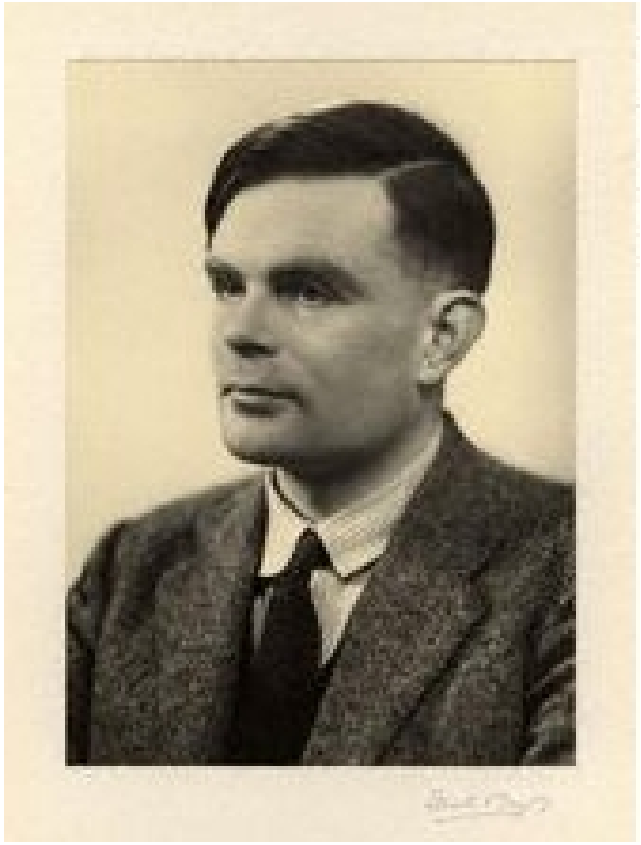
Alan Turing: l'enigma



Fellow della Royal Society, 29 marzo 1951

Lucidi utilizzati per la conferenza per l'Associazione Ligure per l'Insegnamento della MAtematica, proposta da G. Rosolini, DISI, Università di Genova
Si suggerisce di leggere questo testo senza stamparlo, in quanto ci sono alcune pagine in parte ripetute per ottenere opportuni effetti visivi.
Inoltre vi sono link attivi colorati in verde che si riferiscono direttamente a siti in rete, mentre quelli colorati in blu si riferiscono ad altre pagine nel testo,
I punti rossi • rimandano alla pagina principale.

- La macchina universale

  On Computable Numbers, with an application to the Entscheidungsproblem

  Proc. Lond. Math. Soc. 42 pp.230-265 (1936-7)

  correzioni ibid. 43, pp.544-546 (1937)

  http://www.abelard.org/turpap2/turpap2.htm

  http://www-csli.stanford.edu/hp/Logic-software.html

- La decrittazione di Enigma

  Mathematical theory of ENIGMA machine

  Bletchey Park, 1940

  http://www.turing.org.uk/

  http://www.xat.nl/enigma/

- Il gioco d'imitazione

  Computing Machinery and Intelligence

  Mind 49, pp.433-460 (1950)

  http://www.abelard.org/turpap/turpap.htm

  http://www.loebner.net/Prizef/TuringArticle.html

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means.

Although the subject of this paper is ostensibly the computable numbers, it is almost equally easy to define and investigate computable functions of an integral variable or a real computable variable, computable predicates, and so forth.

The fundamental problems involved are, however, the same in each case, and I have chosen the computable numbers for explicit treatment as involving the least cumbrous technique.

I hope shortly to give an account of the relations of the computable numbers, functions, and so forth to one another. This will include a development of the theory of functions of a real variable expressed in terms of computable numbers.

According to my definition, a number is computable if its decimal can be written down by a machine.

I numeri "calcolabili" possono essere descritti in breve come quei numeri reali la cui espressione decimale è calcolabile con strumenti finiti.

Sebbene l'argomento di questo lavoro siano esplicitamente i numeri calcolabili, è quasi altrettanto facile definire e studiare le funzioni calcolabili di variabile intera o di variabile reale calcolabile, i predicati calcolabili, e così via.

I problemi fondamentali sono, comunque, gli stessi in ogni caso, ed ho scelto i numeri calcolabili per una trattazione esplicita perchè richiedono la tecnica meno complicata.

Spero di trattare nel prossimo futuro le relazioni che intercorrono tra numeri calcolabili, funzioni e via di seguito. Questo includerà lo sviluppo della teoria delle funzioni di una variabile reale espresse in termini dei numeri calcolabili.

Nella mia definizione, un numero è calcolabile se la sua parte decimale può essere scritta da una macchina.

Computing machines

. . . For the present I shall only say that the justification lies in the fact that the human memory is necessarily limited.

We may compare a man in the process of computing a real number to a machine which is only capable of a finite number of conditions $q_1, q_2, \ldots, q_R$ which will be called "m-configurations".

The machine is supplied with a "tape", (the analogue of paper) running through it, and divided into sections (called "squares") each capable of bearing a "symbol".

At any moment there is just one square, say the r-th, bearing the symbol $S(r)$ which is "in the machine".

We may call this square the "scanned square". The symbol on the scanned square may be called the "scanned symbol".

The "scanned symbol" is the only one of which the machine is, so to speak, "directly aware".

Le macchine che calcolano

. . . Per il momento, dirò soltanto che la giustificazione sta nel fatto che la memoria umana è necessariamente finita.

Possiamo paragonare un uomo nell'atto di calcolare un numero reale a una macchina che è in grado di considerare soltanto un numero finito di condizioni $q_1, q_2, \ldots, q_R$ che chiameremo "configurazioni-macchina".

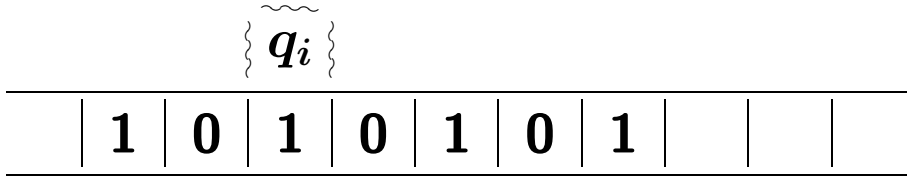
La macchina è provvista di un "nastro", (l'analogo della carta) che scorre attraverso di essa ed è diviso in sezioni (chiamate "quadrati") ciascuna in grado di riportare un "simbolo".

In ogni istante c'è esattamente un quadrato, diciamo l'r-esimo, che riporta il simbolo $S(r)$ che è "all'interno della macchina".

Possiamo chiamare questo il "quadrato in lettura". Il simbolo nel quadrato in lettura può venir chiamato il "simbolo in lettura".

Il "simbolo in lettura" è l'unico di cui la macchina sia, per così dire, "direttamente cosciente".

Computing machines



$$S(r) = 1$$

Le macchine che calcolano

... Per il momento, dirò soltanto che la giustificazione sta nel fatto che la memoria umana è necessariamente finita.

Possiamo paragonare un uomo nell'atto di calcolare un numero reale a una macchina che è in grado di considerare soltanto un numero finito di condizioni $q_1, q_2, \ldots, q_R$ che chiameremo "configurazioni-macchina".

La macchina è provvista di un "nastro", (l'analogo della carta) che scorre attraverso di essa ed è diviso in sezioni (chiamate "quadrati") ciascuna in grado di riportare un "simbolo".

In ogni istante c'è esattamente un quadrato, diciamo l'r-esimo, che riporta il simbolo $S(r)$ che è "all'interno della macchina".

Possiamo chiamare questo il "quadrato in lettura". Il simbolo nel quadrato in lettura può venir chiamato il "simbolo in lettura".

Il "simbolo in lettura" è l'unico di cui la macchina sia, per così dire, "direttamente cosciente".

The possible behaviour of the machine at any moment is determined by the m-configuration q_n and the scanned symbol $S(r)$. This pair $q_n, S(r)$ will be called the "configuration": thus the configuration determines the possible behaviour of the machine.

In some of the configurations in which the scanned square is blank (*i.e.* bears no symbol) the machine writes down a new symbol on the scanned square: in other configurations it erases the scanned symbol.

The machine may also change the square which is being scanned, but only by shifting it one place to right or left.

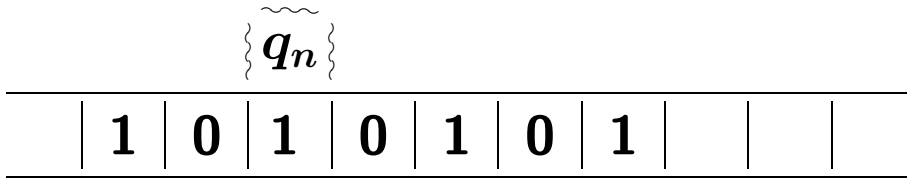
In addition to any of these operations the m-configuration may be changed.

Il comportamento possibile della macchina ad ogni istante è determinato dalla configurazione-macchina q_n e dal simbolo in lettura $S(r)$. Questa coppia $q_n, S(r)$ sarà chiamata "configurazione": in altre parole, la configurazione determina il comportamento della macchina.

In configurazioni in cui il quadrato in lettura è non scritto (cioè non riporta nessun simbolo) la macchina può scrivere un simbolo nel quadrato in lettura, in altre configurazioni può cancellare il simbolo in lettura [o scriverne un altro].

La macchina può anche cambiare il quadrato in lettura, ma soltanto spostandolo di un posto a destra o a sinistra.

In aggiunta a queste operazioni, la configurazione-macchina può essere cambiata.



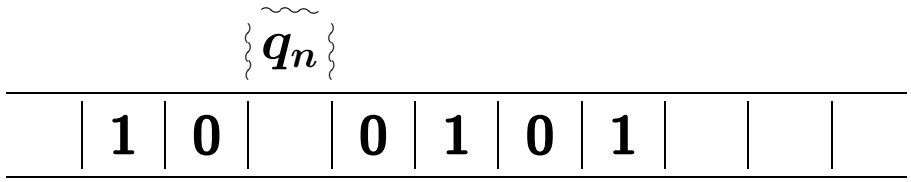
Il comportamento possibile della macchina ad ogni istante è determinato dalla configurazione-macchina q_n e dal simbolo in lettura $S(r)$. Questa coppia $q_n, S(r)$ sarà chiamata "configurazione": in altre parole, la configurazione determina il comportamento della macchina.

In configurazioni in cui il quadrato in lettura è non scritto (cioè non riporta nessun simbolo) la macchina può scrivere un simbolo nel quadrato in lettura, in altre configurazioni può cancellare il simbolo in lettura [o scriverne un altro].

La macchina può anche cambiare il quadrato in lettura, ma soltanto spostandolo di un posto a destra o a sinistra.

In aggiunta a queste operazioni, la configurazione-macchina può essere cambiata.

configurazione		comportamento		
stato	lettura			



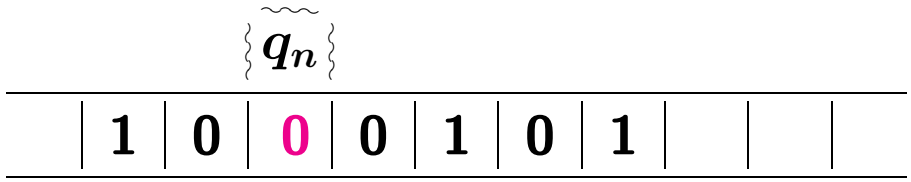
Il comportamento possibile della macchina ad ogni istante è determinato dalla configurazione-macchina q_n e dal simbolo in lettura $S(r)$. Questa coppia $q_n, S(r)$ sarà chiamata "configurazione": in altre parole, la configurazione determina il comportamento della macchina.

In configurazioni in cui il quadrato in lettura è non scritto (cioè non riporta nessun simbolo) la macchina può scrivere un simbolo nel quadrato in lettura, in altre configurazioni può cancellare il simbolo in lettura [o scriverne un altro].

La macchina può anche cambiare il quadrato in lettura, ma soltanto spostandolo di un posto a destra o a sinistra.

In aggiunta a queste operazioni, la configurazione-macchina può essere cambiata.

configurazione		comportamento		
stato	lettura	scrittura		



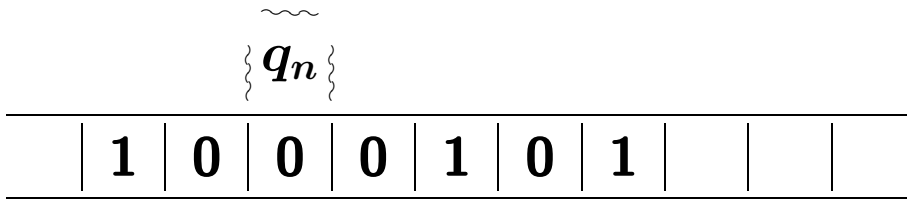
Il comportamento possibile della macchina ad ogni istante è determinato dalla configurazione-macchina q_n e dal simbolo in lettura $S(r)$. Questa coppia $q_n, S(r)$ sarà chiamata "configurazione": in altre parole, la configurazione determina il comportamento della macchina.

In configurazioni in cui il quadrato in lettura è non scritto (cioè non riporta nessun simbolo) la macchina può scrivere un simbolo nel quadrato in lettura, in altre configurazioni può cancellare il simbolo in lettura [o scriverne un altro].

La macchina può anche cambiare il quadrato in lettura, ma soltanto spostandolo di un posto a destra o a sinistra.

In aggiunta a queste operazioni, la configurazione-macchina può essere cambiata.

configurazione		comportamento		
stato	lettura	scrittura		



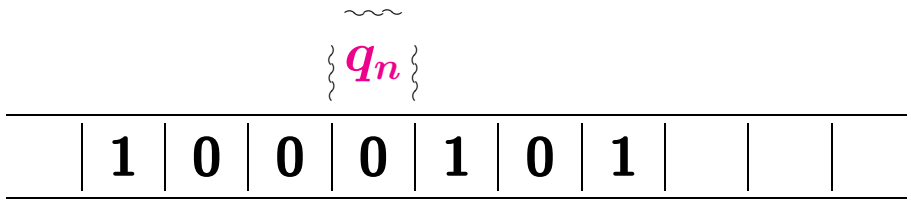
Il comportamento possibile della macchina ad ogni istante è determinato dalla configurazione-macchina q_n e dal simbolo in lettura $S(r)$. Questa coppia $q_n, S(r)$ sarà chiamata "configurazione": in altre parole, la configurazione determina il comportamento della macchina.

In configurazioni in cui il quadrato in lettura è non scritto (cioè non riporta nessun simbolo) la macchina può scrivere un simbolo nel quadrato in lettura, in altre configurazioni può cancellare il simbolo in lettura [o scriverne un altro].

La macchina può anche cambiare il quadrato in lettura, ma soltanto spostandolo di un posto a destra o a sinistra.

In aggiunta a queste operazioni, la configurazione-macchina può essere cambiata.

configurazione		comportamento		
stato	lettura	scrittura		



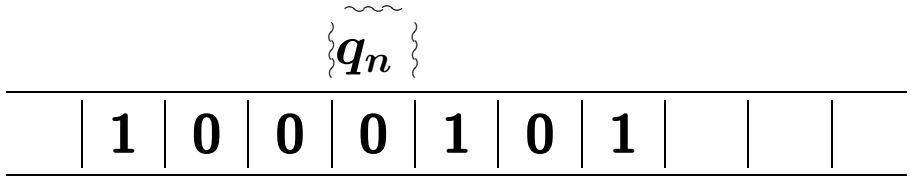
Il comportamento possibile della macchina ad ogni istante è determinato dalla configurazione-macchina q_n e dal simbolo in lettura $S(r)$. Questa coppia $q_n, S(r)$ sarà chiamata "configurazione": in altre parole, la configurazione determina il comportamento della macchina.

In configurazioni in cui il quadrato in lettura è non scritto (cioè non riporta nessun simbolo) la macchina può scrivere un simbolo nel quadrato in lettura, in altre configurazioni può cancellare il simbolo in lettura [o scriverne un altro].

La macchina può anche cambiare il quadrato in lettura, ma soltanto spostandolo di un posto a destra o a sinistra.

In aggiunta a queste operazioni, la configurazione-macchina può essere cambiata.

configurazione		comportamento		
stato	lettura	scrittura	movimento	



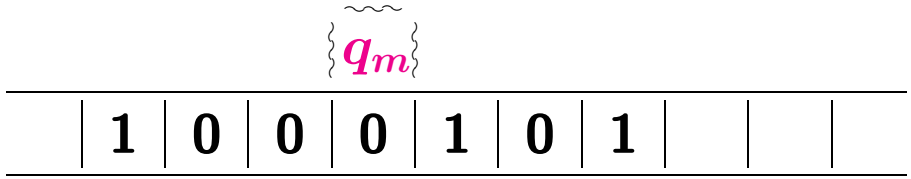
Il comportamento possibile della macchina ad ogni istante è determinato dalla configurazione-macchina q_n e dal simbolo in lettura $S(r)$. Questa coppia $q_n, S(r)$ sarà chiamata "configurazione": in altre parole, la configurazione determina il comportamento della macchina.

In configurazioni in cui il quadrato in lettura è non scritto (cioè non riporta nessun simbolo) la macchina può scrivere un simbolo nel quadrato in lettura, in altre configurazioni può cancellare il simbolo in lettura [o scriverne un altro].

La macchina può anche cambiare il quadrato in lettura, ma soltanto spostandolo di un posto a destra o a sinistra.

In aggiunta a queste operazioni, la configurazione-macchina può essere cambiata.

configurazione		comportamento		
stato	lettura	scrittura	movimento	



Il comportamento possibile della macchina ad ogni istante è determinato dalla configurazione-macchina q_n e dal simbolo in lettura $S(r)$. Questa coppia $q_n, S(r)$ sarà chiamata "configurazione": in altre parole, la configurazione determina il comportamento della macchina.

In configurazioni in cui il quadrato in lettura è non scritto (cioè non riporta nessun simbolo) la macchina può scrivere un simbolo nel quadrato in lettura, in altre configurazioni può cancellare il simbolo in lettura [o scriverne un altro].

La macchina può anche cambiare il quadrato in lettura, ma soltanto spostandolo di un posto a destra o a sinistra.

In aggiunta a queste operazioni, la configurazione-macchina può essere cambiata.

configurazione		comportamento		
stato	lettura	scrittura	movimento	nuovo stato

Esempi

Una macchina per scrivere il numero $\mathbf{.010101010101010\ldots}$

configurazione		comportamento		
stato	lettura	scrittura	movimento	nuovo stato
q_0	.	.	destra	q_0
q_0		0	destra	q_1
q_1		1	destra	q_0

Una macchina per scrivere il numero

$$.\,0101101110111101\underbrace{11111}_{n}0\underbrace{111}_{n+1}\ldots$$

configurazione		comportamento		
stato	lettura	scrittura	movimento	nuovo stato
q_0	.	.	destra	q_0
q_0		0	destra	q_1
q_1		1	destra	q_2
q_2		0	destra	q_3
q_3		1	destra	q_4
q_4		1	destra	q_5
q_5		0	sinistra	q_6
q_6	1	1	sinistra	q_6
q_6	0	0	destra	q_7
q_6	.	1	destra	q_{10}
q_{10}	1	.	destra	q_8
q_{10}	0	0	destra	q_4
q_4	1	1	destra	q_4
q_7	1	.	destra	q_8
q_8	1	1	destra	q_8
q_8	0	0	destra	q_8
q_8		1	sinistra	q_{11}
q_{11}	1	1	sinistra	q_{11}
q_{11}	0	0	sinistra	q_6

Ogni macchina ha una **descrizione standard** come numero decimale:

q_0	.	.	destra	q_0
q_0		0	destra	q_1
q_1		1	destra	q_0

Ogni macchina ha una **descrizione standard** come numero decimale:

q_0	.	.	destra	q_0
q_0		**0**	destra	q_1
q_1		**1**	destra	q_0

La mettiamo in linea:

$$q\mathbf{0}b..dq\mathbf{0}b;q\mathbf{0}b\llcorner\mathbf{0}dq\mathbf{1}b;q\mathbf{1}b\llcorner\mathbf{1}dq\mathbf{0}b;$$

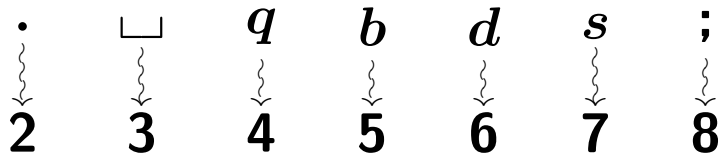
Ogni macchina ha una **descrizione standard** come numero decimale:

q_0	.	.	destra	q_0
q_0		0	destra	q_1
q_1		1	destra	q_0

La mettiamo in linea:

$$q0b..dq0b;q0b\sqcup 0dq1b;q1b\sqcup 1dq0b;$$

Riscriviamo i segni



Ogni macchina ha una **descrizione standard** come numero decimale:

q_0	.	.	destra	q_0
q_0		0	destra	q_1
q_1		1	destra	q_0

La mettiamo in linea:

$$q0b..dq0b;q0b\sqcup 0dq1b;q1b\sqcup 1dq0b;$$

Riscriviamo i segni

.	$\sqcup$	q	b	d	s	;
2	3	4	5	6	7	8

Otteniamo il numero

$$40522640584053064158415316405 8$$

Ogni macchina ha una **descrizione standard** come numero decimale:

q_0	.	.	destra	q_0
q_0		0	destra	q_1
q_1		1	destra	q_0

La mettiamo in linea:

$$q0b..dq0b;q0b␣0dq1b;q1b␣1dq0b;$$

Riscriviamo i segni

.	␣	q	b	d	s	;
2	3	4	5	6	7	8

Otteniamo il numero

$$40522640584053064158415316405 8$$

che possiamo scrivere in notazione binaria

$$\underbrace{1\ldots\ldots\ldots\ldots0}_{98 \text{ cifre}}$$

The universal computing machine

It is possible to invent a single machine which can be used to compute any computable sequence.

If this machine $\mathcal{I}$ is supplied with a tape on the beginning of which is written the standard description of some computing machine $\mathcal{M}$, then $\mathcal{I}$ will compute the same sequence as $\mathcal{M}$.

... The behaviour of the computer at any moment is determined by the symbols which he is observing. and his "state of mind" at that moment.

... Every such operation consists of some change of the physical system consisting of the computer and his tape.

... It is always possible for the computer to break off from his work, to go away and forget all about it, and later to come back and go on with it. If he does this he must leave a note of instructions (written in some standard form) explaining how the work is to be continued. This note is the counterpart of the "state of mind".

La macchina di calcolo universale

E' possibile inventare una singola macchina che può essere usata per calcolare qualunque successione calcolabile.

Se si fornisce tale macchina $\mathcal{I}$ con un nastro all'inizio del quale sta scritto la descrizione standard di una qualche macchina di calcolo $\mathcal{M}$, allora $\mathcal{I}$ calcolerà la stessa successione di $\mathcal{M}$.

... In ogni istante, il comportamento di un calcolatore è determinato dal simbolo che sta osservando e dal suo "stato mentale" in quell'istante.

... Ogni tale operazione risulta in qualche modifica del sistema fisico che consiste del calcolatore e del suo nastro.

... E' sempre possibile che il calcolatore voglia interrompere il proprio lavoro, andarsene e dimenticare tutto, per poi ritornare e continuarlo. Se fa questo, egli deve lasciare una nota di istruzioni (scritte in qualche modo standard) che spieghino come si deve continuare il lavoro. Tale nota è la controparte dello "stato mentale".

Segreti

- Arrivo a Bletchley Park, 4 settembre 1939
- Progetto con G. Welchman della **Bombe** inglese, gennaio 1940
- Risultati quasi nulli per tutto il 1940
- Turing sviluppa tecniche probabilistiche per migliorare la ricerca delle Bombe, gennaio 1941
- Scoprono che le navi tedesche d'osservazione meteorologica sono munite di macchine Enigma, marzo-aprile 1941
- Cattura della *München*, 7 maggio 1941
- Abbordaggio dell'U-110, 9 maggio 1941
- Traffico tedesco letto giornalmente, dal giugno 1941
- Attacco alle navi rifornimento della *Bismarck*, giugno 1941
- Le decrittazioni diventano **ULTRA SECRET**, giugno 1941
- Churchill visita Bletchley Park, incontra Turing, luglio 1941
- Turing richiede personale direttamente a Churchill, 21 ottobre 1941
- Arrivo di nuovo personale a Bletchley Park, 18 novembre 1941

The Imitation Game

I propose to consider the question, "Can machines think?" This should begin with definitions of the meaning of the terms "machine" and "think".

The definitions might be framed so as to reflect so far as possible the normal use of the words, but this attitude is dangerous.

If the meaning of the words "machine" and "think" are to be found by examining how they are commonly used it is difficult to escape the conclusion that the meaning and the answer to the question, "Can machines think?" is to be sought in a statistical survey such as a Gallup poll. But this is absurd.

Instead of attempting such a definition I shall replace the question by another, which is closely related to it and is expressed in relatively unambiguous words.

Il gioco d'imitazione

Propongo di considerare la domanda: "Le macchine possono pensare?" Questo dovrebbe iniziare con le definizioni del significato dei termini "macchina" e "pensare".

Le definizioni potrebbero essere architettate in modo da riflettere per quanto più possibile l'uso comune delle parole, ma questo atteggiamento è pericoloso.

Se si deve trovare il significato delle parole "macchina" e "pensare" esaminando come vengono usati normalmente è difficile evitare la conclusione che il significato e la risposta alla domanda "Le macchine possono pensare?" verranno trovati mediante un sondaggio statistico. Ma questo è assurdo.

Invece di provare a dare una tale definizione, cambierò la domanda con un'altra, che è strettamente connessa a quella e che si esprime in termini relativamente non ambigui.

The new form of the problem can be described in terms of a game which we call the "imitation game".

It is played with three people, a man (A), a woman (B), and an interrogator (C) who may be of either sex. The interrogator stays in a room apart front the other two. The object of the game for the interrogator is to determine which of the other two is the man and which is the woman.

...It is A's object in the game to try and cause C to make the wrong identification.

...The object of the game for the third player (B) is to help the interrogator. The best strategy for her is probably to give truthful answers.

...We now ask the question, "What will happen when a machine takes the part of A in this game?" Will the interrogator decide wrongly as often when the game is played like this as he does when the game is played between a man and a woman? These questions replace our original, "Can machines think?"

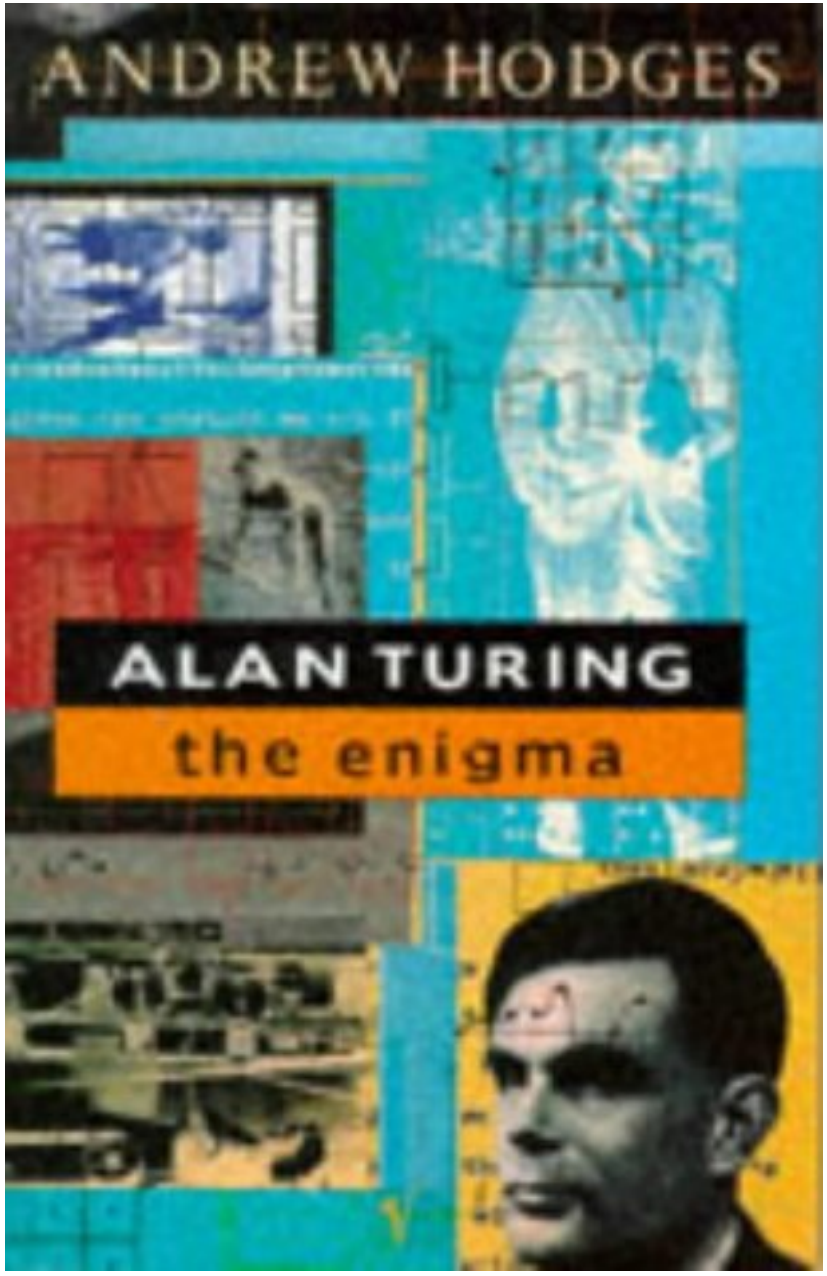
Si può descrivere la nuova forma del problema in termini di un gioco che chiamiamo il "gioco d'imitazione".

Si gioca in tre: un uomo (A), una donna (B) e un interrogatore (C) che può di sesso qualunque. L'interrogatore è in una stanza, separato dagli altri due. Lo scopo del gioco per l'interrogatore è quello di determinare chi sia l'uomo e chi la donna.

...Lo scopo di A nel gioco è di far fare a C le identificazioni errate.

...Lo scopo del gioco del terzo giocatore (B) è di aiutare l'interrogatore, La migliore strategia per lei è probabilmente di dare risposte vere.

...Ora poniamo la domanda: "Che cosa succede quando una macchina prende il posto di A nel gioco?" Le identificazioni errate dell'interrogatore saranno tante quante quelle fatte nel gioco con un uomo e una donna? Queste domande sostituiscono l'originale "Le macchine possono pensare?"


ANDREW HODGES
ALAN TURING
the enigma