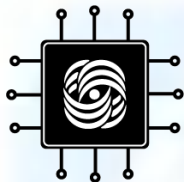


ИСТОРИЯ И МЕТОДОЛОГИЯ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

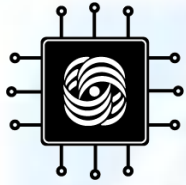
Лекция 09: Философские направления в математики. *Основание компьютерных наук.*

ВМК МГУ им. М.В. Ломоносова, Кафедра АСВК
к.ф.-м.н., доцент Волканов Д.Ю.



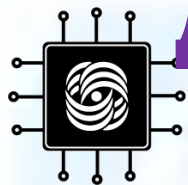
План лекции

- Философские направления в математике. Формализм
- Философские направления в математике. Логицизм
- Философские направления в математике. Интуиционизм
- Основание компьютерных наук
- Предвестники ЭВМ
- Конрад Цузе



Введение в диссертацию

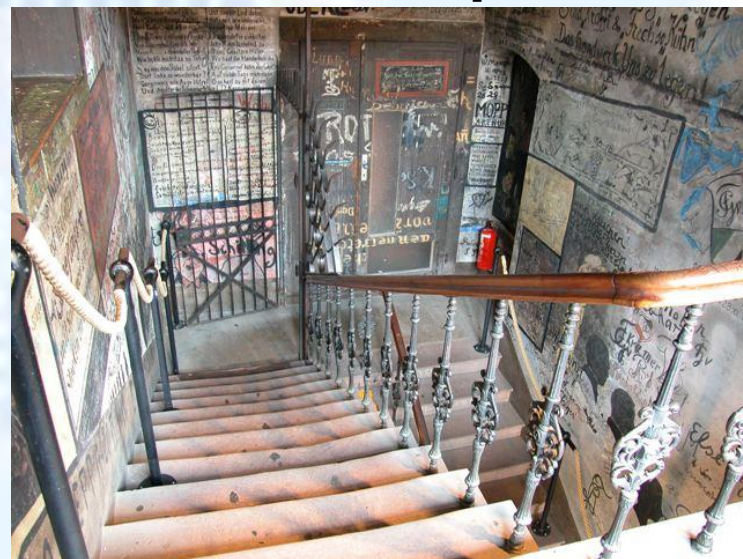
- Введение (включая обзор)
- Постановка задачи
- План решения задачи
- Литература
- Не более 12 страниц
- **ОБЯЗАТЕЛЬНО:**подпись научного руководителя.



Давид Гильберт (1862-1943)



Кёнигсберг

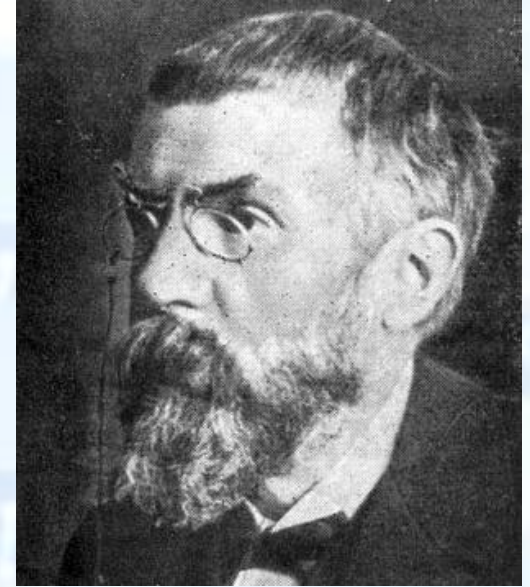
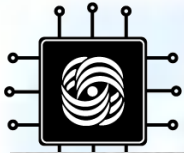


Гейдельберг



Актовый зал Хайдельбергского университета

Д.Гильберт в Париже





Кёнигсберг



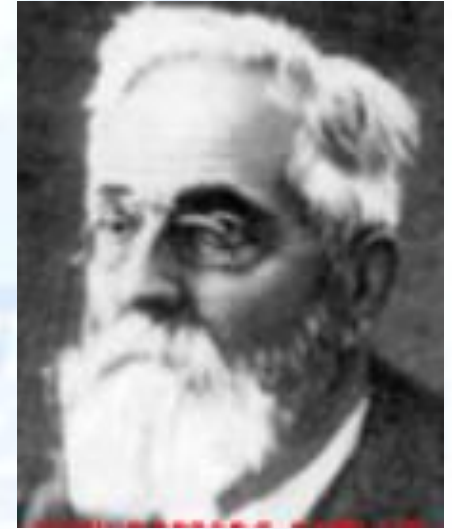
Кёнигсберг



Адольф Гурвиц
1859 - 1919



Фердинанд Линдеман
1852 - 1939



Генрих Вебер
1842 - 1913

- Доктор наук
- Habilitation – представить исследование и прочитать публичную лекцию, чтобы получить право читать лекции (доктор хабилитации)
- Приват-доцент - чтение лекций без оплаты
- Экстраординарный профессор
- Ординарный профессор
- Особняком стоит экзамен на право стать учителем гимназии

Теория инвариантов, проблема Гордана



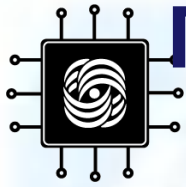
Пауль Гордан
1837 - 1912

Инварианты - алгебраические выражения (многочлены, рациональные функции или их совокупности), изменяющиеся определенным образом при невырожденных линейных заменах переменных

$$f(x_1, \dots, x_n) = \sum_{i_1 + \dots + i_n = r} a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n},$$

$$x_i \rightarrow \sum_{j=1}^n a_{ij} x_j, \quad 1 \leq i \leq n,$$

Известна внутренняя структура всех инвариантных форм. Известен метод, который позволяет, по крайней мере в принципе, выписать все различные инвариантные формы заданной степени от данного числа переменных. Существует ли базис, т.е. конечная система инвариантов, через которые рационально или полиномиально выражается любой другой из бесконечного числа инвариантов?

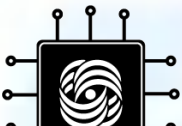


Главные черты великой глубокой математической проблемы



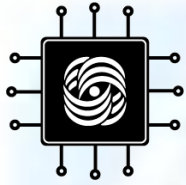
- ❖ *Ясная и легко понимаемая* («так как, в то время как ясное и простое привлекает, сложное отталкивает»).
- ❖ *Трудная* (чтобы нас привлечь») и в то же время не полностью недоступная («чтобы не сделать безнадёжными наши усилия»).
- ❖ *Важная* («путеводная звезда на извилистых тропах к сокрытым истинам»).

Паршин А. Н. Давид Гильберт и теория инвариантов // Историко-математические исследования. — М.: Наука, 1975. — № 20. — С. 171—197



Геттинген





Герман Минковский 1864 - 1909



Гипотеза Минковского

Диаграмма Минковского

Задача Минковского

Кривая Минковского

Неравенство Брунна — Минковского

Неравенство Минковского

Пространство Минковского

Размерность Минковского

Сумма Минковского

Теорема Минковского о выпуклом теле

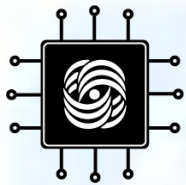
Теорема Минковского о многогранниках

Функционал Минковского

Функция Минковского

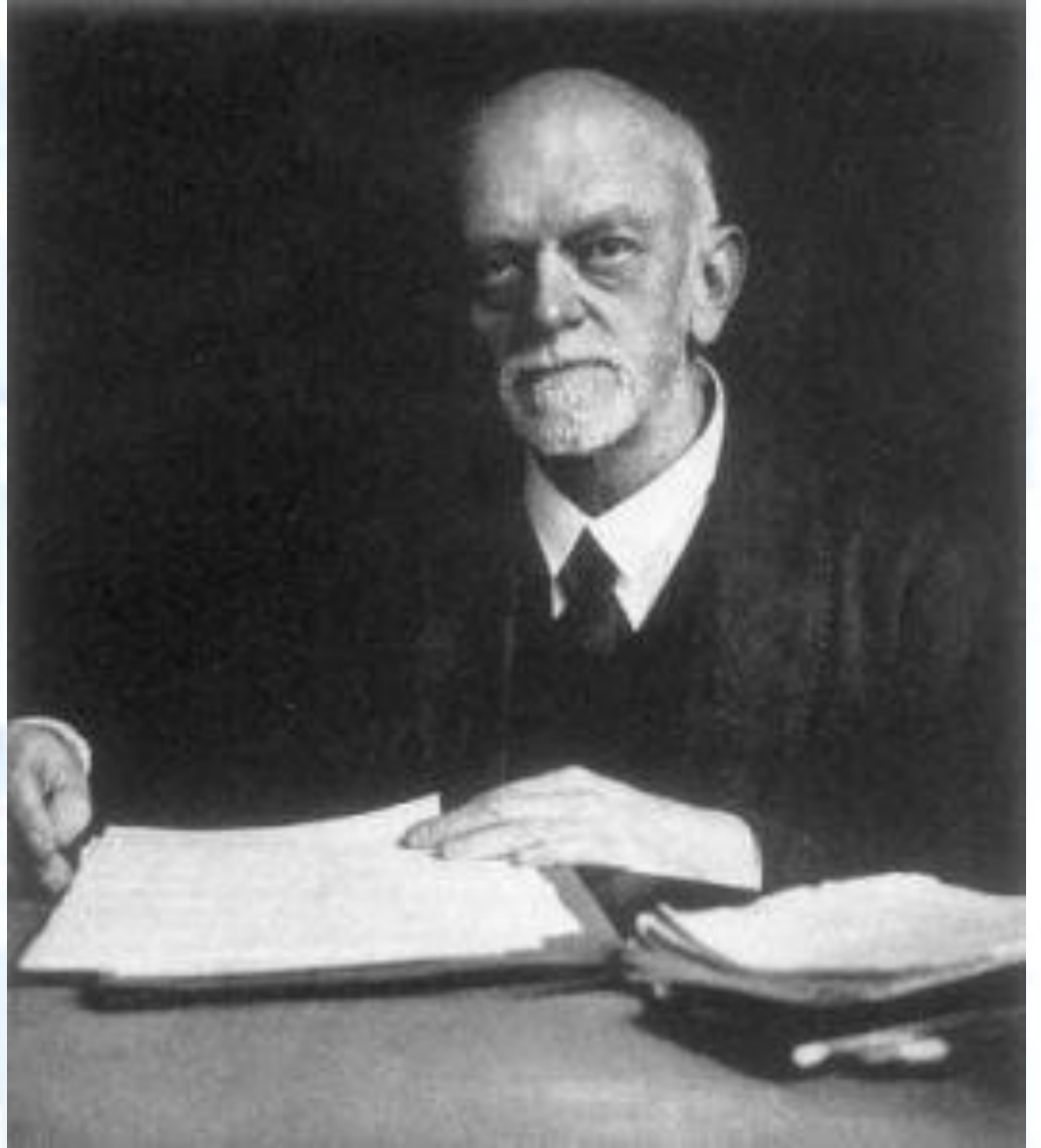
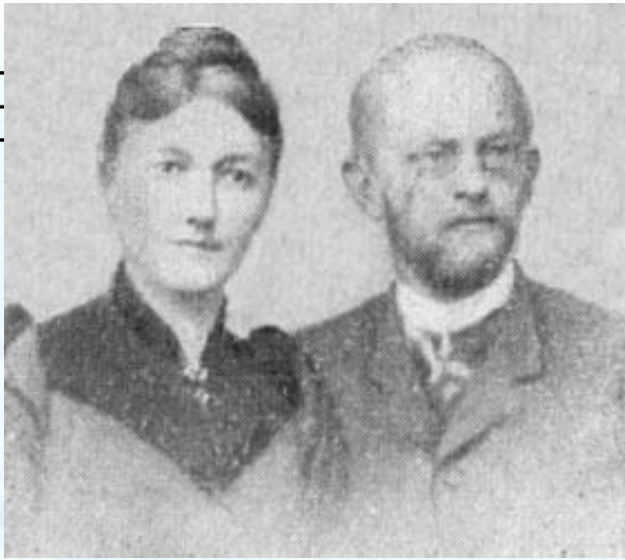


- * теория инвариантов (1885—1893),
- * теория алгебраических чисел (1893—1898),
- * основания геометрии (1898—1902),
- * принцип Дирихле и примыкающие к нему проблемы вариационного исчисления и дифференциальных уравнений (1900—1906),
- * теория интегральных уравнений (1900—1910),
- * решение проблемы Варинга в теории чисел (1908—1909),
- * основы математической физики (1910—1922),
- * логические основы математики (1922—1939).

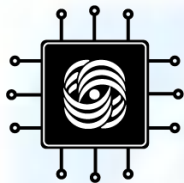


Математический клуб Геттингена





Парижский конгресс



Дворец конгрессов при Всемирной парижской выставке 1900 года.

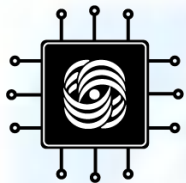
Парижский конгресс, участники и секции



Франция – 90 чел. Германия – 25 чел.
США – 17 чел. Италия – 15 чел
Бельгия – 13 чел. Россия – 9 чел
Австрия, Швейцария – по 8 человек
Англия, Швеция – по 7 человек
Дания, Южная Америка – по 4 человека
Голландия, Испания, Румыния – по 2 человека
Турция, Греция, Норвегия, Канада, Япония, Мексика



- 1) арифметики и алгебры (председатель Д. Гильберт, секретарь Э. Картан)
- 2) анализа (председатель П. Пенлеве, секретарь Ж. Адамар)
- 3) геометрии (председатель Г. Дарбу, секретарь Б. Нивенгловский),
- 4) механики и математической физики (председатель Ж. Лармо, секретарь Т. Леви-Чивита,)
- 5) истории и библиографии математики (председатель принц Роланд Бонапарт, секретарь М. Окань),
- 6) преподавания и методологии математики (председатель М. Кантор, секретарь Ш. Лезан).



основания математики – 1, 2 проблемы;
алгебра – 13, 14, 17 проблемы;
теория чисел – 7-12 проблемы;
геометрия – 3, 4, 18 проблемы;
топология – 16 проблема;
алгебраическая геометрия – 12-16, 22 проблемы;
группы Ли – 5, 14, 18 проблемы;
вещественный и комплексный анализ – 13, 22 проблемы;
дифференциальные уравнения – 16, 19-21 проблемы;
математическая физика и теория вероятностей – 6 проблема;
вариационное исчисление – 23 проблема.

Мы знаем, что каждый век имеет свои проблемы, которые последующая эпоха или решает, или отодвигает в сторону, как бесплодные, чтобы заменить их новыми. (Д.Гильберт)

-Теория бесконечных множеств

-Неевклидова геометрия

-Кватернионы, теория матриц

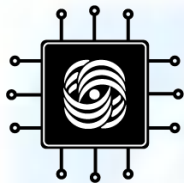
Континуум-гипотеза. С точностью до эквивалентности, существуют только два типа бесконечных числовых множеств: счетное множество и континуум.

Логичизм, направление в основаниях математики и философии математики, основным тезисом которого является утверждение о «сводимости математики к логике», т. е. возможности (и необходимости) определения всех исходных математических понятий (в рамках самой математики не определяемых) в терминах «чистой» логики и доказательства всех математических предложений (в том числе аксиом) опять-таки логическими средствами. (БСЭ)

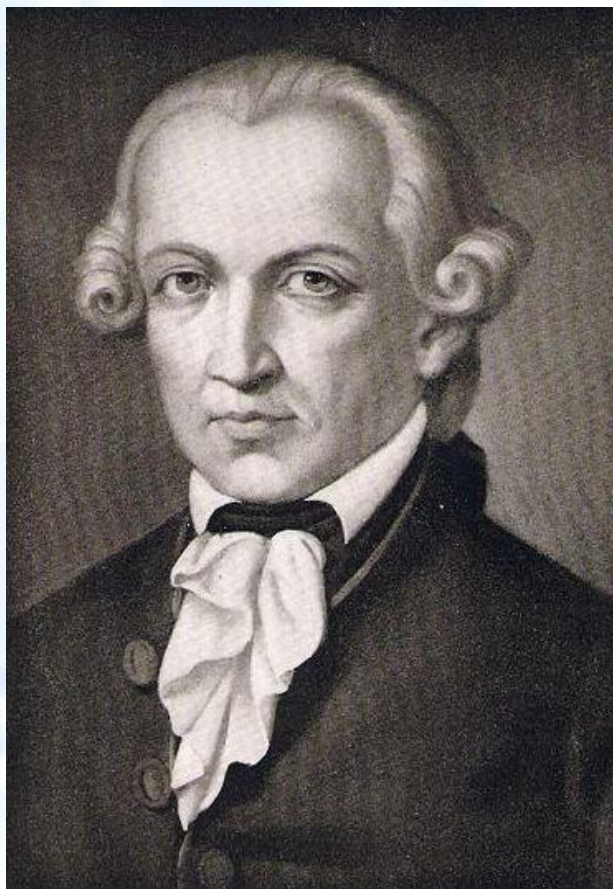
Математический интуиционизм, философско-математическое течение, отвергающее теоретико-множественную трактовку математики и считающее интуицию единственным источником математики и главным критерием строгости её построений. (БСЭ)

Математический формализм, одно из основных направлений в основаниях математики, представители которого считают, что каждый раздел математики может (а на достаточно продвинутой стадии своего построения и должен) быть подвергнут полной формализации, то есть излагаться в виде исчисления (формальной системы), развивающегося по некоторым вполне определённым правилам; при этом гарантией правомерности существования и изучения какого-либо раздела математики должна быть не интерпретация его в терминах некоторой внешней по отношению к нему действительности, а исключительно его непротиворечивость. (БСЭ)

Интуиционизм



*«Под интуицией я
разумею не веру в
шаткое свидетельство
чувств..., но понятие
ясного и внимательного
ума...»(Р.Декарт)*



*Интуиция - естественное и
свободное соответствие
силы воображения законам
разума (И.Кант)*



*«У сердца свои
причины, о
которых не
знает разум»
(Б.Паскаль)*

Интуиционизм



**Леопольд
Кронекер**



Анри Пуанкаре

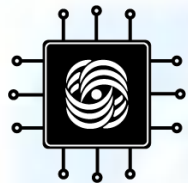


Анри Лебег

Эмиль Борель

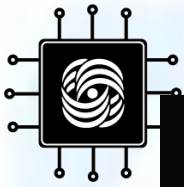


«Кронекер, Борель, Лебег, Пуанкаре высказывали критические замечания по поводу стандартных математических рассуждений и логического подхода, но их собственный вклад в развитие интуиционизма был фрагментарным и случайным» (М.Клайн)

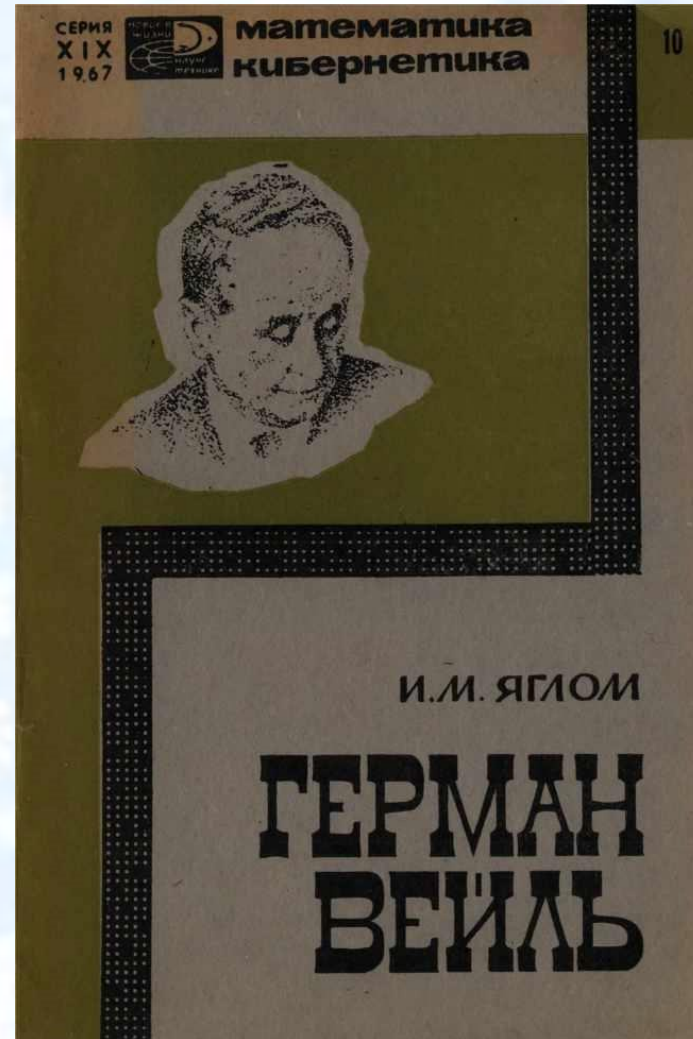


Ян Эгберт Лёйтзен Брауэр 1881-1966





Герман Вейль
1855-1955

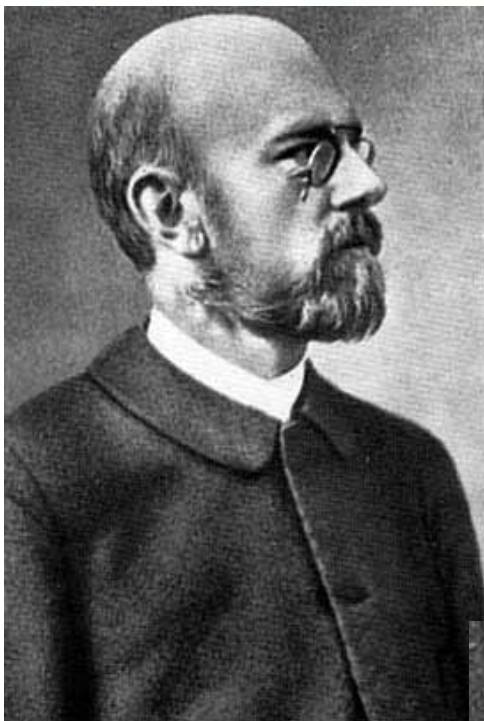


Бирюков Б.В., Бирюкова Л.Г. Г.Вейль (к 85летию знаменитого «Континуума»
// Вестник Московского университета. Серия 7. Философия. №2. 2004. С. 97-110
http://www.philos.msu.ru/vestnik/philos/art/2004/biryuk_veyl.htm

Формализм

Давид
Гильберт

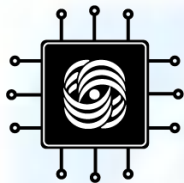
Джон
фон
Нейман
1903-
1957



Вильгельм
Аккерман
1896-1962

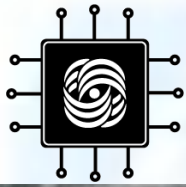


Пауль
Бернайс
1888-1977

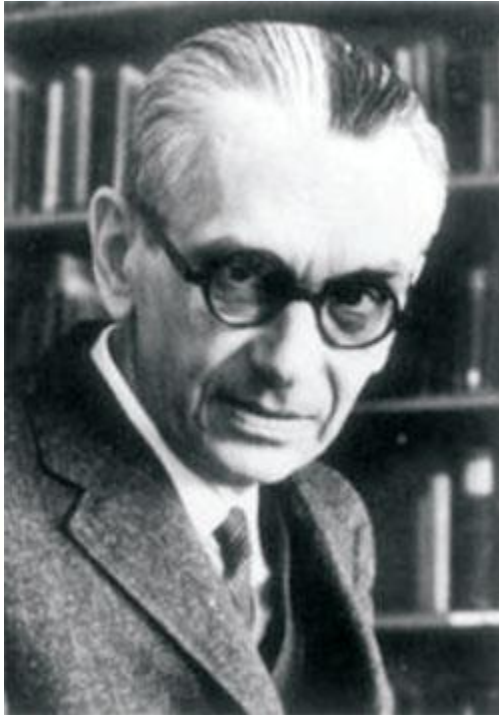


Формализм

- Направление в математике, пытающееся получить решение проблем основания математики при помощи формально-аксиоматических построений.
- Возник в начале XX века (Гильберт)
- Выход из кризиса ищется в строго разработанном формализованном аксиоматическом методе

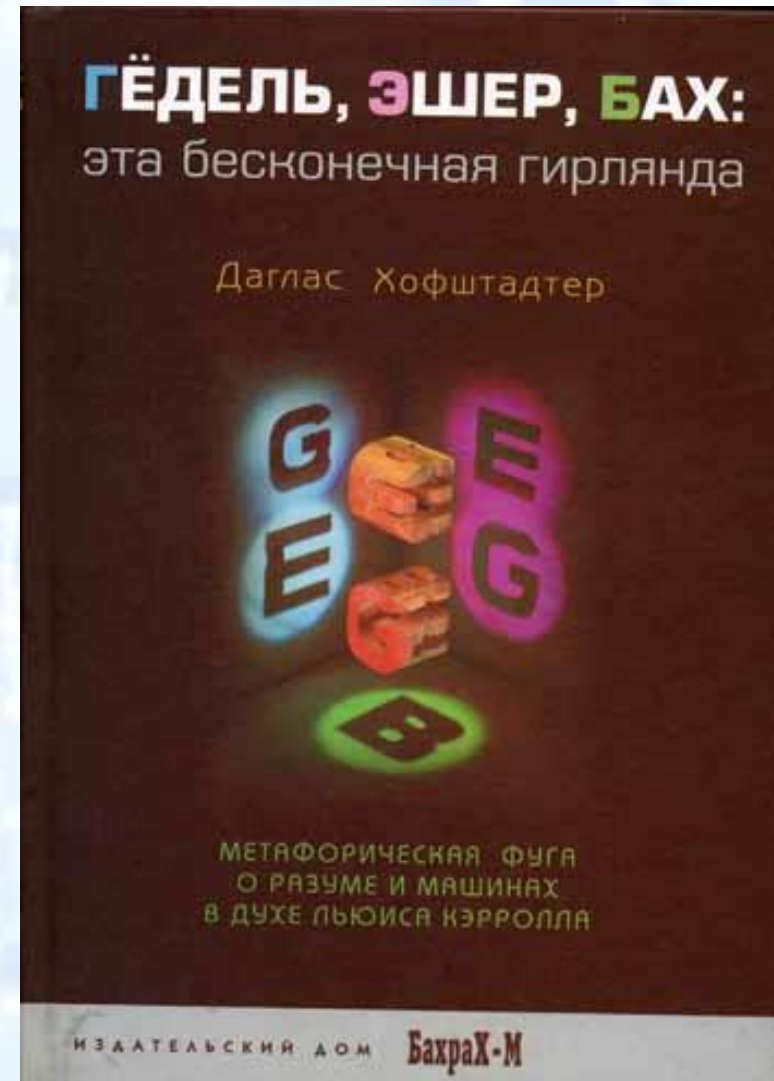


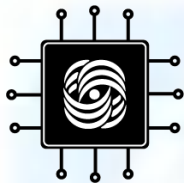
Курт Гёдель (1906-1978)



«Для любой непротиворечивой системы аксиом существует утверждение, которое в рамках принятой аксиоматической системы не может быть ни доказано, ни опровергнуто».

*«Бог существует, поскольку математика, несомненно, непротиворечива; но существует и дьявол, поскольку доказать ее непротиворечивость мы не можем»
(Г.Вейль)*





ЛОГИКОМИКС



ЭПИЧЕСКИЙ ПОИСК ИСТИНЫ

Апостолос ДОКСИАДИС и Христос ПАПАДИМИТРИУ

- Cantor, Georg
- Frege, Gottlob
- Gödel, Kurt
- Hilbert, David
- Moore, G.E.
- Poincaré, Henri
- Russell, Alys
- Russell, Bertrand
- Russell, Dora
- Schlick, Moritz
- Von Neumann, John
- Whitehead, Alfred North
- Wittgenstein, Ludwig

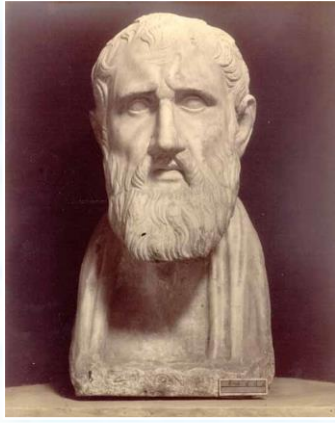
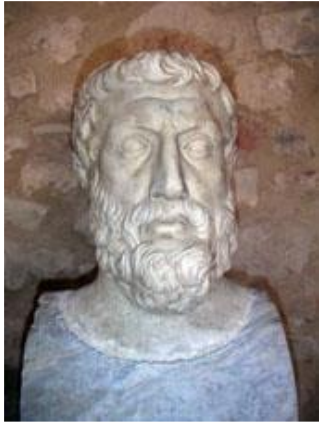




LOGICOMIX: an Epic Search for Truth

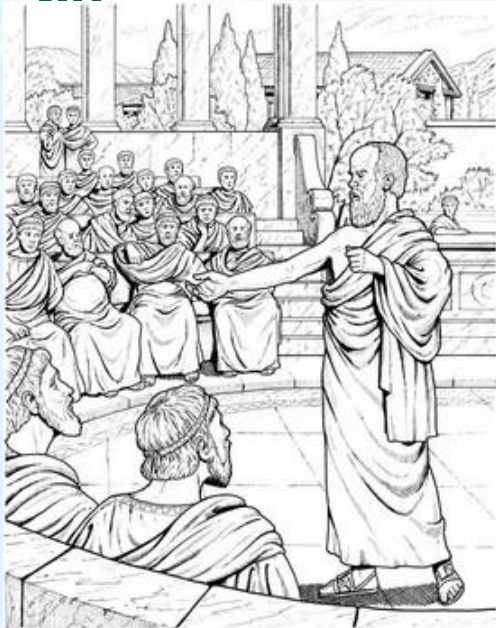
<http://www.labyrinth.ru/books/444924/>

Элеаты



Парменид

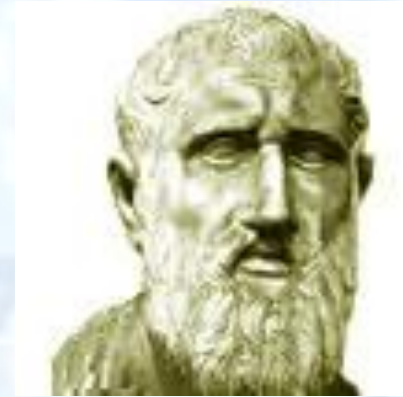
Зенон



Мегарская



ЕВКЛИД из Мегары
(ум. после 369 до н.э.)



Зенон из
Китиона

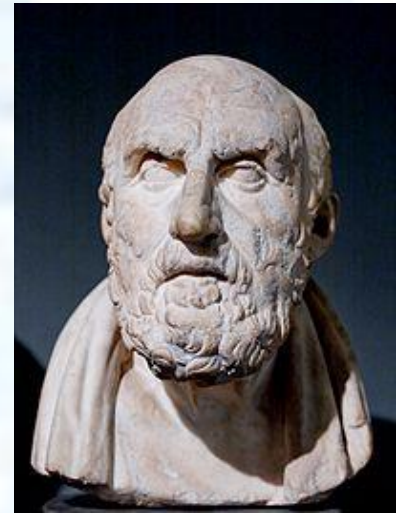
Невозможное не может вытекать из возможного, состоявшееся событие не может быть не тем, чем является; но если в какой-то момент событие могло быть возможным, то из этой возможности могла вытекать и невозможность, таким образом, исходное событие было невозможным.

Диодор Крон (Диалектик)



Стойки

1. Если есть А, то есть и В. А есть. Следовательно, есть и В.
2. Если есть А, то есть и В. Но В не существует. Следовательно, нет и А.
3. А и В не могут существовать одновременно. А есть. Следовательно, В не существует.
4. Существует либо А, либо В. А существует. Следовательно, В не существует.
5. Существует либо А, либо В. В не существует. Следовательно, А существует.



Хрисипп из Сол
(281/278 до н. э. –
208/205 до н. э.)



Марк Аврелий
(121 – 180)

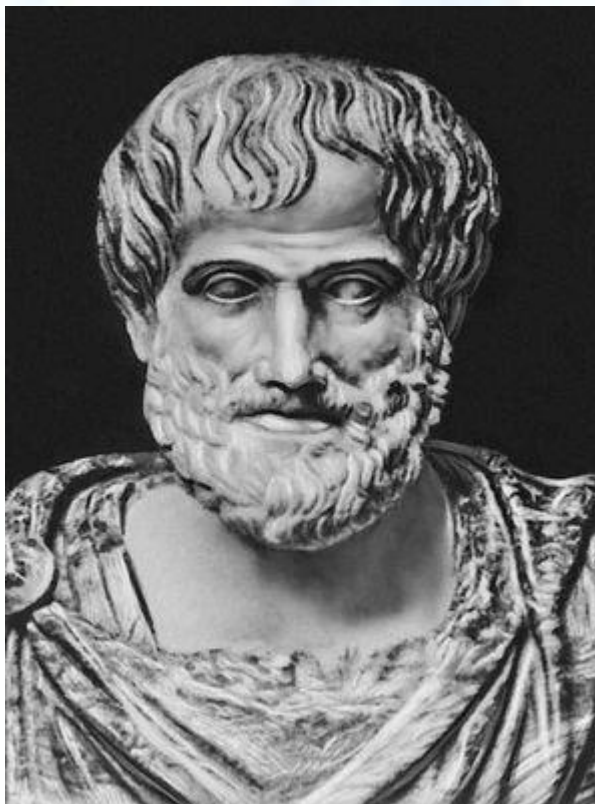


Сенека
(4 до н. э. – 65)



АРИСТОТЕЛЬ

384/283-322 до н.э.



«Вторая аналитика»

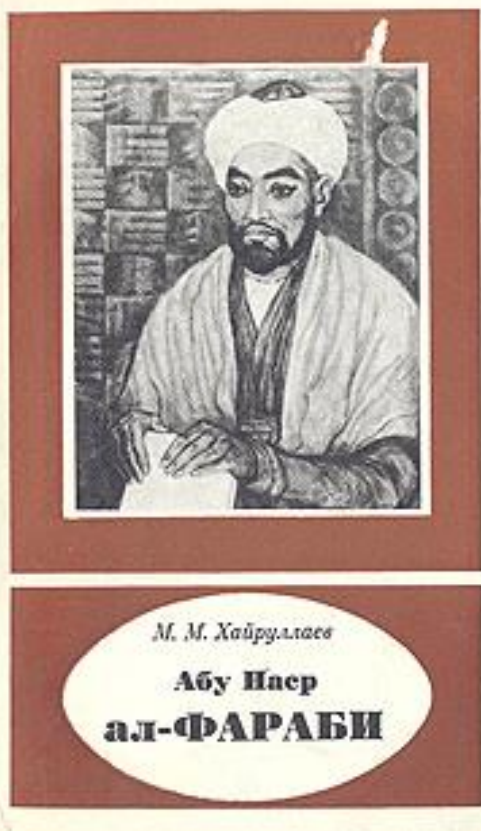


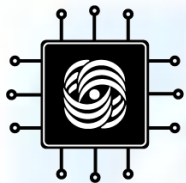
Рембрандт Харменс ван Рейн. Аристотель перед бюстом Гомера. 1653. Музей Метрополитен, Нью Йорк



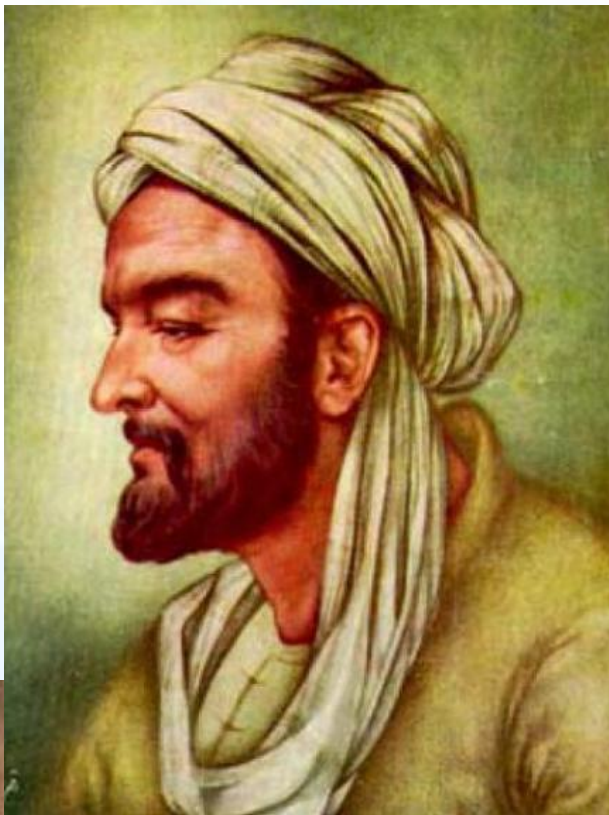
Абу Наср Мухаммед ибн Мухаммед ибн Тархан ибн Узлаг аль-Фараби ат-Тюрки (873 - 150)

- «Слово о субстанции»
- «Существо вопросов»
- «Книга о законах»
- «Книга о постоянстве движения вселенной»
- «О смысле разума»
- «Книга о разуме юных»
- «Большая сокращенная книга по логике»
- «Книга введения в логику»
- «Книга доказательства»
- «Книга об условиях силлогизма»
- «Трактат о сущности души»
- «Слово о сновидениях»
- «Книга об определении и классификации наук»
- «Книга о смысле философии»
- «Книга о том, что нужно знать для изучения философии»
- «Примечания к философии»





**Ибн Рушд Абу-ль-Валид
Мухаммед ибн Ахмед
(1126 – 1198)
(Аверроэс)**



**Насир ад-дин Абу
Джафар Мухаммед
ибн Мухаммед ат
Туси (1201-1274)**



**Абу Али Хусейн ибн
Абдаллах
ибн Сина (980-1037)**





Золотой век схоластики





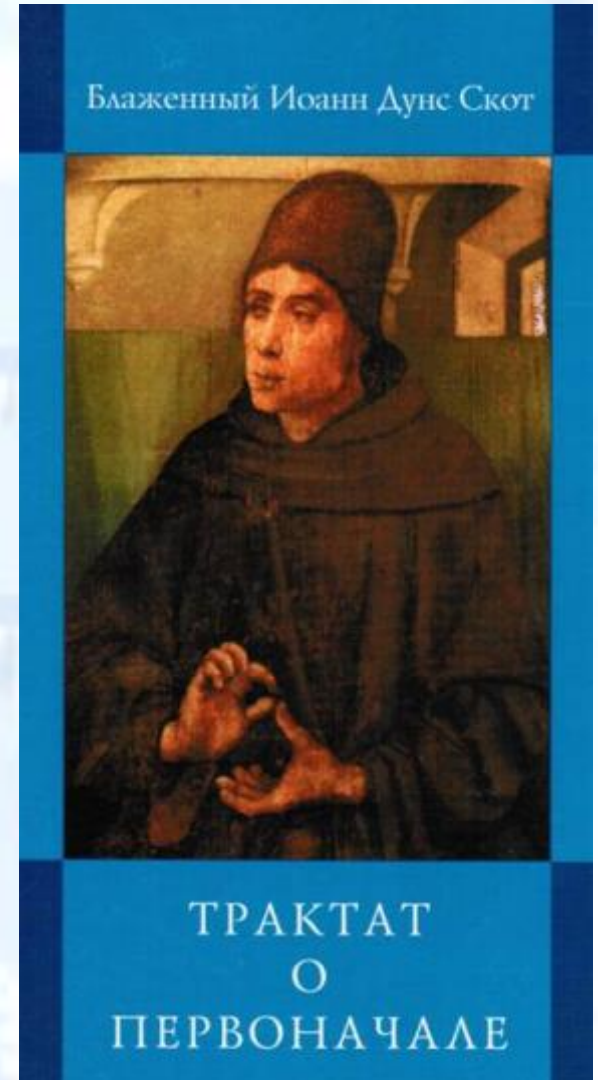
Пьер Абеляр
(1079-1142)



Петр Испанский
(около 1215-1277)



Уильям Оккам (около
1300 – около 1350)

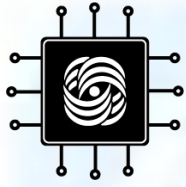


Дунс Скотт
(около 1270 – 1308)



Раймонд Луллий (около 1235 – 1315)





Фрэнсис Бэкон (1561–1626)



Полная индукция означает регулярную повторяемость и исчерпаемость какого-либо свойства предмета в проводимом опыте. Индуктивные обобщения исходят из предположения, что именно так будет обстоять дело во всех сходных случаях.

Неполная индукция включает обобщения, сделанные на основе исследования не всех случаев, а только некоторых (заключение по аналогии), потому что, как правило, число всех случаев практически необозримо, а теоретически доказать их бесконечное число невозможно

Символическая логика

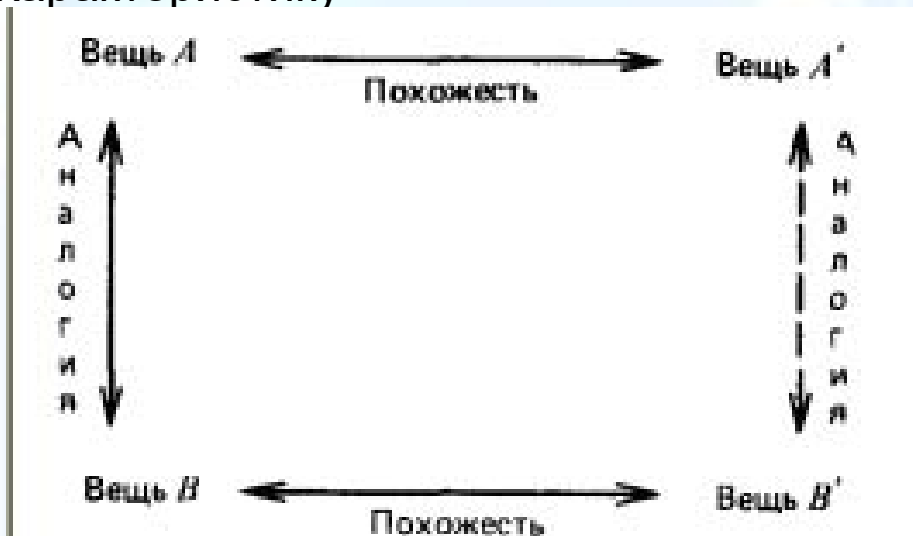
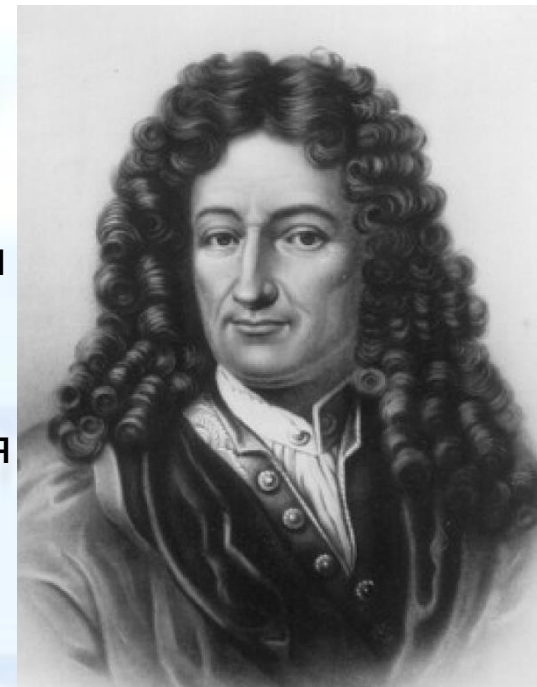
❖ Составить «алгоритм логических мыслей»

(простых неопределяемых понятий)

❖ Получить все остальные определения из этих, путем комбинирования

❖ Составить «доказательную энциклопедию»

❖ Ввести подходящие символические обозначения для исходных и составных понятий и суждений, создать «всеобщую символику» или «универсальную характеристику»



Математика XIX века.

Математическая логика, теория чисел, теория вероятностей. – М.: Наука, 1978 – «Символическая логика Г.В.Лейбница», с.12-18



**Иоганн Андреас фон
Зегнер
(1704-1777),**



**Готфрид Плуке
(Плокке)
(1716 – 1790)**



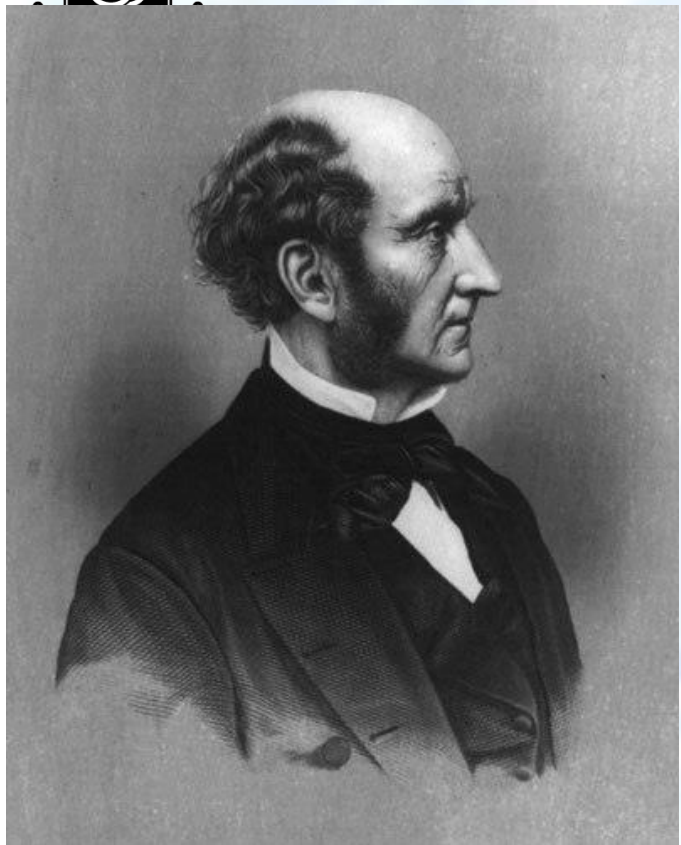
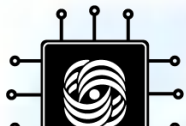
**Иоганн Генрих
Ламберт
(1728–1777)**

два вида СИМВОЛОВ:

- 1) для логических классов (или понятий);
- 2) для логических операций

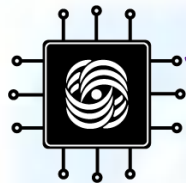
четыре операции:

- 1) комбинирование, или логическое сложение;
- 2) изоляция, или логическое вычитание;
- 3) определение, или логическое умножение;
- 4) абстрагирование, или логическое деление.



Джон Стюарт Милль
(1806 – 1873)

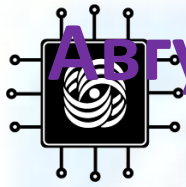
- метод (единственного) сходства (если в двух или более случаях какое-либо явление связано с рядом повторяющихся обстоятельств, то эти обстоятельства суть или причины, или следствия данного явления);
- метод (единственного) различия (если, напротив, некоторое явление W не повторяется в отсутствие определенного обстоятельства A , то явление W зависит от обстоятельства A);
- объединенный метод сходства и различия;
- метод остатков (если W зависит от $A = A_1, A_2, A_3$, то через установление степени зависимости от A_1 и A_2 остается определится меру зависимости от A_3);
- метод сопутствующих изменений (если явление W изменяется, когда изменяется явление U , причем усиление и ослабление W наступает при усилении и ослаблении U , то W зависит от U).



Уильям Гамильтон (1788–1856)

Все x суть все y ,
Все x суть некоторые y ,
Некоторые x суть все y ,
Некоторые x суть некоторые y ,
Ни одно x не есть ни одно y ,
Ни одно x не есть некоторое y ,
Некоторые x не суть некоторые y ,
Некоторые x не суть ни одно y .



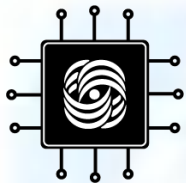


Август (Огёст) де Морган (1806–1871)



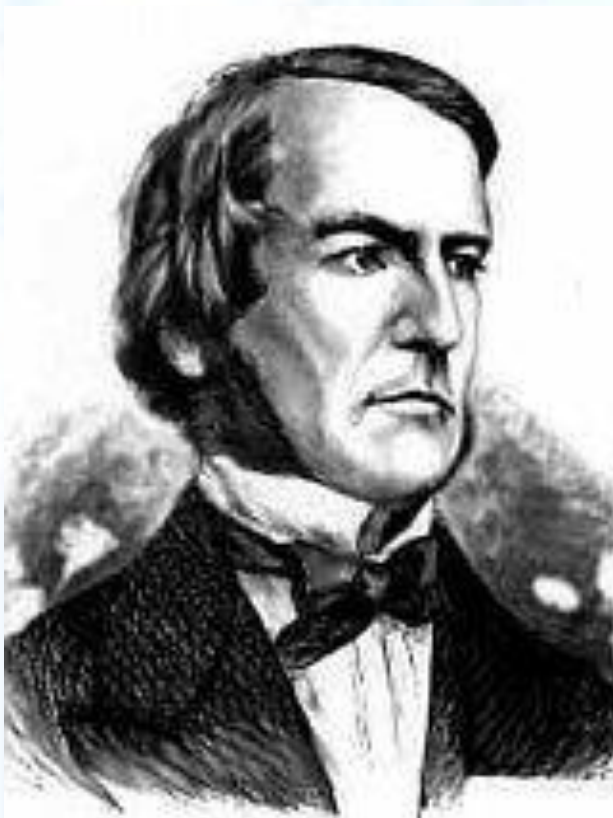
Алгебра отношений Моргана включала в себя шесть основных операций :

- (1) логическая сумма отношений
- (2) логическое произведение тех же отношений,
- (3) операция получения дополнительного для N отношения
- (4) операция получения конверсного отношения или конверсии
- (5) операция порождения относительной суммы отношений
- (6) операция порождения относительного произведения отношений или “композиции”

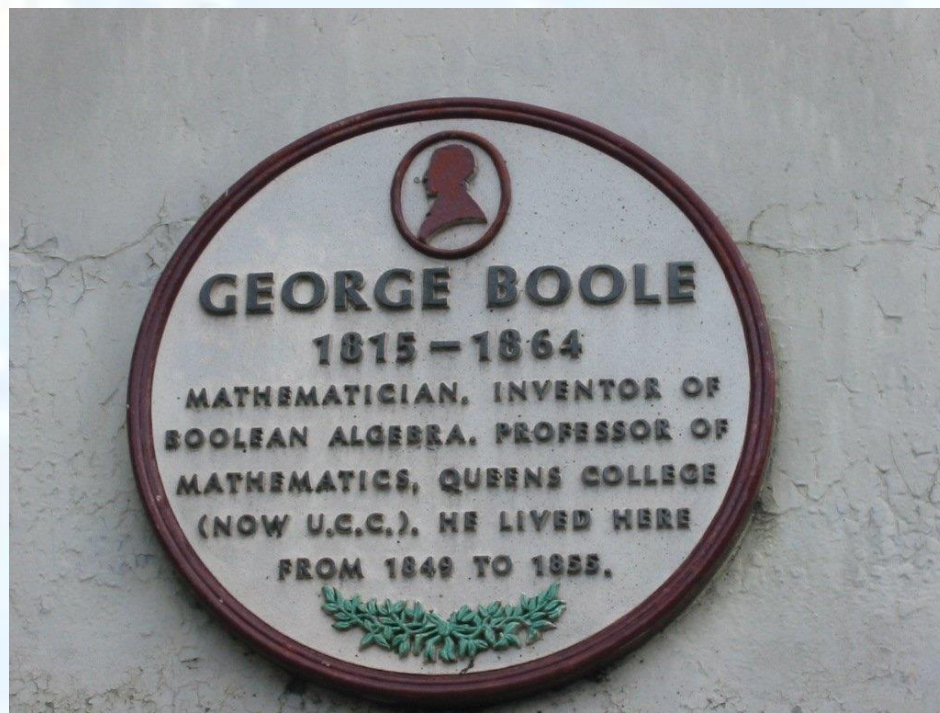


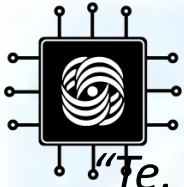
Джордж Буль (1815–1864)

«Математический анализ логики, являющийся опытом исчисления дедуктивного рассуждения» (1847)



«Исследования законов мышления, на которых основаны математические теории логики и вероятности» (1854)





“Те, кто знаком с настоящим состоянием символической алгебры, отдадут себе отчет в том, что обоснованность процессов анализа зависит не от интерпретации используемых символов, а только от законов их комбинирования. Каждая интерпретация, сохраняющая предложенные отношения, равно допустима, и подобный процесс анализа может, таким образом, при одной интерпретации представлять решение вопроса, связанного со свойствами чисел, при другой — решение геометрической задачи и при третьей — решение проблемы динамики или статики. Необходимо подчеркнуть фундаментальность этого принципа”.

$x^2 = x$ для любого x

AND, OR, NOT



Чарльз и
Мэри
Хинтон с
детьми



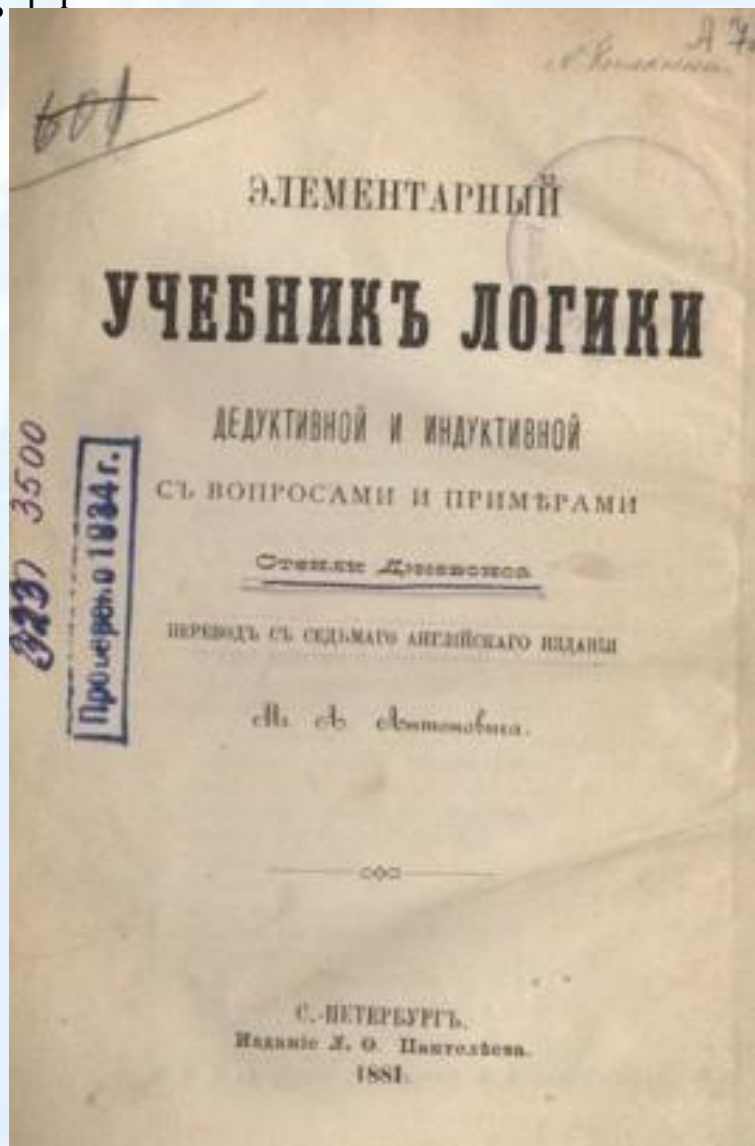
Мэри Эверест Буль
“Философия и развлечения
алгебры”

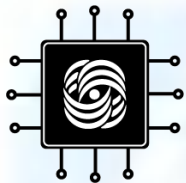


Этель
Лилиан
Войнич



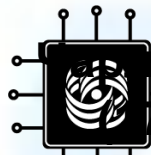
Уильям Стенли Джевонс (1835–1882)





Логические счеты – наклонная доска с четырьмя горизонтальными выступами и набором деревянных пластинок с вырезанными на них конституентами. На одном выступе – все конституенты нужного числа переменных, на другом – содержащиеся в посылках. Противоречащие посылкам конституенты снимаются с верхней линии и на ней остается так называемая логическая единица задачи. После этого можно решать вопросы, касающиеся отдельных классов





Вз Стэнхоуп
(1753– 1816)



Альфред Сми
(1818-1877)
Alfred Smee



Александр Николаевич Жукарев (1864-1936)
- создатель "машины логического мышления",
способной механически осуществлять простые
логические выводы на основе исходных
СМЫСЛОВЫХ ПОСЫЛОК.

DEMONSTRATOR,
INVENTED BY
CHARLES EARL STANHOPE.

The right-hand edge of the gray points out, on this upper scale, the extent of the gray, in the logic of certainty.



The lower edge of the gray points out, on this side scale, the extent of the gray, in the logic of probability.

The area of the square opening, within the black frame, represents the logic, in all cases.

The right-hand side of the square opening points out, on this lower scale, the extent of the red, in all cases.

The right-hand edge of the gray points out, on the same lower scale, the extent of the consequence, (or dark red,) if any, in the logic of certainty.


Rule for the Logic of Certainty.

to the gray, add the red, and deduct the hollow; the remainder, (or dark red,) if any, will be the extent of the consequence.

Rule for the Logic of Probability.

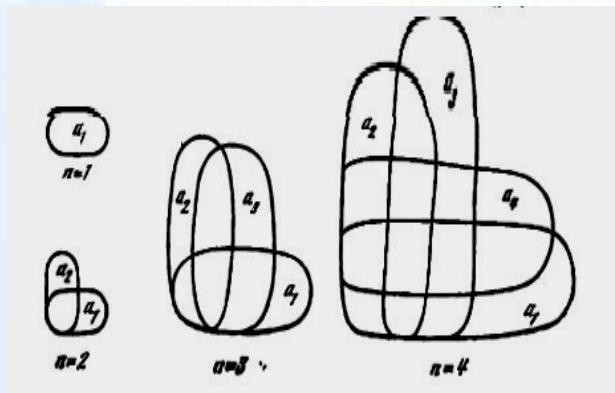
in proportion, between the area of the dark red and the area of the hollow, is the probability which results from the gray and the red.

PRINTED BY EARL STANHOPE, CHEVENING, KENT.

 **Джон Венн**
(1834–1823)



**Эрнест
Шрёдер**
(1841-1902)



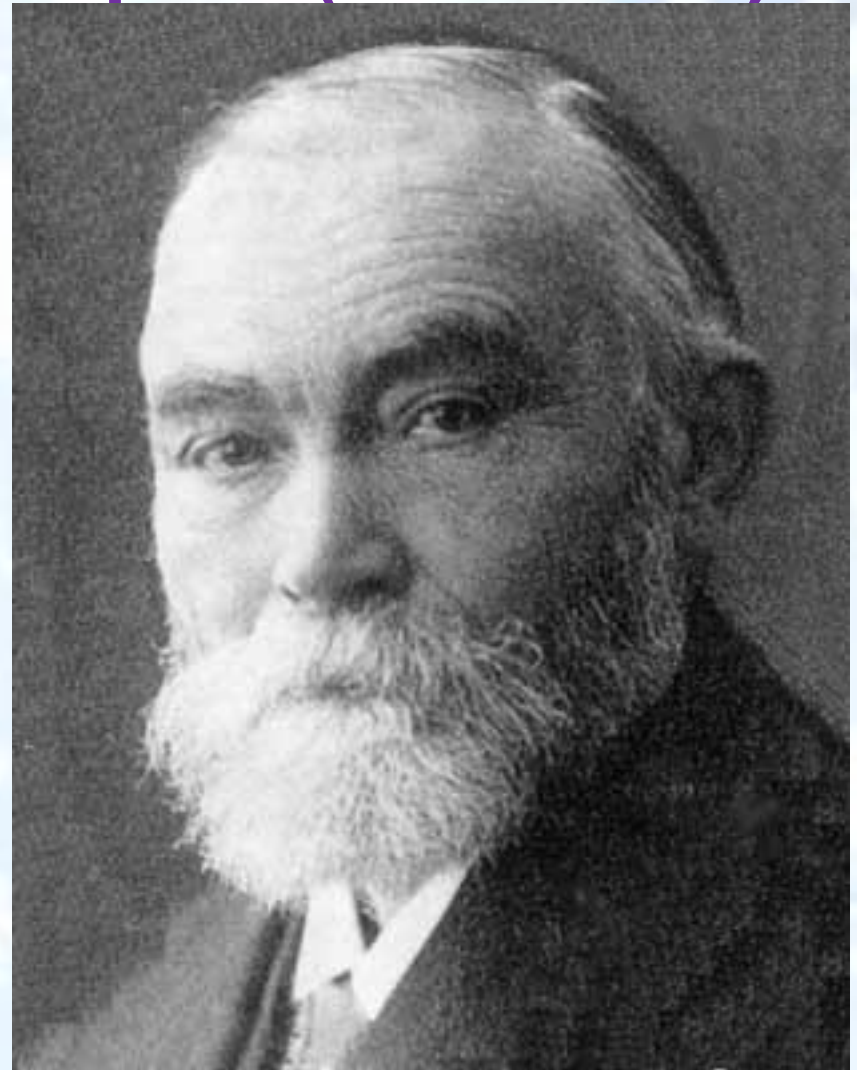
**Платон
Сергеевич
Порецкий**
(1846-1907)

Фридрих Людвиг Готлоб Фреге (1848-1925)



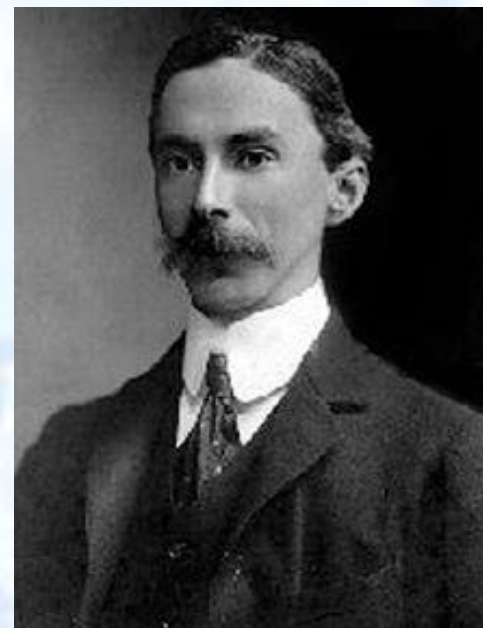
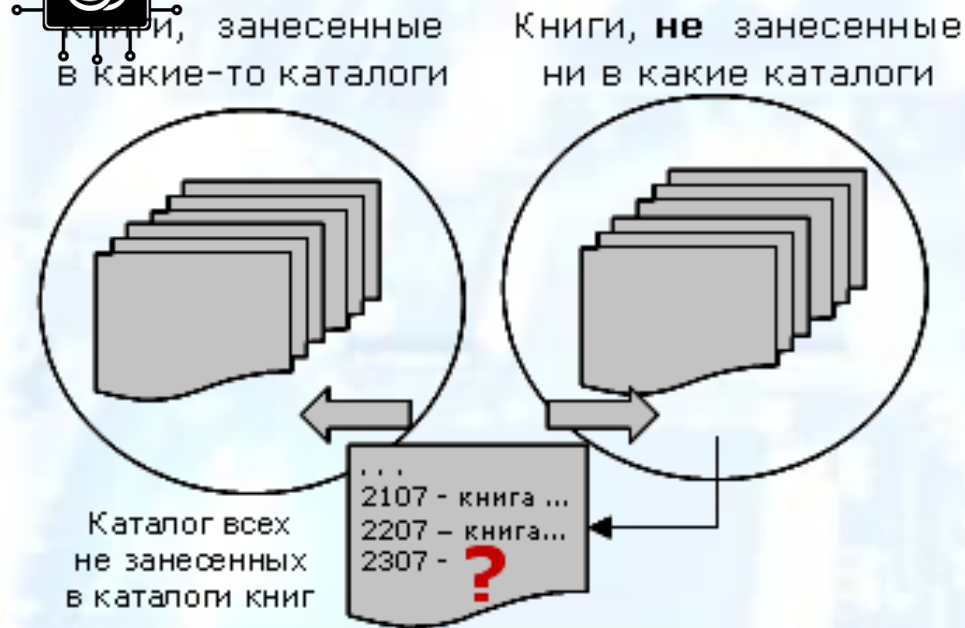
«Запись в понятиях» (1879)

«О смысле и значении», 1892



Двухтомник «Основные законы арифметики» (1893, 1903)

Бертран Рассел (1872-1970)



Одному деревенскому (армейскому) брадобрю приказали "брить всякого, кто сам не бреется, и не брить того, кто сам бреется", как он должен поступить с собой?

«Проблемы философии» (1912)

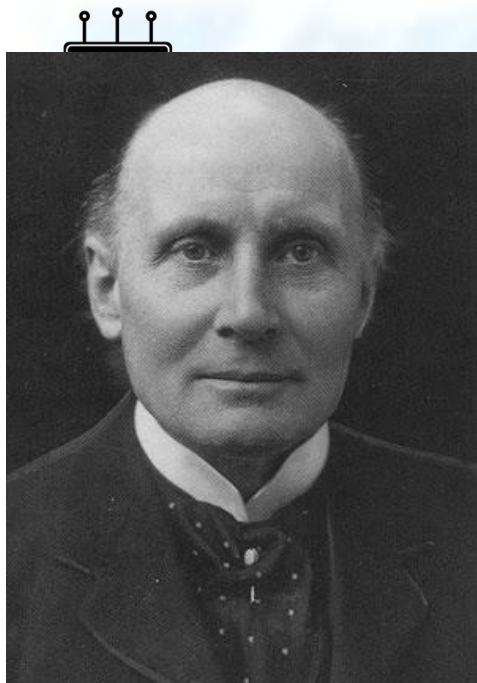
«Принципы математики» (1903)

Страница Бертрانا Рассела:

<http://vivovoco.rsl.ru/VV/PAPERS/ECCE/RSL/RUSSELL.HTM>

Логицизм

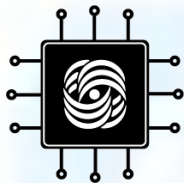
Логицизм, направление в основаниях математики и философии математики, основным тезисом которого является утверждение о «сводимости математики к логике», т. е. возможности (и необходимости) определения всех исходных математических понятий (в рамках самой математики не определяемых) в терминах «чистой» логики и доказательства всех математических предложений (в том числе аксиом) опять-таки логическими средствами. (БСЭ)



**Альфред Норт
Уайтхед (1861-1947)**

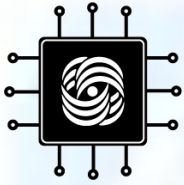
***«Цель научного мышления - видеть общее
в частном и вечное в преходящем»***





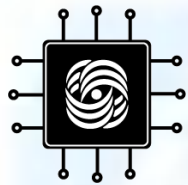
Логицизм (1)

- Взгляд на математику как на часть логики обусловлен тем, что любую математическую теорему в аксиоматической системе можно рассматривать как некоторое утверждение о логическом следовании.
- Попытка сведения натуральных чисел к логическим понятиям была предпринята Г. Фреге. В интерпретации Г. Фреге натуральные числа были кардинальными числами некоторых понятий

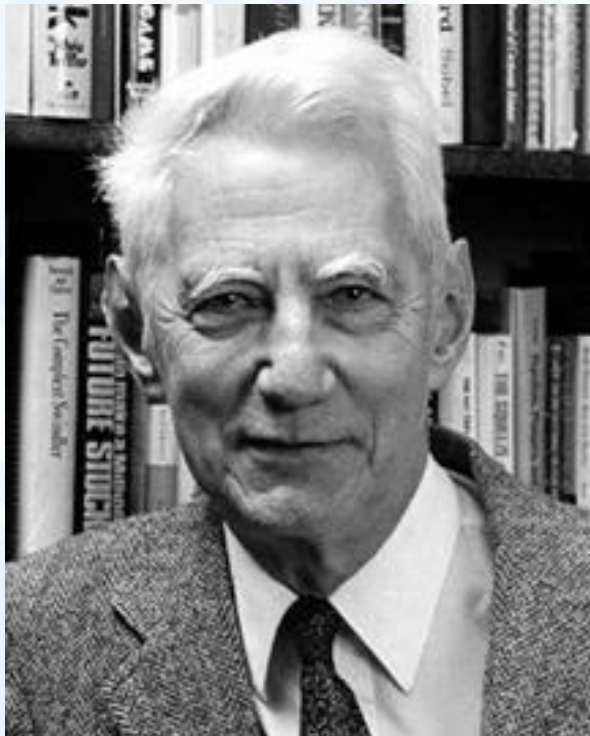


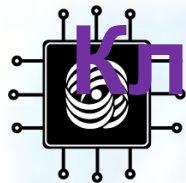
Логицизм (2)

- Однако система Фреге не свободна от противоречий. Это выяснилось, когда Рассел обнаружил противоречие в канторовой теории множеств (парадокс Рассела)
- В целом попытка сведения математики к логике не удалась. Как показал Гёдель, никакая формализованная система логики не может быть адекватной базой математики.



Клод Элвуд Шеннон (1916 - 2001)



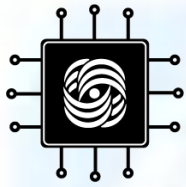


Клод Элвуд Шеннон (1916 - 2001)

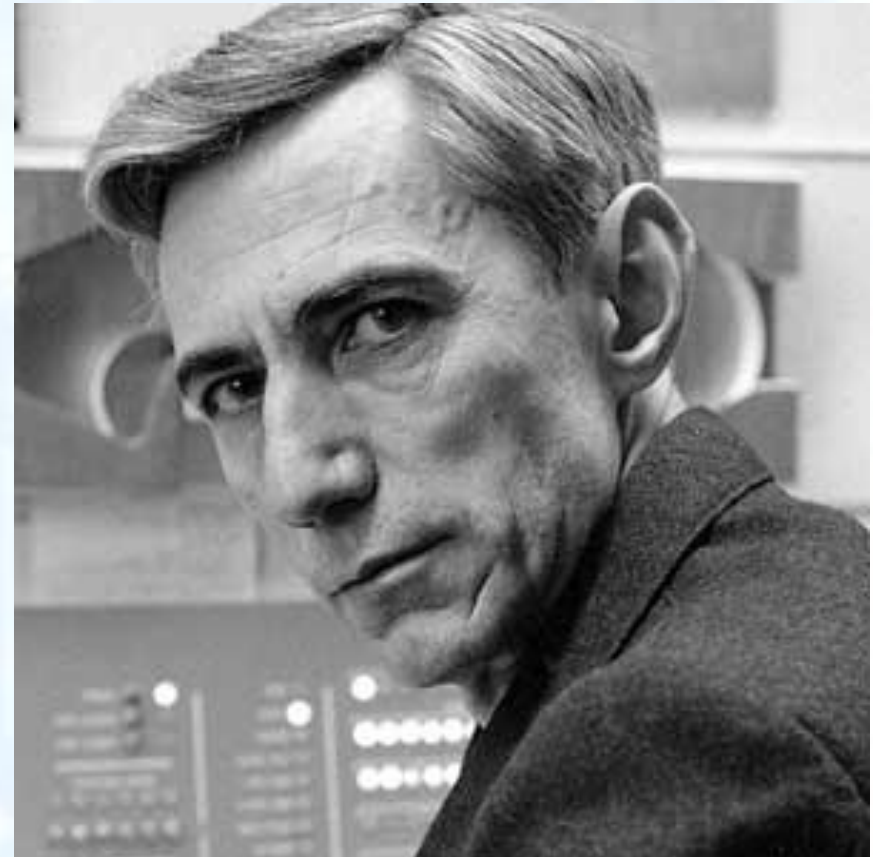
Что такое информация? Оставляя в стороне вопрос о содержании этого понятия, Шеннон показал, что это измеримая величина: количество информации, содержащейся в данном сообщении, есть функция вероятности, что из всех возможных сообщений будет выбрано данное. Он назвал общий потенциал информации в системе сообщений как ее “энтропию”. В термодинамике это понятие означает степень случайности (или, если угодно, “перемешанности”) системы. (Однажды Шеннон сказал, что понятием энтропии ему посоветовал воспользоваться математик Джон фон Нейман, указавший, что, т. к. никто не знает, что это такое, у Шеннона всегда будет преимущество в спорах, касающихся его теории.)

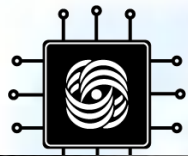
Шеннон определил основную единицу количества информации, названную потом битом, как сообщение, представляющее один из двух вариантов: например, “орел” — “решка”, или “да” — “нет”. Бит можно представить как или 0, или как присутствие или отсутствие тока в цепи.

На этом математическом фундаменте Шеннон затем показал, что любой канал связи имеет свою максимальную пропускную способность для надежной передачи информации. В действительности он доказал, что, хотя можно приблизиться к этому максимуму за счет искусного кодирования, достичь его невозможно.

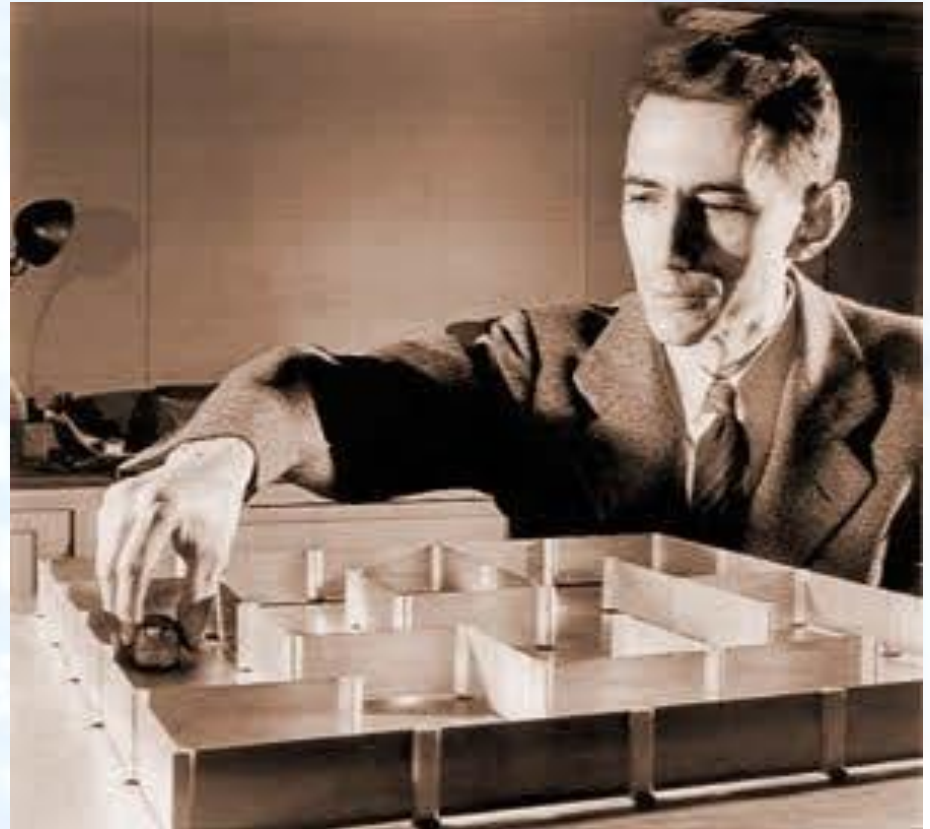


Клод Элвуд Шеннон (1916 - 2001)





Клод Элвуд Шеннон (1916 - 2001)

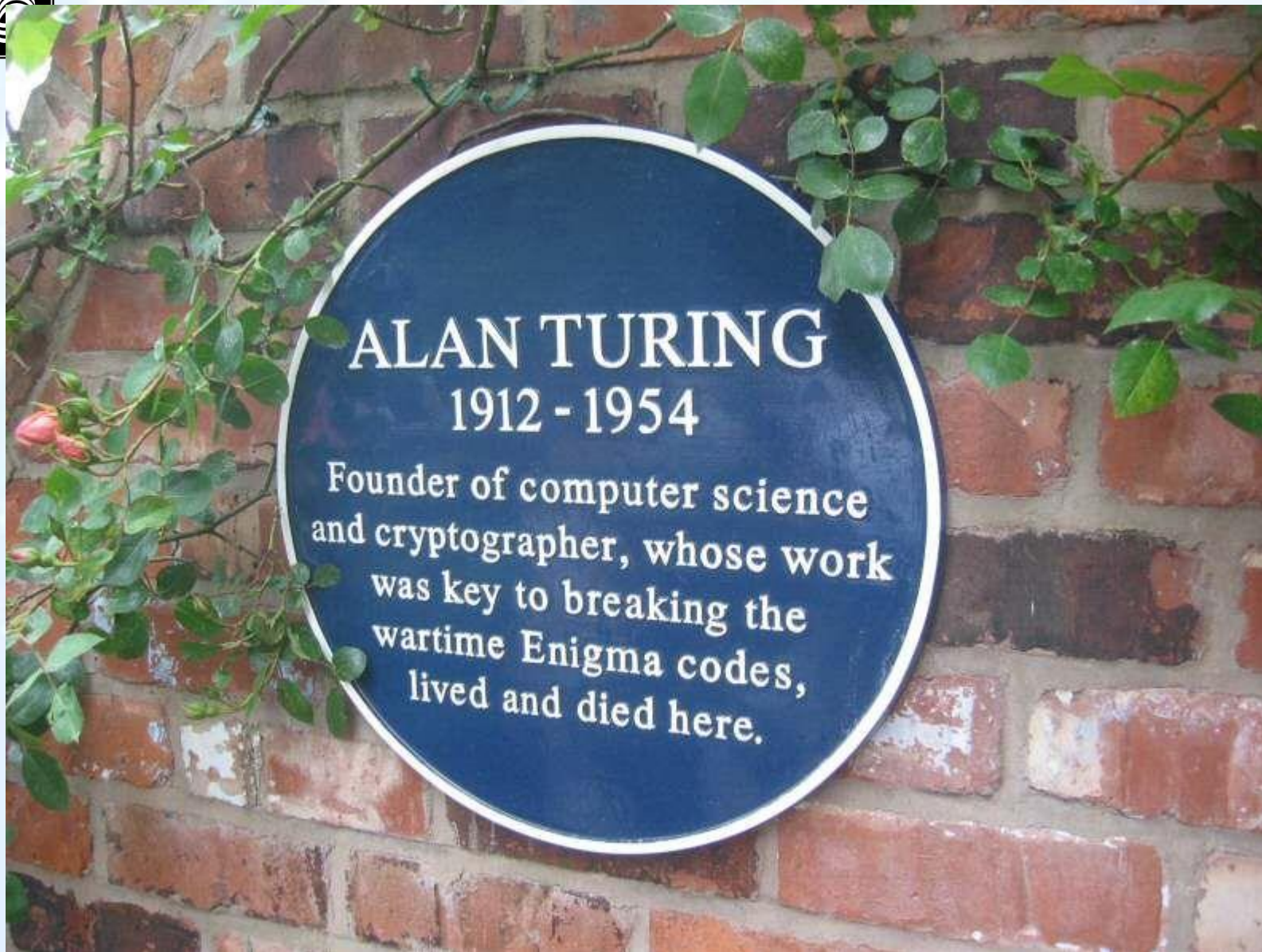


Мышь Шеннона живёт в металлическом лабиринте со множеством запутанных ходов и тупиков. Лабиринт сделан так, что при неправильном ходе электрический ток как бы "отпугивает" мышь, и она возвращается в поисках правильного хода, пока, наконец, не достигнет противоположного конца лабиринта. Если Вы после первого прохода мышью лабиринта, вновь вернете её в исходное положение, она уверенно пойдёт по единственно правильному пути. До некоторой степени мышь Шеннона аналогична телефонным искателям АТС, которые сразу же после набора номера осуществляют нужное соединение.



Клод Элвуд Шеннон (1916 - 2001)

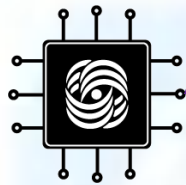




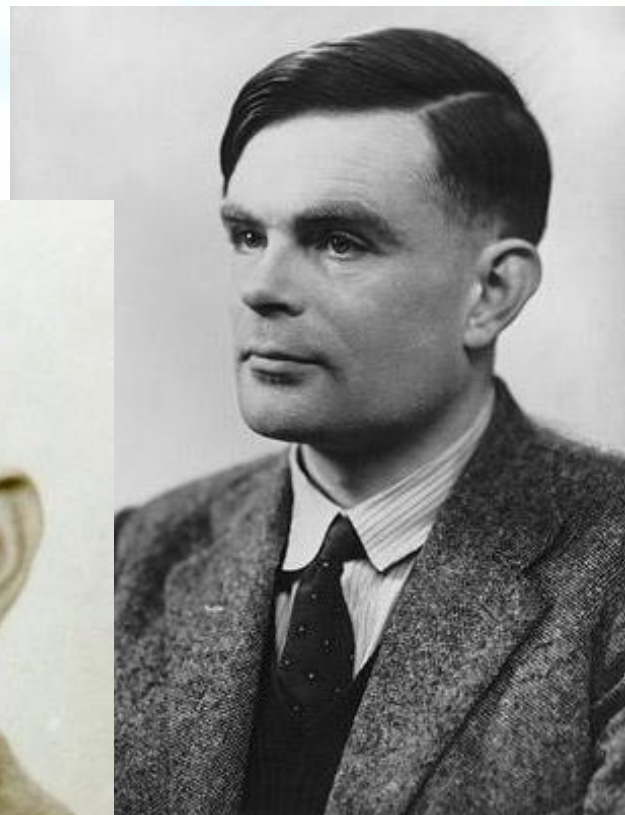
ALAN TURING

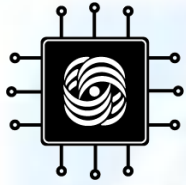
1912 - 1954

Founder of computer science
and cryptographer, whose work
was key to breaking the
wartime Enigma codes,
lived and died here.



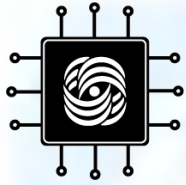
Алан Тьюринг





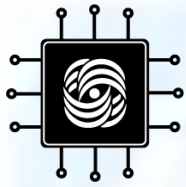
Основные результаты

- Тезис Чёрча-Тьюринга
- Машина Тьюринга
- Криптография
- Тест Тьюринга
- Колоссус

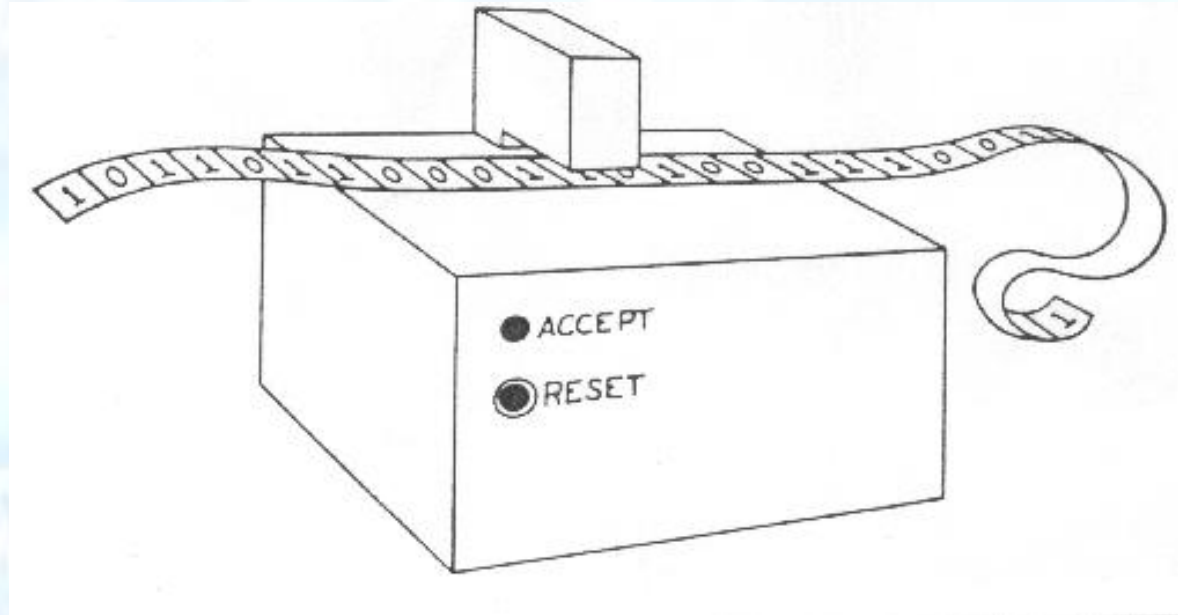


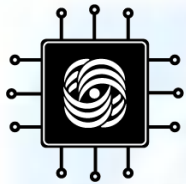
Тезис Чёрча-Тьюринга

- Любая функция, которая может быть вычислена физическим устройством, может быть вычислена машиной Тьюринга



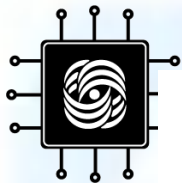
Машина Тьюринга (1)





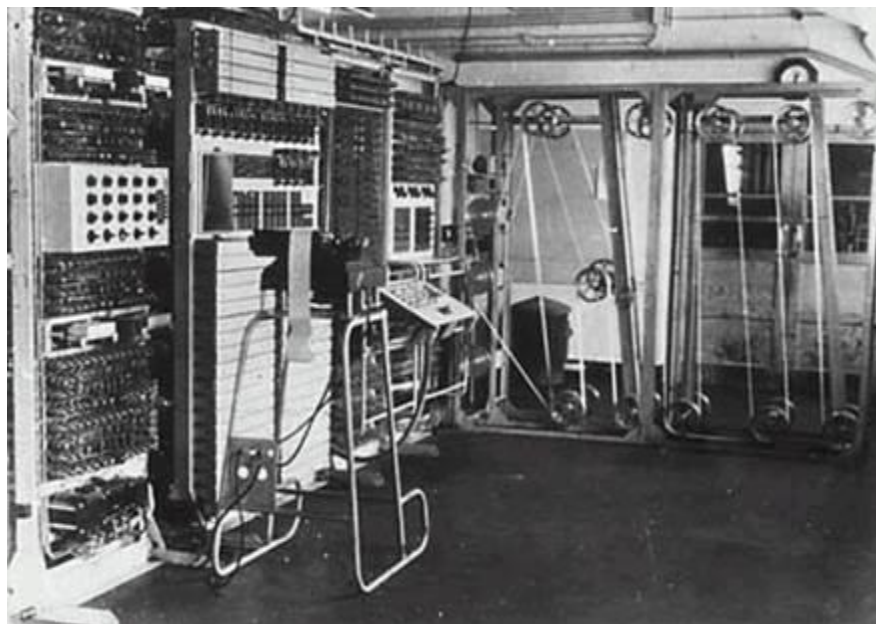
Криптография

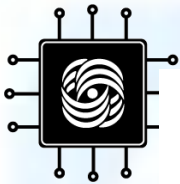
- Тьюринг помогал взломать код Энигмы
- Построен первый программируемый компьютер Колоссус
- Базировался:
 - на его концепции универсальной машины 1936
 - потенциальной скорости и надёжности электронных технологий
 - неэффективность разностных машин для различных логических процессов
- Шифр-код был расшифрован в 1943
- Все компьютеры были разрушены по приказу Черчилля



Collosus

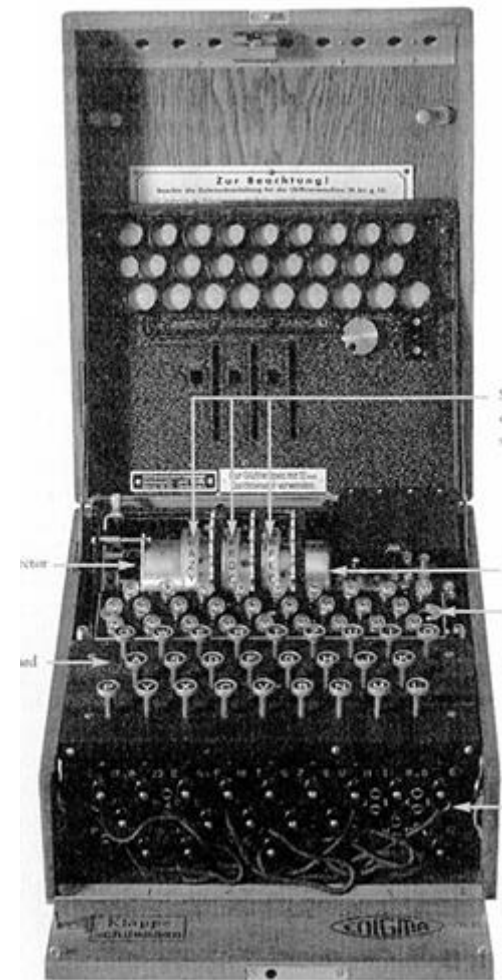
Под руководством выдающегося математика Алана Тьюринга была построена специализированная электронная вычислительная машина **Colossus**. Она насчитывала 2000 радиоламп и обрабатывала 25000 симв./с

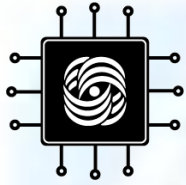




Enigma

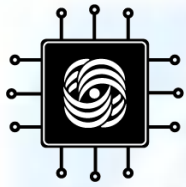
В местечке Блечли-Парк (Bletchley Park) под Лондоном была организована сверхсекретная криптоаналитическая лаборатория для расшифровки немецких военных шифров, используемых в шифровальной машине **Enigma**.





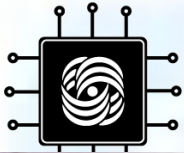
Тест Тьюринга

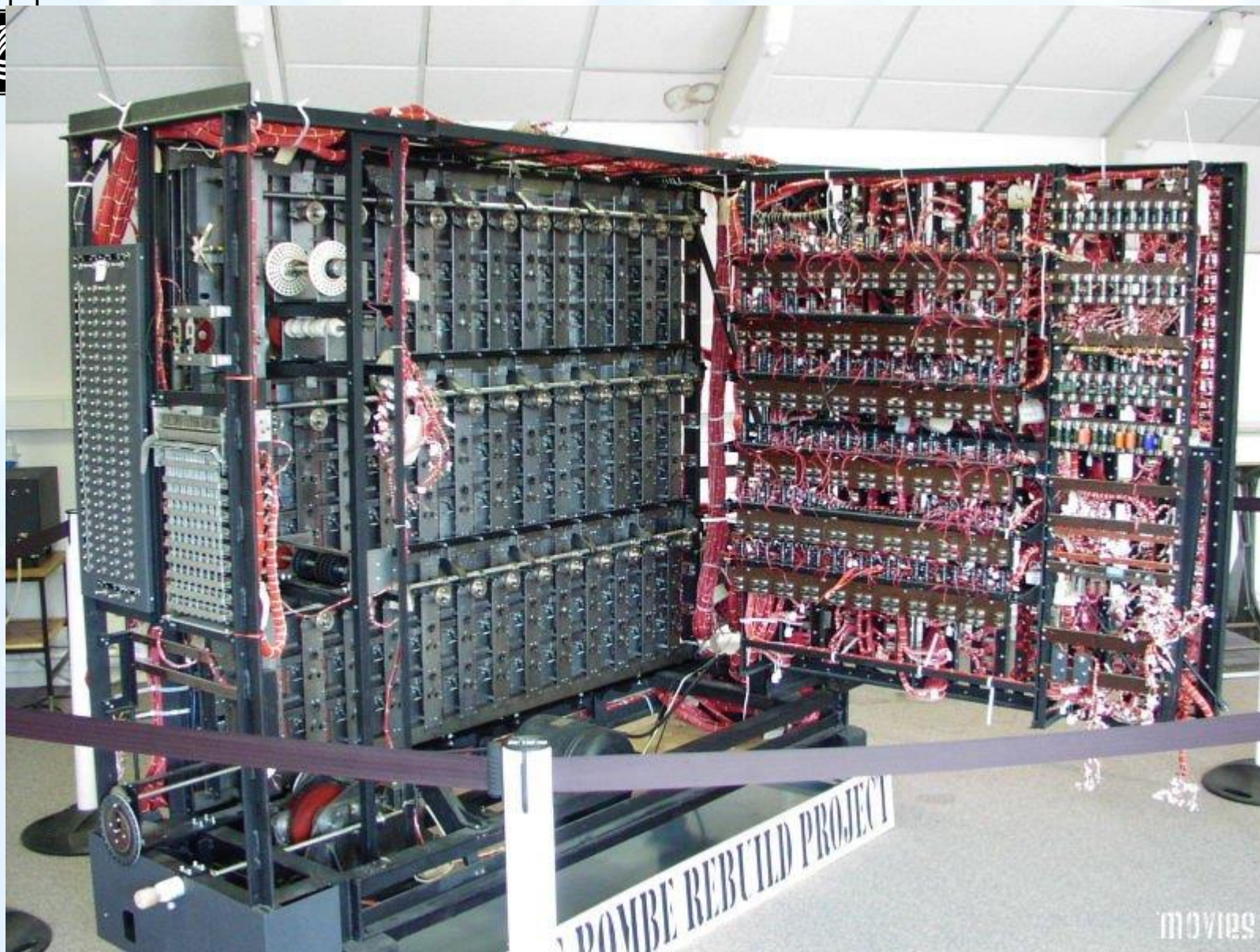
- Опубликован в 1950 году
- Человек обменивается сообщениями на естественном языке с двумя собеседниками (человек и компьютер)
- Если человек не может определить кто есть кто, то считается что компьютер прошёл тест
- Переписка должна производиться через контролируемые промежутки времени
- Тьюринг оценил что программы в 2000 году пройдут тест
- Пока не подошли даже близко



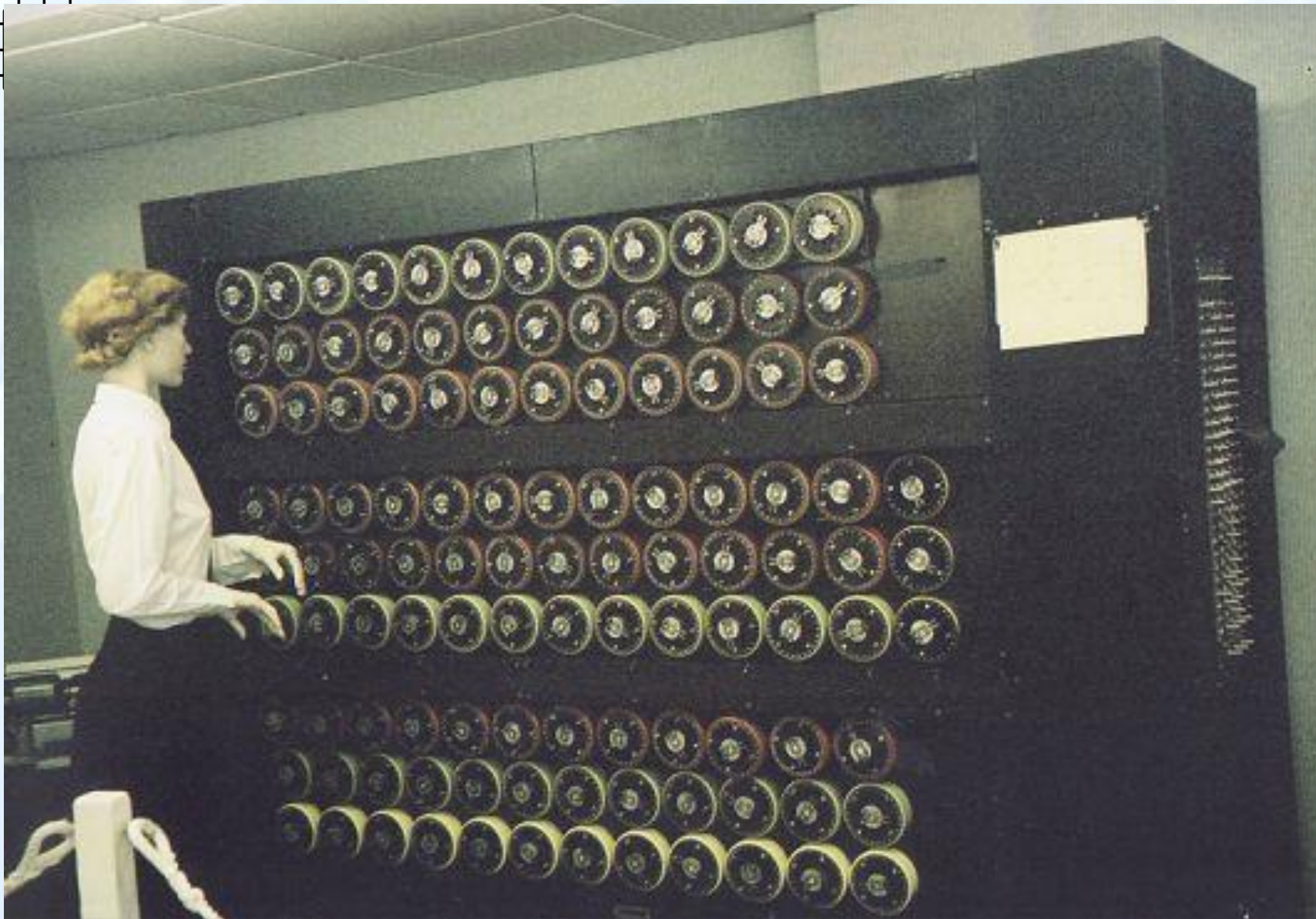
Другие важные результаты

- Проблема самоприменимости МТ
- Универсальная МТ
- Основатель направления ИИ

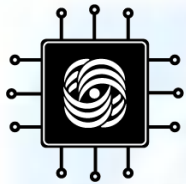




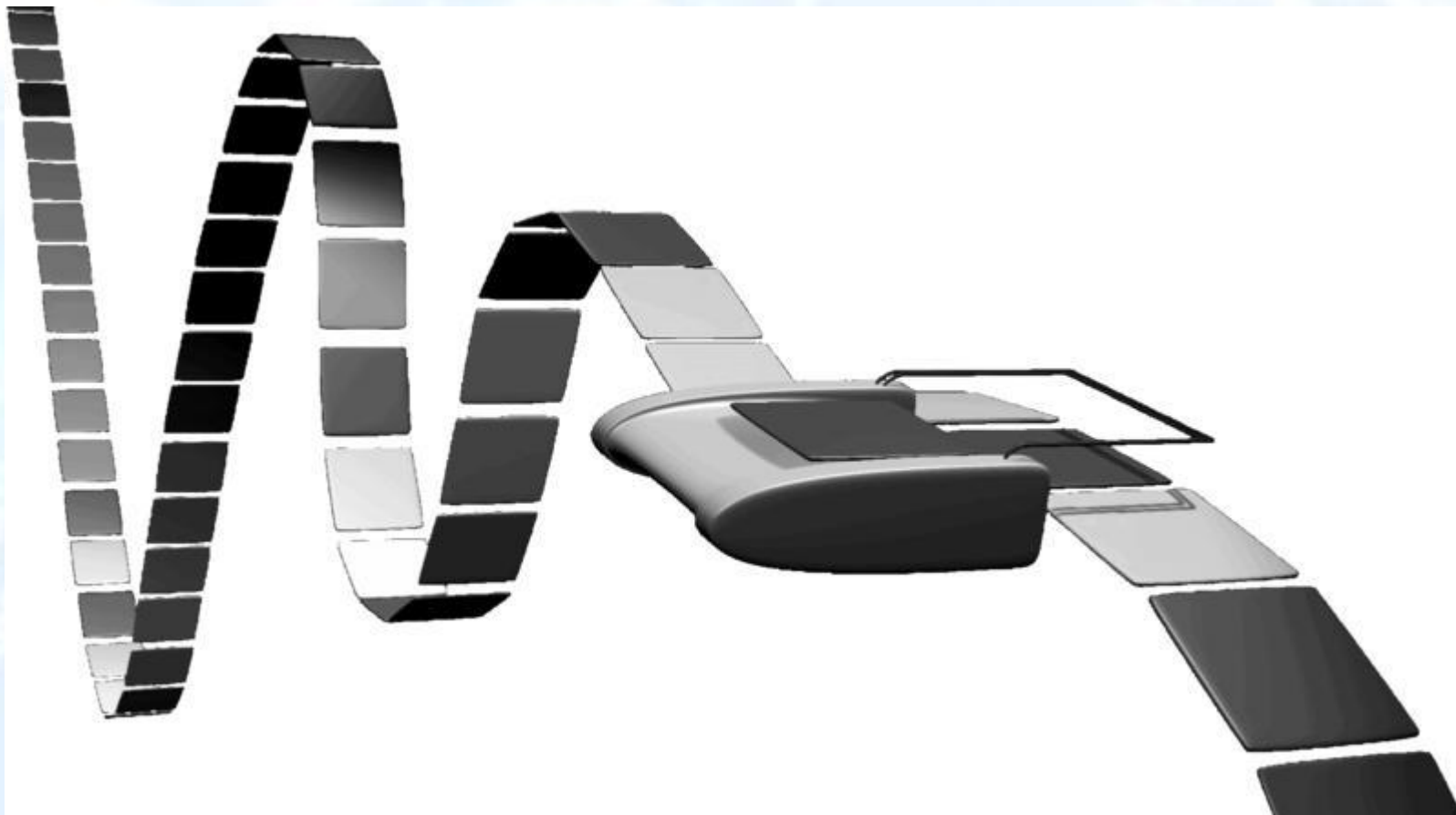
«Бомба»



«Бомба»



Машина Тьюринга



Тест Тьюринга



Судья (человек) переписывается на естественном языке с двумя собеседниками, один из которых — человек, другой — компьютер. Если судья не может надежно определить, кто есть кто, считается, что компьютер прошел тест. Предполагается, что каждый из собеседников стремится, чтобы человеком признали его. Чтобы сделать тест простым и универсальным, переписка сводится к обмену текстовыми сообщениями. Переписка должна производиться через контролируемые промежутки времени, чтобы судья не мог делать заключения исходя из скорости ответов. (Во времена Тьюринга компьютеры реагировали медленнее человека. Сейчас это правило необходимо, потому что они реагируют гораздо быстрее, чем человек.)





Герман Холлерит (1860-1929)



Колесников Е. Краткая биография Г.Холлерита.

<http://eakolesnikov.narod.ru/Hollerith.htm>

Образец схемы, по которой пробивались
карточки
при разработке Австрийской переписи.

I	Pa	aP	m	AG	AB	AL	h	AI	AG	AB	AL	h	AI	GO	GI
II	Am	JB	w	0	5	0	5	0	5	0	5	0	5	0	5	0	5	.	.
III	Bg	KA	.	1	6	1	6	1	6	1	6	1	6	1	6	1	6	.	.
IV	Da	KI	St	2	7	2	7	2	7	2	7	2	7	2	7	2	7	.	.
V	EG	Sp	Ka	3	8	3	8	3	8	3	8	3	8	3	8	3	8	.	.
VI	gO	Va	aA	4	9	4	9
.	.	.	.	1	0	1	0	1	0	1	0	1	0	1	0	1	0	di	ben
.	o	.	HA	2	0	2	0	2	0	2	0	2	0	2	0	2	0	pl	st
EA	h	La	HM	3	0	3	0	3	0	3	0	3	0	3	0	3	0	st	sk
DA	Th	I	GA	4	0	4	0	4	0	4	0	4	0	4	0	4	0	k	tm
.	Ir	Am	GM	5	0	5	0	5	0	5	0	5	0	5	0	5	0	mg	fr
.	Cr	0	B	FS	FB	FA	FT	ci	mh

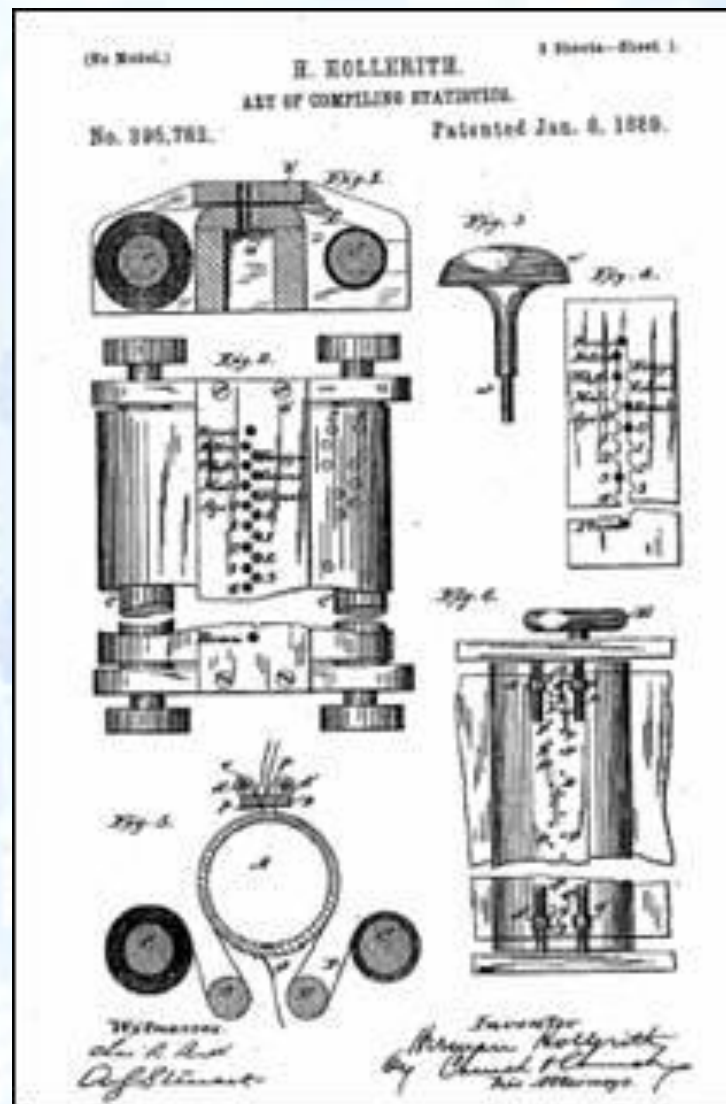
Объяснение условных букв и номеров на Австрийской карточке.

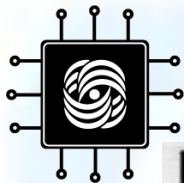
I. Общество по разрядам.

I.	Обитатели общества	состоящие по	болше	500	жителес
II.	>	>	> отъ	501	до 2,000
III.	>	>	> отъ	2,001	до 5,000
IV.	>	>	> отъ	5,001	до 10,000
V.	>	>	> отъ	10,001	до 20,000
VI.	>	>	>	болше	20,000

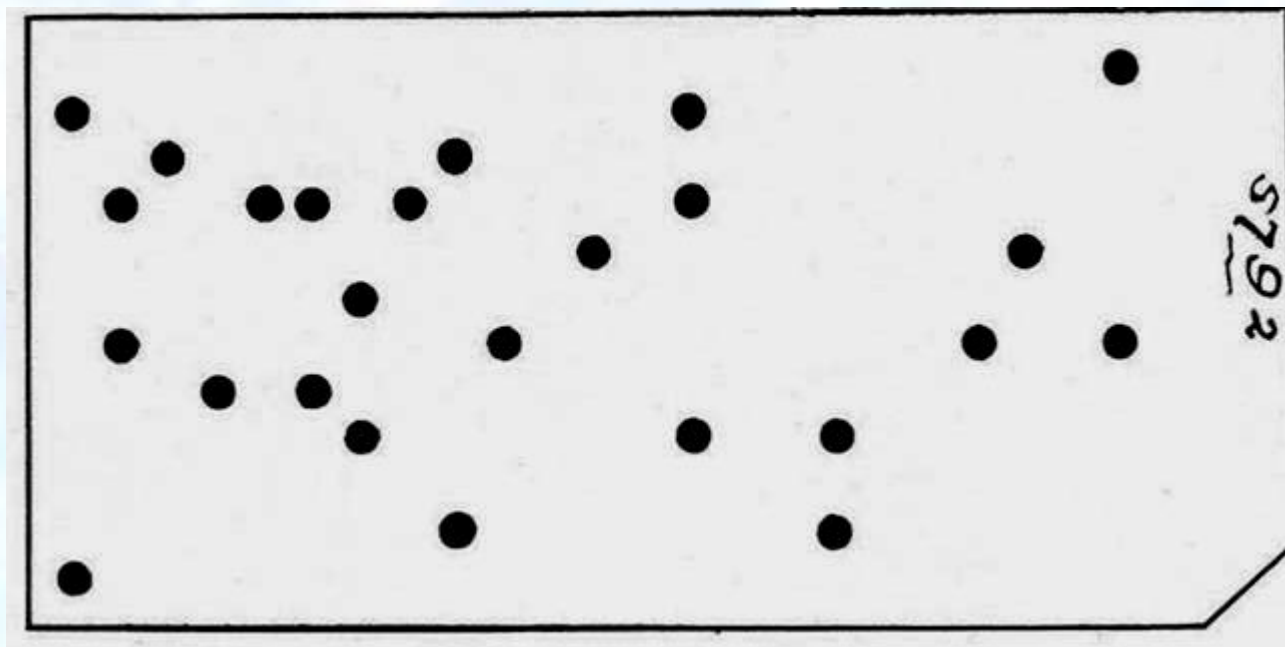
II. Отношение къ классу семейства.

Pa.	Членъ семейства.	KI	Обитатель монастыря.
Am.	Женщина.	Sp	Прислуживающій въ болницѣ.
Bg.	Почтмейстеръ.	Ya	Прислуживающій въ богадѣльнѣ, приютѣ и т. п.
Da.	Прислуга.	St	Заключенный въ тюрьмѣ или въ исправительномъ заведеніи.
EG.	Сельскій работникъ.	Ka	Солдаты въ лагерѣ.
gO.	Проклещивающій работникъ.	aA	Проклещивающій въ какомъ либо другомъ общественномъ учрежденіи.
aP.	Остатки проклящивающія въ квартирѣ лица.		
h.	Проживающій въ гостиницѣ или въ меблированной комнатѣ.		
EA.	Воспитанникъ учебнаго заведенія.		

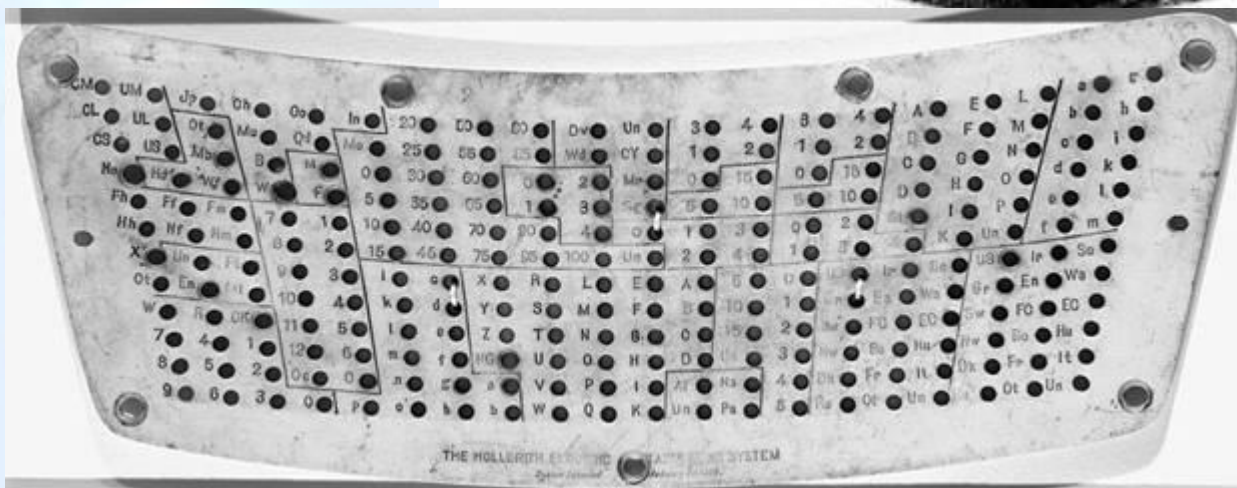
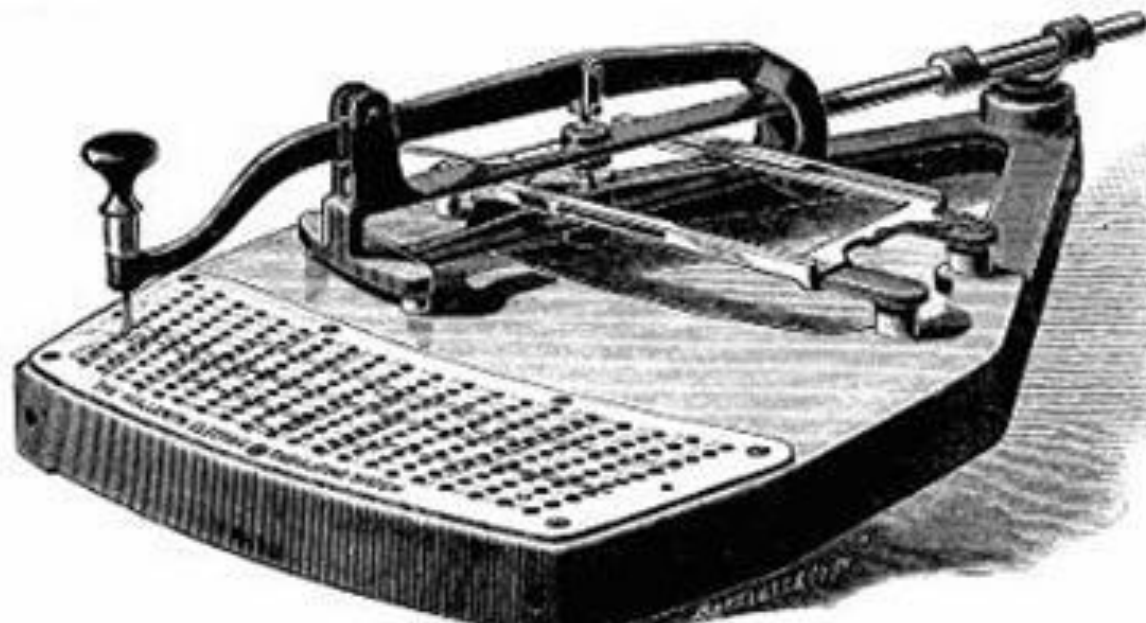
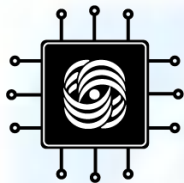




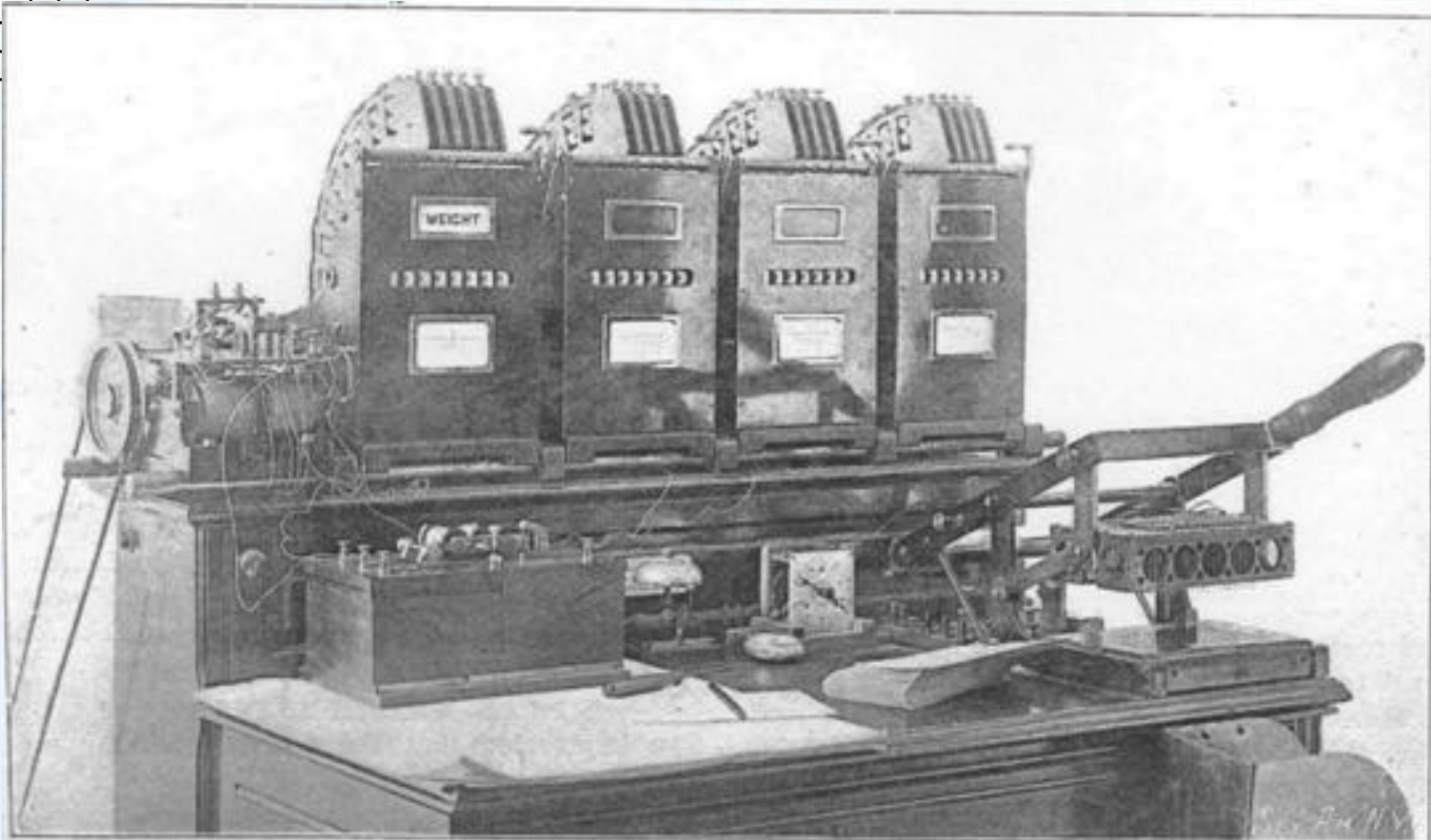
Перфокарты переписи 1890



1. Первые четыре столбца (1), начиная слева, содержали цифровой код района проведения переписи.
2. Раса: Jr, Ch, In, W, B и т.д.
3. Пол: M, F (строки 3..4)
4. Возраст определялся попаданием в пятилетний период: 0,5,10..100
5. Возраст внутри пятилетнего периода: 0..4 (строки 3..5)
6. Семейное положение
7. Закодированное место рождения согласно специальной таблицы.



Пантограф



Табулятор

SCIENTIFIC AMERICAN

A WEEKLY JOURNAL OF PRACTICAL INFORMATION, ART, SCIENCE, MECHANICS, CHEMISTRY, AND MANUFACTURES
NEW YORK, AUGUST 26, 1894





Статистическая машина Г.Холлерита. Государственный Политехнический музей (Москва)



Холлерит, Россия, 1897



**Семён Николаевич
Корсаков (1787-1853)**

Нитусов А. Семен
Корсаков и "машина для
сравнения идей" // PC
WEEK, 2005, № 26.

[http://www.pcweek.ru/themes/detail.php?ID=70819
&THEME_ID=](http://www.pcweek.ru/themes/detail.php?ID=70819&THEME_ID=)

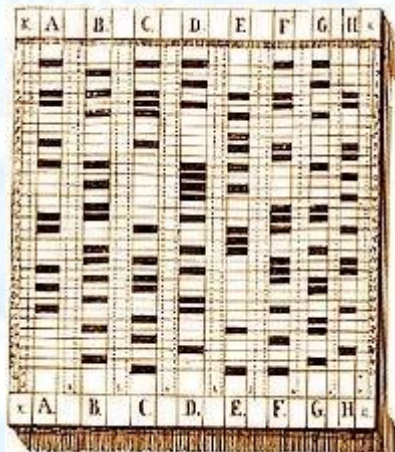
Перфокарты

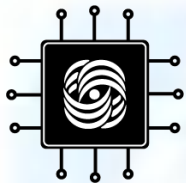
1906 год - Джеймс Пауэрс (James Powers) предложил механические перфораторы с электрическим мотором.

1928 год - фирма IBM ввела новую карту с прямоугольными пробивками, 12 строк и 80 колонок, размер карты $7\frac{3}{8} \times 3\frac{3}{4}$ дюйма (187,325 × 82,55 мм), толщина карты 0,007 дюйма (0,178 мм). Первоначально углы были острые.

1964 год - появились перфокарты со скруглёнными углами.

1985 год - фирма IBM закрыла свою последнюю фабрику по выпуску перфокарт

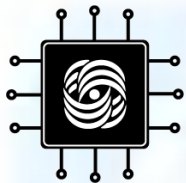




Табуляторы: от Холлерита до машиносчетных станций



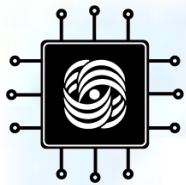
Герман Холлерит
(Hollerith, Hermann; 1860-1929)



Табуляторы: от Холлерита до машиносчетных станций

1	1	3	0	2	4	10	On	5	A	C	E	a	e	v	c		EB	SB	Ch	Sy	U	Sh	Hk	Dr	Rm
2	2	4	1	3	E	15	Off	15	D	D	F	b	d	g	h		SY	X	Fp	Cn	R	X	Al	Cg	Kg
3	0	0	0	0	W	20		0	0	0	U	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A	1	1	1	1	0	25	A	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
B	2	2	2	2	5	30	B	2	2		2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
C	3	3	3	3	0	3	C	3	3	3		3	3	3	3	3	3	3	3	3	3	3	3	3	3
D	4	4	4	4	1	4	D	4	4	4	4		4	4	4	4	4	4	4	4	4	4	4	4	4
E	5	5	5	5	2	C	E	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
F	6	6	6	6	A	D	F	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
G	7	7	7	7	B	E	G	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
H	8	8	8	8	a	F	H	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
I	9	9	9	9	b	c	I	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9

В «машине для переписи населения» (1887 г.) Холлерит предложил использовать перфокарты, подобные жаккардовым. На каждый объект переписи заводилась отдельная перфокарта, в соответствующих позициях которой делались отверстия, отвечающие определенным значениям признаков (пол, возраст и т. д.)



Табуляторы: от Холлерита до машиносчетных станций

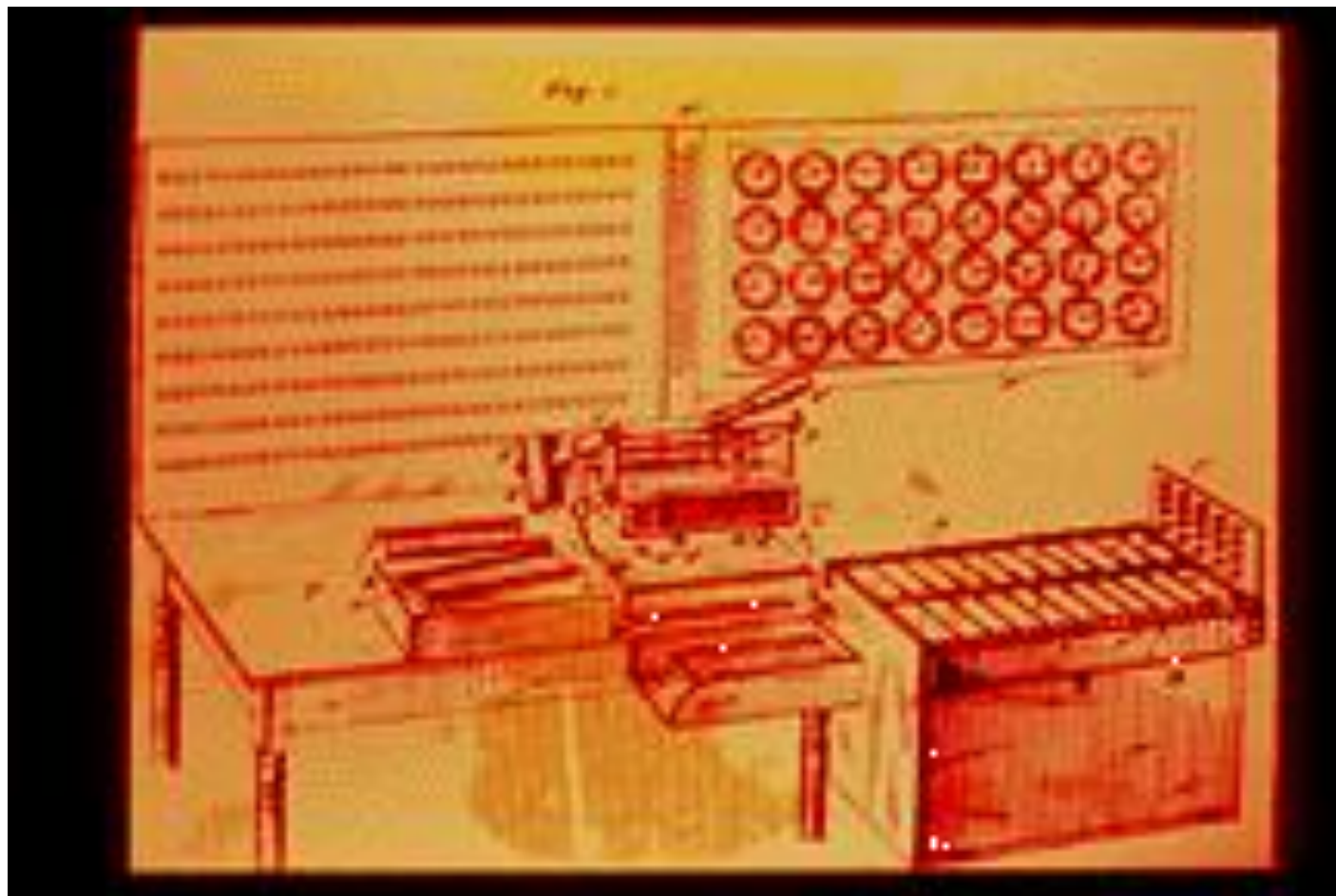
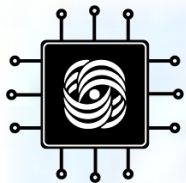


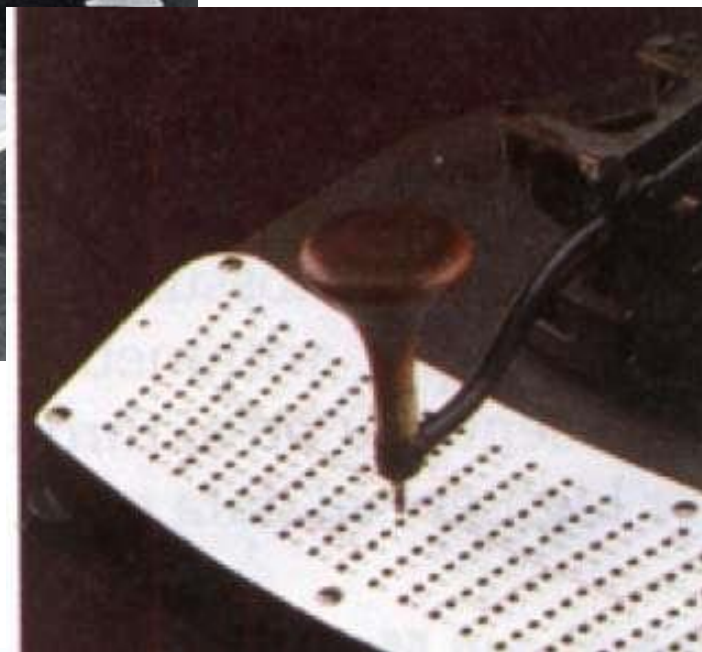
Рисунок из патента Холлерита 1887 г.

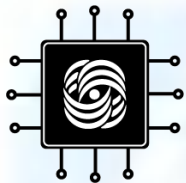


Табуляторы: от Холлерита до машиносчетных станций



Пробивка отверстий в перфокарте Холлерита

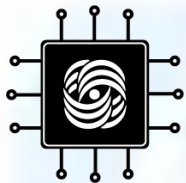




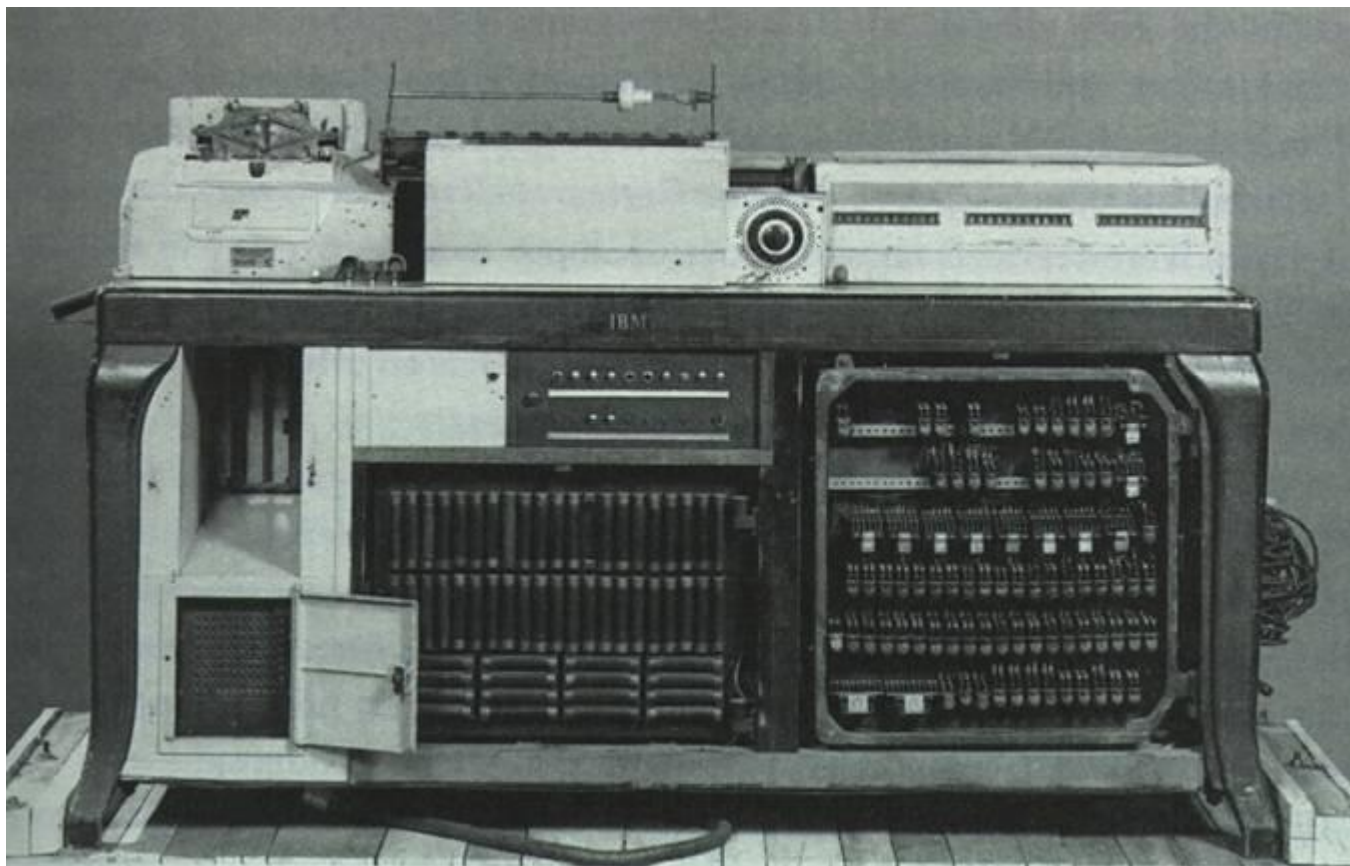
Табуляторы: от Холлерита до машиносчетных станций



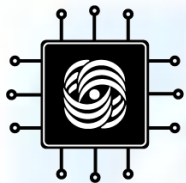
Табулятор Холлерита. Перфокарты считываются устройством, размещенном в углу стола. Сзади расположена панель с электромеханическими счетчиками



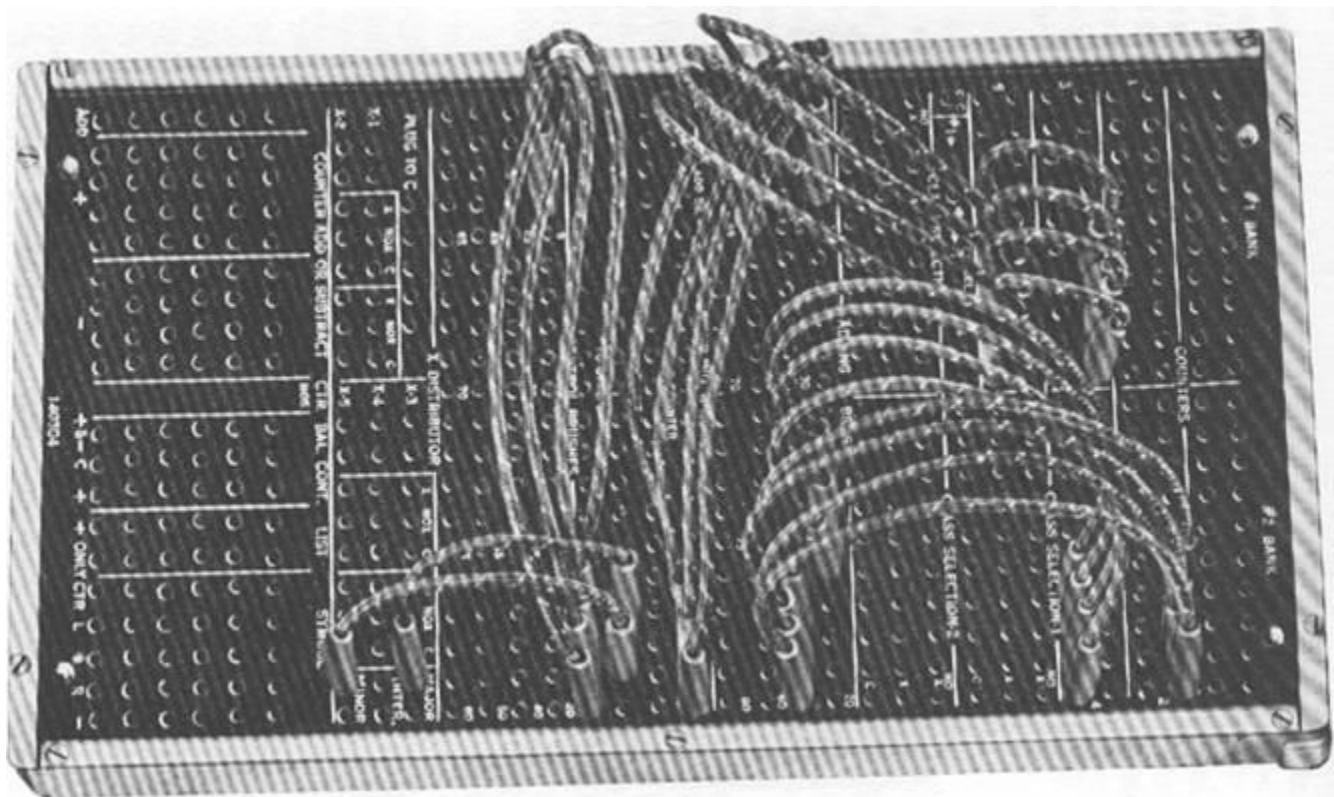
Табуляторы: от Холлерита до машиносчетных станций



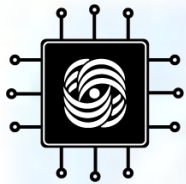
Табулятор фирмы IBM (1920-е годы) представлял собой сложнейшее устройство, содержащее 100 тыс. деталей, 5 км проводов. Результаты расчетов выдавались на печать



Табуляторы: от Холлерита до машиносчетных станций



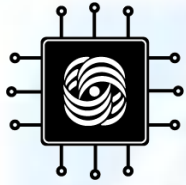
Программа вычислений на табуляторе набиралась штекерами на сменной коммутационной панели



Табуляторы: от Холлерита до машиносчетных станций

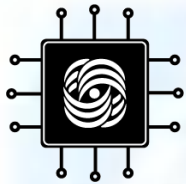


На базе счетно-перфорационных машин в 1930-е годы были организованы «фабрики вычислений» - машиносчетные станции.
На снимке: перфораторный цех МСС



Сложные электромеханические и релейные машины – предвестники ЭВМ

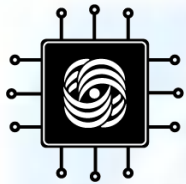
- ✓ Проекты Конрада Цузе (Германия, 1938-1945);
- ✓ Проект Mark-1 Говарда Айкена (Гарвардский университет и IBM, 1939-1944);
- ✓ Проекты Джорджа Стибица (Bell Laboratories, 1939-1947)



Сложные электромеханические и релейные машины – предвестники ЭВМ

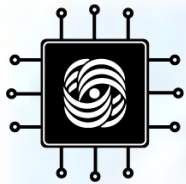


Конрад Цузе (Zuse, Kohnrad; 1910-1995)



Основные результаты

- Первые компьютеры Z1, Z2, Z3, Z4
 - Планкалкюль
 - Принципы построения компьютера
 - Цифровая философия
- (“Вычислительное пространство” (1969(



Принципы Цузе

- Двоичная система счисления;
- Использование устройств, работающих по принципу "да/нет" (логические 1 и 0);
- Полностью автоматизированный процесс работы вычислителя;
- Программное управление процессом вычислений;
- Поддержка арифметики с плавающей запятой;
- Использование памяти большой емкости.

Основные характеристики Z1

Реализация

Частота

Вычислит. блок

Ср. скорость вычислений

Ввод данных

Вывод данных

Память

Вес

Тонкие металлические пластины

1 Гц

Обработка чисел с плавающей запятой, длина машинного слова — 22 бита

Умножение — 5 секунд

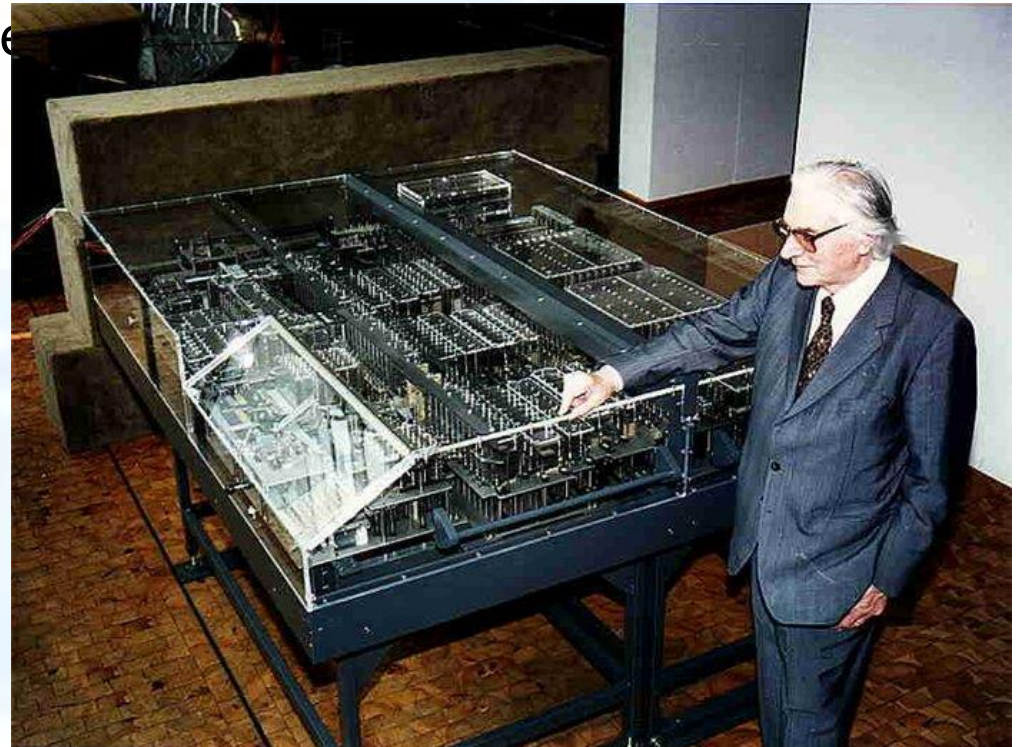
Клавиатура, устройство считывания с перфоленты

Ламповая панель (де

64 слова по 22 бита

Около 500 кг

Профессор Цузе в 1990 году у воссозданного им компьютера Z1



Основные характеристики Z2



Реализация

Тонкие металлические пластины, реле

Частота

3 Гц

Вычислительный блок

Обработка чисел с плавающей запятой, длина машинного слова — 16 бит

Средняя скорость вычислений

Умножение — 5 секунд

Ввод данных

Клавиатура, у перфоленты

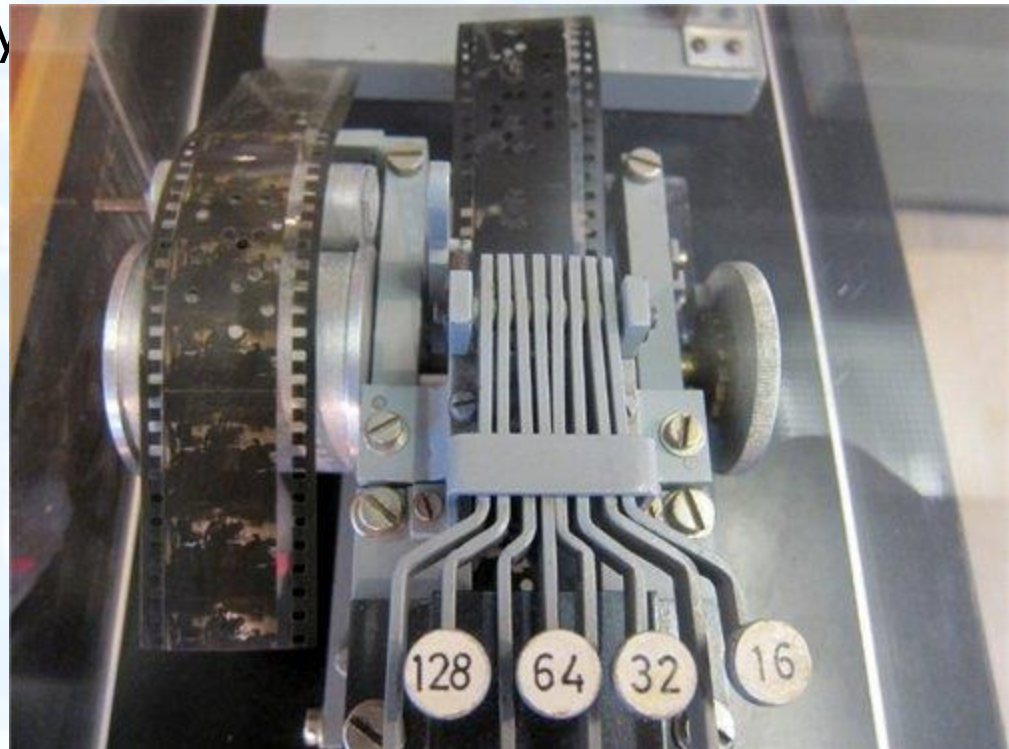
Память

16 слов по 16 бит

Вес

Около 500 кг

Устройство для считывания программ и данных с импровизированной перфоленты в роли которой выступила использованная фотопленка





Основные характеристики Z3

Реализация

Реле (600 — блок вычислений, 1600 — блок памяти)

Частота

5,33 Гц

Вычислительный блок

Обработка чисел с плавающей запятой, длина машинного слова — 22 бита

Средняя скорость вычислений

Умножение, деление — 3 секунды, сложение — 0,7 секунд

Ввод данных

Клавиатура, устройство считывания с перфоленты

Вывод данных

Ламповая панель (десятичное представление)

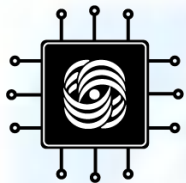
Память

64 слова по 22 бита

Вес

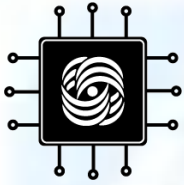
Около 1000 кг



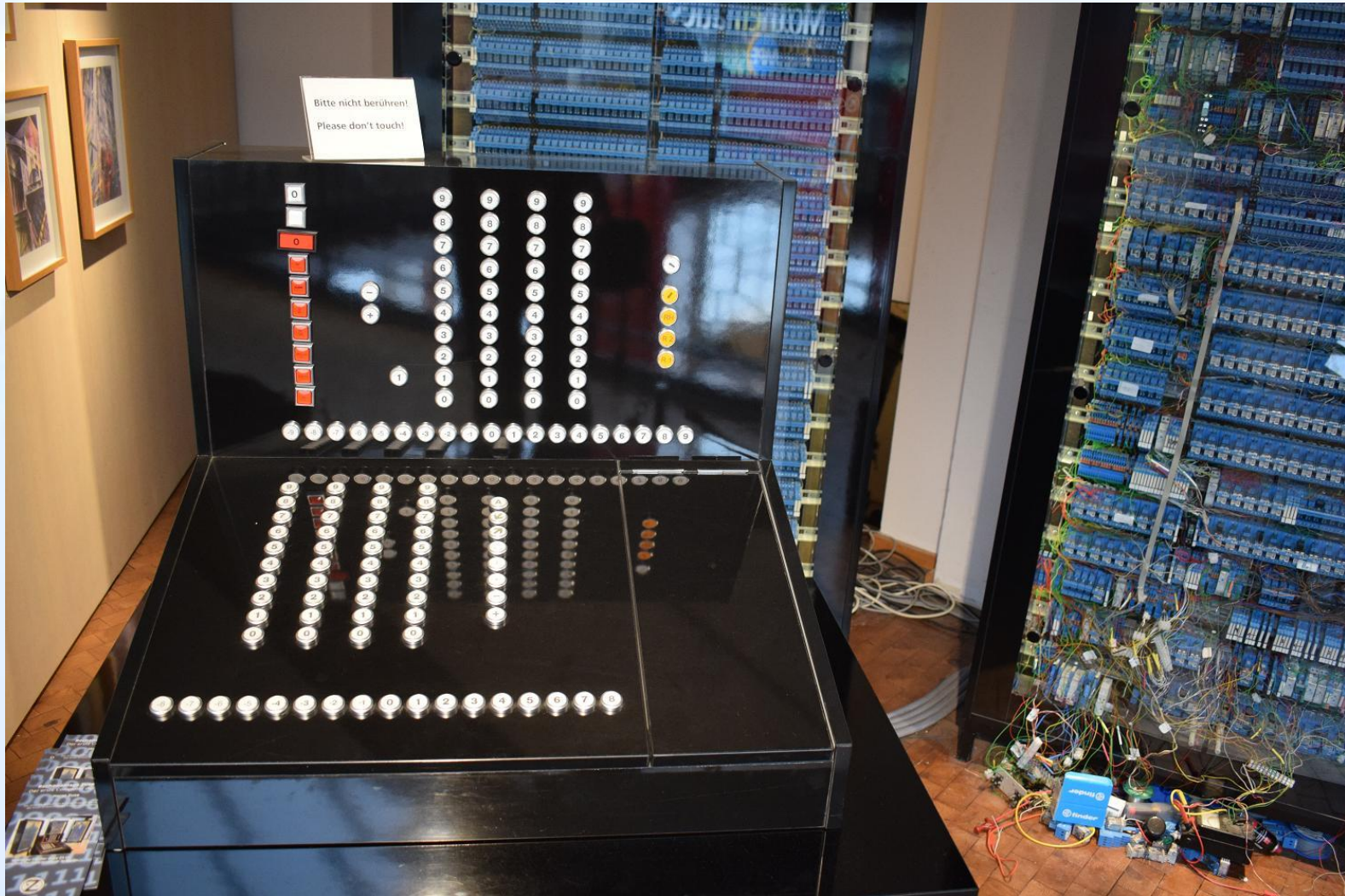


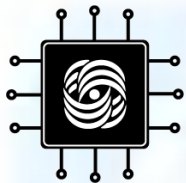
Воссозданная Z3



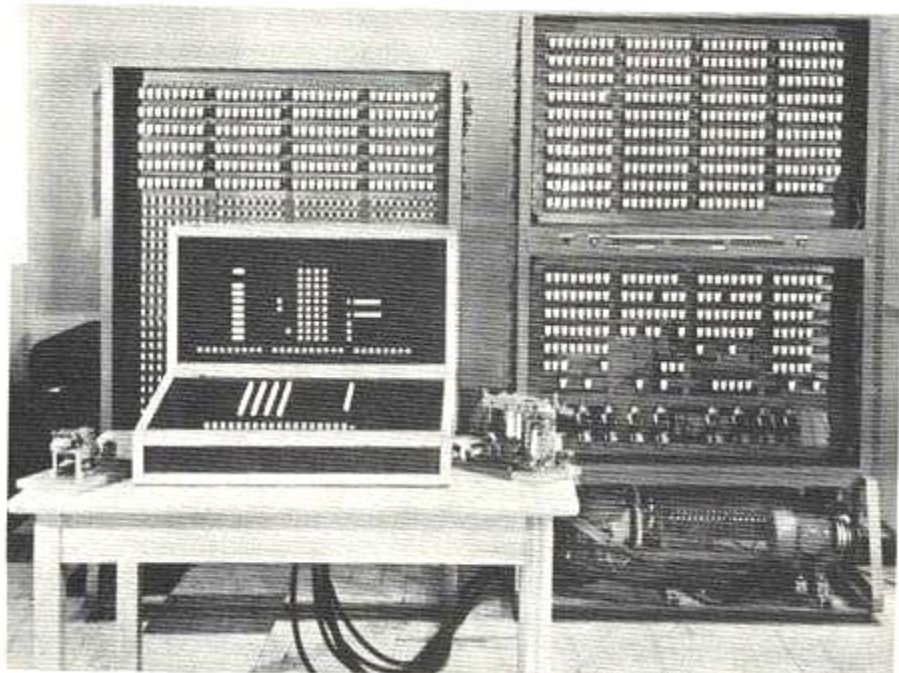


Клавиатура Z3





Сложные электромеханические и релейные машины – предвестники ЭВМ



Первая в истории работающая программно-управляемая универсальная вычислительная машина Z-3 (1941 г.)
2600 реле, ОЗУ 64 22-разрядных слова



Основные характеристики Z4



Реализация

Реле, память — металлические пластины

Частота

30 Гц

Вычислительный блок

Обработка чисел с плавающей запятой, длина машинного слова — 32 бита

Скорость вычислений

11 операций умножения в секунду

Ввод данных

Десятичная клавиатура, устройство считывания с перфоленты

Вывод данных

Печатная машинка марки "Mercedes"

Память

64 слова по 22 бита

Вес

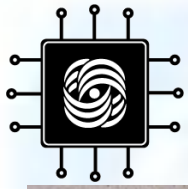
Около 1000 кг

Язык Планкалкюль (нем. Plankalkül исчисление планов). Фрагмент

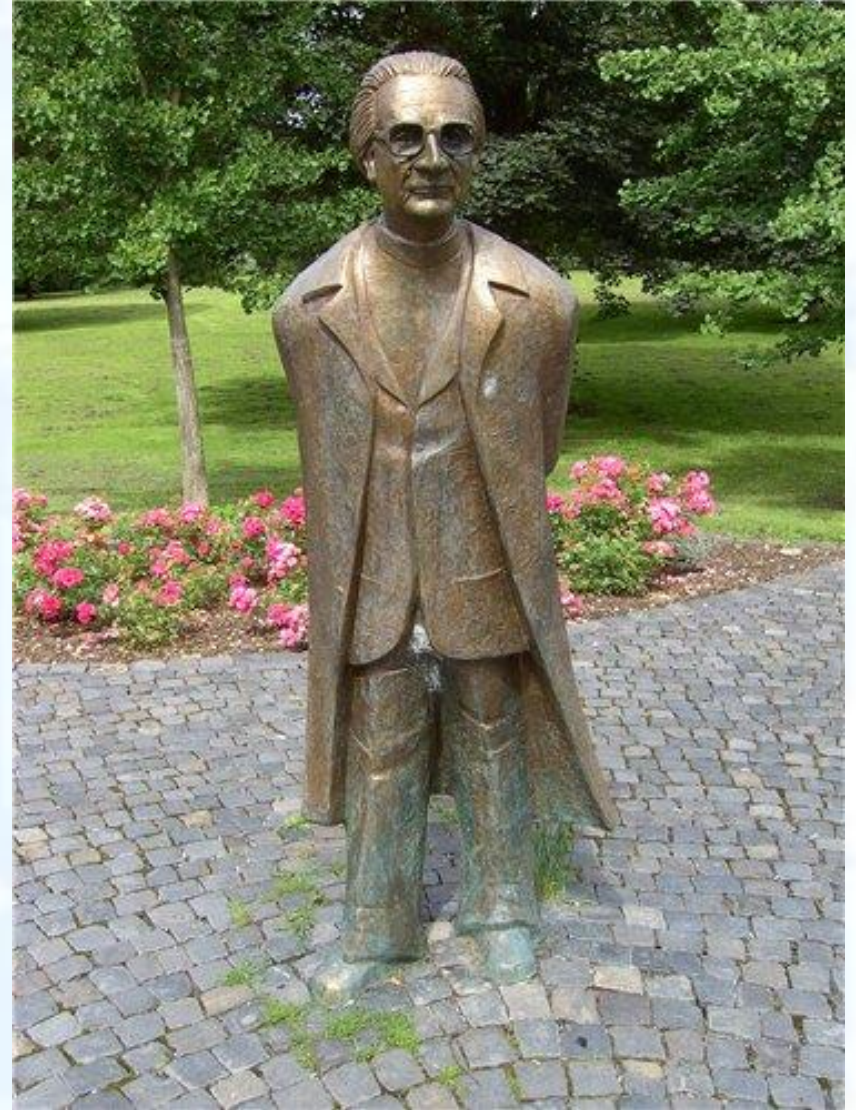
<http://www.pcweek.ru/themes/detail.php?ID=46656>

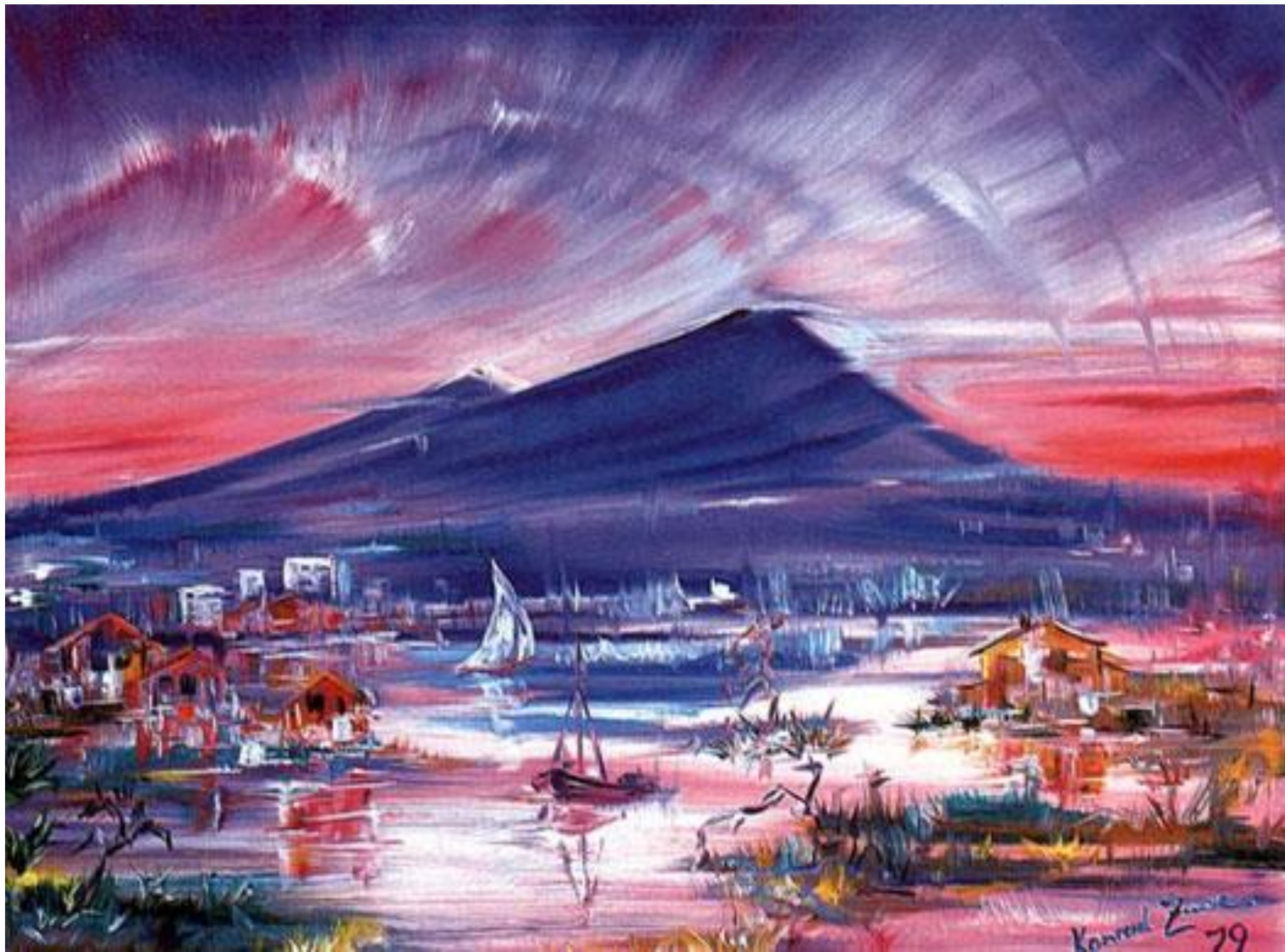
Описание языка Планкалкюль





Конрад Цузе (1910 - 1995)



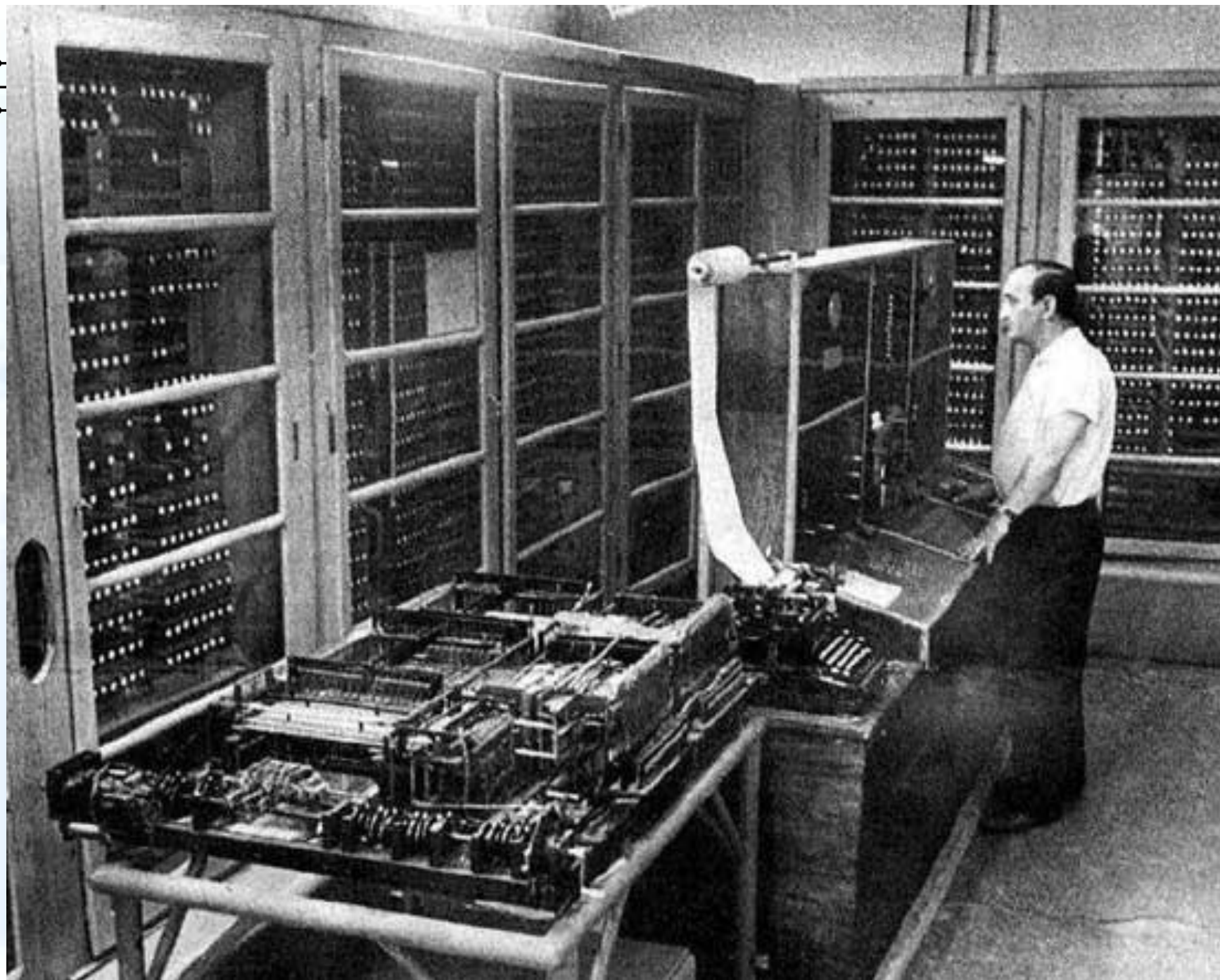


Kenneth Zuckerman
79





“Видение города Stadt”





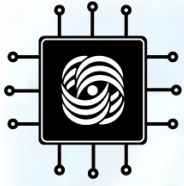


Австрия. В 1947-1952 гг. а инженер, а затем профессор Венского технического университета Хайнц Земанек (Heinz Zemanek)*1 из 700 телефонных реле построил "Универсальную счетную машину 1"

Великобритания. В этой стране было разработано несколько моделей релейных машин, самой известной из которых стала "Автоматическая релейная вычислительная машина" (Automatic Relay Computer), построенная в 1948 г. Эндрю Дональдом Бутом

Венгрия. В 1955-1958 гг. под руководством Ласло Козмы (Laszlo Kozma, 1902-1983) в Венгерском политехническом институте была разработана и изготовлена релейная вычислительная машина MESz-1, содержащая 2000 реле и введенная в регулярную эксплуатацию в 1959-м.

Нидерланды. 21 июня 1952 г. в Математическом центре Амстердама была введена в действие "Амстердамская автоматическая счетная машина"



Спасибо за внимание!