Aproximación al poder expresivo de lógicas

sobre modelos finitos ordenados

UPC, Barcelona, Febrero 10, 2004

Argimiro Arratia

Universidad de Valladolid

arratia@mac.uva.es

Trabajo en colaboración con Carlos Ortiz, Arcadia University, EEUU

Motivaciones

- La descripción lógica de clases de complejidad por debajo de **NP** necesita **orden**
- En presencia de orden técnicas como juegos de Ehrenfeucht–Fraissé para demostrar inexpresabilidad resultan poco efectivas; por lo tanto inútiles para ayudar a obtener cotas inferiores significativas en las clases de complejidad computacional de mayor interés.

Plan

- Definir una lógica con mecanismos de expresión que en presencia de un orden débil aproxime el poder expresivo de lógicas que capturan clases por debajo de **NP** pero no inutilicen por completo técnicas para demostrar inexpresabilidad.
- Obtener resultados de inexpresabilidad en estas lógicas respecto a modelos donde el orden (y otras relaciones que lo simulen, eg. $+$, $\times$) sea una versión débil o aproximada.
- Determinar cómo se traducen nuestros resultados de definibilidad en nuestros universos de aproximaciones a definibilidad en el universo real (i.e. donde el orden y demás relaciones aritméticas son las naturales).

La Lógica de Cuantificadores Probabilísticos, $\mathcal{LP}$

Es una extensión de la lógica de Primer Orden (PO) con los cuantificadores

$$(P(z) > r)\phi(\overline{x}, z) \text{ y } (P(z) \geq r)\phi(\overline{x}, z)$$

donde $0 \leq r < 1$ y $\phi(\overline{x}, z)$ es una fórmula del lenguaje

Semántica

Sea $\mathcal{B}_m$ una estructura adecuada de cardinalidad m,

$$\mathcal{B}_m \models (P(z) > r)\phi(\overline{a}, z) \iff \frac{|\{z < m : \mathcal{B}_m \models \phi(\overline{a}, z)\}|}{m} > r$$

análogamente

$$\mathcal{B}_m \models (P(z) \geq r)\phi(\overline{a}, z) \iff \frac{|\{z < m : \mathcal{B}_m \models \phi(\overline{a}, z)\}|}{m} \geq r$$

Antecedentes: H.J. Keisler, Hyperfinite model theory (Logic Colloquium 76)

Fragmentos de Interés

Sean $r_1, r_2, \ldots r_k$ naturales distintos, τ un vocabulario.
$\mathcal{LP}(\tau)[r_1, r_2, \ldots, r_k]$ es el subconjunto más pequeño de $\mathcal{LP}(\tau)$ que contiene a las fórmulas atómicas, cerrado bajo negación, conjunción, existencial y

$$P(z) > q_{ij}/r_i \qquad P(z) \geq q_{ij}/r_i$$

donde $i \leq k$ y $0 \leq q_{ij} < r_i$

Nuestro vocabulario de interés: $\Gamma = \{\oplus, \otimes, \lhd, 0, 1\}$

donde $\oplus$, $\otimes$ son relaciones de aridad 3 y siempre se interpretarán como la suma y el producto

$\lhd$ es binaria y siempre se interpretará como el orden

0 y 1 constantes; el cero y el uno

Ejemplos

Como consecuencia de [Barrington,Immerman, Straubing, JCSS 1990]: $\mathrm{AC}^0 = \mathrm{PO}(\Gamma)$ y $\mathrm{TC}^0 = \mathcal{LP}(\Gamma)[2]$ donde

AC^0 = clase de problemas aceptados por circuitos de tamaño polinomial, profundidad constante y "abanico de inclusión" (*fan–in*) no acotado

TC^0 = clase de problemas aceptados por circuitos de tamaño polinomial, profundidad constante y puertos umbrales con abanico de inclusión no acotado (puertos que cuentan el número de 1's y compara el total con un número prefijado)

Aproximaciones a las verdaderas interpretaciones

Fijamos $F : \mathbb{N} \to \mathbb{N}$ sublineal (i.e. para todo $m > 0$, $0 < F(m) \leq m$). Una fórmula $\theta(\overline{x})$ es **F-modular** en el modelo $\mathcal{B}_m$ si y sólo si para todos $\overline{a}, \overline{b} < m$, si $\overline{a} \equiv_{F(m)} \overline{b}$ entonces

$$\mathcal{B}_m \models \theta(\overline{a}) \iff \mathcal{B}_m \models \theta(\overline{b})$$

- F-modularidad se preserva bajo las operaciones lógicas y cuantificación en $\mathcal{LP}(\Gamma)$

(Por lo tanto, la F-modularidad de las fórmulas en un modelo $\mathcal{B}_m$ depende sólo de la interpretación modular de los símbolos relacionales en $\mathcal{B}_m$ y es razonable entonces llamar a estas estructuras F–modulares.)

Aproximación F-modular de estructura $\mathcal{A}_m$

Para naturales $e, f > 0$ denotamos $[e]_f$ el resto de dividir e por f.
Dada F sublineal y estructura aritmética

$$\mathcal{A}_m = \langle \{0, 1, \ldots m-1\}, \oplus, \otimes, \lhd, 0, 1 \rangle .$$

su aproximación F-modular es

$$\mathcal{A}_m^F = \langle \{0, 1, \ldots m-1\}, \oplus, \otimes, \lhd, 0, 1 \rangle$$

tal que para todo $a, b, c, a_1, \ldots, a_r < m$,

- $\mathcal{A}_m^F \models \oplus(a, b, c)$ sii $\mathcal{A}_m \models \oplus([a]_{F(m)}, [b]_{F(m)}, [c]_{F(m)})$.
- $\mathcal{A}_m^F \models \otimes(a, b, c)$ sii $\mathcal{A}_m \models \otimes([a]_{F(m)}, [b]_{F(m)}, [c]_{F(m)})$.
- $\mathcal{A}_m^F \models \lhd(a, b)$ sii $\mathcal{A}_m \models \lhd([a]_{F(m)}, [b]_{F(m)})$.

Es fácil ver que $\mathcal{A}_m^F$ es F-modular

Ademas ...

Para todo s, para todo símbolo relacional R_s, el conjunto

$$\{(a_1, \ldots, a_r) < m : \mathcal{A}_m^F \models R_s^F(a_1, \ldots, a_r)\}$$

y el conjunto

$$\{(a_1, \ldots, a_r) < m : \mathcal{A}_m \models R_s(a_1, \ldots, a_r)\}$$

coinciden en $\{(a_1, \ldots, a_r) : a_1, \ldots, a_r < F(m)\}$.

Esto justifica el nombre de aproximación F-modular de $\mathcal{A}_m$

Un caso particular de interés

Fijemos $n > 0$. Para todo m, sean r y t los únicos naturales tales que $m = tn + r$ y $0 \leq r < n$. Sea $g_n : \mathbb{N} \mapsto \mathbb{N}$ dada por

$$g_n(m) = \begin{cases} tn & \text{si } m \geq n \\ 1 & \text{caso contrario} \end{cases}$$

Para todo $n > 0$, g_n es sublineal.

Denotaremos por $\mathcal{LP}_{g_n}$ la lógica de cuantificadores probabilisticos restringida a aproximaciones g_n-modulares de estructuras aritméticas. Denotamos por PO_{g_n} el menor fragmento de $\mathcal{LP}_{g_n}$ que contiene las fmlas atómicas, cerrado bajo $\neg$, $\wedge$ y $\exists$.

Definimos la lógica probabilística modular como

$$\mathcal{LP}_{MOD} = \cup\{\mathcal{LP}_{g_n} : n \in \mathbb{N}\}$$

Por otra parte $\mathrm{PO}_{MOD} = \cup\{\mathrm{PO}_{g_n} : n \in \mathbb{N}\}$

Observe que estos lenguajes no tienen el orden, suma y producto sino (para cada n) g_n–aproximaciones de estas relaciones. La relación entre estos y los lenguajes para estructuras aritméticas es:

$$\begin{array}{ccc} \mathrm{PO}(\Gamma) & \longrightarrow & \mathcal{LP}(\Gamma) \\ \uparrow & & \uparrow \\ \mathrm{PO}_{MOD} & \longrightarrow & \mathcal{LP}_{MOD} \end{array}$$

La capacidad expresiva de $\mathcal{LP}_{MOD}$

La sentencia en $\mathcal{LP}_{MOD}(\Gamma)[2]$:

$$\begin{aligned} \theta_2 := \quad & \exists x \quad [(P(y) \geq 1/2)(x \lhd y \vee \oplus(0,x,y)) \\ & \wedge \quad (P(y) \leq 1/2)(x \lhd y \vee \oplus(0,x,y))] \end{aligned}$$

es tal que para todo n, para toda estructura aritmética $\mathcal{A}_m$ con $m > n$,

$$\mathcal{A}_m^{g_n} \models \theta_2 \iff m \text{ es par}$$

Similarmente, para todo natural $d > 2$, existe formula θ_d en $\mathrm{PO} + \{P(z) \geq 1/d, P(z) > (d-1)/d\}(\{\oplus, \otimes, \lhd, 0, 1\})$ tal que para todo natural n, para toda estructura aritmética $\mathcal{A}_m$ con $m > n$,

$$\mathcal{A}_m^{g_n} \models \theta_d \text{ sii } m \text{ es un múltiplo de } d.$$

Resultados de Separación para lógicas modulares

Sea F sublineal. Una **F-cadena de modelos C** es una colección de Γ–estructuras tales que

- Para todo símbolo relacional $R(\overline{x})$ de Γ, para todo par $\mathcal{B}_m, \mathcal{B}_n$ en $\mathbf{C}$ con $m \leq n$ y $F(m) = F(n)$, y para todo $\overline{a} < F(m)$, $\mathcal{B}_m \models R(\overline{a})$ si y sólo si $\mathcal{B}_n \models R(\overline{a})$.

Cadenas son colecciones de estructuras finitas con inter-compatibilidad entre sus predicados

Nuestra herramienta principal de separación es el siguiente Lema:

Lema de Separación:

Sea F sublineal y $\mathbf{C}$ una F-cadena de modelos. Sean r_1, r_2, ..., r_k enteros positivos distintos. Sea $\phi(x_1, \ldots, x_s)$ una fórmula en $\mathcal{LP}(\Gamma)[r_1, r_2, \ldots, r_k]$. Entonces una de las dos posibilidades siguientes es verdad:

1. Para todo par de modelos F-modulares $\mathcal{B}_m$ y $\mathcal{B}_{m+1}$ en $\mathbf{C}$ tal que $m+1 > r_i$ y $m \equiv_{r_i} -1$, para todo $i \leq k$ y $F(m) = F(m+1)$, se tiene que, para todo a_1, ..., $a_s < m$, $\mathcal{B}_m \models \phi(a_1, \ldots, a_s)$ implica $\mathcal{B}_{m+1} \models \phi(a_1, \ldots, a_s)$, o
2. Para todo par de modelos F-modulares $\mathcal{B}_m$ y $\mathcal{B}_{m+1}$ en $\mathbf{C}$ tal que $m+1 > r_i$ y $m \equiv_{r_i} -1$, para todo $i \leq k$ y $F(m) = F(m+1)$, se tiene que, para todo a_1, ..., $a_s < m$, $\mathcal{B}_{m+1} \models \phi(a_1, \ldots, a_s)$ implica $\mathcal{B}_m \models \phi(a_1, \ldots, a_s)$.

El lema de Separación tiene la siguiente consecuencia:

Sean $r, r_1, r_2, \ldots, r_k$ naturales, no nulos, distintos, y tal que r es primo relativo con cada $r_1, \ldots, r_k$. Entonces $\mathcal{LP}_{MOD}[r_1, \ldots, r_k]$ está propiamente contenido en $\mathcal{LP}_{MOD}[r_1 \ldots r_k, r]$.

Demostración: Usamos el Lema de Separación para demostrar que la afirmación

"la cardinalidad del modelo es un múltiplo de r"

no es expresable en $\mathcal{LP}[r_1 \ldots, r_k]_{MOD}(\Gamma)$ (y ya vimos que si es expresable en $\mathcal{LP}[r]_{MOD}(\Gamma)$)

Corolario: PO_{MOD} está propiamente contenido en $\mathcal{LP}_{MOD}[2]$. □

Esta separación en las lógicas modulares tiene su correspondiente en las aritméticas $PO(\Gamma)$ y $\mathcal{LP}(\Gamma)[2]$, que equivalen a la notable separación de AC^0 y TC^0 descubierta por Ajtai [APAL 1983] e independientemente Furst, Saxe y Sipser [Math. Syst. Theory 1984].

Lógica de 2do. Orden de Cuantificadores Probabilísticos, $\mathcal{SOLP}$

Extendemos PO con cuantificadores que actuan sobre fmlas.

$\alpha(\overline{x}, X)$ con X var. de 2do. orden de aridad k:

$$(P(X) > r)\alpha(\overline{x}, X) \text{ y } (P(X) \geq r)\alpha(\overline{x}, X)$$
$$(P(X) < r)\alpha(\overline{x}, X) \text{ y } (P(X) \leq r)\alpha(\overline{x}, X)$$

Semántica

Sea $\mathcal{B}_m$ una estructura adecuada de cardinalidad m,

$$\mathcal{B}_m \models (P(X) > r)\alpha(\overline{a}, X) \iff$$

$$\text{existe } A \subseteq \{b_0, \ldots, b_{m-1}\}^k : \mathcal{B}_m \models \phi(\overline{a}, A) \text{ y } |A| > rm^k$$

análogamente se define para $(P(X) \geq r)$, $(P(X) < r)$, $(P(X) \leq r)$

Ejemplos

1. $\mathbf{NCON}_{\geq r} := \{\mathcal{A} = \langle A, E, s\rangle : \langle A, E\rangle$ es digrafo y **al menos** una fracción r de A **no** estan conectados a $s\}$

Sea

$$\alpha_{ncon}(B) \quad := \quad \neg B(s) \wedge \forall x \forall y (E(x,y) \wedge B(x) \longrightarrow B(y))$$

Entonces

$$\mathcal{A}_n \in \mathbf{NCON}_{\geq r} \iff \mathcal{A}_n \models (P(B) \geq r)\alpha_{ncon}(B)$$

(La version no dirigida $\mathbf{UNCON}_{\geq r}$ de este problema de aproximación es también expresable en $\mathcal{SOLP}$)

Prop.: $\mathbf{NCON}_{\geq r}$ es completo para **NL** via *fop*.
($\mathbf{UNCON}_{\geq r}$ es completo para **SymLog** via *fop*.)

2. $\mathbf{ACCES}_{\geq r} := \{\mathcal{A} = \langle A, R, s\rangle : \mathcal{A}$ es un sistema de caminos y **al menos** una fracción r de elementos son *accesibles* desde $s\}$

($R \subseteq A \times A \times A$, $s, t \in A$. Un vértice v es *accesible* si $v = s$ o $R(x, y, v)$ para unos accesibles x e y)

Sea

$$\begin{aligned} \alpha_{acs}(X) \quad &:= \quad \forall x(x = s \longrightarrow X(x)) \\ &\wedge \quad \forall x \forall y \forall z(X(x) \wedge X(y) \wedge R(x, y, z) \longrightarrow X(z)) \end{aligned}$$

Entonces

$$\mathcal{A}_n \in \mathrm{ACCES}_{\geq r} \iff \mathcal{A}_n \models (P(X) \geq r)\alpha_{acs}(X)$$

Prop.: $\mathbf{ACCES}_{\geq 1/n}$ es completo para $\mathbf{P}$ via *fop*.

$\mathcal{SOLP}_{Horn}$, $\mathcal{SOLP}_{Krom}$

Restringimos $\mathcal{SOLP}$ a su fragmento positivo: sólo los cuantif. $(P(X) > r)$ y $(P(X) \geq r)$ y tal que estos no pueden estar en el alcance de $\neg$.

Restringimos las fórmulas de primer orden a ser sólo universales y en forma CNF.

Una tal formula $(P(X) > r)\alpha(\overline{x}, X)$ es:

Horn si cada clausula en α contiene a lo sumo una ocurrencia positiva de X (i.e. es una instrucción de PROLOG)

Krom si cada clausula en α contiene a lo sumo 2 ocurrencias de X

S-Krom (Symmetric Krom) como Krom + para cada clausula de la forma $\Psi \vee \beta \vee \gamma$ con Ψ (sub)clausula que no contiene X y β y γ literales que posiblemente incluyen X, debe estar presente también $\Psi \vee \neg\alpha \vee \neg\beta$

$\mathcal{SOLP}_{Horn}$ **(resp.** $\mathcal{SOLP}_{Krom}$**,** $\mathcal{SOLP}_{SKrom}$ **)** es el fragmento positivo de $\mathcal{SOLP}$ donde la parte de primer orden de las fórmulas en CNF es universal y Horn (resp. Krom, S-Krom).

Proposición: respecto a estructuras finitas ordenadas

1. $\mathcal{SOLP}_{Horn} = \mathbf{P}$
2. $\mathcal{SOLP}_{Krom} = \mathbf{NL}$
3. $\mathcal{SOLP}_{SKrom} = \mathbf{SymLog}$

Antecedentes: E. Grädel, TCS 1992.

Pero, nosotros caracterizamos directamente problemas de aproximación y observamos que con la posibilidad de contar (aprox.) basta variable X monádica para definir muchos problemas.

¿ Será suficiente X monádico para capturar estas clases? e.g. ¿ Es $\mathcal{SOMLP}_{Horn} = \mathbf{P}$?

Interés en $\mathcal{SOMLP}$: obtenemos todos los resultados sobre F-aproximaciones (incluyendo análogo a Lema Separación) en el contexto monádico.

y $\mathcal{SOMLP}$ es capaz de expresar problemas **NP**-completos

3. $\mathbf{CLIQUE}_{\geq r} := \{\mathcal{A} = \langle A, E\rangle : \mathcal{A}$ es un grafo y **al menos** una fracción r de A forman un grafo completo$\}$

Sea

$$\alpha_{cliq}(X) := \forall x \forall y (X(x) \wedge X(y) \wedge x \neq y \longrightarrow E(x,y))$$

Entonces

$$\mathcal{A}_n \in \mathbf{CLIQUE}_{\geq r} \iff \mathcal{A}_n \models (P(X) \geq r)\alpha_{cliq}(X)$$

Prop.: $\mathbf{CLIQUE}_{\geq r}$ es completo para **NP** via *log*.
(Pregunta: Será posible debilitar la reducción a *fop*?)

La Proximidad de $\mathcal{LP}_{MOD}$ con $\mathcal{LP}$

Para toda fórmula $\theta(\overline{x}) \in \mathcal{LP}(\Gamma)$, para todo $0 \leq \epsilon < 1$, la ϵ-aproximación de $\theta(\overline{x})$, $\theta_\epsilon(\overline{x})$ se define induct.:

Atomicas y sus negaciones $\theta_\epsilon(\overline{x})$ es igual a $\theta(\overline{x})$

Conjunción Si $\theta(\overline{x}) := \phi(\overline{x}) \wedge \psi(\overline{x})$ entonces
$\theta_\epsilon(\overline{x}) := \phi_\epsilon(\overline{x}) \wedge \psi_\epsilon(\overline{x})$.

Existencial Si $\theta(\overline{x}) := \exists z \phi(\overline{x}, z)$ entonces $\theta_\epsilon(\overline{x}) := \exists z \phi_\epsilon(\overline{x}, z)$.

Universal Si $\theta(\overline{x}) := \forall z \phi(\overline{x}, z)$ entonces
$\theta_\epsilon(\overline{x}) := (P(z) > 1 - \epsilon)\phi_\epsilon(\overline{x}, z)$.

Probabilidad Si $\theta(\overline{x}) := (P(z) > r)\phi(\overline{x}, z)$ entonces
$\theta_\epsilon(\overline{x}) := (P(z) > r - \min(\epsilon, r))\phi_\epsilon(\overline{x}, z)$.
Si $\theta(\overline{x}) := (P(z) \geq r)\phi(\overline{x}, z)$ entonces
$\theta_\epsilon(\overline{x}) := (P(z) \geq r - \min(\epsilon, r))\phi_\epsilon(\overline{x}, z)$.

(Antecedentes: Henson, Iovino, Ortiz - modelos para espacios de Banach)

Lema Puente: Fijemos n. Para toda fmla. $\theta(\overline{x}) \in \mathcal{LP}(\Gamma)$, para todo modelo aritmético $\mathcal{A}_m$ con $m > n^2$, para todo $\overline{a} < g_n(m)$, lo siguiente es cierto

$$\mathcal{A}_m^{g_n} \models \theta(\overline{a}) \text{ implica } \mathcal{A}_m \models \theta_{1/n}(\overline{a}).$$

Corolario: Si un problema B es expresable en $\mathcal{LP}_(MOD)$ (i.e. existe θ : para algún n, $\mathcal{A}_m \models_{g_n} \theta$ sii $\mathcal{A}_m \in B$, entonces

$$\begin{array}{lll} \text{si } \mathcal{A}_m \in B & \text{entonces} & \mathcal{A}_m \models \theta_{1/\sqrt{m}} \quad \text{y} \\ \text{si } \mathcal{A}_m \notin B & \text{entonces} & \mathcal{A}_m \models (\neg\theta)_{1/\sqrt{m}} \end{array}$$