18 April 2017

Independence

A formula F is called independent of some theory if that theory is unable to assign a truth value to the formula.

Example: Axiom 0 of "Zermelo-Fraenkel set theory with choice" (ZFC) is technically **not** independent from Axioms 1-7 (but we did not observe this directly).

Example: Axiom 8 of "Zermelo-Fraenkel set theory" is independent of Axioms 0-7.

Example: Axiom 9 of "Zermelo-Fraenkel set theory with choice ("ZFC") is independent of Axioms 0-8. We would say it is "independent of Zermelo set theory" and we would say that it is independent of "Zermelo-Fraenkel set theory".

When is an axiom independent of other axioms?

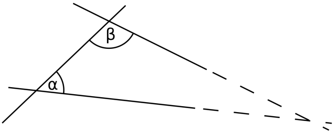
We use interpretations for this!

If we want to show "Axiom n" of a theory is independent of all the other axioms of the theory, all we must do is find an interpretation that makes "Axiom n" false while keeping the remaining axioms true.

Euclidean Geometry

Informally: the axioms of "Euclidean geometry", as Euclid wrote it, are:

1. A line segment can be formed by any two points.
2. A(n infinite) line can be formed from any line segment.
3. Given any line segment, a circle can be drawn having that segment as a radius and one endpoint as its center.
4. All right angles are equal.
5. ("Parallel postulate") If a line segment intersects two straight lines forming two interior angles on the same side that sum to less than 2 right angles, then the two lines (if extended indefinitely) meet on that side which the angles sum to less than two right angles.



Axiom 5 “feels like” a statement that could be proven from Axioms 1-4.

Consequently: mathematicians starting in Euclid’s time tried to prove it from Axioms 1-4 for thousands of years...

Their efforts ended in failure! Led to... projective geometry, spherical geometry, hyperbolic geometry, and other “non-Euclidean” geometries...

Finite geometries - five-point geometry

We have three axioms:

1. there are exactly five points
2. each two distinct points have exactly one line on both of them
3. each line has exactly two points

Theorem: There are exactly 10 lines.

Theorem: Each point touches exactly four lines.

Finite geometries – five-point geometry

- Create an interpretation to show that Axiom 1 is independent of Axioms 2 and 3
- Create an interpretation to show show Axiom 2 is independent of Axioms 1 and 3
- Create an interpretation to show show Axiom 3 is independent of Axioms 1 and 2

Finite geometries – four-line geometry

We have three axioms:

1. there exist exactly four lines
2. any two distinct lines have exactly one point in common
3. each point lies on exactly two lines

Theorem: There are exactly six points.

Theorem: Each line contains exactly three points.

Consistency and completeness

A theory is called consistent if it does **not** derive a contradiction. A theory is called complete if every sentence (or its negation) has a proof in that theory (i.e. nothing is "undecidable"). A desirable goal: to have an axiomatic system be both complete and consistent.

Example: "Naive set theory" is **not** consistent because we were able to derive a contradiction from it (Russell's paradox).

Example: We ~~**don't know**~~ **cannot tell** whether or not "first order arithmetic" is consistent (from inside of first order arithmetic...).

Consistency and completeness

The following theory, called Presburger arithmetic, is a complete and consistent theory of (additive) arithmetic with a single one-term predicate S ("successor") and a two-term predicate $+$:

1. $(\forall x)\neg(0 = Sx)$
2. $(\forall x)(\forall y)(Sx = Sy \rightarrow x = y)$
3. $(\forall x)(x + 0 = x)$
4. $(\forall x)(\forall y)(x + Sy = S(x + y))$
5. (Induction Schema) For any first predicate Px, the following is an axiom:

$$(P(0) \wedge (\forall x)(Px \rightarrow P(Sx))) \rightarrow (\forall y)(Py)$$

There is, in fact, a "decision procedure" that can be used to determine if a given formula F is true or false in Presburger arithmetic! However, Presburger arithmetic is "weak" in that it cannot even define prime numbers (or multiplication, in general). (also see "Skolem Arithmetic")

Peano Arithmetic

Note: axioms 1-7 match "first order arithmetic"; axiom 8 is "induction"

1. $(\forall x)\neg(0 = Sx)$
2. $(\forall x)(\forall y)(Sx = Sy \to x = y)$
3. $(\forall y)(y = 0 \lor (\exists x)(Sx = y))$
4. $(\forall x)(x + 0 = x)$
5. $(\forall x)(\forall y)(x + Sy = S(x + y))$
6. $(\forall x)(x \cdot 0 = 0)$
7. $(\forall x)(\forall y)(x \cdot Sy = (x \cdot y) + x)$
8. (Induction schema) For any predicate Px, the following is an axiom:

$$(P(0) \land (\forall x)(Px \to P(Sx))) \to (\forall y)(Py).$$

Is Peano arithmetic consistent?

Next time... a summary of what Gödel showed us...

Hilbert's 23 Problems

Problem	Resolved?
1. the "continuum hypothesis"	Shown independent of ZFC by Gödel (provided an interp. of ZFC where CH true) and Cohen (provided an interp. of ZFC where $\neg CH$ is true)
2. prove arithmetic is consistent	Gödel showed arithmetic can't prove itself consistent (1931), Gentzen showed it is consistent (provided some other theory is consistent)
3. can any two polyhedra be cut up and rearranged into each other?	no, proven by Max Dehn (1900)
4. finding metrics whose lines are geodesics	multiple interpretations of meaning with various levels of resolution
5. are continuous groups differential groups?	multiple interpretations of meaning with various levels of resolution

Hilbert's 23 Problems

Problem	Resolved?
6. find "axioms of physics"	partially answered for certain physics (probabilities $\rightarrow$ Kolmogorov)
7. question on "transcendental" numbers	yes, "Gelfond-Schneider theorem" (1934)
8. "Riemann hypothesis" and friends	no, and its solution is worth $\$1,000,000$
9. question about "quadratic reciprocity"	partially solved
10. find an algorithm to solve a "Diophantine equation"	false, "Matiyasevich's theorem" (1970)
11. question on "quadratic forms"	partially solved

Hilbert's 23 problems

Problem	Resolved?
12. question on generalizing the "Kronecker-Weber" theorem	unresolved
13. a question about the solution of $x^7 + ax^3+bx^2+cx+1=0$	partially solved
14. question about "ring of invariants of an algebraic group"	yes (counterexample by Masayoshi Nagata 1959)
15. make "Schubert's enumerative calculus" rigorous	partially solved
16. question about "real algebraic curves" in the plane	unresolved

Hilbert's 23 problems

Problem	Resolved?
17. write rational functions in terms of quotients of sums of squares	proven by Emil Artin (1927)
18. two questions about tilings and sphere packings	tilings problem resolved by Reinhardt (1928), sphere packings resolved by *computer assisted proof* by Hales (1998)
19. question about "calculus of variations"	solved independently by Giorgi and by Nash (fellow West Virginian!) (1957)
20. question about "variational problems"	answered over time
21. question about "mondronomy"	depends on how it's stated

Hilbert's 23 problems

Problem	Resolved?
22. question about "automorphic functions"	answered
23. make "calculus of variations" better	work in progress
(24.) how should a "simple proof" be defined?	