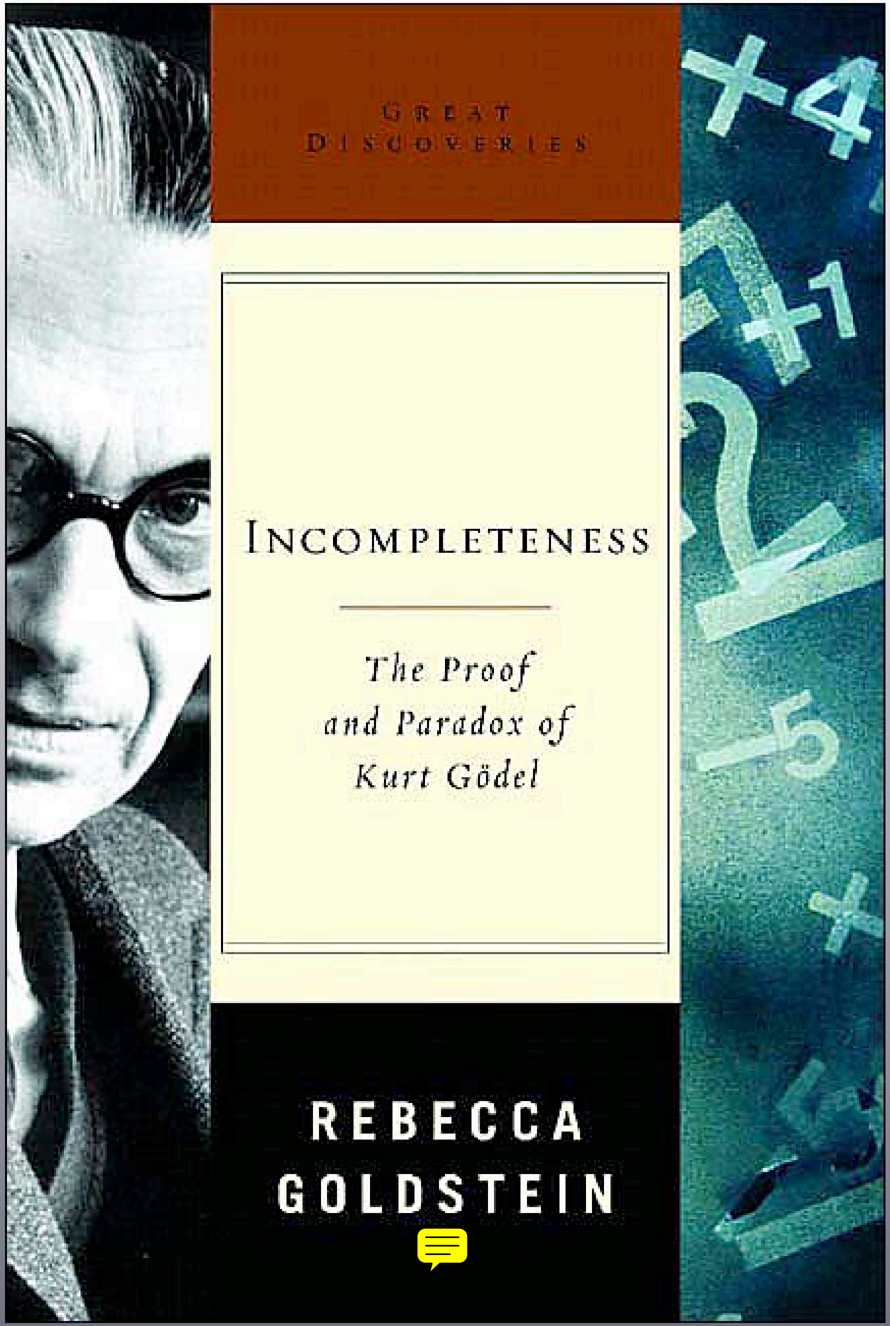
COMPLEXITY, PROVABILITY AND INCOMPLETENESS

Cristian S. Calude

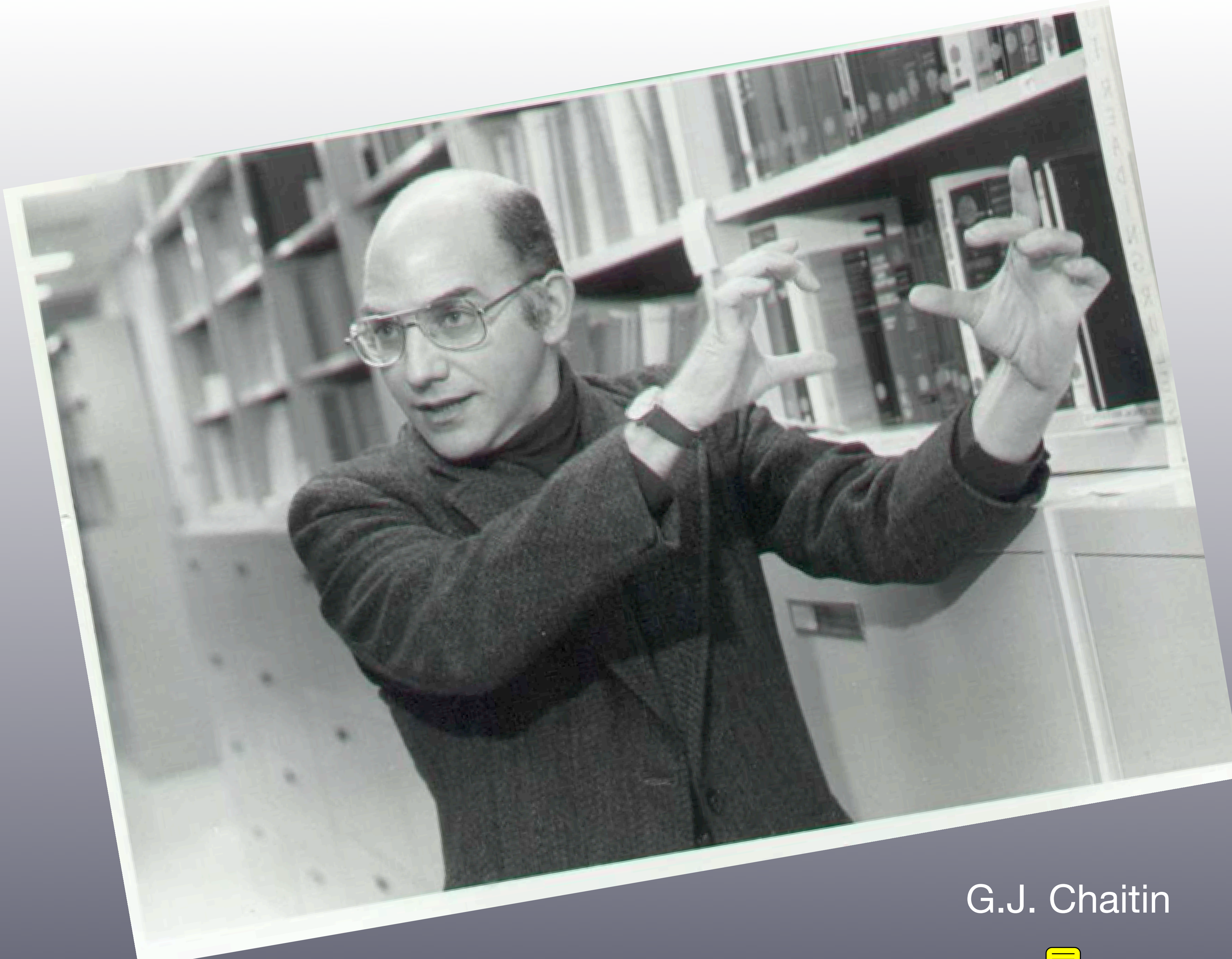
"*Either mathematics is too big for the human mind or the human mind is more than a machine.*"

K. Gödel

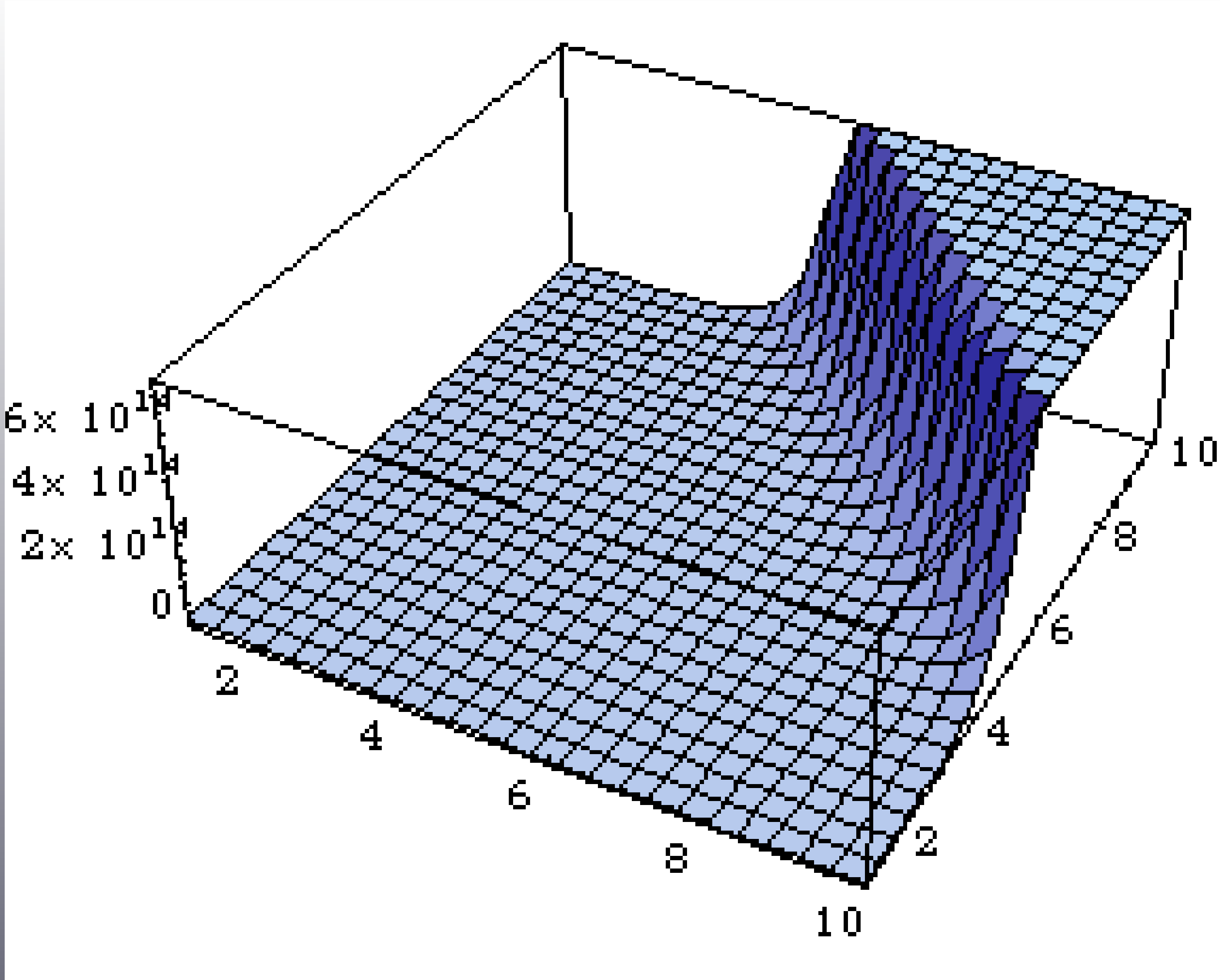


Gödel's theorem, announced 75 years ago this October is the

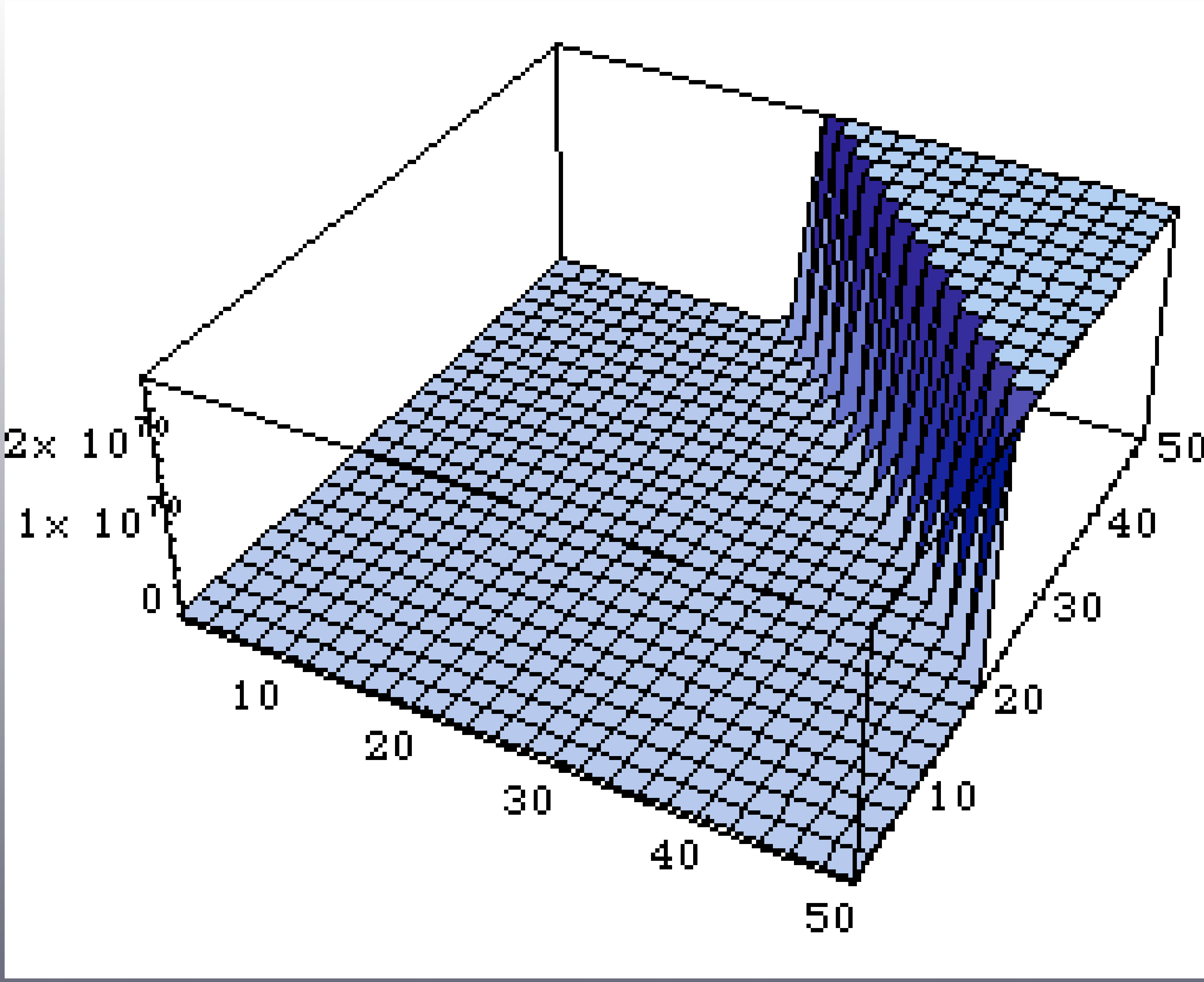
“*the third leg, together with Heisenberg's uncertainty principle and Einstein's relativity, of that tripod of theoretical cataclysms that have been felt to force disturbances deep down in the foundations of the ‘exact sciences.’*”



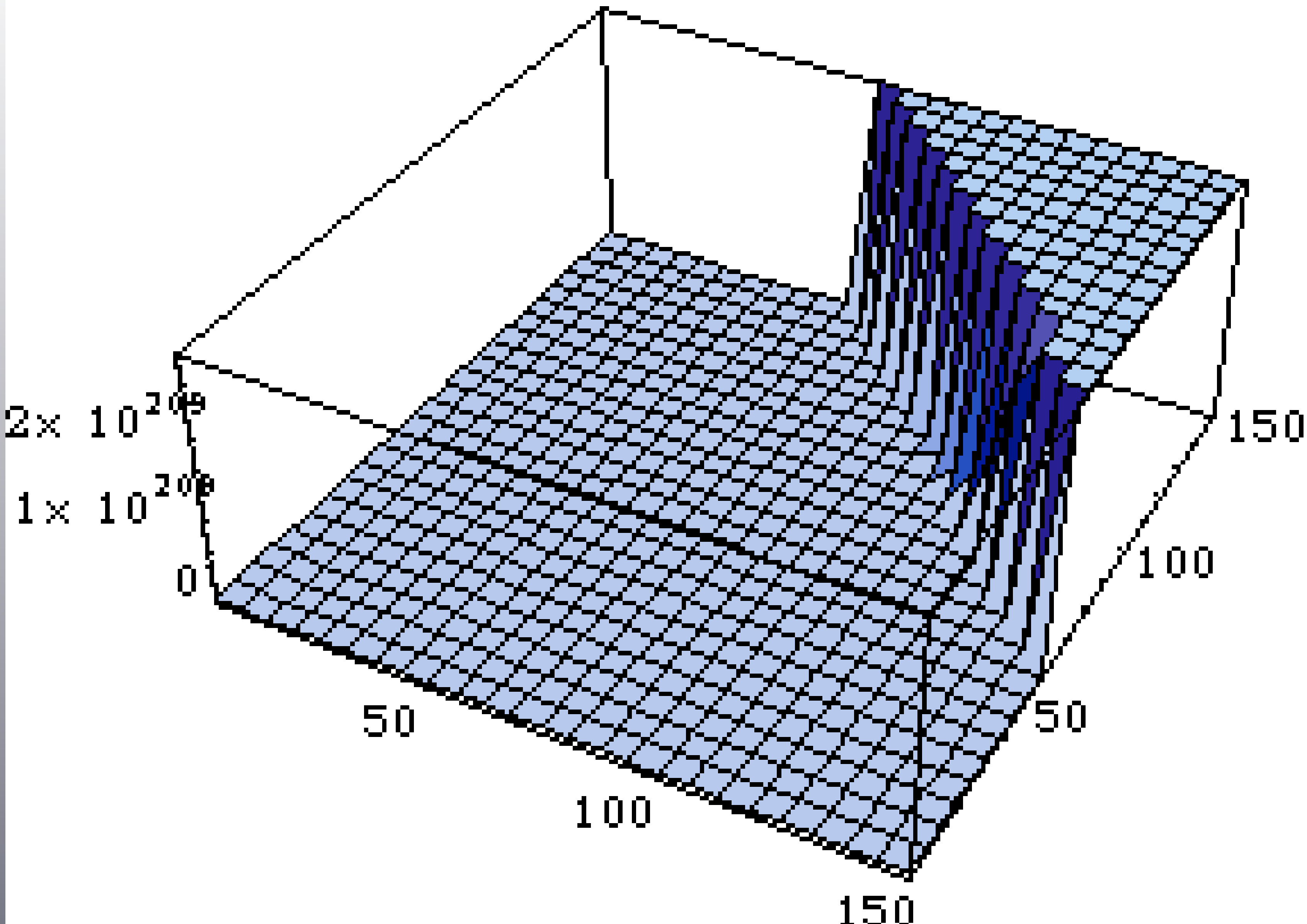
G.J. Chaitin



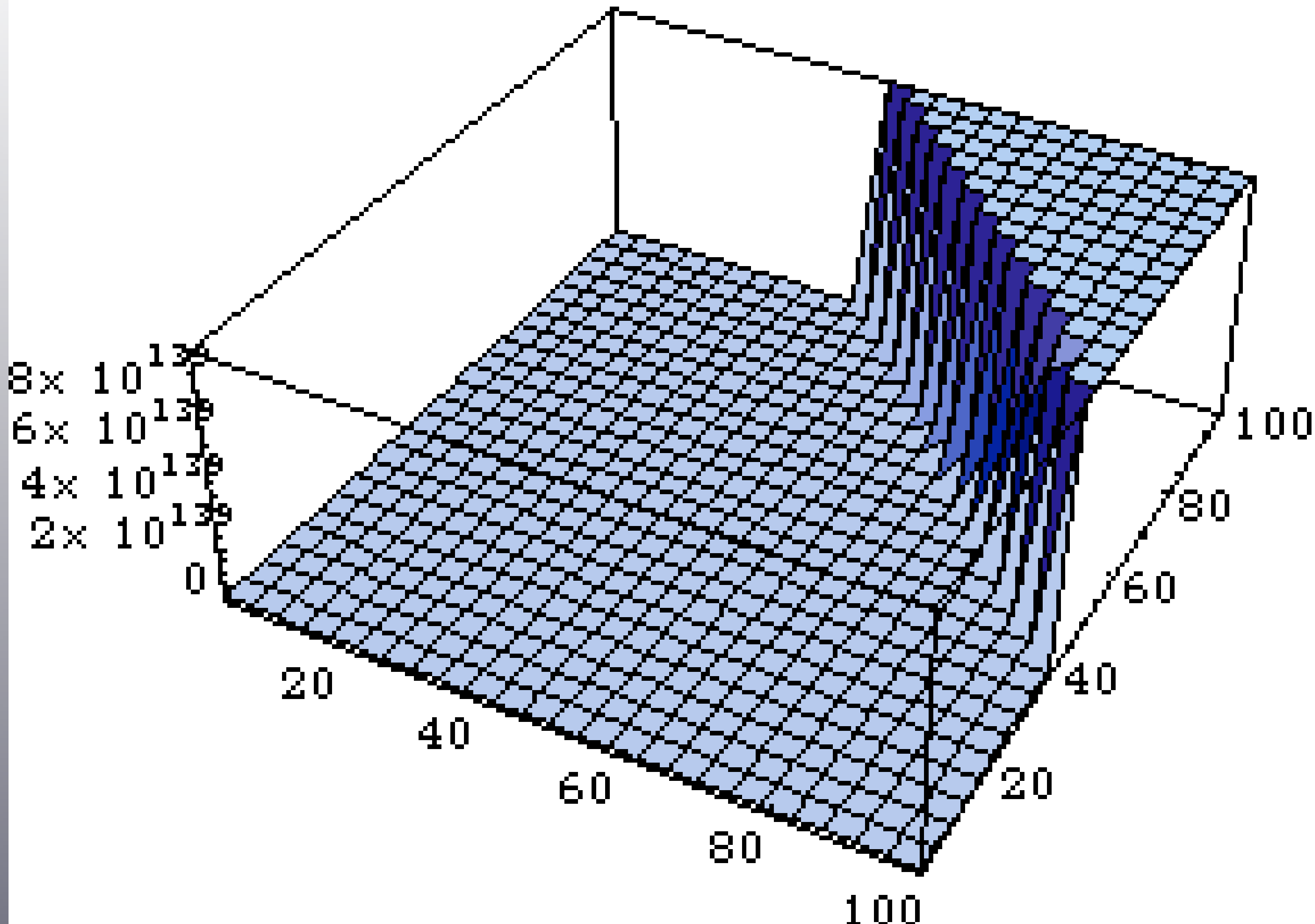
6x 10^14
4x 10^14
2x 10^14
0
2
4
6
8
10
2
4
6
8
10



2x 10^70
1x 10^70
0
10
20
30
40
50
10
20
30
40
50



2×10^{209}
1×10^{208}
0
50
100
150
50
100
150



8x 10^13
6x 10^13
4x 10^13
2x 10^13
0
20
40
60
80
100
20
40
60
80
100

Gödel's Incompleteness Theorem, announced on 7 October 1930 in Koenigsberg at the First International Conference on the Philosophy of Mathematics, is a landmark of the twentieth century mathematics.

According to Hintikka, with the exception of von Neumann, who immediately grasped Gödel's line of thought and its importance, incompleteness passed un-noticed in Koenigsberg: even the speaker who summarized the discussion omitted Gödel's result.

Encyclopedia of Philosophy: Gödel's Theorem

In any formal system adequate for number theory there exists an undecidable formula-that is, a formula that is not provable and whose negation is not provable.

No classical proof of incompleteness answers the questions of whether independence is a widespread phenomenon nor which kinds of sentences can be expected to be unprovable.

Chaitin presented a complexity-theoretic proof of Gödel's Incompleteness Theorem which shows that high complexity is a reason of the unprovability of infinitely many (true) sentences. This result suggested to him the following ``heuristic principle'', an information-preservation principle:

the theorems of a finitely specified theory cannot be significantly more complex than the theory itself.

Chaitin's proof is based on program-size complexity *H*: the complexity *H(s)* of a binary string *s* is the size, in bits, of the shortest program for a universal self-delimiting Turing machine to calculate *s*.

The proof shows that

for every finitely-specified, sound, consistent theory strong enough to formalize arithmetic, there exists a positive constant *M* such that no sentence of the form "$H(x) > m$" is provable in the theory unless *m* is less than *M*.

There are infinitely many true sentences of the form "$H(x) > m$" with $m > M$, and each of them is unprovable in the theory.

The high *H*-complexity of the sentences "$H(x) > m$" with $m > M$ is a source of their unprovability.

Is every true sentence s with $H(s) > M$ unprovable by the theory?

Unfortunately, the answer is negative: only finitely many sentences *s* have complexity $H(s) < M$, in contrast with the fact that the set of all theorems of the theory is infinite.

For example, ZFC or Peano Arithmetic trivially prove all sentences of the form "$n + 1 = 1 + n$". The *H*-complexity of the sentences "$n + 1 = 1 + n$" grows unbounded with n.

Can Chaitin's ``heuristic principle'':

the theorems of a finitely specified theory cannot be significantly more complex than the theory itself

be proved for an appropriate complexity measure?

The δ-complexity is

$$\delta(\mathbf{x}) = \mathbf{H}(\mathbf{x}) - |\mathbf{x}|.$$

The complexity measures *H* and δ have similarities as δ is defined from *H* by means of some simple computable functions; for example, they are both uncomputable.

But *H* and δ are drastically different:

the set strings *x* with $H(x) \leq N$ is finite while,

the set of strings *x* with $\delta(x) \leq N$ is infinite.

To be able to measure somehow the ``intrinsic'' complexity of a theorem we need to prove that the property is invariant with respect to a system of acceptable names, i.e. Gödel numberings.

Let us fix a formal language L of well-formed formulae.

A Gödel numbering for L is a computable, one-to-one function g from L to the set of binary strings, i.e. a system of unique binary names for the formulae of L.

As the set of theorems T is a c.e. subset of L, we will work only with computable, one-to-one functions g from T to binary strings.

The δ-complexity of a theorem u in T induced by the Gödel numbering g is defined by:

$$\delta_g(u) = H_2(g(u)) - \lceil \log_2 Q \rceil \cdot |u|_Q.$$

Theorem: There effectively exists a constant *c* such that for all *u* in T we have:

$$|\delta_g(u) - \lceil \log_2 Q \rceil \cdot \delta_Q(u)| \leq c.$$

Corollary: Let T be c.e. and g, *g'* be two Gödel numbering defined on T. Then, there effectively exists a constant *c* such that for all *u* in T we have:

$$|\delta_g(u) - \delta_{g'}(u)| \leq c.$$

Theorem (Calude-Juergensen): Consider a finitely-specified, arithmetically sound (i.e. each arithmetical proven sentence is true), consistent theory strong enough to formalize arithmetic, and denote by T its set of theorems. Let g be a Gödel numbering for T. Then, there exists a constant N, which depends upon T, such that T contains no x with

$$\delta_g(x) > N.$$

Corollary: Every finitely-specified, arithmetically sound, consistent theory strong enough to formalize arithmetic can prove only, for finitely many of its theorems, that they have high δ-complexity.

Is incompleteness wide-spread?

Theorem: Consider a consistent, sound, finitely-specified theory strong enough to formalize arithmetic. The probability that a true sentence of length n is provable in the theory tends to zero when n tends to infinity, while the probability that a sentence of length n is true is strictly positive.

Open questions:

a) Sentences expressed by strings with large δ-complexity are unprovable. Is the converse implication true?

In other words, given a theory as above, are there independent sentences ***x*** with low δ-complexity? Even if such sentences do exist, the probability that a true sentence of length n with δ-complexity less than or equal to ***N*** is unprovable in the theory tends to zero when n tends to infinity.

b) Calculate the δ-complexity of some concrete independent sentences, like the sentence expressing the consistency of the theory itself.

c) Find other (more interesting?) measures of complexity satisfying Chaitin's "heuristic principle".

d) Check the validity of the following stronger result: under the same conditions, the probability that a sentence of length n, expressible in the language of the theory, is provable in the theory tends to zero when n tends to infinity.