"TALK ABOUT INDEPENDENCE, forcing since it's a major achievement of set theory and math. logic in general".

1. Independence

Let's talk about independence proofs. "Proofs" is in the name, so let's look at those first. Pure mathematicians' number one job is to **find proofs**. They do it every day.

But: there are two types of proofs.

Most proofs are *natural proofs* (or *convincing arguments*). They follow inference rules, but are written down in English (or some other natural language), as opposed to some *formal language* and *formal reasoning*. Equally, assumptions or *axioms* are written down in natural language.

Formal proofs only work in formal languages, not in English. They are *syntactical*: they are just manipulations of symbols, there is no inherent meaning to the formulas.

Natural proofs are *semantical*. They rely on the properties of objects as described by formulas.

... and the connection between formal proofs and natural proofs is given by the following:

Luckily, this distinction doesn't really matter...

Theorem 1 (Gödel's Completeness Theorem). *Every natural proof can be turned into a formal proof, and vice versa.*

So we don't need to worry too much about formal proofs... **Unless we want to formalise all of mathematics uniformly.** That was David Hilbert's goal in 1900 – solving the *Foundational Crisis of Mathematics.*

To get an idea what he attempted, let's look at proofs, **formal and natural**. How do proofs work? We take a set of *axioms*, and then use *inference rules* to deduce new results, or *theorems*. Axioms are what we assume to be true.

Crucial is the following:

Theorem 2. *Proofs are finite.*

- The more we assume, the easier the proof. (extreme case: just assume what you want to prove)
- A result is stronger if its proof assumes less. Example: "If G is abelian, then the identity of G is unique."; "If n is odd, then $2n$ is even."
- If we assume a contradiction, we can prove anything.

Definition 3. *A set of axioms is called* consistent *if one cannot prove a contradiction from it.*

So here's the goal:

Find a consistent set of axioms that proves all mathematical facts.

David Hilbert came up with this in 1900, he imposed further restrictions: there should be a machine that can check whether a mathematical statement is true or false, based on the set of axioms. And: there should be a **proof that the system is consistent, within the system.**

We can **make any theory inconsistent**: if S is a set of sentences, just take some sentence in S and add its negation to S. **But this can also happen accidentally; maybe we added an axiom that now, in combination with the other axioms, proves a contradiction...**

The foundations of mathematics should be formal, though; only then can they be formally scrutinised. Hence we look at...

1.1. The axiomatic approach.

Definition 4. *A formal language $\mathcal{L}$ is a set of function, relation, and constant symbols. Relations and functions carry an arity. The language builds* well-formed formulas.

These formulas are what we call *formal mathematical statements.*

Do we **need formal languages to do mathematics**? Most certainly **not**. One can work with groups without referring to the "language of groups". This all works due to GCT.

But to progress, we'll need some formal stuff. Let's talk about models.

E.g. $\mathcal{L}_{Gr} = (*, e)$

$\mathcal{L}_{Fields} = (+, \cdot, 0, 1)$.

- A language builds terms.
- Terms give rise to sentences.
- Sentences are built using very strict *syntactical* rules. **There's no meaning associated to these symbols!**

For instance: $\mathcal{L} = (*, e, f)$. This is a language. We can build well-formed sentences:
- $e + e = e$
- $f + e = e + f$
- $f + f + f = f + f$

We may also introduce *variables* and *quantifiers*:
- $\forall x(x + e = x)$
- $\exists x \exists y(x + y = e)$
- $\forall x \exists y(x + y = e))$

Again, **this does not say anything about truth of these formulas!** It depends how we interpret these symbols.

Interpret $\mathcal{L}$ so that $* = +, e = 0, f = 1$, and the model is the integers $\mathbb{Z}$, then some of these are true, and some are false.

Definition 5. *Let S be a set of sentences. We say that M is a* model *of S if every sentence in S is true in M. We write $M \vDash S$.*

We know what this means, intuitively. Take $\mathcal{L}_{Grp} = (*, e)$, the language of groups. The set of group theory axioms comprises three sentences:

4.

- $\forall x(x * e = x \wedge e * x = x)$ (e is the identity)
- $\forall x, y, z(x(yz) = (xy)z)$ ($*$ is associative)
- $\forall x \exists y(x * y = e \wedge y * x = e)$ (inverses exist)

$-\exists x(x \cdot x = 1 + 1)$ in fields

$-\forall x \exists y (x * y = e)$

$-\forall x (x = e)$ } in groups.

How do we check that $\mathbb{Z}$ under addition is a group? We replace each $*$ above with $+$ and turn e into 0, and then we check that all these sentences are true – **and we do this informally**, which is allowed by GCT.

Equally, we see $(\mathbb{Z}, -, 0)$ is not a group; it's not associative. Or take any other counterexample here. **The point is: we know intuitively what it means to be a model of a set of sentences, even though we don't spell out the definition here.**

What does this have to do with formal proofs? We write $T \vdash S$ if every sentence in S is provable from T. We write $T \vDash S$ if every model of T satisfies S. Now we can restate GCT:

Theorem 6. *$T \vdash S$ if and only if $T \vDash S$.*

So exhibiting models suffice to prove independence.

So if you can prove something *formally*, then it holds in every model (soundness). And if something holds in every model, then we can prove it formally (completeness).

Definition 7. *A theory T is* complete *if for every sentence φ there is a proof of φ or of $\neg\varphi$ from T.*

Some examples: the theory of **DLOs without endpoints** is complete. So e.g. $(\mathbb{R}, <)$ and $(\mathbb{Q}, <)$ are elementarily equivalent. **Presburger arithmetic**; weak theory of elementary number theory including addition but not multiplication, that is also consistent and decidable.

Is **group theory** complete? **No.** Some groups are commutative (the abelian ones), and some are not. So the formal sentence "the structure is commutative" is **neither proven nor refuted from the axioms of groups**.

It's called independent.

Here is an example from geometry: Euclid's postulates of geometry:

(1) A straight line may be drawn between any two points;
(2) Any terminated straight line may be extended indefinitely;
(3) A circle may be drawn with any given center and any given radius;
(4) All right angles are equal;

(5) Let L be a line and P be a point not on L. Then there is exactly one line L' such that L, L' do not intersect.

Euclid lived 300BC!

This *Parallel Postulate* is independent of (1) to (4). Non-Euclidean geometry was the result, its existence deduced in 1823. Euclid tried to prove this one, but couldn't so he added it as an axiom – it is needed to prove that the sum of angles in a triangle (in Euclidean geometry) is 180.

Or in the **theory of fields**: "There exists x such that $x * x = 1 + 1$" cannot be proven from the field axioms. $\mathbb{R}$ satisfies it, but $\mathbb{Q}$ doesn't. Clearly, both are fields.

The natural question now:

Can we make a theory complete by adding enough axioms?

via the Gödel sentence.

No, not in general. Look at Peano arithmetic, or PA, that models elementary number theory as well as induction. Much stronger than Presburger arithmetic. The language is $(+, \cdot, S, <, 0)$. The standard model of PA is $\mathbb{N}$, the natural numbers.

Theorem 8 (Gödel's First Incompleteness Theorem, simplified). *PA is incomplete.*

Corollary 8.1. *Every theory that can interpret PA is incomplete..*

So Hilbert's dream is dead. Any reasonable formalisation of mathematics should really include elementary number theory – but then it will be incomplete.

Here's an outline, all proved in PA: we can code formulas by numbers (effectively): for any formula φ, let $\underline{\varphi}$ be its code.

Theorem 9 (Fixed Point Lemma). *If $\varphi(v)$ is a formula with one free variable v, then there is ψ such that $\mathsf{PA} \vdash \psi \leftrightarrow \varphi(\underline{\psi})$.*

So to check whether ψ holds, we just need to check whether $\varphi(\underline{\psi})$ holds. Now, apart from formulas, we can also code proofs, and logic within the theory. Hence we have a computable predicate

$$\mathrm{IsProofOf}(v, w)$$

with two free variables v, w which expresses that v codes a proof of the formula coded by w.

Now consider the formula

$$\neg\exists x\, \mathrm{IsProofOf}(x, w)$$

where w is free. Hence, by the fixed point lemma, there is a formula ψ such that

$$\mathsf{PA} \vdash \psi \leftrightarrow \neg\exists x\, \mathrm{IsProofOf}(x, \underline{\psi}).$$

Now suppose $\mathsf{PA} \vdash \psi$. Then there is a proof of ψ, yet PA proves there is no proof. Contradiction.

Equally, if $\mathsf{PA} \vdash \neg\psi$ then PA proves $\exists x\, \mathrm{IsProofOf}(x, \underline{\psi})$, so there is a proof of ψ from PA. Contradiction.

We call $\psi = \beta_{\mathsf{PA}}$ the *Gödel sentence* of PA.

But this is quite contrived, isn't it?

Takeaway: independent statements exist, and we have seen many of them:

- the Gödel sentence (in any reasonable and sufficiently strong theory);
- being abelian in the theory of groups;
- solving the equation $X^2 - 2 = 0$ in the theory of fields;

and many more.

And: any theory that formalises (elementary) number theory is necessarily incomplete.

Crucially: we show independence by exhibiting models. And once we have done so, we can stop looking for proofs.

Let's now look for some interesting independence results in set theory.

2. Set Theory

Why set theory? It was an early candidate for providing foundations for mathematics. Early *natural* attempts at formalising what it means to be a set failed.

Theorem 10. *Naive set theory is inconsistent.*

Proof. What we mean by naive here is exemplified in what is now known as Russell's paradox. Let $S = \{x \mid x \notin x\}$. Now we have

$$S \in S \leftrightarrow S \notin S$$

a contradiction. □

In some sense, naive set theory is not restrictive enough. We resolve this by formalising things, by introducing the formal language of set theory.

We put forward: **Axiomatic set theory**, which should really be called *Universe theory*.

In this theory, elements of its structures are called sets. There is one relation symbol: $\in$. The set of axioms we pick is called ZFC. **Just like groups: we have a set of axioms, we are interested in models.**

What do we expect from sets? For instance:

- $x = y$ iff they have the same elements;
- if x, y are sets then so should be $\{x, y\}$;
- if x is a set, then its power set should exist;
- if x is a set, then the set containing all the elements of x, i.e. $\bigcup x$ should exist;
- if x is a set and φ is a property, then $\{y \in x \mid \varphi(y)\}$ is a set;
- infinite sets should exist.

...as well as Choice:

a combinatorial axiom that ~~whatever~~ says we can pick elements from infinitely many sets "uniformly"

Definition 11. *The* Axiom of Choice *states the following: if $\{X_i \mid i \in I\}$ is a set of non-empty sets, then there is a function f defined on I such that $f(i) \in X_i$.*

ZFC does all that. But ZFC does even more.

2.1. Theorems of ZFC.

ZFC covers **ordinary mathematics**: one can formalise elementary number theory, analysis, etc. Virtually **every mathematical object is formalisable in ZFC.** As a consequence, the Gödel sentence β_{ZFC} will be independent of ZFC. So ZFC **is incomplete.**

Here are some theorems of ZFC:

Theorem 12. *Every set has a size, a* cardinality*: we can assign to any set a unique set called a* cardinal*. Cardinals are well-ordered.*

Socks example

There are infinitely many cardinals. The finite ones are just the natural numbers. $0, 1, 2, 3, \ldots$. The least infinite cardinal is called $\aleph_0$. Every set that is in bijection with $0, 1, \ldots$ is called finite; in bijection with $\aleph_0$ is called countably infinite; in bijection with $\kappa > \aleph_0$ is called uncountable.

Theorem 13. $|\mathbb{N}| = \aleph_0$.

Not all sets are countable.

Theorem 14 (Cantor's Theorem)**.** $|\mathcal{P}(x)| > |x|$.

This is obvious for finite sets, but not for infinite ones. This extends our hierarchy: we have

$$0 < 1 < \ldots < \aleph_0 < \aleph_1 < \ldots$$

with a lot of structure omitted. **But all cardinals appear in this hierarchy, and the hierarchy is linearly ordered!**

There is a nice characterisation of the size of the reals.

Theorem 15. $2^{\aleph_0} = |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$.

We know $|\mathcal{P}(\mathbb{N})| > \aleph_0$. But what is it?

What is the value of $2^{\aleph_0}$? $|\mathcal{P}(\mathbb{N})|$?

2.2. **Models of ZFC.** Let us assume ZFC is consistent.

What does a model of ZFC look like? Everything ZFC proves to be true is true in such a model. For example: ZFC $\vdash$ " there is an uncountable set". Thus if M models ZFC then M contains an uncountable set. Not so fast...

Theorem 16 (Downward Skolem-Löwenheim-Theorem). *If $M \models T$ where M is infinite, and the language of T is countable, then there is a countable model M' of T.*

So if $M \models$ ZFC then Skolem-Löwenheim implies there is a countable model. But it is a theorem of ZFC that there are sets that are not countable. What is going on?

M contains a set that it "believes" is uncountable. So, by definition: if there is no injection from $\mathbb{N}$ into x *in M* then M thinks x is uncountable. But, from the outside, we know that x is not "actually" uncountable.

~~Draw V, and indicate a model M.~~

This is called **Skolem's paradox.**

V is the actual universe, that contains all the actual objects of mathematics. M contains things that it believes are the real numbers, is the power set of the naturals, etc. **Distinction:** $\mathbb{R}$ **versus** $\mathbb{R}^M$.

Independence:

We have seen that ZFC is incomplete: the Gödel sentence is an example. Are there other examples?

Yes! Choice itself is independent of ZF.

1938, GÖDEL

Theorem 17. *If ZF is consistent, then so is ZFC.*

The model exhibited by Gödel that proves this is called the *constructible universe*, found in 1938. So by GCT, there cannot be a proof of $\neg$AC from ZF. Could there be a proof of AC from ZF?

Theorem 18. *If ZF is consistent, then so is ZF+$\neg$AC.* 1963, COHEN.

This is a result of Paul Cohen in 1963. So: **There is no proof of AC and there is no proof of $\neg$AC from ZF.** He employed forcing, which we shall look at soon.

Let's first look at some interesting consequences of this independence.

Just mention this.

2.3. **If Choice fails.** Some statements of ordinary mathematics are equivalent to AC:

- Tychonoff's theorem;
- Trichotomoy of cardinalities;
- Every vector space has a basis;
- Every connected graph has a spanning tree.

Since there is a model of ZF +$\neg$AC, there is a model of set theory *that can formalise virtually all of mathematics* in which there is a collection of compact topological spaces whose product is not compact.

3. Forcing

We assume that ZFC **is consistent**. This gives rise to *relative* consistency results.

We learned that $0 < 1 < 2 < \ldots < \aleph_0 < \aleph_1 < \aleph_2 < \ldots$. We also know that $|\mathcal{P}(\mathbb{N})| \cancel{= 2^{\aleph_0}} > \aleph_0$. What is the value of $2^{\aleph_0}$? It must be a cardinal... but which one is it?

What does CH say?

The *Continuum Hypothesis* says that $\cancel{2^{\aleph_0} =} |\mathcal{P}(\mathbb{N})| = |\mathbb{R}| = \aleph_1$.

What does that mean? If $S \subset \mathbb{R}$ then S has a cardinality (by AC). So if S is infinite then either $|S| = \aleph_0$ or $|S| = |\mathbb{R}| = \aleph_1$. **So there is no set of intermediate cardinality.**

Theorem 19. *The constructible universe satisfies* CH. *So if* ZFC *is consistent so is* ZFC+ CH.

Hence there is no proof of $\neg$CH from ZFC. But is there a proof of CH?

3.1. **What is forcing?** We know what to do: to show that there is no proof of CH from ZFC, it suffices to find a model of ZFC in which CH fails. How can we do that?

Think of **field extensions.** $\mathbb{Q}$ is a field, yet it does not satisfy the sentence

$$\exists x(x * x = 1 + 1)$$

but we can extend $\mathbb{Q}$ (using ring theory, namely the right irreducible polynomial, so its ideal is maximal, so the quotient is a field) to get the extension $\mathbb{Q}[\sqrt{2}]$. Now THAT ring is also a field (so it satisfies the field axioms), but it also satisfies the sentence above.

NOTE: it is not enough to just pick $\mathbb{Q} \cup \{\sqrt{2}\}$ as this is not a ring: it's not closed under addition or multiplication. So we have to make sure the extension is in some sense *closed*. Ring theory tells us that

$$\mathbb{Q}[X]/\langle X^2 - 2\rangle = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

and this is a nice description of the extension.

Two things to note:

- The field extension is indeed a **field**;
- $\mathbb{Q}$ has a way of **describing** its root: it's an element that satisfies $X^2 - 2 = 0$, which is describable in $\mathbb{Q}[X]$.

So now take a nice model M of ZFC: **countable and transitive**. We want to extend it so that it fails CH. What does that mean? We need an extension N such that

Draw V here!

$$N \vDash |\mathcal{P}(\mathbb{N})| > \aleph_1.$$

So if we can somehow find an extension $N \supset M$ that **adds enough subsets of the natural numbers**, then we are done.

Let's start off by adding one subset first. Every subset of the naturals can be expressed as an $\mathbb{N}$-sequence of natural numbers. Hence

E.g.: $(0,1,0,1,0,1,\ldots) \longleftrightarrow \{1,3,5,7,\ldots\}$

$$\mathcal{P}(\mathbb{N}) \cong 2^{\mathbb{N}}$$

3.2. **Cohen Forcing.** Consider the set of finite partial functions from ω to $\{0,1\}$. We denote this set by $\mathbb{P}$. These are **approximations to some new object, that we shall call *generic*.**

Draw bin tree here!

Definition 20. *For finite partial functions $p, q \in \mathbb{P}$, we say $p \leq q$ (has less freedom) iff $q \subset p$.*

Each subset of $\mathbb{N}$ that is in M is a union of such finite partial functions. But we know that $\mathcal{P}(\mathbb{N})^M$ is countable (viewed from the outside). So M misses subsets.

This is like: $\mathbb{Q}$ thinks it contains "all the numbers", when it evidently doesn't (in a sense): $\mathbb{Q} \subset \mathbb{R}$.

How can we add sets?

Definition 21. *A subset $G \subset \mathbb{P}$ is a filter if:*

- *$p \in G$ and $p \leq q$ then $q \in G$;*
- *$p, q \in G$ then there is $r \in G$ such that $r \leq p, q$.*

{finite bin strings} = $\mathbb{P}$.

no common extension.

⇒ So $f_G \in 2^\omega$

DFN: A property φ is called dense in M if (*) for any $p \in \mathbb{P}$ there is $q \leq p$ s.t. $\varphi(q)$.

(*) "M models that"

Draw the complete binary tree, and indicate what a filter can and cannot look like.

Dense properties cannot be avoided

Definition 22. *A subset $D \subset \mathbb{P}$ is called dense if for any $p \in \mathbb{P}$ there is $q \in D$ such that $q \leq p$.*

So **dense sets cannot be avoided!** Finally, a filter is called M-generic if it meets every dense subset of $\mathbb{P}$ that is in M.

For example, the set

$$D_n = \{p \in \mathbb{P} \mid p(n) = 0 \vee p(n) = 1\}$$

is dense (easy check). Equally,

$$E_{m0} = \{p \in \mathbb{P} \mid \exists n > m(p(n) = 0)\}$$

is dense, and the same for E_{m1}. So an M-generic G is not eventually constant.

• "being defined at bit n" is dense (†)

• "differing from $f \in (2^\omega)^M$" is dense.

Theorem 23. *If $\mathbb{P}$ is nice and G is M-generic, then $G \notin M$.*

Compare this with $\sqrt{2}$ not being in $\mathbb{Q}$. We now also see: if $f \in (2^{\mathbb{N}})^M$ then

$$F_f = \{p \in \mathbb{P} \mid \exists n(p(n) \neq f(n))\}$$

is dense.

DFN: f_G is M-generic if f_G satisfies every dense-in-M property.

Now suppose G is M-generic. Then we can construct a model $M[G]$ that extends M by defining *names*. G decides how those names are interpreted, based on its elements. So it depends on G what the elements of $M[G]$ are.

Some facts:

- $M \subset M[G]$;
- $G \in M[G]$;
- $M[G]$ is the least transitive model extension of M containing G;
- M and $M[G]$ have the same ordinals (so they are nicely behaved);
- $M[G]$ is an end-extension: elements in M do not gain new elements ("what about $\mathcal{P}(\mathbb{N})$ and $\mathcal{P}(\mathbb{N})^M$?".

Compare with $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]$.

Theorem 24. *For Cohen forcing, $\bigcup G \in M[G]$ and $\bigcup G \in 2^{\mathbb{N}}$ and differs from every subset of naturals in M.*

Pf: Now follows from (†).

Proof. First part follows from union axiom. Let $f_G = \bigcup G$. Now f_G is defined on all of ω since G meets every D_n. Suppose f_G is not a function; so there is n such that $p, q \in G$ and $p(n) \neq q(n)$. But then p, q have no common extension in G, so G is not a filter. Finally, let $f \in (2^\omega)^M$. Then F_f is dense, so there is $p \in G \cap F_f$. Thus $f_G \neq f$. □

So here we are: we have added a subset of the natural numbers. We say, we have **added a *Cohen real***.

In order to violate CH, we have to add $\aleph_2$-many reals. How could we do that? We build approximations to $\aleph_2$-many new reals, not just one. **Within** M, we look at finite partial functions from ~~$\omega_2 \times \omega$~~ $\aleph_2 \times \aleph_0$ into the set $\{0, 1\}$.

By the same argument, we can show that, in the extension, we get $\aleph_2$-many *distinct* reals. So, the extension $M[G]$ satisfies $|\mathcal{P}(\mathbb{N})| \geq \aleph_2$. Not so fast...

What we have shown is that

$$M[G] \vDash |\mathcal{P}(\mathbb{N})| \geq \aleph_2^M$$

which is not quite what we need. We also have to show that our forcing notion does not *collapse cardinals*: **we need** $\aleph_2^M = \aleph_2^{M[G]}$. *Note that neither of these is the actual $\aleph_2$ which lives in V and is actually uncountable.* Who says we didn't accidentally add a function that maps ω to ω_1^M surjectively? Then ω_1^M would be countable in $M[G]$ so $\omega_2^M \neq \omega_2^{M[G]}$...

We need to ensure that M agrees cardinals in M are still cardinals in $M[G]$... but that can be proven

But this follows from the *countable chain condition*, and is shown combinatorially. This completes the proof:

Theorem 25. *If* ZFC *is consistent, then so is* $\mathsf{ZFC}+\neg\,\mathsf{CH}$.

Set-theoretical forcing is **versatile**: almost any partially ordered set can be a forcing notion. And different forcing notions yield different properties of the generics (computability theory: n-generics, for example).

Some relative consistency results due to forcing. Assuming consistency of the ZFC-fragment, also consistent is:

- $\mathsf{ZFC}+\neg\,\mathsf{GCH}$ (follows straight from the above);
- $\mathsf{ZF}+V \neq L$;
- $\mathsf{ZF}+\mathsf{LM}$ (Solovay model; every set of reals is Lebesgue measurable; cannot satisfy AC since Vitali's construction uses AC to find sets that aren't measurable; this actually also needs an inaccessible (so large) cardinal axiom);
- Kleene-Post theorem; the fact that there are incomparable Turing degrees is essentially a forcing argument (but predates Cohen's results, so wasn't immediately recognised as such).

Note that models of all of these theories still model all of mathematics!

Limitations of forcing: we can only add sets, not take any away; we are looking at extensions after all. So for example, we will never be able to turn a countable set uncountable.

But its power lies in its **combinatorial** structure, and the fact that we can define partial orders ad hoc whenever needed, and use its conditions as approximations to build the generic we need.