InT 1*. Пусть дан граф G без петель. Алиса и Боб получают две вершины данного графа x, y и хотят узнать существует ли ребро (x, y). Докажите, что детерминированная сложность данной задачи не менее $\log \chi(G)$, где $\chi(G)$ — хроматическое число графа G.
Подсказка: попробуйте предъявить хорошую раскраску, если есть короткий коммуникационный протокол.

InT 2. Покажите, что существует такая монотонная функция $f\colon \{0,1\}^n \to \{0,1\}$, что $\mathrm{D}(\mathsf{KW}_f) \geq n - o(n)$.

1: *Подсказка:* формульная сложность такой функции будет $2^{\Omega(n)}$. – **Dmitry**

Определение

Неформально. Вероятностным коммуникационным протоколом будем называть протокол Π, в котором у Алисы и Боба есть доступ к общим (т.е. оба игрока видят случайные биты) случайным битам. Их цель найти значение функции $f(x, y)$ при этом:

$$\forall x, y \ \Pr_r[\Pi(x, y) \neq f(x, y)] \leq \varepsilon,$$

для некоторого параметра ε.
Минимальное число бит, которым нужно обменяться Алисе и Бобу для того, чтобы посчитать значение функции с указанными ограничениями будем обозначать $\mathrm{R}^{\mathrm{pub}}_{\varepsilon}$.

InT 3. Покажите, что $\mathrm{R}^{\mathrm{pub}}_{\frac{1}{10}}(\mathsf{EQ}) = \mathcal{O}(1)$.

InT 4. Пусть для некоторой функции $f\colon X \times Y \to Z$ существует коммуникационный протокол с ℓ листьями. Докажите, что $\mathrm{D}(f) = \mathcal{O}(\log \ell)$.

InT 5. Докажите, что $\mathrm{D}(\mathsf{CIS}_G) = \mathcal{O}\left(\log^2 n\right)$. Где x интерпретируется как характеристическая функция некоторой клики в графе G, а y — как характеристическая функция некоторого независимого множества в графе G. $\mathsf{CIS}(x, y) = 1$, если клика и независимое множество имеют общую вершину, обе стороны знают граф G.

Определение

Пусть $f\colon X \times Y \to Z$ и μ — распределение на $X \times Y$. Заметим, что для любого коммуникационного протокола Π для функции f распределение μ индуцирует распределение на листьях данного протокола естественным образом. **Внешней информационной стоимостью** (или **внешним информационным разглашением**) протокола Π по распределению μ будем называть величину:

$$\mathrm{IC}^{\mathrm{ext}}_{\mu}(\Pi) := I(\Pi(X, Y)\colon X, Y).$$

Также определим внешнюю информационную сложность самой функции $\mathrm{IC}^{\mathrm{ext}}_{\mu}(f) := \min_{\Pi} \mathrm{IC}^{\mathrm{ext}}_{\mu}(\Pi)$.
Внутренней информационной стоимостью протокола Π по распределению μ будем называть величину:

$$\mathrm{IC}^{\mathrm{ext}}_{\mu}(\Pi) := I(\Pi(X, Y)\colon X \mid Y) + I(\Pi(X, Y)\colon Y \mid X).$$

InT 6. Докажите, что для любой булевой функции f и любого распределения μ существует такой протокол Π для KW_f, что $\mathrm{IC}^{\mathrm{int}}_{\mu}(\Pi) \leq 2 \log n$.
Подсказка: попробуйте рассмотреть прокол, где Алиса пересылает Бобу биты входа до тех пор, пока они не найдут бит различия.

ІNТ 7. Определим функцию GT: $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ следующим образом: $\mathsf{GT}(x, y) = 1 \Leftrightarrow x \geq y$, где x, y мы воспринимаем как числа в битовой записи.
Докажите, что:

а) $\mathrm{R}^{\mathrm{pub}}_{\frac{1}{10}}(\mathsf{GT}) = \mathcal{O}\left(\log n \cdot \log\log n\right)$.

б) $\mathrm{R}^{\mathrm{pub}}_{\frac{1}{10}}(\mathsf{GT}) = \mathcal{O}\left(\log n\right)$.

2: Пункт б сложный, пункт а будет оцениваться отдельно. – **Dmitry**

Определение

Идеальная схема разделения секрета — это совершенная схема разделения секрета с дополнительным требованием «экономности».

$$\forall i \in \{1, 2, \ldots, n\},\ h(S_i) \leq h(S_0).$$

ІNТ 8. Рассмотрим задачу разделения секрета для следующей структуры доступа с 4 участниками: минимальными группами участников, знающих секрет, являются три пары

$$\{1,2\}, \{2,3\}, \{3,4\}.$$

Покажите, что:

а) $\mathrm{H}(S_2 \mid S_1, S_3) \geq \mathrm{H}(S_0)$;

б) $\mathrm{H}(S_3 \mid S_1) \geq \mathrm{H}(S_0)$;

в) $I(S_1 \colon S_3 \mid S_2) \geq \mathrm{H}(S_0)$;

г) $\max\limits_i \frac{\mathrm{H}(S_i)}{\mathrm{H}(S_0)} \geq \frac{3}{2}$.