Спектральный метод оценки выделяемости взаимной информации.

Колмогоровский семинар.

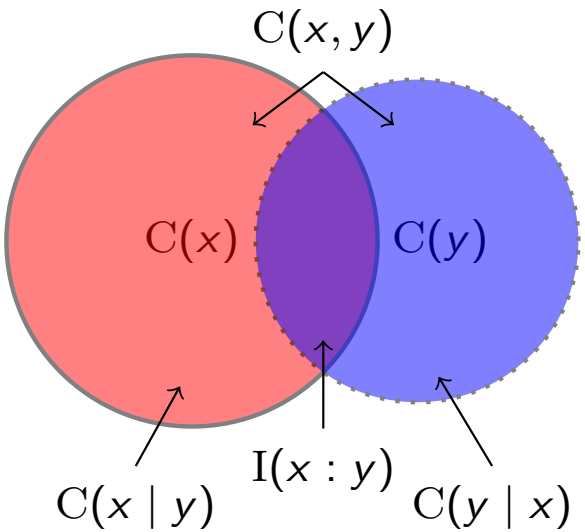
{06,08}.04.2020

Докладчик: Андрей Ромащенко

Credits:

- Ан. Мучник (начало 1990-х?)
- Верещагин–Шень–Чернов (конец 1990-х)
- Разенштейн (2011)
- Emirhan Gürpınar (прямо сейчас)

Колмогоровской профиль пары слов x, y



$\mathrm{C}(x)$ = длина кратч. прогр. получающей x.
$\mathrm{C}(x|y)$ = длина кратч. прогр. получающей x из y.

Взаимную информацию x и y можно определить как $\mathrm{I}(x : y) = \mathrm{C}(x) + \mathrm{C}(y) - \mathrm{C}(x, y)$.

Теорема Колмогорова–Левина:

$$\mathrm{I}(x : y) \approx \mathrm{C}(x) - \mathrm{C}(x \mid y),$$
$$\mathrm{I}(x : y) \approx \mathrm{C}(y) - \mathrm{C}(y \mid x)$$

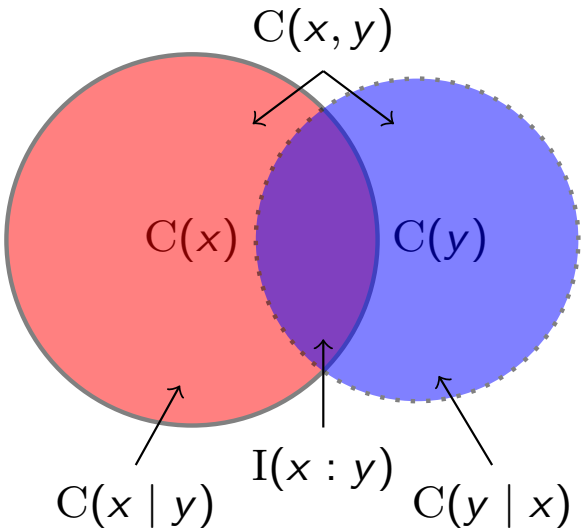
($\approx$ подразумевает $\pm O(\log |x| + |y|)$)

Профиль состоит из стандартных информационных величин:
$\mathrm{C}(x), \mathrm{C}(y), \mathrm{C}(x, y), \mathrm{C}(x|y), \mathrm{C}(y|x), \mathrm{I}(x : y)$

С точностью до $O(\log |x| + |y|)$ профиль определяется тремя координатами достаточно знать, e.g., $(\mathrm{C}(x), \mathrm{C}(y), \mathrm{C}(x, y))$ или $(\mathrm{C}(x|y), \mathrm{C}(y|x), \mathrm{I}(x : y))$

Для набора из $n > 2$ слов **профиль** определяется $2^n - 1$ координатой.

Сложностной профиль: первый (наивный) пример



$x = [a_1 \dots a_{\frac{n}{2}} b_1 \dots b_{\frac{n}{2}}]$

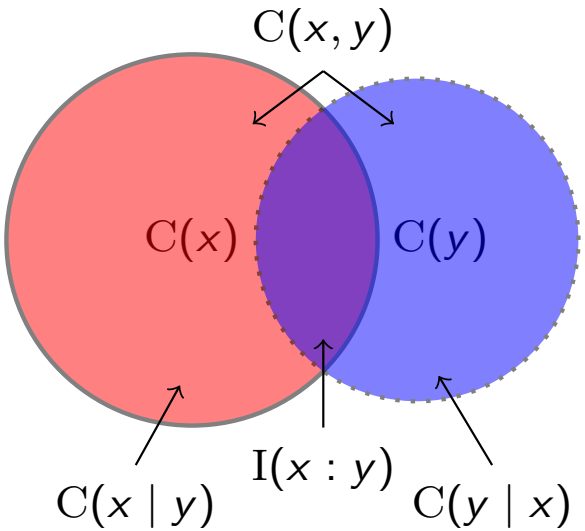
$y = [a_1 \dots a_{\frac{n}{2}} c_1 \dots c_{\frac{n}{2}}]$

(a_i, b_j, c_k – это биты, x и y – слова длины n)

Для типичных (x, y) указанного типа их профиль устроен следующим образом:

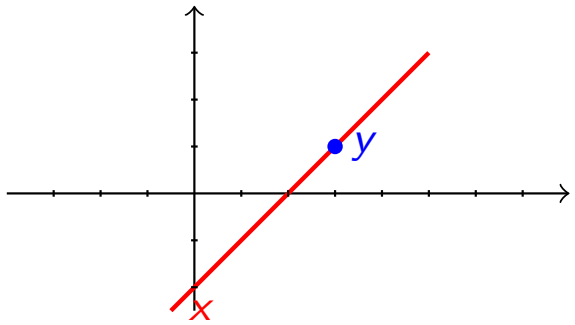
$$\begin{array}{rcl} \mathrm{C}(x) & \approx & n \\ \mathrm{C}(y) & \approx & n \\ \mathrm{C}(x, y) & \approx & 1.5n \\ \mathrm{C}(x|y) & \approx & 0.5n \\ \mathrm{C}(y|x) & \approx & 0.5n \\ \mathrm{I}(x : y) & \approx & 0.5n \end{array}$$

Сложностной профиль: второй пример



x представляет прямую на плоскости над конечным полем $\mathbb{F}_{2^{n/2}}$;

y представляет точку на этой прямой

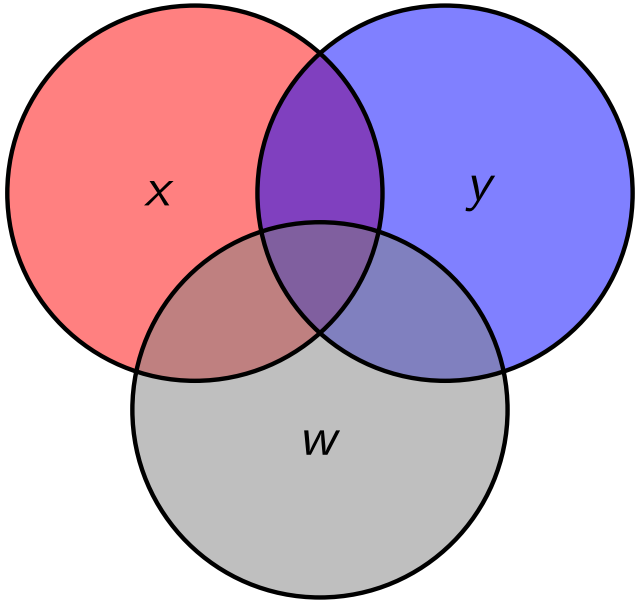


Для типичных (x, y) указанного типа их профиль устроен следующим образом:

$$
\begin{array}{rcl}
\mathrm{C}(x) & \approx & n \\
\mathrm{C}(y) & \approx & n \\
\mathrm{C}(x, y) & \approx & 1.5n \\
\mathrm{C}(x|y) & \approx & 0.5n \\
\mathrm{C}(y|x) & \approx & 0.5n \\
\mathrm{I}(x : y) & \approx & 0.5n
\end{array}
$$

Профиль расширений для пары (x, y)

Профилем расширений для пары (x, y) назовем класс все реализуемых профилей (x, y, w) для всевозможных w



Напомним обозначения:

$\mathrm{I}(x : y|w)$,
$\mathrm{I}(x : w|y)$,
$\mathrm{I}(y : w|x)$;

$\mathrm{I}(x : y : w)$

Профиль для тройки слов имеет 7 степеней свободы

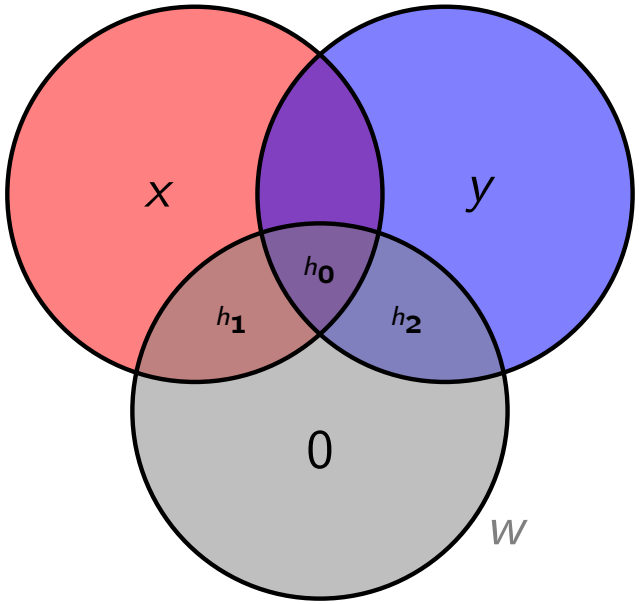
3 степени свободы уже фиксированы (профиль (x, y))

Остается 4 степени свободы, зависящие от w.

Бывает удобно наложить ограничение $\mathrm{C}(w|x, y) \approx 0$ и оставить профилю расширений 3 степени свободы.

Профиль расширений для log-**стохастических** (x, y)

Профиль расширений для пары (x, y) есть класс реализуемых профилей (x, y, w) для всевозможных w



Напомним обозначения:

$h_0 = \mathrm{I}(x : y : w),$
$h_1 = \mathrm{I}(x : w|y),$
$h_2 = \mathrm{I}(y : w|x)$

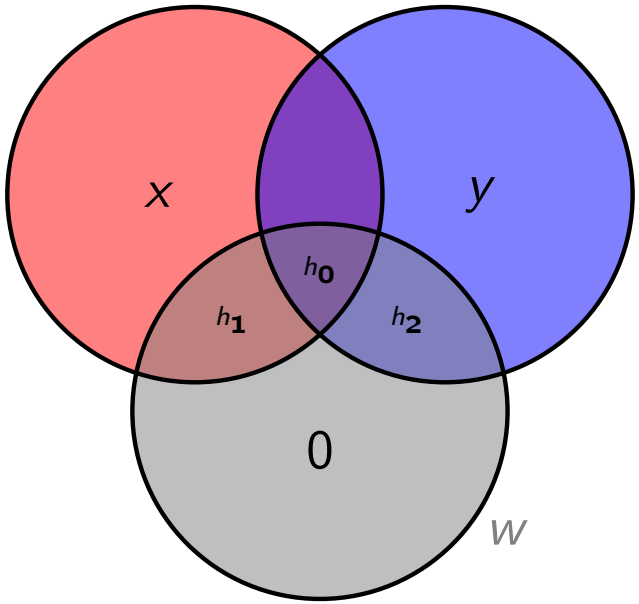
три степени свободы уже фиксированы (профиль (x, y))

б.о.о. можно положить $\mathrm{C}(w|x, y) \approx 0$

у профиля расширений остается 3 степени свободы.

Профиль расширений — специальный случай (1)

Профиль расширений для пары (x, y) есть класс реализуемых профилей (x, y, w) для всевозможных w



Напомним обозначения:

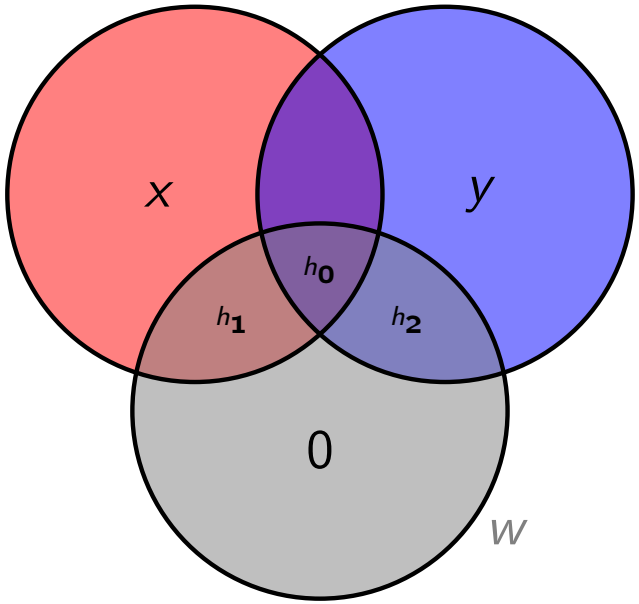
$h_0 = \mathrm{I}(x : y : w),$
$h_1 = \mathrm{I}(x : w|y),$
$h_2 = \mathrm{I}(y : w|x)$

У профиля расширений остается 3 степени свободы.

Информация Гача–Кёрнера: $h_1 \approx 0$ и $h_2 \approx 0$, $h_0 \to max$

Профиль расширений — специальный случай (2)

Профиль расширений для пары (x, y) есть класс реализуемых профилей (x, y, w) для всевозможных w



Напомним обозначения:

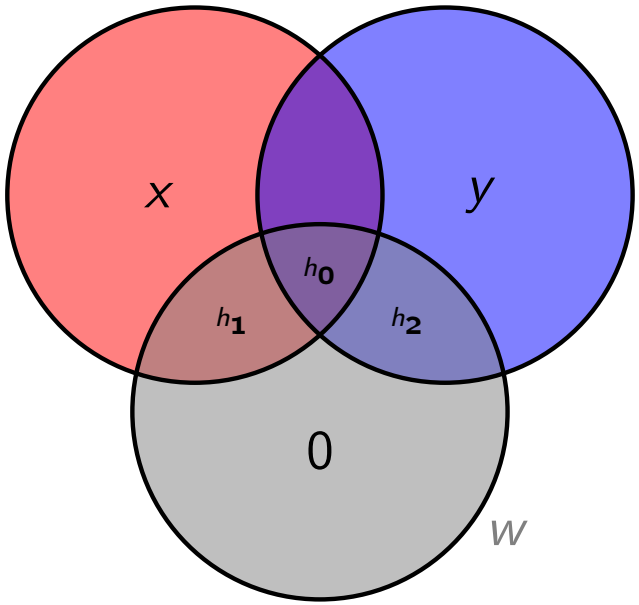
$h_0 = \mathrm{I}(x : y : w),$
$h_1 = \mathrm{I}(x : w|y),$
$h_2 = \mathrm{I}(y : w|x)$

У профиля расширений остается 3 степени свободы.

Информация Вайнера (Wyner): $h_0 \approx \mathrm{I}(x : y)$, $h_0 + h_1 + h_2 \to min$

Профиль расширений для (x, y) с фикс. профилем

Профиль расширений для (x, y) т.ч. $\mathrm{C}(x|y) = \mathrm{C}(y|x) = \mathrm{I}(x : y) = \frac{n}{2}$



Наивный пример:

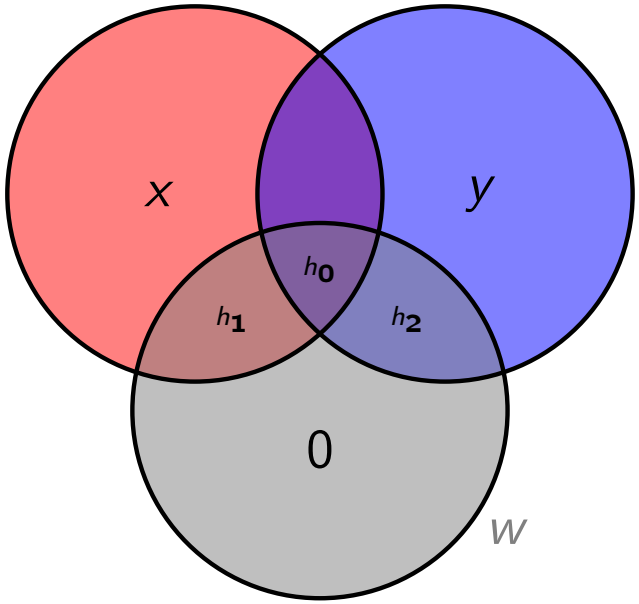
$x = [a_1 \ldots a_{\frac{n}{2}} b_1 \ldots b_{\frac{n}{2}}]$
$y = [a_1 \ldots a_{\frac{n}{2}} c_1 \ldots c_{\frac{n}{2}}]$

У наивного примера (x, y) самый «большой» возможный профиль расширений (можно показать, что разрешено всё, что не запрещено очевидными неравенствами)

$0 \le h_1 \le 0.5n$, $0 \le h_2 \le 0.5n$, $h_0 \le 0.5n$,
$0 \le h_0 + h_1 \le n$, $0 \le h_0 + h_2 \le n$,

Профиль расширений для (x, y) с фикс. профилем

Профиль расширений для (x, y) т.ч. $\mathrm{C}(x|y) = \mathrm{C}(y|x) = \mathrm{I}(x : y) = \frac{n}{2}$



Неконструктивный
«максимально плохой»
пример Мучника

и аналогичный
«почти конструктивный»
пример Разенштейна

У этой пары (x, y) самый «маленький» возможный профиль расширений

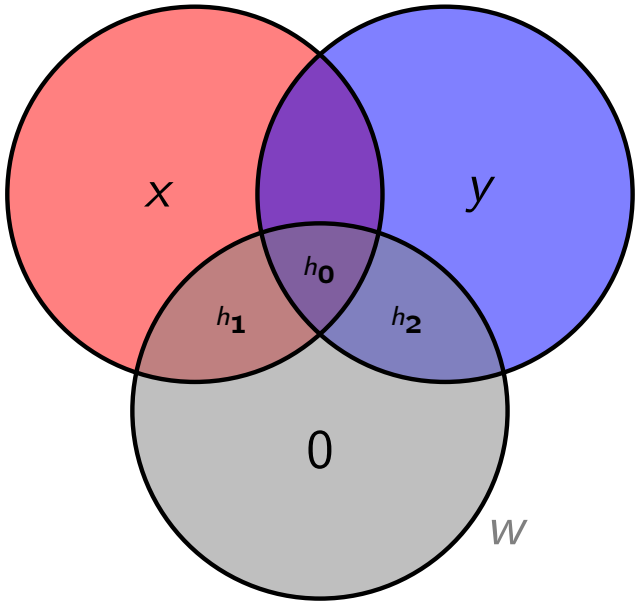
(можно показать, что запрещено всё, что не получается простыми конструкциями)

Кроме «минимально необходимых» условий оказывается необходимым, чтобы

$h_1 \geq 0.5n$ или $h_2 \geq 0.5n$ или $h_0 \leq 0$

Профиль расширений для (x, y) с фикс. профилем

Профиль расширений для (x, y) т.ч. $\mathrm{C}(x|y) = \mathrm{C}(y|x) = \mathrm{I}(x : y) = \frac{n}{2}$



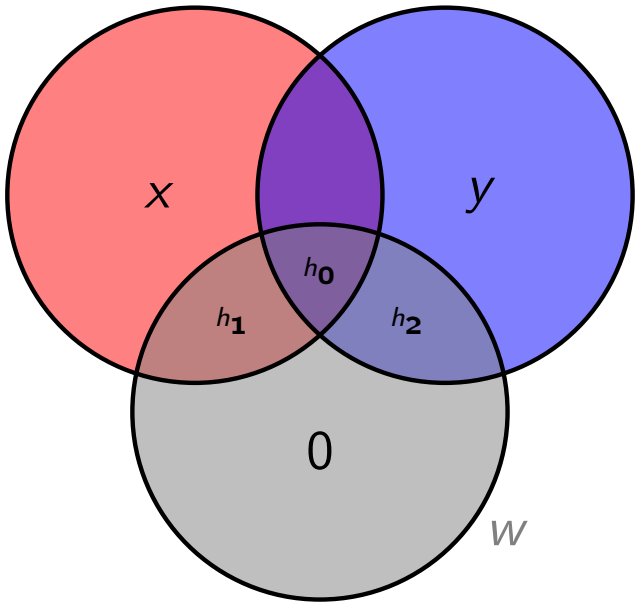
x есть прямая на плоскости
y есть точка на этой прямой
(над конечным полем $\mathbb{F}_{2^{n/2}}$)

Для этой пары (x, y) мы не знаем полного ответа,
но это скорее пример с «маленьким» профилем расширений.

Далее мы докажем некоторые нижние оценки (запреты) для этого профиля расширений, используя комбинаторные свойства отношения <точка, прямая>.

Профиль расширений для (x, y) с фикс. профилем

Профиль расширений для (x, y) т.ч. $\mathrm{C}(x|y) = \mathrm{C}(y|x) = \mathrm{I}(x : y) = \frac{n}{2}$



x есть прямая на плоскости
y есть точка на этой прямой
(над конечным полем $\mathbb{F}_{2^{n/2}}$)

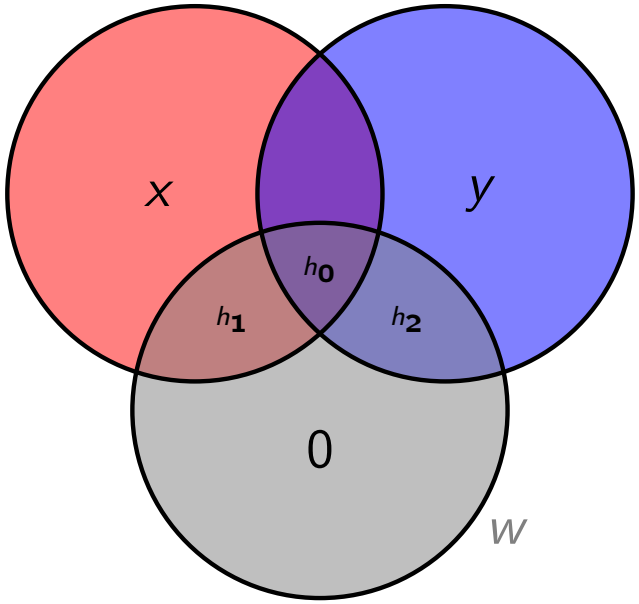
Докажем некоторые нижние оценки (запреты) для этого профиля расширений, используя комбинаторные свойства отношения <точка, прямая>.

1. две прямые пересекаются в одной точке $\Longrightarrow \mathrm{I}(x : y|w) \geq \frac{1}{2} \min\{\mathrm{C}(x|w), \mathrm{C}(y|w)\}$

т.е., $\frac{1}{2} h_0 \leq \max\{h_1, h_2\}$

Профиль расширений для (x, y) с фикс. профилем

Профиль расширений для (x, y) т.ч. $\mathrm{C}(x|y) = \mathrm{C}(y|x) = \mathrm{I}(x : y) = \frac{n}{2}$



x есть прямая на плоскости
y есть точка на этой прямой
(над конечным полем $\mathbb{F}_{2^{n/2}}$)

Докажем некоторые нижние оценки (запреты) для этого профиля расширений, используя спектральные свойства графа <точка, прямая>.

2. большой спектральный зазор $\Longrightarrow$

если $\mathrm{C}(x|w) + \mathrm{C}(y|w) > 1.5n$, то $\mathrm{I}(x : y|w) \geq 0.5n$

т.е., если $h_1 + h_2 + 2h_0 < 0.5n$, то $h_0 \leq 0.5n$

Информационный профиль и комбинаторика графа

Наша задача: изучить профиль расширений (x, y)

Удобные сейчас координаты: $\mathrm{C}(x|w)$, $\mathrm{C}(y|w)$, $\mathrm{C}(x, y|w)$

Стандартный прием: рассмотрим двудольный граф $G = (L \cup R, E)$ где $L = R = \{0,1\}^n$ и E есть множество пар (x', y') *аналогичных* нашим (x, y)

$A_w := \{x' \in L : \mathrm{C}(x'|w) \leq \mathrm{C}(x|w)\}$
$B_w := \{y' \in R : \mathrm{C}(y'|w) \leq \mathrm{C}(y|w)\}$

Предложение 1. $|A_w| = 2^{\mathrm{C}(x|w)+O(\log n)}$ и $|B_w| = 2^{\mathrm{C}(y|w)+O(\log n)}$

Предложение 2. $\mathrm{C}(x, y|w) \leq \log |E(A_w, B_w)| + O(\log n)$

Мораль: полезно научиться оценивать $|E(A, B)|$ в терминах $|A|$ и $|B|$.

Информационный профиль и комбинаторика графа

Первая оценка, см. [CMRSV2002]:

Две прямые пересекаются в одной точке (в графе запрещены циклы длины 4)

$$\Downarrow$$

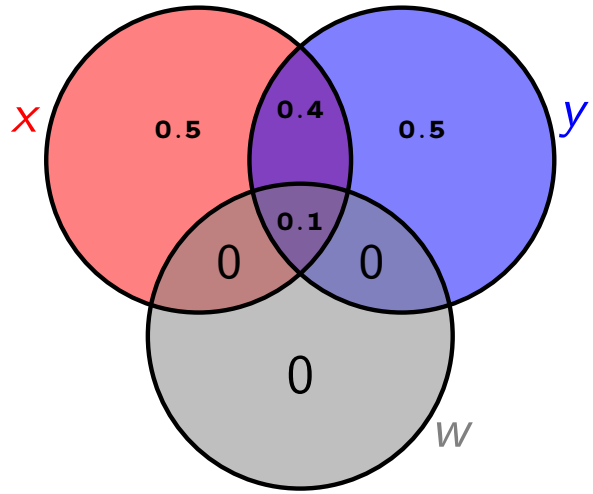
$$\mathrm{I}(x : y|w) \geq \tfrac{1}{2} \min\{\mathrm{C}(x|w), \mathrm{C}(y|w)\}$$

В терминах графов:

$$|E(A, B)| \leq \max\{O(\sqrt{|A|} \cdot |B|), O(|A| \cdot \sqrt{|B|})\}$$

[техника: неравенство Коши–Буняковского или ф-ла включений-исключений]

Пример **запрещенного** профиля:



Информационный профиль и комбинаторика графа

Вторая оценка: спектральная техника

Первое собственное число $= D = 2^{0.5n}$, второе собственное число $= \sqrt{D}$

$$\Downarrow$$

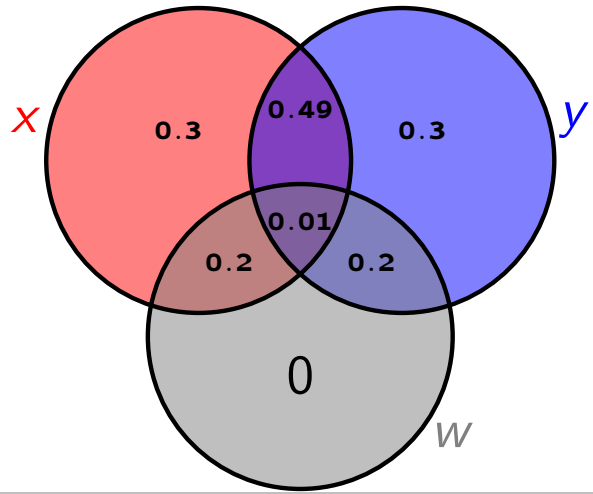
если $\mathrm{C}(x|w) + \mathrm{C}(y|w) > 1.5n$, то $\mathrm{I}(x : y|w) \geq 0.5n$

В терминах графов:

$|E(A,B)| \leq \frac{D \cdot |A| \cdot |B|}{N} + \lambda_2 \cdot \sqrt{|A| \cdot |B|}$ (expander mixing lemma)

т.о., если $|A| \cdot |B| \geq N^2/D$, то $|E(A,B)| \leq O\left(\frac{D \cdot |A| \cdot |B|}{N}\right)$

Пример **запрещенного** профиля:



R.-Zimand [2018, 2019]

Secret key agreement protocol:

- Alice knows x
- Bob knows y
- they exchange messages and compute a shared secret key z
- z must look random for the adversary
  (i.e., be random conditioned by the transcript of the protocol)

Our setting:

(1) Alice and Bob also know how their x and y are correlated.
Technically, they know the complexity profile of x and y : $(\mathrm{C}(x), \mathrm{C}(y), \mathrm{C}(x,y))$.

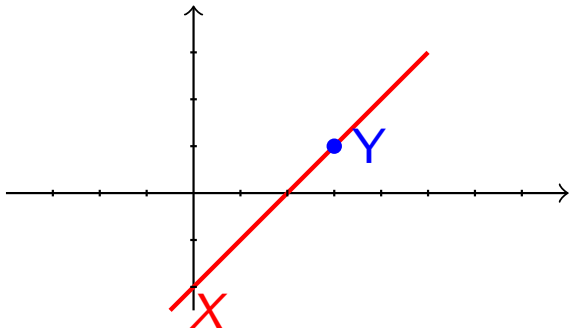
(2) Alice and Bob use randomized algorithms to compute their messages.

Theorem (Characterization of the mutual information)

1. *There is a protocol that for every n-bit strings x and y allows to compute with high probability a shared secret key of length $\approx \mathrm{I}(x : y)$.*
2. *No protocol can produce a longer shared secret key.*

Secret key agreement protocol: simple example

- - Alice knows line X in the plane: $\mathcal{X}(t) = a_1 t + a_0$;
  - Bob knows point Y in the plane: (b_1, b_2);
  - the line and the point are incident
- X : n bits of information (intercept, slope in $\mathbb{F}_{2^{0.5n}}$).
- Y: n bits of information (the 2 coord. in $\mathbb{F}_{2^{0.5n}}$).
- mutual information: $0.5n$ bits.
- Alice and Bob want to agree on a secret key of size $0.5n$. They communicate via a public channel.



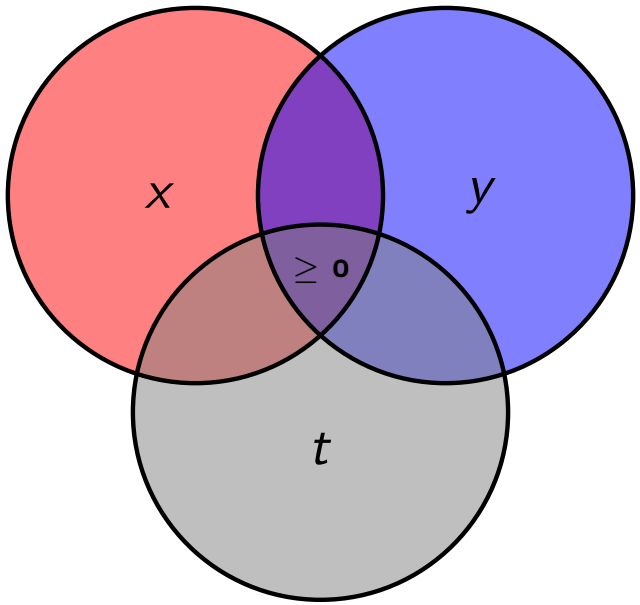
Ad hoc solution:

- Alice sends a_1 to Bob.
- Bob, knowing that $Y \in X$, finds X.
- Alice and Bob use a_0 as a secret key.
- It works! The adversary has seen a_1, but a_1 and a_0 are independent.

Communication complexity: $0.5n$. **Оптимальна ли эта оценка? Да!**

Нижняя оценка на коммуникационную сложность (1)

Старая лемма [Kaced-R.-Верещагин, R.-Zimand]: для транскрипта коммуникационного протокола $t = t(x, y)$ выполнено $\mathrm{I}(x : y : t) \geq 0$



Новая лемма: б.о.о. можно считать, что $\mathrm{I}(x : y : t) = 0$.

Идея доказательства:
Старая лемма + «сжатие» транскрипта с помощью теоремы Мучника

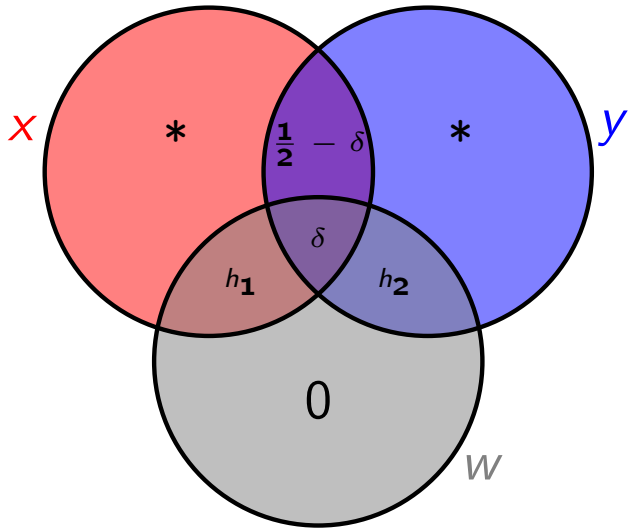
Нижняя оценка на коммуникационную сложность (2)

Теорема: для транскрипта коммуникационного протокола secret key agreement выполнено $\mathrm{C}(t) \geq 0.499n$

Шаг 1 (странный): б.о.о. секретный можно считать ключ маленьким, e.g., $\mathrm{C}(z) = \delta n = 0.0001n$

Шаг 2 (технический): б.о.о. $\mathrm{I}(x : y : t) = 0$

Шаг 3 (спектральный): $w := \langle z, t \rangle$ (объединили секрет и транскрипт)



Спектральная оценка: профиль запрещен, если $h_1 + h_2 + 2\delta < 0.5$

Нижняя оценка на коммуникационную сложность (3)

Заключительное замечание: рассуждение обобщается на случай, когда Алиса и Боб используют приватные случайные биты.

В терминах колмогоровской сложности: мы присоединяем к исходным x и y (точка и прямая) независимые случайные r_{Alice} и r_{Bob} соответственно и изучаем **профиль расширений** новой пары $(x \cdot r_{\mathrm{Alice}}, y \cdot r_{\mathrm{Bob}})$.

В терминах графов: мы тензорно умножаем исходный граф (для точек и прямых) на полный двудольный граф.

Коммуникационная сложность задачи о секретном ключе остается $\frac{n}{2}$. Новых идей не требуется, но подсчеты становятся более громоздкими.