Лекция №14. Коды с малой плотностью проверки на чётность

Tuesday 1 December 2020 11:53

(Low-density parity check codes, LDPC)

802.3 Ethernet

802.11 Wireless Lan

I Мотивация: улучшить алг-м декодирования, а не min. расстояние.

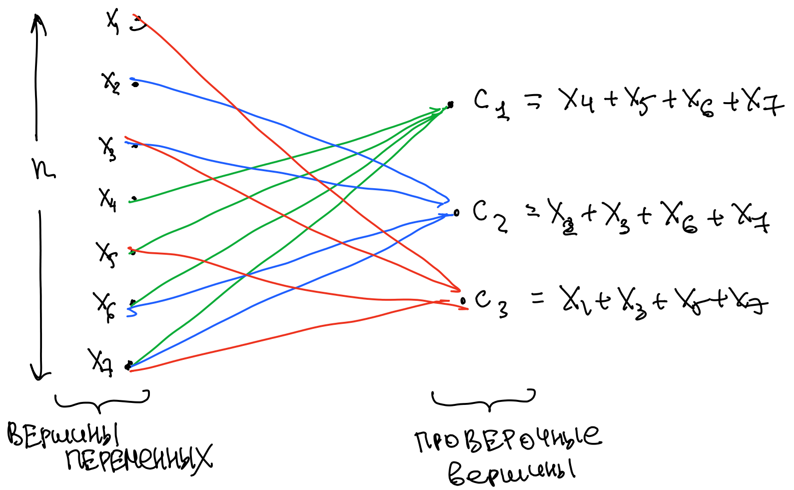
LDPC код - код на графах.

Любой лин. код может быть представлен в виде двудольного графа, т.е. графа, мн-во вершин которого можно разбить на два мн-ва U, V, т.ч. рёбра графа соединяют вершины из U только с вершинами из V.

Пример: $[7,4,3]_2$ - код Хэмминга

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} x_4 + x_5 + x_6 + x_7 \\ x_2 + x_3 + x_6 + x_7 \\ x_1 + x_3 + x_5 + x_7 \end{bmatrix}$$

Двудольный граф $[7,4,3]_2$:



Коды LDPC соответствуют "разряженным" графам, т.е. графам с малым кол-вом рёбер; экв.-но проверочная матрица H LDPC кода содержит число 1-ц в каждой строке $\ll n$, число 1-ц в каждом столбце $\ll n-k$.

Код LDPC называется <u>регулярным</u>, если его граф является регулярным, т.е. степени вершин x_i равны N/g собой и степени проверочных вершин c_j равны M/g собой. (Код Хэмминга не явл. регулярным);

II Жёсткое декодирование LDPC кодов

(метод вероятностного итеративного декодирования)

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$n = 8$ $\qquad y = [0\ 1\ 0\ 0\ 1\ 0\ 0\ 1]$

Раунд 1

[0 0 0]	$c_1\,c_2\,c_3$ [1 1 0]	x_1	$\boxed{0}$
[1 1 1]	$c_4\,c_5\,c_6$ [1 0 1]	x_2	$\boxed{1}$
[0 0 0]	$c_2\,c_3\,c_6$ [1 0 0]	x_3	$\boxed{0}$
[0 0 0]	$c_1\,c_3\,c_4$ [1 0 0]	x_4	$\boxed{0}$
[0 0 0]	$c_1\,c_2\,c_5$ [0 0 0]	x_5	$\boxed{1}$ ← ошибка
[0 0 0]	$c_1\,c_2\,c_3$ [1 1 0]	x_6	$\boxed{0}$
[0 0 0]	$c_4\,c_5\,c_6$ [0 1 0]	x_7	$\boxed{0}$
[1 1 1]	$c_4\,c_5\,c_6$ [1 0 1]	x_8	$\boxed{1}$

Раунд 2

- $c_1 = x_1 + x_4 + x_5 + x_6$ (0 0 1 0) → 0 0 0 0 ← 0 mod 2
- $c_2 = x_1 + x_3 + x_5 + x_6$ (0 0 1 0) → 0 0 0 0
- $c_3 = x_1 + x_3 + x_4 + x_6$ (0 0 0 0) → 1 0 0 1
- $c_4 = x_2 + x_4 + x_7 + x_8$ (1 0 0 1) → 1 0 0 1
- $c_5 = x_2 + x_5 + x_7 + x_8$ (1 1 0 1) → 1 0 0 1
- $c_6 = x_2 + x_3 + x_7 + x_8$ (1 0 0 1) → 1 0 0 1

Алгоритм:

I Раунд 0

1. Вершины x_i получают значения y_i; x_i посылает y_i смежным вершинам c_j.

II Раунд i:

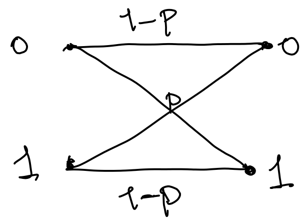
1. Для всех c: вершина c посылает смежному x сумму всех полученных y_j (mod 2) за исключением бита y, полученного от x (экв. c посылает x_i полученный от x_i бит, если $\sum x_i$ имеет зн-ие 0, обратный бит, если 1)
2. Для всех x: вершина x посылает смежному

c бит $\underline{b}$, если x получил $\underline{b}$ ото всех вершин, кроме c.
иначе (если хотя бы одно значение не совпадает), x посылает полученный бит от y

$\underline{\text{III}}$ шаг II пока все проверочные условия не будут удовлетворены

$\underline{\text{III}}$ Анализ LDPC кодов состоит в вычислении вероятности ошибки, т.е. передачи неверного бита от $\underline{x}$ к $\underline{c}$ и обратно в раунде $\underline{i}$.

Модель канала коммуникаций
(бинарный симметричный канал)



$p \in [0,1]$ – вероятность ошибки.

Положим, исходное кодовое слово было нулевым ($c = 0$)
т.е. "ошибка" = передан бит "1".

Вершины x_i получат 0 с в-тью $1-p$
1 — // — p

обозначим за p_i – вероятность передачи от $\underline{\underline{x}}$ к $\underline{\underline{c}}$ "1" в раунде i

$p_0 = p$

q_i – —————— // ——— $\underline{\underline{c}}$ к $\underline{\underline{x}}$ "1" — // —

положим, что $\deg(x) = d$, $\deg(c) = e$

1) выразим p_{i+1} через p_i (для фикс. x и c)

$Pr[x \xrightarrow{"1"} c]$: 1. $Pr[y = 1 \wedge$ хотя бы одно значение, полученное $x = 1$ ото всех смежных вершин, кроме c]

$= p \cdot (1 - Pr[\overbrace{\text{все смежные к } x \text{ вершины}}^{\text{всего } d-1}$ отправили "0"])

$= p \cdot (1 - (1-q_i)^{d-1})$

2. $Pr[y = 0 \wedge$ все значения, полученные x ото всех смежных вершин, кроме c, = "1"]

$$= (1-p)\cdot (q_i)^{d-1}$$

$$p_{i+1} = p\left(1-(1-q_i)^{d-1}\right) + (1-p)\, q_i^{d-1} \qquad (1)$$

оценим q_i для фикс. c и x.

$$q_i = 1 \iff \sum_{\substack{X_j - \text{смежные с } C \\ X_j \neq X}} X_j = 1 \mod 2$$

<u>Лемма</u> Положим, X_j – независ. случ. величины $\in \{0,1\}$ т.ч. $Pr[X_j=1]=p$.
Тогда $$Pr\left[\sum_{j=1}^{e-1} X_j \mod 2 = 1\right] = \frac{1-(1-2p)^{e-1}}{2}$$

(док-во с помощью мат. индукции).

(1) + Лемма:

$$\boxed{p_{i+1} = p\left(1 - \left[\frac{1+(1-2p_i)^{e-1}}{2}\right]^{d-1}\right) + (1-p)\left[\frac{1-(1-2p_i)^{e-1}}{2}\right]^{d-1}} \qquad (*)$$

Т.о., зная исходный пар-р канала связи p и пар-ры кода d, e, мы можем опр-ть:

1) является ли $(*)$ монотонно убывающей ф-цией
2) для какого значения i, p_i близко к 0.

<u>Замечание</u> Мажоритарное декодирование: вершина X решает об изменении бита $\square$ с помощью мажоритарного голосования.

<u>Пример:</u>

$[1, 0] \overset{X}{\cdot} [0] \implies Maj(1,0,0) = 0$