Una mirada computacional a la lógica

(o de cómo ganar chicas hablando de lógica)

Daniel Gorín   Sergio Mera

Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales
Departamento de Computación

Charla de Borrachos 2004

Levante tradicional

Levante tradicional

La crisis de los fundamentos de la matemática

- A mediados del s. XIX se empieza a considerar la necesidad de *unificar* todo el conocimiento matemático en una teoría común
- Idea: Explicar todo a partir de la aritmética, y formalizar ésta utilizando dos herramientas novedosas:
  1. la lógica de primer orden
  2. la teoría de conjuntos
- Gottlob Frege se dedica, durante 40 años, a plasmar esta idea en dos gigantescos volúmenes
- En 1902, con el segundo volumen ya en la imprenta, Bertrand Russell encuentra una contradicción fundamental en la teoría de conjuntos usada por Frege

La crisis de los fundamentos de la matemática

- A mediados del s. XIX se empieza a considerar la necesidad de *unificar* todo el conocimiento matemático en una teoría común
- Idea: Explicar todo a partir de la aritmética, y formalizar ésta utilizando dos herramientas novedosas:
  1. la lógica de primer orden
  2. la teoría de conjuntos
- Gottlob Frege se dedica, durante 40 años, a plasmar esta idea en dos gigantescos volúmenes
- En 1902, con el segundo volumen ya en la imprenta, Bertrand Russell encuentra una contradicción fundamental en la teoría de conjuntos usada por Frege

La crisis de los fundamentos de la matemática

- A mediados del s. XIX se empieza a considerar la necesidad de *unificar* todo el conocimiento matemático en una teoría común
- Idea: Explicar todo a partir de la aritmética, y formalizar ésta utilizando dos herramientas novedosas:
  1. la lógica de primer orden
  2. la teoría de conjuntos
- Gottlob Frege se dedica, durante 40 años, a plasmar esta idea en dos gigantescos volúmenes
- En 1902, con el segundo volumen ya en la imprenta, Bertrand Russell encuentra una contradicción fundamental en la teoría de conjuntos usada por Frege

La crisis de los fundamentos de la matemática

- A mediados del s. XIX se empieza a considerar la necesidad de *unificar* todo el conocimiento matemático en una teoría común
- Idea: Explicar todo a partir de la aritmética, y formalizar ésta utilizando dos herramientas novedosas:
  1. la lógica de primer orden
  2. la teoría de conjuntos
- Gottlob Frege se dedica, durante 40 años, a plasmar esta idea en dos gigantescos volúmenes
- En 1902, con el segundo volumen ya en la imprenta, Bertrand Russell encuentra una contradicción fundamental en la teoría de conjuntos usada por Frege

La crisis de los fundamentos de la matemática (cont.)

La paradoja de Russell

- El *Conjunto Universal* es un conjunto cuyos elementos son todos los conjuntos, por lo tanto pertenece a sí mismo
- Claramente, no todo conjunto pertenece a sí mismo
- Sea, entonces, C el conjunto de todos los conjuntos que no pertenecen a sí mismos

---

- Pregunta: ¿Pertenece C a sí mismo?

La crisis de los fundamentos de la matemática (cont.)

La paradoja de Russell

- El *Conjunto Universal* es un conjunto cuyos elementos son todos los conjuntos, por lo tanto pertenece a sí mismo
- Claramente, no todo conjunto pertenece a sí mismo
- Sea, entonces, C el conjunto de todos los conjuntos que no pertenecen a sí mismos

---

- Pregunta: ¿Pertenece C a sí mismo?

La crisis de los fundamentos de la matemática (cont.)

La paradoja de Russell

- El *Conjunto Universal* es un conjunto cuyos elementos son todos los conjuntos, por lo tanto pertenece a sí mismo
- Claramente, no todo conjunto pertenece a sí mismo
- Sea, entonces, C el conjunto de todos los conjuntos que no pertenecen a sí mismos

---

- Pregunta: ¿Pertenece C a sí mismo?

La crisis de los fundamentos de la matemática (cont.)

La paradoja de Russell

- El *Conjunto Universal* es un conjunto cuyos elementos son todos los conjuntos, por lo tanto pertenece a sí mismo
- Claramente, no todo conjunto pertenece a sí mismo
- Sea, entonces, C el conjunto de todos los conjuntos que no pertenecen a sí mismos

---

- Pregunta: ¿Pertenece C a sí mismo?

La crisis de los fundamentos de la matemática (cont.)

La paradoja de Russell (cont.)

- Si C pertenece a sí mismo, entonces por definición no debe pertenecer a sí mismo
- Entonces C no pertenece a sí mismo. Pero nuevamente por su definición, C debe pertenecer a sí mismo

---

- Por lo tanto, nuestra noción de conjunto no está bien definida

La crisis de los fundamentos de la matemática (cont.)

La paradoja de Russell (cont.)

- Si C pertenece a sí mismo, entonces por definición no debe pertenecer a sí mismo
- Entonces C no pertenece a sí mismo. Pero nuevamente por su definición, C debe pertenecer a sí mismo

---

- Por lo tanto, nuestra noción de conjunto no está bien definida

La crisis de los fundamentos de la matemática (cont.)

La paradoja de Russell (cont.)

- Si C pertenece a sí mismo, entonces por definición no debe pertenecer a sí mismo
- Entonces C no pertenece a sí mismo. Pero nuevamente por su definición, C debe pertenecer a sí mismo

---

- Por lo tanto, nuestra noción de conjunto no está bien definida

Levante paradójico

Levante paradójico

Levante paradójico

Levante paradójico

El programa de Hilbert

- En 1900, David Hilbert presenta un programa con los problemas más importantes a resolver durante el s. XX dentro de los fundamentos de la matemática
- Buscaba formalizar la matemática y comprobar que ésta es:
  - I. Consistente: No se pueden "demostrar" tanto una afirmación matemática como su negación
  - II. Completa: Todas las afirmaciones matemáticas "verdaderas" pueden ser "demostradas"
  - III. Decidible: Existe una forma *mecánica* de decidir, dada cualquier afirmación matemática, si ésta es "verdadera" o "falsa"

El programa de Hilbert

- En 1900, David Hilbert presenta un programa con los problemas más importantes a resolver durante el s. XX dentro de los fundamentos de la matemática
- Buscaba formalizar la matemática y comprobar que ésta es:
  1. Consistente: No se pueden "demostrar" tanto una afirmación matemática como su negación
  2. Completa: Todas las afirmaciones matemáticas "verdaderas" pueden ser "demostradas"
  3. Decidible: Existe una forma *mecánica* de decidir, dada cualquier afirmación matemática, si ésta es "verdadera" o "falsa"

El programa de Hilbert

- En 1900, David Hilbert presenta un programa con los problemas más importantes a resolver durante el s. XX dentro de los fundamentos de la matemática
- Buscaba formalizar la matemática y comprobar que ésta es:
  1. Consistente: No se pueden "demostrar" tanto una afirmación matemática como su negación
  2. Completa: Todas las afirmaciones matemáticas "verdaderas" pueden ser "demostradas"
  3. Decidible: Existe una forma *mecánica* de decidir, dada cualquier afirmación matemática, si ésta es "verdadera" o "falsa"

El programa de Hilbert

- En 1900, David Hilbert presenta un programa con los problemas más importantes a resolver durante el s. XX dentro de los fundamentos de la matemática
- Buscaba formalizar la matemática y comprobar que ésta es:
  1. Consistente: No se pueden "demostrar" tanto una afirmación matemática como su negación
  2. Completa: Todas las afirmaciones matemáticas "verdaderas" pueden ser "demostradas"
  3. Decidible: Existe una forma *mecánica* de decidir, dada cualquier afirmación matemática, si ésta es "verdadera" o "falsa"

El programa de Hilbert, nace la computación!

Resultados de la investigación dentro del programa de Hilbert

- La teoría de las funciones recursivas
- Las máquinas de Turing y la teoría de la computabilidad
- El λ-cálculo

El programa de Hilbert, desilusión. . .

Kurt Gödel (1930-1933)

- La aritmética es incompleta
- No es posible "demostrar" la consistencia de la aritmética ni de la teoría de conjuntos

Alonzo Church y Alan Turing (1936-1937)

- La lógica de primer orden es indecidible:
    - No existe ningún "algoritmo" que dada una fórmula de primer orden nos diga si es *válida* o no

Paul Cohen (1963-1964)

- Demostró resultados importantes en donde la aritmética es incompleta (axioma de elección, hipótesis del continuo)

Levante independiente

Levante independiente

Levante independiente

Fórmulas satisfacibles

Definición informal

Una fórmula es *satisfacible* si puede ser verdadera en alguna interpretación

Ejemplo

$(\forall x)\,(\mathrm{presenteEnEstaCharla}(x) \rightarrow \mathrm{estaBorracho}(x))$

Ejemplo

$(\exists x)\,(\mathrm{presenteEnEstaCharla}(x) \wedge \neg \mathrm{estaBorracho}(x))$

Fórmulas satisfacibles

Definición informal

Una fórmula es *satisfacible* si puede ser verdadera en alguna interpretación

Ejemplo

$(\forall x)\,(\mathrm{presenteEnEstaCharla}(x) \rightarrow \mathrm{estaBorracho}(x))$

Ejemplo

$(\exists x)\,(\mathrm{presenteEnEstaCharla}(x) \wedge \neg \mathrm{estaBorracho}(x))$

Fórmulas satisfacibles

Definición informal

Una fórmula es *satisfacible* si puede ser verdadera en alguna interpretación

Ejemplo

$$(\forall x)\,(\mathrm{presenteEnEstaCharla}(x) \rightarrow \mathrm{estaBorracho}(x))$$

Ejemplo

$$(\exists x)\,(\mathrm{presenteEnEstaCharla}(x) \wedge \neg\mathrm{estaBorracho}(x))$$

Fórmulas válidas

Definición informal

Una fórmula es *válida* si tiene que ser verdadera, sin importar cómo la interpretemos

Ejemplo

$$(\forall x)\,(\mathrm{presenteEnEstaCharla}(x) \rightarrow \mathrm{estaBorracho}(x)) \lor (\exists x)\,(\mathrm{presenteEnEstaCharla}(x) \land \neg \mathrm{estaBorracho}(x))$$

Fórmulas válidas

Definición informal

Una fórmula es *válida* si tiene que ser verdadera, sin importar cómo la interpretemos

Ejemplo

$$(\forall x)\left(\text{presenteEnEstaCharla}(x) \rightarrow \text{estaBorracho}(x)\right) \lor$$
$$(\exists x)\left(\text{presenteEnEstaCharla}(x) \land \neg\text{estaBorracho}(x)\right)$$

Levante de primer orden

Levante de primer orden

Levante de primer orden

Proposicional vs. primer orden

- Todo lo que podemos decir en proposicional, lo podemos decir también en primer orden (i.e., primer orden es más expresiva)
- ¿Tiene sentido, entonces, usar proposicional para algo?
  - La lógica proposicional es decidible
  - Si nos alcanza con proposicional para describir nuestros problemas y queremos *razonar* sobre ellos, nos conviene usarla

Ejemplo – Diseño de circuitos lógicos

Razonamiento: El circuito A es mejor que el circuito B porque tiene menos compuertas lógicas (i.e., es más barato) pero, ¿son realmente equivalentes?

Proposicional vs. primer orden

- Todo lo que podemos decir en proposicional, lo podemos decir también en primer orden (i.e., primer orden es más expresiva)
- ¿Tiene sentido, entonces, usar proposicional para algo?
  - La lógica proposicional es decidible
  - Si nos alcanza con proposicional para describir nuestros problemas y queremos *razonar* sobre ellos, nos conviene usarla

Ejemplo – Diseño de circuitos lógicos

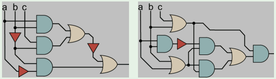
Razonamiento: El circuito A es mejor que el circuito B porque tiene menos compuertas lógicas (i.e., es más barato) pero, ¿son realmente equivalentes?

Proposicional vs. primer orden

- Todo lo que podemos decir en proposicional, lo podemos decir también en primer orden (i.e., primer orden es más expresiva)
- ¿Tiene sentido, entonces, usar proposicional para algo?
  - La lógica proposicional es decidible
  - Si nos alcanza con proposicional para describir nuestros problemas y queremos *razonar* sobre ellos, nos conviene usarla

Ejemplo – Diseño de circuitos lógicos

Razonamiento: El circuito A es mejor que el circuito B porque tiene menos compuertas lógicas (i.e., es más barato) pero, ¿son realmente equivalentes?



¿Existen cosas en el medio?

- Problema: Proposicional queda chico demasiado rápido (es muy poco expresivo)
- ¿Estamos condenados a usar en esos casos primer orden, que es indecidible?
- NO! (gracias a Dios, sino no tendríamos trabajo. . .)

¿Existen cosas en el medio?

- Problema: Proposicional queda chico demasiado rápido (es muy poco expresivo)
- ¿Estamos condenados a usar en esos casos primer orden, que es indecidible?
- NO! (gracias a Dios, sino no tendríamos trabajo. . .)

¿Existen cosas en el medio?

- Problema: Proposicional queda chico demasiado rápido (es muy poco expresivo)
- ¿Estamos condenados a usar en esos casos primer orden, que es indecidible?
- NO! (gracias a Dios, sino no tendríamos trabajo. . .)

Más allá de la lógica proposicional (pero no tanto)

Lógicas modales

- Podemos extender la lógica proposicional agregando modalidades
- Modalidades clásicas: $\Box$, $\Diamond$

Ejemplo – Una fórmula modal

$$\Box(p \wedge \Diamond q) \leftrightarrow \neg\Diamond(\neg p \vee \neg\Box q)^{1}$$

[1] Es obvio lo que significa, no?

Más allá de la lógica proposicional (pero no tanto)

Lógicas modales

- Podemos extender la lógica proposicional agregando modalidades
- Modalidades clásicas: $\Box$, $\Diamond$

Ejemplo – Una fórmula modal

$$\Box(p \wedge \Diamond q) \leftrightarrow \neg\Diamond(\neg p \vee \neg\Box q)^1$$

[1] Es obvio lo que significa, no?

Más allá de la lógica proposicional (pero no tanto)

Lógicas modales

- Podemos extender la lógica proposicional agregando modalidades
- Modalidades clásicas: $\Box, \Diamond$

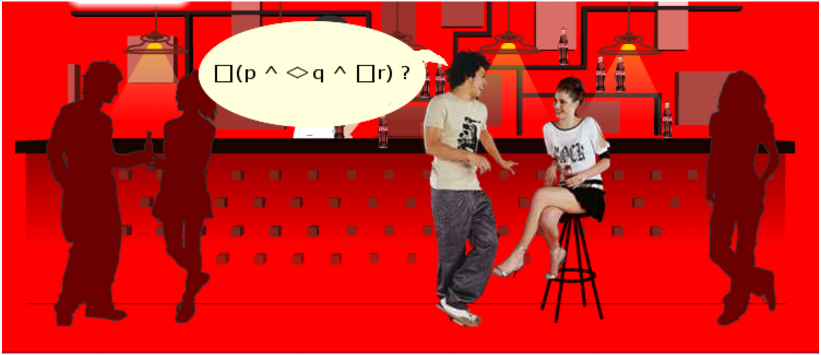
Ejemplo – Una fórmula modal

$$\Box(p \wedge \Diamond q) \leftrightarrow \neg\Diamond(\neg p \vee \neg\Box q)^{1}$$

[1] Es obvio lo que significa, no?

Levante □

Levante □



Levante □

Levante □

Logicas modales al mejor precio. Llame ya!

- Las modalidaes $\Box$ y $\Diamond$ se pueden interpretar de distintas formas
- Cada interpretación nos da una lógica modal distinta

Interpretaciones clásicas de $\Box\varphi$

- Es necesario que φ sea verdadero
- De aquí en más, siempre en el futuro será verdadero φ
- Es obligatorio que se cumpla φ
- Determinado sujeto sabe que φ es verdadero
- Después de ejecutar cierto programa, φ siempre vale

Logicas modales al mejor precio. Llame ya!

- Las modalidaes $\Box$ y $\Diamond$ se pueden interpretar de distintas formas
- Cada interpretación nos da una lógica modal distinta

Interpretaciones clásicas de $\Box\varphi$

- Es necesario que φ sea verdadero
- De aquí en más, siempre en el futuro será verdadero φ
- Es obligatorio que se cumpla φ
- Determinado sujeto sabe que φ es verdadero
- Después de ejecutar cierto programa, φ siempre vale

Esto es más grosso que proposicional

Un esquema de razonamiento para $\Box$ como siempre en el futuro

$$\frac{\Box\varphi \to \Box\Box\varphi}{\begin{array}{l} \Box estoy\_borracho \to \Box\Box estoy\_borracho \\ \Box(encaro\_minas \wedge pierdo) \to \Box\Box(encaro\_minas \wedge pierdo) \\ \Box\Box tengo\_caspa \to \Box\Box\Box tengo\_caspa \\ \vdots \end{array}}$$

Características computacionalmente copadas

- A pesar de ser más expresivas que proposicional, estas lógicas también son decidibles
- Su complejidad, sin embargo, es más alta:
  1. Proposicional: NP-completo
  2. Lógicas modales clásicas: PSPACE-completo

(sin entrar en detalles: $NP \subseteq PSPACE$)

Características computacionalmente copadas

- A pesar de ser más expresivas que proposicional, estas lógicas también son decidibles
- Su complejidad, sin embargo, es más alta:
    1. Proposicional: NP-completo
    2. Lógicas modales clásicas: PSPACE-completo

(sin entrar en detalles: $NP \subseteq PSPACE$)

Primer orden y más allá

Algunas lógicas que escapan a primer orden

- Lógicas de segundo orden
  - Incluyen toda la lógica de primer orden
  - Pero también permiten cuantificar predicados
- Operadores de punto fijo
  - Incluyen toda la lógica de primer orden
  - Pero son menos expresivas que segundo orden
- PDL (Propositional Dynamic Logic)
  - Infinitas modalidades
  - Operador de clausura transitiva
  - Su poder expresivo se solapa con el de primer orden
  - Es decidible!

Primer orden y más allá

Algunas lógicas que escapan a primer orden

- Lógicas de segundo orden
  - Incluyen toda la lógica de primer orden
  - Pero también permiten cuantificar predicados
- Operadores de punto fijo
  - Incluyen toda la lógica de primer orden
  - Pero son menos expresivas que segundo orden
- PDL (Propositional Dynamic Logic)
  - Infinitas modalidades
  - Operador de clausura transitiva
  - Su poder expresivo se solapa con el de primer orden
  - Es decidible!

Primer orden y más allá

Algunas lógicas que escapan a primer orden

- Lógicas de segundo orden
  - Incluyen toda la lógica de primer orden
  - Pero también permiten cuantificar predicados
- Operadores de punto fijo
  - Incluyen toda la lógica de primer orden
  - Pero son menos expresivas que segundo orden
- PDL (Propositional Dynamic Logic)
  - Infinitas modalidades
  - Operador de clausura transitiva
  - Su poder expresivo se solapa con el de primer orden
  - Es decidible!

Levante de orden superior

Levante de orden superior

Levante de orden superior

El karma en las lógicas

¿Qué hay que considerar al momento de elegir una lógica?

- Debería estar claro que no hace falta quedarse con primer orden
- Algunas lógicas ofrecen una sintaxis más apropiada para un contexto que otras
- En general, cuanto más poder expresivo buscamos, mayor complejidad obtenemos. Hay que encontrar un balance (ingeniería de lenguajes)
- Una actividad del grupo consiste en investigar el poder expresivo y la complejidad de distintas lógicas, especialmente modales

El karma en las lógicas

¿Qué hay que considerar al momento de elegir una lógica?

- Debería estar claro que no hace falta quedarse con primer orden
- Algunas lógicas ofrecen una sintaxis más apropiada para un contexto que otras
- En general, cuanto más poder expresivo buscamos, mayor complejidad obtenemos. Hay que encontrar un balance (ingeniería de lenguajes)
- Una actividad del grupo consiste en investigar el poder expresivo y la complejidad de distintas lógicas, especialmente modales

El karma en las lógicas

¿Qué hay que considerar al momento de elegir una lógica?

- Debería estar claro que no hace falta quedarse con primer orden
- Algunas lógicas ofrecen una sintaxis más apropiada para un contexto que otras
- En general, cuanto más poder expresivo buscamos, mayor complejidad obtenemos. Hay que encontrar un balance (ingeniería de lenguajes)
- Una actividad del grupo consiste en investigar el poder expresivo y la complejidad de distintas lógicas, especialmente modales

El karma en las lógicas

¿Qué hay que considerar al momento de elegir una lógica?

- Debería estar claro que no hace falta quedarse con primer orden
- Algunas lógicas ofrecen una sintaxis más apropiada para un contexto que otras
- En general, cuanto más poder expresivo buscamos, mayor complejidad obtenemos. Hay que encontrar un balance (ingeniería de lenguajes)
- Una actividad del grupo consiste en investigar el poder expresivo y la complejidad de distintas lógicas, especialmente modales

Demostración automática

¿Para qué?

- Verificación de demostraciones matemáticas complejas (Teorema de Fermat, Conjetura de Kepler)
- Procesamiento de lenguaje natural
- Bases de conocimiento
- Cambio de creencias
- Verificación de software

Demostración automática

¿Para qué?

- Verificación de demostraciones matemáticas complejas (Teorema de Fermat, Conjetura de Kepler)
- Procesamiento de lenguaje natural
- Bases de conocimiento
- Cambio de creencias
- Verificación de software

Demostración automática

¿Para qué?

- Verificación de demostraciones matemáticas complejas (Teorema de Fermat, Conjetura de Kepler)
- Procesamiento de lenguaje natural
- Bases de conocimiento
- Cambio de creencias
- Verificación de software

Demostración automática

¿Para qué?

- Verificación de demostraciones matemáticas complejas (Teorema de Fermat, Conjetura de Kepler)
- Procesamiento de lenguaje natural
- Bases de conocimiento
- Cambio de creencias
- Verificación de software

Demostración automática

¿Para qué?

- Verificación de demostraciones matemáticas complejas (Teorema de Fermat, Conjetura de Kepler)
- Procesamiento de lenguaje natural
- Bases de conocimiento
- Cambio de creencias
- Verificación de software

Demostración automática (cont.)

¿Qué es?

- Es un "algoritmo" que verifica si una fórmula se deduce de un conjunto de fórmulas
- Los demostradores se pueden clasificar en dos categorías:
  - Demostradores asistidos
  - Demostradores automáticos
- Existen "demostradores" para lógicas indecidibles (como primer orden), pero el interés de nuestro grupo está puesto en demostradores para lógicas decidibles

Demostración automática (cont.)

¿Qué es?

- Es un "algoritmo" que verifica si una fórmula se deduce de un conjunto de fórmulas
- Los demostradores se pueden clasificar en dos categorías:
  - Demostradores asistidos
  - Demostradores automáticos
- Existen "demostradores" para lógicas indecidibles (como primer orden), pero el interés de nuestro grupo está puesto en demostradores para lógicas decidibles

Demostración automática (cont.)

¿Qué es?

- Es un "algoritmo" que verifica si una fórmula se deduce de un conjunto de fórmulas
- Los demostradores se pueden clasificar en dos categorías:
  - Demostradores asistidos
  - Demostradores automáticos
- Existen "demostradores" para lógicas indecidibles (como primer orden), pero el interés de nuestro grupo está puesto en demostradores para lógicas decidibles

Un buen ejemplo de bases de conocimiento

Edipo y Yocasta: un problema de familia

- Edipo *EsHijoDe* Yocasta
- Polínices *EsHijoDe* Edipo
- Edipo *EsPatricida*
- Polínices *EsHijoDe* Yocasta
- Tersandro *EsHijoDe* Polínices
- Tersandro **no** *EsPatricida*

¿Hay algún hijo patricida de Yocasta que tenga un hijo no patricida?

A brindar!


Che, por suerte se terminó esta farsa del levante, no?
Si, ya no lo soportaba más...