Критерий надежности канала с запрещениями

Казаков И.Б.

В работе исследуется возможность надежной передачи информации в ситуации, когда противник в каждой момент времени может блокировать некоторое подмножество символов алфавита. Показано, что гарантированно надежный канал существует тогда и только тогда, когда мощность алфавита n и число разрешенных символов k удовлетворяют неравенству $n \leq 2k - 2$.

Ключевые слова: скрытые каналы, блуждания по плоскости, запрещения алфавитных символов, передаваемый язык

1. Введение

В работе изучается вопрос о том, возможно ли передавать каким-либо образом информацию, используя алфавит из n символов, если при каждом акте передачи какие-то произвольные символы этого алфавита могут быть объявленными запрещенными к передаче. Однако, перед тем, как будет дано формальное точное определение тому, что же это означает, мы приведем мотивировку исследования данного вопроса.

Прежде всего, скажем, что изначальный пункт — это теория скрытых каналов. Скрытым каналом называется называется коммуникационный канал, пересылающий информацию методом, который изначально не был для этого предназначен. То есть существуют злоумышленники, передающие информацию таким образом, что сторонние наблюдатели не могут зафиксировать сам факт передачи.

Исторически первой работой, посвященной теории скрытых каналов, считается статья [1]. Также упомянем о современном обзоре [2], посвященном сетевым скрытым каналам.

Конкретно в данной работе речь идет о скрытом канале блужданий по плоскости. Блуждания по плоскости изучаются в связи с задачей построения скрытых каналов через online-шутеры, то есть многопользовательские игры, в которых некий клиент может передавать игровому

серверу команды о перемещении своего персонажа по плоскости, а другие клиенты могут получать от сервера данные о местоположении (и, следовательно, также о изменениях местоположения) этого персонажа.

Задача построения скрытых каналов через online-шутеры ранее исследовалась в [3]. Там использовался подход, несколько отличающийся от применяемого в настоящей работе, а именно: передача информации осуществлялась через *малые отклонения* от «естественного движения». Также использовался дополнительный параметр «угол зрения персонажа», который исключен здесь из рассмотрения.

Однако, в [3] не изучался вопрос исправления ошибок, а также вопрос о возможности блокирования направлений движения, которому и посвящена настоящая работа.

С технической точки зрения, протокол передачи данных через блуждания по плоскости задан следующим образом. Вся игровая плоскость разбита на квадраты прямыми линиями. Игрок, который хочет передать некое скрытое сообщение, должен находиться в области видимости игрока, которому он хочет передать это сообщение. Актом передачи информации считается пересечение границы квадрата (в котором в данный момент находится передающий игрок) в одном из четырех возможных направлений. Таким образом, на каждом акте могут быть переданы 4 возможных значения, или 2 бита информации.

Как вариант, можно разбивать плоскость не на квадраты, а на шестиугольники. При таком разбиении каждый шестиугольник имеет 6 соседних. Аналогично считая актом передачи переход в соседний шестиугольник, можно передавать уже не 4, а 6 возможных значений.

Однако в реальных online-играх движение персонажей по игровому полю не является абсолютно свободным. Во-первых, у игрового поля есть границы, и персонаж не может находиться за этими границами. Во-вторых, существуют предусмотренные игрой препятствия для перемещения, такие как «камни», «вода» и так далее, которые игрок вынужден обходить. В-третьих, сервер может передавать игроку, принимающему скрытое сообщение, координаты не всех игроков на поле, а лишь тех, которые расположены в «зоне видимости» (то есть где-то недалеко от местонахождения игрока-приемника). Поэтому для игрока-передатчика переход в ячейки, находящиеся за пределами области видимости игрока-приемника, недопустим: это означает разрыв связи в канале. В-четвертых, есть местонахождения, крайне нежелательные по игровым причинам: например, около этой точки на игровом поле находится враг, её просматривающий. Враг начинает атаковать любого игрока, пер-

сонаж которого там находится, и персонаж игрока-передатчика может оказаться слишком слаб для того, чтобы этого врага победить.

Таким образом, на любом шаге может оказаться так, что по некоторым направлениям игроку-передатчику ходить нельзя, то есть невозможно передать некоторые из значений. При этом игрок-приемник может как знать, какие именно направления сейчас запрещены (например, в случае края поля), так и не знать, *куда же игрок-передатчик «не хочет идти»*.

И, следовательно, возникает задача конструирования схемы кодирования информации для передачи в вышеописанных условиях. Мы рассмотрим следующую абстрактную постановку задачи: пусть дан алфавит из n символов, и пусть на каждом шаге может быть запрещено не более, чем $n - k$ из них. При каких n и k гарантированно возможно что-либо передать?

2. Протокол

Для того, чтобы ответить на вышепоставленный вопрос, необходимо дать формальное математическое определение выражению «возможно что-либо передать». Отметим, что если вообще «возможно что-либо передать», то очевидно, что прежде всего возможно передать 1 бит информации.

Уметь передавать 1 бит информации — это значит уметь передавать некие два различных «сигнала». Это означает, что игрок-передатчик сначала выбирает, какое же из двух значений (0 или 1) ему передавать, и соответственно с выбором значения передает символы игроку-приемнику по одному из двух заранее определенных способов. Игрок-приемник, считывая принятые символы, должен уметь распознавать, какой же из двух способов был использован игроком-передатчиком.

Следовательно, нужно далее определить, что же такое «способ передачи» сигнала. Игрок-приемник, считывая изменения местоположения игрока-передатчика, принимает последовательность символов алфавита, соответствующую происходящим перемещениям. В некоторый момент игрок-приемник, очевидно, должен решить, что «сигнал передан».

Игроку-приемнику недоступна никакая другая информация, кроме последовательности получаемых им символов. Следовательно, алгоритм, принимающий решение о том, произошло ли событие «сигнал передан», на одинаковых *конечных последовательностях уже принятых символов* (то есть на одинаковых *словах*) должен выдавать одинаковый ответ.

А это означает ничто иное как то, что «способ передачи сигнала» может быть описан исключительно *как множество слов* (или *язык*). Событие «сигнал передан» тождественно событию «последовательность уже принятых символов образует слово, принадлежащее заданному языку».

Таким образом, для передачи 1 бита информации предзадаются два языка X и Y. Соответственно значению бита выбирается один из них, и игрок-передатчик пытается передавать символы так, чтобы на каком-то шаге было передано какое-то слово из выбранного языка. Заметим, что так как здесь речь идет не об одном языке, а о двух, то для *различаемости* соответствующих «сигналов» необходимо потребовать соблюдения ещё одного условия (далее формально определенного как *кросс-префиксность*): чтобы никакое начало слова, принадлежащего одному из языков, не совпадало с каким-нибудь словом из другого языка. Действительно, если, например, на некотором шаге произошло событие «передано значение 1», то ни на каком предыдущем шаге (а также, разумеется, и на данном) не могло произойти события «передано значение 0».

Замечание. *Можно потребовать не только кросс-префиксности пары языков, но также префиксности каждого из них, то есть того, чтобы никакое слово не являлось началом другого слова этого же языка. Так как, если, например, на каком-то шаге уже «передано значение 1», то на этом передачу следует остановить, и тем самым исключить то, что на каком-то последующем шаге снова произойдет событие «передано значение 1». Это совершенно необходимо, если мы хотим всё же передавать не 1 бит, а сообщения произвольной длины: игрок-приемник должен определять, в какой момент можно считать завершенной передачу очередного бита.*

3. Противодействующий субъект

Осталось учесть только лишь только тот факт, что на каждом шаге некоторые символы (не более чем $n - k$ из них) запрещены к передаче. Для краткости мы будем далее говорить, что в некоторый момент достигнуто состояние, описываваемое словом α (или просто состояние α), если к этому моменту уже была передана конечная последовательность символов, это слово образующая.

Пусть для передачи выбран язык X. Тогда задача игрока-передатчика *при любых запрещениях на всех ходах* прийти в любое из

состояний из X. Возможность этого, очевидно, зависит только от самого языка X. Если это возможно, то такой язык называется *передаваемым*.

Так как запрещения символов могут быть любыми, то нам следует изучать самый худший случай: как будто бы запрещения происходят именно так, чтобы во чтобы то ни стало не дать прийти в состояние из X.

Следовательно, можно представить себе дело так, как будто запрещениями управляет некий третий субъект, пытающийся сорвать передачу, а сама эта передача суть игра между передатчиком и данным субъектом. Далее, следуя сложившийся традиции, мы будем именовать игрока-передатчика — *Алисой*, игрока-приемника — *Бобом*, а мешающего третьего субъекта — *Евой*.

Ход Евы состоит в выборе множества запрещенных символов, причем если этот ход корректен, то количество запрещаемых символов не может превышать $n - k$. Следующий за ним корректный ход Алисы состоит в выборе какого-нибудь не запрещенного Евой символа с последующей отправкой его Бобу. Алиса выигрывает игру на языке X в момент, когда достигается состояние, соответствующее слову из X.

И, следовательно, вопрос о том, передаваем ли язык X, является по существу вопросом о том, существует ли страгегия, выигрышная (относительно языка X) для Алисы. А вопрос о том, возможно ли передача 1 бита, таким образом, сводится к вопросу: существуют ли два кросс-префиксных передаваемых языка при заданных n и k.

Теперь осталось только лишь формально записать уже напрашивающиеся определения, а также установить немедленно следующие из этих определений свойства.

4. Передаваемый язык

Для начал дадим определение языка как такового.

Определение 4.1. *Алфавит $A = \{a_1, a_2, ..., a_n\}$ — это конечное множество (n) символов.*

Определение 4.2. *Слово α, составленное из символов алфавита A — это некая конечная последовательность символов из A. Множество всех таких слов обозначается как A^*. В этом множестве, отдельно отметим, есть последовательность из 0 символов, то есть пустое слово $\Lambda \in A^*$.*

Определение 4.3. *Бесконечное слово — это бесконечная последовательность символов алфавита A. Множество всех бесконечных слов обозначается как A^∞.*

Определение 4.4. *Язык X — это просто некое множество слов: $X \subset A^*$.*

Теперь нужно выразить вышеупомянутые накладываемые на языки условия.

Определение 4.5. *Слово $\alpha\alpha'$ — это конкатенация слов α и α', то есть результат приписывания α' после α.*

Определение 4.6. *Слово α' называется префиксом слова α, если существует такое α'', что $\alpha = \alpha'\alpha''$. Особо отметим, что может быть $\alpha'' = \Lambda$, то есть любое слово согласно данному определению является префиксом самого же себя. Также отметим, что далее полагается допустимым говорить о конечном слове как о префиксе бесконечного.*

Замечание. *Пустое слово Λ считается префиксом любого слова.*

Определение 4.7. *Язык X называется префиксным, если в нем нет двух таких слов $\alpha, \alpha' \in X$, таких что α' — префикс α.*

Определение 4.8. $pr(X) \stackrel{\text{def}}{=} \{\alpha \in A^* | \exists \alpha' \in X : \alpha$ *— префикс* $\alpha'\}$ *— префиксное замыкание, то есть множество всех слов, которые являются префиксом какого-нибудь слова из X.*

Утверждение 4.1. $X \subset pr(X)$

Доказательство. Немедленно следует из того, что любое слово суть префикс самого себя. □

Утверждение 4.2. $pr(pr(X)) = pr(X)$

Доказательство. Немедленно следует из того, что префикс префикса — суть префикс. □

Определение 4.9. *Пара языков X, Y называется кросспрефиксной при выполнении следующих условий:*
1) $pr(X) \cap Y = \emptyset$
2) $pr(Y) \cap X = \emptyset$

Утверждение 4.3. *Если пара X, Y кросспрефиксна, то $X \cap Y = \emptyset$.*

Доказательство.
1. Пусть $\alpha \in X \cap Y$.
2. Так как $X \subset pr(X)$, то $\alpha \in pr(X) \cap Y$, что немедленно противоречит определению кросспрефиксности.

□

Далее нужно приписать Алисе стратегию и определить, что же означает, что Алиса всегда может выиграть игру, то есть определить для стратегии свойство «быть выигрышной». Это возможно сделать, также определив последовательность ходов Евы и задав отношение: побеждает ли Алиса при заданной страгетии, если Ева сделает определённые ходы.

Определение 4.10. *Стратегия Алисы — это функция* $f : A^* \times 2^A \to A$

Определение 4.11. *Корректная стратегия Алисы — это стратегия Алисы, для которой выполнено следующее свойство:* $\forall \alpha \in A^* \ \forall B \in 2^A \ ||B| \geq k| : f(\alpha, B) \in B$

Первый аргумент функции f — это текущее состояние игры, второй — это сделанный Евой ход, значение функции — ответный ход Алисы. Условие корректности, таким образом, означает, что в ответ выбор Евой допустимого множества символов (т.е. любое множество символов, в котором их k и более штук), разрешенных на текущем ходе, Алиса, как и положено, выбрает какой-то символ именно из этого множества.

Что касается Евы, то любое возможное её поведение может быть описано как последовательность множеств символов, которые она оставляет незапрещенными для Алисы.

Определение 4.12. *Последовательность ходов Евы — это отображение* $g : \mathbb{N} \to 2^A$*, то есть попросту последовательность неких подмножеств алфавита* A*.*

По условию, Ева всегда должна оставлять хотя бы k символов незапрещенными, что соответственно накладывает ограничения на последовательности ходов Евы, рассматриваемые как описания её поведения.

Определение 4.13. *Допустимая последовательность ходов Евы — это та, для которой выполнено* $\forall i \ |g(i)| \geq k$*.*

Определение 4.14. *Будем говорить, что бесконечное слово* $\alpha^\infty = \alpha^\infty(1)\alpha^\infty(2)\alpha^\infty(3)... \in A^\infty$ *согласованно с стратегией Алисы* f*, а также последовательностью ходов Евы* g*, если выполнено:*

1) $\alpha^\infty(1) = f(\Lambda, g(1))$
2) $\alpha^\infty(i+1) = f(\alpha^\infty(1)...\alpha^\infty(i), g(i+1))$

Утверждение 4.4. *Для любой страгегии Алисы f и любой последовательности ходов Евы согласованное бесконечное слово существует и единственно.*

Доказательство. Очевидно по индукции: определение задает явное посимвольное построение. □

Согласованное слово — это и есть «реально печатаемая Алисой последовательность символов».

Теперь наконец можно дать формальное определение понятию «передаваемый язык», исходя из того, что Алиса по определению выигрывает, если на каком-то шаге последовательность переданных ей символов складывается в слово из искомого языка.

Определение 4.15. *Будем говорить, что некий начальный отрезок бесконечного слова α^∞ лежит в X, если в языке X найдется такое слово α', что α' — префикс α^∞.*

Определение 4.16. *Корректная стратегия Алисы f передает язык X, если для всякой допустимой последовательность ходов Евы g согласованное с такими f и g бесконечное слово α таково, что некий его начальный отрезок лежит в X.*

Определение 4.17. *Язык X — передаваемый, если существует передающая его корректная стратегия.*

5. Особый случай

Рассмотрим отдельно случай $n \leq 2k-2$.

В этом случае дан алфавит $A = \{a_1, ..., a_n\}$. Положим $X = \{a_1, ...a_{n-k+1}\}$, $Y = \{a_{n-k+2}, ..., a_{2n-2k+2}\}$.

Очевидно, что X, Y — кросспрефиксная пара.

Утверждение 5.1. *X, Y – передаваемы (как языки).*

Доказательство. Возьмем для примера X. Так как в X (как множестве символов) более чем $n-k$ символов, то Ева не может запретить всё из X. Следовательно, Алиса может победить за один ход, выбрав символ из X, который оказался разрешенным, и передав его Бобу. □

Таким образом, при $n \leq 2k-2$ передача информации от Алисы к Бобу возможна, и осуществляется весьма *тривиальным* образом: просто среди символов выбираются два непересекающихся множества мощности больше, чем $n-k$.

А возможна ли передача (хотя бы 1 бита) информации при каком-нибудь другом n? Ответ на данный вопрос является отрицательным, и это составляет собственно главный результат данной работы.

6. Вспомогательные понятия

Прежде всего, мы введем некоторые определения технического характера, а также установим немедленно вытекающие из них тривиальные утверждения, которые будут использованы в дальнейших формальных доказательствах.

Здесь $X \subset A^*$ — некий произвольный язык.

Определение 6.1. $succ_X(\alpha) \stackrel{\text{def}}{=} \{a \in A | \alpha a \in X\}$ — *множество «последователей (а точнее их последних символов) слова α в языке X», т.е. множество таких символов a, что αa является словом из языка X.*

Утверждение 6.1. *Если $a \in succ_X(\alpha)$, то $\alpha a \in X$*

Доказательство. Немедленно из определения. □

Утверждение 6.2. $succ_{A^* \setminus X}(\alpha) = A \setminus (succ_X(\alpha))$

Доказательство.

1. $a \in succ_{A^* \setminus X}(\alpha) \Leftrightarrow \alpha a \in A^* \setminus X \Leftrightarrow \alpha a \notin X$.
2. $a \in A \setminus (succ_X(\alpha)) \Leftrightarrow a \notin succ_X(\alpha) \Leftrightarrow \alpha a \notin X$
3. Как видно, условия принадлежности эти двум множествам равносильны. □

Утверждение 6.3. *Пусть $\alpha \in X$ такое, что $|succ_X(\alpha)| \geq k$. Также пусть f — некая корректная стратегия Алисы, и $a = f(\alpha, succ_X(\alpha))$.*

Тогда $\alpha a \in X$.

Доказательство.
1. Согласно определению корректной стратегии, из $|succ_X(\alpha)| \geq k$ и $a = f(\alpha, succ_X(\alpha))$ следует $a \in succ_X(\alpha)$.
2. $a \in succ_X(\alpha) \Rightarrow \alpha a \in X$, по утверждению 6.1. □

Утверждение 6.4. *Пусть* $A_1 \subset A$, $A_2 \subset A$, $|A| = n$, $|A_1| \geq n - k + 1$, $|A_2| \geq n - k + 1$, *а также* $n > 2k - 2$. *Тогда* $A_1 \cap A_2 \neq \emptyset$.

Доказательство.
1. Рассмотрим множество $A_1 \cup A_2$. Из условий немедленно следует $A_1 \cup A_2 \subset A$, и, стало быть, $|A_1 \cup A_2| \leq n$.
2. С другой стороны, согласно общеизвестной формуле включений-исключений, $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| \geq 2(n-k+1) - |A_1 \cap A_2| = 2n - 2k + 2 - |A_1 \cap A_2|$.
3. Таким образом, $2n-2k+2-|A_1 \cap A_2| \leq n$, откуда $n \leq 2k-2+|A_1 \cap A_2|$, и, следовательно, $|A_1 \cap A_2| \geq n - (2k-2) > 0$.
4. Но $|A_1 \cap A_2| > 0$ и означает, что $A_1 \cap A_2 \neq 0$. □

Утверждение 6.5. *Пусть* $A_1 \subset A$, $B \subset A$, $|A| = n$, $|A_1| \geq n - k + 1$, $|B| \geq k$. *Тогда* $A_1 \cap B \neq \emptyset$

Доказательство.
1. Аналогично предыдущему доказательству: $n \geq |A_1 \cup B| = |A_1| + |B| - |A_1 \cap B| \geq (n - k + 1) + k - |A_1 \cap B| = n + 1 - |A_1 \cap B|$.
2. Откуда немедленно $|A_1 \cap B| \geq 1$, т.е. $A_1 \cap B \neq \emptyset$.

□

7. Необходимое условие передаваемости

Установим достаточное условие того, что некий язык X не является передаваемым. Отрицание данного условия, соответственно, является необходимым условием передаваемости.

Определение 7.1. *Будем говорить, что язык* S *является предблокирующим для языка* X, *если выполнено следующее:*
1) $S \cap X = \emptyset$
2) $\forall \alpha \in S \ |succ_S(\alpha)| \geq k$

Определение 7.2. *Предблокирующий язык* S *блокирует* X, *если также* $\Lambda \in S$.

Интуитивно, условие 2) предблокирования — это условие того, что «если уж Алиса завела игру в какое-то состояние из S, то Ева может больше не выпускать Алису из S». Действительно, пусть $\alpha \in S$, тогда Ева своим ходом может оставить разрешенными лишь символы из $succ_S(\alpha)$. Ответный ход Алисы, таким образом, не выведет из S.

Соответственно, добавление условия 1) означает, что оставаясь в S, нельзя прийти ни к чему из X, а блокирование — что Алиса «ещё не начав игру, уже находится в S — ловушке».

Далее формализуем эти соображения.

Теорема 7.1. *Пусть S блокирует X. Тогда X не является передаваемым языком.*

Доказательство.
1. Предположим обратное. Пусть X — передаваемый язык. Тогда, согласно определению, найдется передающая его корректная стратегия Алисы f.
2. Положим $\hat{f}(\alpha) \stackrel{\text{def}}{=} f(\alpha, succ_S(\alpha))$ — ход Алисы из состояния α, если Ева оставила разрешенным множество символов $succ_S(\alpha)$.
3. Так как по условию блокирования $|succ_S(\alpha)| \geq k$, то согласно утверждению 6.3 $\alpha \in S \Rightarrow \alpha\hat{f}(\alpha) \in S$.
4. Зададим посредством индуктивного определения бесконечное слово $\alpha^\infty \in A^\infty$: $\alpha^\infty(1) \stackrel{\text{def}}{=} \hat{f}(\Lambda) = f(\Lambda, succ_S(\Lambda))$, $\alpha^\infty(i+1) \stackrel{\text{def}}{=} \hat{f}(\alpha^\infty(1)...\alpha^\infty(i)) = f(\alpha^\infty(1)...\alpha^\infty(i), succ_S(\alpha^\infty(1)...\alpha^\infty(i)))$.
5. Докажем по индукции, что $\forall m\ \alpha^\infty(1)...\alpha^\infty(m) \in S$.

5.1. Базис. $\Lambda \in S$. Согласно п.3, $\Lambda\hat{f}(\Lambda) = \alpha^\infty(1) \in S$.

5.2. Шаг индукции. Пусть $\alpha^\infty(1)...\alpha^\infty(m) \in S$. Тогда $\alpha^\infty(1)...\alpha^\infty(m)\alpha^\infty(m+1) = \alpha^\infty(1)...\alpha^\infty(m)\hat{f}(\alpha^\infty(1)...\alpha^\infty(m)) \in S$, согласно тому же пункту 3.
6. Положим $g : \mathbb{N} \to 2^A$, $g(1) \stackrel{\text{def}}{=} succ_S(\Lambda)$, $g(i+1) \stackrel{\text{def}}{=} succ_S(\alpha^\infty(1)...\alpha^\infty(i))$ — последовательность ходов Евы. По только что доказанному в п.5, а также уже упомянутому условию $\forall\alpha \in S\ |succ_S(\alpha)| \geq k$, эта последовательность ходов Евы является *допустимой*.
7. Очевидно, что выполнено $\alpha^\infty(1) = f(\Lambda, g(1))$, $\alpha^\infty(i+1) = f(\alpha^\infty(1)...\alpha^\infty(i), g(i))$, что по определению означает, что α^∞ согласовано с f, g.
8. Так как g — допустимая последовательность ходов Евы, а корректная стратегия f передает X, то некий начальный отрезок α^∞ лежит в X. То есть найдется такое m (в том числе это может быть и $m = 0$, что соответствует пустому слову Λ), такое что $\alpha^\infty(1)...\alpha^\infty(m) \in X$.
9. Таким образом, по п.5 и п.9 получаем: $\alpha^\infty(1)...\alpha^\infty(m) \in S \cap X$, что противоречит условию 1) предблокирования. Следовательно, предположение п.1 неверно, и X не является передаваемым языком.
ч.т.д.

□

8. Достаточное условие передаваемости

Пусть некоторым словам α приписаны какие-то числовые значения, и из состояния α с данным значением (*ненулевым*) Алиса всегда может выполнить ход, приводящий к состоянию, которому приписано меньшее значение. Также предположим, что Алиса не только может, но и всегда делает именно такой ход.

Тогда очевидно, что если пустому слову Λ приписано числовое значение, то за конечное число ходов Алисы состояние игры всегда оказывается среди слов, которым приписан 0. Следовательно, если все такие слова лежат в X, то X оказывается передаваемым языком.

Выразим сказанное формальным образом.

Определение 8.1. *Градуировка — это отображение* $d : A^* \to \{0\} \cup \mathbb{N} \cup \{+\infty\}$

Определение 8.2. $succ_d(\alpha) \stackrel{\text{def}}{=} \{a \in A | d(\alpha a) < d(\alpha)\}$ — *«множество (последних символов) последователей по градуировке», т.е. множество таких символов* a*, что значение градуировки на* αa *меньше, чем на исходном слове* α*.*

Определение 8.3. *Градуировка называется предправильной, если из* $0 < d(\alpha) < +\infty$ *следует* $|succ_d(\alpha)| \geq n - k + 1$

Определение 8.4. *Правильная градуировка — это предправильная, у которой* $d(\Lambda) < +\infty$*.*

Определение 8.5. $bott(d) \stackrel{\text{def}}{=} \{\alpha \in A^* | d(\alpha) = 0\}$ – *дно градуировки* d*. То есть это те слова, на которых она равна* 0*.*

Лемма 8.1. *Пусть* d *— предправильная градуировка. Тогда существует корректная стратегия Алисы* f*, такая что если* $0 < d(\alpha) < +\infty$ *и* $|B| \geq k$*, то* $d(\alpha f(\alpha, B)) < d(\alpha)$*.*

Доказательство.

1. Достаточно определить $f(\alpha, B)$ лишь при $|B| \geq k$, причем так, чтобы в этом случае $f(\alpha, B) \in B$. Во всех остальных случаях значение f можно выбрать произвольным: это не влиет на корректность. Далее рассматриваем только данный случай.

2. При $d(\alpha) = 0$ или $d(\alpha) = +\infty$ в качестве $f(\alpha, B)$ можно выбрать любой символ $a \in B$. ($|B| \geq k \geq 1 \Rightarrow B \neq \emptyset$). Аналогично, далее рассматриваем только случай $0 < d(\alpha) < +\infty$.
3. В обозначенном случае, так как по условию d — предправильно, $|succ_d(\alpha)| \geq n - k + 1$. И так как $|B| \geq k$, то согласно утверждению 6.5 $succ_d(\alpha) \cap B \neq \emptyset$.
4. В качестве $f(\alpha, B)$ выберем любое $a \in succ_d(\alpha) \cap B$.
5. Из определения $succ_d$ немедленно следует, что $d(\alpha a) < d(\alpha)$.
ч.т.д. □

Теорема 8.1. *Пусть d — правильная градуировка, и $bott(d) \subset X$. Тогда X — передаваемый язык.*

Доказательство.

1. Согласно предыдущей лемме, найдется такая корректная стратегия Алисы f, что при $0 < d(\alpha) < +\infty$, $|B| \geq k$ выполнено $d(\alpha f(\alpha, B)) < d(\alpha)$.
2. Зафиксируем $g : \mathbb{N} \to 2^A$ — допустимую последовательность ходов Евы, т.е. $\forall i \in \mathbb{N}\ |g(i)| \geq k$.
3. Пусть α^∞ — бесконечное слово, согласованное с f и g: $\alpha^\infty(1) = f(\Lambda, g(1))$, $\alpha^\infty(i+1) = f(\alpha^\infty(1)...\alpha^\infty(i), g(i+1))$.
4. Предположим, что никакой его начальный отрезок не лежит в X, т.е. $\Lambda \notin X$, $\forall m \in \mathbb{N}\ \alpha^\infty(1)...\alpha^\infty(m) \notin X$.
5. И, следовательно, так как $B(d) \subset X$, то $d(\Lambda) \neq 0$, $d(\alpha^\infty(1)...\alpha^\infty(m)) \neq 0$.
6. Докажем по индукции, что $\forall m \in \mathbb{N}$
$0 < d(\alpha^\infty(1)...\alpha^\infty(m)) < +\infty$ и $d(\alpha^\infty(1)...\alpha^\infty(m)\alpha(m+1)) < d(\alpha^\infty(1)...\alpha^\infty(m))$

6.1. Известно, что $d(\Lambda) < +\infty$, так как d — правильная градуировка, а также $d(\Lambda) \neq 0$ (п.5). Таким образом, $0 < d(\Lambda) < +\infty$. И, следовательно, согласно п.1,2: $d(\Lambda f(\alpha, g(1))) = d(\alpha^\infty(1)) < d(\Lambda) < +\infty$.

6.2. Также по п.5, $0 < d(\alpha^\infty(1))$.

6.3. Шаг индукции. Предположим, что $0 < d(\alpha^\infty(1)...\alpha^\infty(m)) < +\infty$. Тогда, согласно тем же п.1,2: $d(\alpha^\infty(1)...\alpha^\infty(m) f(\alpha^\infty(1)...\alpha^\infty(m), g(m+1))) = d(\alpha^\infty(1)...\alpha^\infty(m)\alpha^\infty(m+1)) < d(\alpha^\infty(1)...\alpha^\infty(m)) < +\infty$.

6.4. $0 < d(\alpha^\infty(1)...\alpha^\infty(m)\alpha^\infty(m+1))$ по п.5.
7. Таким образом, получаем: $+\infty > d(\Lambda) > d(\alpha^\infty(1)) > d(\alpha^\infty(1)\alpha^\infty(2)) > d(\alpha^\infty(1)\alpha^\infty(2)\alpha^\infty(3)) > ...$ — бесконечная убывающая последовательность натуральных чисел. Но такого не может быть в принципе, поэтому

предположение п.4 является ложным, т.е. некий начальный отрезок α^∞ лежит в X.
8. g было выбрано произольно. То есть для любой допустимой стратегии Евы g некий начальный отрезок согласованного с f и g бесконечного слова α^∞ лежит в X. Что и означает, что корректная стратегия f передает X.
9. И, следовательно, X — передаваемый язык.
ч.т.д.

□

9. Выигрышные состояния

Предположим, что Алиса уже привела игру в состояние α. И что $|succ_X(\alpha)| \geq n - k + 1$. Тогда, какой бы ход не сделала Ева, она не может запретить все символы из $succ_X(\alpha)$, и следовательно, Алиса сможет победить ответным ходом.

Стало быть, о таких α можно говорить как о «заведомо выигрышных для Алисы состояниях». Более того, это рассуждение можно повторять индуктивно: пусть для множества $\{\alpha a_1, ..., \alpha a_n\}$ уже известно, что хотя бы $n-k+1$ из них «заведомо выигрышны для Алисы». Тогда, аналогично, само α тоже может считаться «заведомо выигрышным».

Проведем формальное построение множества «заведомо выигрышных состояний» указанным образом.

Определение 9.1. $X' \stackrel{\text{def}}{=} \{\alpha \in A^* | \ |succ_X(\alpha)| \geq n - k + 1\}$ — *язык X, называемый производной языка X, т.е. ничто иное, как множество состояний, в которых Алиса «находится в одном шаге от X».*

Соответственно множество $X \cup X'$ может быть интерпретировано как множество состояний, в которых «Алиса находится в *не более чем одном* шаге от X».

Находиться в не более чем одном шаге от множества слов, находящихся в не более чем в одном шаге от X, значит находиться в не более чем в *двух* шагах от X. Соответственно, быть в не более чем одном шаге от нахождения в не более чем двух — это нахождение в *трех* шагах, и так далее.

Определение 9.2.
$X^{(0)} \stackrel{\text{def}}{=} X$
$X^{(i+1)} \stackrel{\text{def}}{=} X^{(i)} \cup (X^{(i)})'$

Утверждение 9.1. $X^{(0)} \subset X^{(1)} \subset X^{(2)} \subset X^{(3)} \subset X^{(4)} \subset ...$

Доказательство. Немедленно из определения: $X^{(i)} \subset X^{(i+1)}$ □

Таким образом, «находиться в не более, чем в n шагах от X» означает лежать в $X^{(n)}$.

И, стало быть, теперь можно определить, что значит «находиться в каком-нибудь конечном числе шагов от X». Что и означает «находиться в выигрышном для Алисы состоянии».

Определение 9.3. $X^{(\infty)} \stackrel{\text{def}}{=} \bigcup\limits_{i=0}^{\infty} X^{(i)}$

Все выигрышные состояния лежат в префиксном замыкании.

Утверждение 9.2. *Пусть $Z \subset pr(X)$. Тогда $Z' \subset pr(X)$.*

Доказательство.

1. Пусть $\alpha \in Z'$. Тогда $|succ_X(\alpha)| \geq n - k + 1 \geq 1$.
2. То есть найдется такой символ $a \in A$, что $\alpha a \in Z$.
3. По условию это тут же означает, что $\alpha a \in pr(X)$, т.е. найдется такое $\alpha' \in X$, что αa — префикс α'.
4. Следовательно, α — также префикс $\alpha' \in X$, а значит $\alpha \in pr(X)$.

ч.т.д.

□

Теорема 9.1. $X^{(\infty)} \subset pr(X)$.

Доказательство.

1. Базис индукции. $X = X^{(0)} \subset X^{(\infty)}$.
2. Шаг индукции. Пусть $X^{(i)} \subset pr(X)$. Тогда, по предыдущему утверждению, $(X^{(i)})' \subset pr(X)$, и следовательно, также $X^{(i+1)} = X^{(i)} \cup (X^{(i)})' \subset pr(X)$.
3. Все $X^{(i)} \subset pr(X)$, поэтому $X^{(\infty)} = \bigcup\limits_{i=0}^{\infty} X^{(i)} \subset pr(X)$.

ч.т.д.

□

10. Критерий передаваемости

Теперь можно задаться следующим вопросом: пусть некое $\alpha \in X^{(\infty)}$. В скольких шагах от победы находится Алиса, если она уже привела игру в состояние α?

Из определения очевидно, что если $\alpha \in X^{(\infty)}$, то найдутся такие k, что $\alpha \in X^{(k)}$. Для ответа на вышепоставленный вопрос нужно выбрать минимальное из таких k.

Тем самым, каждому $\alpha \in X^{(\infty)}$ можно приписать некую *степень*, выражаемую конечным числом. Всем остальным словам можно приписать бесконечную степень, и тем самым получить некую *градуировку.*

Определение 10.1. *Градуировка* $deg_X : A^* \to \{0\} \cup \mathbb{N} \cup \{+\infty\}$ *определяется как* $deg_X(\alpha) \stackrel{\text{def}}{=} \begin{cases} min\{k|\alpha \in X^{(k)}\}, & \alpha \in X^{(\infty)} \\ +\infty, & \alpha \notin X^{(\infty)} \end{cases}$

Утверждение 10.1. $bott(deg_X) = X$

Доказательство.

1. Пусть $deg_X(\alpha) = 0$. Из определения deg_X немедленно вытекает, что $\alpha \in X^{(0)} = X$.
2. Обратно, пусть $\alpha \in X = X^{(0)}$. Тогда, очевидно, $deg_X(\alpha) = 0$.

□

Утверждение 10.2. $X^{(\infty)} \setminus X = \{\alpha \in A^* | 0 < deg_X(\alpha) < +\infty\}$

Доказательство.

1. Из определения ясно, что $\alpha \in X^{(\infty)} \Leftrightarrow deg_X(\alpha) < +\infty$.
2. По предыдущему утверждению $\alpha \notin X \Leftrightarrow deg_X(\alpha) > 0$.

□

Установим тривиальные свойства:

Утверждение 10.3. *Пусть* $\alpha \in X^{(k)}$. *Тогда* $deg_X(\alpha) \leq k$.

Доказательство. Очевидно по определению. □

Утверждение 10.4. *Пусть* $deg_X(\alpha) = k$, $k < +\infty$. *Тогда* $\alpha \in X^{(k)}$.

Доказательство. Очевидно по определению. □

А также более сложные:

Утверждение 10.5. *Пусть* $deg_X(\alpha) = k$, $0 < k < +\infty$. *Тогда* $\alpha \in (X^{(k-1)})'$.

Доказательство.

1. Из условий и предыдущего утверждения: $\alpha \in X^{(k)}$.
2. Если бы $\alpha \in X^{(k-1)}$, то было бы $deg_X(\alpha) \leq k-1 < k$. Следовательно, $\alpha \notin X^{(k-1)}$.
3. $\alpha \in X^{(k)} = X^{(k-1)} \cup (X^{(k-1)})'$, $\alpha \notin X^{(k-1)} \Rightarrow \alpha \in (X^{(k-1)})'$.

□

Утверждение 10.6. *Пусть* $deg_X(\alpha) = k$, $0 < k < +\infty$.
Тогда $succ_{deg_X}(\alpha) = succ_{X^{(k-1)}}(\alpha)$

Доказательство.

I. ($\Rightarrow$)
1. Пусть $a \in succ_{deg_X}(\alpha)$. Это означает, что $deg_X(\alpha a) < deg_X(\alpha) = k$. Обозначим $k' = deg_X(\alpha a)$, тогда $k' < k$, что равносильно $k' \leq k-1$.
2. Тогда $\alpha a \in X^{(k')} \subset X^{(k-1)}$.
3. И, следовательно, $a \in succ_{X^{(k-1)}}(\alpha)$.

II. ($\Leftarrow$)
1. Пусть теперь $a \in succ_{X^{(k-1)}}(\alpha)$. Тогда $\alpha a \in X^{(k-1)}$.
2. Следовательно, $deg_X(\alpha a) \leq k-1 < k = deg_X(\alpha)$
3. $deg_X(\alpha a) < deg_X(\alpha) \Rightarrow a \in succ_{deg_X}(\alpha)$
ч.т.д.

□

Всё готово для получения важного промежуточного результата.

Лемма 10.1. *Для любого языка* X *градуировка* deg_X *является предправильной.*

Доказательство.

1. Пусть α — такое слово, что $0 < deg_X(\alpha) < +\infty$.
2. Тогда по утверждению 10.5 $\alpha \in (X^{(k-1)})'$. Это означает, что $|succ_{X^{(k-1)}}(\alpha)| \geq n-k+1$

3. Но по утверждению 10.6 $|succ_{deg_X}(\alpha)| = |succ_{X^{(k-1)}}(\alpha)| \geq n-k+1$
4. Что и требуется определением предправильной градуировки.
ч.т.д.

□

Дополнение $A^* \setminus X^{(\infty)}$ также обладает интересным свойством:

Лемма 10.2. *$A^* \setminus X^{(\infty)}$ — предблокирует язык X.*

Доказательство.

1. Так как $X = X^{(0)} \subset X^{(\infty)}$, то $(A^* \setminus X^{(\infty)}) \cap X = \emptyset$. Тем самым, выполнено условие 1) предблокирования.
2. Предположим, что условие 2) не выполнено, тогда найдется $\alpha \in A^* \setminus X^{(\infty)}$ такое, что $|succ_{A^* \setminus X^{(\infty)}}(\alpha)| < k$.
3. Пользуясь утверждением 6.2, это можно переписать как $|succ_{X^{(\infty)}}(\alpha)| > n-k$.
4. И, следовательно, найдутся (хотя бы) $n-k+1$ различных символов $a_1, ..., a_{n-k+1}$ такие, что $\alpha a_1, ..., \alpha a_{n-k+1} \in X^{(\infty)}$.
5. Стало быть, найдутся также такие $i_1, ..., i_{n-k+1}$, что $\alpha a_1 \in X^{(i_1)}, ..., \alpha a_{n-k+1} \in X^{(i_{n-k+1})}$.
6. Положим $i = \max(i_1, ..., i_{n-k+1})$. Тогда все $\alpha a_1, ..., \alpha a_{n-k+1} \in X^{(i)}$.
7. Из этого вытекает, что $a_1, ..., a_{n-k+1} \in succ_{X^{(i)}}(\alpha)$.
8. Таким образом, $succ_{X^{(i)}}(\alpha) \supset \{a_1, ..., a_{n-k+1}\}$. Откуда, естественно, $|succ_{X^{(i)}}(\alpha)| \geq n-k+1$.
9. Это означает, что $\alpha \in (X^{(i)})'$. Так как $X^{(i+1)} = X^{(i)} \cup (X^{(i)})'$, то и $\alpha \in X^{(i+1)} \subset X^{(\infty)}$.
10. Согласно п.2, $\alpha \in A^* \setminus X^{(\infty)}$. Согласно п.9, $\alpha \in X^{(\infty)}$. Получившееся противоречие показывает, что предположение из п.2 неверно, т.е. выполнен условие 2) предблокирования.
ч.т.д.

□

Сформулируем фундаментальный критерий (и докажем его, собрав вместе результаты ранее проделанной работы), позволяющий «заменить определение передаваемости» (т.е. необходимое и достаточное условие), и далее при исследовании передаваемых языков не иметь дело с стратегиями Алисы, допустимимыми последовательностями ходов Евы и т.д.

Теорема 10.1. *Язык X передаваем тогда и только тогда, когда $\Lambda \in X^{(\infty)}$.*

Доказательство.

I. ($\Leftarrow$)
1. Пусть $\Lambda \in X^{(\infty)}$.
2. Тогда $deg_X(\Lambda) < \infty$. И, следовательно, $\deg_X$ — правильная градуировка. (предправильной она же уже является по лемме 10.1)
3. Также, согласно утверждению 10.1 $bott(deg_X) = X$. И, следовательно, согласно достаточному условию (теорема 8.1) X — передаваемый язык.

II. ($\Rightarrow$)
1. Пусть $\Lambda \notin X^{(\infty)}$. Переформулируем: $\Lambda \in A^* \setminus X^{(\infty)}$.
2. Тогда $A^* \setminus X^{(\infty)}$ — блокирует X. ($A^* \setminus X^{(\infty)}$ предблокирует X по лемме 10.2)
3. Согласно теореме 7.1 этого достаточно для того, чтобы X не являлся передаваемым языком.
ч.т.д.

□

Замечание. *Из представленных рассуждений можно видеть, как именно должна действовать Алиса, если язык передаваем, и как же должна действовать Ева, если нет. В случае передаваемости Алисе на каждом ходу следует выбирать символ из $succ_{deg_X}(\alpha)$, в случае непередаваемости Еве следует «не пускать Алису в $X^{(\infty)}$»*

11. Одновременно передаваемые языки

В данном разделе будет приведен главный результат настоящей работы. Доказывать мы его начнем с изучения некоторых специфических свойств, относящихся к *парам* языков X, Y (а точнее относящихся к ним предправильных градуировок deg_X, deg_Y).

Лемма 11.1. *Пусть X, Y — произвольные языки, и для некоего слова α выполнено: $0 < deg_X(\alpha) < +\infty$, $0 < deg_Y(\alpha) < +\infty$. А также верно $n > 2k - 2$.*
Тогда найдется символ a такой, что $deg_X(\alpha a) < deg_X(\alpha)$, $deg_Y(\alpha a) < deg_Y(\alpha)$

Доказательство.

1. Так как градуировки deg_X, deg_Y (см. лемму 10.1) предправильны, то $|succ_{deg_X}(\alpha)|, |succ_{deg_Y}(\alpha)| \geq n - k + 1$.
2. Согласно утверждению 6.4, из этого следует, что $succ_{deg_X}(\alpha) \cap succ_{deg_Y}(\alpha) \neq \emptyset$.
3. Выберем некое $a \in succ_{deg_X}(\alpha) \cap succ_{deg_Y}(\alpha)$. Тогда по определению «последователей по градуировке» $deg_X(\alpha a) < deg_X(\alpha)$, $deg_Y(\alpha a) < deg_Y(\alpha)$.
ч.т.д

□

Изучим также свойства $X^{(\infty)}, Y^{(\infty)}$, следующие из кросспрефиксности:

Утверждение 11.1. *Пусть X, Y — кросспрефиксны. Тогда*
1) $(X^{(\infty)} \cap Y^{(\infty)}) \cap X = \emptyset$
2) $(X^{(\infty)} \cap Y^{(\infty)}) \cap Y = \emptyset$

Доказательство.

1. $X^{(\infty)} \subset pr(X) \Rightarrow (X^{(\infty)} \cap Y^{(\infty)}) \cap Y \subset X^{(\infty)} \cap Y \subset pr(X) \cap Y = \emptyset$, согласно кросспрефиксности.
2. $Y^{(\infty)} \subset pr(Y) \Rightarrow (X^{(\infty)} \cap Y^{(\infty)}) \cap X \subset Y^{(\infty)} \cap X \subset pr(Y) \cap X = \emptyset$, аналогично.

□

Оказывается, при выполнении условия $n > 2k - 2$, если существует какое-то общее выигрышное состояние $\alpha \in X^{(\infty)} \cap Y^{(\infty)}$, то существует целый «бесконечный спуск» таких состояний.

Лемма 11.2. *Пусть X, Y — кросспрефиксны, $\alpha \in X^{(\infty)} \cap Y^{(\infty)}$, $n > 2k - 2$. Тогда найдется такое $a \in A$, что $\alpha a \in X^{(\infty)} \cap Y^{(\infty)}$, причем $deg_X(\alpha a) < deg_X(\alpha)$, $deg_Y(\alpha a) < deg_Y(\alpha)$*

Доказательство.

1. По предыдущему утверждению, из условия $\alpha \in X^{(\infty)} \cap Y^{(\infty)}$ следует, что $\alpha \notin X$, $\alpha \notin Y$.
2. Так как $\alpha \in X^{(\infty)}, \alpha \notin X$, то $0 < deg_X(\alpha) < +\infty$. (см. утверждение 10.2)
3. Аналогично $\alpha \in Y^{(\infty)}, \alpha \notin Y \Rightarrow 0 < deg_Y(\alpha) < +\infty$
4. Применяя лемму 11.1, находим символ $a \in A$ такой, что $deg_X(\alpha a) < deg_X(\alpha)$, $deg_Y(\alpha a) < deg_Y(\alpha)$.

5. При этом $deg_X(\alpha a) < deg_X(\alpha) < +\infty$, $deg_Y(\alpha a) < deg_Y(\alpha) < +\infty$, а значит $\alpha a \in X^{(\infty)}$, $\alpha a \in Y^{(\infty)}$
ч.т.д.

□

Однако, «бесконечных спусков» *с убывающей на каждом шаге степенью* не может быть.

Лемма 11.3. *Пусть X, Y — кросспрефиксная пара языков, $n > 2k - 2$. Тогда $X^{(\infty)} \cap Y^{(\infty)} = \emptyset$.*

Доказательство.

1. Пусть $\alpha \in X^{(\infty)} \cap Y^{(\infty)}$.
2. Тогда, индуктивно применяя (это возможно, так как заключение леммы относительно αa «повторяет условие») предыдущую лемму, построим *бесконечную* последовательность слов $\alpha, \alpha a_1, \alpha a_1 a_2, \alpha a_1 a_2 a_3, ... \in X^{(\infty)} \cap Y^{(\infty)}$
3. При этом $deg_X(\alpha) > deg_X(\alpha a_1) > deg_X(\alpha a_1 a_2) > deg_X(\alpha a_1 a_2 a_3) > ...$ и $deg_Y(\alpha) > deg_Y(\alpha a_1) > deg_Y(\alpha a_1 a_2) > deg_Y(\alpha a_1 a_2 a_3) > ...$ — бесконечные убывающие последовательности натуральных чисел.
4. Бесконечных убывающих последовательностей натуральных чисел не существует.
ч.т.д.

□

Замечание. *Сам по себе «бесконечный спуск в $X^{(\infty)}$» (без убывания степени) существовать может. Построим пример.*

Положим $n = 3, k = 2$, $A = \{a_1, a_2, a_3\}$. Язык X составим из слов вида $a_1, a_2 a_1, a_2 a_2 a_1, a_2 a_2 a_2 a_1, ...$, а также вида $a_2, a_2 a_3, a_2 a_2 a_3, a_2 a_2 a_2 a_3, ...$

Тогда все слова $a_2, a_2 a_2, a_2 a_2 a_2 ... \in X' \subset X^{(1)} \subset X^{(\infty)}$ — образуют «бесконечный спуск».

Это показывает, что вышеприведенные рассуждения «не могут быть упрощены», то есть для получения противоречия, недостаточно продемонстрировать сам факт того, что существует бесконечный спуск (а это может быть сделано без использования понятия степени deg_X)

Финальный результат.

Теорема 11.1. *Пара одновременно передаваемых кросспрефиксных языков X, Y существует тогда и только тогда, когда $n \leq 2k - 2$*

Доказательство.

I. При $n > 2k - 2$
1. Если X, Y передаваемые языки, то согласно критерию (теорема 10.1) $\Lambda \in X^{(\infty)} \cap Y^{(\infty)}$.
2. Однако, это запрещено предыдущей леммой.
II. При $n \leq 2k - 2$.
1. См. пример, построеный в разделе 5 «Особый случай».

□

Замечание. *Таким образом, при выполнении условия $n \leq 2k - 2$ Алиса и Боб могут построить скрытый канал, имеющий пропускную способность 1 бит на каждый передаваемый Алисой символ.*

Полученный результат означает, что передача информации при поставленных условиях или осуществляется весьма тривиальным образом (при $n \leq 2k - 2$ с помощью языков X, Y, в которых все слова являются односимвольными), или же вовсе невозможна. Как видно из представленных в работе рассуждений, для того, чтобы Ева могла гарантированно сорвать передачу информации от Алисы к Бобу, ей достаточно знать используемую пару кросспрефиксных языков и какое именно значение (0 или 1) Алиса в этот раз намеривается передать Бобу.

Другим важным результатом, который может быть использован в дальшейшем, является представленный в работе критерий (теорема 10.1), дающий исчерпывающий ответ на вопрос о передаваемости языка.

В настоящей работе изучался лишь вопрос того, возможна ли *гарантированная* передача при *любых возможных* помехах. Это соответствует тому предположению, что Ева ведёт идеальную игру. Однако, реальные запрещения направлений передвижений по плоскости в online-игре таковыми, разумеется, не являются, так как возникают весьма случайно. Следовательно, в подавляющем большинстве случаев, Алиса успешно пересылает информацию Бобу, а случайный срыв передачи происходит на самом деле с исчезающе малой вероятностью.

Изучение подобных вопросов выходит за рамки настоящей статьи и будет предпринято в последующих работах. Однако, для примера, рассмотрим далее один частный случай.

Позволим Еве *менять* множество запрещенных символов не на каждом ходе, а например, раз в два хода. Это означает, что на ходах с номерами $2s, 2s+1$ Алисе разрешены к передаче *одни и те же* символы. Соответственно принятым ограничениям очевидным образом модифицируется понятие «допустимой последовательности ходов Евы», и, следовательно, понятие «передаваемого языка».

Положим $k = 2, n = 3$, и рассмотрим пару (кросспрефиксных) языков $X = \{a_0a_0, a_1a_1, a_2a_2\}$, $Y = \{a_1a_2, a_2a_0, a_0a_1\}$. На первом ходу Ева может запретить для Алисы лишь какой-то один символ из $\{a_0, a_1, a_2\}$, и *тот же самый* символ она должна запретить и на втором ходу.

Если запрещается a_0, то в языке X есть слово a_1a_1, которое может передать Алиса при данном решении Евы. Соответственно, в Y есть a_1a_2. Аналогично, для a_1: $a_2a_2 \in X$ и $a_2a_0 \in Y$, а для a_2: $a_0a_0 \in X$ и $a_0a_1 \in Y$. Остался лишь случай, когда Ева выбрала вообще не запрещать никаких символов. Однако, он тривиален: тогда Алиса может передать любое из слов в языках X, Y.

Таким образом, X, Y — «передаваемые языки». А следовательно, с принятым ограничением (для прочих n, k подобные языки конструируются аналогично) передача информации осуществима.

Список литературы

[1] Lampson B. W., A Note on the Confinement Problem. *Communications of the ACM* (1973) **16**:10, 613–615.

[2] Llamas D, Allison C, Miller, A., Covert channels in internet protocols: a survey. *Proceedings of the 6th Annual Postgraduate Symposium about the Convergence of Telecommunications, Networking and Broadcasting, PGNET*, 2005.

[3] Zander S., Armitage G., Branch P., Covert channels in multiplayer first person shooter online games, *2008 33rd IEEE Conference on Local Computer Networks, LCN*, 2008, 215–222.

Reliabilty criterion for channels with prohibitions

Kazakov I.B.

We investigate the possibility of reliable transmission in a situation when an adversary can prohibit some characters, and a set of prohibitions can change at every clock cycle. We show that reliable transmission is possible if and only if the cardinality of the alphabet n and the number of allowed characters k satisfy the inequality $n \leq 2k-2$.

Keywords: covert channels, walks in a plane, character prohibition, transmittable language