Lecture 5

Vaught's test
application of compactness to RG and ACF_0

Topics

- from completeness to decidability (HW problem)
- formulation of the Lowenheim-Skolem theorem down (a proof in Lect.6)
- Vaught's test and its proof
- two particular complete theories: RG and ACF_0
- 0-1 law for finite graphs
- the Ax-Grothendieck theorem on polynomial maps on the complex field

from completeness to decidability

The HW problem was to devise - using the fact that ACF_0 is complete - an algorithm that decides whether or not a sentence is a logical consequence of the theory.

Idea:
By the Completeness thm $ACF_0 \models \varphi$ is equivalent to $ACF_0 \vdash \varphi$ and hence the completeness of ACF_0 means that for all φ

$$ACF_0 \vdash \varphi \text{ or } ACF_0 \vdash \neg\varphi.$$

Algorithm: enumerate systematically all finite sequences of symbols in the language of ACF_0 (plus the common FO symbols) until you find a valid proof of either φ or of $\neg\varphi$.

HW cont'd

For this to work you have to be able to algorithmically verify various syntactic notions:

- a string is a term, a formula, ...,
- a fla is a valid logical axiom (propositional, quantifier or equality ax.),
- a fla was derived using a valid inference rule,
- a fla is an axiom of ACF_0.

The first three items can be algorithmically decided because they have a schematic character: e.g. a valid use of modus ponens

$$\frac{\alpha \qquad \alpha \to \beta}{\beta}$$

means that the 2nd fla is an implication whose antecedent is the 1st fla and whose succedent is the bottom fla, i.e. you need to check that some strings are flas and that a string equals to a substring, etc.

HW cont'd

To be able to algorithmically verify also the last condition:

- a fla is an axiom of ACF_0

note that ACF_0 has some finite number of ad hoc axioms (Fields) which the algorithm can remember, plus two infinite sets of axioms:

- $\forall x_0, \ldots, x_n \exists y \; (x_n \neq 0 \to \sum_{i \leq n} x_i y^i = 0)$, all $n \geq 1$,
- $0 \neq 1 + \cdots + 1 \;\; (p\text{-times})$, all primes p

which are also "schematic" and easy to recognize.

Theorem

Let T be a theory in a finite language whose set of axioms (i.e. T) is algorithmically decidable (these theories are also called recursive).
If T is complete then it is decidable: there is an algorithm deciding if a sentence is a logical consequence of T.

Lowenheim-Skolem thm

In the proof of Vaught's test we shall need the following special case of the Lowenheim-Skolem thm: we shall prove it in Lect.6 (we proved the upwards L.-S. thm. already but this needs the downwards version).

The Lowenheim-Skolem thm.

Let T be a theory in a countable language which has an infinite model. Then T has models of all infinite cardinalities.

Vaught's test

Last time we formulated

Vaught's test

Let T be a satisfiable theory in a countable language that has no finite models.
If T is categorical in some (infinite) power then it is complete.

and we need to prove it now.

Recall important

Corollary

All theories DLO, RG, SUC, $Vect_Q$ and ACF_p (any p) are complete.

prf of Vaught's test

Prf.:
Assume for the sake of a contradiction that T satisfies the hypothesis of Vaught's test and, in particular, is κ-categorical, but is not complete:

- for some sentence φ neither the sentence nor its negation are logical consequences of T.

By the completeness thm. this means that both theories

$$T_1 := T + \varphi \text{ and } T_0 := T + \neg\varphi$$

have some models **A** and **B**, and because T has no finite models both **A** and **B** are infinite. Hence by the Lowenheim-Skolem thm. both T_1 and T_0 have models of size κ but these - as they are, in particular, models of T - must be isomorphic.
But that is a contradiction because they are not elem.equivalent.

□

injective maps

Consider

$$F : U \rightarrow U$$

where U is infinite. We can always choose such F injective but not surjective.

We shall study the situation when there is an additional requirement on F and U: U is a universe of a structure and F ought to be definable in it.

Our example:

- the complex field $\mathbf{C} := (C, 0, 1, +, \cdot)$ and $U := C^n$,
- polynomial maps:

  $$F \ : \ C^n \rightarrow C^n$$

  where

  $$F(z_1, \ldots, z_n) \ := \ (f_1(\overline{z}), \ldots, f_n(\overline{z}))$$

  with f_i being polynomials over $\mathbf{C}$.

Ax-Grothendieck

The Ax-Grothendieck theorem

If a polynomial map $F : C^n \to C^n$ is injective then it is also surjective.

Towards a formalization: injectivity can be written as

$$Inj(f_1, \ldots, f_n) \;\Leftrightarrow_{df}\; \forall x_1, \ldots, x_n, y_1, \ldots, y_n \, (\bigvee_i x_i \neq y_i \to \bigvee_j f_j(\overline{x}) \neq f_j(\overline{y}))$$

and surjectivity as

$$Sur(f_1, \ldots, f_n) \;\Leftrightarrow_{df}\; \forall v_1, \ldots, v_n \exists u_1, \ldots, u_n \, \bigwedge_j f_j(\overline{u}) = v_j$$

formalization

Hence the thm can be written as

$$\forall n \geq 1 \forall f_1, \ldots, f_n \in \mathbf{C}[z_1, \ldots, z_n] \; Inj(f_1, \ldots, f_n) \to Sur(f_1, \ldots, f_n) \; .$$

Difficulty: this is not FO. We cannot quantify over n or over polynomials f_i.

Idea: formalize the statement separately for each fixed $n, d \geq 1$ by representing degree $\leq d$ polynomials in n variables by their coefficients.

ex

For example, consider $n = d = 2$. Polynomials in 2 variables z_1, z_2 of degree ≤ 2 have only six possible monomials

$$1,\ z_1,\ z_2,\ z_1^2,\ z_1 z_2,\ z_2^2\ .$$

(In general there are $\binom{n+d}{d}$ of them.) Hence such f is determined by six coefficients $w_0, w_1, w_2, w_{11}, w_{12}, w_{22}$ as:

$$f(z_1, z_2) := w_0 \cdot 1 + w_1 \cdot z_1 + w_2 \cdot z_2 + w_{11} \cdot z_1^2 + w_{12} \cdot z_1 z_2 + w_{22} \cdot z_2^2\ .$$

Instead of writing $\forall f\ (f(z_1, z_2)$ has property $\ldots)$ we can now write

$$\forall w_0, w_1, w_2, w_{11}, w_{12}, w_{22}$$

$$(w_0 \cdot 1 + w_1 \cdot z_1 + w_2 \cdot z_2 + w_{11} \cdot z_1^2 + w_{12} \cdot z_1 z_2 + w_{22} \cdot z_2^2 \text{ has } \ldots)$$

final formalization

$\Phi_{n,d}$: the formalization of the Ax-Grothendieck theorem for polynomials in n variables and of degree $\leq d$

$$\text{Ax-Grothendieck} \quad \Leftrightarrow \quad \text{all axioms } \Phi_{n,d},\ n, d \geq 1$$

a proof

Prf.:
Assume for the sake of a contradiction that the theorem is false and that there is some polynomial map $F : C^n \to C^n$ of degree d that violates it. In particular,

$$\mathbf{C} \models \neg\Phi_{n,d} \ .$$

By the completeness of ACF_0:

$$ACF_0 \models \neg\Phi_{n,d} \ .$$

prf cont'd

Now we remember that ACF_0 can be written as

$$T \; + \; \{char \; \neq p \mid \; \text{all primes} \; \; p\}$$

where

$$T \; := \; Fields + \; \text{axioms that the field is alg.closed}$$

Applying now the compactness we get

$$T + \{char \; \neq p \mid p \in P\} \; \models \; \neg\Phi_{n,d}$$

where P is some finite set of primes.

prf cont'd

Choose a prime $q \notin P$. Then it is easy to see that for all $p \neq q$:

$$\text{Fields} \models (char = q) \to (char \neq p)\ .$$

Thus we have:

$$T + char = q \models \neg\Phi_{n,d}$$

i.e.

$$ACF_q \models \neg\Phi_{n,d}\ .$$

We shall bring this statement to a contradiction.

prf cont'd

Algebraic fact:

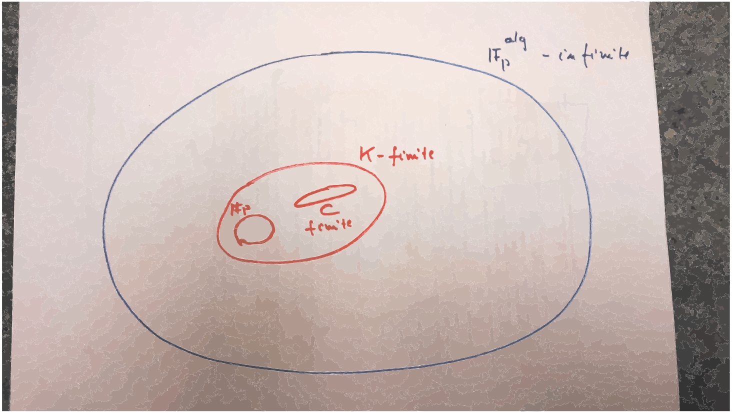
$(\mathbf{F}_q)^{alg}$, the algebraic closure of $\mathbf{F}_q$, is locally finite: all finitely generated subfields are finite.

We have $(\mathbf{F}_q)^{alg} \models \neg\Phi_{n,d}$ so there are some elements witnessing the $\exists$ quantifiers:

- coefficients defining the map F violating $\phi_{n,d}$,
- n coordinates of a point in the n-fold Cartesian power that is not in the range of F.

Define a subset set C of the universe: all these coefficients and coordinates. It is finite.

locally finite



prf end

Take a subfield K of $(\mathbf{F}_q)^{alg}$ generated by C, and note:

- because all coefficients of F are in K, K is closed under F and hence

$$F \ : K^n \to K^n \ ,$$

- F is injective on K^n (because it is even injective in a bigger structure $(\mathbf{F}_q)^{alg}$).

Key fact: Every injective map from a finite set into itself must be surjective!

Hence all points in K^n must be in $Rng(F)$ but that contradicts the choice of C: we have included coordinates of a point that is not in the range even in the whole of $(\mathbf{F}_q)^{alg}$.

$\square$

HW problem

a problem to take away:

The final step in the proof was the observation that

$$\text{injective} \quad \Rightarrow \quad \text{surjective}$$

holds for maps on a finite set.
However, this is true also for the opposite implication

$$\text{surjective} \quad \Rightarrow \quad \text{injective}$$

but the theorem does not hold: consider map

$$z \longrightarrow z^2 \ .$$

Find the place in the proof which breaks down in this case.

We shall consider FO properties of finite, simple, undirected graphs without loops.

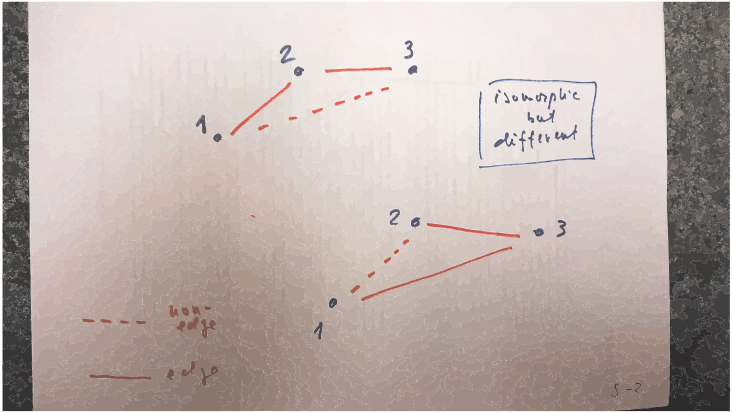
language: $R(x, y)$ (as in theory RG)
structure: sets with irreflexive and symmetric R

We are interested in the following informal question:

- Given a sentence φ, how likely it is that a graph will satisfy it?

$\mathcal{G}_n$: all graphs with the universe $\{1, \ldots, n\}$
Important: isomorphic but different graphs are considered different!

pic



probabilistic model

We shall define two quantities (probabilities):

$$\mathrm{Prob}_n[\varphi] \;:=\; \frac{|W(\varphi)|}{|\mathcal{G}_n|} = |W(\varphi)| \cdot 2^{-\binom{n}{2}}$$

where

$W(\varphi)$: the set of all $G \in \mathcal{G}_n$ satisfying φ

$$\mathrm{Prob}[\varphi] \;:=\; \lim_{n \to \infty} \mathrm{Prob}_n[\varphi]\;, \quad \text{if it exists}$$

alternative prob. model

Assume that we create a graph in $\mathcal{G}_n$ by choosing for each pair of different vertices whether to include edge or non-edge by throwing a random coin: with probability $1/2$ include the edge, with probability $1/2$ do not include it.

There are $\binom{n}{2}$ different outcomes of how the coin produces (non-)edges: all graphs in $\mathcal{G}_n$ appear in exactly one such random experiment.

We study: How likely it is that a random experiment produces a graph satisfying φ?

This model gives the same probabilities as the first one.

almost sure theory

Theorem

- The 0-1 law: For every φ, $\mathrm{Prob}[\varphi]$ exists and equals to 0 or 1.
- The almost sure theory of graphs:

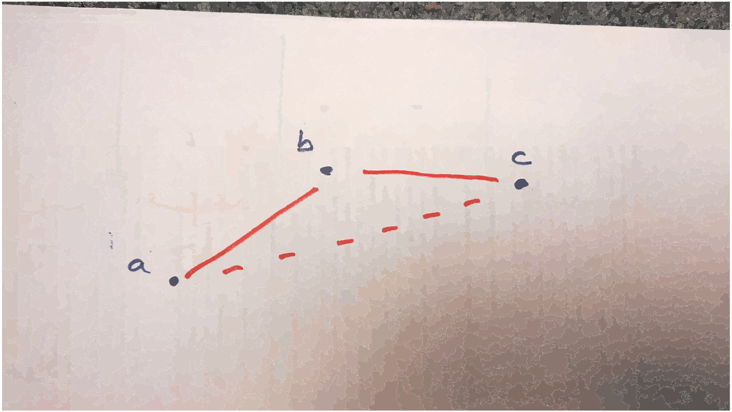
$$\{\varphi \mid \mathrm{Prob}[\varphi] = 1\}$$

is complete and decidable.

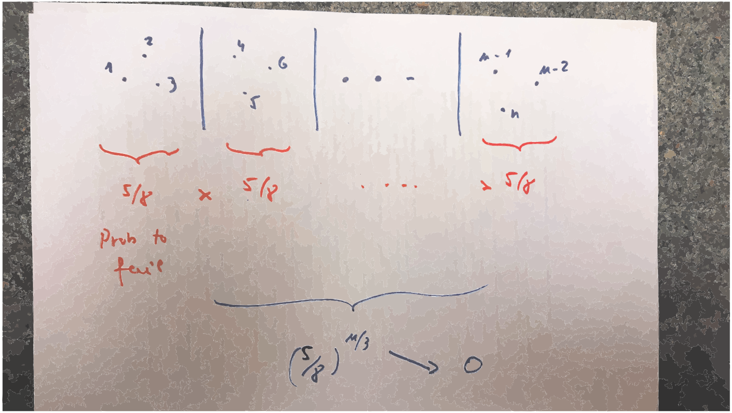
First item due to Glebskii et.al., our proof follows Fagin's.

ex.

$$\varphi \ := \ \exists x, y, z,\ x \neq y \neq z \neq x \wedge R(x,y) \wedge R(y,z) \wedge \neg R(x,z)$$



a computation



$\exists$ sentences

More generally: if φ has the form

$$\exists x_1, \ldots, x_k \ (\ldots \text{ open fla } \ldots)$$

then

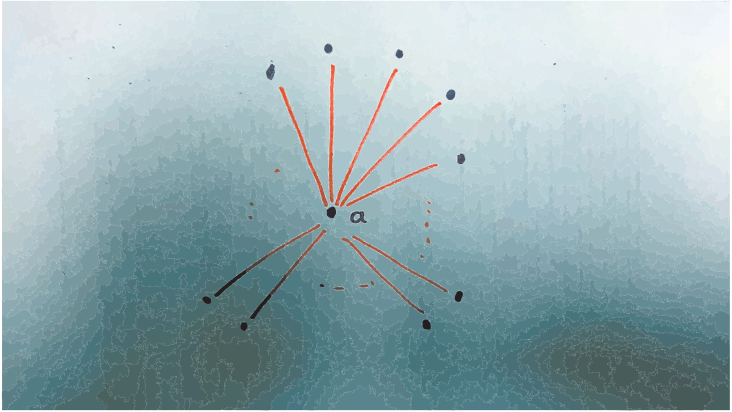
- either φ is not satisfiable and then $\text{Prob}[\varphi] = 0$, or
- $\text{Prob}[\varphi] = 1$.

Even if just one of $2^{\binom{k}{2}}$ configurations on k points witnesses φ it will occur with probability $\to 1$ as $n \to \infty$ (same calculation as before).

Analogously: universal sentences are either logically valid (and then have probability 1) or their probability $\to 0$.

more quantifiers

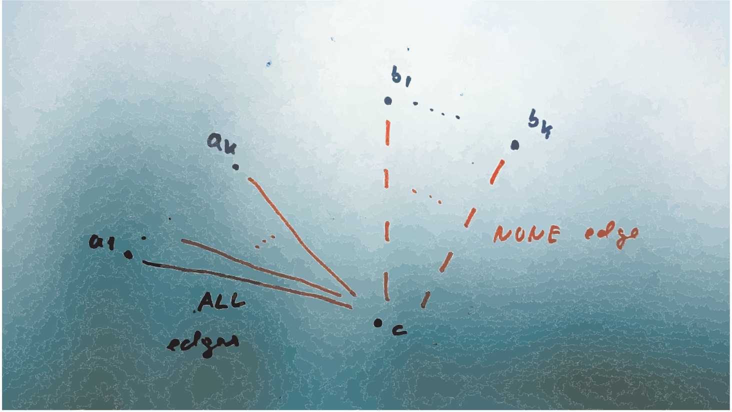
$$\varphi \;:=\; \exists x \forall y\ (x \neq y \rightarrow R(x,y))$$



$$\mathrm{Prob}_n[\varphi] \;\leq\; n \cdot 2^{-(n-1)} \longrightarrow 0$$

ext. axioms

Recall the extension axioms Ex_k of theory RG:



key lemma

We are going to to show that RG equals to the almost sure theory of graphs.

Key lemma

For any fixed $k \geq 1$: $\mathrm{Prob}[Ex_k] = 1$.

Prf.:

$$\mathrm{Prob}_n[\forall z \ \ (z \text{ is not a witness for } \overline{a}, \overline{b})\ ] \leq (1 - 2^{-2k})^{n-2k}$$

as for different c these are independent events.

Hence:

$$\mathrm{Prob}_n[\neg Ex_k] \leq n^{2k} \cdot (1 - 2^{-2k})^{n-2k} \to 0$$

$\square$

a prf of the thm

Let φ be any sentence. Because RG is complete

- (a) either $RG \models \varphi$, or
- (b) $RG \models \neg\varphi$.

Assume (a) holds (the case of (b) is analogous).

By compactness there is $k \geq 1$ such that

$$(R \text{ irrefl. and symmetr. }) \; + \; Ex_k \;\; \models \;\; \varphi$$

But by the key lemma $\mathrm{Prob}_n[Ex_k] \to 1$ and in all graphs where Ex_k holds also φ must hold. Hence:

$$\mathrm{Prob}[\varphi] \;=\; 1\;.$$

$\square$ (thm)