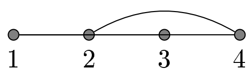
Домашнее задание №5

17 февраля 2020 г.

1. Доказать, что для любой схемы разделения секреты для ниже представленной структуры $\max_i \frac{H(S_i)}{H(S_0)} \geq 3/2$.



2. Докажите, что в игре со ставками только на значения 0 и 1, можно гарантировать выйгрыш не менее $\frac{2^n}{|A|}$, если начальный капитал составлял 1 и было заранее известно, что при случайной генерации $0, 1$ выпадет какая-то последовательность $x \in A$.

Задачи на дополнительные баллы

1. Известно, что в некоторой структуре доступа $D \subset \mathcal{P}(1, ..., n)$ нет ни одно участника, который в одиночку может узнать секрет (в каждой авторизованной группе не меньше 2 участников). Пусть распределение вероятностей $(S_0, S_1, \ldots, S_n)$ является совершенной схемой разделения секрета для , причём значение секрета S_0 принимает с ненулевыми вероятностями k разных значений. Докажите, что существует такая схема разделения секрета $(S_0', S_1', \ldots, S_n')$, в которой S_0' равномерно распределено на k-элементном множестве, а для всех $i = 1, \ldots, n$ выполнено $H(S_i') = H(S_i)$ (т.е., распределение на множестве секретов можно сделать равномерным, не изменяя энтропию долей участников схемы).

2. Постройте совместно распределенные случайные величины ξ, η, β, γ, для которых не выполнено неравенство:

$$I(\xi : \eta) \leq I(\xi : \eta|\beta) + I(\xi : \eta|\gamma) + I(\beta : \gamma).$$