УДК 004.83

КИТАЙСКАЯ КОМНАТА И СИСТЕМЫ ШИФРОВАНИЯ

Протько М.А., студент гр.050502

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Борисенко О.Ф. – канд. физ.-мат. наук

Аннотация. Рассматривается мысленный эксперимент и его влияние на производительность систем машинного обучения в области шифрования.

Ключевые слова. Генетический алгоритм, нейронные сети, эволюция, «китайская комната».

Введение

Рассмотрим мысленный эксперимент, описанный в [1]. Суть его проста. Вы – человек, не знающий китайского языка и находящийся в замкнутом пространстве. У вас есть инструкция, которую вы неукоснительно выполняете, и заключается она в следующем: когда вы видите некий символ, вы находите этот же символ, и инструкцию, позволяющую вам ответить на этот символ. Ваш собеседник за дверью комнаты наверняка может подумать, что вы знаете китайский язык. На деле вы лишь следуете предписанной инструкции.

Данный мыслительный эксперимент приводит к очень четкому выводу, о том, что же такое понимание. «свойство программ — их чисто формальный или синтаксический характер — фатально для взгляда, согласно которому ментальные и программные процессы тождественны друг другу. Объяснить это можно очень просто. Сознание есть нечто большее, чем формальные или синтаксические процессы. Наши внутренние ментальные состояния, по определению, обладают содержанием.» (глава 2 из [1]). Т.е., мы не можем сказать «машина понимает», пока единицы, с которыми она работает, не обладают неким семантическим смыслом.

То, что все операции определены лишь синтаксически и максимально абстрактно позволяет описать многие линейные задачи и выполнить их вне зависимости от самой программы, в которой они находятся, а также аппаратуры, в которой они выполняются.

Но что необходимо обеспечить в ситуации, когда нужно обращать внимание на семантику?

Рассмотрим следующую задачу [2]: в нашей системе есть изначальный алфавит. Каждому участнику системы разрешается создавать свою версию алфавита, посредством подстановок и перестановок символов (операции на множестве вычетов). Каждому участнику выдаются фрагменты изначального текста. Их задача сделать так, чтобы при обмене зашифрованным текстом соперник не смог его расшифровать. До участия в игре ни один из участников не знает ни одного шифра. Он знает лишь, что его соперник говорит с ним на одном языке.

Человек справится с этой задачей, но возможно ли на формальной логике не допускающей семантику решить данную задачу?

Какие решения мы можем использовать и как поймем, что решение найдено?

Целевая функция и криптостойкость

Для решения поставленной задачи воспользуемся генетическими алгоритмами (далее – г.а.).

В целях упрощения, рассмотрим системы симметричного шифрования.

Согласно [3], г.а. используются для решения задачи оптимизации. Т.е. поисков экстремумов некой функции. Опишем эту функцию для поставленной задачи по аналогии с [4].

$$f(a,b) = \cup_{j,i}^{c,k}(a_i * b_j) mod\ n\ ,\ i = \overline{1,k}, j = \overline{1,c}\ , \quad (1)$$

где f(a,b) – некая функция симметричного шифрования (биекция), a и b – множество символов текста и ключа соответственно, k – количество символов текста, c - количество символов ключа, n – мощность алфавита символов, * - любая обратимая операция на множестве вычетов n.

Видимых ограничений для использования этой функции в данной задаче нет.

Содержательное значение поиска экстремума данной функции такого: поскольку мы не ограничиваем выбор * и порядка i и j, согласно свойству шифра, называемого криптостойкостью, нам необходимо найти множество таких значений f(a,b), что не должно существовать полиномиального алгоритма, который, имея половину строки s (где s – строка объединений символов из функции f(a,b)) последовательности, сможет предсказать k + 1 бит с вероятность большей 50%.

Т.е. в ситуации, когда мы несколько раз применим (1), мы должны получать дискретное равномерное распределение для каждого элемента из n, даже если этот элемент не встречается в a и b.

Определим на основании вышеописанных требований г.а.

«Хромосомой» в г.а. выступает алгоритм по шагам, где слот представлен неким действием (взять элемент из a или b, совершить * и т.д.).

Способы выбора генотипов для скрещивания и видоизменения в данной работе рассмотрены не будут.

Дадим определение фитнес-функции согласно [3].

$$\mu(s) = \frac{1}{n}\sum_{i=1}^{n} p(u_i) \quad (2)$$

где s – отбираемый генотип («хромосома» г.а.), $p(u_i)$ – вероятность встречи u_i символа, u_i - символ, полученный с помощью f(a,b), где n – мощность множества a.

Расчет данной функции можно в дальнейшем упрощать с помощью свойств дискретного равномерного распределения.

В данном случае, чем ближе результат μ(s) к 1/n, тем лучше. Т.е., данный генотип будет отобран в дальнейшие популяции, продолжая свое развитие.

$$\lim_{n\to\infty} \mu\,(s) = \frac{1}{n} \quad (3)$$

Т.е., выборка генотипов для следующей популяции будет основываться на близости к пределу μ(s).

Одной из возможных реализаций (2) в г.а. будет составление множеств s_1 и s_2, полученных из f(a,b) и f(c,b) с мощностью множеств a и c равной n, а затем проверка (4):

$$(s_1 \cap s_2) \underset{n\to\infty}{\longrightarrow} \emptyset \quad (4)$$

Выводы – можем ли мы решить поставленную задачу?

Да. Но в худшем случае нам придется рассмотреть все возможные комбинации из s (число размещений из w всевозможных слотов предусмотренных в г.а.).

Согласно [3], особенности г.а., которые не позволяют получить решение поставленной задачи при описанных условиях таковы:

- г.а. оперирует закодированным множеством параметров, а не с самими параметрами
- в г.а. применяется вероятностное правило перехода, а не детерминистическое

Из чего следует, что, используя г.а, мы получаем NP-задачу (перебор всех вариантов).

Полученный г.а. – самоадаптирующийся (согласно определению из [3]). Откуда следует, что он зависит от случайного выбора. Если рассмотреть все возможные решения s на отображении μ(s), может получиться ситуация с очень большим разбросом локальных экстремумов. Что значительно влияет на скорость поиска решения.

Также данная реализация никак не учитывает выбор параметров i и j из (1), когда эти индексы должны описываться также некими обратимыми функциями.

В данной реализации совершенно не учитывается семантический смысл выполняемого алгоритма. Она строго формализована, но практическое применение данному алгоритму получить так и не удалось [2].

Если возвращаться к аналогии с «китайской» комнатой, мы получили эксперимент, где человеку не была выдана инструкция по выбору подходящих иероглифов.

«Эволюция» и нейронные сети

Попытаемся учесть вышеописанные пункты используя нейронные сети.

Учитывая изначальные условия задачи, нам необходима самоорганизующаяся сеть – «Без учителя». В этом случае нейронная сеть формирует выходное пространство решений только на основе входных воздействий.

Об устройстве нейронной сети (далее н.с.) и её свойствах подробнее в [5].

Для использования н.с. следует ответить на следующие вопросы:

- реализуемый «алгоритм» (см. далее)
- максимальное число слоев
- Функция активации

На данные вопросы может ответить практическая реализация с сравнением получаемых характеристик и параметров.

Объединим г.а. и н.с. следующим образом:

Целевая функция останется как в (2), но генотип будет описывать не алгоритм по шагам, а нейронную сеть. Каждая единичная операция в данном случае будет представлять характеристику веса, или количество промежуточных слоев, или связь между конкретными нейронами.

Разобьем «хромосому» г.а. на три элемента: ген, кодирующий f(a) – обратимую функцию, выдающую псевдослучайную последовательность i и j для (1) и ген, кодирующий операцию *, а также ген, который объединяет параметры в (1).

В данном случае, разбиение «хромосомы» на гены описывает «алгоритм», реализуемый нейронной сетью.

В данном случае нам уже необходимо учитывать три подобные друг другу независимые целевые функции для каждого гена.

Можем ли мы сказать, что, реализовав такую систему, мы получим решение данной задачи? Да. Будет ли оно оптимальным для заданных условий, к тому же, реализуемым (под реализацией имеется в виду количество поколений с учетом вероятности получения сходящихся последовательностей г.а. в случайной точке, иначе – сколько вычислений необходимо произвести, чтобы получить результат, и в скольких итерациях получить его невозможно)? Нет, поскольку использование параметра криптостойкости без учета семантики не гарантирует создание шифра (изначально криптостойкость – параметр, учитывающий использование прочих алгоритмов, помимо простого перебора, а также возможностей частотного анализа).

Определим необходимую семантику [1] через использование принципа «естественного отбора».

Под семантикой в данном случае будем понимать наличие некого содержания.

Рассмотрим некое пространство, в котором будут существовать фенотипы популяции описанного г.а. У каждого фенотипа, далее называемого особью, будет определено время жизни. Особь будет продолжать существование, пока она способна выдать результат (1). Конкуренция между особями будем заключаться в поочередном применении параметра (2) к особи. У каждой особи есть возможность вычислить как (1), так и (2). Во время итерации на этапе отбора (см. [3]), между двумя особями будет проводиться соревнование на основе (2). Причем способ расчета вероятности оставляется на формируемую генотипом нейронную сеть.

Выводы:

Мы не можем в данном случае проверить избыточность данного разбиения, как и его оптимальность. Не можем также определить работоспособность топологии. Возможно ли оптимизировать этот процесс?

В данном случае, у нас имеется ситуация, когда была найдена лишь корреляция, а не причинно-следственные связи. Проблема китайской комнаты все также существенна для этого решения. Можно привести пример с дрессировкой собаки, которая включает свет, нажимая на кнопку. Можно ли сказать, что собака понимает предназначение кнопки? Проверить это очень просто – если избавиться от лампочки в данной цепочке, собака все так же будет жать на кнопку. Понятия «кнопка – свет- награда» и «кнопка - награда» для нее равноценны. Точнее, для собаки это выглядит так «действие – награда». Пока она не поймет сематический смысл «действия» («найти кнопку – включить свет – увидеть награду») она не научиться включать и выключать свет. (подробнее об этом вопросе в [6])

Аналогично, пока в описанной системе не получится избавиться от формальных целевых функций, мы будем получать все ту же «китайскую комнату».

Но возможно ли создать такую вычисляемую систему?

Заключение

Рассмотренные в данной работе решения поставленной задачи позволяют в полной мере определить необходимость в наполненности семантическим смыслом. Используя генетические алгоритмы и нейронные сети возможно добиться весьма впечатляющих результатов, но только если они уже были повторены человеком. Т.е., данная система не способна выйти за рамки изначально предположенного решения задачи. По-другому ее просто невозможно сформулировать. Если использовать генетические алгоритмы, мы могли бы чисто случайным образом наткнуться на способ, о котором не подозревали. Но сможем ли мы распознать это решение, если его не понимаем?

Возможно, ответить на данный вопрос позволит идея клеточных автоматов. С их помощью, при определении нескольких правил возможно симулировать даже работу составляющих компьютера [7]. Уже существуют реализации, использующие нейронные сети и клеточные автоматы [8].

Если определить правила клеточных автоматов, как аксиомы некого пространства, нейронные сети – как функции, а генетический алгоритм – как функцию отбора желаемых параметров, то возможно получить систему, выходящую за рамки предположенных решений. Т.е., если правила системы будут составляться на основании простейших шифров подстановки и перестановки, но с учетом тех свойств, которые присущи всем симметричным шифрам, используя достаточное количество усложнений, можно прийти к фундаментальным принципам, заложенных в них, таким образом создавая (или же узнавая) новые шифры или решения, о которых изначально не было известно.

Список использованных источников:

1. *Searle J. Minds, Brains and Science. / Перевод на русский язык: А. Ф. Грязнов. — М., 1993. Глава 2. «Могут ли компьютеры мыслить?».*
2. *Протько, М.А., Борисенко, О.Ф Простейшие шифры и генетический алгоритм / репозиторий БГУИР. 2023. - 24 с.*
3. *Панченко, Т.В. Генетические алгоритмы: учеб.пособие / под ред. Ю. Ю. Тарасевича. — Астрахань : Издательский дом «Астраханский университет», 2007. — 87 с*
4. *Уральский Н.Б., Сизов В.А., Капустин Н.К. Оптимизация вычислительного процесса фитнесс функции генетического алгоритма в распределённых системах обработки данных // Интернет-журнал «Науковедение» ISSN 2223-5167; Том 7, N 6 (2015).*
5. *Головко В.А, Краснопрошин В.В. Нейросетевые технологии обработки данных: учеб.пособие – Минск : БГУ, 2017. – 263 с.*
6. *Протько М.А. Формализация и исследование операций замкнутых систем // материалы 59 конференции студентов, магистрантов и аспирантов БГУИР, 2023.*
7. *Nicolas Loizeau Building a computer in Conway's game of life – Источник : https://www.nicolasloizeau.com/gol-computer Дата доступа:7.04.2023.*
8. *Gabriel Morariu, Hugo Lamarche, Elizabeth Pyvovarov and Karl-Philippe Bluteau Creation of alternate Game of life realities and rules using Neural Networks - Источник : https://medium.com/@flygongaby/creation-of-alternate-game-of-life-realities-and-rules-using-neural-networks-4db169f30adc. Дата доступа: 7.04.2023.*

UDC 004.83

CHINESE ROOM AND ENCRYPTION SYSTEMS

Protsko M.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Borisenko O.F. – PhD in Physics and Mathematics

Annotation. Contains influence of one thought experiments in relation of machine learning systems in the field of encryption.

Keywords. Genetic algorithm, neural networks, evolution, "chinese room".