## 8 Генерация ключа

**Задача.** Бобу требуется сгенерировать ключ, который обладает свойствами $C_1, \ldots, C_n$. Боб выбирает ключ наудачу и проверяет его свойства. Как только одно из свойств не выполняется, Боб генерирует новый ключ, проверяет его и так далее, до тех пор, пока не будет найден ключ, обладающий всеми свойствами. Известно, что случайный ключ обладает свойством $C_i$ с вероятностью $p_i$ независимо от других свойств. Известно также, что для проверки свойства $C_i$ требуется время $t_i$. В какой очередности Боб должен проверять свойства, чтобы среднее время генерации ключа было минимальным?

**Решение.** Если одна из вероятностей $p_i$ равняется 0, то искомый ключ никогда не будет найден и порядок проверки свойств значения не имеет. Будем далее считать, что $p_i \neq 0$, $i = 1, 2, \ldots, m$.

Докажем, что свойства $C_i$ следует проверять в порядке неубывания отношений

$$\frac{t_i}{q_i}, \quad q_i = 1 - p_i.$$

Введем в рассмотрение производящие функции

$$f_i(x) = \sum_{m \geq 0} p_i q_i^{m-1} x^{mt_i} = \frac{p_i x^{t_i}}{1 - q_i x^{t_i}}.$$

Коэффициент при $x^{mt_i}$ в $f_i(x)$ есть вероятность того, что для определения ключа, удовлетворяющего $C_i$, потребуется проверить $m$ случайных ключей. Используя свойства производящих функций, можно находить различные характеристики времени поиска. Например, среднее время поиска ключа, удовлетворящего $C_i$, есть

$$f_i'(1) = \frac{t_i}{p_i}.$$

Время поиска объекта, удовлетворяющего сначала свойству $C_i$, а затем и свойству $C_j$, описывают композиции $f_{ij}(x) = f_j(f_i(x))$. Среднее время поиска в этом случае есть

$$f_{ij}'(x) = \frac{1}{p_j}\left(t_j + \frac{t_i}{p_i}\right).$$

Для сравнения, среднее время поиска ключа, удовлетворяющего сначала $C_j$, а затем и $C_i$, есть

$$f_{ji}'(x) = \frac{1}{p_i}\left(t_i + \frac{t_j}{p_j}\right).$$

Если $t_i/q_i < t_j/q_j$, то

$$\frac{1}{p_j}\left(t_j + \frac{t_i}{p_i}\right) < \frac{1}{p_i}\left(t_i + \frac{t_j}{p_j}\right).$$

Поэтому в этом случае $C_i$ лучше проверять перед $C_j$.

Проведенные рассуждения можно распространить на тройки, четверки,..., $n$-ки свойств и получить нужный результат. Например, при рассмотрении троек мы имеем дело с композициями $f_{ijk} = f_k(f_j(f_i(x)))$ и средними временами

$$\frac{1}{p_k}\left(t_k + \frac{1}{p_j}\left(t_j + \frac{t_i}{p_i}\right)\right).$$

Среднее время будет минимальным (относительно перестановок $C_i$, $C_j$, $C_k$), если

$$\frac{t_i}{q_i} \leq \frac{t_j}{q_j} \leq \frac{t_k}{q_k}.$$

□