

词典

排解冲突：平方试探

09-C5

三十六计，走为上计

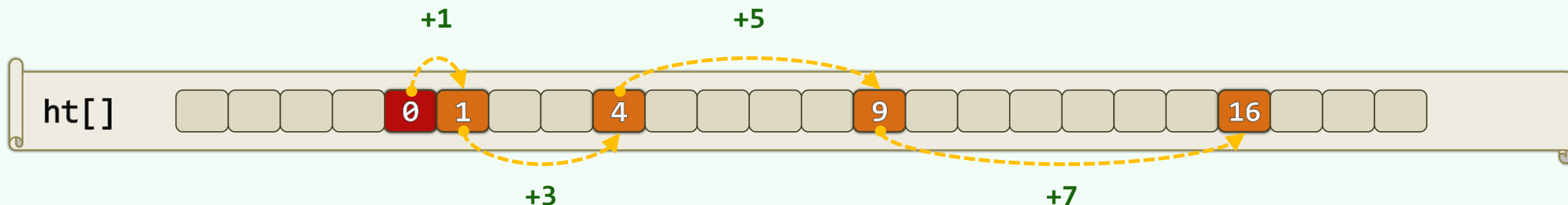
我真的以为，这样何尝不是一种所谓的解脱
要背负的辛苦又有谁能够清楚，那内心的冲突

邓俊辉

deng@tsinghua.edu.cn

平方试探

❖ Quadratic Probing: $r_i(key) = (\text{hash}(key) + i^2) \bmod \mathcal{M}$, $i = 0, 1, 2, 3, \dots$



❖ 沿着试探链，各桶的间距**线性**递增：一旦冲突，可“**聪明**”地跳离是非之地

❖ 数据**堆积**现象有所改善

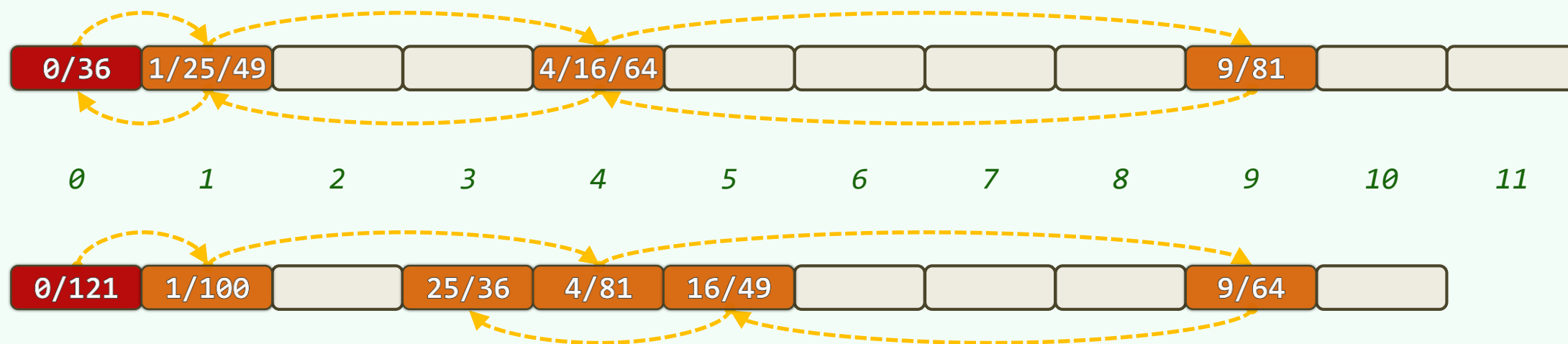
❖ **cache**的利用率有所下降，好在还不算差

❖ 只要有**空桶**，就...一定能...找到吗？毕竟，可不再是**逐个**地试探了

素数表长时，只要 $\lambda < 0.5$ 就一定能够找出；否则，不见得

❖ $\{0, 1, 2, 3, 4, 5, \dots\}^2 \% 12 = \{0, 1, 4, 9\}$

❖ M 若为合数， $n^2 \% M$ 可能的取值可能少于 $\lceil M/2 \rceil$ 种——此时，只要对应的桶均非空...



❖ Quadratic Residue: 若 M 为素数，则 $n^2 \% M$ 恰有 $\lceil M/2 \rceil$ 种取值，且由试探链的前 $\lceil M/2 \rceil$ 项取遍

❖ $\{0, 1, 2, 3, 4, 5, \dots\}^2 \% 11 = \{0, 1, 4, 9, 5, 3\}$

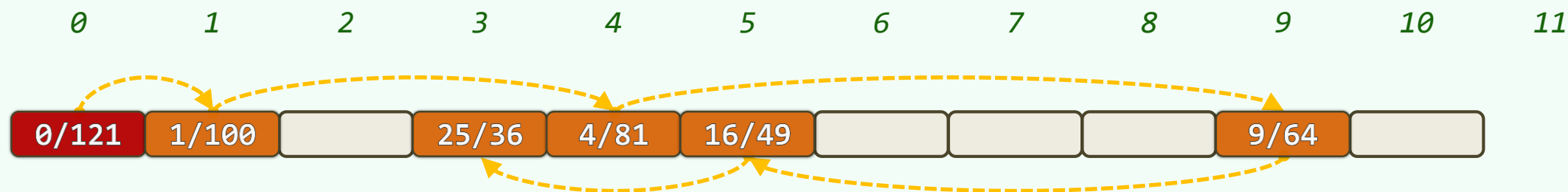
每一条试探链，都有一个足够长的无重前缀

❖ 反证：假设存在 $0 \leq a < b < \lceil \mathcal{M}/2 \rceil$ ，使得沿着试探链，第 a 项和第 b 项彼此冲突

❖ 于是： a^2 和 b^2 自然关于 \mathcal{M} 同余，亦即 $a^2 \equiv b^2 \pmod{\mathcal{M}}$

$$b^2 - a^2 = (b + a) \cdot (b - a) \equiv 0 \pmod{\mathcal{M}}$$

❖ 然而， $0 < b - a \leq b + a < \lceil \mathcal{M}/2 \rceil + (\lceil \mathcal{M}/2 \rceil - 1) \leq \lceil \mathcal{M}/2 \rceil + \lfloor \mathcal{M}/2 \rfloor = \mathcal{M}$



... 无论 $b - a$ 还是 $b + a$ 都不可能整除 \mathcal{M} [QED]

❖ 那么，另一半的桶，可否也利用起来呢...