Лекция 9. Экстракторы

1 Общая идея

Есть ряд процессов, результат которых довольно случайный, но никаких гарантий, как можно использовать такую случайность, нет. Так появляется задача получения независимых случайных бит из не совсем случайной последовательности.

Пример 1. Если есть независимые одинаково распределенные случайные биты, но вероятность единицы не равна $\frac{1}{2}$, то можно получать случайные биты так двукратным бросанием: если выпало 01, то вернем 0, если 10, то 1, в противном случае бросим еще раз.

Если биты независимые, но вероятности разные на отрезке $[\delta; 1-\delta]$, то $P(b_1 \oplus \ldots \oplus b_m = 1) \to \frac{1}{2}$, так как $p(1-\delta_m) + (1-p)\delta_m$ это выпуклая комбинация.

Более общий класс источников это k-слабые источники случайности. Мин-энтропия это $H_\infty(B) = -\log_2 \left(\max\limits_x P(\vec{b} = x)\right)$.

$H_\infty(\vec{b}) \geqslant k \Leftrightarrow \forall x P(\vec{b} = x) \leqslant \frac{1}{2^k}$. В этом случае $\vec{b}$ содержит хотя бы k случайных битов.

Плоские распределения на $K \subset \{0,1\}^n$, $|K| = 2^k$ — это равномерные распределения.

Теорема 1. *Если $H_\infty(\vec{b}) \geqslant k$, то $\vec{b}$ — выпуклая комбинация плоских источников.*

Определение 1. Seeded extractor $Ext : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ с параметрами (k, ε) обладает свойством, что: $\forall \xi, H_\infty(\xi) \geqslant k \Rightarrow Ext(\xi, U_\alpha)\varepsilon$-близка к U_m.

Вероятностно можно показать существование экстрактора с параметрами $m = k + d - 2\log\frac{1}{\varepsilon} - O(1)$ и $d = \log(n-k) + 2\log\frac{1}{\varepsilon} + O(1)$.