Introduction to Kleene Algebra	**Lecture 27**
CS786 Spring 2002	**Thursday, May 2, 2002**

1 Π^1_1-Completeness of $\mathcal{H}\,\mathsf{KA}^*$

In this lecture we prove that the universal Horn theory of the star-continuous Kleene algebras is Π^1_1-complete. This result is from [2].

Let $G = (\omega,\ R)$ be a recursive directed graph on vertices ω, the natural numbers. For $m \in \omega$, denote by $R(m)$ the set of R-successors of m:

$$R(m) \quad = \quad \{n \mid (m,n) \in R\}.$$

Let $\mathsf{WF} \subseteq \omega$ be the set of all m such that all R-paths out of m are finite. Alternatively, we could define WF as the least solution of the following recursive equation:

$$\mathsf{WF} \quad = \quad \{m \mid R(m) \subseteq \mathsf{WF}\}.$$

Let us call G *well-founded* if $0 \in \mathsf{WF}$; that is, if all R-paths out of 0 are finite.

A well-known Π^1_1-complete problem is:

> *Given a recursive graph (say by a total Turing machine accepting the set of encodings of edges $(m,n) \in R$), is it well-founded?*

We reduce this problem to $\mathcal{H}\,\mathsf{KA}^*$, thereby showing that the latter problem is Π^1_1-hard.

By assumption, R is a recursive set, thus there is a total deterministic Turing machine M that decides whether $(m,n) \in R$. We can assume without loss of generality that M satisfies the restrictions on Turing machines imposed in the previous lecture and operates as follows.

In addition to its start state s, M has three halt states t, r, u. When started in configuration $\vdash a^m s a^n \dashv$, it first performs a check that the tape initially contains a contiguous string of a's surrounded by blanks and enters halt state u if not. It then determines whether $(m,n) \in R$. If so, it halts in configuration $\vdash a^n t \dashv$, and if not, it halts in configuration $\vdash r \dashv$. Thus

$$\vdash a^m s a^n \dashv \quad \xrightarrow[M]{*} \quad \begin{cases} \vdash a^n t \dashv, & \text{if } (m,n) \in R, \\ \vdash r \dashv, & \text{if } (m,n) \notin R. \end{cases}$$

By Lemma **??** of the previous lecture, we have

$$\begin{aligned} \vdash a^m s a^n \dashv \;\approx\; \vdash a^n t \dashv \quad &\Leftrightarrow \quad (m,n) \in R, \\ \vdash a^m s a^n \dashv \;\approx\; \vdash r \dashv \quad &\Leftrightarrow \quad (m,n) \notin R, \end{aligned}$$

where $\approx$ denotes congruence modulo equations (E1)–(E3) of the previous lecture.

Now consider the Kleene algebra equation

$$t \;\leq\; sa^*. \tag{1}$$

Let E be the set of equations (E1)–(E3) together with (1).

The following is our main lemma.

Lemma 1.1 *For all $m \geq 0$,*

$$\mathsf{KA}^* \;\models\; E \;\rightarrow \vdash a^m t \dashv \;\leq\; \vdash r \dashv$$

if and only if $m \in \mathsf{WF}$.

Proof. The reverse implication ($\Leftarrow$) is proved by transfinite induction on the stages of the inductive definition of WF. Suppose that $m \in \mathsf{WF}$. Let $\tau : 2^\omega \rightarrow 2^\omega$ be the monotone map

$$\tau(A) \;=\; \{m \mid R(m) \subseteq A\}$$

and define

$$\begin{aligned} \tau^0(A) &= A \\ \tau^{\alpha+1}(A) &= \tau(\tau^\alpha(A)) \\ \tau^\lambda(A) &= \bigcup_{\alpha<\lambda} \tau^\alpha(A), \quad \lambda \text{ a limit ordinal.} \end{aligned}$$

Then

$$\mathsf{WF} \;=\; \bigcup_\alpha \tau^\alpha(\varnothing).$$

Let α be the smallest ordinal such that $m \in \tau^\alpha(\varnothing)$. Then α must be a successor ordinal $\beta+1$, therefore $m \in \tau(\tau^\beta(\varnothing))$, so $R(m) \subseteq \tau^\beta(\varnothing)$. By the induction hypothesis, if $n \in R(m)$, then

$$\mathsf{KA}^* \;\models\; E \;\rightarrow \vdash a^n t \dashv \;\leq\; \vdash r \dashv,$$

and $\vdash a^m s a^n \dashv \;\approx\; \vdash a^n t \dashv$, therefore

$$\mathsf{KA}^* \;\models\; E \;\rightarrow \vdash a^m s a^n \dashv \;\leq\; \vdash r \dashv .$$

For $n \notin R(m)$, $\vdash a^m s a^n \dashv \;\approx\; \vdash r \dashv$. Thus for all n,

$$\mathsf{KA}^* \;\models\; E \;\rightarrow \vdash a^m s a^n \dashv \;\leq\; \vdash r \dashv .$$

By star-continuity,

$$\mathsf{KA}^* \ \vDash \ E \ \to \vdash a^m s a^* \dashv \ \leq \ \vdash r \dashv,$$

and by (1),

$$\mathsf{KA}^* \ \vDash \ E \ \to \vdash a^m t \dashv \ \leq \ \vdash r \dashv \ .$$

Conversely, for the forward implication ($\Rightarrow$), we construct a particular interpretation satisfying E in which for all $m \in \omega$, $\vdash a^m t \dashv \ \leq \ \vdash r \dashv$ implies $m \in \mathsf{WF}$.

For $A \subseteq \Delta^*$, define the monotone map

$$\sigma(A) \ = \ A \ \cup \ \{x \mid \exists y \in A \ x \approx y\} \ \cup \ \{utv \mid \forall n \ usa^n v \in A\}. \tag{2}$$

Call a subset of Δ^* *closed* if it is closed under the operation σ. The *closure* of A is the smallest closed set containing A and is denoted $\overline{A}$. Build a Kleene algebra consisting of the closed sets with operations

$$\begin{array}{rcl} A \oplus B & = & \overline{A \cup B} \\ A \odot B & = & \overline{AB} \\ A^{\circledast} & = & \overline{\bigcup_n A^n} \end{array} \qquad \begin{array}{rcl} 0 & = & \varnothing \\ 1 & = & \{\varepsilon\}, \\ & & \end{array}$$

where ε is the null string and A^n is the n^{th} power of A under the operation $\odot$. It is not difficult to show that the family of closed sets forms a star-continuous Kleene algebra under these operations.

We show now that under the interpretation $a \mapsto \overline{\{a\}}$, the equations E are satisfied. For an equation $x = y$ of type (E1)–(E3), we need to show that $\overline{\{x\}} = \overline{\{y\}}$. It suffices to show that $x \in \overline{\{y\}}$ and $y \in \overline{\{x\}}$. But since $x \approx y$, this follows immediately from (2).

For the equation $t \leq sa^*$, we need to show that

$$t \in \overline{\{s\}} \odot \overline{\bigcup_n \overline{\{a\}}^n}.$$

It suffices to show $t \in \overline{\{sa^n \mid n \geq 0\}}$. Again, this follows immediately from (2).

Finally, we show that for $x \in \overline{\{\vdash r \dashv\}}$, either

(i) $x \ \xrightarrow[M]{*} \ \vdash r \dashv$;

(ii) $x \ \xrightarrow[M]{*} \ \vdash a^n t \dashv$ for some $n \in \mathsf{WF}$; or

(iii) $x \ \sim \ \vdash a^n t a^k \dashv$ for some $k \geq 1$.

The argument proceeds by transfinite induction on the inductive definition of closure:

$$\begin{array}{rcl} \sigma^0(A) & = & A \\ \sigma^{\alpha+1}(A) & = & \sigma(\sigma^\alpha(A)) \\ \sigma^\lambda(A) & = & \displaystyle\bigcup_{\alpha<\lambda} \sigma^\alpha(A), \quad \lambda \text{ a limit ordinal} \\ \overline{A} & = & \displaystyle\bigcup_{\alpha} \sigma^\alpha(A). \end{array}$$

Let α be the least ordinal such that

$$x \;\in\; \sigma^\alpha(\{\vdash r \dashv\}).$$

Then α must be a successor ordinal $\beta + 1$, thus

$$x \;\in\; \sigma(\sigma^\beta(\{\vdash r \dashv\})).$$

There are two cases, one for each clause in the definition (2) of σ.

If there exists $y \in \sigma^\beta(\{\vdash r \dashv\})$ such that $x \approx y$, then by the induction hypothesis, y satisfies one of (i)–(iii), therefore so does x; the argument here is similar to [1, Theorem 4.3, p. 98].

Otherwise, $x = utv$ and

$$usa^n v \;\in\; \sigma^\beta(\{\vdash r \dashv\})$$

for all n. By the induction hypothesis, one of (i)–(iii) holds for each $usa^n v$. But (iii) is impossible because of the form of (E3). Moreover, by construction of M, each of (i) and (ii) implies that $u \sim\vdash a^m$ and $v \sim a^k \dashv$ for some k, m. Thus $x \sim\vdash a^m t a^k \dashv$. If $k \geq 1$, then x satisfies (iii). Otherwise, $x \sim\vdash a^m t \dashv$ and

$$\vdash a^m s a^n \dashv \;\in\; \sigma^\beta(\{\vdash r \dashv\})$$

for all n, therefore either (i) or (ii) holds for $\vdash a^m s a^n \dashv$. If (i), then $(m, n) \notin R$. If (ii), then $(m, n) \in R$ and $n \in \mathsf{WF}$. Thus $R(m) \subseteq \mathsf{WF}$ and $m \in \mathsf{WF}$. □

Theorem 1.2 $\mathcal{H}\,\mathsf{KA}^*$ *is* Π^1_1*-complete.*

Proof. Taking $m = 0$ in Lemma 1.1, we have

$$\mathsf{KA}^* \;\vDash\; E \rightarrow \vdash t \dashv \;\leq\; \vdash r \dashv$$

if and only if G is well-founded. This gives the desired lower bound. The upper bound follows from the form of the infinitary axiomatization of star-continuous Kleene algebra; validity is equivalent to the existence of a well-founded proof tree. □

References

[1] Martin Davis. *Computability and Unsolvability.* McGraw-Hill, New York, 1958.

[2] Dexter Kozen. On the complexity of reasoning in Kleene algebra. In *Proc. 12th Symp. Logic in Comput. Sci.*, pages 195–202, Los Alamitos, Ca., June 1997. IEEE.