

アラン・チューリング

チューリングマシンと
コンピューターの歴史

第46回 関西蔵前 懇話会 [Sep. 14 2017]

蔵前-大阪支部 黒岩 學而(くろいわ がくじ)

アラン・チューリング

チューリングマシンと コンピューターの歴史

チューリングマシン

チューリングにより1936年の論文「計算可能な数について」で公表された。
計算モデルのひとつで、計算機を数学的に議論するための単純化・理想化された**仮想機械**

- 無限に長いテープ (テープはマス目に区切られていて、1マスに1文字書くことができる)
- その中に格納された情報を読み書きする (ヘッドは双方向に移動できる)
- 機械の内部状態を記憶するメモリ

で構成され、内部状態とヘッドから読み出した情報の組み合わせに応じて、次の動作を実行する。

- ヘッド位置のテープに情報を書き込む
- 機械の内部状態を変える
- ヘッドを右か左に一つ移動する

上の動作を、機械は内部状態が停止状態になるまで反復して実行し続ける

加算のチューリングマシン

3+2の例

テープの6区画を使って、二つの整数を空白($_$)で区切って
111_11と書き込みます。
111_11を読み取り111111に置き換える。

〈手順〉

1. 1のつながりを分離する空白記号($_$)を見つけたら、それを1で置き換える。
2. 右端の1を見つけたら、それを空白で置き換える

〈加算を行うチューリングマシン〉

状態1 : 1, P1, R, →状態1

状態1 : $_$, P1, R, →状態2

状態2 : 1, P1, R, →状態2 **この機械は足し算しかできない : 専用マシン**

状態2 : $_$, P $_$, L, →状態3

状態3 : 1, P $_$, N, →状態4

状態4 : 終わり

乗算のチューリングマシン

4X2の例

テープ上に1111X11と書き込む
Xの右側の数だけ、Xの左側の塊(1111)を書けばよい。

左端を認識するためにまず左端に*を印字する

Xの右側の数を数える

① 右端の1を認識するまでヘッドを右に動かす、その間の記号は読み飛ばす。手順上は読み取った記号をそのマス目に書き込む。

② 右端の1を見つけたらそれを空白で置き換える。

Xの左側の数を数える

① Xの左側の1を1つAに書き換え、*の左側に1を印字する。Aに置き換えられた1を数えたことになる。

② Xの位置を求めXの左側のAに置き換わっていない1を1つAに書き換え、*の左側に1を印字することを全ての1が置き換わるまで繰り返す。この状態で*の左が4と認識される。

③ Xの左側のAを全て1に戻す。

④ 右端の空白を読み取る。2→②へ。Xの右側に1がある限り2,3を繰り返す。Xの右側の1がなくなったら掛算は終わったので4へ。

この時点で*の左側に結果が出ている。*と*の右側のすべての文字を消せばよい。

〈掛算を行うチューリングマシン〉

状態1: 1, P1, L →状態2		状態8: 1, P1, R →状態8	
状態2: $_$, P*, R →状態3	* 1111X11	状態8: A, PA, R →状態8	
状態3: $_$, P $_$, L →状態4		状態8: X, PX, L →状態6	
状態3: *, P*, R →状態3		状態8: *, P*, R →状態8	
状態3: 1, P1, R →状態3		状態9: $_$, P $_$, L →状態4	1111 * 1111X1
状態3: X, PX, R →状態3		状態9: 1, P1, R →状態9	
状態3: A, PA, R →状態3		状態9: X, PX, R →状態9	
状態4: 1, P $_$, L →状態5	* 1111X1	状態9: A, P1, R →状態9	1111 * 1AAAX1
状態4: X, PX, L →状態10	11111111 * 1111X	状態10: *, P $_$, R →状態11	11111111 *
状態5: 1, P1, L →状態5		状態10: 1, P1, L →状態10	
状態5: X, PX, L →状態5		状態11: $_$, P $_$, N →状態12	11111111
状態6: *, P*, R →状態9		状態11: 1, P $_$, R →状態11	
状態6: 1, PA, L →状態7	* 111AX1	状態11: X, P $_$, R →状態11	11111111 * 1111
状態6: A, PA, L →状態6		状態11: A, P $_$, R →状態11	
状態7: $_$, P1, R →状態8	1 * 111AX1	状態12: 終わり	
状態7: *, P*, L →状態7			
状態7: 1, P1, L →状態7			

この機械は掛け算しかできない : 専用マシン

論文「計算可能数ならびにその決定問題への応用」

- ニューマンが講義する数学基礎論を受講していた。
- その中でヒルベルトの決定問題の講義を受けて、チューリングは「厳密に機械的な手順では解決できない、数学的な問題が存在する」という直感を持った。ニューマンは数学的手順はすべて機械がこなせると学生たちに説いた。
- 決定問題の証明のためチューリングマシンを考案した。

万能チューリング・マシン

チューリング・マシンMのコード: 入力

足し算専用のマシンのコードと入力データを一緒にチューリングのテープ上に書込む

足し算専用のマシンの動作をまねる専用のチューリングマシンを作った

そのためには、どのような手順でやればできるか手順を明確にする

状態1: 1, P1, R, →状態1; 状態1: , P1, R, →状態2; 状態2: 1, P1, R, →状態2;
.....; 状態4: 終わり:: 111+11 :::

状態1: 1, P1, R, →状態1; 状態1: , P1, R, →状態2; 状態2: 1, P1, R, →状態2;
.....; 状態4: 終わり:: H11+11 ::: 状態1:

状態1: 1, P1, R, →状態1; 状態1: , P1, R, →状態2; 状態2: 1, P1, R, →状態2;
.....; 状態4: 終わり:: 1H1+11 ::: 状態1: 1, ; 状態2: 1,

手順が明確になればチューリングマシンを作れる

足し算専用のマシンの動作をまねる専用のチューリングマシンのコード部分を掛け算専用のマシンのコード変えれば

このマシンは掛け算もできる。すなはち万能のマシンを作ったことになる

ヒルベルトの決定問題の証明

- 「停止するか、永遠に止まらずに動き続けるか」を判定できるチューリング・マシンをHとする。Hは、入力されたチューリング・マシンMの実行が終わるなら「YES」、終わらないなら「NO」を出力する。このようなHが存在すると仮定する。
- ここで、Hを少し変更して、入力されたMの実行が終わるなら止まらない、終わらないなら「NO」を出力して止まる、チューリング・マシンH'を作る。(無限ループにすればよい) このH'にH'を入力すると、H'の実行が終わるなら止まらない、H'の実行が終わらないなら「NO」を出力して止まる。矛盾が生じる。
- ゆえに「停止判定チューリング・マシンは作れない」

コンピューターの歴史(1)

1903.12.28		フォン・ノイマン。ハンガリーに生まれる
1912.6.23	アラン・チューリング、ロンドンで生まれる	
1931		ノイマン、プリンストン大学の教授
1931-34	ケンブリッジ大学キングス・カレッジ学部生	
1935	キングス・カレッジ特別研究員	
1936	論文「計算可能な数について」でチューリング・マシン提唱	
1936-38	プリンストン大学で論理学、算術、数論を学び博士号	
1938-39	ケンブリッジ大学に戻り、ドイツ軍のエニグマ暗号解読に着手	
1939.9.3		第二次世界大戦開始
1940	ボンプ稼働	ロンドン空襲
1941	海軍エニグマ解読	
1942	アメリカに再度渡る。タニーの暗号解読開始	
1943	電子工学を学ぶ。	アメリカでボンプ稼働 ENIACの設計開始
1944	コロッサス稼働。	ルマンディー上陸作戦
1945	国立物理学研究院。ドイツ降伏	ノイマンEDVAC開発に参加
		広島、長崎原爆投下
1946	ウィリアムス管	

エニグマ

- 第二次世界大戦の時にナチス・ドイツが用いていたことで有名なローター式暗号機のこと。幾つかの型がある。エニグマ暗号機は、1918年にドイツの発明家アルトウール・シエルビウスによって発明された電気機械式暗号機械で、1925年にはドイツ軍が正式採用し約3万台が軍用として使用された。
- 大戦中に連合国側はエニグマ解読に成功したが、その事実は徹底して秘密にされ、ドイツ軍は終戦までエニグマを使用し続けた。

エニグマ換字の原理

ローターは、その内部配線により26!通りの中から所望の単文字換字表を一つだけ設定することができる。1文字換字する度にローターを駆動させ多表を頭から順繰りに切り替えていく。三つのローターを連結して3回換字することで見かけ上、 $26^3=17,576$ 表を利用できる。またローターを連結する順序を変えることにより、異なる多表を用意できる。17,576表が6倍の105,456表に増える。

ボンブ

エニグマには、その暗号化方法に特有の癖があり、それを利用し暗号文と、それを解読した平文の組み合わせを作り、ボンブに入力する。

ボンブには108個の回転ドラムが付いていて、「エニグマ」のローターと同じ動作をする。エニグマにはローターが3枚あるので、1台のボンブは36台のエニグマと同じ性能を持つ。

ボンブは、モーターでドラムを自動的に回転させながら、平文を暗号化し、暗号文と比較し、一致すると停止する。

つまり、しらみつぶしに「暗号を作るためのローター位置」を探し出す装置である。

タニー

- タニーはエニグマより技術的にも進歩しており、理論的にも安全性が高く、最高の極秘情報のみを扱った。エニグマは戦争開始前より古い技術になっていた。送受信に3人ずつオペレーターが6人もの必要だが、タニーは双方で一人でよい。
- タニーで暗号化された電文は、国際テレプリンターの5桁の二進コードで表現されていた。12のローターを使って5桁の二進数を2つ作成して加える。加算式の暗号機である。
- ティルトマンとタットの努力により機械の動作が明らかになり、チューリングが毎日の暗号文を解読するための方式を考えた。

コロッサス

- ドイツ軍はエニグマより強力な暗号機である「ゲハイムシュライバー」を開発し、これを解読するコンピューター「コロッサス」を、技術者トミー・フラワーズを中心としたチームが設計した。
- 戦争が終わるまでに10台の Colossus が製造された。
- コロッサスは2進数を使用した電子式で、真空管1,500本を使用していた。暗号解読以外にもある程度汎用の計算も行なえるようになっていた。しかし、機密保持のため、ハードウェアと設計図はほとんど破棄され、1970年代まで機密が保持された。

ENIAC

Electronic Numerical Integrator and Computer

- アメリカで開発された黎明期の電子計算機(コンピュータ)。チューリング完全でデジタル式だがプログラム内蔵方式とするにはプログラムのためのメモリがごくわずかで、パッチパネルによるプログラミングは煩雑ではあったものの、必ずしも専用計算機ではなく広範囲の計算問題を解くことができた。
- ENIACはアメリカ陸軍の弾道研究室での砲撃射表の計算向けに設計された。1946年に発表されたとき、報道では「巨大頭脳」(Giant Brain)と称された。当時の電気機械式計算機に比べて千倍の計算速度だった。その演算能力と汎用プログラム能力に科学者や実業家は興奮した。
- ENIACを考案・設計したのはペンシルベニア大学のジョン・モークリーとジョン・エッカートである。
- ENIACは17,468本の真空管、7,200個のダイオード、1,500個のリレー、70,000個の抵抗器、10,000個のコンデンサ等で構成されていた。
- 現在のコンピュータは二進法で計算を行うものがほとんどだが、ENIACは内部構造に十進法を採用した。

EDVAC

Electronic Discrete Variable Automatic Computer

- ENIACを開発したジョン・モークリーとジョン・エッカートはENIACがまともに動作するようになる前の1944年8月、EDVACの設計と構築を提案した。その設計はENIAC構築中に考案された多くの重要なアーキテクチャ上または論理上の改良を取り入れるもので、高速な遅延記憶装置を採用することになっていた。ENIACと同様、EDVACはペンシルベニア大学が米陸軍のアーバディーン実験場にある弾道学研究室のために製作した。エッカートとモークリーを含むENIAC設計者らはコンサルタントという立場のジョン・フォン・ノイマンと合流して設計を開始した。1945年、フォン・ノイマンは論理設計について話し合った結果をFirst Draft of a Report on the EDVACという草稿にまとめた。
- 開発されたコンピュータは二進数を使用し、加算、減算、乗算、プログラムによる除算などが可能で、メモリは遅延記憶装置(水銀遅延管)で1000ワード(後に1024ワードに拡張)であった(1ワードは44ビット)。
- モークリーとエッカートはノイマンが単独で草稿を発表したことに反発し、開発メンバーから離脱した。主要メンバーが離脱したEDVAC開発は大きく遅れ、世界初の実用的に稼働したプログラム内蔵方式コンピュータは1949年のEDSACとなってしまった。EDVACは1951年に完成する。

フォン・ノイマン型コンピュータの特徴

これではENIACの開発者モークリーとエッカート達はへそを曲げて当然
ノイマンがモークリーとエッカートに見せる前に第3者が皆にばらまいた。

1. 中央演算/制御装置 ENIAC
2. アドレス付記憶装置 ENIAC
3. 入力/出力装置 ENIAC
4. データとプログラムの区別をしない記憶
プログラムを変えれば汎用のコンピュータができる チューリング
5. 逐次処理 ENIAC
6. 二進法の採用 ライフニッツ

ウィリアムス管

- 正確にウィリアムス・キルバーン管は陰極線管による記憶装置で、ブラウン管の一種とすることもある。名前は開発者であるフレディー・ウィリアムスとトム・キルバーンに由来する。戦時中のレーダー表示用ブラウン管の研究・開発が関連しているが、コンピュータの記憶装置用としては1946年-1947年頃発明された。磁気コアメモリが登場する1950年代前半まで用いられていた。
- 陰極線管の蛍光面に電子が衝突すると光が放出される。このとき副作用として衝突箇所の周囲は電荷がわずかに変化する。これを測定することによって陰極線管を単純な記憶装置として使用することが可能になる。電荷はすぐに失われるため繰り返し電子を衝突させることが必要であり、記憶保持動作が必要ないわゆる

コンピューターの歴史(2)

- 1947 ニューラルネットと人工知能のプログラムを開発し、一般向け講演
- 1948 マンチェスター大学に移籍。6月にベビー-ACEが初の蓄積プログラム実行
- 1950 チューリング・テスト提唱
- 1951 王立協会特別研究員。生物の成長に関する理論研究
マンチェスター大学フェランティ・マーク I (最初の商用万能チューリング・マシン)
UNIVAC発売
- 1952 ホモセクシャルを理由に逮捕。政府の機密関係から遮断される
- 1953 マンチェスター大学特別講師 ワトソンとクリックがDNAの構造解明
- 1954 **ビキニ環礁で水爆実験(第5福竜丸)**
- 1954.6.7 アラン・チューリング青酸中毒死(41才)
- 1964 IBMが360シリーズ発売
- 1966 ACM(計算機科学の国際学会)がチューリング賞創設
- 1974 コロサスの存在が公になる
- 1974 アップルコンピュータ設立
- 1997 IBMのディー・フブルー世界チャンピオン
- 2000 ターの秘密文書公開
- 2009 イギリス首相がチューリングに正式謝罪

プリンストン高等研究所 (Institute for Advanced Study) 電子計算機で取り組まれた主要な問題(1946-1958)

恒星の進化

生物の進化

1943年バリチェリ「進化する生命体の数値モデル」で認められIASに招聘される。デジタル計算の力を進化に適用した。

気象学

1946年に、ノイマンは数値天気予報の問題解決のため気象学者を採用した(水爆に関する研究をうまく覆い隠せた)

衝撃波

反射衝撃波のノイマンの理論は爆弾の効果を最大化するために利用された。

核爆発

1946年ロスアラモスの水爆の問題を1か月以上ENIACで計算。

1951年大規模な熱核爆弾関連の計算が60日間行った。

ACE

Automatic Computing Engine

- 1946年2月19日、チューリングは国立物理学研究所(NPL)運営委員会に世界初のプログラム内蔵式コンピュータの完全な設計に関する論文を提出した。他の同時期のコンピュータと異なりACEはチューリングが単独で設計したもので、EDVACに関するジョン・フォン・ノイマンの草稿の影響を受けていない。
- チューリングは万能チューリングマシンを実現することを目指し、そのうえで人工知能を構築することを目指していた。NPLの数学部門にはコンピュータを実際に製作する能力がなかったため、通信研究所(TRE)に製作を依頼した。しかし、TREは戦後の電話網の復興に忙しく、世論もACE開発には批判的であった。このためチューリングは1947年にNPLを去った。しかし、ACEは国家プロジェクトであったため中止することもできず、ジェームズ・H・ウィルキンソンがプロジェクトを引き継ぎ、ハリー・ハスキーがこれを補佐した。1950年にはプロトタイプのパilot ACEが完成し、1957年にはようやくACEが完成する。しかし、完成したときにはACEはすでに時代遅れとなっていた。

チューリング・テスト

- アラン・チューリングによって考案された、ある機械が知的かどうか(人工知能であるかどうか)を判定するためのテスト。
- アラン・チューリングの1950年の論文、「Computing Machinery and Intelligence」の中で書かれたもので、以下のように行われる。人間の判定者が、一人の(別の)人間と機械に対して通常の言語での会話を行う。このとき人間も機械も人間らしく見えるように対応する。これらの参加者はそれぞれ隔離されている。判定者は、機械の言葉を音声に変換する能力に左右されることなく、その知性を判定するために、会話はたとえばキーボードとディスプレイのみといった、文字のみでの交信に制限しておく。判定者が、機械と人間との確実な区別ができなかった場合、この機械はテストに合格したことになる。

マンチェスター・マークワン

- 1949年にイギリスのマンチェスター・ビクトリア大学で製作された。Manchester Automatic Digital Machine (MADM)とも呼ばれる。1948年8月に開発が始まり、1949年4月に稼働開始した。メルセンヌ数を探すプログラムがエラーとなることなく9時間動作したのは、1949年6月16日から17日にかけてのことである。このマシンの稼働成功は"electronic brain"(電子頭脳)という呼称を使ってイギリスの報道機関が広く取り上げた。そういった扱いにマンチェスター大学の神経外科部門のトップが反応を示し、電子計算機は真の創造性を獲得することができるのか、という長い議論が始まることになった。
- 当初 Mark 1 は大学内の計算資源を提供するために開発され、研究者らにコンピュータの利用を体験させる役に立ったが、まもなくフェランティが商用版を設計する際のプロトタイプとして利用されることになった。開発は1949年末に終り、1950年末にはマシンが廃棄され、1951年2月には世界初の商用汎用電子計算機 Ferranti Mark 1 に置き換えられた。
- 歴史上重要な特徴として、初めて一種のインデックスレジスタをアーキテクチャ上採用し、メモリ上のワードの配列を順次アクセスするプログラムを容易に書けるようになった。このマシンを開発したことで34件の特許が成立し、設計上のアイデアはその後の商用機である IBM 701/702 や Ferranti Mark 1 に取り入れられた。

UNIVAC I

Universal Automatic Computer

- 世界初の商用コンピュータ。1950年に完成し、1951年にレミントンランド社(現Unisys)が発売。初の事務処理用途のコンピュータでもある。
 - ENIACと比較して真空管の本数は3分の1以下の5200本。メモリには100本の水銀遅延管を使用し、10000本のダイオードを搭載していた。重量7.2トン。入出力装置には、初めて磁気テープが搭載されプログラム内蔵方式で、1秒間に10万回の加算が可能だった。
 - ENIACを開発したモークリーとエッカートt)が設立したエッカート・モークリ社で開発が開始された。しかし、資金不足に陥り、IBMからは資金援助を断られ、1950年にレミントンランド社が買収し、発売にこぎつける。1号機は国勢調査局に納入された。
-