# Incompleteness: A Personal Perspective

Cristian S. Calude

University of Auckland

DCFS08, July, 2008

## The incompleteness theorem

*Every axiomatic system $\mathcal{F}$ which is*
*(1) finitely specified,*

## The incompleteness theorem

*Every axiomatic system $\mathcal{F}$ which is*
*(1) finitely specified,*
*(2) rich enough to include the arithmetic, and*

## The incompleteness theorem

*Every axiomatic system $\mathcal{F}$ which is*
*(1) finitely specified,*
*(2) rich enough to include the arithmetic, and*
*(3) arithmetically sound,*

## The incompleteness theorem

*Every axiomatic system $\mathcal{F}$ which is*
*(1) finitely specified,*
*(2) rich enough to include the arithmetic, and*
*(3) arithmetically sound,*
*is incomplete;*

## The incompleteness theorem

*Every axiomatic system $\mathcal{F}$ which is*
*(1) finitely specified,*
*(2) rich enough to include the arithmetic, and*
*(3) arithmetically sound,*
*is incomplete; that is, there exists (and can be effectively constructed) a sentence of arithmetic which*

## The incompleteness theorem

*Every axiomatic system $\mathcal{F}$ which is*
*(1) finitely specified,*
*(2) rich enough to include the arithmetic, and*
*(3) arithmetically sound,*
*is incomplete; that is, there exists (and can be effectively constructed) a sentence of arithmetic which*
*(A) can be expressed in $\mathcal{F}$,*

## The incompleteness theorem

*Every axiomatic system $\mathcal{F}$ which is*
*(1) finitely specified,*
*(2) rich enough to include the arithmetic, and*
*(3) arithmetically sound,*
*is incomplete; that is, there exists (and can be effectively constructed) a sentence of arithmetic which*
*(A) can be expressed in $\mathcal{F}$,*
*(B) is true, and*

## The incompleteness theorem

*Every axiomatic system $\mathcal{F}$ which is*
*(1) finitely specified,*
*(2) rich enough to include the arithmetic, and*
*(3) arithmetically sound,*
*is incomplete; that is, there exists (and can be effectively constructed) a sentence of arithmetic which*
*(A) can be expressed in $\mathcal{F}$,*
*(B) is true, and*
*(C) is unprovable by $\mathcal{F}$.*

## The incompleteness theorem

*Every axiomatic system $\mathcal{F}$ which is*
*(1) finitely specified,*
*(2) rich enough to include the arithmetic, and*
*(3) arithmetically sound,*
*is incomplete; that is, there exists (and can be effectively constructed) a sentence of arithmetic which*
*(A) can be expressed in $\mathcal{F}$,*
*(B) is true, and*
*(C) is unprovable by $\mathcal{F}$.*

Conditions *(B)* and *(C)* can be replaced by the following condition

## The incompleteness theorem

*Every axiomatic system $\mathcal{F}$ which is*
*(1) finitely specified,*
*(2) rich enough to include the arithmetic, and*
*(3) arithmetically sound,*
*is incomplete; that is, there exists (and can be effectively constructed) a sentence of arithmetic which*
*(A) can be expressed in $\mathcal{F}$,*
*(B) is true, and*
*(C) is unprovable by $\mathcal{F}$.*

Conditions *(B)* and *(C)* can be replaced by the following condition

*(B') is neither provable or disprovable by $\mathcal{F}$.*

## The incompleteness theorem

*Every axiomatic system $\mathcal{F}$ which is*
*(1) finitely specified,*
*(2) rich enough to include the arithmetic, and*
*(3) arithmetically sound,*
*is incomplete; that is, there exists (and can be effectively constructed) a sentence of arithmetic which*
*(A) can be expressed in $\mathcal{F}$,*
*(B) is true, and*
*(C) is unprovable by $\mathcal{F}$.*

Conditions *(B)* and *(C)* can be replaced by the following condition

*(B') is neither provable or disprovable by $\mathcal{F}$.*

The sentence satisfying *(B')* is called *independent*.

## An example

The main example of an axiomatic theory is the Zermelo–Fraenkel set theory with choice, *ZFC*. We fix an interpretation of Peano Arithmetic (*PA*) in *ZFC*. Each sentence of the language of *PA* has a translation into a sentence of the language of *ZFC*, determined by the interpretation of *PA* in *ZFC*.

## An example

The main example of an axiomatic theory is the Zermelo–Fraenkel set theory with choice, *ZFC*. We fix an interpretation of Peano Arithmetic (*PA*) in *ZFC*. Each sentence of the language of *PA* has a translation into a sentence of the language of *ZFC*, determined by the interpretation of *PA* in *ZFC*.

A "sentence of arithmetic" indicates a sentence of the language of *ZFC* that is the translation of some sentence of *PA*.

## Incompleteness as a theorem in computability theory

Consider all propositions $s_n$ of the form "$n \notin S$", where $S$ is a non-c.e. set of naturals and $n$ is a natural number. Let $\mathcal{F}$ be an axiomatic theory containing all propositions $s_n$, and assume that:

## Incompleteness as a theorem in computability theory

Consider all propositions $s_n$ of the form "$n \notin S$", where $S$ is a non-c.e. set of naturals and $n$ is a natural number. Let $\mathcal{F}$ be an axiomatic theory containing all propositions $s_n$, and assume that:

*a) $\mathcal{F}$ is sound for all $s_n$, i.e. whenever $\mathcal{F}$ proves $s_n$, then $n \notin S$,*

## Incompleteness as a theorem in computability theory

Consider all propositions $s_n$ of the form "$n \notin S$", where $S$ is a non-c.e. set of naturals and $n$ is a natural number. Let $\mathcal{F}$ be an axiomatic theory containing all propositions $s_n$, and assume that:

*a) $\mathcal{F}$ is sound for all $s_n$, i.e. whenever $\mathcal{F}$ proves $s_n$, then $n \notin S$,*
*b) there is a computable function $t$ which enumerates all propositions $s_n$ that $\mathcal{F}$ can prove:*

$$\{t(0), t(1), \ldots, t(m), \ldots\} = \{s_i \mid \mathcal{F} \text{ proves } s_i, i \geq 0\}.$$

In this setting the incompleteness theorem can be stated as follows:

## Incompleteness as a theorem in computability theory

Consider all propositions $s_n$ of the form "$n \notin S$", where $S$ is a non-c.e. set of naturals and $n$ is a natural number. Let $\mathcal{F}$ be an axiomatic theory containing all propositions $s_n$, and assume that:

*a) $\mathcal{F}$ is sound for all $s_n$, i.e. whenever $\mathcal{F}$ proves $s_n$, then $n \notin S$,*
*b) there is a computable function $t$ which enumerates all propositions $s_n$ that $\mathcal{F}$ can prove:*

$$\{t(0), t(1), \ldots, t(m), \ldots\} = \{s_i \mid \mathcal{F} \text{ proves } s_i, i \geq 0\}.$$

In this setting the incompleteness theorem can be stated as follows:

*If $\mathcal{F}$ is an axiomatic system satisfying a) and b) above, then there is a natural number $N$ such that $N \notin S$, but $\mathcal{F}$ cannot prove $s_N$ ($\mathcal{F}$ cannot prove the true proposition $s_N$).*

## Three questions

In what follows we will discuss the following three questions on incompleteness:

- Are there interesting/natural concrete independent sentences?

## Three questions

In what follows we will discuss the following three questions on incompleteness:

- Are there interesting/natural concrete independent sentences?
- What is the source of incompleteness?

## Three questions

In what follows we will discuss the following three questions on incompleteness:

- Are there interesting/natural concrete independent sentences?
- What is the source of incompleteness?
- How common is the incompleteness phenomenon?

## An analogy

Cantor's diagonal proof shows the existence of transcendental reals but doesn't provide any natural/interesting concrete examples.

## An analogy

Cantor's diagonal proof shows the existence of transcendental reals but doesn't provide any natural/interesting concrete examples.

Liouville constructed an interesting class of examples of transcendental reals, but his method was not directly useful for showing that a natural example of real (like $\pi, e$) is transcendental; however, Liouville's method shows a source of transcendence (Liouville numbers can be approximated "quite closely" by rationals).

## An analogy

Cantor's diagonal proof shows the existence of transcendental reals but doesn't provide any natural/interesting concrete examples.

Liouville constructed an interesting class of examples of transcendental reals, but his method was not directly useful for showing that a natural example of real (like $\pi, e$) is transcendental; however, Liouville's method shows a source of transcendence (Liouville numbers can be approximated "quite closely" by rationals).

Ferdinand von Lindemann's proof showed that $\pi$, the most interesting real number, is transcendental.

## An analogy

Cantor's diagonal proof shows the existence of transcendental reals but doesn't provide any natural/interesting concrete examples.

Liouville constructed an interesting class of examples of transcendental reals, but his method was not directly useful for showing that a natural example of real (like $\pi, e$) is transcendental; however, Liouville's method shows a source of transcendence (Liouville numbers can be approximated "quite closely" by rationals).

Ferdinand von Lindemann's proof showed that $\pi$, the most interesting real number, is transcendental.

Finally, are there "many" transcendental reals? The answer is yes in both measure and category.

## Examples 1

We will fix an axiomatic theory $\mathcal{F}$ satisfying the properties *(1)*, *(2)*, *(3)* in the incompleteness theorem.

## Examples 1

We will fix an axiomatic theory $\mathcal{F}$ satisfying the properties *(1)*, *(2)*, *(3)* in the incompleteness theorem.

**Gödel's second incompleteness theorem.** *Every axiomatic theory $\mathcal{F}$ cannot prove its own consistency.*

## Examples 1

We will fix an axiomatic theory $\mathcal{F}$ satisfying the properties *(1)*, *(2)*, *(3)* in the incompleteness theorem.

**Gödel's second incompleteness theorem.** *Every axiomatic theory $\mathcal{F}$ cannot prove its own consistency.*

Referring to normalisation for a typed extension of lambda-calculus—the system T, Gödel found the first combinatorial $\forall\exists$–sentence which is independent in *PA*.

## Examples 1

We will fix an axiomatic theory $\mathcal{F}$ satisfying the properties *(1), (2), (3)* in the incompleteness theorem.

**Gödel's second incompleteness theorem.** *Every axiomatic theory $\mathcal{F}$ cannot prove its own consistency.*

Referring to normalisation for a typed extension of lambda-calculus—the system T, Gödel found the first combinatorial $\forall\exists$–sentence which is independent in *PA*.

Other combinatorial $\forall\exists$–sentences true but unprovable in *PA* include Paris and Harrington modified form of the finite Ramsey theorem and Kruskal-Friedman theorem. Matiyasevich discussed Diophantine examples.

## Examples 2

Interesting $\forall\exists$–sentences appear in algorithmic information theory.

## Examples 2

Interesting $\forall\exists$–sentences appear in algorithmic information theory.

**Chaitin first incompleteness theorem.** *Consider an axiomatic theory $\mathcal{F}$. Then, there exists a constant $c$ (depending on $\mathcal{F}$) such that if $\mathcal{F}$ proves a sentence of the form "$H(x) > m$", then $m < c$.*

## Examples 2

Interesting $\forall\exists$–sentences appear in algorithmic information theory.

**Chaitin first incompleteness theorem.** *Consider an axiomatic theory $\mathcal{F}$. Then, there exists a constant $c$ (depending on $\mathcal{F}$) such that if $\mathcal{F}$ proves a sentence of the form "$H(x) > m$", then $m < c$.*

The halting probability $\Omega_U$ of a prefix-free universal machine $U$ is defined by $\Omega_U = \sum_{U(x) \text{ is defined}} 2^{-|x|}$.

## Examples 2

Interesting $\forall\exists$–sentences appear in algorithmic information theory.

**Chaitin first incompleteness theorem.** *Consider an axiomatic theory $\mathcal{F}$. Then, there exists a constant $c$ (depending on $\mathcal{F}$) such that if $\mathcal{F}$ proves a sentence of the form "$H(x) > m$", then $m < c$.*

The halting probability $\Omega_U$ of a prefix-free universal machine $U$ is defined by $\Omega_U = \sum_{U(x) \text{ is defined}} 2^{-|x|}$.

**Chaitin second incompleteness theorem.** *Assume that ZFC is arithmetically sound. Then, for every prefix-free universal machine $U$, ZFC can determine the value of only finitely many bits of $\Omega_U$, and one can give a bound on the number of bits of $\Omega_U$ which ZFC can determine.*

## Examples 3

**Solovay incompleteness theorem.** *There effectively exists a prefix-free universal machine $U$ such that ZFC (if arithmetically sound) cannot determine any bit of $\Omega_U$.*

## Examples 3

**Solovay incompleteness theorem.** *There effectively exists a prefix-free universal machine $U$ such that ZFC (if arithmetically sound) cannot determine any bit of $\Omega_U$.*

**CC incompleteness theorem.** *Assume that ZFC is arithmetically sound. Consider a prefix-free machine $U$ which PA proves universal and assume that $\Omega_U$ is written in binary as follows:*

$$\Omega_U = 0.\omega_0\omega_1\ldots\omega_{i-1}\omega_i\omega_{i+1}\ldots, \text{ where } \omega_0 = \omega_1 = \ldots = \omega_{i-1} = 1, \omega_i = 0.$$

*Then, we can effectively construct a prefix-free universal machine $U'$ (depending upon ZFC and $U$) such that PA proves universal, $\Omega_U = \Omega'_U$, and ZFC can determine at most $i$ initial bits of $\Omega'_U$.*

## Are there simpler examples? 1

What about Goldbach's conjecture or Riemann hypothesis: Are they independent of *ZFC*? Of course, *this is not known*.

## Are there simpler examples? 1

What about Goldbach's conjecture or Riemann hypothesis: Are they independent of *ZFC*? Of course, *this is not known*.

As they are $\forall$–sentences one can associate to each of them a program which never halts iff the conjecture is true.

## Are there simpler examples? 1

What about Goldbach's conjecture or Riemann hypothesis: Are they independent of *ZFC*? Of course, *this is not known*.

As they are $\forall$–sentences one can associate to each of them a program which never halts iff the conjecture is true.

Such programs have been effectively constructed, $\Pi_G$ (for Goldbach's conjecture) has 3,484 bits and $\Pi_R$ (for Riemann hypothesis ) has 7,780 bits. Solving the Halting Problem for relatively small-size programs would solve these questions.

## Are there simpler examples? 2

Define $T(x) = x/2$, if $x$ is even, and $T(x) = 3x + 1$, if $x$ is odd.

## Are there simpler examples? 2

Define $T(x) = x/2$, if $x$ is even, and $T(x) = 3x + 1$, if $x$ is odd.

**Collatz' conjecture.** *For every $a > 0$, there is an iteration $N$ such that $T^N(a) = 1$.*

## Are there simpler examples? 2

Define $T(x) = x/2$, if $x$ is even, and $T(x) = 3x + 1$, if $x$ is odd.

**Collatz' conjecture.** *For every $a > 0$, there is an iteration $N$ such that $T^N(a) = 1$.*

The reverse of a number is the number formed with the same decimal digits but written in the opposite order. Start with the decimal representation of a natural $a$, reverse the digits and add the constructed number to $a$; iterate.

## Are there simpler examples? 2

Define $T(x) = x/2$, if $x$ is even, and $T(x) = 3x + 1$, if $x$ is odd.

**Collatz' conjecture.** *For every $a > 0$, there is an iteration $N$ such that $T^N(a) = 1$.*

The reverse of a number is the number formed with the same decimal digits but written in the opposite order. Start with the decimal representation of a natural $a$, reverse the digits and add the constructed number to $a$; iterate.

**The palindrome conjecture.** *For every $a$, a palindrome number will be obtained after finitely many iterations of the above procedure.*

## Are there simpler examples? 2

Both conjectures are $\forall$–sentences, but the proof—based on the fact that the set of natural numbers $a$ satisfying each conjecture is c.e.—*is not constructive*. We don't know whether there is no constructive proof for the fact that each conjecture is a $\forall$–sentence.

## Are there simpler examples? 2

Both conjectures are $\forall$–sentences, but the proof—based on the fact that the set of natural numbers $a$ satisfying each conjecture is c.e.—*is not constructive*. We don't know whether there is no constructive proof for the fact that each conjecture is a $\forall$–sentence.

This suggests that

## Are there simpler examples? 2

Both conjectures are $\forall$–sentences, but the proof—based on the fact that the set of natural numbers *a* satisfying each conjecture is c.e.—*is not constructive*. We don't know whether there is no constructive proof for the fact that each conjecture is a $\forall$–sentence.

This suggests that

> *the Collatz and palindrome conjectures are more likely to be unprovable than Goldbach or Riemann conjectures.*

## Dyson's conjectures

**Dyson's first conjecture.** *The reverse (in decimal) of a power of two is never a power of five.*

## Dyson's conjectures

**Dyson's first conjecture.** *The reverse (in decimal) of a power of two is never a power of five.*

**Dyson's plausibility argument:** The digits in a big power of two seem to occur in a random way without any regular pattern. If it ever happened that the reverse of a power of two was a power of five, this would be an unlikely accident, and the chance of it happening grows rapidly smaller as the numbers grow bigger. If we assume that the digits occur at random, then the chance of the accident happening for any power of two greater than a billion is less than one in a billion. It is easy to check that it does not happen for powers of two smaller than a billion. So the chance that it ever happens at all is less than one in a billion.

## Dyson's conjectures

**Dyson's first conjecture.** *The reverse (in decimal) of a power of two is never a power of five.*

**Dyson's plausibility argument:** The digits in a big power of two seem to occur in a random way without any regular pattern. If it ever happened that the reverse of a power of two was a power of five, this would be an unlikely accident, and the chance of it happening grows rapidly smaller as the numbers grow bigger. If we assume that the digits occur at random, then the chance of the accident happening for any power of two greater than a billion is less than one in a billion. It is easy to check that it does not happen for powers of two smaller than a billion. So the chance that it ever happens at all is less than one in a billion.

**Dyson's second conjecture.** *Dyson's first conjecture is unprovable in ZFC.*

## An information-preservation principle

The high $H$–complexity of sentences "$H(x) > m$" with $m > c$ is a source of their unprovability. Chaitin has formulated the following "information-preservation principle":

## An information-preservation principle

The high $H$–complexity of sentences "$H(x) > m$" with $m > c$ is a source of their unprovability. Chaitin has formulated the following "information-preservation principle":

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

## An information-preservation theorem

Let $X$ be an alphabet with $Q$ elements for the axiomatic theory $\mathcal{F}$. Consider a computable, one-to-one binary coding $g$ of the set of sentences of $\mathcal{F}$. The $\delta$-complexity of a sentence $u \in \mathcal{F}$ induced by $g$ is defined by:

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

**CC-Jürgensen theorem.** *For every axiomatic theory $\mathcal{F}$ and for any computable, one-to-one function $g$, we can compute a bound $N$ such that no sentence $x$ with complexity $\delta_g(x) > N$ can be proved in the theory.*

## An information-preservation theorem

Let $X$ be an alphabet with $Q$ elements for the axiomatic theory $\mathcal{F}$. Consider a computable, one-to-one binary coding $g$ of the set of sentences of $\mathcal{F}$. The $\delta$-complexity of a sentence $u \in \mathcal{F}$ induced by $g$ is defined by:

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

**CC-Jürgensen theorem.** *For every axiomatic theory $\mathcal{F}$ and for any computable, one-to-one function $g$, we can compute a bound $N$ such that no sentence $x$ with complexity $\delta_g(x) > N$ can be proved in the theory.*

**Question 1.** *Find other natural measures of complexity for which Chaitin's "heuristic principle" holds true.*

## An information-preservation theorem

Let $X$ be an alphabet with $Q$ elements for the axiomatic theory $\mathcal{F}$. Consider a computable, one-to-one binary coding $g$ of the set of sentences of $\mathcal{F}$. The $\delta$-complexity of a sentence $u \in \mathcal{F}$ induced by $g$ is defined by:

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

**CC-Jürgensen theorem.** *For every axiomatic theory $\mathcal{F}$ and for any computable, one-to-one function $g$, we can compute a bound $N$ such that no sentence $x$ with complexity $\delta_g(x) > N$ can be proved in the theory.*

**Question 1.** *Find other natural measures of complexity for which Chaitin's "heuristic principle" holds true.*

**Question 2.** *Are there independent sentences $x$ with low $\delta_g$-complexity?*

## Is incompleteness an accidental phenomenon?

To answer this question we need to measure the "size of the set of independent sentences" of an axiomatic theory $\mathcal{F}$. There are two possibilities and an important restriction: we can use either topological or probabilistic methods, but we have to work with constructive notions as the space of sentences is countable.

## Is incompleteness an accidental phenomenon?

To answer this question we need to measure the "size of the set of independent sentences" of an axiomatic theory $\mathcal{F}$. There are two possibilities and an important restriction: we can use either topological or probabilistic methods, but we have to work with constructive notions as the space of sentences is countable.

For every non c.e. set $A \subseteq X^*$ expressible in $\mathcal{F}$, the set $I(A)$ of all independent sentences of the form "$s \in A$" is non-empty and, indeed, infinite. *How large is $I(A)$?*

## A topological result

**CC-Jürgensen-Zimand theorem.** *Suppose that the topology $\tau$ is generated by a computable and length preserving partial order and satisfies the condition:*

> *There is a computable equivalence relation $\equiv$ on $X^*$ such that for every $x \in X^*$ and every open neighbourhood $N_x$ of $x$, the set $\{y \mid y \in X^*,\ N_x \cap [y]_{\equiv} = \emptyset\}$ is finite*

*with respect to a computable equivalence relation $\equiv$. For every non c.e. set $A \subseteq X^*$ expressible in an axiomatic theory $\mathcal{F}$ saturated by $\equiv$, the set $I(A)$ is co-rare in $\tau$.*

## A probabilistic result

Let $g$ be a computable, one-to-one binary coding for the sentences of $\mathcal{F}$, and consider:

- the probability $p_g^{\text{prov}}(n)$ that a sentence of length $n$ is provable in $\mathcal{F}$ and
- the probability $p_g^{\text{true}}(n)$ that a sentence of length $n$ is true.

These probabilities depend on $g$ in the same way as the complexity $\delta_g$ depends on $g$.

## A probabilistic result

Let $g$ be a computable, one-to-one binary coding for the sentences of $\mathcal{F}$, and consider:

- the probability $p_g^{\text{prov}}(n)$ that a sentence of length $n$ is provable in $\mathcal{F}$ and
- the probability $p_g^{\text{true}}(n)$ that a sentence of length $n$ is true.

These probabilities depend on $g$ in the same way as the complexity $\delta_g$ depends on $g$.

**CC-Jürgensen theorem.** *In every axiomatic theory $\mathcal{F}$, for all $g$, we have* $\lim_{n\to\infty} p_g^{\text{prov}}(n) = 0$, *but* $\lim_{n\to\infty} p_g^{\text{true}}(n) > 0$.

## A probabilistic result

Let $g$ be a computable, one-to-one binary coding for the sentences of $\mathcal{F}$, and consider:

- the probability $p_g^{\text{prov}}(n)$ that a sentence of length $n$ is provable in $\mathcal{F}$ and
- the probability $p_g^{\text{true}}(n)$ that a sentence of length $n$ is true.

These probabilities depend on $g$ in the same way as the complexity $\delta_g$ depends on $g$.

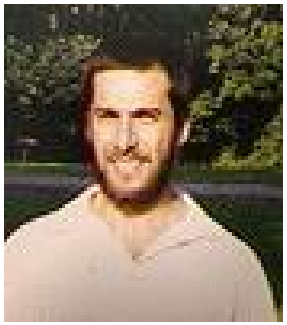
**CC-Jürgensen theorem.** *In every axiomatic theory $\mathcal{F}$, for all $g$, we have $\lim_{n\to\infty} p_g^{\text{prov}}(n) = 0$, but $\lim_{n\to\infty} p_g^{\text{true}}(n) > 0$.*

**Question 3. [P. Cholak]** *Is there is a sequence of computable, one-to-one binary codings $g_i$ such that $\lim_{n,i\to\infty} p_{i,n}^{\text{true}} = 0$?*

# Thank you!



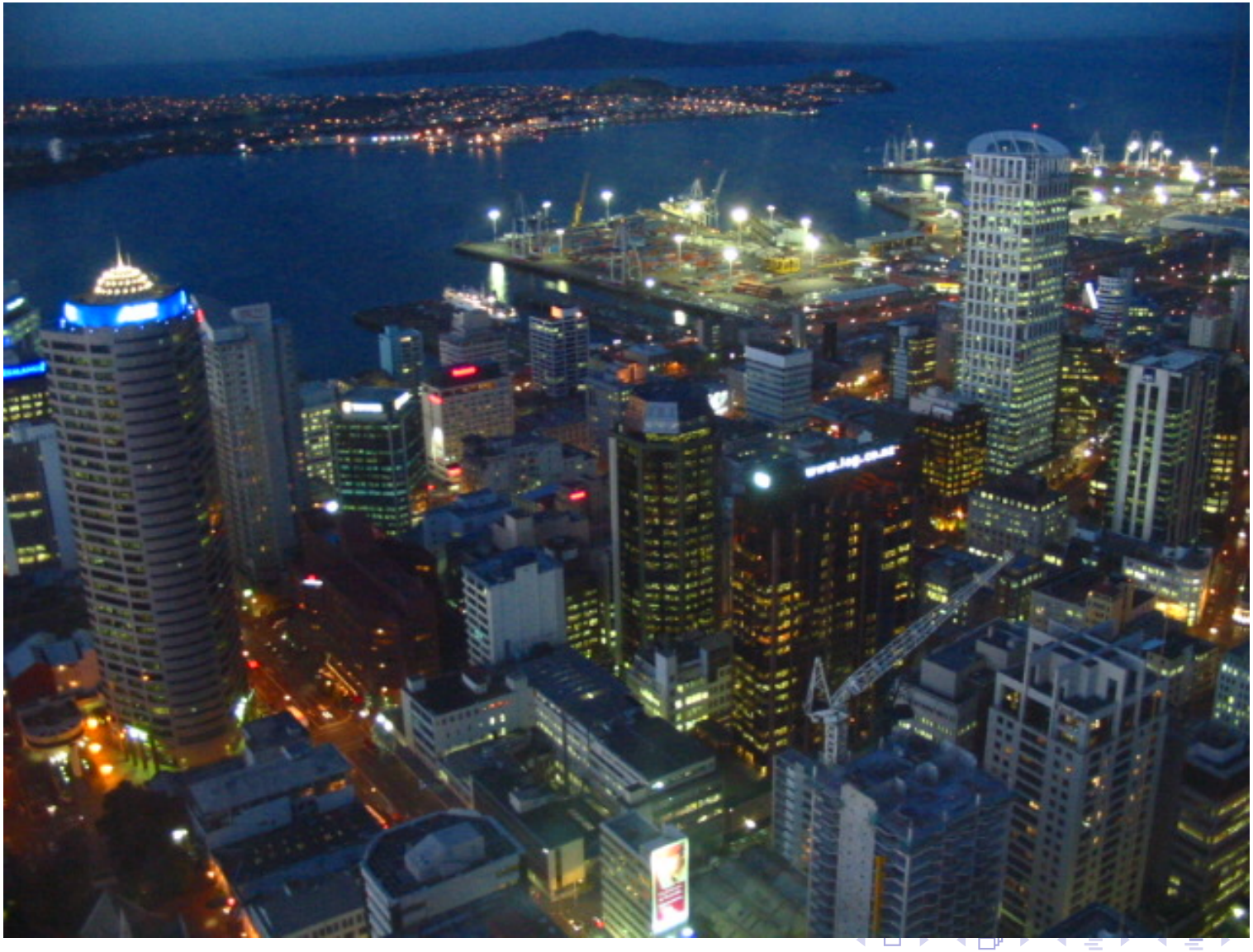
K. Gödel G. Chaitin R. Solovay


H. Jürgensen M. Zimand F. Dyson



P. Cholak Theories


THE
END