Использование идей фонтанного кодирования при передаче малого числа битовых пакетов

Иванов Е. Р.
Московский государственный университет имени М.В. Ломоносова
Факультет Вычислительной математики и кибернетики
E-mail: `ivanover@my.msu.ru`

ВМК МГУ

2024

Глобальная задача

Общая задача

Требуется передать по стирающему каналу[a] связи информацию в виде K битовых векторов.

[a] BEC (Binary Erasure channel)

- Информацию нельзя просто перезапросить (Backward Error Correction, BEC), так как на сервере ее может уже не быть (пример: потоковое телевещание)
- Алгебраические коды оказываются неприменимыми к данной задаче, так как они эффективны лишь при достаточно малой длине кода и ошибках на уровне битов / байтов.

Новая аксиоматика

- Минимальная единица информации – **пакет** – длинный битовый вектор.
- Над пакетами определена операция суммы по модулю 2 ($\oplus$) как соответствующая покомпонентная.
- Обращаться к битовой структуре пакета **нельзя**:
    - для отправителя и получателя это означает, что нельзя использовать что-то, кроме операции $\oplus$
    - для канала это означает, что пакет либо доходит целиком, либо не доходит вовсе

Замечание

Примем следующее допущение: цена утери пакета достаточно низкая. Иными словами, ошибки декодирования, конечно, нежелательны, но могут происходить «не слишком часто». Пример: потоковое вещание.

Такая постановка позволяет перейти от алгебраических подходов к стохастическим / фонтанным.

Графовое представление

Предложение 1

Представим задачу в виде двудольного графа: в одной доле пакеты, в другой – кодирующие символы.
Отношение связности – это отношение включения в сумму: то есть символ s_i и пакет x_j смежны тогда и только тогда, когда $s_i = x_j \bigoplus \dots$.

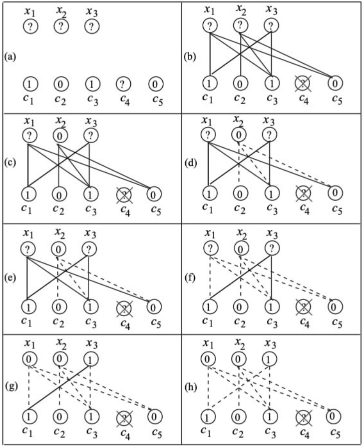
Определение

Граф, описанный в предложении 1, называется *графом Таннера*[a].

[a] Tanner, "A recursive approach to low complexity codes"

Предложение 2

Последовательно декодируем то, что можем декодировать, и переходим к задаче меньшей размерности.



a) символы c_1, c_2, c_3, c_5 прошли через канал

b) визуализируем информацию о связности

c) пакет x_2 дошел «как есть» в виде символа c_2, восстановим его

d) пакет x_2 присутствует участвовал в следующих символах:

$c_3 = x_1 \oplus x_2 \oplus x_3$ и $c_5 = x_1 \oplus x_2$

e) прибавим к обеим частям уравнений выше x_2: $c_3 \oplus x_2 = x_1 \oplus x_3$, $c_5 = x_1$

f)-h) по тому же алгоритму решаем задачу меньшей размерности

Процесс генерации символов

Предложение

Подберем такой алгоритм генерации символов, чтобы ЛТ-процесс завершался успешно с достаточно большой вероятностью.

Схема генерации выглядит так: у нас есть заданное распределение степеней символов

$$\boldsymbol{\rho} = (\rho_1, \ldots, \rho_K),\ \rho_i \geq 0,\ \sum_i \rho_i = 1$$

При формировании нового символа из этого распределения сэмплируется величина d и для суммирования равновероятно выбираются d из K пакетов:

$$d \sim \boldsymbol{\rho},\ s_{new} = \sum_{i=1}^{d} x_{j_i},\ j_i \in \{1, \ldots, K\},\ s \neq p \Rightarrow j_s \neq j_p$$

Постановка задачи

Идея фонтанного кодирования не содержит внутри себя обращения к **порядку** отправки пакетов, поэтому коды работают даже если канал передачи информации крайне ненадежен. На практике же канал заведомо «хороший», то есть теряет небольшой процент пакетов. Используя идеи фонтанного кодирования, будем пытаться сделать хорошего канала **почти идеальный** – с вероятностью утери пакета π.

- Процент потерь τ в канале достаточно мал ($\leq 5 - 7\%$)
- Количество пакетов, высылаемых при одних и тех же параметрах, невелико (пропускная способность канала зависит от времени)
- Коды систематические – сначала высылаем все «как есть»

Стратегии исследования

Опишем общие стратегии решения. Имеются 2 степени свободы: алгоритм декодирования $\mathcal{D}$ и распределение $\rho(\cdot)$.

Стратегия простого алгоритма и сложного распределения

Использование простого алгоритма декодирования (допускающего аналитический вывод формул) и решение задачи условной оптимизации.

Стратегия сложного алгоритма и простого распределения

Использование сложного алгоритма декодирования (слабо поддающегося анализу) и хорошо изученных (Бернулли, Пуассона) или просто устроенных распределений.

Стратегия простого алгоритма и сложного распределения

Приведем пример **простого алгоритма** декодирования.
Пусть x_i, $i = 1, \ldots, 5$ – пакеты. Отправитель пересылает их через канал и до получателя доходят x_1, x_2, x_4. Далее пересылаются 2 проверочных пакета:

$$s_1 = x_1 \oplus x_2 \oplus x_3$$

$$s_2 = x_1 \oplus x_3 \oplus x_5$$

- Получен s_1. Декодирование будет проведено – восстановим x_3.
- Получен s_2. Декодирование проведено **не** будет: среди пакетов в символе есть два не из полученных информационных – x_3 и x_5.

Данный пример иллюстрирует возможную *нерациональность* простого алгоритма: к моменту получения s_2 пакет x_3 уже восстановлен и s_5 на самом деле восстановить можно.

Аналитические формулы

$$\mathsf{P}\{\text{пакет с номером } K \text{ не будет восстановлен}\} =$$

$$= \tau \sum_{l=0}^{K-1} \binom{K-1}{l} \sum_{C=0}^{M} \binom{M}{C} \tau^{K-1+M-l-C} (1-\tau)^{l+C} \left[1 - \sum_{d=1}^{l+1} \rho_d \frac{\binom{l}{d-1}}{\binom{K}{d}} \right]^C$$

$$=: \tau \cdot \mathcal{L}(\boldsymbol{\rho}, K, M)$$

Получили задачу условной оптимизации:

$$\begin{cases} \mathcal{L}(\boldsymbol{\rho}, K, M) \to \min \\ \rho_i \geq 0 \\ \sum\limits_i \rho_i = 1 \end{cases}$$

Результаты экспериментов. Метрики

K	M	$\tau\mathcal{L}$, %	Parity Packet Baseline, %
20	2	1.23	1.32
30	2	1.54	1.76
40	2	1.78	2.09
20	3	0.93	1.32
30	3	1.23	1.76
40	3	1.47	2.09
20	4	0.74	1.32
30	4	1.01	1.76
40	4	1.25	2.09

Таблица: Результаты экспериментов. $\tau = 0.03$

Под колонкой «Parity Packet Baseline» подразумевается улучшение пропускной спобосности в случае отправки M пакетов четности.

Результаты экспериментов. Пример распределения

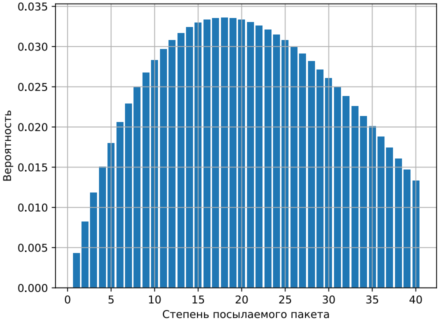


Рис.: $K = 40, \; M = 4$

По оси абсцисс отложена степень кодирующего пакета, по оси ординат – соответствующая вероятность.

Стратегия сложного алгоритма и простого распределения. Выбор распределений

Наблюдение

Предложенные ранее удачные распределения идейно имеют общее свойство: чаще всего генерируются символы одной и той же степени, которые постепенно расходуются для поддержания размера очереди.

Таким условиям удовлетворяют биномиальное и Пуассоновские распределения, а также, например:

$$\rho(d) = \delta_{dd^*} = \begin{cases} 1, & d = d^* \\ 0, & d \neq d^* \end{cases}$$

Рассмотрим их подробнее.

Результаты экспериментов

K	N	$p_{\text{опт}}$	τ	π
20	24	0.571	0.05	0.01
20	24	0.776	0.03	0.003
50	60	0.286	0.05	0.008
50	60	0.327	0.03	0.002

Таблица: Результаты экспериментов. Биномиальное распределение. Избыточность 20%

K	N	$\lambda_{\text{опт}}$	τ	π
20	24	10.6	0.05	0.01
20	24	11.0	0.03	0.004
50	60	15.3	0.05	0.007
50	60	18.6	0.03	0.001

Таблица: Результаты экспериментов. Пуассоновское распределение. Избыточность 20%

По оси абсцисс отложено математическое ожидание степени каждого кодирующего символа, по оси ординат – вычисленная оценка.

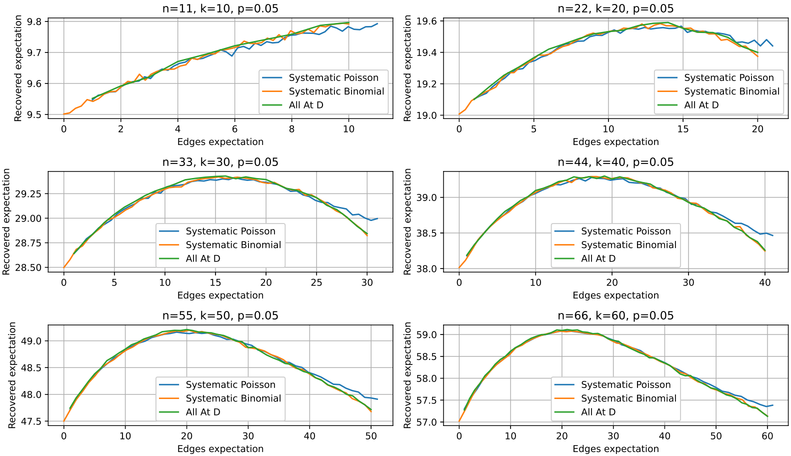


Рис.: $n = 1.1\,k; \tau = 0.05$

- Методы, соответствующие использованию сложного алгоритма и малопараметрического распределения способны снизить вероятность утери пакета **на порядок** относительно собственной пропускной способности
- Методы, использующие простой алгоритм декодирования могут обеспечить улучшение только в **2-3 раза**; однако, большим преимуществом таких подходов является очень дешевый процесс декодирования совершаемый **«на ходу»** (т.е. без памяти), что может быть существенно для некоторых типов систем передачи информации.