Ответы на вопросы по курсу ТОИ 2006 год.

Великий и ужасный _junk

24 декабря 2006 г.

1 Понятие информации

Информация (лат. Informatio) Осведомленность, знания, сведения, данные.
Информация возникает в процессе отражения.
Информация может содержать три аспекта:

- Прагматический (зачем)
- Синтаксический (какой наоситель)
- Семантический (ценность информации)

Основные подходы к подсчету количества информации:

- Статистический (используется в курсе). Использует теорию вероятности. Основа – функция энтропии. *Энтропия* – мера количества информации в данном подходе. Содержание информации не рассматнривается, но учитывается, что неожиданная информация обладает большей значимостью
- Семантический подход – базируется на ценности информации.
- Структурный подход – нашел применение при хранении информации. *Реквизит* – единица информации.

Модель: [И] ———КС——— [П]
И выдает $X \in X_0\{x_{01}, x_{02} \ldots\}$

1.1 Количество информации в сообщении

$I(x_{0j})$ – количество информации в сообщении j
Свойства I (собственной информации):

- $I \geq 0$
- Аддитивность
- Должна зависеть от вероятности возникновения информации, чем больше вероятность, тем меньше I

- $I(0) = 0$
- $I(1) = 0$
- два равновероятных события дат 1 инф.

Собственная информация:

$$I(x_{0j}) = -\log_2 P(x_{0j})[bit]$$

Среднее количество информации (энтропия):

$$H(X_0) = -\sum_{j=1}^{m} P(x_{0j}) \log_2 P(x_{0j})$$

2 Понятие информации в равновероятных сообщениях

Код – последовательность символов, однозначно отображающих одно или несколько сообщений. Любой код характеризуется основанием k, длиной n и избыточностью.

Рассмотрим количественную меру информации, при следующих ограничениях:

- сообщения дискретны;
- сообщения равновероятны и независимы;
- символы кода, отображающие сообщения, взаимно независимы;
- система счисления кода конечна.

Формула Хартли:

$$I(x_{0j}) = \log_2 M$$

Энтропия:

$$\sum P(x_{0j}) I(x_{0j}) = M P(x_{0j}) I(x_{0j}) = I(x_{0j})$$

Количество информации в любом символе равномерного равновероятнеого кода:

$$I(x_j) = \log_2 K$$

3 Понятие информации в неравновероятных сообщениях

Количество информации: $I(x_{0j}) = -\log_2 P(x_{0j})$
Энтропия: $H(x_{0j}) = -\sum_{j=1}^{M} P(x_{0j}) \log_2 P(x_{0j})$

$$I(x_{0j}) = nH(x_j)$$

4 Энтропия дискретных сообщений

Энтропия – мера неопределенности состояния системы. *Энтропия* в информатике может рассматриваться как величина обратная количеству информации с точки зрения знака. Так как с приходом информации неопределенность уменьшается.

Функция энтропии:

- непрерывна относительно вероятности;
- при равновероятных событиях монотонно возрастает с увеличением числа событий;
- независит от пути выбора событий.

Для обеспечения максимума передаваемой информации, символы кода должны быть равновероятны.

$$H(P_1, P_2, P_3 \dots P_k) = -\sum_{j=1}^{k} P_j \log_2 P_j$$

5 Виды энтропиии дискретных сообщений

Безусловная энтропия Физически это информация перносимая любым случайно выбранным сообщением.

$$H(X_0) = -\sum_{j=1}^{n} P(x_{0j}) \log_2 P(x_{0j})$$

Взаимная энтропия Относиться к множеству ансамблей сообщений и означает среднее количество информации, которое переноситься заданным числом сообщений, выбранным из нескольких ансамблей.

- множества сообщений – взаимно независимы Взаимная энтропия – сумма безусловных энтропий:

$$H(X_0, Y_0) = H(X_0) + H(Y_0)$$

- множества сообщений – взаимно зависимы Для зависимых ансамблей энтропия равна сумме безусловной и условной энтропий.

$$H(X_0, Y_0) = H(X_0) + H(Y_0|X_0)$$

Условная энтропия – математическое ожидание условной собственной информации. Отображает среднее количество информации, которое вносит помеха в передаваемый сигнал.

$$H(Y_0|X_0) = -\sum_{j}\sum_{i} P(X_{0j}) P(Y_{0i}|X_{0j}) \log_2 P(Y_{0i}|X_{0j})$$

6 Взаимная информация

Количество информации проходящей через канал связи. Взаимная информация показывает количество информации в сообщении на вызоде КС относительно сообщения заданного на входе.

$$I(X_0, Y_0) = H(Y_0) - H(Y_0|X_0)$$

7 Энтропия источника, энтропия сообщения

Энтропия источника:

$$H(x) = -\sum_{q=1}^{L}\sum_{j=1}^{k} P_q P_q(x_j) \log_2 P_q(x_j)$$

Не избыточный максимальный код обладает максимальной энтропией источника:

$$H_{max}(x) = \log_2 K$$

Избыточность $= 1 - \frac{H(x)}{H_{max}(x)} = 1 - \frac{H(x)}{log_2 K}$
Избыточность сообщения $= 1 - \frac{H(X_0)}{H_{max}(X_0)} = 1 - \frac{nH(x)}{nH_{max}(x)} = 1 - \frac{H(x)}{H_{max}(x)}$

8 Энтропия непрерывных сообщений

Количество информации и энтропия в jтом отсчете:

$$I(x_j) = -\log_2 (W(x_j)\Delta x)$$

$$H(x_j) = P(x_j) \log_2 P(x_j)$$

Приведенная энтропия:

$$H_{\text{пр}}(x) = -\int_{-\infty}^{+\infty} W(x) \log_2 W(x) dx$$

Свойства приведенной энтропии:

- зависит от статистики отсчетов функции
- существует оптимальное распределение $W(x)$ (нормальное), для которого ПЭ максимальна
- определяется амплитудой исходной функции и значением Δx
- весьма важен и способ квантования (равномерный, неравномерный, с передачей отклонения от мат.ожидания)

9 Понятие и типы каналов связи

Канал связи – совокупность программно-аппаратных средств, обеспечивающих передачу требуемого количества информации с заданной вероятностью ошибки.

Типы каналов связи:

- Проводные (металлические, телефонной связи, коаксиал, оптоволокно)
- Радиоканалы (длинноволновые, средне, коротко, ультракоротко)
- Гидроакустические каналы (в водной среде)
- Сейсмические каналы связи
- Спутниковые каналы связи
- Каналы искуственных инженерных сооружений (батарея отопления, электропроводка)

10 Модель и характеристики НКС

Модель: $x(t)$ —–НКС—– $y(t)$

Характеристики НКС:

- физические свойства и вид модуляции F_k
- время, на которое канал предоставлен для передачи сигнала T_k
- предельная мощность $H_{\text{доп}}$

Произведение вышеуказанных трех величин – объем канала.

Необходимое условие передачи – объем сигнала не больше объема канала.

Достаточные условия – все три параметра сигнала не больше аналогичных параметров канала (допустим обмен между параметрами за счет кодирования)

11 Классификация и модели ДКС

ДКС:[М]—–НКС—–[ДМ]

Модель: (X)—-ДКС—-(Y)

ДКС можно представить графом, где вершины — символы, вес ребер — вероятность прохождения или трансформации.

Классификация ДКС:

- по основанию системы счисления
- по соотношению K_x и K_y (без стирания, со стиранием)
- по зависимости вероятности от времени (стационарные, нестационарные)

- по зависимости вероятностей от предшествующих значений (с памятью, без памяти)
- по соотношению вероятностией в матрице переходов (симметричные по входу, по выходу, по входу и выходу)

12 Скорость передачи информации и пропускная способность ДКС без шума

Скорость передачи – взаимная информация передаваемая через канал:

$$R = I(x,y) = H(Y) - H(Y|X) = H(Y) = -\sum_{j=1}^{k}\sum_{i=1}^{k} P(x_j)P(y_i|x_j)\log_2(P(x_j)P(y_i|x_j))$$

Верхний предел скорости передачи — *пропускная способность*.

$$C = I_{max} = H_{max}(Y) = \log_2 K$$

Для канала без шума увеличение пропускной способности возможно увеличением основания кода.

13 Скорость передачи информации и пропускная способность ДКС с шумом

Скорость передачи:

$$R = H(y) - H(y|x) = -\sum_{j=1}^{k}\sum_{i=1}^{k} P(x_j)P(y_i|x_j)\log_2(P(x_j)P(y_i|x_j)) + \sum_{j=1}^{k}\sum_{i=1}^{k} P(x_j)P(y_i|x_j)\log_2(P(y_i|x_j))$$

Пропускная способность:

$$C = H_{max}(y) - H_{min}(y|x) = \log_2 K - H_{min}(y|x) = \log_2 K - (1-p^*)\log_2(1-p^*) - p^*\log_2\frac{p^*}{K-1}$$

Для ДКС с шумом пропускная способность определяется основанием кода и вероятностью искажения символа.

14 Кодирование дискретной информации в канале связи без шума (процедура Шеннона)

Основная проблема – приближение скорости передачи к пропускной способности.

Если производительность источника $H(x) \le C$, то возможна передача информации со скоростью коль угодно близкой к пропускной способности канала $I = C - \epsilon$.

Дано:

$$X_0\{x_{01}, x_{02}, \dots x_{0n}\}$$

$$P(x_{01}) \ge P(x_{02}) \ge \dots \ge P(x_{0n})$$

Применим способ кодирования, при котором длины кодов — расположение некоторых вероятностей с учетом двоичной системы счисления.

$$\log_2[\frac{1}{P(x_{0j})}] \leq n_j \leq 1 + \log_2[\frac{1}{P(X_{0j})}]$$

n_j выбирается как целое число.

Средняя длина кода:

$$n_{\text{ср}} = \sum_{j=1}^{M} P(x_{0j}) n_j$$

$n_{\text{ср}}$ – энтропия любого случайно выбранного сообщения из переданных.

$$n_{\text{опт}} = \frac{H(X_0)}{H_{max}(X)}$$

Два критерия оценки оптимальности:

- $n_{\text{ср}} - n_{\text{опт}} = \varepsilon$
- $H(x) = H_{max}(x)$ (все символы равновероятны)

Алгоритм:

1. На горизонтальной оси отмечаются точки, соответствующие порядку убывания их вероятностей.
2. Выбирается корень кодового дерева(разбив ось на две части 1/2-1/2; 2/3-1/3;3/4-1/4). На горизонтальной оси выбираются места расположения вершин первого яруса для чего сообщения разбиваются на k групп с примерно равной вероятностью. Точки деления соединяются с корнем кодового дерева образуя k ветвей. Ветвям присваиваем индексы от 0 до $k-1$
3. Каждая группа образованная на предшествующем этапе разбивается на k подгрупп. При этом образуются вершины второго яруса.
4. Процесс продолжается до тех пор, пока в каждой подгруппе не останется единственное сообщение. Сообщения располагаются только в концевых узлах кодового дерева.

$$n_{\text{ср}} = \frac{H(X_0)}{H(x)}$$

15 ?Кодирование дискретной информации в канале связи без шума (процедура Хаффмана)

Алгоритм:

1. Все m сообщений располагаются в порядке убывания вероятностей из появления по вертикальной оси сверху вниз.

2. ???

3. Образованная группа рассматривается как новое сообщение с сумарной вероятностью появления. Производиться новое упорядочивание.

4. Образуется группа из k сообщений с наименьшими вероятностями появления.

5. Повторять два предыдущих пункта до тех пор, пока не останется одно сообщение с вероятностью 1.

6. Ветви полученного дерева индексируются от 0 до $k-1$.

16 ?Прямая теорема Шеннона для ДКС с шумом

Если $\nu \leq C$, то при $n \to \infty$ $P_{\text{ош}} \to 0$

17 Понятие и типы кодов

Код — последовательность символов во времени или пространстве отображающая одно или несколько сообщений.

Код характеризуется:

- основанием
- количеством элементов
- базовым временем
- временем одного символа
- избыточностью
- кодовым расстоянием

Классификация кодов:

- по основанию (двоичный, троичный, ...)
- по наличию избыточности (избыточные, безызбыточные)
- по корректирующим свойствам (обнаруживающие, корректирующие)
- по расположению контрольнгых элементов в коде (систематические, несистематические)
- по расположению элементов кода во времени (последовательные, паралельные, посл.-пар.)
- по используемым сигнальным признакам (простой позиционный, число-импульсный, амплитудо-импульсный, частотно-импульсный, полярно-импульсный, кодо-импульсный, со смешанным сигнальным признаком)

18 ?Геометрические модели кодов

19 Методика постоениея линейных систематических кодов (образующая матрица)

Линейные коды — коды, в которых. проверочные элементы представляют собой линейные комбинации информационных.

Вес кодового вектора — число его ненулевых элементов.

Кодовое расстояние — вес вектора полученного в результате сложения исходных векторов.

Групповые коды удобно задавать в виде матриц, размерности $m \times n$ (m — информационные элементы, k — контрольные, $n = k + m$). Коды пораждаемые этими матрицами известны как (n,m) коды, а матрицы как *образующие* (производящие).

$$|A| = |I||D|$$

В теории и на практике установлено, что в качестве информационных матриц удобно брать единичную матрицу $I_{m \times m}$ в канонической форме.

При выборе d учитывается:

1. Чем больше «1» в матрице тем порождаемый код ближе к оптимальному.
2. Чем больше «1» в матрице тем сложнее аппаратура кодера и декодера.
3. Вес каждой строки дополнительной матрицы должен быть не меньше чем $d_0 - 1$

Левый канонический вид порождающей матрицы:

$$A = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & d_{11} & d_{12} & \dots & d_{1k} \\ 0 & 1 & 0 & \dots & 0 & d_{21} & d_{22} & \dots & d_{2k} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & d_{m1} & d_{m2} & \dots & d_{mk} \end{pmatrix}$$

Оптимальный корректирующий код — групповой код, при использовании которого вероятность ошибки не больше, чем при использовании любого другого кода при таких же m и k.

Пример кодирования:

$$\begin{pmatrix} 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

20 Процедура декодирования линейных кодов (проверочная матрица)

Пусть дана образующая матрица:

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Построение проверочной матрицы: Выразим каждый контрольный символ через информационные:

$$\begin{aligned} \nu_2 &= \nu_0 \oplus \nu_1 \\ \nu_3 &= \nu_1 \\ \nu_4 &= \nu_0 \end{aligned}$$

Если в канале произошла ошибка, то в принятом векторе r хотя бы одно из равенств не будет выполняться. Запишем полученные соотношения в виде системы уравнений для компонент вектора r:

$$\begin{aligned} r_0 \oplus r_1 \oplus r_2 &= s_1 \\ r_1 \oplus r_3 &= s_2 \\ r_0 \oplus r_4 &= s_3 \end{aligned}$$

Вектор s принято называть *синдромом*, ошибка обнаружена, если хотя бы одна из его компонент не равна нулю.

По второй системе уравнений построим проверочную матрицу:

$$H_{k\times n} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Пример декодирования:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$$

Полученный синдром указывает на 2 (с нуля) столбец проверочной матрицы, ошибка на второй позиции вектора r.

21 Коды Хемминга

Положительные стороны:

- не нужно считать нижний предел Хемминга
- синдром указывает на место ошибки

Рассмотрим кодовый вектор:

$$\{x_1, x_2, x_3 \dots x_n\}$$

В коде Хемминга выделяют контрольные позиции (номер — степень двойки):

$$\{x_1, x_2, x_4, x_8 \ldots\}$$

и информационные (все остальные):

$$\{x_3, x_5, x_6, x_7, x_9 \ldots\}$$

Контрольные и информационные позиции находятся зависимости такой что, сумма по модулю два позиций с «1» в одининаковых разрядах (в двоичном представлении номеров) равна нулю[1]:

$$\begin{aligned} x_1 \oplus x_3 \oplus x_5 \oplus x_7 \quad \ldots \quad &= 0 \\ x_2 \oplus x_3 \oplus x_6 \oplus x_7 \quad \ldots \quad &= 0 \\ x_4 \oplus x_5 \oplus x_6 \oplus x_7 \quad \ldots \quad &= 0 \end{aligned}$$

Синдром ошибки строиться по этим же правилам (нули заменяем на компоненты вектора s). Перевод синдрома в десятичную систему счисления даст нам порядковый номер позиции ошибки.

22 Коды Хемминга с проверкой на четность

При желании обнаруживать две ошибки и исправлять одну $d = r + s + 1 = 2 + 1 + 1 = 4$, можно воспользоваться кодом Хемминга, добавив контрольную позицию с общей проверкой на четность.

Алгоритм исправления ошибок (не уверен):

Синдром	Опознаватель	Результат
0	0	нет ошибок*
0	1	нечетное число ошибок >1
1	1	одна ошибка*
1	0	четное число ошибок

23 ?Модель ошибок в ДКС без памяти

24 ?Информационный предел избыточности для ДКС без памяти

25 Модель ошибок в ДКС с памятью

Реальный канал связи использует двоичные коды и обладает памятью, то есть ошибки приобретают пакетный характер. Такой канал формально описывается *моделью Гилберта*, которая предполагает наличие двух состояний в канале связи с определенными вероятностями перехода и сохранения состояний.

[1] Существует мнемоническое правило: один по одному через один с одного, два по два через два со второго, 4:4:4:4, 8:8:8:8, ...

Модель Гиберта (плохого состояния):

$$M(j,n) = \begin{cases} C_n^0 = 1 & j = 0 \\ C_n^1 = n & j = 1 \\ (n-j+2)2^{j-2} & j \geq 2 \end{cases}$$

Уточненная модель Гилберта("просвет" в плохом состоянии):

ПХ — ошибок нет

ПП — ошибки есть

$$P(s) = \begin{vmatrix} \text{Х} & \text{ПХ} & \text{ПП} \\ P_{00} & P_{01}(1-p) & P_{01}p \\ P_{10} & P_{11}(1-p) & P_{11}p \\ P_{10} & P_{11}(1-p) & P_{11}p \end{vmatrix}$$

Модель Гилберта *всегда* дает более оптимистичный результат нежели модель независимых ошибок.

26 Минимальная избыточность для обнаружения и исправления ошибок в ДКС

$$k_{min} = \frac{I_k}{\log_2 k} = I_k$$

$$I_k = log_2[1 + n + \sum_{j=1}^{s}(n-j+2)2^{(j-2)}]$$

27 Обратная теорема Шеннона

Если производительность источника превышает пропускную способность канала ($H(X_0) > nC$), то в канале с шумом невозможна передача информации с бесконечно малой вероятностью ошибки. Нижняя граница вероятности ошибки находиться из выражения:

$$-p_0 log_2 p_0 - (1-p_0) log_2 (1-p_0) + p_0 log_2 (m-1) = H(X_0) - nC$$

где p_0 — вероятность ошибки, $H(X_0)$ — производительность источника сообщений, nC — пропускная способность ОДКС.

28 Циклические коды. Процедура кодирования.

Циклический код отличается тем, что каждая последущая комбинация может быть получена путем циклического сдвига элементов на шаг.

Потребуем, чтобы все комбинации циклического кода, представленные в виде многочленов делились на некоторый многочлен без остатка. Этот многочлен — $p(x)$ назван порождающим,

он задает корректирующие свойства кода, поэтому имеет степень k. Порождающий многочлен должен быть неприводимым (берутся из таблиц).

$$P_2(x) = x^3 + x^2 + 1 \quad k = 3 \quad m = 4$$
$$P_3(x) = x^2 + x + 1 \quad k = 2 \quad m = 4$$

Образующая матрица:

$$A_{m\times n} = \begin{vmatrix} a_0 & a_1 & a_2 & \dots & a_k & 0 & 0 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & \dots & a_k & 0 & 0 & 0 \\ 0 & 0 & a_0 & a_1 & a_2 & \dots & a_k & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & a_0 & a_1 & a_2 & \dots & a_k \end{vmatrix}$$

Вышеописанный способ не используется, так как нужно расчитывать и хранить на принимающей стороне обратную матрицу.

Другой способ:

1. Выбираем из таблицы неприводимых в двоичном поле многочленов. $g(x)$ следует выбирать так, чтобы он был как можно более коротким, степень была $\leq K$ а длина $\geq d_0$

2. Определим элементы дополнителбной матрицы производя деление единицы с нулями на образующий многочлен. Полученные остатки должны удолветворять следующим требованиям:

   - число разрядов каждого остатка $= K$;
   - число самих остатков $\geq m$;
   - вес остатка $\geq d_0 - 1$.

   Из этих соображений выбирается требуемое число «0» приписываемых к «1».

3. Составим образующую матрицу. Дополнительная матрица распологается слева, единичная матрица справа.

Пример ($g(x) = x^3 + x^2 + 1$; $m = 4$;$k = 3$;$d_0 = 3$):

$$\begin{array}{ccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ & & & 1 & 0 & 1 & 1 \\ & & & 1 & 0 & 1 & 0 \\ & & 1 & 0 & 1 & 1 & \\ & & 1 & 1 & 1 & 0 & \\ & 1 & 0 & 1 & 1 & & \\ & 1 & 1 & 0 & 0 & & \\ 1 & 0 & 1 & 1 & & & \\ 1 & 1 & 0 & 1 & & & \\ 0 & 1 & 1 & 0 & & & \end{array}$$

образующая матрица:

$$A_{m\times n} = \left(\begin{array}{ccc|cccc} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

29 Циклические коды. Процедура декодирования.

Алгоритм:

1. Принятую кодовую комбинацию $f(x)$ делим на образующий многочлен $g(x)$ и подсчитываем вес остатка. Если вес $\leq s$, то принятую комбинацию складываем по модулю два с полученным остатком. Сумма дает правильную комбинацию.

2. Производим циклический сдвиг принятой кодовой комбинации на один разряд вправо, делим на образующий многочлен, если вес остатка $\leq s$, то делимое суммируем с остатком.

3. Сдвиг суммы влево на один разряд дает правильную комбинацию.

4. Если после первого сдвига вес остата $\geq s$, то повторяем второй пункт пока условие не будет выполненно. Далее суммируем делимое с остатком и сдвигаем влево на количество разрядов равное количеству сдвигов вправо. Мы получили правильную комбинацию.

5. Если после n сдвигов вправо необходимый остаток не был получен, комбинация не подлежит коррекции и происходит защитный отказ.

30 Нижний предел Хемминга

$$2^m \leq \frac{2^n}{\sum_{i=0}^{s} C_n^i}$$

Упрощенное правило:

$$K =]log_2(m+1+]log_2(m+1)[)[$$