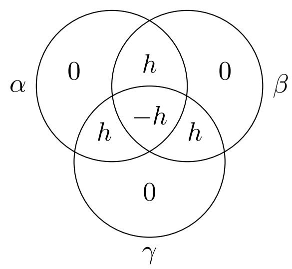
Задачи на дополнительные баллы

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).

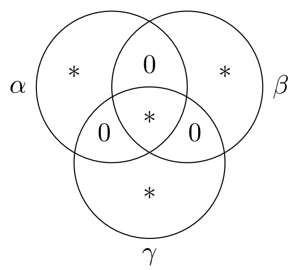
2. Постройте совместно распределенные случайные величины ξ, η, β, γ, для которых не выполнено неравенство:

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

3. Доказать, что следующий профиль реализуется только при $h = \log n$ для некоторого целого n.



4. Пусть α, β и γ имеют следующий профиль.



Докажите, что существует случайная величина δ, такая что

$$\begin{cases} H(\delta \mid \alpha) = 0, \\ H(\delta \mid \beta) = 0, \\ H(\delta \mid \gamma) = 0, \\ H(\delta) = I(\alpha : \beta : \gamma). \end{cases}$$

И при этом $I(\alpha : \beta \mid \delta) = I(\alpha : \gamma \mid \delta) = I(\beta : \gamma \mid \delta) = 0$.