Исследование совместной информации

Joint information research

Синюк / Sinyuk A.
Александр Демьянович
(eentrop@rambler.ru)
доктор технических наук, доцент.
ФГКВОУ ВО «Военная академия связи имени Маршала Советского Союза С. М. Буденного» (ВАС им. С. М. Буденного) МО РФ,
доцент.
г. Санкт-Петербург

Остроумов / Ostroumov O.
Олег Александрович
(oleg-26stav@mail.ru)
кандидат технических наук.
ВАС им. С. М. Буденного,
преподаватель.
г. Санкт-Петербург

Ключевые слова: широковещательный канал связи – broadcast channel; оценка информационной эффективности передачи информации по широковещательному каналу – assessment of information efficiency of information transfer on broadcast channel; пропускная способность канала связи – throughput of communication link; средняя совместная информация – average joint information; условная совместная информация – conventional joint information; свойства совместной информации – properties of joint information.

В предшествующих работах введены модель широковещательного канала и совместная информация для оценки информационной эффективности. Статья посвящена исследованиям совместной информации. Доказательно выявлены свойства перестановок, аддитивности, тождества совместной и взаимной информаций, не увеличения при преобразованиях, граничные значения. Сделан вывод, что совместная информация формирует фундамент для получения точных оценок пропускной способности, очерчивающих потенциальные возможности в ходе разработки систем связи с широковещательными каналами.

The model of broadcast channel and joint information for assessment of information efficiency are entered in prior operations. Article is devoted to researches of joint information. Properties of swaps, additivities, identities of joint and mutual information, not increases in case of conversions, boundary values are revealed evidentiary. The conclusion is that joint information creates the base for receiving the exact estimates of throughput contouring potential opportunities during development of systems of communication with broadcast channels.

Введение

В ходе проведенных исследований [1–3] дано описание модели и выполнена постановка задачи кодирования дискретного широковещательного канала без памяти (ДШВК БП), а также введена новая информационная мера [1], позволяющая описать передачу сообщения в разработанной модели канала на основе известного метода соответствия теоретико-информационных тождеств с их эквивалентами из теории множеств [4]. Конечной целью научного поиска определено получение точных оценок информационной эффективности, которые могут упростить реализацию процедур разработки оптимальных систем связи, включающих широковещательные каналы связи (ШВК). Для этого в работе выполняется всестороннее исследование свойств нововведенной меры на основе корректной формулировки и строгих доказательствах утверждений. Полученные результаты сформируют предпосылки для достижения цели определяющей получение точной оценки пропускной способности исследуемой модели ШВК.

Терминология совместной информации

Ранее было определено, что передача сигналов по ДШВК БП [1] определяется двумя каналами с общим входным алфавитом X, выходными алфавитами Y, M. Алфавиты X, Y и M представляются тремя дискретными множествами с сообщениями $x \in X$, $y \in Y$, $m \in M$. На основе ансамбля $\{XYM, p(x,y,m)\}$, который образован всеми тройками $(x,y,m) \in XYM$, и ансамблей $\{X, p(x)\}, \{Y, p(y)\}, \{M, p(m)\}, \{XY, p(x,y)\}, \{XM, p(x,m)\}$ в [1, 5] введена совместная информация (СИ) $F(x;y;m)$, которая рассматривается, как случайная величина (СВ) на ансамбле $\{XYM, p(x,y,m)\}$, что позволило ввести для нее различные числовые характеристики и, в частности, математическое ожидание. В [1, 5] определено понятие среднего количества СИ $F(X;Y;M)$ ансамблей $\{X, p(x)\}, \{Y, p(y)\}, \{M, p(m)\}$ как математическое ожидание СВ $F(x;y;m)$ на ансамбле $\{XYM, p(x,y,m)\}$:

$$F(X;Y;M) = \mathrm{M}F(x;y;m) =$$
$$= \sum_{x\in X}\sum_{y\in Y}\sum_{m\in M} p(x,y,m)\log\left(\frac{p(x/y)p(x/m)}{p(x)p(x/y,m)}\right) =$$
$$= I(X;Y) - I(X;Y/M) = I(X;M) - I(X;M/Y), \quad (1)$$

где M – обозначение математического ожидания, $I(X;Y)$ взаимная информация X и Y [4, 6]; $I(X;Y/M)$ – условная взаимная информация X и Y при известном M [4, 6]; $I(X;M)$ взаимная информация X и M; $I(X;M/Y)$ – условная взаимная информация X и M при известном Y.

В случае если в дополнение к ранее рассмотренному случаю для троек сообщений в модели ДШВК БП в [5] добавлена еще одна составляющая (канал), для которой определены ансамбли $\{Z, p(z)\}$, $\{XZ, p(x,z)\}$, определившие ансамбль $\{XYMZ, p(x, y, m, z)\}$, образованный всевозможными четверками $(x, y, m, z) \in XYMZ$. Это введение позволило определить понятие условной средней СИ $F(X;Y;M/Z)$ ансамблей X, Y и M относительно ансамбля Z:

$$F(X;Y;M/Z) = \\ = \sum_{XYMZ} p(x,y,m,z)\log\left(\frac{p(x/y,z)p(x/m,z)}{p(x/z)p(x/y,m,z)}\right). \quad (2)$$

Исследование совместной информации

Проведем исследование СИ с использованием известной терминологии теории информации [4, 6], корректной формулировки и строгих математических доказательствах представляемых утверждений.

1. Свойство аддитивности. Совместная информация тройки сообщений, одно из которых представляет пару сообщений $F(x;(y,m);z)$ может быть представлена суммой безусловной и условной СИ после преобразований:

$$F(X;(Y,M);Z) = I(X;(Y,M)) - I(X;(Y,M)/Z) = \\ = [I(X;Y) + I(X,M/Y)] - [I(X;Y/Z) + I(X;M/Y,Z)] = \\ = [I(X;Y) - I(X;Y/Z)] + [I(X;M/Y) - I(X;M/Y,Z)] = \\ F(X;Y;Z) + F(X;M;Z/Y). \quad (3)$$

Показанное свойство имеет аналог для взаимной информации [4, 6].

2. Утверждение 1. Для модели ДШВК БП выполняется следующее равенство:

$$F(X;Y;M) = I(Y;M). \quad (4)$$

Доказательство. Согласно (1) запишем

$$F(X;Y;M) = I(X;Y) - I(X;Y/M) = \\ = [H(Y) - H(Y/X)] - [H(Y/M) - H(Y/X,M)] = \\ = [H(Y) - H(Y/X)] - [H(Y/M) - \\ - H(Y/X)] = H(Y) - H(Y/M) = I(Y;M), \quad (5)$$

где $H(Y)$ – энтропия Y [4, 6], $H(Y/X)$ – условная энтропия Y при известном X [4, 6], $H(Y/M)$ – условная энтропия Y при известном M, $H(Y/X,M)$ – условная энтропия Y при условии, что известны X и M.

В (5) учтено, что $H(Y/X,M) = H(Y/X)$, т.к. при фиксированном ансамбле X ансамбли Y и M статистически независимы [7]. Утверждение доказано.

3. Утверждение 2. Для модели ДШВК БП определены границы СИ:

$$\min\left[I(X;M), I(X;Y)\right] \geq F(X;Y;M) \geq 0. \quad (6)$$

Доказательство. Верхняя граница $F(X;Y;M)$ определяется из (1), причем $F(X;Y;M) = I(X;M)$ в случае отсутствия ошибок в первой составляющей ДШВК БП [1], а $F(X;Y;M) = I(X;Y)$ в подобном случае во второй составляющей. Нижняя граница $F(X;Y;M)$ определяется теоремой о неотрицательности средней взаимной информации [4, 6]. $F(X;Y;M) = 0$ в случаях попарной или полной статистической независимости ансамблей друг от друга X, Y и M. Утверждение доказано.

4. Одно из важнейших свойств СИ состоит в том, что она не увеличивается при преобразованиях. Для того чтобы точно сформулировать и доказать это свойство, введем в рассмотрение некоторые преобразования $\psi(\bullet)$ и $f(\bullet)$, отображающие элементы множеств Y и M на элементы других множеств, скажем V и W, соответственно. Предположим, что каждый элемент множества V (W) является образом некоторого (возможно, не одного) элемента из $Y(M)$, что описывается выражением: $V = \psi(Y)$ $(W = f(M))$. Пусть задан $\{XYM, p(x,y,m)\}$ и определена величина средней СИ $F(X;Y;M)$. $\psi(\bullet)$ определяет $\{VX, p(v,x)\}$, для которого

$$p(v,x) = \sum_{y:\psi(y)=v} p(y,x), \quad (7)$$

а преобразование $f(\bullet)$ определяет ансамбль $\{WX, p(w,x)\}$, для которого

$$p(w,x) = \sum_{m:f(m)=w} p(m,x). \quad (8)$$

Поэтому средняя СИ $F(X;Y;M)$ определена для каждого из отображений $\psi(\bullet)$ и $f(\bullet)$ и принимает значения, определяемые выбором $\psi(\bullet)$ и $f(\bullet)$.

Теорема. Для любых отображений $V = \psi(Y)$ и $W = f(M)$ ансамблей Y и M в ансамбли V и W соответственно

$$F(X;Y;M) \geq F(X;V;W), \quad (9)$$

причем равенство достигается, когда отображения обратимы, т. е. каждой паре $v \in V$ и $w \in W$ соответствует единственная пара $y \in Y$ и $m \in M$.

Доказательство. Рассмотрим множество XYV. Так как при выбранном сообщении $x \in X$ сообщение $v \in V$ однозначно определено $y \in Y$ и, следовательно, не зависит от сообщения $x \in X$, то распределение вероятностей на тройках (x,y,v), соответствующее описанному выше отображению, удовлетворяет условию

$$p(v/y,x) = p(v/y), \quad (10)$$

или $p(v,y,x) = p(y,x)p(v/y)$ для всех $(v,y,x) \in YXV$.

Действительно

$$p(v/y,x)=(v/y)=\begin{cases}1, \text{ если } v=\psi(Y),\\ 0, \text{ если } v\neq\psi(Y).\end{cases} \quad (11)$$

Из условия (10) следует, что

$$I(x,v/y)=\mathbf{log}\left(\frac{p(v/y,x)}{p(v/y)}\right)=0. \quad (12)$$

для всех $(y,x,v)\in YXV$,для которых $p(y,x,v)\neq 0$, и, следовательно, . Тогда

$$I(Y,V;X)=I(Y;X)+I(V;X/Y)=I(Y;X). \quad (13)$$

С другой стороны, в силу неотрицательности $I(Y;X/V)$

$$I(Y,V;X)=I(V;X)+I(Y;X/V). \quad (14)$$

Тогда, как и в доказательстве теоремы о неувеличении средней взаимной информации при преобразованиях [4, 6]

$$I(Y;X)=I(V;X)+I(Y;X/V), \quad (15)$$

или

$$I(Y;X)\geq I(V;X). \quad (16)$$

Рассматривая ансамбль *MXW* и определяя по аналогии как в (10–16), получаем

$$p(w/m,x)=p(w/m). \quad (17)$$

$$p(w/m,x)=(w/m)=\begin{cases}1, \text{ если } w=f(M),\\ 0, \text{ если } w\neq f(M).\end{cases} \quad (18)$$

$$I(X;W/M)=0. \quad (19)$$

$$I(M,W;X)=I(M;X)+I(W;X/M)=I(M;X). \quad (20)$$

$$I(M,W;X)=I(W;X)+I(M;X/W). \quad (21)$$

$$I(M;X)=I(W;X)+I(M;X/W). \quad (22)$$

$$I(M;X)\geq I(W;X). \quad (23)$$

Перепишем (9) с учетом (1)

$$I(X;Y)-I(X;Y/M)\geq I(X;V)-I(X;V/W). \quad (24)$$

Используя (16), запишем (24)

$$I(X;Y)-I(X;V)\geq 0\geq I(X;Y/M)-I(X;V/W). \quad (25)$$

Отсюда исключая левую часть, запишем

$$I(X;V/W)-I(X;Y/M)\geq 0. \quad (26)$$

Расписывая взаимную информацию как разность энтропий, перепишем (26) и (23)

$$\left[H(X/W)-H(X/W,V)\right]-\left[H(X/M)-H(X/M,Y)\right]\geq 0. \quad (27)$$

$$H(X)-H(X/M)\geq H(X)-H(X/W). \quad (28)$$

Отсюда

$$H(X/W)-H(X/M)\geq 0. \quad (29)$$

Подставляя (29) в (27), запишем

$$H(X/W)-H(X/M)\geq 0\geq H(X/W,V)-H(X/M,Y). \quad (30)$$

Отсюда, исключая левую часть, запишем

$$H(X/M,Y)\geq H(X/W,V). \quad (31)$$

Из (29) и свойства не превышения условной энтропии над безусловной [4, 6], запишем

$$H(X/W)\geq H(X/M)\geq H(X/M,Y). \quad (32)$$

Тогда (31) можно переписать в виде

$$H(X/W)\geq H(X/W,V). \quad (33)$$

Истинность (33) определяется свойством непревышения условной энтропии над безусловной [4, 6] и доказывает истинность (24) и (9). Равенство в (9) имеет место в том случае, когда $I(Y;X/V)=0$ и $I(M;X/W)=0$ (см. (15) и (22)). Очевидно, что первое равенство выполняется, если для всех *(x, y,v) XYV*

$$p(y/x,v)=p(y/v). \quad (34)$$

Условие (34) означает, что при выбранном $v\in V$ сообщение $y\in Y$ не зависит от $x\in X$. Условие выполняется, если v однозначно определяет y и, если отображение $\psi(\bullet)$ обратимо. Второе равенство выполняется, если для $(x,m,w)\in XMW$

$$p(m/x,w)=p(m/w). \quad (35)$$

Условие (35) означает, что при выбранном $m\in M$ сообщение $w\in W$ не зависит от $x\in X$. Условие выполняется, если сообщения m и w однозначно определяют друг друга и, следовательно, если $f(\bullet)$ обратимо.

Рассмотрим взаимную информацию ансамбля $\{XYMVW, p(x,y,m,v,w)\}$.

$$I(X;(Y,M),(V,W)) = I(X;V,W) + I(X;Y,M/V,W) = \\ = I(X;Y,M) + I(X;V,W/Y,M). \quad (36)$$

Совместное выполнение (10) и (17) определяют равенство нулю $I(X;V,W/Y,M)=0$. Тогда с использованием (36) можно записать

$$I(X;V,W) \geq I(X;Y,M). \quad (37)$$

Совместное выполнение условий обратимости $\psi(\bullet)$ и $f(\bullet)$ (см. (34) и (35)) определяет $I(X;Y,M/V,W)=0$. С использованием (37) запишем

$$I(X;V,W) = I(X;Y,M). \quad (38)$$

Согласно (1) можно записать

$$F(X;V;W) = I(X;V) + I(X;W) - I(X;V,W), \quad (39)$$

$$F(X;Y;M) = I(X;Y) + I(X;M) - I(X;Y,M). \quad (40)$$

Выполнение (34–35) определяет равенства в (16), (33), (38). Тогда с использованием (39) и (40) можно записать $F(X;V;W) = F(X;Y;M)$. Теорема доказана.

Заметим, что в теореме доказано нечто большее, чем утверждается. А именно, доказано, что неравенство (24) имеет место не только при детерминированных отображениях $\psi(\bullet)$ и $f(\bullet)$, но и при произвольных случайных отображениях для которых выполнены условия (10) и (17). Никакая обработка наблюдений не может увеличить средней СИ об объекте. Информация сохраняется, если преобразование обратимо. Очевидно, что теорема остается верной в тех случаях, когда преобразование осуществляется или над XY или над XM или только над X (Y или M).

5. Свойства перестановок и непревосходства условной СИ.

Лемма. Для модели ДШВК БП выполняются следующие соотношения:

$$F(X;Y;M) = F(Y;M;X) = F(M;X;Y),$$

$$F(X;Y;M) \geq F(X;Y;M/Z). \quad (41)$$

Доказательство. Докажем истинность первого равенства. Согласно (1) запишем

$$F(Y;M;X) = I(Y;M) - I(Y;M/X) = \\ = I(Y;M) - [H(Y/X) - H(Y/X,M)] = I(Y;M).$$

В (41) учтено, что энтропия $H(Y/X,M) = H(Y/X)$ при фиксированном ансамбле X ансамбли Y и M независимы. Подобно можно показать, что $F(M;X;Y) = I(Y;M)$, тогда учет (4) из утверждения 1 завершает доказательство.

В целях доказательства истинности второго неравенства рассмотрим $F(Y;M;(X,Z))$ с использованием свойства аддитивности СИ (см. (3)), запишем

$$F(Y;M;(X,Z)) = F(Y;M;X) + F(Y;M;Z/X) = \\ = F(Y;M;Z) + F(Y;M;X/Z). \quad (42)$$

Учтем, что $F(Y;M;Z/X)=0$, т.к. при фиксированном X ансамбли Y и M независимы. Тогда, используя свойство перестановок, перепишем (42) и завершим доказательство $F(X;Y;M) = F(X;Y;M/Z) + F(Y;M;Z)$. Лемма доказана.

Заключение

Основные результаты статьи заключаются доказательном определении свойств СИ: аддитивности, тождества СИ ДШВК БП и взаимной информации сообщений на выходах канала, границы изменения СИ, неувеличения СИ при преобразованиях, свойства перестановок и не превосходства условной СИ. Анализ свойств показывает, что часть их коррелирована с свойствами известной ИМ взаимной информации [4, 6], а другая часть имеет новизну, связанную с особенностями передачи сообщения по ДШВК БП. Совокупность полученных результатов исследования совместной информации позволяют сделать вывод о том, что создаются условия для доказательства прямой и обратной теорем кодирования в ДШВК БП, чтобы получить точные оценки пропускной способности разработанной модели канала.

Литература

1. Синюк, А. Д. Совместная информация трех ансамблей сообщений дискретного широковещательного канала связи без памяти / А.Д. Синюк // Информация и Космос. – 2010. – № 1. – С. 27–31.

2. Остроумов, О. А. Протокол открытого формирования трехстороннего ключа / О.А. Остроумов, А.Д. Синюк // Наукоемкие технологии в космических исследованиях Земли. – 2014. – Т. 6, вып. 2. – С. 48–52.

3. Пат. № 2480923 Российская Федерация, МПК: H 04 L 9/00. Способ формирования ключа шифрования/дешифрования / А. Д. Синюк [и др.]; заявитель и патентообладатель ФГВОУ ВПО «Военная академия связи им. Маршала Советского Союза С. М. Буденного»; № 2180469; заявл. 21.02.2012; опубл. 27.04.2013, Бюл. № 12. – 40 с.

4. Чисар, И. Теория информации: теоремы кодирования для дискретных систем без памяти [: пер. с англ.] / И. Чисар, Я. Кернер.– М.: Мир, 1985. – 400 с.

5. Синюк, А. Д. Формирование трехстороннего шифр-ключа по открытым каналам связи с ошибками: монография / А.Д. Синюк. – СПб.: Военная Академия связи, 2009. – 360 с.

6. Галлагер, Р. Теория информации и надежная связь / Р. Галлагер ; пер. с англ под ред. М. С. Пинскера и Б. С. Цыбакова. – М.: «Советское радио», 1974. – 720 с.

7. Фано, Р. Передача информации. Статистическая теория связи / Р. Фано ; пер. И. Овсеевич, Р. Добрушин. – М.: Мир, 1965 – 440 с.