Теория кодирования

МФТИ, осень 2013

Александр Дайняк

www.dainiak.com

Граф канала

Можно задать модель канала графом, вершины которого — символы алфавита канала.

Дуга идёт из x в y, если в канале возможна ошибка замещения x на y.

Если в канале для каждой пары символов (x, y) возможны либо оба замещения $x \to y$, $y \to x$, либо ни одно из них, то граф канала можно считать неориентированным.

Граф канала

Пример: если алфавит канала $\{0,1,2\}$, и возможны только замещения $0 \to 1$ и $1 \to 2$, то граф такой:

$$0 \longrightarrow 1 \longrightarrow 2$$

Если возможны замещения $0 \to 1,\ 1 \to 0,\ 1 \to 2$ и $2 \to 1$, то граф такой:

$$0 \;\text{———}\; 1 \;\text{———}\; 2$$

Граф канала

Пусть G — граф канала.

Если считать каждый символ канала отдельным сообщением, то во избежание ошибок придётся использовать множество символов C_1, являющееся *независимым множеством* в G:

$$\underline{\mathbf{0}} \;\text{———}\; 1 \;\text{———}\; \underline{\mathbf{2}}$$

При этом в лучшем случае пропускная способность канала получается такой же, как у канала без ошибок, алфавит которого имеет мощность $\alpha(G)$.

Граф канала

Пусть $G = (V, E)$ — граф канала.

Если по каналу мы посылаем пары символов, то следует выбирать для использования такое множество пар C_2, чтобы

$$\nexists (x', y'), (x'', y'') \in C_2:$$
$$\big((x' = x'' \lor x'x'' \in E) \land (y' = y'' \lor y'y'' \in E)\big)$$

Если мы рассмотрим такое C_2, имеющее максимально возможную мощность, то данный код позволяет достичь пропускной способности $\sqrt{|C_2|}$.

Граф канала

Замечание. В чём смысл извлечения квадратного корня из $|C_2|$:

Это скорость передачи данных в канале в расчёте на один передаваемый символ.

Если бы у нас был *безошибочный* канал, в алфавите которого ровно $\sqrt{|C_2|}$ символов, то мы могли бы передавать по нему как раз $|C_2|$ сообщений длины 2.

Граф канала

Если G — граф канала, и мы посылаем тройки символов, то следует выбирать такое множество троек C_3, чтобы в нём не было двух троек, соответствующие компоненты которых совпадают или образуют ребро в G.

Если мы рассмотрим такое C_3, имеющее максимально возможную мощность, то данный код позволит достичь пропускной способности $\sqrt[3]{|C_3|}$.

И так далее…

Шенноновское произведение

Шенноновское произведение графов G *и* H — это граф $G \times H$ со множеством вершин

$$V(G \times H) = \{(x, y) \mid x \in V(G), y \in V(H)\}$$

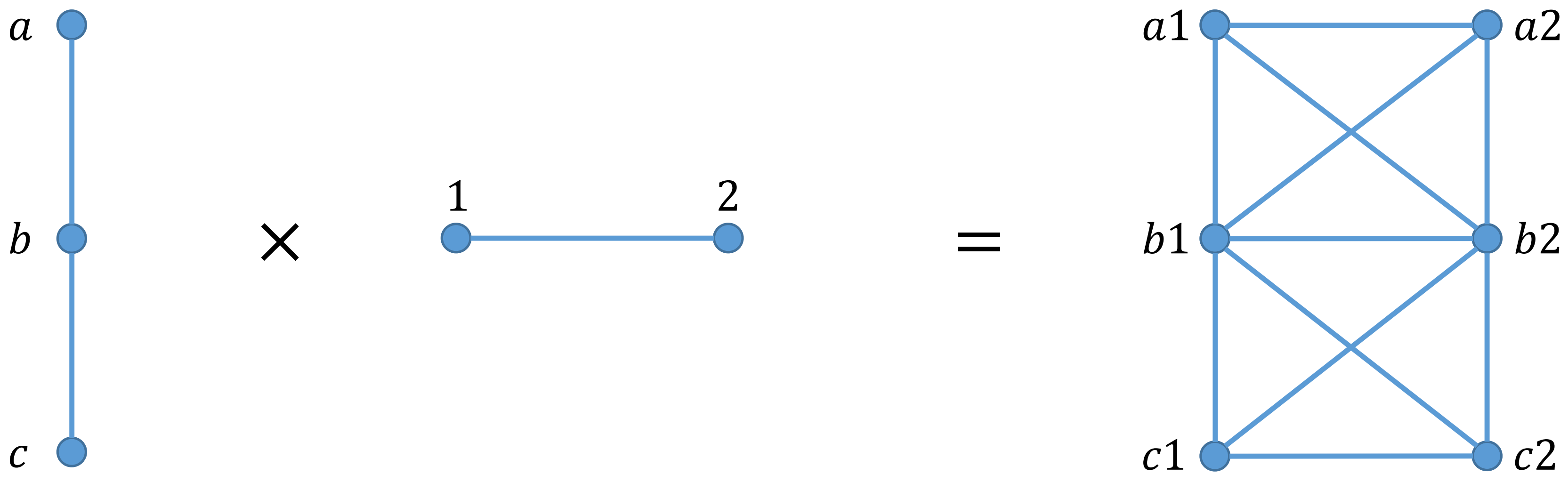
Рёбра в $G \times H$ между парами (x', y') и (x'', y''), для которых

$$\left(x' = x'' \vee x'x'' \in E(G)\right) \wedge \left(y' = y'' \vee y'y'' \in E(H)\right)$$

Очевидно, $(G_1 \times G_2) \times G_3 \simeq G_1 \times (G_2 \times G_3)$ и $G_1 \times G_2 \simeq G_2 \times G_1$ для любых G_1, G_2, G_3.

Шенноновское произведение

Пример:



Шенноновская ёмкость

Шенноновская ёмкость графа G:

$$\operatorname{cap}(G) = \sup_{n \in \mathbb{N}} \sqrt[n]{\alpha(\underbrace{G \times G \times \cdots \times G}_{n \text{ раз}})}$$

Это наибольшая возможная (в пределе) «скорость», с которой можно передавать без ошибок данные по каналу, моделью которого является граф G.

Верхняя оценка шенноновской ёмкости графа

Пусть G — произвольный граф.
Будем рассматривать наборы весов $\boldsymbol{w}$ на вершинах графа G, такие, что

- $\forall x \;\; w(x) \geq 0$
- $\sum_{x \in V(G)} w(x) = 1$

Для любого множества $A \subseteq G$ обозначим

$$w(A) \coloneqq \sum_{x \in A} w(x)$$

Верхняя оценка шенноновской ёмкости графа

Для произвольного графа G рассмотрим величину

$$\nu(G) \coloneqq \min_{\boldsymbol{w}} \max_{\substack{K-\text{клика} \\ \text{в } G}} w(K)$$

(ясно, что $\max$ достаточно брать только по *максимальным по включению* кликам)

Теорема Шеннона о верхней оценке ёмкости:
Для любого G справедливо неравенство

$$\operatorname{cap}(G) \leq \left(\nu(G)\right)^{-1}$$

Доказательство верхней оценки шенноновской ёмкости графа

Докажем, что $\sqrt[n]{\alpha(G^n)} \le \big(\nu(G)\big)^{-1}$ для каждого n.

Пусть $A \subseteq V(G)$ — независимое множество размера $\alpha(G)$.

Рассмотрим набор весов $\boldsymbol{w}_0$, в котором

- $w_0(x) \coloneqq 0$, если $x \notin A$,
- $w_0(x) \coloneqq \big(\alpha(G)\big)^{-1}$, если $x \in A$.

Для таких весов получим

$$\nu(G) \le \max_{\substack{K-\text{клика} \\ \text{в } G}} w_0(K) = \big(\alpha(G)\big)^{-1}$$

откуда $\alpha(G) \le \big(\nu(G)\big)^{-1}$.

Доказательство верхней оценки шенноновской ёмкости графа

Итак, $\nu(G) \leq \left(\alpha(G)\right)^{-1}$ для любого G.

Лемма. Для любых графов G, H выполнено

$$\nu(G \times H) = \nu(G) \cdot \nu(H)$$

Если докажем лемму, то докажем и теорему:

$$\nu(G^n) = \left(\nu(G)\right)^n \quad \Rightarrow \quad \sqrt[n]{\alpha(G^n)} \leq \sqrt[n]{\left(\nu(G^n)\right)^{-1}} = \left(\nu(G)\right)^{-1}$$

Доказательство верхней оценки шенноновской ёмкости графа

Лемма. Для любых графов G, H выполнено

$$\nu(G \times H) = \nu(G) \cdot \nu(H)$$

Доказательство леммы:

Пусть $\boldsymbol{w}_G^*$ и $\boldsymbol{w}_H^*$ — наборы весов на вершинах графов G и H, на которых достигаются минимумы в $\nu(G)$ и $\nu(H)$.

Рассмотрим набор весов $\widehat{\boldsymbol{w}}_{G\times H}$ на вершинах графа $G \times H$, такой, что

$$\widehat{w}_{G\times H}(x, y) \coloneqq w_G^*(x) \cdot w_H^*(y)$$

Доказательство верхней оценки шенноновской ёмкости графа

Берём набор весов $\widehat{w}_{G\times H}(x,y) \coloneqq w_G^*(x)\cdot w_H^*(y)$.

Любая максимальная по включению клика K в графе $G\times H$ является множеством пар вида

$$\{(x,y) \mid x\in K_G, y\in K_H\}$$

где K_G и K_H — клики в G и H соответственно. Для таких клик K имеем

$$\widehat{w}_{G\times H}(K) = \sum_{(x,y)\in K} w_G^*(x)\cdot w_H^*(y) = \left(\sum_{x\in K_G} w_G^*(x)\right)\left(\sum_{y\in K_H} w_H^*(y)\right) =$$
$$= w_G^*(K_G)\cdot w_H^*(K_H)$$

Доказательство верхней оценки шенноновской ёмкости графа

Имеем

$$\nu(G \times H) = \min_{\boldsymbol{w}} \max_{\substack{K-\text{клика} \\ \text{в } G\times H}} w(K) \leq$$

$$\leq \max_{\substack{K-\text{клика} \\ \text{в } G\times H}} \widehat{w}_{G\times H}(K) = \max_{\substack{K-\text{клика} \\ \text{в } G\times H}} w_G^*(K_G) \cdot w_H^*(K_H) \leq$$

$$\leq \max_{\substack{K-\text{клика} \\ \text{в } G}} w_G^*(K) \cdot \max_{\substack{K-\text{клика} \\ \text{в } H}} w_H^*(K) = \nu(G) \cdot \nu(H)$$

В итоге, $\nu(G \times H) \leq \nu(G) \cdot \nu(H)$.

Доказательство верхней оценки шенноновской ёмкости графа

Обозначим через $\widetilde{\boldsymbol{w}}$ набор весов на кликах графа (неотрицательны, сумма равна единице).

По теореме о свойствах двойственных задач линейного программирования, для любого графа имеет место равенство

$$\min_{\boldsymbol{w}} \max_{K} \sum_{x \in K} w(x) = \max_{\widetilde{\boldsymbol{w}}} \min_{x} \sum_{K \ni x} \widetilde{w}(K)$$

Доказательство верхней оценки шенноновской ёмкости графа

$$\max_{\widetilde{\boldsymbol{w}}} \min_{x} \sum_{K \ni x} \widetilde{w}(K)$$

Пусть $\widetilde{\boldsymbol{w}}_G^*$ и $\widetilde{\boldsymbol{w}}_H^*$ — наборы весов, на которых достигается $\max$ для графов G и H.

Построим набор весов $\widetilde{w}_{G\times H}$ на кликах графа $G \times H$:

- Пусть клика K может быть представлена в виде $K_G \times K_H$, где K_G и K_H — клики в G и H. Тогда полагаем $\widetilde{w}_{G\times H}(K) \coloneqq \widetilde{w}_G^*(K_G) \cdot \widetilde{w}_H^*(K_H)$.
- Для остальных клик K полагаем $\widetilde{w}_{G\times H}(K) \coloneqq 0$.

Доказательство верхней оценки шенноновской ёмкости графа

Для такого набора весов и для любой фиксированной вершины $(x, y) \in V(G \times H)$ имеем

$$\sum_{K \ni (x,y)} \widetilde{w}_{G\times H}(K) \geq \sum_{\substack{K \ni (x,y) \\ \exists K_G, K_H :\, K = K_G \times K_H}} \widetilde{w}_{G\times H}(K) = \sum_{\substack{K_G \ni x, \\ K_H \ni y}} \widetilde{w}_G^*(K_G) \cdot \widetilde{w}_H^*(K_H) =$$

$$= \left(\sum_{K_G \ni x} \widetilde{w}_G^*(K_G)\right)\left(\sum_{K_H \ni y} \widetilde{w}_H^*(K_H)\right) \geq \nu(G) \cdot \nu(H)$$

Отсюда следует неравенство $\nu(G \times H) \geq \nu(G) \cdot \nu(H)$, а значит верно равенство $\nu(G \times H) = \nu(G) \cdot \nu(H)$.

Пример применения теоремы

Оценим шенноновскую ёмкость цепи на трёх вершинах. Рассмотрим набор весов на вершинах графа P_3, на котором достигается минимум.

Пусть веса на крайних вершинах цепи равны x и z, а у средней вершины вес равен y. Получаем задачу линейного программирования:

$$\begin{cases} x, y, z \geq 0 \\ x + y + z = 1 \\ x + y \leq \nu \\ y + z \leq \nu \\ \nu \to \min \end{cases}$$

Решение этой задачи: $x = z = 1/2\,, y = 0$ и $\nu = 1/2$. Отсюда $\operatorname{cap} P_3 \leq 2$.

При этом очевидны соотношения $\operatorname{cap} P_3 \geq \alpha(P_3) = 2$, а значит $\operatorname{cap} P_3 = 2$.