  时，表示系统中的所有时间都花费在加密操作上，没有解密操作。此时：

$$S = \frac{1}{(1 - 1 - 0) + \frac{1}{20} + \frac{0}{10}} = \frac{1}{\frac{1}{20}} = 20$$

当  $e = 0$  且  $d = 1$  时，表示系统中的所有时间都花费在解密操作上，没有加密操作。此时：

$$S = \frac{1}{(1 - 0 - 1) + \frac{0}{20} + \frac{1}{10}} = \frac{1}{\frac{1}{10}} = 10$$

从上述两种情况可以看出，**加密操作的加速比更高（20 倍），因此最大加速比发生在  $e = 1$  且  $d = 0$  的情况下。**

#### 结论

1. 最大总体加速比为 20。
2. 当所有时间都花费在加密操作上（即  $e = 1$ ,  $d = 0$ ）时，可以得到最大的加速比。
3. 获得最大加速比时  $e = 1$ ,  $d = 0$ 。