ДЗ 1. Основные понятия. Спасение из пиратского плена

Условие

Пираты захватили судно с экипажем из $n = 2^m - 1$ человека. Отчаявшись получить выкуп, они приняли решение избавиться от заложников. Главарь пиратов сгенерировал n независимых двоичных равномерно распределенных случайных значений x_i. Заложники размещаются в одиночных камерах. Главарь сообщает i-ому заложнику значения $x_j, j \neq i$ вместе с их номерами j и предлагает угадать значение x_i. Заложник может дать ответы 0,1 и "не знаю". В том случае, если все заложники дают ответ "не знаю" или любой из них оглашает неправильное значение x_i, всех заложников казнят. В противном случае все заложники будут освобождены. После оглашения условий этой игры, но до распределения заложников по камерам и выдачи значений x_j, заложникам разрешается встретиться и выработать стратегию действий.

Необходимо:

- Предложить стратегию действий заложников, максимизирующую вероятность их спасения.
- Оценить кровожадность пиратов, т.е. вероятность казни заложников при использовании ими предложенной стратегии.

Тривиальная стратегия.

Для начала рассмотрим стратегию, которая приходит на ум сразу же. Пусть экипаж (далее - игроки) выберет человека, который всегда будет давать ответ, а все остальные игроки воздержатся от ответа. Очевидно, что такая стратегия выигрышна в 50% случаев. Однако в таком подходе мы не используем всю информацию, данную нам из условия.

Будем описывать состояние игры (т.е. любой момент времени во время игры) как число с $2^m - 1$ бит, где каждый бит - сгенерированное для игрока число. Представим себя на месте игрока: мы знаем сгенерированные числа для всех, кроме себя. Значит, мы знаем $2^m - 2$ бит числа. Из правил игры мы знаем, что игроки могут заранее договориться о своем последовательном порядке. Следовательно, мы также знаем индекс нашего неизвестного бита. Если бы мы могли каким-либо образом использовать все остальные биты, чтобы

определить наш, мы могли бы правильно ответить и выиграть игру. И на этом этапе нам помогут коды Хемминга.

Коды Хемминга

Будем использовать матричный подход, т.е. задание кодов с помощью порождающих или проверочных матриц, что позволит использовать нам преобразования из линейной алгебры. Мы будем работать с векторами над полем $\mathbb{F}_2$, т.е. над целыми числами по модулю 2.

Таблица с результатами операций над битами по модулю 2:

x	y	$x + y$	$x * y$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Наш код Хемминга будет использовать $n = 2^m - 1$ битные слова и кодировать $n - m$ бит данных, он будет давать возможность исправить ошибку в произвольном 1 бите.

Наше множество кодов Хемминга объявим как:

$$C = \{c \in \{0,1\}^n \mid H_{m,n}c = 0\},$$

где $H_{r,n}$ это $m \times n$ матрица, в которой i-я колонка обозначает m-й бит двоичной записи числа i.

▼ **Пример:**

Для $m = 3,\ n = 7$ матрица будет иметь вид:

$$H_{3,7} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Будем называть матрицу H проверочной, поскольку для заданного не кодового слова z (т.е. $Hz \neq 0$), Hz будет являться двоичной записью номера позиции “ошибки” в z. В таком случае, если мы инвертируем бит Hz в z, получившийся результат будет кодовым словом.

▼ **Пример:**

Например:

$$H_{3,7}z = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}^T = \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}$$

Если мы инвертируем шестой (110) бит в z, мы получим кодовое слово (1010101).

Это нам говорит о том, что ***каждое некодовое слово может быть преобразовано в уникальное кодовое слово, перевернув ровно один бит.***

▼ **Доказательство:**

Мы знаем, что любые две колонки в H различаются хотя бы в 1 позиции. Это значит, что каждая пара колонок линейно независима - т.е. мы не можем сложить две колонки и получить нулевой вектор. Будем учитывать, что для любого ненулевого кода c, Hc - линейная комбинация колонок H. Поскольку c - кодовое слово, мы знаем, что $Hc = 0$, значит c должен сложить вместе по крайней мере 3 колонки из H.

Теперь рассмотрим любые два кодовых слова $c_1 \neq c_2$:

$$\begin{aligned} & Hc_2 = 0 \\ \implies \quad & H(c_1 + (c_2 - c_1)) = 0 \\ \implies \quad & Hc_1 + H(c_2 - c_1) = 0 \\ \implies \quad & H(c_2 - c_1) = 0 \end{aligned} \qquad (Hc_1 = 0)$$

То есть разница между любыми двумя кодовыми словами сама по себе является кодовым словом — и должно быть установлено не менее трех битов. Получается, что все кодовые слова отличаются от всех остальных по крайней мере в трех позициях.

Рассмотрим n-битное кодовое слово c. Из него мы можем составить n кодовых слов, которые различаются *ровно в одном бите со словом* c. А поскольку преобразование одного кодового слова в другое кодовое слово потребовало бы изменить *хотя бы* 3 бита, мы знаем, что ни одно из наших новых слов не может ни на один бит отличаться от любого другого кодового слова, кроме c.

Теперь посчитаем количество кодовых слов. Мы знаем, что H имеет m-битные базисные вектора, значит, она имеет ранг m и ранг пустого пространства $n - m$. А поскольку мы определили C как нулевое пространство H, всего мы имеем 2^{n-m} кодовых слов.

Для каждого кодового слова мы можем сгенерировать n уникальных некодовых слов, которые учтут все слова:

$$\begin{aligned}\underbrace{2^{n-m}}_{\text{codewords}} + \underbrace{n \times 2^{n-m}}_{\text{non-codewords}} &= 2^{n-m} + (2^m - 1)(2^{n-m}) \\ &= 2^{n-m}2^m \\ &= 2^n \text{ words}\end{aligned}$$

Следовательно, каждое слово либо является кодовым словом, либо отличается от уникального кодового слова ровно на один бит. ■

Улучшенная стратегия

Теперь разработаем улучшенную стратегию для игры. Для начала игроки установят порядок, в котором они будут отвечать, и составят матрицу Хемминга $H_{m,n}$.

Когда значение для каждого игрока сгенерировано, каждый игрок представляет собой два как-бы игровых состояния: s_0, если предполагается, что игроку сгенерировалось 0, и s_1, если предполагается, что игроку сгенерировалось 1.

В таком случае игроки могут давать ответы на следующих выводах:

- Если $H_{m,n}s_0 \neq 0$ и $Hs_1 = 0$, то ответом будет 0.
- Если $H_{m,n}s_0 = 0$ и $Hs_1 \neq 0$, то ответом будет 1.
- Если $H_{m,n}s_0 \neq 0$ и $Hs_1 \neq 0$, то ответом будет “не знаю”.

⚠️ Заметим, что ситуация, когда оба результата равны 0, невозможна.

Стратегия с кодами Хемминга выигрывает игру всякий раз, когда первоначальное распределение шляп не является кодовым словом. Из доказательства выше мы знаем, что когда состояние не является кодовым словом, оно отличается от ровно одного кодового слова ровно на один бит. Это значит, что есть один игрок, для которого изменение s_0 на s_1 (или наоборот) позволит получить кодовое слово, поскольку игрок получит $Hs = 0$ при неверном ответе и $Hs \neq 0$ при правильном варианте ответа. В это же время все остальные игроки будут иметь $Hs \neq 0$ при как при s_0, так и при s_1, потому что их изменение их битов не позволит получить кодовое слово. И получается,

что все ответят “не знаю” и только один игрок ответит 1 или 0, и игроки выиграют.

▼ **Пример:**

Игра на 7 игроков с начальным распределением:
$\begin{bmatrix}1 & 0 & 1 & 0 & 1 & 1 & 1\end{bmatrix}$:

- Игрок 1 получит:

$$H_{3,7}\begin{bmatrix}0_? & 0 & 1 & 0 & 1 & 1 & 1\end{bmatrix}^T = \begin{bmatrix}1 & 1 & 1\end{bmatrix}$$
$$H_{3,7}\begin{bmatrix}1_? & 0 & 1 & 0 & 1 & 1 & 1\end{bmatrix}^T = \begin{bmatrix}1 & 1 & 0\end{bmatrix}$$

- Игроки 2-5, 7 также получат $H_{3,7}\boldsymbol{s}_0 \neq 0$ и $H_{3,7}\boldsymbol{s}_1 \neq 0$.
- Игрок 6 получит:

$$H_{3,7}\begin{bmatrix}1 & 0 & 1 & 0 & 1 & 0_? & 1\end{bmatrix}^T = \begin{bmatrix}0 & 0 & 0\end{bmatrix}$$
$$H_{3,7}\begin{bmatrix}1 & 0 & 1 & 0 & 1 & 1_? & 1\end{bmatrix}^T = \begin{bmatrix}1 & 1 & 0\end{bmatrix}$$

Остается только игроку 6 ответить 1, а всем остальным ответить “не знаю”.

С другой стороны, игроки будут проигрывать, когда начальное распределение значений является кодовым словом. В этом случае все игроки определят, что один ответ - правильный - приводит к кодовому слову, а другой - нет. Это связано с тем, что, когда истинное состояние является кодовым словом, изменение любого бита приведет к некодовому слову. В этом случае все игроки объявят неправильный цвет, и группа проиграет.

▼ **Пример:**

Рассмотрим игру на 7 игроков с начальным распределением
$\begin{bmatrix}1 & 0 & 1 & 0 & 1 & 0 & 1\end{bmatrix}$:

- Для игрока 1 будет:

$$\begin{aligned} H_{3,7}\begin{bmatrix}0_? & 0 & 1 & 0 & 1 & 0 & 1\end{bmatrix}^T &= \begin{bmatrix}0 & 0 & 1\end{bmatrix} \\ H_{3,7}\begin{bmatrix}1_? & 0 & 1 & 0 & 1 & 0 & 1\end{bmatrix}^T &= \begin{bmatrix}0 & 0 & 0\end{bmatrix} \end{aligned} \quad (\text{that's 1!})$$

- Для игрока 2 будет:

$$H_{3,7}\begin{bmatrix}1 & 0_? & 1 & 0 & 1 & 0 & 1\end{bmatrix}^T = \begin{bmatrix}0 & 0 & 0\end{bmatrix}$$
$$H_{3,7}\begin{bmatrix}1 & 1_? & 1 & 0 & 1 & 0 & 1\end{bmatrix}^T = \begin{bmatrix}0 & 1 & 0\end{bmatrix} \quad (\text{that's } 2!)$$

- Аналогично для всех остальных игроков.

В результате все игроки назовут неправильный цвет.

Оценка кровожадности пиратов

Представленная стратегия выигрывает всегда, когда расстановка и порядок игроков не отображают кодовое слово. А поскольку существует $n \times 2^{n-m}$ некодовых слов из 2^n слов, то:

$$\mathbb{P}(\text{win}) = \frac{n \times 2^{n-r}}{2^n} = \frac{n}{2^r} = \frac{n}{n+1}$$

А лучшая ли это оценка?

Давайте определим максимальное количество игр, в которых может выиграть любая возможная стратегия. Учитывая произвольную стратегию, каждый отдельный игрок будет угадывать правильно и неправильно в равном количестве игровых состояний. Это связано с тем, что процесс принятия решения каждым игроком должен быть независимым от сгенерированного значения: учитывая ту же информацию о других значениях, игрок должен либо воздержаться, либо угадать сгенерированное число, будь то 0 или 1. Следовательно, чтобы игрок был прав в одном состоянии, он должен быть неправ в другом.

Однако этот факт не означает, что наша общая стратегия должна проигрывать столько же, сколько и выигрывать: если мы сможем использовать больше неверных догадок в проигрышных раундах, чем правильных догадок в выигрышных раундах, наш общий коэффициент выигрыша увеличится. В оптимальном случае у нас было бы ровно одно правильное предположение игрока в каждом выигрышном раунде и чтобы все игроки угадывали неправильно в каждом проигрышном раунде. Это означает, что на каждые n выигрышных раундов должен быть хотя бы один проигрышный раунд.

Следовательно, если стратегия выигрывает W раундов и проигрывает L раундов из 2^n всего, то мы знаем, что $L \geq \frac{W}{n}$. А поскольку $W + L = 2^n$, получаем:

$$
\begin{aligned}
2^n - W &\geq \frac{W}{n} \\
n2^n &\geq W(n+1) \\
\frac{n}{n+1} &\geq \frac{W}{2^n}
\end{aligned}
$$

Что означает максимум для вероятности выигрыша равной $\frac{n}{n+1}$, которой мы можем достигнуть с использованием кодов Хемминга.

В таком случае, вероятность казни заложников при использовании ими предложенной стратегии равна $1 - \frac{n}{n+1} = \frac{1}{n+1}$.