ЧЕБЫШЕВСКИЙ СБОРНИК
Том 22. Выпуск 1.

УДК 519.724.2 DOI 10.22405/2226-8383-2021-22-1-133-151

Критерий существования корректного протокола в канале частичного стирания

И. Б. Казаков

Илья Борисович Казаков — Московский государственный университет им. Ломоносова (г. Москва).
e-mail: i_b_kazakov@mail.ru

Аннотация

Скрытые каналы позволяют передавать информацию с использованием механизмов, изначально не предназначенных для передачи. В качестве примера можно рассмотреть процесс, в рамках которого передатчик передвигает своего персонажа в многопользовательской игре, кодируя информацию движениями, а приемник считывает сообщение, отслеживая перемещения. При этом в канале могут возникать ошибки, связанные с пропаданием персонажа из области видимости приемника и потерей сетевых пакетов. Естественным образом возникает задача организации надежного канала. В работе рассматривается формальная модель канала частичного стирания, описывающая процесс взаимодействия приемника и передатчика, вводится понятие корректности протокола передачи, формулируется и доказывается критериальное условие корректности протокола передатчика, а также строится оптимальное поведение приемника.

Ключевые слова: скрытый канал, канал частичного стирания, протокол передачи информации

Библиография: 25 названий.

Для цитирования:
И. Б. Казаков. Критерий существования корректного протокола в канале частичного стирания // Чебышевский сборник, 2021, т. 22, вып. 1, с. 133–151.

CHEBYSHEVSKII SBORNIK
Vol. 22. No. 1.

UDC 519.724.2 DOI 10.22405/2226-8383-2021-22-1-133-151

Criterion for the existence of a consistent protocol in a partial erasure channel

I. B. Kazakov

Ilya Borisovich Kazakov — Lomonosov Moscow State University (Moscow).
e-mail: i_b_kazakov@mail.ru

Abstract

Covert channels allow one to transmit information using mechanisms that were not originally intended for transmission. An example is a process in which a transmitter encodes information in moves of a character of a multiplayer game, and a receiver observes the moves and decodes the original message. This channel may be noisy, since the character may fall out of the receiver's sight, a number of network packets may be lost, etc. Thus there emerges a natural problem of ogranizing a reliable channel. We propose a formal model called a partial erasure channel that describes the interaction of a transmitter and a receiver, introduce the notion of a consistent transmission protocol, formulate and prove the consistency criterion on the transmitting side and construct the optimal receiver for the given consistent transmitter.

Keywords: covert channels, partial erasure channels, information transmission protocol

Bibliography: 25 titles.

For citation:
I. B. Kazakov, 2021 "Criterion for the existence of a consistent protocol in a partial erasure channel" , *Chebyshevskii sbornik*, vol. 22, no. 1, pp. 133–151.

1. Введение

В настоящей работе предметом изучения является так называемый канал частичного стирания. Поясним сразу, в чем заключается его суть. Прежде всего, задан некий алфавит символов. Имеются два участника взаимодействия — передающий информацию и принимающий её. Передающего участника, следуя традиции, будем называть Алисой, принимающего, соответственно, Бобом. Алиса отправляет Бобу символ из данного алфавита, а Боб, в свою очередь, получает часть информации об отправленном символе. Определим, что конкретно означает «получение частичной информации»: на исходном алфавите определен некий набор разбиений, или, иначе выражаясь, отношений эквивалентности. В процессе передачи символа выбирается одно из данных отношений. Боб получает следующую информацию: какое именно отношение эквивалентности было выбрано, а также какому классу по данному отношению принадлежал отправленный Алисой символ. Общей задачей Алисы и Боба является корректная и эффективная передача информации по каналу с вышеописанными свойствами. Положим, что имеется также и алфавит «исходных символов», а у Алисы и Боба есть соответственно входная и выходная ленты. На входной ленте Алисы предварительно напечатаны символы указанного алфавита, а Боб может печать на выходной ленте символы из этого же алфавита. Зарезервируем специальный символ, который называется символом стирания. Этот символ имеет смысл «информация потеряна». Дозволим Бобу печатать также и его на выходной ленте.

Вышесказанное позволяет определить, что такое «корректность» передачи: совместное поведение Алисы и Боба, называемое протоколом, корректно, если в результате работы на выходной ленте отпечатывается то же самое, что было изначально напечатано на входной, при этом, может быть, заменяя некоторые символы на символ стирания. Таким образом, возникает задача построения корректного протокола. Точнее выражаясь, указанная задача, в том виде, в котором она решается в настоящей работе, формулируется следующим образом. Пусть поведение Алисы определено. Тогда требуется определить поведение Боба таковое, что в паре с ним данное поведение Алисы образует корректный протокол. Однако, не для всякого поведения Алиса соответствующее поведение Боба существует. Таким образом, следует определить, каким свойством должно обладать поведение Алисы, чтобы существовало поведение Боба, в паре с которым оно составляет корректный протокол. В настоящей работе будет изложена формализация представленных понятий, а также доказаны соответствующие теоремы, которые и являются ответами на эти вопросы. Однако перед указанным изложением, следует

предварительно представить сведения о контексте настоящего исследования, т.е. обосновать его актуальность.

Во-первых, начальным пунктом является теория скрытых каналов. Скрытым канал — это коммуникационный канал, пересылающий информацию методом, который изначально не был для этого предназначен. Исторически первой работой, посвященной теории скрытых каналов, является статья [15]. Современный краткий обзор, посвященный скрытым каналам и их классификации имеется в [17], [19]. Следует упомянуть также о двух отечественных обзорных статьях [9], [1].

Скрытые каналы, как правило, [16] делятся на два типа: скрытые каналы по памяти и скрытые каналы по времени. Суть скрытого канала по памяти заключается в том, что один процесс записывает в некую информацию в хранилище, а другой процесс её прямо или косвенно считывает. Скрытый канал по времени характеризуется доступом отправителя и получателя к одному и тому же процессу или изменяемому во времени атрибуту.

В связи со стремительным ростом использования сети Интернет, в настоящее время особенно важны сетевые скрытые каналы. Упомянем некоторые способы, которым может быть организован скрытый канал в стеке протоколов TCP/IP. Во-первых, имеется модуляция значений полей заголовков пакетов, например, полей TTL [23], IP ID [10], ToS [14]. Другой способ заключается в изменении длин передаваемых пакетов и освещен, например, в работе [2]. Скрытые каналы по времени в IP-сетях могут быть построены путем изменения длин межпакетных интервалов [11], [20], и при помощи изменения скорости передачи пакетов [22]. Достаточно полный обзор и классификацию указанных каналов можно найти в работах [24], [21] соответственно.

Сетевые каналы по времени, как правило, всегда зашумлены, так как время следования пакета — случайная величина, распределение которой зависит от нагрузки на сеть [12]. В целях максимизации пропускной способности в условиях зашумления могут применяться [13] коды, исправляющие ошибки. Решению указанной задачи посвящен цикл работ [3], [4], [5], [6], [7], [8] автора, в который входит также и данная статья.

Выражаясь более определенным образом, предмет настоящего исследования связан с так называемым скрытым каналом блужданий по плоскости, возможность построения которого предоставляют многопользовательские online-игры. Этот скрытый канал также может быть отнесен к сетевым скрытым каналам, однако в отличие от упомянутых выше, относится не транспортному, а к прикладному уровню модели OSI.

Сделаем необходимые пояснения. В рассматриваемом классе игр имеется плоскость, на которой расположены игровые сущности. Сервер хранит местоположения этих сущностей на плоскости, т.е. их координаты. Предполагается также, что у каждого игрока, т.е. подключенного к серверу клиента, имеется сущность, поведением которой он может управлять. Как правило, данная сущность называется игровым персонажем. Один из клиентов передает серверу команды о перемещении управляемого им персонажа по плоскости, а другие клиенты могут получать от сервера данные о местоположении (и, следовательно, также об изменениях местоположения) данного игрового персонажа. Согласно представленному описанию, канал блужданий по плоскости относится к скрытым каналам по времени. Ранее задача построения скрытых каналов через online-шутеры исследовалась в статье [25]. Под online-играми могут пониматься не только «шутеры от первого лица», но также и игры с произвольной механикой. Упомянем, что построению скрытого канала в отмеченном общем случае посвящена, например, статья [18].

Однако, в упомянутых выше работах не рассматривается вопрос возможных ошибок, совершаемых при передаче информации, и обеспечения отказоустойчивости построяемого скрытого канала. Предполагалось, что каждый клиент получает от сервера информацию обо всех последовательных состояниях игры. Применительно к блужданиям по плоскости это означает

получение сведений о местоположении всех других (точнее, находящихся в зоне видимости) игроков на плоскости во все моменты времени. В реальных условиях сформулированое предположение не соблюдается в силу переменности задержки между отправкой данных сервером и их получением клиентом, а также потому что сервер не обязан отправлять их на каждом такте. Таким образом, часть информации теряется, и клиент получает сведения о местоположениях прочих игроков лишь в некоторые моменты времени. Как следствие, возникает задача построения скрытого канала именно в условиях потери и/или зашумления информации.

Опишем способ передачи информации посредством блужданий по плоскости. Имеется игровое поле и два игрока: первый игрок движется по полю, а второй — наблюдает движение первого. Относительно этих движений принято следующее. Во-первых, время принимается дискретным, т.е. состоящим из последовательных тактов. Во-вторых, полагаем, что Алиса движется только лишь вдоль конечного числа направлений, отстоящих друг от друга на равные углы, причем может менять направление своего движения на каждом такте. Таковые допущения естественны в силу того, что в реальности может передаваться только лишь конечный объем информации. Подразумевается, что она «всегда движется», т.е. не может покоиться. В третьих, скорость движения Алисы постоянна. Также зафиксируем некое «начальное местоположение».

Таким образом, как это было показано в [3], фактически Алиса движется по некоторому счетному графу местоположений G_{loc}, на каждом такте переходя в смежную вершину. Далее, зафиксируем число N и рассмотрим множество путей длины N в G_{loc}, начинающихся в ранее упомянутой начальной точке. Таковые пути будем называть траекториями.

На протяжении N тактов Алиса движется по некоторой траектории, т.е. проходит последовательно N соответствующих местоположений. Боб, в свою очередь, посредством анализа получаемых с сервера данных, на протяжении этих же N тактов считывает местоположения Алисы. Полагаем, что Бобу удается считать местоположения Алисы не на всех прошедших тактах $\{1, 2, ..., N\}$, а только лишь на некоторых из них, т.е. на подмножестве $T \subseteq \{1, 2, 3, ...N\}$.

Для двух выбранных траекторий будем говорить, что они пересекаются на i-м такте, если на данном также совпадают соответствующие местоположения Алисы. Выбор множества T тактов задает разбиение (или, иначе выражаясь, отношение эквивалентности) на множестве траекторий: две траектории считаются эквивалентными, если они пересекаются на всех тактах $i \in T$, т.е если Боб не может в этом случае отличить их друг от друга. Таким образом, соответственно подмножествам $\{1, 2, ..., N\}$, на траекториях определено 2^N разбиений. Кроме того, разбиению, соответствующему множеству T, возможно приписать вероятность p_T того, что Боб «увидит Алису именно на тактах из T».

Далее, посредством абстрагирования от самих траекторий и конкретных определенных на них разбиений, была получена формальная модель, называемая структурой частичного стирания. Соответственно, имеется также канал частичного стирания, которой, таким образом, является «надстроенным» над каналом блужданий по плоскости. И, следовательно, можно говорить о протоколах передачи информации в указанном канале. В [4] рассматривался определенный класс таковых протоколов, называемый «схемой равномерного кодирования». Однако, как будет видно из дальнейшего формализованного изложения, указанный класс не исчерпывает собой все возможные протоколы. В настоящей работе изучен общий случай и тем самым решена поставленная в [4] задача.

Представим структуру дальнейшего изложения. В следующем разделе 2 вновь изложим введенные в предшествующей работе [3] понятия структуры частичного стирания и равномерного кодирования, а также произведем требуемое обобщение понятия протокола. Раздел 3 посвящен полученным результатам исследования, доказательства которых представлены в разделе 4. В заключительном разделе 5 подведены итоги и поставлены задачи для дальнейших исследований.

2. Основные определения и обозначения

Введенное выше множество траекторий Алисы обозначается как A. Множество всех слов в алфавите A, т.е. множество конечных последовательностей символов из A, (включая, в том числе, и пустую последовательность) обозначается как A^*.

Определение 1. *Структура частичного стирания — тройка, состоящая из алфавита A, множества определённых на нем разбиений (отношений эквивалентности) $\mathfrak{T}$, а также приписанных данным разбиениям неотрицательных весов p_T, сумма которых принимается равной 1.*

Опишем теперь канал частичного стирания. Алиса отправляет Бобу символ $a \in A$. Боб получает лишь часть информации об отправленном символе: выбранное отношение эквивалентности T, а также класс $\pi_T(a)$ по данному отношению. Множество всех пар $(\pi_T(a), T)$ обозначается как алфавит Боба B.

Определение 2. *Для символов $a \in A$, $b \in B$ полагаем $a \mapsto b$, если в структуре частичного стирания имеется разбиение T такое, что $b = (\pi_T(a), T)$. Также, для слов $\alpha \in A^*, \beta \in B^*$ полагаем $\alpha \mapsto \beta$, если $|\alpha| = |\beta| = l$ и для всех $i = 1...l$ выполнено $\alpha(i) \mapsto \beta(i)$.*

У Алисы есть входная лента, а у Боба, соответственно, выходная лента. На входной ленте находятся символы некоторого алфавита S, которые считывает Алиса. Боб печатает на выходную ленту те же символы из S плюс ещё один специальный символ $*$. Предполагается, что множество S конечно и не содержит само символа $*$. Общая цель как Алисы, так и Боба состоит в том, чтобы отпечатать на выходной ленте ту же самую последовательность символов, что и имеющуюся на входной ленте изначально, при этом, может быть, заменяя некоторые символы алфавита S на $*$.

Представим также описание вышеупомянутой схемы «равномерного кодирования». Прежде всего, зафиксировано некое число n — длина кодового слова.

Определение 3. *Равномерный код — это инъективное отображение $K : S \to A^n$, т.е. каждому символу $s \in S$ поставлено в соответствие кодовое слово α_s, $|\alpha_s| = n$*

Алиса, прочитав с ленты очередной символ $s \in S$, в течение последующих n тактов выбрасывает слово α_s, т.е. последовательно высылает по каналу символы $\alpha_s(1), ..., \alpha_s(n)$. Боб же в свою очередь, на протяжении этих тактов последовательно получает символы $\beta(1)...\beta(n)$, такие что $\beta(i) = (\pi_{T_i}(\alpha(i)), T_i)$, где T_i — разбиение, выбранное на i-ом такте. Иначе говоря, совокупно Боб получает слово $\beta = \beta(1)...\beta(n)$, для которого $\alpha \mapsto \beta$.

Получив слово β, Боб принимает решение относительно того, какой именно символ из множества $S \cup \{*\}$ ему следует отпечатать на выходной ленте. Возможны два случая. Если имеется только один символ $s \in S$ такой, что $\alpha_s \mapsto \beta$, то именно его и следует отпечатать. Иначе, т.е. если таковых имеется несколько, то следует напечатать символ стирания $*$. Отдельно отметим, что существование хотя бы одного такого $s \in S$, для которого $\alpha_s \mapsto \beta$, гарантировано вышеопределенным поведением Алисы.

Таким образом, схема равномерного кодирования надстраивает поверх канала частичного стирания так называемый канал полного стирания. Соответствующая ему структура полного стирания — это некий алфавит A', каждому символу которого приписана вероятность его замены на символ стирания $*$ в процессе передачи по указанному каналу. A' — это ничто иное, как множество кодовых слов α_s, $s \in S$. Упомянутые вероятности, в свою очередь, определяются входящими в состав структуры частичного стирания вероятностями p_T.

Легко заметить, что рассмотренная схема «равномерного кодирования» не исчерпывает множества всех возможных протоколов, так как были приняты два упрощающих предположения. Во-первых, выбрасываемое Алисой слово не зависит от предыстории чтения с ленты,

а во-вторых, выбрасываемые слова имеют одинаковую длину для всех символов $s \in S$. И, следовательно, если эти предположения отбросить, то естественным образом получается общее понятие протокола. В качестве соображения, обосновывающего рассмотрение также и неравномерного кода, скажем, что ожидается уменьшение средней длины выбрасываемого слова (и, следовательно, увеличение пропускной способности) в случае неравномерного распределения частот встречаемости символов алфавита S на входной ленте.

Определение 4. *Протокол — это пара (F, G), состоящая из функции поведения Алисы $F : S^* \to A^*$ и функции поведения Боба $G : B^* \to S \cup \{*, \Lambda\}$. Наложено ограничение: $G(\Lambda) = \Lambda$*

Замечание 1. *Следует обратить внимание, что одно и то же обозначение «Λ» используется как для «пустого символа», так и для пустых слов (т.е. слов длины 0), которые являются элементами множеств A^*, B^*, S^*. Конкретный его смысл всегда будет ясен из контекста.*

Представим сведения, относящиеся к интерпретации введенных выше функций поведения. Пусть Алиса только что прочитала с входной ленты очередной символ $s \in S$, предварительно уже считав слово $\hat{s} = s_1 ... s_m$. Тогда считаем, что Алиса выбрасывает слово $F(\hat{s}s)$. До первого чтения с ленты Алиса выбрасывает $F(\Lambda)$. Что касается Боба, то на каждом такте он получает некий символ $b \in B$. Получив указанный символ, он должен принять решение о том, что печатать на выходной ленте: или какой-нибудь символ из $s \in S \cup \{*\}$, или же ничего не печатать. Полагаем, что если $G(\beta) \in S \cup \{*\}$, то Боб и печатает $G(\beta)$. Иначе, т.е. если $G(\beta) = \Lambda$, то Боб ничего не печатает.

В целях удобства изложения определим также производные функции $\hat{F}$, $\hat{G}$:

Определение 5. *Пусть $\hat{s} = s_1 ... s_m$. Тогда полагаем:*
$\hat{F}(\hat{s}) = F(\Lambda)F(s_1)F(s_1 s_2)...F(s_1 ... s_m)$
Для слова $\beta = b_1 ... b_n$ аналогично:
$\hat{G}(\beta) = G(\Lambda)G(b_1)G(b_1 b_2)...G(b_1 ... b_n)$

При этом относительно конкатенации с «пустым символом» Λ принимается: $\hat{s}\Lambda = \hat{s}$, $\Lambda\hat{s} = \hat{s}$

В дальнейшем часто будет использоваться свойство функции $\hat{G}$, непосредственно очевидное из представленного определения:

Утверждение 1. *Пусть β_1 — префикс β_2. Тогда также $\hat{G}(\beta_1)$ — префикс $\hat{G}(\beta_2)$.*

3. Результаты

Распространим на общий случай упомянутое ранее требование корректности «отпечатать на выходной ленте то же самое содержание, каковое имеется изначально на входной, при этом, может быть, заменяя некоторые символы алфавита S на символ стирания $*$». Для его формализации понадобится определить на словах из $(S \cup \{*\})^*$ соответствующий частичный порядок.

Определение 6. *Для слов $\hat{s}_1, \hat{s}_2 \in (S \cup \{*\})^*$ полагаем $\hat{s}_1 \preceq \hat{s}_2$, если выполнено $|\hat{s}_1| = |\hat{s}_2|$, и слово $\hat{s}_1$ может быть получено из слова $\hat{s}_2$ посредством замены некоторых его символов на символ частичного стирания $*$.*

Определение 7. *Протокол (F, G) называется корректным, если для всех слов $\hat{s} \in S^*$, $\beta \in B^*$ из выполнения $\hat{F}(\hat{s}) \mapsto \beta$ следует выполнение $\hat{G}(\beta) \preceq \hat{s}$. В целях удобства дальнейшего изложения, если (F, G) — корректный протокол, то будем также говорить, что функция поведения Боба G согласована с функцией поведения Алисы F.*

Указанное выше условие корректности накладывается на все такие слова β, для которых найдется $\hat{s} \in S^*$ такое, что $\hat{F}(\hat{s}) \mapsto \beta$. Обозначим их множество как H_F.

Пусть дана произвольная функция поведения Алисы $F : S^* \to A^*$. Первый вопрос, рассматриваемый в настоящей работе, формулируется следующим образом: «существует ли для данной функции поведения Алисы F согласованная с ней функция поведения Боба G».

Предположим, что ответ на данный вопрос положителен. В этом случае таковых функций поведения Боба может быть несколько: т.е. могут иметься две функции G_1, G_2, согласованных с G.

На множестве согласованных с F функций возможно определить частичный порядок, означающий, что одно поведение «лучше» другого. Это означает, что «худшее» поведение отпечатывает на выходной ленте то же самое, что и «лучшее», заменяя, может быть, некоторые символы на символ стирания $*$. Выражаясь более формально, для предварительно зафиксированной F и согласованных с ней G_1, G_2 полагаем $G_1 \preceq G_2$, если для всех $\beta \in H_F$ выполнено $G_1(\beta) \preceq G_2(\beta)$.

Достаточно очевидно, что если имеется «лучшее» поведение, то для передачи информации следует использовать именно его, а не «худшее». Таким образом, вторым рассматриваемым вопросом является существование среди всех поведений Боба наилучшего, т.е. максимального по отношению $\preceq$.

Определение 8. *Функция поведения Алисы F называется правильной, если из выполнения $\hat{F}(\hat{s}_1) \mapsto \beta_1$, $\hat{F}(\hat{s}_2) \mapsto \beta_2$, β_1 — префикс β_2 следует выполнение $|\hat{s}_1| \leqslant |\hat{s}_2|$*

Выразим представляемые в настоящей работе результаты в виде следующих теорем:

Теорема 1. *Пусть (F, G) — корректный протокол. Тогда F — правильная функция.*

Теорема 2. *Пусть F — правильная функция. Тогда существует функция G^F_{best} такая, что:*
1) (F, G^F_{best}) — корректный протокол.
2) Пусть (F, G) — корректный протокол. Тогда для любого слова $\beta \in H_F$ выполнено $G(\beta) \preceq G^F_{best}(\beta)$.

Следствие 1. *Таким образом, для заданной функции поведения Алисы F существует согласованная с ней функция поведения Боба G тогда и только тогда, когда F правильна.*

Замечание 2. *В число результатов исследования входит не только лишь факт существования наилучшего протокола, то также и его конкретное однозначное описание. Однако, поскольку данное описание требует некоторых вспомогательных понятий и утверждений, то определение G^F_{best} будет представлено в подразделе 4.4.*

Замечание 3. *Упомянутое ранее «равномерное кодирование» является, очевидно, частным случаем корректного протокола.*

4. Доказательства

Изложим доказательства представленных результатов. Теорема 1 доказывается в подразделе 4.1. В подразделах 4.2, 4.3 представлены вспомогательные понятия и утверждения, необходимые для осуществленного в подразделе 4.4 построения функции поведения Боба G^F_{best}, а также проверки соответствующих свойств, указанных в условии теоремы 2.

Отдельно отметим, что в подразделах 4.2 — 4.4 функция поведения Алисы F зафиксирована, а также считается правильной.

4.1. Доказательство теоремы 1

Утверждение 2. *Пусть (F, G) — корректный протокол. Тогда F — правильная функция.*

Доказательство.
1. Зафиксируем слова $\hat{s}_1, \hat{s}_2 \in S^*$, для которых найдутся $\beta_1, \beta_2 \in B^*$ такие, что β_1 — префикс β_2, $\hat{F}(\hat{s}_1) \mapsto \beta_1$, $\hat{F}(\hat{s}_2) \mapsto \beta_2$. Согласно определению правильной функции, необходимо доказать выполнение $|\hat{s}_1| \leqslant |\hat{s}_2|$.
2. Так как (F, G) — корректный протокол, то $\hat{G}(\beta_1) \preceq \hat{s}_1$, $\hat{G}(\beta_2) \preceq \hat{s}_2$, откуда немедленно следует $|\hat{G}(\beta_1)| = |\hat{s}_1|$, $|\hat{G}(\beta_2)| = |\hat{s}_2|$.
3. Согласно утверждению 1, выполнение β_1 — префикс β_2 влечет за собой выполнение $\hat{G}(\beta_1)$ — префикс $\hat{G}(\beta_2)$. И, следовательно, $|\hat{G}(\beta_1)| \leqslant |\hat{G}(\beta_2)|$.
4. Сопоставляя выводы п.2 и п.3, получаем требуемое: $|\hat{s}_1| = |\hat{G}(\beta_1)| \leqslant |\hat{G}(\beta_2)| = |\hat{s}_2|$

□

Теорема 1 доказана.

4.2. Правильные функции и их свойства

Данный подраздел посвящен изучению свойств предварительно зафиксированной правильной функции F. В 4.2.1 определена функции длин l_F. В 4.2.2 введено понятие элементарного отрезка. Наконец, в 4.2.3 представлено разбиение множества H_F на непересекающиеся классы.

4.2.1. Функция l_F

От правильной функции F возможно абстрагировать целочисленную функцию длин l_F, определенную на словах из H_F.

Утверждение 3. *Пусть F — правильная функция поведения Алисы. Тогда корректно определена функция длин функция длин $l_F : H_F \to \mathbb{Z}_+$, для которой выполняется $\hat{F}(\hat{s}) \mapsto \beta \Rightarrow l_F(\beta) = |\hat{s}|$*

Доказательство.
Действительно, пусть $\hat{F}(\hat{s}_1), \hat{F}(\hat{s}_2) \mapsto \beta$. Тогда, согласно определению правильной функции, одновременно выполнено $|\hat{s}_1| \leqslant |\hat{s}_2|$ и $|\hat{s}_2| \leqslant |\hat{s}_1|$, т.е. выполнено $|\hat{s}_1| = |\hat{s}_2|$.

И, следовательно, для всех слов $\beta \in H_F$ значение $l_F(\beta)$ определено однозначно. □

Определенная таковым образом функция l_F является «возрастающей»:

Утверждение 4. *Пусть $\beta_1, \beta_2 \in H_F$, β_1 — префикс β_2. Тогда $l_F(\beta_1) \leqslant l_F(\beta_2)$*

Доказательство.
1. Пусть $\hat{F}(\hat{s}_1) \mapsto \beta_1$, $\hat{F}(\hat{s}_2) \mapsto \beta_2$.
2. Так как β_1 — префикс β_2, то $|\hat{s}_1| \leqslant |\hat{s}_2|$ согласно определению правильности для функции F.
3. Далее, применяя утверждение 3, получаем: $l_F(\beta_1) = |\hat{s}_1| \leqslant |\hat{s}_2| = l_F(\beta_2)$.
ч.т.д.

□

Установим также связь с поведением Боба, входящим в соответствующий корректный протокол.

Утверждение 5. *Пусть (F, G) — корректный протокол, $\beta \in H_F$. Тогда $|G(\beta)| = l_F(\beta)$*

Доказательство.
Действительно, найдется $\hat{s}$ такое, что $\hat{F}(\hat{s}) \mapsto \beta$. И, следовательно, $l_F(\beta) = |\hat{s}|$. По определению корректности протокола, $\hat{G}(\beta) \preceq \hat{s}$, а значит $|\hat{G}(\beta)| = |\hat{s}| = l_F(\beta)$ □

4.2.2. Элементарные отрезки

Слово β_1 будем называть строгим префиксом слова β_2, если β_1 — префикс β_2, но при этом $\beta_1 \neq \beta_2$.

Определение 9. *Пусть β_1 — строгий префикс β_2. Отрезок $(\beta_1, \beta_2]$ — это множество слов β таких, что β_1 — строгий префикс β, а β — префикс β_2*

Пусть теперь имеется множество слов $H \subseteq B^*$, а также определенная на данном множестве целочисленная функция $l : H \to \mathbb{Z}_+$

Определение 10. *Отрезок $(\beta_1, \beta_2]$ называется элементарным в контексте функции $l : H \to \mathbb{Z}_+$, если $\beta_1, \beta_2 \in H$, а также из $\beta' \in (\beta_1, \beta_2]$ и $\beta' \neq \beta_2$ следует $\beta' \notin H$.*

Элементарные отрезки делятся на классы в соответствии с тем, на какую величину возрастает соответствующая функция l на их протяжении.

Определение 11. *Элементарный отрезок в контексте функции l называется n - элементарным, если выполнено $l(\beta_2) = l(\beta_1) + n$*

Представим также некоторые утверждения технического характера, на которые будут ссылаться дальнейшие рассуждения.

Утверждение 6. *Пусть имеются два отрезка $(\beta_1, \beta_2], (\beta_3, \beta_4]$ такие, что $\beta_2 \in (\beta_3, \beta_4]$. Пусть отрезок $(\beta_1, \beta_2]$ — элементарен в контексте $l : H \to \mathbb{Z}_+$, а также $\beta_3, \beta_4 \in H$. Тогда выполнено $(\beta_1, \beta_2] \subseteq (\beta_3, \beta_4]$*

Доказательство.
1. По условию, β_1 — префикс β_2, β_2 — префикс β_4. Следовательно, β_1 — префикс β_4.
2. По условию также β_3 — префикс β_4, откуда следует что или β_1 — строгий префикс β_3, или β_3 — префикс β_1.
3. Предположим, что β_1 — строгий префикс β_3. Так как по условию β_3 — строгий префикс β_2, то это означает, что $\beta_3 \in (\beta_1, \beta_2]$ и $\beta_3 \neq \beta_2$.
4. Однако, $\beta_3 \in H$, что противоречит элементарности отрезка $(\beta_1, \beta_2]$. Таким образом, предположение предыдущего пункта ложно, и, следовательно, β_3 — префикс β_1.
5. Зафиксируем теперь слово $\beta' \in (\beta_1, \beta_2]$. Следует доказать, что выполнено $\beta' \in (\beta_3, \beta_4]$
6. β_1 — строгий префикс β', β_3 — префикс β_1 (п.4). Следовательно, β_3 — строгий префикс β'.
7. β' — префикс β_2, β_2 — префикс β_4 (см. п.1). Следовательно, β' — префикс β_4.
8. Сопоставляя выводы п.6 и п.7, получаем требуемое.
□

Утверждение 7. *Пусть для слов $\hat{s}s \in S^*$, $\beta \in B^*$ выполнено $\hat{F}(\hat{s}s) \mapsto \beta$. Тогда существует β' такое, что $\hat{F}(\hat{s}) \mapsto \beta'$, β' — строгий префикс β.*

Доказательство.
1. В первую очередь заметим, что $\hat{F}(\hat{s}s) = \hat{F}(\hat{s})F(\hat{s}s)$. Далее будем обозначать $\alpha_1 = \hat{F}(\hat{s})$, $\alpha_2 = F(\hat{s}s)$. Примем также обозначение для длин: $|\alpha_1| = k_1$, $|\alpha_2| = k_2$
2. Так как $\alpha_1\alpha_2 \mapsto \beta$, то $|\beta| = k_1 + k_2$. Соответственно, β разделяется на два слова: $\beta = \beta'\beta''$, причем $|\beta'| = k_1$, $|\beta''| = k_2$
3. При этом достаточно очевидно, что $\hat{F}(\hat{s}) = \alpha_1 \mapsto \beta'$, $F(\hat{s}s) = \alpha_2 \mapsto \beta'$.
4. Предположим, что $\beta' = \beta$. Тогда $\hat{F}(\hat{s}), \hat{F}(\hat{s}s) \mapsto \beta$. Так как слово β — префикс самого себя, то из правильности F заключаем, что выполнено $|\hat{s}| + 1 = |\hat{s}s| \leqslant |\hat{s}|$. Противоречие. □

4.2.3. Разбиение множества H_F

Изучим теперь вопрос о том, какие элементарные отрезки имеются в контексте введенной выше функции $l_F : H_F \to \mathbb{Z}_+$.

Утверждение 8. *В контексте функции $l_F : H_F \to \mathbb{Z}_+$ элементарные отрезки могут быть или 0-элементарными, или 1-элементарными.*

Доказательство.
1. Пусть $(\beta_1, \beta_2]$ — n-элементарный отрезок в контексте l_F. Согласно утверждению 4, l_F неубывает, т.е. выполнено $n = l_F(\beta_2) - l_F(\beta_1) \geqslant 0$.
2. Так как $\beta_1, \beta_2 \in H_F$, то найдутся такие слова $\hat{s}_1, \hat{s}_2 \in S^*$, что $\hat{F}(\hat{s}_1) \mapsto \beta_1$, $\hat{F}(\hat{s}_2) \mapsto \beta_2$. И, следовательно, $|\hat{s}_2| = l_F(\beta_2) = l_F(\beta_1) + n = |\hat{s}_1| + n$.
3. Предположим теперь, что $n \geqslant 2$. Немедленно получаем, что $|\hat{s}_2| \geqslant 2$
4. И, следовательно, возможно положить $\hat{s}_2 = \hat{s}'_2 s_2$, $s_2 \in S$. Согласно утверждению 7, найдется слово β' такое, что $\hat{F}(\hat{s}'_2) \mapsto \beta'$, β' — строгий префикс β_2. Кроме того, $l_F(\beta') = |\hat{s}'_2| = |\hat{s}_2| - 1 = |\hat{s}_1| + n - 1 > |\hat{s}_1| = l_F(\beta_1)$.
5. Слова β_1, β' оба суть префиксы β_2. Следовательно, возможны два случая: или β_1 — строгий префикс β', или β' — префикс β_1.
6. Рассмотрим первый случай: β_1 — строгий префикс β'. Тогда верно $\beta' \in (\beta_1, \beta_2]$. Так как данный отрезок элементарен, а $\beta' \in H_F$, то выполнено $\beta' = \beta_2$, что противоречит п.4.
7. Теперь рассмотрим второй случай: β' — префикс β_1. Тогда, вновь применяя утверждение 4, получаем $l_F(\beta') \leqslant l_F(\beta_1)$, что также противоречит выводу из п.4.
8. Полученные в обоих случаях противоречия показывают, что предположение п.3 ложно. И, следовательно, или $n = 0$, или $n = 1$.

□

Представленное утверждение об элементарных отрезках позволяет разбить множество H_F на три класса. Введем для данных классов следующие обозначения:
$H_F^{00} = \{\beta \in H_F | \hat{F}(\Lambda) \mapsto \beta\}$
$H_F^0 = \{\beta \in H_F | \beta$ — конец 0-элементарного отрезка в контексте $l_F\}$
$H_F^1 = \{\beta \in H_F | \beta$ — конец 1-элементарного отрезка в контексте $l_F\}$

Утверждение 9. $H_F = H_F^{00} \sqcup H_F^0 \sqcup H_F^1$

Доказательство.
I. $H_F = H_F^{00} \cup H_F^0 \cup H_F^1$
1. Пусть дано некое $\beta \in H_F$. Тогда найдется $\hat{s}$ такое, что $\hat{F}(\hat{s}) \mapsto \beta$.
2. Если $\hat{s} = \Lambda$, то это означает, что $F(\Lambda) = \hat{F}(\Lambda) \mapsto \beta$, т.е. $\beta \in H_F^{00}$.
3. В случае, если $\hat{s} = \hat{s}'s$, то согласно утверждению 7 существует $\beta' \in H_F$ — строгий префикс β такой, что $\hat{F}(\hat{s}') \mapsto \beta'$. И, следовательно, среди префиксов β существует и максимальный лежащий в H_F префикс β''.
4. А значит, слово β является концом элементарного в контексте l_F отрезка $(\beta'', \beta]$. Согласно утверждению 8, он может быть только 0-элементарным или 1-элементарным, т.е. $\beta \in H_F^0 \cup H_F^1$
5. Таким образом, осталось только лишь показать, что множества H_F^0, H_F^1, H_F^{00} попарно не пересекаются.
II. $H_F^0 \cap H_F^1 = \emptyset$
1. Предположим, что найдется слово $\beta \in H_F^0 \cap H_F^1$. Тогда таковое β является концом двух элементарных отрезков $(\beta_1, \beta]$ и $(\beta_2, \beta]$. Также отметим, что так как это пара, состоящая из 0-элементарного и 1-элементарного отрезков, то $\beta_1 \neq \beta_2$. Также по определению отрезка $\beta_1, \beta_2 \neq \beta$.

2. И, следовательно, или β_1 — строгий префикс β_2, или β_2 — строгий префикс β_2. В первом случае выполнено $\beta_2 \in (\beta_1, \beta]$, а во втором $\beta_1 \in (\beta_2, \beta]$. Так как отрезки элементарны, то оба случая невозможны. Таким образом, $H_F^0 \cap H_F^1 = \emptyset$.
III. $H_F^{00} \cap (H_F^0 \cup H_F^1) = \emptyset$
1. Предположим теперь, что существует слово $\beta \in H_F^{00} \cap (H_F^0 \cup H_F^1)$. Это означает, что $\hat{F}(\Lambda) \mapsto \beta$, а также что найдется слово β' — строгий префикс β такой, что $(\beta', \beta]$ — элементарный отрезок в контексте l_F.
2. Тогда есть слово $\hat{s}$, для которого $\hat{F}(\hat{s}) \mapsto \beta'$. Согласно определению правильной функции, получаем: $|\hat{s}| \leqslant |\Lambda| = 0$. Таким образом, $\hat{F}(\Lambda) \mapsto \beta'$.
3. Из $\hat{F}(\Lambda) \mapsto \beta$, $\hat{F}(\Lambda) \mapsto \beta'$ следует $|\beta| = |\beta'| = |\hat{F}(\Lambda)|$. И, следовательно, $\beta' = \beta$, что противоречит п.III.1.
4. Таким образом, $H_F^{00} \cap H_F^0 = \emptyset$, $H_F^{00} \cap H_F^1 = \emptyset$. Вместе с выводом II это и означает, что множества H_F^0, H_F^1, H_F^{00} попарно не пересекаются.

□

Установим также связь между множеством H_F^1 и значениями функции l_F.

Утверждение 10. *Каждое слово $\beta \in H_F$ имеет ровно $l_F(\beta)$ префиксов, лежащих в H_F^1.*

Доказательство.
1. Пусть $\beta_0, \beta_1, ..., \beta_m = \beta$ — возрастающая последовательность, состоящая из всех префиксов слова β, лежащих в H_F.
2. Тогда $(\beta_0, \beta_1], ..., (\beta_{m-1}, \beta_m]$ — элементарные отрезки в контексте функции l_F. Будем считать, что среди них имеется n 1-элементарных и $m-n$ 0-элементарных. Среди слов $\beta_0, \beta_1 ... \beta_m$, таким образом, имеется n элементов множества H_F^1.
3. Согласно утверждению 9, так как β_0 не является концом какого-либо элементарного отрезка, то $\beta_0 \in H_F^{00}$, т.е. $\hat{F}(\Lambda) \mapsto \beta_0$. Откуда немедленно следует $l_F(\beta_0) = 0$
4. Подсчитаем: $l_F(\beta) = l_F(\beta_m) - l_F(\beta_0) = l_F(\beta_m) - l_F(\beta_{m-1}) + ... + (l_F(\beta_1) - l_F(\beta_0)) = n$. Действительно, если $(\beta_i, \beta_{i+1}]$ — 1-элементарный отрезок, то $l_F(\beta_{i+1}) - l_F(\beta_i) = 1$. В противном случае, т.е. если данный отрезок 0-элементарен, то $l_F(\beta_{i+1}) - l_F(\beta_i) = 0$

□

4.3. Связанные и приписанные символы

Изучим вопрос о том, какие символы на заданном слове β может печатать функция поведения Боба G, согласованная с функцией поведения Алисы F.

Определение 12. *Будем говорить, что со словом $\beta \in B^*$ связан символ $s \in S$, если найдутся слова $\beta_1, \beta_2 \in B^*$, $\hat{s} \in S^*$ такие, что β_1 — строгий префикс β_2, $\beta' \in (\beta_1, \beta_2]$, $\hat{F}(\hat{s}) \mapsto \beta_1$, $\hat{F}(\hat{s}s) \mapsto \beta_2$*

Определение 13. *Пусть дано некоторое слово $\beta \in B^*$. Определим для него приписанный символ из множества $S \cup \{*, \Lambda\}$ в соответствии со следующими правилами:*

1) Если с β не связан никакой символ, то считаем, что данному слову приписан символ Λ.

2) Если с β связан единственный символ $s \in S$, то считаем, что данному слову этот же символ s и приписан.

3) Если с β связаны хотя бы два различных символа $s_1, s_2 \in S$, то считаем, что данному слову приписан символ $*$

Установим связь представленных понятий с понятием элементарного отрезка.

Утверждение 11. *Пусть $(\beta_1, \beta_2]$ — элементарный отрезок в контексте l_F и с β_2 связан символ $s \in S$. Тогда данный символ s связан со всеми словами из этого элементарного отрезка.*

Доказательство.
1. По определению, найдутся слова $\hat{s} \in S^*$, β_3, β_4 такие, что β_3 — префикс β_4, $\hat{F}(\hat{s}) \mapsto \beta_3$, $\hat{F}(\hat{s}s) \mapsto \beta_4$, $\beta_2 \in (\beta_3, \beta_4]$. Отметим также, что символ s связан с каждым словом из отрезка $(\beta_3, \beta_4]$.
2. Согласно утверждению 6, из $\beta_2 \in (\beta_3, \beta_4]$ и элементарности $(\beta_1, \beta_2]$ вытекает включение $(\beta_1, \beta_2] \subseteq (\beta_3, \beta_4]$. И, следовательно, символ s связан со всеми словами из $(\beta_1, \beta_2]$.
□

Утверждение 12. *Пусть $(\beta_1, \beta_2]$ — элементарный отрезок в контексте l_F, концу отрезка β_2 приписан символ $*$. Тогда данный символ $*$ приписан всем словам из отрезка $(\beta_1, \beta_2]$*

Доказательство.
Действительно, так как β_2 приписан символ $*$, то с данным словом связаны два различных символа $s_1, s_2 \in S$. Которые, согласно утверждению 11, связаны со всеми словами из $(\beta_1, \beta_2]$. Следовательно, всем словам из данного отрезка приписан символ $*$. □

Приписанный слову β символ задает соответствующие ограничения на возможные значения функции поведения Боба на данном слове.

Утверждение 13. *Пусть (F, G) — корректный протокол, а также дано некое слово β, для которого $G(\beta) \neq \Lambda$. Тогда выполнено следующее:*

1) Если со словом β связан некий символ $s \in S$, то или $G(\beta) = s$, или $G(\beta) = *$.

2) Если слову β приписан символ $*$, то $G(\beta) = *$

Доказательство.
1. Рассмотрим сначала случай, когда со словом β связан символ s. По определению, это означает, что найдутся такие слова $\hat{s} \in S^*$, $\beta_1, \beta_2 \in B^*$, что β_1 — строгий префикс β_2, $\hat{F}(\hat{s}) \mapsto \beta_1$, $\hat{F}(\hat{s}s) \mapsto \beta_2$, $\beta \in (\beta_1, \beta_2]$.
2. Так как по условию (F, G) — правильный протокол, то применяя утверждение 5, а также основное свойство функции l_F, выраженное в утверждении 3, получаем: $|\hat{G}(\beta_1)| = l_F(\beta_1) = |\hat{s}|$, $|\hat{G}(\beta_2)| = l_F(\beta_2) = |\hat{s}s|$. И, следовательно, $|\hat{G}(\beta_2)| = |\hat{G}(\beta_1)| + 1$
3. Так как β_1 — строгий префикс β_2, то согласно утверждению 1 $\hat{G}(\beta_1)$ — префикс $\hat{G}(\beta_2)$. Таким образом, $\hat{G}(\beta_2) = \hat{G}(\beta_1)s'$, причем для символов s, s', рассматриваемых как слова длины 1, выполнено $s' \preceq s$, т.е. $s' \in \{s, *\}$.
4. Следовательно, функция G печатает на отрезке $(\beta_1, \beta_2]$ ровно один раз, причем печатает символ s'. Так как по условию $G(\beta) \neq \Lambda$, то $G(\beta) = s'$. Т.е. или $G(\beta) = s$, или $G(\beta) = *$.
5. Пусть теперь слову β приписан символ $*$. Это означает, что с данным словом связаны два различных символа $s_1, s_2 \in S$. Применяя уже доказанный пункт 1), получаем, что $G(\beta) = s'$, где $s' \in \{s_1, *\} \cap \{s_2, *\}$. Т.е. $G(\beta) = *$.
□

Утверждение 14. *Пусть $\beta \in H_F^1$. Тогда с этим словом β связан хотя бы один символ $s \in S$. И, следовательно, β не может быть приписан «пустой символ» Λ.*

Доказательство.
1. Пусть $(\beta', \beta]$ — 1-элементарный отрезок, концом которого является β. Соответственно, $\beta', \beta \in H_F$, $l_F(\beta) = l_F(\beta') + 1 \geqslant 1$.
2. Пусть также $\hat{s} \in S^*$ такое слово, что $\hat{F}(\hat{s}) \mapsto \beta$. Тогда $|\hat{s}| = l_F(\beta) \geqslant 1$, и, следовательно, $\hat{s} = \hat{s}'s$, $s \in S$.

3. Используя утверждение 7, установим, что найдется слово β_0 такое, что β_0 — строгий префикс β, $\hat{F}(\hat{s}') \mapsto \beta_0$.
4. Таким образом, $\hat{F}(\hat{s}') \mapsto \beta_0$, $\hat{F}(\hat{s}'s) \mapsto \beta$, β_0 — строгий префикс β, $\beta \in (\beta_0, \beta]$. Согласно определению, это означает, что слову β приписан символ s.

□

4.4. Построение G^F_{best}

В данном подразделе представим построение функции поведения Боба G^F_{best} и проверим её свойства, указанные в формулировке теоремы 2.

Определение 14. *Определим функцию G^F_{best} следующим образом. Если $\beta \in H^1_F$, то полагаем $G^F_{best}(\beta) = s$, где (см. утверждение 14) $s \in S \cup \{*\}$ — символ, приписанный β. В случае, если $\beta \notin H^1_F$, полагаем $G^F_{best}(\beta) = \Lambda$.*

Замечание 4. *Отдельно отметим, что так как пустое слово Λ не является концом какого-либо отрезка, то, согласно определению множества H^1_F, $\Lambda \notin H^1_F$. Таким образом, $G^F_{best}(\Lambda) = \Lambda$, т.е. пара (F, G^F_{best}) удовлетворяет ограничению, наложенному в соответствии с определением на понятие протокола.*

4.4.1. Проверка условия пункта 1) теоремы 2

Утверждение 15. *Пусть $\hat{F}(\hat{s}) \mapsto \beta$. Тогда $|\hat{G}^F_{best}(\beta)| = |\hat{s}|$.*

Доказательство.
Действительно, согласно утверждению 10, префиксов слова β, лежащих в H^1_F, т.е. именно тех префиксов, на которых печатает функция G^F_{best}, имеется $l_F(\beta) = |\hat{s}|$. И, следовательно, $|\hat{G}^F_{best}(\beta)| = |\hat{s}| = l_F(\beta)$. □

Утверждение 16. *(F, G^F_{best}) — корректный протокол.*

Доказательство.
1. Зафиксируем слова $\hat{s} \in S^*$, $\beta \in B^*$ такие, что $\hat{F}(\hat{s}) \mapsto \beta$. Согласно определению корректного протокола, необходимо доказать выполнение $\hat{G}^F_{best}(\beta) \preceq \hat{s}$.
2. Применяя утверждение 15, получаем $|\hat{G}^F_{best}(\beta)| = |\hat{s}|$. Таким образом, посимвольно возможно записать: $\hat{s} = s_1 ... s_m$, $\hat{G}^F_{best}(\beta) = s'_1 ... s'_m$. Предположим теперь, что $\hat{G}^F_{best}(\beta) \preceq \hat{s}$ не выполнено.
3. Это возможно, только лишь когда найдется i-я позиция такая, что $s'_i \not\preceq s_i$ для символов s_i, s'_i, рассматриваемых как слова длины 1. Так как $s_i \in S$, то из этого следует, что $s'_i \neq *$, а также $s'_i \neq s_i$.
4. Положим $\hat{s}_1 = s_1 ... s_i$. Установим существование слова β_1 такого, что $\hat{F}(\hat{s}_1) \mapsto \beta_1$, β_1 — строгий префикс β, последовательно применяя необходимое количество раз утверждение 7.
5. Вновь используя утверждение 15, установим выполнение $|\hat{G}^F_{best}(\beta_1)| = |\hat{s}_1|$. С другой стороны, так как β_1 — префикс β, то и $\hat{G}^F_{best}(\beta_1)$ — префикс $\hat{G}^F_{best}(\beta)$ (см. утверждение 1). И, следовательно, $\hat{G}^F_{best}(\beta_1) = s'_1 ... s'_i$.
6. Определим слово $\hat{s}'_1$ следующим образом. Если $i \neq 0$, то $\hat{s}'_1 = s_1 ... s_{i-1}$, иначе $\hat{s}'_1 = \Lambda$. Отметим, что в обоих случаях $\hat{s}_1 = \hat{s}_1 s_i$.
7. Ещё раз применяя утверждение 7, заключаем, что существует слово β'_1 такое, что β'_1 — строгий префикс β_1, и $\hat{F}(\hat{s}'_1) \mapsto \beta'_1$.
8. В очередной раз сославшись на утверждение 15, а также используя утверждение 1, получаем: $|\hat{G}^F_{best}(\beta'_1)| = |\hat{s}'_1| = |\hat{s}_1| - 1$, $\hat{G}^F_{best}(\beta'_1)$ — префикс $\hat{G}^F_{best}(\beta_1)$. И, следовательно, $\hat{G}^F_{best}(\beta'_1) = s'_1 ... s'_{i-1}$. Запишем вывод: $\hat{G}^F_{best}(\beta_1) = \hat{G}^F_{best}(\beta'_1) s'_i$.

9. Таким образом, так как $\hat{F}(\hat{s}'_1) \mapsto \beta'_1$, $\hat{F}(\hat{s}'_1 s_i) \mapsto \beta_1$, β'_1 — строгий префикс β_1, то со всеми словами из отрезка $(\beta'_1, \beta_1]$ связан символ s_i.
10. С другой стороны, так как $\hat{G}^F_{best}(\beta_1) = \hat{G}^F_{best}(\beta'_1)s'_i$, то G^F_{best} печатает символ s'_i на некотором слове $\beta_0 \in (\beta_1, \beta_2]$, а на всех остальных словах из этого отрезка ничего не печатает. Применяя пункт 1) утверждения 13, получаем, что слову β_0 приписан символ s'_i.
11. Одновременно слову β_0 приписан символ s'_i и с ним же связан символ s_i, причем $s_i \neq s'_i$, $s_i, s'_i \in S$. Согласно определению приписанного символа, это невозможно.
□

4.4.2. Проверка условия пункта 2) теоремы 2

Предварительно установим, что если на некотором отрезке функция G^F_{best} отпечатывает символ стирания $*$, то и любая согласованная с F функция G также отпечатывает на данном отрезке символ стирания.

Утверждение 17. *Пусть (F, G) — корректный протокол, $\beta_0, \beta_1 \in H_F$ — слова такие, что β_0 — строгий префикс β_1, а также выполнено $\hat{G}^F_{best}(\beta_1) = \hat{G}^F_{best}(\beta_0)*$. Тогда $\hat{G}(\beta_1) = \hat{G}(\beta_0)*$*

Доказательство.
1. Согласно утверждению 16, протокол (F, G^F_{best}) — корректен. Из корректности протоколов (F, G), (F, G^F_{best}) в соответствии с утверждением 5 следует выполнение $|\hat{G}(\beta_0)| = |\hat{G}^F_{best}(\beta_0)| = l_F(\beta_0)$, $|\hat{G}(\beta_1)| = |\hat{G}^F_{best}(\beta_1)| = l_F(\beta_1)$.
2. Таким образом, выполнено, $|\hat{G}(\beta_1)| - |\hat{G}(\beta_0)| = l_F(\beta_1) - l_F(\beta_0) = |\hat{G}^F_{best}(\beta_1)| - |\hat{G}^F_{best}(\beta_0)| = |\hat{G}^F_{best}(\beta_0) * | - |\hat{G}^F_{best}(\beta_0)| = 1$.
3. Таким образом, обе функции G, G^F_{best} печатают ровно один раз на отрезке $(\beta_0, \beta_1]$.
4. Полагаем далее, что $G^F_{best}(\beta) = *$ на слове $\beta \in (\beta_0, \beta_1]$. По определению функции G^F_{best}, это означает, что β является концом некоторого 1-элементарного отрезка $(\beta', \beta]$, причем слову β приписан символ $*$.
5. Так как отрезок $(\beta', \beta]$ элементарен и $\beta \in (\beta_0, \beta_1]$, то, применяя утверждение 6, получаем $(\beta', \beta] \subseteq (\beta_0, \beta_1]$.
6. Так как $(\beta', \beta]$ — элементарный отрезок, то $\beta', \beta \in H_F$. Вновь применяя утверждение 5, получаем $\hat{G}(\beta) - \hat{G}(\beta') = l_F(\beta) - l_F(\beta') = 1$. Таким образом, функция G печатает ровно один раз на отрезке $(\beta', \beta]$. Пусть она печатает на слове $\beta'' \in (\beta', \beta] \subseteq (\beta_0, \beta_1]$.
7. И, следовательно, также можно записать $\hat{G}(\beta_1) = \hat{G}(\beta_0)G(\beta'')$. Таким образом, осталось лишь доказать, что $G(\beta'') = *$.
8. Так как $(\beta, \beta']$ — элементарный отрезок, а слову β приписан символ $*$, то согласно утверждению 12, символ $*$ приписан всем словам из данного элементарного отрезка, в том числе и слову $\beta'' \in (\beta, \beta']$.
9. Таким образом, слову β'' приписан символ $*$, а также $G(\beta'') \neq \Lambda$. Сославшись на пункт 2) утверждения 13, получаем $G(\beta'') = *$.
□

Утверждение 18. *Пусть (F, G) — корректный протокол, $\beta \in H_F$. Тогда $\hat{G}(\beta) \preceq \hat{G}^F_{best}(\beta)$*

Доказательство.
1. Так как $\beta \in H_F$, то найдется $\hat{s} \in S^*$ такое, что $\hat{F}(\hat{s}) \mapsto \beta$. Запишем посимвольно: $\hat{s} = s_1 ... s_m$.
2. Протоколы (F, G) и (F, G^F_{best}) корректны, следовательно, $\hat{G}^F_{best}(\beta), \hat{G}(\beta) \preceq \hat{s}$. Также запишем посимвольно: $\hat{G}^F_{best}(\beta) = s'_1 ... s'_m$, $\hat{G}(\beta) = s''_1 ... s''_m$, где $s_k, s'_k \in S \cup \{*\}$ при $k = 1...m$. Из данных соотношений следует, что для всех $k = 1...m$ $s'_k, s''_k \in \{s_i, *\}$.

3. Предположим теперь, что $\hat{G}(\beta) \preceq \hat{G}^F_{best}(\beta)$ не выполняется. Это возможно, только если найдется i-ая позиция такая, что $s''_i \not\preceq s_i$ для символов s'_i, s''_i, рассматриваемых как слова длины 1. Откуда следует, что $s''_i = s_i \neq *$, $s'_i = *$.
4. Применяя утверждение 6, установим, что найдутся слова β_0, β_1 такие, что они оба — строгие префиксы β, β_0 — строгий префикс β_1, $\hat{F}(s_1...s_{i-1}) \mapsto \beta_0$, $\hat{F}(s_1...s_{i-1}s_i) \mapsto \beta_1$. Отдельно отметим, что в случае $i = 1$ под словом $s_1...s_{i-1}$ (и, аналогично, словами $s'_1...s'_{i-1}$, $s''_1...s''_{i-1}$) понимается пустое слово Λ.
5. Таким образом, $\beta_0, \beta_1 \in H_F$. Применяя утверждение 5, получаем $|\hat{G}(\beta_0)| = |\hat{G}^F_{best}(\beta_0)| = l_F(\beta_0) = |s_1...s_{i-1}| = i - 1$, а также $|\hat{G}(\beta_1)| = |\hat{G}^F_{best}(\beta_1)| = l_F(\beta_1) = |s_1...s_i| = i$
6. И, следовательно, возможно записать: $\hat{G}^F_{best}(\beta_0) = s'_1...s'_{i-1}$, $\hat{G}^F_{best}(\beta_1) = s'_1...s'_{i-1}s'_i = \hat{G}^F_{best}(\beta_0)s'_i$, $\hat{G}(\beta_0) = s''_1...s''_{i-1}$, $\hat{G}(\beta_1) = s''_1...s''_{i-1}s''_i = \hat{G}(\beta_0)s''_i$.
7. Таким образом, $\hat{G}^F_{best}(\beta_1) = \hat{G}^F_{best}(\beta_0)*$, так как $s'_i = *$. Согласно утверждению 17, отсюда следует $\hat{G}(\beta_1) = \hat{G}(\beta_0)*$, что неверно, так как $s''_i \neq *$. Противоречие означает, что предположение п.3 ложно, и, следовательно, выполняется $\hat{G}(\beta) \preceq \hat{G}^F_{best}(\beta)$.

□

Теорема 2 доказана.

5. Заключение

В настоящей работе решены две связанные между собой задачи. Во-первых, указано необходимое и достаточное условие существования функции поведения Боба G, согласованной с заданной функцией поведения Алисы F. В соответствии с доказанной в настоящей работе теоремой 1, такое условие есть ничто иное как условие правильности, представленное в определении 8. Во-вторых, установлено, что среди всех возможных G, согласованных с F, имеется «наилучшая функция», что позволяет исключить из рассмотрения все альтернативные варианты. Таковая функция, в соответствии с определением 14, имеет описание вида «печатать на конце 1-элементарного отрезка приписанный символ». Таким образом, было произведено «уменьшение количества степеней свободы», т.е. представлено однозначное построение поведения Боба по заданному поведению Алисы. Следовательно, в дальнейшем, само понятие протокола может быть переопределено следующим образом: функция F заведомо полагается правильной, а протоколом считается пара (F, G^F_{best}).

Отметим далее, что поведение Алисы имеет автоматное описание. Представим необходимые пояснения. Заметим, что функция поведения F детерминирована, и, следовательно, может быть представлена в виде (не обязательно конечного) абстрактного автомата. Действительно, рассмотрим множество слов S^* как множество состояний данного автомата, сам алфавит S примем как алфавит входных символов. В качестве выходного алфавита рассматривается множество слов A^*. Принимая символ $s \in S$, автомат из состояния $\hat{s}$ переходит в состояние $\hat{s}s$ и выбрасывает слово $F(\hat{s}s)$. Подвергнем полученный автомат преобразованию, отождествляющему его неотличимые состояния. Полученный приведенный автомат и является альтернативным описанием поведения Алисы. Интерес представляют именно ограниченно-детерминированные функции, т.е. те, которые представимы указанным образом в виде конечного автомата. Отдельно отметим, что в случае конечного числа состояний число слов, которые может выбрасывать Алиса, также конечно, и, таким образом, соответствующий автомат имеет конечный выходной алфавит.

Обозначим задачи дальнейших исследований. Во-первых, пусть дана некая ограниченно-детерминированная функция F. Требуется по виду соответствующего конечного автомата определить, является ли соответствующее поведение Алисы пригодным для построения протокола, т.е. является ли F правильной функцией. Таким образом, возникает задача построения алгоритма, проверяющего указанное условие правильности.

Во-вторых, пусть теперь F — ограниченно-детерминированная функция, про которую уже известно, что она правильна. Далее, таким образом, требуется построить соответствующую функцию поведения Боба G^F_{best}, т.е. требуется построить соответствующий автомат. Сделаем также пояснения относительно автоматного представления поведения Боба. Входным алфавитом является алфавит B, выходным — множество $S \cup \{*, \Lambda\}$. Выходной функцией является соответствующая функция поведения, т.е. G^F_{best}. Таким образом, во-первых, следует доказать, что если поведение Алисы задается конечным автоматом, то автомат, задающий соответствующее ему поведение Боба, также имеет конечное число состояний. Во-вторых, требуется привести в явном виде алгоритм, строящий второй из указанных автоматов по первому из них, в соответствии с представленным в настоящей работе описанием G^F_{best}.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Галатенко А. В. О скрытых каналах и не только // Jet Info. 2002. Т. 14, № 114. С. 12 – 20.
2. Епишкина А. В., Когос К. Г. Об оценке пропускной способности скрытых информационных каналов, основанных на изменении длин передаваемых пакетов // Информация и космос. 2015. № 4. С. 78 — 82.
3. Казаков И. Б. Кодирование в скрытом канале перестановки пакетов // Программная инженерия. 2018. Т. 9, № 4. С. 163 — 173.
4. Казаков И. Б. Структура графа на множестве перестановок S_n, задаваемая моделью ошибки в скрытом канале перестановки пакетов // Интеллектуальные системы. Теория и приложения. 2018. Т. 22, № 2. С. 53 — 79.
5. Казаков И. Б. Разностный код и протокол циклической поблочной передачи в скрытом канале по памяти // Программная инженерия. 2019. Т. 10, № 5. С. 204 – 218.
6. Казаков И. Б. Критерий надежности канала с запрещениями // Интеллектуальные системы. Теория и приложения. 2019. Т.23, № 2. С. 33 – 55.
7. Казаков И. Б. Передача информации в каналах, задаваемых структурами частичного стирания. Часть 1 // Программная инженерия. 2020. Т.11, № 5. С. 277 – 284.
8. Казаков И. Б. Передача информации в каналах, задаваемых структурами частичного стирания. Часть 2 // Программная инженерия. 2020. Т.11, № 6. С. 322 – 329.
9. Тимонина Е. Е. Скрытые каналы (обзор) // Jet Info. 2002. Т. 14, № 114. С. 3 – 11.
10. Ahsan K., Kundur D., Practical data hiding in TCP/IP // In proceedings of: Multimedia and Security Workshop at ACM Multimedia. 2002.
11. Berk, V., Giani A., Cybenko G. Detection of covert channel encoding in network packet delays // Technical report TR2005-536. 2005. 11 p.
12. Bovy C.J., Mertodimedjo H.T., Hooghiemstra G., Uijterwaal H., Mieghem P. Analysis of end-to-end delay measurements in Internet // Proc. 3rd Int. Workshop on Passive and Active Network Measurement. 2002. P. 1 – 8
13. Gallager R. G., Information Theory and Reliable Communications // New York: John Wiley and Sons Inc., 1968. 604 p.
14. Handel T., Sandford M. Hiding data in the OSI network model // Proc. of the first International workshop on information hiding. 1996. P. 23 – 38

15. Lampson B. W. A note on the confinement problem // Communications of ACM. 1973. Vol. 16, N. 10. P. 613 — 615.

16. Lipner S. B. A Comment on the Confinement Problem // Proceedings of the Fifth ACM Symposium on Operating Systems Principles. 1975. vol.9, no. 5. pp. 192 — 196.

17. McFarland J. Covert Channels: An Overview // Preprint. 2017.

18. Murdoch S., Zielinski P. Covert Channels for Collusion in Online Computer Games // IH'04: Proceedings of the 6th international conference on Information Hiding. 2004. pp. 355–369.

19. Salwan N., Singh S., Arora S., Singh A. An Insight to Covert Channels // arXiv:1306.2252. 2013.

20. Sellke S. H., Wang C. C., Bagchi S., Shroff N. B. Covert TCP/IP timing channels: theory to implementation // Proc. of the twenty-eighth Conference on computer communications. 2009. P. 2204 – 2212.

21. Wendzel S., Zander S., Fechner B., Herdin C. Pattern-Based Survey and Categorization of Network Covert Channel Techniques // ACM Comput. Surv. 2015. vol. 47, pp. 50:1 – 50:26.

22. Yao L., Zi X., Pan L., Li J. A study of on/off timing channel based on packet delay distribution // Computers and security. 2009. Vol. 28. No. 8. P. 785 – 794.

23. Zander S., Armitage G., Branch P. Covert channels in the IP time to live field // Proc. of the 2006 Australian telecommunication networks and applications conference. 2006. pp. 298 – 302.

24. Zander S., Armitage G., Branch P. A survey of covert channels and countermeasures in computer network protocols // IEEE Communications Surveys & Tutorials. 2007. vol. 9, pp. 44 – 57.

25. Zander S., Armitage G., Branch P. Covert channels in multiplayer first person shooter online games // Proc. 33rd IEEE Conf. LCN. 2008. pp. 215 – 222.

REFERENCES

1. Galatenko, A. V. 2002, «On covert channels and not only», Jet Info, vol. 14, no. 114. pp. 12 – 20.

2. Epishkina, A. V. & Kogos, K. G. 2015, «On assessing throughput capacity of covert information channels by measuring the length of packets transmitted», Informaciya i kosmos, no. 4, pp. 78 — 82

3. Kazakov, I. B. 2018, «Coding in a covert channel of data packages' permutations», Programmnaya Ingeneria, vol. 9, no. 4, pp. 163 — 173

4. Kazakov, I. B. 2018, «The structure of a graph induced on the set of permutations Sn by an error model of a covert channel based on packet permutations», Intelligent systems. Theory and applications, vol. 22, no. 2, pp. 53 – 81

5. Kazakov, I. B. 2019, «Difference code and a protocol for cyclic blockwise transmission in a memory-based covert channel», Programmnaya Ingeneria, vol. 10, no. 5, pp. 204 — 218

6. Kazakov, I. B. 2019, «Reliabilty criterion for channels with prohibitions», Intelligent systems. Theory and applications, vol. 23, no. 2, pp. 33 – 55

7. Kazakov, I. B. 2020, «Transmission of information in channels specified by structures of partial erasure (part 1)», Programmnaya Ingeneria, vol. 11, no. 5. pp. 277 – 284

8. Kazakov, I. B. 2020, «Transmission of information in channels specified by structures of partial erasure (part 2)», Programmnaya Ingeneria, vol. 11, no. 6. pp. 322 – 329

9. Timonina, E. E. 2002, «Covert channels (survey)», Jet Info, vol. 14, no. 114, pp. 3 – 11

10. Ahsan, K. & Kundur, D. 2002, «Practical data hiding in TCP/IP», In proceedings of: Multimedia and Security Workshop at ACM Multimedia.

11. Berk, V., Giani, A. & Cybenko, G. 2005, «Detection of covert channel encoding in network packet delays», Technical report TR2005-536, 11 p.

12. Bovy, C.J., Mertodimedjo, H.T., Hooghiemstra, G., Uijterwaal, H. & Mieghem, P. 2002, «Analysis of end-to-end delay measurements in Internet», Proc. 3rd Int. Workshop on Passive and Active Network Measurement, pp. 1 – 8

13. Gallager, R. G. 1968, Information theory and reliable Communications, John Wiley & Sons Inc., New York, 604 p.

14. Handel, T. & Sandford, M. 1996, «Hiding data in the OSI network model», Proc. of the first International workshop on information hiding, pp. 23 – 38

15. Lampson, B. W. 1973, «A note on the confinement problem», Communications of ACM., vol. 16, no. 10, pp. 613 — 615

16. Lipner, S. B. 1975, «A comment on the confinement Problem», Proceedings of the Fifth ACM Symposium on Operating Systems Principles, vol.9, no. 5, pp. 192 — 196

17. McFarland, J. 2017, «Covert channels: an overview», Preprint.

18. Murdoch, S. & Zielinski, P. 2004, «Covert channels for collusion in online computer games», IH'04: Proceedings of the 6th international conference on Information Hiding, pp. 355 – 369

19. Salwan, N., Singh, S., Arora, S. & Singh A. 2013, «An insight to covert channels», arkhiv:1306.2252

20. Sellke, S. H., Wang, C. C., Bagchi, S. & Shroff, N. B. 2009, «Covert TCP/IP timing channels: theory to implementation», Proc. of the twenty-eighth Conference on computer communications, pp. 2204 – 2212

21. Wendzel, S., Zander, S., Fechner, B. & Herdin C. 2015, «Pattern-based survey and categorization of network covert channel techniques», ACM Comput. Surv., vol. 47, pp. 50:1 – 50:26

22. Yao, L., Zi, X., Pan, L. & Li, J. 2009, «A study of on/off timing channel based on packet delay distribution», Computers and security, vol. 28, no. 8, pp. 785 – 794

23. Zander, S., Armitage, G. & Branch, P. 2006, «Covert channels in the IP time to live field», Proc. of the 2006 Australian telecommunication networks and applications conference. pp. 298 – 302

24. Zander, S., Armitage, G. & Branch, P. 2007, «A survey of covert channels and countermeasures in computer network protocols», IEEE Communications Surveys & Tutorials, vol. 9, pp. 44 – 57

25. Zander, S., Armitage, G. & Branch, P. 2008, «Covert channels in multiplayer first person shooter online games», Proc. 33rd IEEE Conf. LCN, pp. 215 – 222

Получено 29.09.2020 г.
Принято в печать 21.02.2021 г.