
**Artificial societies. 2013-2021**

ISSN 2077-5180

URL - http://artsoc.jes.su



Issue 1-4 Volume 11. 2016

# The reason

## Timur Gataullin

### Abstract

This article represents the short review of Ignasi Beld's book «Reason, machines and mathematics. Artificial intelligence and its tasks» / translation from Spanish. - Moscow: De Agostini, 2014. Follows from the name of the book that the book is devoted to the «Reason» concept, but what is it - remained unknown after acquaintance to this book. This work is popular introduction to a subject of artificial intelligence. In Russia there are many experts (we call only V. L. Makarov and D. V. Pospelov), who could write similar introduction not worse, and, perhaps, more better. This book contains a short list and the description of the main objectives and methods of artificial intelligence. However in these descriptions some important points are missed. This descriptions are stated in the books published in Soviet period and will be hardly republished. In this article we briefly will stop on some of them.

**Keywords list (en):** Reason, machines, an artificial intelligence, complexity of algorithms according to A. N. Kolmogorov, the Turing machine, cryptography protocols

**Date of publication:** 29.12.2016

**Citation link:**

Gataullin T. The reason // Artificial societies. – 2016. – V. 11. – Issue 1-4 [Electronic resource]. URL: https://artsoc.jes.su/s207751800000010-0-3/ (circulation date: 08.05.2021).

1 «Пильман: - Да. И все было бы хорошо, если бы мы знали, что такое разум. Нунан: - А разве мы не знаем?» Из беседы Нобелевского лауреата В.Пильмана с рядовым чиновником Р. Нунаном из Международного института в «Пикнике на обочине» Стругацких.

2 Из названия книги «Разум, машины и математика» [1] следует, что она посвящена в том числе «разуму», но что это такое - осталось неизвестным и эпиграф свидетельствует, что не только автору данной заметки. Приведем оглавление книги:

Глава 1. Что такое искусственный интеллект

Глава 2. Поиск

Глава 3. Машинное обучение

Глава 4. Автоматическое планирование и принятие решений.

Глава 5. Анализ данных

Глава 6. Искусственная жизнь

Книга представляет собой популярное введение в тему искусственного интеллекта. У нас в России есть немало специалистов (например, В. Л. Макаров и Д. А. Поспелов), которые могли бы написать подобное введение не хуже, а, пожалуй, даже лучше. Приведенное выше содержание книги содержит вкратце перечень и описание важнейших методов и задач искусственного интеллекта. Однако в этих описаниях некоторые важные моменты упущены. Они содержатся в книгах, изданных еще в советское время, и вряд ли эти книги будут переизданы. В этой заметке мы кратко остановимся на некоторых из них. Так, в первой главе много внимания уделено тесту Тьюринга, который должна пройти машина, чтобы беседующий с ней живой человек согласился считать эту машину разумной. Сам Тьюринг придумал этот свой тест еще до второй мировой войны, но затем было найдено много контрдоводов против этого теста. Основа всех этих доводов - уход активной стороны от содержательной основы беседы в чисто формальную переделку вопросов и ответов беседы. Пример подобной переделки приведен в одной из книг Д. А. Поспелова [2]. В рецензируемой книге описана «китайская комната» - мыслимый эксперимент, предложенный Д. Серлем в 1980 г. в известной статье «Minds, Brains, and Programs», который, в частности, является критикой теста Тьюринга. Тематика проблем, связанная с тестом Тьюринга до сих пор привлекает к себе внимание исследователей. В этой связи отметим лишь диссертацию А. Ю. Алексеева на соискание ученой степени доктора философских наук «Философия искусственного интеллекта: концептуальный статус комплексного теста Тьюринга» [3]. И еще одно замечание, относящееся ко всем материалам книги по искусственному интеллекту. Оно связано со сложностью рассматриваемых алгоритмов. Это понятие и основные утверждения о сложности были впервые введены и рассмотрены нашим великим соотечественником А. Н. Колмогоровым [4]. Эти вопросы достаточно сложны. Один из ведущих математиков мира С. Смейл, который по просьбе В. Арнольда, занимавшего в то время пост Президента международного математического союза, составил список из 18 нерешенных математических проблем, включил данный вопрос в число важнейших нерешенных проблем XXI века [5]. Например, необходимо ответить на вопрос, есть ли у данного многочлена с целыми коэффициентами целый корень? Оказывается (и это доказал наш российский математик Ю. В. Матиясевич в 1969 г., когда он нашел оригинальное решение, использующее свойства чисел Фиббоначчи, 10-й проблемы Гильберта [6]), что не существует алгоритма (компьютерной программы), который бы по целочисленному вектору коэффициентов многочлена давал однозначный ответ «да» или «нет». Таким образом, все попытки запрограммировать решение данной задачи с помощью компьютеров потерпят крах. Или, например, пусть даны три целых числа a,b,c. Имеет ли квадратное уравнение $ax^2 + bx + c = 0$ целый корень? Нетрудно запрограммировать эту задачу на компьютере. Записывая указанные числа через запятую, можем считать, что на вход компьютера подается число длиной n символов. Ясно, что чем больше длина этого слова, тем дольше будет работать компьютер над решением конкретного уравнения. Но как долго? В теории сложности вычислений говорят, что алгоритм является полиномиальным, если существует константа d, такая, что время работы алгоритма не более чем $n^d$.

10 Для рассматриваемой задачи подобный полиномиальный алгоритм существует. Но стоит чуть изменить задачу, и вопрос о существовании решающего полиномиального алгоритма становится нерешенной научной проблемой. Именно так обстоит дело с задачей, сформулированной следующим образом: «Дана система линейных неравенств с целыми коэффициентами. Есть ли у этой системы целочисленное решение?» Интересно, что ответ положителен для очень похожей задачи: «Дана система линейных неравенств с рациональными коэффициентами. Является ли данная система совместной?» Рассмотрим задачу разложения натурального числа на простые множители. Это типичная задача дискретного программирования. Имеется алгоритм ее решения. Он очень прост: чтобы узнать, является ли число x простым, необходимо последовательно разделить x на каждое натуральное число, не большее $\sqrt{x}$.

11 Если x записать в виде двоичного числа из n символов, то потребуется примерно $2^{n/2}$ делений. Этот алгоритм явно не полиномиальный. Так, для разложения на простые множители числа x, записываемого с 200 двоичными знаками, потребуется около $2^{100}$ делений. Это приблизительно соответствует десятичному числу, содержащему 30 знаков. Для современных суперкомпьютеров данная процедура займет примерно 25 млн. лет непрерывной работы (числа примерно такого же размера используются в криптографии для шифрования важных сообщений - и чтобы разгадать такой шифр, это число нужно разложить на простые множители). А для разложения на простые множители 1000- значного числа современным компьютерам, если они будут работать по указанному алгоритму, не хватит всего времени существования Вселенной около $10^{10}$ лет.

12 До сих пор неизвестно, существует ли полиномиальный алгоритм для разложения натуральных чисел на простые множители. Однако в последние 10-20 лет в этом направлении забрезжила надежда на решение многих задач за приемлемое время, и связана она с так называемыми квантовыми компьютерами. Теория этих компьютеров достаточно сложна. В своей работе они используют принципы квантовой механики и обещают очень многое. Так, доказано, что квантовые компьютеры (если удастся их построить) могут разложить 1000-значное число на простые множители всего за несколько часов. Однако специалисты предупреждают, что, хотя принципиальных трудностей для создания квантовых компьютеров вроде бы и не существует, технических трудностей здесь не меньше, чем в проблеме построения реактора термоядерного синтеза, над которой ведущие физики и конструкторы всего мира бьются уже свыше 50 лет. Оптимизм вселяет то, что спецслужбы мира готовы потратить на соответствующие исследования миллиарды долларов - ведь в случае успеха они получат возможность расшифровать многие перехваченные сообщения, которые десятилетиями лежат нерасшифрованными. Огромное количество используемых в математике алгоритмов полиномиальны и гипотеза существования не полиномиальных алгоритмов называется P NP гипотезой. В наступившем тысячелетии она является одной из важнейших. Во всем мире к понятию сложности алгоритмов по Колмогорову проявляется огромный внимание и очень жаль, что ей не уделено соответствующего внимания в книге. И еще одно важное замечание. В книге совершенно не уделено внимания криптографическим протоколам. А ведь это - средство взаимодействия человека и компьютера. В работе М. Н. Аршинова и Л. Е. Садовского [7] утверждалось, что «... приемов тайнописи - великое множество, и, скорее всего, это та область, где уже нет нужды придумывать что-нибудь существенно новое». Бурное развитие криптографических протоколов, а также новые направления в математике, получили в 1976 году с выходом в свет работы американских математиков У. Диффи и М. Э. Хеллмана «Новые направления в криптографии» [8].

13 Новым и центральным объектом в криптографии стало понятие «односторонней функции». Односторонней называется функция F(x) из X в Y, обладающая двумя свойствами: а) существует полиномиальный алгоритм вычисления значений функции F(x); б) не существует

полиномиального алгоритма инвертирования функции F. Заметим, что пункт б) может быть немного уточнен. Похожим на понятие односторонней функции является понятие функции с секретом. Так называется функция двух переменных F(K,x), некоторое значение параметра K которой и называется секретом. Остальные значения параметра секретом не являются. Хорошим примером функции с секретом является банковская карточка, в которой секретом является пин-код. Начиная с 1976 года тема, криптографических протоколов интенсивно развивается. Перечислим лишь некоторые криптографические протоколы: - протокол аутентификации - звонящий в банк с помощью этого протокола должен убедить банковский компьютер или банковского служащего, что он именно тот, за кого он себя выдает; - протокол электронной подписи - что это такое - уже достаточно хорошо известно; - протокол бросания жребия;- протокол проверки корректности доказательства с нулевым разглашением;- протокол византийских генералов; - и т.д. Предполагается, что криптографические протоколы в ближайшее время станут одним из важнейших предметов в вузах и вызывает только сожаление, что в достаточно хорошей и интересной рецензируемой книге о них ничего не сказано.

# Разум


## Гатауллин Тимур Малютович



**Аннотация**

Статья представляет собой краткую рецензию на книгу Игнаси Белда «Разум, машины и математика. Искусственный интеллект и его задачи» / перевод с испанского. - М.: Де Агостини, 2014. Из названия книги следует, что она посвящена в том числе и «Разуму», но что это такое - осталось неизвестным после знакомства с этой книгой. Эта работа - популярное введение в тему искусственного интеллекта. В России есть немало специалистов (назовем лишь В. Л. Макарова и Д. В. Поспелова), которые могли бы написать подобное введение не хуже, а, пожалуй, лучше. Книга содержит краткий перечень и описание основных задач и методов искусственного интеллекта. Однако в этих описаниях некоторые важные моменты упущены. Они изложены в книгах, выпущенных в советское время, и вряд ли будут переизданы. В данной статье мы кратко остановимся на некоторых из них.



**Ключевые слова:** Разум, машины, искусственный интеллект, сложность алгоритмов по А.Н.Колмогорову, машина Тьюринга, криптографические протоколы

**Дата публикации:** 29.12.2016

**Ссылка для цитирования:**

Гатауллин Т. М. Разум // Искусственные общества. – 2016. – Т. 11. – Выпуск 1-4 [Электронный ресурс]. URL: https://artsoc.jes.su/s207751800000010-0-3/ (дата обращения: 08.05.2021).


---