On One Variable Fragment of First Order Logic with Modulo Counting Quantifiers

Bartosz Bednarczyk

bbednarczyk@stud.cs.uni.wroc.pl
Institute of Computer Science
University of Wrocław
Wrocław, Poland

Toulouse, July 20, 2017

~~On One Variable Fragment of First Order Logic with Modulo Counting Quantifiers~~
A few words about logics with modulo counting

Bartosz Bednarczyk

bbednarczyk@stud.cs.uni.wroc.pl
Institute of Computer Science
University of Wrocław
Wrocław, Poland

Toulouse, July 20, 2017

Agenda

- Some historical results about FO and related logics
- A little about my current work
- Motivation example - modal logic $\mathrm{K5}$ with modulo modalities
- Satisfiability of $\mathrm{FO}^1_{\mathrm{MOD}}$
- A few minutes for questions

Basic facts about SAT and fragments of FO

- We are interested in (finite) satisfiability problems
- Models $=$ relational structures, no constants, no functions

Basic facts about SAT and fragments of FO

- We are interested in (finite) satisfiability problems
- Models = relational structures, no constants, no functions
- Some classical results:
  - FO undecidable (Church, Turing; 1930s)
  - FO^3 undecidable (Kahr, Moore, Wang; 1959)
  - FO^2 decidable (Mortimer; 1975)
  - FO^2 exponential model property (Gradel, Kolaitis, Vardi; 1997)
    Hence, FO^2 is $\mathrm{NE{\scriptsize XP}T{\scriptsize IME}}$-completeness

Basic facts about SAT and fragments of FO

- We are interested in (finite) satisfiability problems
- Models = relational structures, no constants, no functions
- Some classical results:
  - FO undecidable (Church, Turing; 1930s)
  - FO^3 undecidable (Kahr, Moore, Wang; 1959)
  - FO^2 decidable (Mortimer; 1975)
  - FO^2 exponential model property (Gradel, Kolaitis, Vardi; 1997) Hence, FO^2 is NExpTime-completeness
  - Even when the expressive power of FO^2 seems to be limited, there are many connection between FO^2 and modal, temporal, descriptive logics; many applications in verification and databases
  - FO^1 is NPTime-complete (Folklore)

Special structures

- What happens if we restrict the class of structures to words or trees?

Special structures

- What happens if we restrict the class of structures to words or trees?
- FO and MSO become decidable (Rabin; 1969).
- The complexity is non-elementary even for FO^3 (Stockmeyer; 1974).
- Complexity for FO^2 on words and trees - next slide

FO^2 words and trees

- No additional binary predicates
  - $\mathrm{FO}^2[+1, \leq]$ on words is $\mathrm{NExpTime}$-complete (Etessami, Vardi, Wilke; 2002).
  - $\mathrm{FO}^2[\downarrow, \downarrow^+, \rightarrow, \rightarrow^+]$ on trees is $\mathrm{ExpSpace}$-complete (Benaim, Benedikt, Charatonik, Kieronski, Lenhardt, Mazowiecki, Worrell; 2013).
- Additional binary predicates
  - $\mathrm{FO}^2[+1, \leq, \tau_{bin}]$ on words is $\mathrm{NExpTime}$-complete (Thomas Zeume, Frederik Harwath; 2016).
  - $\mathrm{FO}^2[\downarrow, \downarrow^+, \rightarrow, \rightarrow^+, \tau_{bin}]$ on trees is $\mathrm{ExpSpace}$-complete (Bartosz Bednarczyk, Witold Charatonik, Emanuel Kieronski, to appear CSL 2017).
- $\downarrow$ - child relation, $\rightarrow$ - right sibling relation, $+1$ successor

What next?

We will add counting quantifiers to increase expressive power.

C - logic with counting

- We add quantifiers of the form $\exists^{\leq n}, \exists^{\geq n}$ to the logic
- Numbers in quantifiers are encoded in binary (!!!)
- $\mathrm{C}=\mathrm{FO}$ is of course undecidable
- Lots of problems with C^2:
  - C^2 is decidable (Erich Gradel, Martin Otto, Eric Rosen, 1997)
  - C^2 is in 2–NEXPTIME (Leszek Pacholski, Wieslaw Szwast, Lidia Tendera; 1997)
  - C^2 is in NEXPTIME-complete (Ian Pratt-Hartmann, 2004)
  - Simplier proof via linear programming (Ian Pratt-Hartmann, 2010)
- C^1 is NPTIME-complete (Ian Pratt-Hartmann, 2007)
- What about words and trees?

C^2 words and trees

- No additional binary predicates
  - $\mathrm{C}^2[+1, \leq]$ on words is $\textsc{NExpTime}$-complete (Witold Charatonik, Piotr Witkowski; 2015).
  - $\mathrm{C}^2[\downarrow, \downarrow^+, \rightarrow, \rightarrow^+]$ on trees is $\textsc{ExpSpace}$-complete (Bartosz Bednarczyk, Witold Charatonik, Emanuel Kieronski, to appear CSL 2017).
- Additional binary predicates
  - $\mathrm{C}^2[+1, \leq, \tau_{bin}]$ on words is VASS-complete (Witold Charatonik, Piotr Witkowski; 2015).
  - $\mathrm{C}^2[\downarrow, \downarrow^+, \rightarrow, \rightarrow^+, \tau_{bin}]$ on trees is super hard - harder than VATA (Bartosz Bednarczyk, Witold Charatonik, Emanuel Kieronski, to appear CSL 2017).
- $\downarrow$ - child relation, $\rightarrow$ - right brother relation, $+1$ successor

Summary

Adding counting is hard and requires years of research

Modulo counting quantifiers

- Parity is a very simple property not expressible in FO
- We add to the logic quantifiers of the form $\exists^{=a \pmod{b}}$
- Current research involves:
  - equivalences of finite structures
  - locality
  - databases with modulo queries
  - definable tree languages
  - definability of regular languages on words and its connections to algebra
  - and other topics
- Surprisingly, satisfiability almost untouched

Our current results and research plans

- $\mathrm{FO}^1_{\mathrm{MOD}}$ is $\mathrm{NP}\textsc{Time}$-complete (Bartosz Bednarczyk; ESSLLI StuS 2017; this talk)
- $\mathrm{FO}^2_{\mathrm{MOD}}$ is $\textsc{ExpSpace}$-complete over words and 2–$\textsc{ExpTime}$ complete over trees (Bartosz Bednarczyk, Witold Charatonik; 2017; submitted)
- Current research plans:
  - Modal logic with modulo modalities over various kind of frames
  - $\mathrm{FO}^2_{\mathrm{MOD}}$ on arbitrary structures
  - Consider weaker frameworks like $\mathrm{GF}^2_{\mathrm{MOD}}$

Today's motivation

Modal logic with modulo modalities

Modal logic ML- basics

- Syntax

$$\varphi ::= p \in \Sigma \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \Box\varphi \mid \Diamond\varphi$$

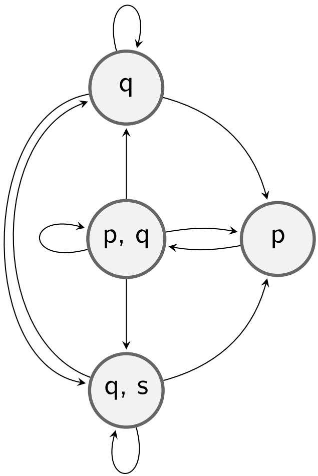
- Structures, worlds, satisfaction
  - $\mathfrak{W}$ - structure with its domain W (worlds), Σ signature,
  - $R \subseteq W \times W$ access relation
- Sometimes we additionally require relation R to be:
  - reflexive $\forall x\ R(x, x)$
  - serial $\forall x \exists y R(x, y)$
  - symmetric $\forall x \forall y\ R(x, y) \rightarrow R(y, x)$
  - transitive $\forall x \forall y \forall z\ R(x, y) \wedge R(y, z) \rightarrow R(x, z)$
  - Euclidean $\forall x \forall y \forall z\ R(x, y) \wedge R(x, z) \rightarrow R(y, z)$

Satisfaction relation $\models$.

1. $\mathfrak{W}, w \models p$, iff $w \in p^{\mathfrak{W}}$
2. $\mathfrak{W}, w \models \neg\varphi$, iff not $\mathfrak{W}, w \models \varphi$
3. $\mathfrak{W}, w \models \varphi \wedge \psi$,
   iff $\mathfrak{W}, w \models \varphi$ and $\mathfrak{W}, w \models \psi$
4. $\mathfrak{W}, w \models \Box\psi$,
   iff $\mathfrak{W}, w \models \varphi$ or $\mathfrak{W}, w \models \psi$
5. $\mathfrak{W}, w \models \Box\psi$,
   iff $\forall v \in W$ s. t. $R(w, v)$ we have $\mathfrak{W}, v \models \varphi$
6. $\mathfrak{W}, w \models \Diamond\psi$,
   iff $\exists v \in W$ s. t. $R(w, v)$ we have $\mathfrak{W}, v \models \varphi$

Example structure

$$\mathfrak{W} = (\Sigma = \{p, q\}, W, R)$$



Modulo-graded Modal logic - syntax

- Syntax

$$\varphi ::= p \in \Sigma \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \Box\varphi \mid \Diamond\varphi \mid \Diamond_{\mathbf{a,b}}\, \varphi$$

$\mathfrak{W}, w \models \Diamond_{a,b}\, \varphi$, iff there **exists exactly** a **mod** b **worlds** $v \in W$, such that $R(w, v)$ and $\mathfrak{W}, v \models \varphi$

- Satisfiability problem

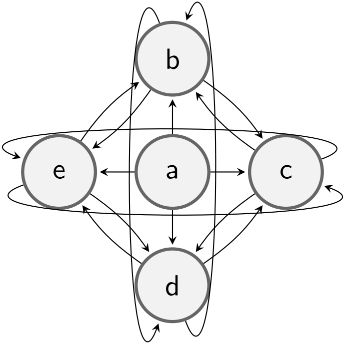
(Local) Satisfiability problem

Given a modulo-graded modal logic formula φ. Is there a structure $\mathfrak{W}$ and a world $w \in W$, such that $\mathfrak{W}, w \models \varphi$?

- Goal of this talk: R is Euclidean $\Rightarrow$ LocalSat is NPTIME-complete

Example Euclidean structure

Euclidean property:$\forall x \forall y \forall z\ R(x, y) \wedge R(x, z) \rightarrow R(y, z)$



Let's focus on the main topic

$\mathrm{FO}^1_{\mathrm{MOD}}$ is $\mathrm{NP}\textsc{Time}$-complete

Language examples for $\mathrm{FO}^1_{\mathrm{MOD}}$

Every ESSLLI participant speaks English, French or German

$$\forall x(\mathsf{English}(x) \vee \mathsf{French}(x) \vee \mathsf{German}(x))$$

Someone speaks both French and German

$$\exists x(\mathsf{French}(x) \wedge \mathsf{German}(x))$$

Every speaker of German speaks English

$$\forall x(\mathsf{German}(x) \rightarrow \mathsf{English}(x))$$

The number of Polish speakers is even.

$$\exists^{=0 (\mathrm{mod}\ 2)} x\ (\mathsf{Polish}(x))$$

$\mathrm{FO}^1_{\mathrm{MOD}}$ - basics

- Syntax

$$\varphi ::= p \in \Sigma \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \forall x \varphi(x) \mid \exists x \varphi(x) \mid \exists^{\bowtie a (\mathrm{mod}\ b)} x\ \varphi(x)$$

- $\exists^{\bowtie a (\mathrm{mod}\ \infty)}$ is an abbreviation of $\exists^{\bowtie a}$
- Formal description of modulo counting quantifiers

$$\mathfrak{M} \models \left(\exists^{\bowtie a (\mathrm{mod}\ b)}\ x\ \varphi(x)\right) \overset{\mathrm{def}}{\iff}$$

$$\exists r \in \mathbb{Z}_b\ |\{x \in M : \varphi(x)\}| \equiv r \pmod{b} \wedge r \bowtie a,$$

where $\bowtie \in \{\leq, =, \geq\}$.

$\mathrm{FO}^1_{\mathrm{MOD}}$ - normal form

Definition

We say that a formula $\varphi \in \mathrm{FO}^1_{\mathrm{MOD}}$ is *flat*, if:

$$\varphi = \bigwedge_{i=1}^{n} \exists^{\bowtie_i a_i (\mathrm{mod}\ b_i)} x\ \psi_i(x),$$

where $\bowtie_i \in \{\leq, \geq\}$, each a_i is a natural number, each b_i is a natural number or infinity and all ψ_i are quantifier-free formulas.

Lemma

There exists a nondeterministic polynomial time procedure, taking as its input an $\mathrm{FO}^1_{\mathrm{MOD}}$–formula over a signature τ and producing a flat formula φ' over the same signature τ, such that φ is satisfiable iff the procedure has a run producing a satisfiable φ'.

Systems of congruences - Example

$$\varphi = \exists^{=0 (\text{mod } 10)} x \; French(x) \bigwedge$$

$$\exists^{\geq 8 (\text{mod } 22)} x \; German(x) \vee Spanish(x) \bigwedge$$

$$\exists^{\leq 10 (\text{mod } \infty)} x \; German(x) \wedge Spanish(x) \wedge French(x)$$

Denote the 1-types over the signature French, German, Spanish by $t_\emptyset, t_F, t_G, t_S, t_{FG}, t_{FS}, t_{GS}, t_{FGS}$ (the letters in the subscript indicate the positive subformulas of the type). $\mathcal{E}_\phi$ contains:

Obvious observation: $x \equiv r (\text{mod } m)$ iff there exists q s.t. $x = r + qm$

Systems of congruences - Example

$$\varphi = \exists^{=0(\text{mod } 10)} x\ French(x) \bigwedge$$

$$\exists^{\geq 8(\text{mod } 22)} x\ German(x) \vee Spanish(x) \bigwedge$$

$$\exists^{\leq 10(\text{mod } \infty)} x\ German(x) \wedge Spanish(x) \wedge French(x)$$

Denote the 1-types over the signature French, German, Spanish by $t_\emptyset, t_F, t_G, t_S, t_{FG}, t_{FS}, t_{GS}, t_{FGS}$ (the letters in the subscript indicate the positive subformulas of the type). $\mathcal{E}_\phi$ contains:

$$x_F + x_{FG} + x_{FS} + x_{GS} + x_{FGS} \equiv r_1 \ (\text{mod } 10) \wedge r_1 = 0$$

Obvious observation: $x \equiv r(\text{mod } m)$ iff there exists q s.t. $x = r + qm$

Systems of congruences - Example

$$\varphi = \exists^{=0(\text{mod } 10)} x \; French(x) \bigwedge$$

$$\exists^{\geq 8(\text{mod } 22)} x \; German(x) \vee Spanish(x) \bigwedge$$

$$\exists^{\leq 10(\text{mod } \infty)} x \; German(x) \wedge Spanish(x) \wedge French(x)$$

Denote the 1-types over the signature $\text{French}, \text{German}, \text{Spanish}$ by $t_\emptyset, t_F, t_G, t_S, t_{FG}, t_{FS}, t_{GS}, t_{FGS}$ (the letters in the subscript indicate the positive subformulas of the type). $\mathcal{E}_\phi$ contains:

$$x_F + x_{FG} + x_{FS} + x_{GS} + x_{FGS} \equiv r_1 \text{ (mod 10)} \wedge r_1 = 0$$
$$x_G + x_S + x_{FG} + x_{FS} + x_{GS} + x_{FGS} \equiv r_2 \text{ (mod 22)} \wedge r_2 \geq 8 \wedge r_2 < 22$$

Obvious observation: $x \equiv r (\text{mod } m)$ iff there exists q s.t. $x = r + qm$

Systems of congruences - Example

$$\varphi = \exists^{=0(\text{mod } 10)} x \; French(x) \bigwedge$$

$$\exists^{\geq 8(\text{mod } 22)} x \; German(x) \vee Spanish(x) \bigwedge$$

$$\exists^{\leq 10(\text{mod } \infty)} x \; German(x) \wedge Spanish(x) \wedge French(x)$$

Denote the 1-types over the signature $\text{French}, \text{German}, \text{Spanish}$ by $t_\emptyset, t_F, t_G, t_S, t_{FG}, t_{FS}, t_{GS}, t_{FGS}$ (the letters in the subscript indicate the positive subformulas of the type). $\mathcal{E}_\phi$ contains:

$$x_F + x_{FG} + x_{FS} + x_{GS} + x_{FGS} \equiv r_1 \;(\text{mod } 10) \wedge r_1 = 0$$

$$x_G + x_S + x_{FG} + x_{FS} + x_{GS} + x_{FGS} \equiv r_2 \;(\text{mod } 22) \wedge r_2 \geq 8 \wedge r_2 < 22$$

$$x_{FGS} \equiv r_3 \;(\text{mod } 10) \wedge r_3 \leq 10$$

Obvious observation: $x \equiv r(\text{mod } m)$ iff there exists q s.t. $x = r + qm$

From systems of congruences to system of inequalities

$$\varphi = \exists^{=0 (\text{mod } 10)} x \; French(x) \bigwedge$$

$$\exists^{\geq 8 (\text{mod } 22)} x \; German(x) \vee Spanish(x) \bigwedge$$

$$\exists^{\leq 10 (\text{mod } \infty)} x \; German(x) \wedge Spanish(x) \wedge French(x)$$

$$x_F + x_{FG} + x_{FS} + x_{GS} + x_{FGS} = r_1 + 10 q_1 \wedge r_1 = 0$$

$$x_G + x_S + x_{FG} + x_{FS} + x_{GS} + x_{FGS} = r_2 + 22 q_2 \wedge r_2 \geq 8 \wedge r_2 < 22$$

$$x_{FGS} \equiv r_3 \pmod{10} \wedge r_3 \leq 10$$

Useful algebraic theorems

Lemma (Small solution)

Let $\mathcal{E}$ be a system of I inequalities with U unknowns. Assume that all coefficients are integers absolutely bounded by C. If there is a solution for the system $\mathcal{E}$ over $\mathbb{N}$, there is also a solution in which the values assigned to the unknowns are all bounded by $U(IC)^{2I+1}$.

Lemma (Small system size)

Let $\mathcal{E}$ be a system of I inequalities with integer coefficients such that the absolute value of each coefficient from $\mathcal{E}$ is bounded by C. If $\mathcal{E}$ has a solution over $\mathbb{N}$, then it has a solution over $\mathbb{N}$ with the number of non-zero unknowns bounded by $2I\log(4IC)$.

Algorithm 1 $\mathrm{FO}^1_{\mathrm{MOD}}$-sat-test

Require: a $\mathrm{FO}^1_{\mathrm{MOD}}$–formula φ
1: **Guess** φ' – a flattened φ.
2: **Guess** which 1-types are realized at least one time.
3: Write the system of inequalities $\mathcal{E}$ for the guessed 1-types.
4: Return **True**, if $\mathcal{E}$ has a solution over $\mathbb{N}$ and **False** otherwise.

Theorem

The satisfiability problem for $\mathrm{FO}^1_{\mathrm{MOD}}$ *is* $\mathrm{NP}\textsc{Time}$*-complete.*

Questions?

Thank you for your attention