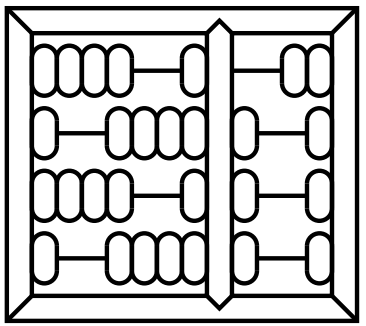
Caminhos cruzados: Alan Turing e John von Neumann

Tomasz Kowaltowski

Instituto de Computação
Universidade Estadual de Campinas



Março de 2017

www.ic.unicamp.br/∼tk
tk@ic.unicamp.br

Instituto de Computação

Universidade Estadual de Campinas

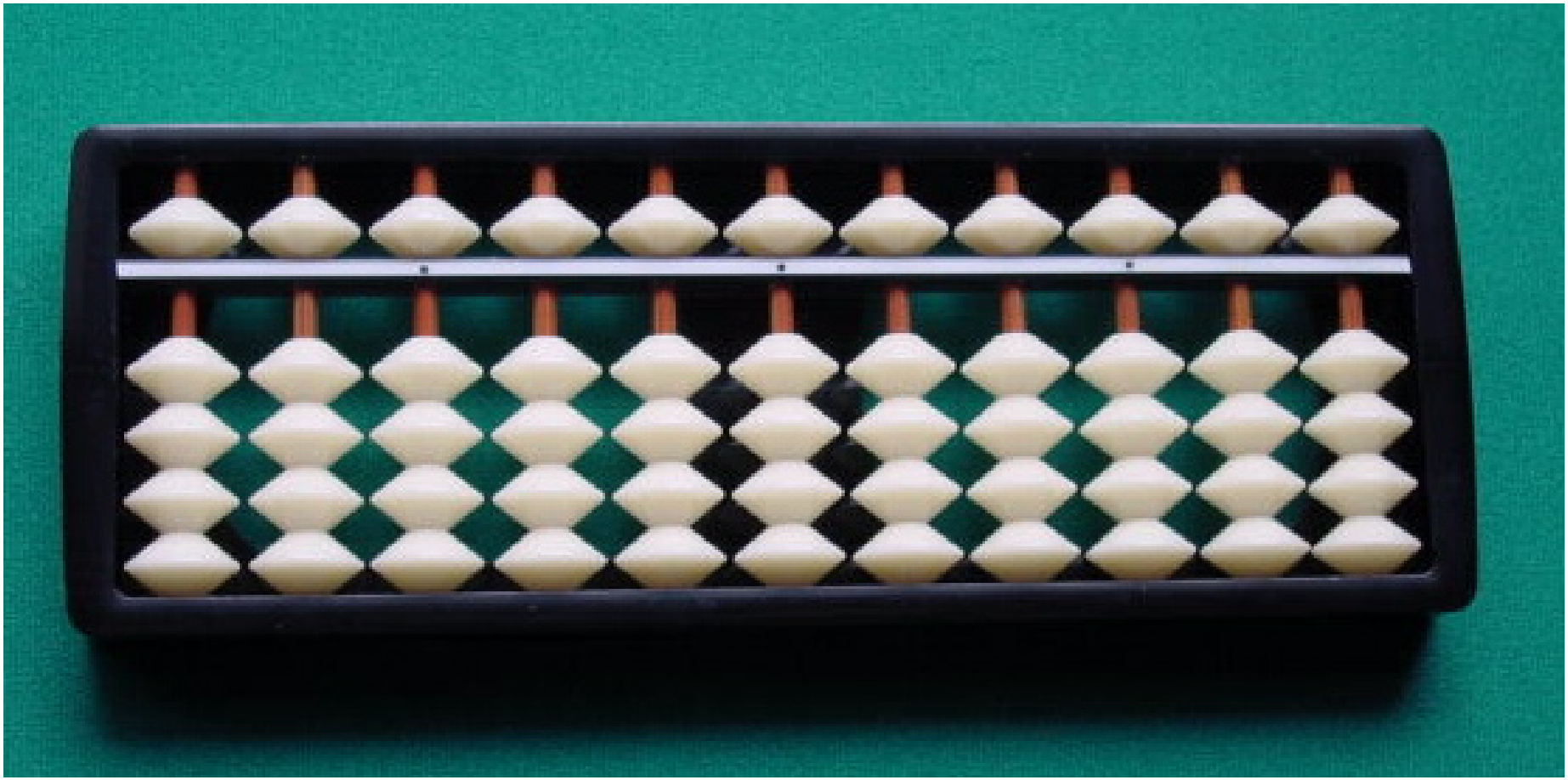
Arquivo PDF gerado em 18 de março de 2017

Introdução

- Por que Turing e von Neumann?
- "Máquina de Turing" e "Arquitetura [de] von Neumann"
- Roteiro:
  - Pré-história: cálculos manuais, máquinas calculadoras, computadores
  - História
    - computadores digitais "modernos": ∼1930-1950
    - teoria de computabilidade
  - Alan Turing: sua vida e suas contribuições
  - John von Neumann: sua vida e suas contribuições
  - Caminhos cruzados
  - Controvérsia famosa: conceito de programa armazenado na memória
  - Contrastes

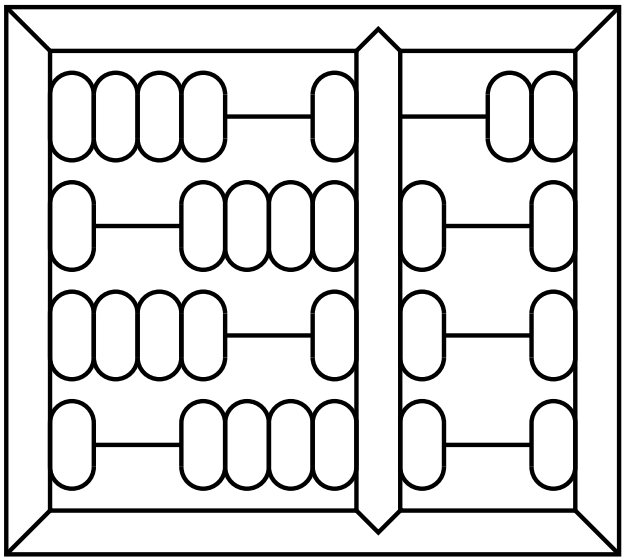
Pré-história: cálculos manuais

- Dedos (latim: *digitus, pl. digiti*)
- Pedras (latim: *calculus, pl. calculi*)
- Ábacos e dispositivos semelhantes

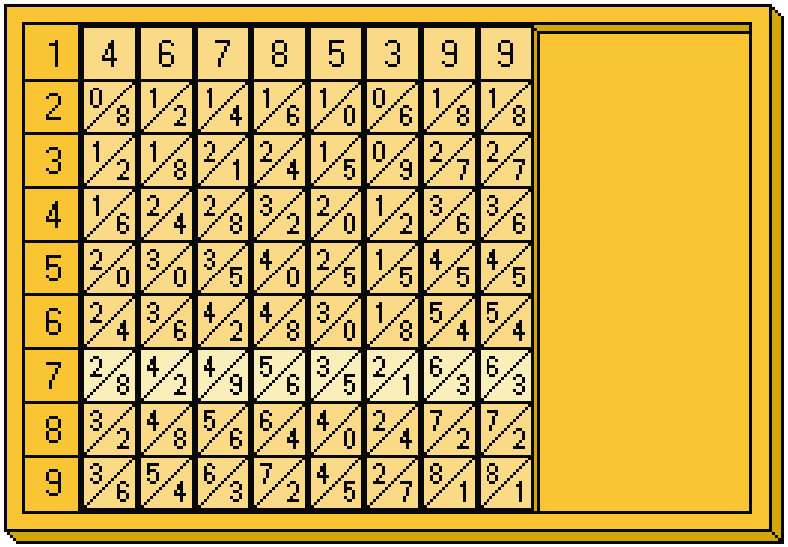


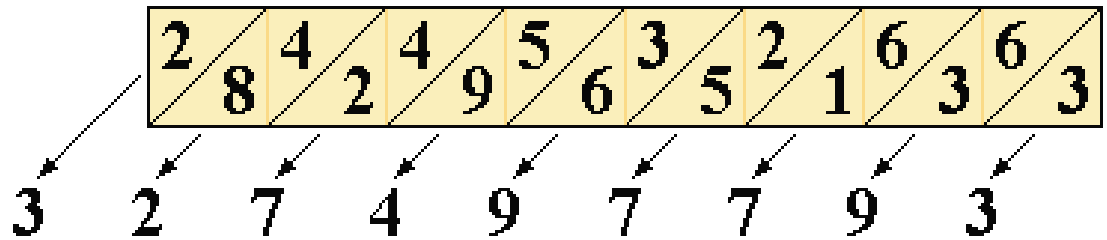
Ábaco japonês: soroban,
(http://www.japanese-games-shop.com/other-goods/soroban/)

Ábaco chinês: suanpan
(070710678)
(Wikipedia: *Suanpan*)



Logotipo do IC da UNICAMP
(1969)



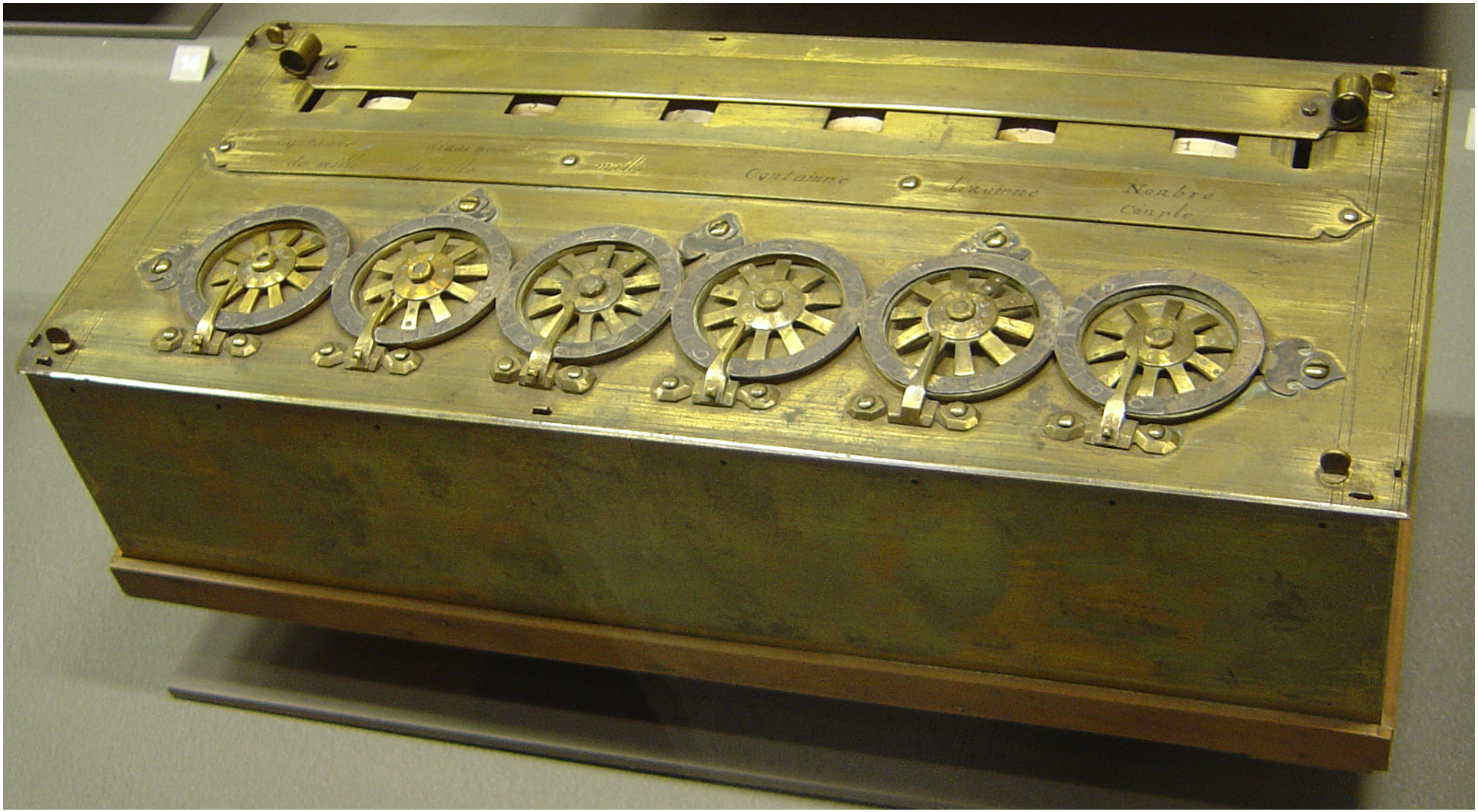


Varetas de Napier, http://en.wikipedia.org/wiki/Napier_rods

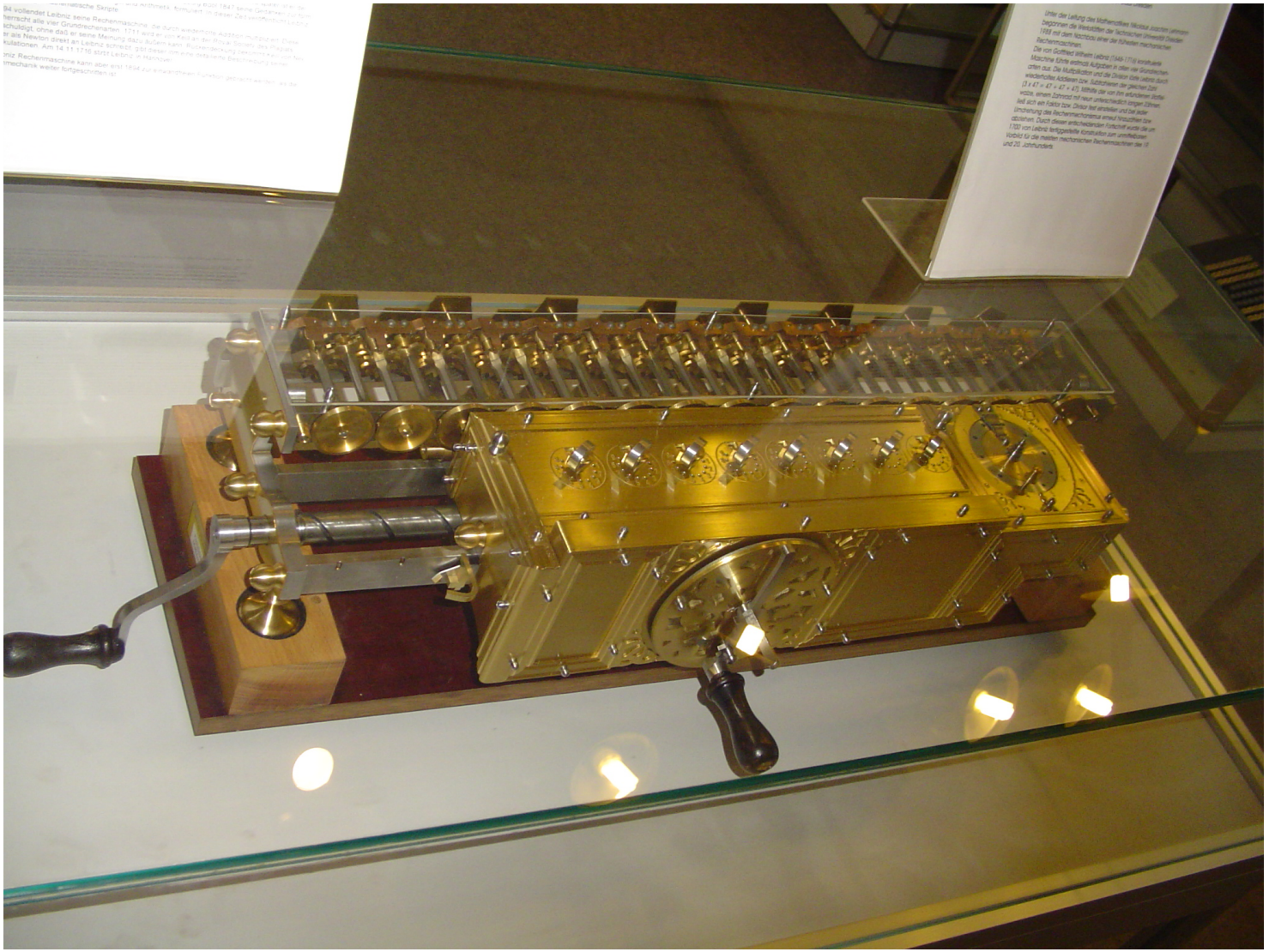
(Operação: $7 \times 46.785.399 = 327.497.793$)

Pré-história: máquinas mecânicas de calcular

- Blaise Pascal (1623-1662)
- Gottfried Leibnitz (1646-1716)
- ...
- Até a década de 1970 (ou mais!)



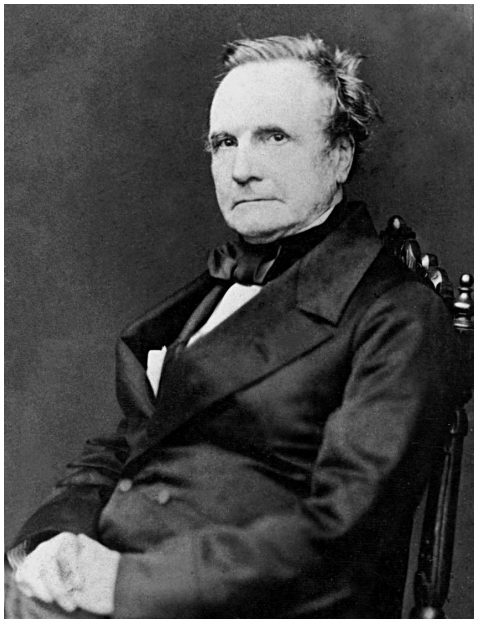
Pascaline (1642), Wikipedia: *Pascal's calculator*



Staffelwalze (1672-1694), Wikipedia: *Stepped Reckoner* – Leibnitz

Odhner (∼1970 – desde 1874), `home.comcast.net/~wtodhner/calcs.html`

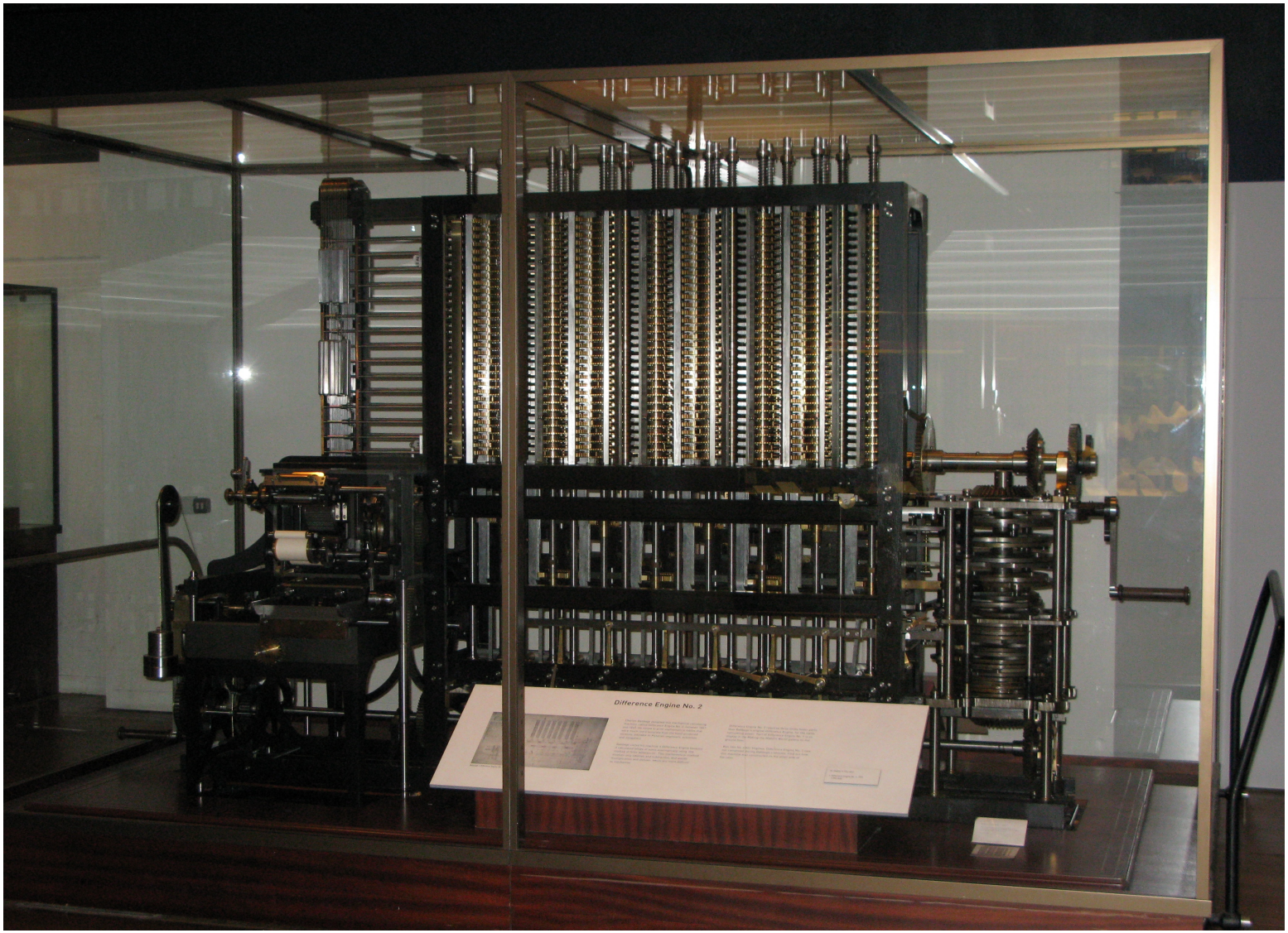
Pré-história de computadores digitais



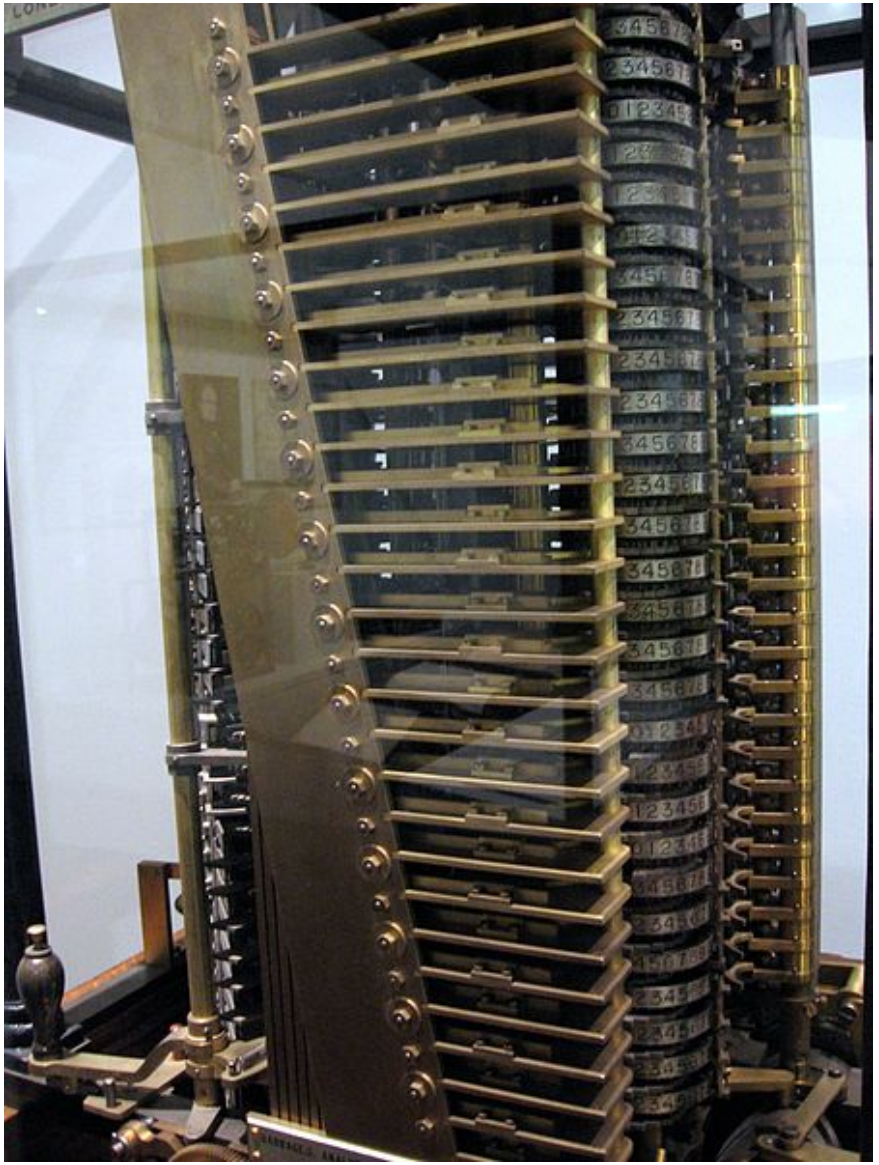
Charles Babbage (Grã-Bretanha, 1791-1871)

Máquinas mecânicas:

- máquina de diferenças ($\sim$1823) para cálculo de aproximações polinomiais: construção não terminou
- máquina analítica de propósito geral (1837-1871): parcialmente completada pelo filho Henry Babbage em 1910 – programável por meio de cartões perfurados
- Ada Lovelace descreveu a máquina analítica em 1843 – considerada a primeira programadora (linguagem *Ada* nomeada em sua homenagem)
- várias máquinas de diferenças de irmãos Scheutz (Suécia) baseadas no projeto de Babbage (1855 em diante)
- implementação difícil devido à necessidade de mecânica de alta precisão



Máquina de diferenças – modelo (1991), Wikipedia: *Difference engine*

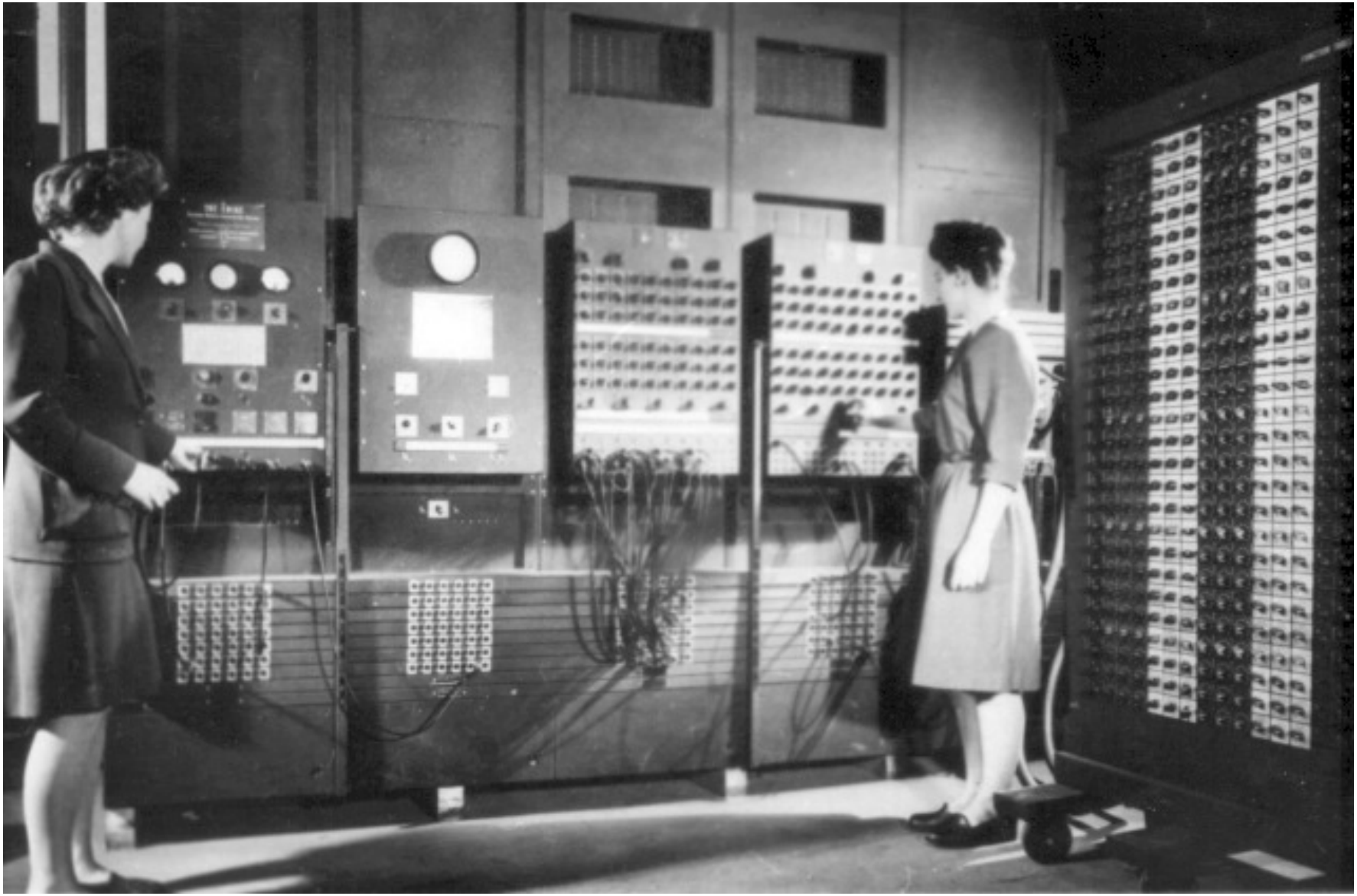


Máquina analítica parcial de Henry Babbage (1910), Wikipedia: *Analytical engine*

Ada Lovelace, Wikipedia: *Ada Lovelace*

História "moderna" de computadores digitais: ∼1930-1950

- 1934-1941: máquinas de Konrad Zuse (Alemanha)
- 1937-1944: máquinas especializadas para cálculos específicos (Atanasoff, Aiken, Stibitz e outros, EUA)
- 1939-1945: máquinas para criptoanálise – Bombe, Colossus (Bletchley Park, GB): Alan Turing, Newman, Welchman, Flowers, ...
- 1942-1945: ENIAC – primeiro computador eletrônico de propósito geral (Eckert e Mauchly, Universidade de Pennsylvania, EUA)
- 1944-1951: EDVAC – primeiro projeto de computador com programa armazenado na memória (von Neumann, Eckert, Mauchly e outros, Universidade de Pennsylvania, EUA)
- 1945-1951: computador do Instituto de Estudo Avançado (IAS, Princeton, EUA): von Neumann e outros
- 1946-1950: projeto ACE de Alan Turing (Pilot ACE, NPL, GB)
- 1947-1948: máquina experimental SSEM de Manchester (Kilburn)
- 1947-1949: EDSAC – primeiro computador real com programa armazenado a entrar em funcionamento (Wilkes, Cambridge, GB)
- 1950 em diante: sucessores de EDVAC e IAS – JOHNNIAC, ORDVAC, ILLIAC, MANIAC, SILLIAC, WEIZAC, ...



ENIAC (1942-1945), Wikipedia: *ENIAC*

História da teoria de computabilidade

- Gottfried Leibnitz (1646-1716) imaginou a possibilidade de construir uma máquina de manipulação simbólica que pudesse determinar a veracidade de proposições matemáticas
- Formalização da lógica matemática: George Boole ($\sim$1850)
- Diagonalização de Georg Cantor (1891): reais não são enumeráveis
- *Entscheidungsproblem* (problema de decisão) de David Hilbert (1920): decidibilidade da lógica de primeira ordem
- Incompletude da lógica de primeira ordem por Kurt Gödel (1931, numeração de Gödel)
- Indecidibilidade de problemas relacionados com cálculo λ e com funções recursivas por Alonzo Church (1936)
- Máquina universal e indecidibilidade da parada por Alan Turing (1936)
- Equivalência das abordagens de Church e Turing
- Várias formulações equivalentes: Emil Post (1936)

Alan Turing (1912-1954)

Wikipedia: *Alan Turing*

Biografia resumida de Turing

- 1912: nascimento em Londres (Inglaterra)
- 1931-1934: graduação em matemática no King's College (Cambridge)
- 1935-1936: *fellowship* no King's College
- 1936: publicação do trabalho *On Computable Numbers, with an Application to the Entscheidungsproblem*
- 1936-1938: pós-graduação na Universidade de Princeton onde estudou também criptografia e fez experimentos com multiplicadores eletro-mecânicos
- 1938: conclusão do doutorado sob a orientação de Alonzo Church – introduziu a ideia de oráculo
- 1938-1939: pós-doutorado na Universidade de Cambridge
- 1939-1945: serviço de inteligência britânico e laboratório de criptoanálise em Bletchley Park
- 1945-1947: Laboratório Nacional de Física (NPL) e projeto ACE
- 1948-1954: Universidade de Manchester
- 1952: processo e condenação por homossexualismo
- 1954: suicídio em Manchester aos 42 anos de idade
- 2009: pedido formal de desculpas do governo britânico
- 2013: perdão real

Contribuições de Turing

- Teoria da computabilidade usando a noção de máquinas ideais em contraposição a outros formalismos (Gödel e Church) – máquina de Turing
- Resultados mais famosos: problema da parada e máquina universal
- Trabalho de criptoanálise (Bletchley Park) – mais adiante
- Um misturador (*scrambler*) seguro de voz
- Projeto ACE (Automatic Computing Engine) no NPL– inacabado
- Inteligência artificial: teste de Turing
- Biologia matemática: morfogênese (formação de padrões)

Máquina de Turing

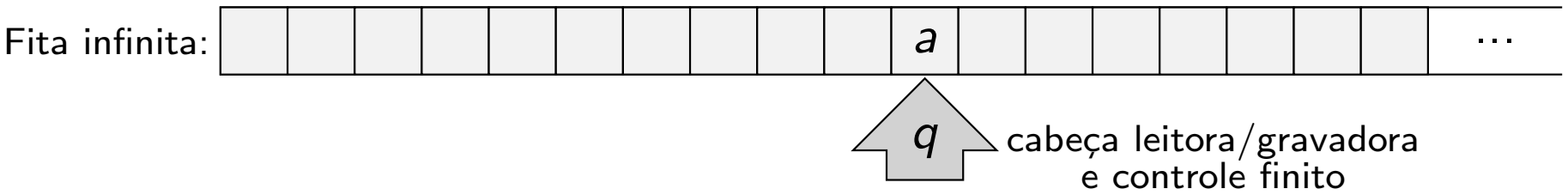


Tabela finita (programa) de regras de transição da forma:

$$(q_1, a) \Rightarrow (q_2, b, d)$$

onde:

- q_is são os estados (número finito)
- 'a' e 'b' são os símbolos do alfabeto $\{0, 1\}$ ou brancos
- $d = -1$ ou $d = +1$: é o movimento da cabeça leitora/gravadora
- existem estados q_0 (inicial) e q_f (final)
- o conteúdo inicial da fita constitui os dados
- o conteúdo final da fita constitui os resultados

A máquina para quando for alcançado o estado q_f.

(cont.)

Máquina de Turing (cont.)

Exemplo trivial: programa que multiplica por dois um número em notação binária

$$
\begin{aligned}
(q_0, 0) &\Rightarrow (q_0, 0, +1) \\
(q_0, 1) &\Rightarrow (q_0, 1, +1) \\
(q_0, \sqcup) &\Rightarrow (q_f, 0, +1)
\end{aligned}
$$

Máquina de Turing (cont.)

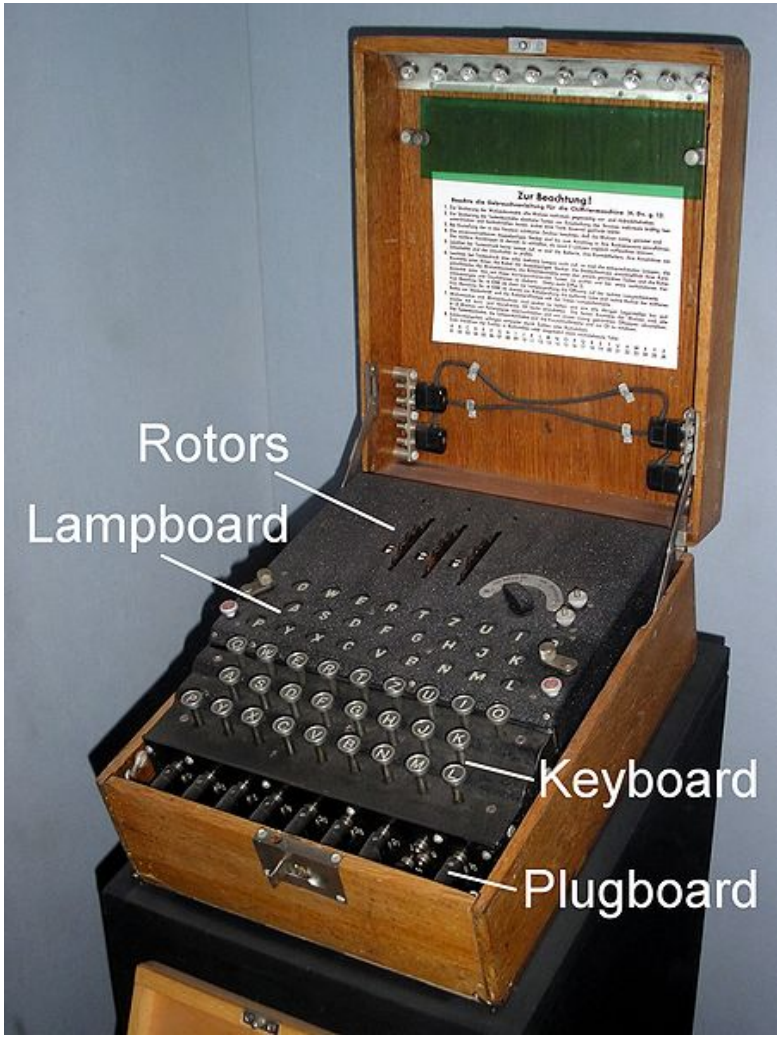
- Existem várias formulações diferentes mas equivalentes
- A máquina pode não parar ou chegar numa configuração (q, a) não prevista na sua tabela
- O alfabeto pode ser qualquer (um ou mais símbolos)
- O conteúdo da fita pode ser interpretado como representação de números, de cadeias de caracteres, etc
- Apesar da extrema simplicidade do modelo, é intuitivo que qualquer cálculo mecânico sobre este tipo de representações pode ser implementado por uma máquina de Turing – tese de Church-Turing
- Máquina universal: supõe que o conteúdo inicial da fita é a descrição de uma máquina de Turing que deve ser interpretada
- Usando o conceito de máquina universal e uma construção equivalente à diagonalização de Cantor, Turing demonstrou a indecidibilidade do problema da parada: *não existe um algoritmo (i. é, uma máquina de Turing) que possa decidir se uma dada máquina para depois de um número finito de transições*
- O reconhecimento da importância deste trabalho não foi imediato

Turing e criptoanálise

- Durante o estágio em Princeton, Turing idealizou alguns métodos primários de criptografia e chegou a construir dispositivos eletro-mecânicos para sua implementação
- Idealizou várias técnicas algébricas, combinatoriais e probabilísticas, usadas no deciframento de mensagens cifradas pela máquina *Enigma*
- Projetou a máquina eletro-mecânicanica *Bombe* para o deciframento destas mensagens (com G. Welchman)
- Formulou uma técnica para para auxiliar no deciframento de mensagens cifradas pela máquina *Lorenz* (com W. Tutte)
- Importância fundamental para o esforço militar aliado
- Segundo algumas avaliações, o trabalho de Turing e seus colaboradores encurtou em dois anos a Segunda Guerra Mundial
- Reconhecimento pleno muito tardio e póstumo devido às leis de confidencialidade

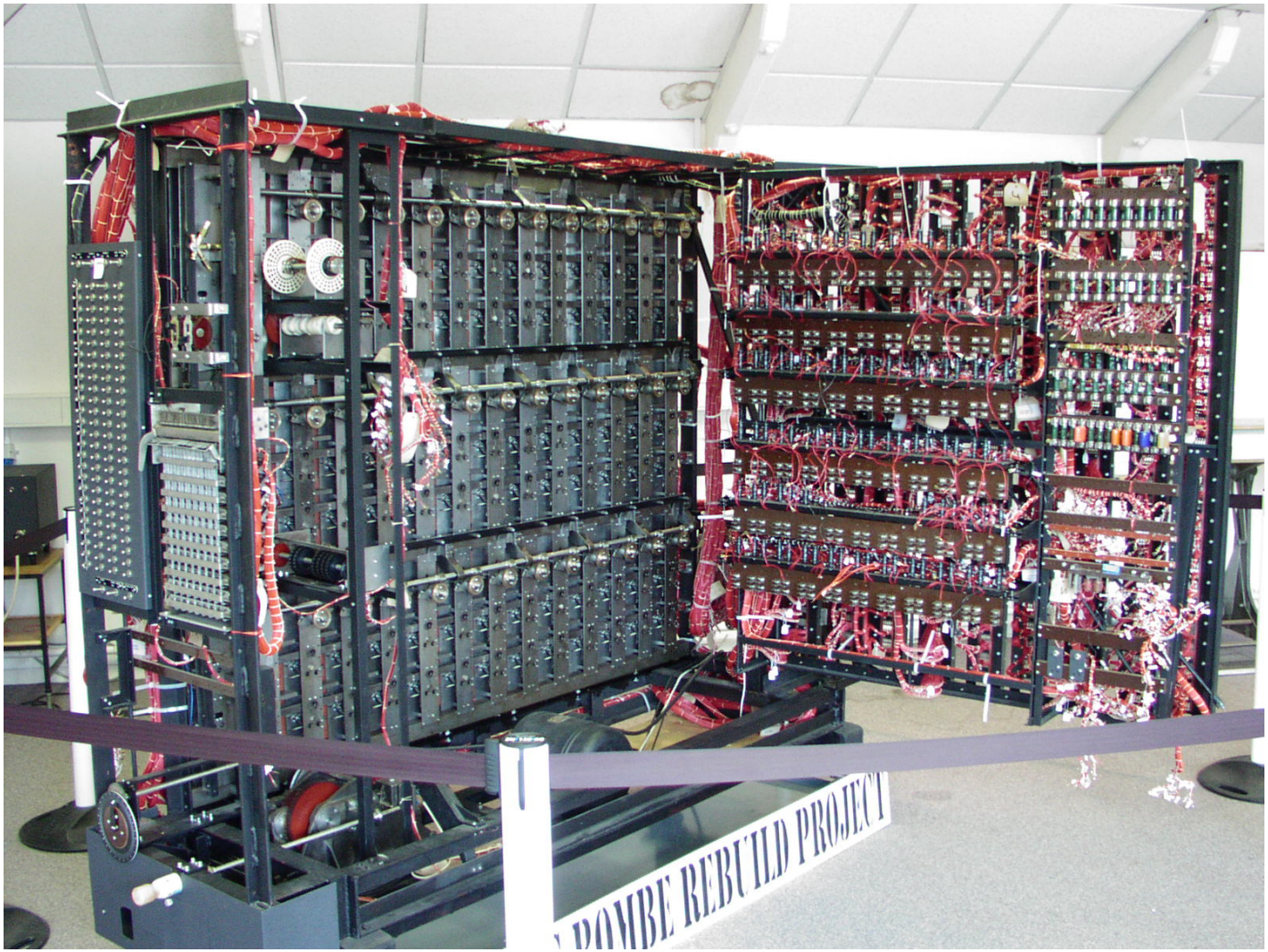
Enigma e *Bombe*

- *Enigma:* uma família de máquinas de ciframento eletro-mecânicas alemãs usada comercialmente desde ∼1920
- Versões mais sofisticadas adotadas pelas forças armadas alemãs na época nazista
- 1932: o serviço de criptoanálise polonês estabeleceu uma técnica e construiu um equipamento (*Bomba*) para deciframento de mensagens da versão mais simples da *Enigma*
- 1939: a técnica e o equipamento poloneses foram transferidos para os serviços de inteligência francês e britânico
- Turing estabeleceu os princípios para quebra da versão mais complexa da *Enigma*
- Turing e G. Welchman projetaram a *Bombe* que automatizou uma grande parte do trabalho de deciframento
- 1940: a *Bombe* entrou em funcionamento
- Outros modelos de *Bombe* foram construídos mais tarde na Grã-Bretanha e nos EUA

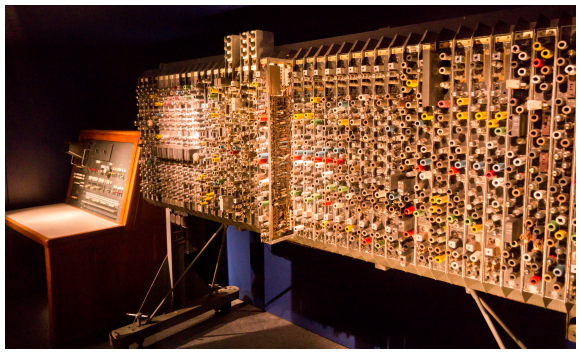


Enigma militar, Wikipedia: *Enigma machine*

Bombe (1939-1940) – réplica, (Prof. C. L. Lucchesi)



Bombe (1939-1940) – réplica, Wikipedia: *Alan Turing*



Pilot ACE (1946-1950), Wikipedia: *Automatic Computing Engine*

John von Neumann (1903-1957)

Wikipedia: *John von Neumann*

Biografia resumida de von Neumann

- 1903: nascimento em Budapeste (então Império Austro-Húngaro)
- 1926: engenheiro químico (ETH, Suíça) e doutor em matemática (Budapeste)
- 1927-1930: *Privatdozent* (Berlim e Hamburgo)
- 1930-1933: professor visitante na Universidade de Princeton
- 1933-1957: professor do Instituto de Estudo Avançado de Princeton (um dos cinco membros iniciais, incluindo Albert Einstein)
- 1940-1957: consultor do Laboratório de Pesquisas Balísticas de Aberdeen
- 1943-1955: consultor do Laboratório Científico de Los Alamos (*Projeto Manhattan*) – primeiro contato com *ENIAC*
- 1944-1945: projeto *EDVAC* (com Eckert, Mauchly, Goldstine e outros)
- 1945-1957: diretor do projeto do computador do IAS baseado no *EDVAC*
- 1952-1957: consultor da Comissão de Energia Atômica dos EUA
- 1957: falecimento em Washington, DC, de câncer, aos 53 anos

Contribuições de von Neumann

- Física quântica
- Análise funcional
- Teoria dos conjuntos
- Hidrodinâmica
- Análise numérica
- Economia, teoria dos jogos
- Meteorologia
- Estatística
- Lógica matemática
- Eletrônica
- Computação

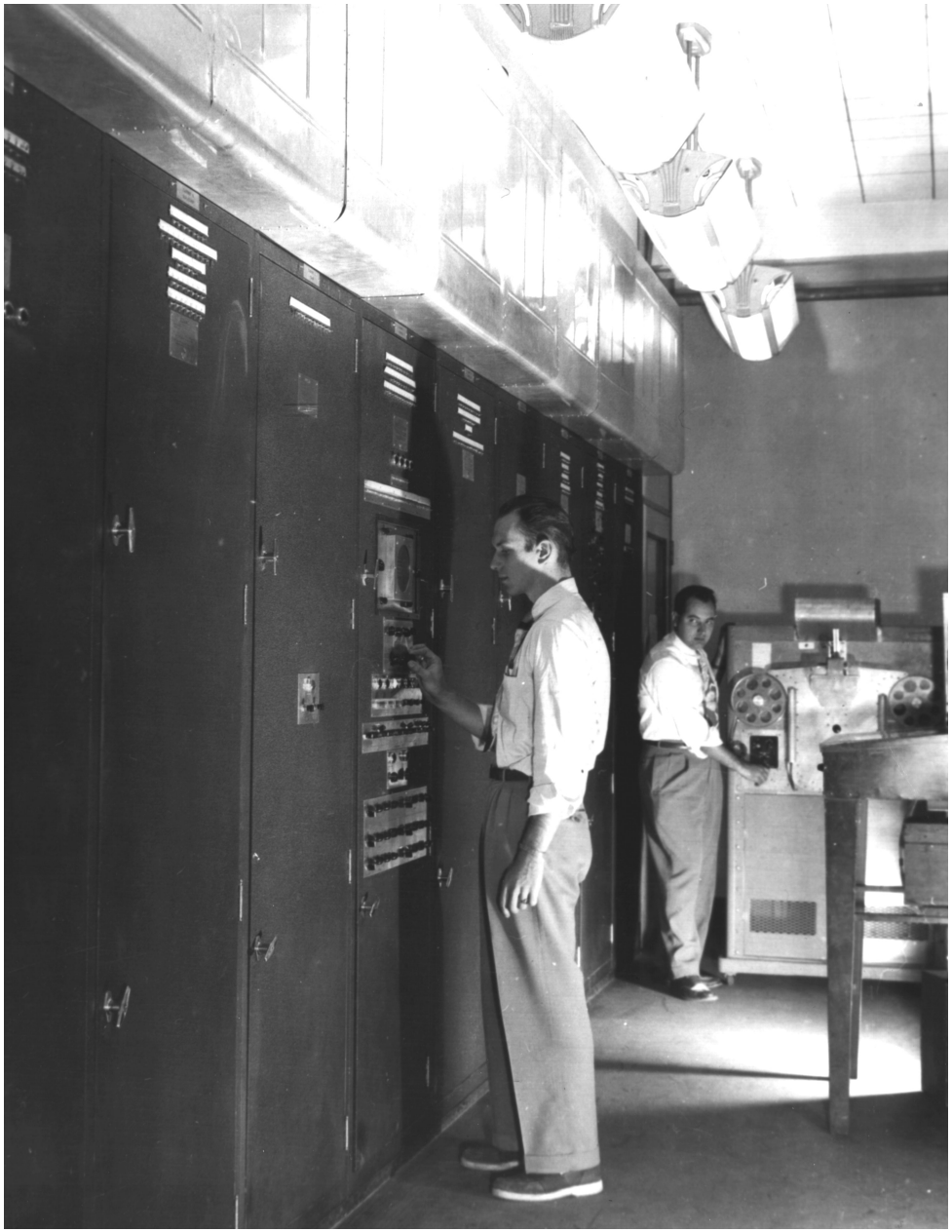
(Seminário *A Obra e o Legado de John von Neumann*, organizado pelo Instituto de Estudos Avançados da USP e pela Academia Brasileira de Ciências, no dia 14 de novembro de 1995, no IME/USP.)

Contribuições de von Neumann à Computação

- Arquitetura (projetos *EDVAC* e *IAS*)
- Provavelmente o primeiro programa de computador (1945) para ordenação de vetores – *merge-sort* – e sua análise de eficiência: $n \log n$ (trabalho analisado posteriormente por D. Knuth)
- Técnicas de programação
- Asserções indutivas e provas de correção de programas
- Análise de algoritmos
- Teoria dos autômatos, autômatos auto-replicadores
- Confiabilidade, tolerância a falhas, redundância
- Aplicações numéricas

Projeto do EDVAC: Eckert, Mauchly e von Neumann

- Unidades: controle, aritmética, memória, E/S
- Memória: linhas de atraso acústico de mercúrio (8.196 palavras de 32 bits) – equivalente a 32 kBytes
- Representação binária, ponto fixo, complemento de 2
- Processamento serial
- Instruções e dados armazenados na memória
- Instruções: carga, armazenamento, operações aritméticas, desvios condicionais e incondicionais
- Instruções projetadas com um endreço vs implementação com quatro endereços (discussão RISC vs. CISC ?)
- Cerca de 3.000 válvulas eletrônicas (ENIAC usou mais de 17.000, para uma memória de 200 dígitos decimais)
- von Neumann: *First Draft of a Report on the EDVAC* (1945) de grande impacto (circulação informal) – deu origem ao termo arquitetura de von Neumann
- Primeiras técnicas de programação
- Controvérsias



EDVAC (1944-1951), Wikipedia: *EDVAC*

Válvulas eletrônicas, Wikipedia: *Vacuum tube*

Caminhos cruzados

- Ambos demonstraram muito cedo habilidades matemáticas
- Leitura de um livro de von Neumann sobre mecânica quântica, em 1932, foi importante para Turing em seus estudos de alguns assuntos correntes em matemática e lógica
- Em 1934, von Neumann visitou Cambridge e ministrou um curso sobre teoria dos grupos
- Turing publicou, em 1935, um artigo que estendeu um resultado de 1934 de von Neumann nesta área
- Turing passou dois anos em Princeton (1936-1938) sob a orientação de Alonzo Church
- von Neumann teve alguma interação com Turing e chegou a sugerir um assunto de pesquisa na área de teoria dos grupos
- von Neumann conhecia o trabalho de Turing e a ideia de máquina universal, análogo teórico de programa armazenado na memória
- von Neumann escreveu a recomendação para prorrogar a bolsa de Turing em Princeton

(cont)

Caminhos cruzados (cont.)

- Turing recusou o convite de von Neumann para ficar no IAS como seu assistente de pesquisa, voltando à Grã-Bretanha
- O trabalho de von Neumann (1951) sobre teoria dos autômatos frisou a importância da máquina universal de Turing
- Ambos tinham interesse em mecânica quântica
- Ambos deixaram trabalhos inacabados ligados à Biologia
- Ambos, apesar de formação muito teórica, tinham interesse muito forte em aplicações
- Ambos aprenderam noções de eletrônica e de eletro-mecânica para projetar suas máquinas
- Ambos participaram ativamente do esforço de guerra contra a Alemanha nazista
- Ambos fizeram contribuições fundamentais à Computação
- Prêmio Turing da ACM, Medalha John von Neumann da IEEE e Prêmio John von Neumann da INFORMS
- Ambos faleceram prematuramente

Controvérsia famosa: programa armazenado na memória

- Babbage (?)
- Gödel, Church
- Turing
- Eckert e Mauchly
- von Neumann
- ...

Minha opinião:

- Turing: ideia abstrata usada na sua máquina universal para obtenção de resultados teóricos, sem vislumbrar aplicações futuras
- Eckert e Mauchly: substituto para programas externos, separado dos dados, a fim de facilitar a programação e execução
- von Neumann: programa armazenado na mesma memória dos dados e parcialmente modificável, facilitando várias técnicas de programação como indexação, tornando viável uso de linguagens simbólicas (montagem e compilação)
- von Neumann reconheceu a importância fundamental das ideias de Turing mas não explicitou contribuição à ideia de programa armazenado
- Artigo de M. Y. Vardi na revista *Comm. ACM* (Jan. 2013): "Who Begat Computing?"

Contrastes

Turing:

- nasceu numa família de origem aristocrática mas empobrecida
- pai era funcionário colonial na Índia
- desde infância educado longe da família
- ambiente escolar pouco propício para ciências
- reservado, introvertido
- educado como anglicano, tornou-se ateu
- nenhuma atividade política ou ideológica, inclinação pacifista
- não demonstrava ambição pela fama ou riqueza
- pouco reconhecimento em vida
- homossexual, vida reprimida, morte trágica

(cont.)

Contrastes (cont.)

von Neumann:

- nasceu numa família rica de origem judaica; pai banqueiro
- família recebeu título de nobreza do imperador austro-húngaro
- educação muito cuidadosa, humanística e científica
- matemático famoso antes de enveredar pela computação
- homenagens e cargos importantes
- liberal, anti-comunista, mas crítico do maccarthismo
- muito social, extrovertido
- ateu (controvérsias sobre sua suposta conversão ao catolicismo)
- *bon vivant*, gostava de companhia feminina, casado duas vezes
- morreu prematuramente de câncer

FIM

Obrigado!