Witnessing Theorems and Conservation results for T_2^i

Chun-Yu "Max" Lin

Department of Logic, Faculty of Arts, Charles University

May 12, 2023

T_2^i and S_2^i in Sequent Calculus

Axioms

$$\frac{}{A \to A} \qquad \frac{}{\to \varphi(\bar{x})}\ \varphi(\bar{x}) \in BASIC$$

Inference rules :

1. Weak structural rules
2. Logical rules
3. Cut rules
4. Equality axioms
5. Bounded quantifiers rules

T_2^i and S_2^i in Sequent Calculus

Induction inference rule : Let Φ be a set of formulas. for $A \in \Phi$

- Φ-IND :

$$\frac{A(b), \Gamma \to \Delta, A(b+1)}{A(0), \Gamma \to \Delta, A(t)}$$

- Φ-PIND :

$$\frac{A(\lfloor \frac{1}{2} b \rfloor), \Gamma \to \Delta, A(b)}{A(0), \Gamma \to \Delta, A(t)}$$

Definition

S_2^i : BASIC + Σ_i^b-PIND.
T_2^i : BASIC + Σ_i^b-IND

Remark : We let T_2^0 denote PV_1 defined as follows : first order language consisting of symbols for $\square_1^p$ and Δ_1^p, and to have as axioms (1) BASIC (2) axioms that define the non-logical symbols in the sense of constructions for $\square_i^p$ (3) IND for sharply bounded formulas.

Every single function and predicate symbol which was claimed to be Σ_1-definable or Δ_1-definable in $I\Delta_0$ is likewise Σ_i^b-definable or Δ_i^b-definable in S_2^1, T_2^1, BASIC + Π_1^b-PIND, BASIC + Σ_1^b-LIND, BASIC + Π_1^b-LIND and BASIC + Π_1^b-IND.

Theorem (Buss,1986)

Let $i \geq 1$

1. T_2^i *proves* Π_i^b*-IND and* $T_2^i \models S_2^i$.
2. S_2^i *proves* Σ_i^b*-LIND,* Π_i^b*-PIND and* Π_i^b*-LIND.*

Definition (Cobham,1965)

The polynomial time function on $\mathbb{N}$ are inductive defined by

1. The following function are polynomial time :
   - The nullary constant function 0.
   - The successor function S(x)
   - The doubling function D(x)=2x
   - The conditional function $Cond(x,y,z) = \begin{cases} y & \text{if } x = 0 \\ z & \text{otherwise.} \end{cases}$
2. The projection functions are polynomial time functions; the composition of polynomial time functions is a polynomial time function.
3. If g is a $(n-1)$-ary polynomial time function and h is a $(n+1)$-ary polynomial time function and p is a polynomial, then the following function f, defined by limited iteration on notation from g and h , is also polynomial time : $f(0,\vec{x}) = g(\vec{x})$
   $f(z,\vec{x}) = h(z,\vec{x},f(\lfloor \frac{1}{2}z \rfloor,\vec{x}))$ for $z \neq 0$ provided $|f(z,\vec{x})| \leq p(|z|,|\vec{x}|)$

Notation

The class of polynomial time functions is denoted as $\square_1^p$, and the class of polynomial time predicates is denoted Δ_1^p.

Theorem (Buss,1986)

1. *Every polynomial time function is Σ_1^b-definable in S_2^1.*
2. *Every polynomial time predicate (i.e. its characteristic function is polynomial time) is Δ_1^b-definable in S_2^1.*

Theorem (Buss,1986)

Let $i \geq 1$.

1. $T_2^i \supseteq S_2^i$.
2. $S_2^i \supseteq T_2^{i-1}$.

Definition

The classes Δ_1^p and $\square_1^p$ have already been defined. Further define, by induction on i,

1. Σ_i^p is the class of predicate $R(\vec{x})$ definable by $R(\vec{x}) \leftrightarrow (\exists y) \leq s(\vec{x})(Q(\vec{x}, y))$ for some term s in ther language of bounded arithmetic, and some Δ_i^p predicate Q.
2. Π_i^p is the class of complements of predicates in Σ_i^p.
3. $\square_{i+1}^p$ is the class of predicates computable on a polynomial time Turing machine using an oracle from Σ_i^p.
4. Δ_i^p is the class of predicates which have characteristic function in $\square_{i+1}^p$.

Theorem (Wrathall'76,Stockmeyer'76,Kent-Hodgson'82)

A predicate is Σ_i^p if and only if there is a Σ_i^b-formula which defines it.

There are two important witnessing theorems for T_2^i. The first follows from the 'Main Theorem' for S_2^{i+1} and the fact that S_2^{i+1} is Σ_{i+1}^b-conservative over T_2^i: this witnessing theorem states that the Σ_{i+1}^b-definable functions of T_2^i are precisely the functions which can be computed in polynomial time with a Σ_i^b-oracle (i.e., the $\square_{i+1}^p$-functions). The second witnessing theorem puts a necessary condition on the Σ_{i+2}^b- and Σ_{i+3}^p-definable functions of T_2^i; we call this the 'KPT witnessing theorem'. It is this latter witnessing theorem that we need for our proofs:

The Σ^b_{i+1}-definable functions of T^i_2

Theorem (Buss,1990)

Let $i \geq 0$.

1. *T^i_2 can Σ^b_{i+1}-define every $\square^p_{i+1}$ function.*
2. *Every Σ^b_{i+1}-definable function of in T^i_2 is a $\square^p_{i+1}$-function.*
3. *S^{i+1}_2 is Σ^b_{i+1}-conservative over T^i_2.*
4. *S^{i+1}_2 is conservative over $T^i_2 + \Sigma^b_{i+1}$-replacement w.r.t Boolean combination of Σ^b_{i+1} formulas.*

Recall : $LSP(w,j)$ is the Σ_i^b-defined function of S_2^1 which is equal to $w \bmod 2^j$.

Definition

A theory R can Q_i-define the function $f(\vec{x})$ if and only if there is a Σ_i^b-formula $U(w,j,\vec{x})$, a term $t(\vec{x})$, and a Σ_1^b-defined function f^* of S_2^1 such that $R \vdash (\forall x)(\exists y) DEF_{U,t}(w,\vec{x})$ where $DEF_{U,t}(w,\vec{x})$ is the following formula :

$$(\forall j < |t|)[Bit(j,w) \leftrightarrow U(LSP(w,j),j,\vec{x})]$$

and such that, for all $\vec{n}, w \in \mathbb{N}$, if $DEF_{U,t}(w,\vec{n})$ then $f(\vec{n}) = f^*(w,\vec{n})$.

Idea : The letter Q stands for "query" and the idea is that a function is Q_i -definable if and only if it is computable by a polynomial time Turing machine with a Σ_i^p-oracle.

Proof.

(1) : For $i = 0$, it is clear because the temporary convention that T_2^0 denotes PV_1. For $i > 0$, one shows that T_2^i can Q_i-define every $\square_{i+1}^p$ formula.

(2) : This is immediate from the fact that every Σ_i^b-definable function of S_2^i is in $\square_i^p$ and $T_2^i \subseteq S_2^{i+1}$.

(3) : This is based on the following Witnessing Lemma for S_2^{i+1}.

(4) : This can be obtained from the Witnessing Lemma using the fact that $T_2^i + \Sigma_{i+1}^b$-replacement can prove that $A(\vec{c})$ is equivalent to $(\exists w) Witness_A^{i+1}(w, \vec{c})$ for any $A \in \Sigma_{i+1}^b$. □

Witness Lemma for S_2^{i+1}

Lemma

Let $i \geq 1$. Let $\Gamma \to \Delta$ be a sequent of formulas in Σ_{i+1}^b in prenex form, and suppose S_2^{i+1} proves $\Gamma \to \Delta$; let $\vec{c}$ include all free variables in the sequent. Then there is a $\square_{i+1}^p$-function $h(w, \vec{c})$ which is Q_i-defined in T_2^i such that T_2^i proves

$$Witnes_{\wedge\Gamma}^{i+1}(w, \vec{c}) \to Witnes_{\vee\Delta}^{i+1}(h(w, \vec{c}), \vec{c}).$$

Proof.

The proof of this Witnessing Lemma is almost exactly the same as the proof of the Witnessing Lemma for S_2^i; the only difference is that the witnessing functions are now proved to be Q_i -definable in T_2^i . (1) implies the necessary functions are Q-defined by T_2^i since we already know they are Σ_{i+1}^b-defined by S_2^{i+1}. So the main new aspect is showing that T_2^i can prove that the witnessing functions work. □

The Σ^b_{i+2}-definable functions of T^i_2

The Σ^b_{i+2}-definable functions of T^i_2 can be characterized by the following theorem :

Theorem (Krajíček-Pudlák-Takeuti, 1991)

Let $i \geq 0$. Suppose T^i_2 proves $(\forall x)(\exists y)(\forall z \leq t(x))A(y,x,z)$ where $A \in \Pi^b_i$. Then there is a $k > 0$ and there are Σ^b_{i+1}-definable function symbols $f_1(x), f_2(x,z_1), \ldots, f_k(x,z_1,\ldots,z_{k-1})$ such that T^i_2 proves

$$\begin{aligned}(\forall x)(\forall z_1 \leq t)[A(f_1(x),x,z_1) \vee (\forall z_2 \leq t)[A(f_2(x,z_1),x,z_2)\\ \vee (\forall z_3 \leq t)[A(f_3(x,z_1,z_2),x,z_3)\\ \vee \cdots \vee (\forall z_k \leq t)[A(f_k(x,z_1,\ldots,z_{k-1}),x,z_k)] \cdots]]]\end{aligned}$$

Conversely, whenever the above formula is provable, then T^i_2 can also prove $(\forall x)(\exists y)(\forall z \leq t(x))A(y,x,z)$.

Proof

Proof I. Let $\varphi(a, x, y)$ be of the form

$$\exists z\, \psi(a, x, y, z),$$

where ψ is Π_i^b. ψ is in PV_{i+1} equivalent to $g(a, x, y, z) = 1$, where g is the characteristic function of ψ.

From the assumption of the theorem we have:

$$\mathrm{PV}_{i+1} \vdash \exists x\, \forall y\, \exists z\, g(a, x, y, z) = 1.$$

PV_{i+1} is a universal theory and thus we can apply Gentzen's midsequent theorem, cf. [13], (or equivalently Herbrand's theorem) to find PV_{i+1}-terms t_u and $s_{u,v}$ such that (after possible renaming of free variables) the disjunction:

$$(g(a, t_1(a), b_1, s_{1,1}) = 1 \vee \cdots \vee g(a, t_1(a), b_1, s_{1,n}) = 1)$$

$$\vee \cdots \vee$$

$$(g(a, t_k(a, b_1, \ldots, b_{k-1}), b_k, s_{k,1}) = 1 \vee \cdots g(a, t_k(a, b_1, \ldots, b_{k-1}), b_k, s_{k,n}) = 1)$$

is provable in PV_{i+1} (terms $s_{u,v}$ generally depend on all a, $\boldsymbol{b}$, and t_u depends only on $a, b_1, \ldots, b_{u-1}$).

Now existentially quantify terms $s_{u,v}$ and contract occurrences of $\exists z \quad g(a, t_j, b_j, z) = 1$, for $1 \leqslant j \leqslant k$. The required functions f_j are those defined by terms t_j. □

Applications to the polynomial hierarchy

Theorem (Buss'95,Zambella'96)

Let $i \geq 0$. If $T_2^i = S_2^{i+1}$, then

1. *$T_2^i = S_2$ and therefore S_2 is finitely axiomatized,*
2. *T_2^i proves the polynomial time hierarchy collapses*
   - *T_2^i proves that every Σ_{i+3}^b-formula is equivalent to a Boolean combination of Σ_{i+2}^b-formulas*
   - *T_2^i proves the polynomial time hierarchy collapses to $\Sigma_{i+1}^p/poly$.*

Proof.

(1) : We need the method of proof of the following claim : if $T_2^i = S_2^{i+1}$ then $T_2^i \vdash \Sigma_{i+1}^b$-IND and $T_2^i = T_2^{i+1}$. By iterating the same method with some modifications, one can show $T_2^i = T_2^{i+2}$, $T_2^i = T_2^{i+3}$ and so on. □

Corollary (Buss,1995)

S_2 is finitely axiomatized if and only if S_2 proves the polynomial hierarchy collapses.

The Σ_1^b-definable functions of T_2^1

Polynomial Local Search problem : a maximization problem satisfying the following conditions :

1. For every instance $x \in \{0,1\}^*$, there is a set $F_L(x)$ of solutions, an integer valued cost function $c_L(s,x)$ and a neighborhood function $N_L(s,x)$,
2. The binary predicate $s \in F_L(x)$ and the function $c_L(s,x)$ and $N_L(s,x)$ are polynomial time computable. There is a polynomial p_L so that for all $s \in F_L(x)$, $|s| \leq p_L(|x|)$. Also, $0 \in F_L(x)$.
3. For all $s \in \{0,1\}^*$, $N_L(s,x) \in F_L(x)$.
4. For all $s \in F_L(x)$, if $N_L(s,x) \neq s$ then $c_L(s,x) < c_L(N_L(s,x),x)$
5. The problem is solved by finding a locally optimal $s \in F_L(x)$, i.e. an s such that $N_L(s,x) = s$.

Remark 1

A PLS-problem L can be expressed as a Π_1^b-sentence saying that the conditions above hold; if these are provable in T_2^1 then we say L is a PLS-problem.

Theorem (Buss-Krajíček, 1994)

Let the formula $Opt_L(x,s)$ be the Δ_1^b-formula $N_L(s,x) = s$.

1. *For every PLS problem L, T_2^1 can prove $(\forall x)(\exists y)Opt_L(x,y)$.*
2. *If $A \in \Sigma_1^b$ and if T_2^1 proves $(\forall \vec{x})(\exists y)A(\vec{x},y)$, then there is a polynomial time function $\pi(y)$ and a PLS problem L such that T_2^1 proves $(\forall \vec{x})(\forall y)(Opt_L(\vec{x},y) \to A(\vec{x},\pi(y)))$.*

(2) gives an exact complexity characterization of the $\forall\Sigma_1^b$-definable functions of T_2^1 in terms of PLS-computability.

Proof

(1) : It is known that T_2^1 proves the Σ-MIN axioms; this immediately implies also the Σ-MAX principle. Arguing informally in T_2^1, we have that, for all s, there is a maximum value $C_0 < M_L(x)$ satisfying $(\exists s \in F_L(x))(c_L(s,x) = c_0)$. Taking s to be witness for this last formula, we see that s is globally optimal and hence satisfies, and the theorem is proved.

(2) : By free-cut elimination, there is a T_2^1-proof P in LKB of the sequent $\rightarrow A(\vec{b}, t)$ such that every sequent in P is of the form $A_1(\vec{u}, t), \ldots, A_k(\vec{u}, t) \rightarrow B_1(\vec{u}, t), \ldots B_l(\vec{u}, t)$ where $\vec{u}$ is a sequence of variables and $A_i, B_i \in \Sigma_i^b$. We shall prove by induction on the number of proof steps that any sequent of the above form provable in T_2^1 corresponds computationally to a PLS-problem.