Matemática Reversa.

Antonio Montalbán.
University of Chicago.

Diciembre 2011

Matemática Reversa

Matemática Reversa es el programa cuya *pregunta principal* es

“Qué axiomas son realmente necesarios en matemática?”

considerada en el entorno de la aritmética de segundo orden.

La pregunta principal

Qué axiomas son realmente necesarios en matemática?

Es una pregunta muy vieja.
Los matemáticos griegos ya se preguntaban si el 5to postulado de Euclides es necesario para la geometría.

Motivaciones:

- Filosofía – Entender las *fundaciones* que soportan la matemática que hacemos hoy.
- Matemática Pura – Estudiar la *complejidad computacional* de los objetos y las construcciones que usamos en matemática.

La pregunta principal: en detalle

1. Fijemos una teoría *base*.
   (Usamos RCA_0: *los conjuntos computables existen*)
2. Elijamos un teorema T.
3. Cuáles axiomas hay que agregar RCA_0 para probar T?
4. Supongamos que encontramos axiomas $A_0, ..., A_k$ tales que
   $$\mathrm{RCA}_0 \text{ prueba } A_0 \,\&\, ... \,\&\, A_k \Rightarrow T.$$
   Cómo sabemos que son necesarios?
5. Muchas veces RCA_0 también prueba $T \Rightarrow A_0 \,\&\, ... \,\&\, A_k$
6. En ese caso sabríamos que $\mathrm{RCA}_0 + A_0, ..., A_k$ es el menor sistema (extendiendo RCA_0) donde podemos probar T.

El contexto de la Matemática reversa

Aritmética de segundo orden (ASO).

- *ASO* es mucho más débil que la teoría de conjuntos (ZFC).
- *ASO* es suficientemente poderosa para desarrollar la mayoría de la matemática.
- *ASO* es suficientemente débil como para permitir calibrar los diferentes teoremas.

Toda la matemática numerable se puede desarrollar en ASO.
Ésto incluye:

- Álgebra numerable,
- Combinatoria,
- Números reales,
- Variedades, funciones continuas, ecuaciones diferenciales...
- Espacios métricos separables y completos.
- ....

Axiomas de ASO

Sólo tenemos números naturales y conjuntos de números naturales.

Axiomas de semi-anillo: $\mathbb{N}$ es un semi-anillo ordenado.

Axiomas de Inducción: Para toda formula $\varphi(n)$,
$IND(\varphi)$ $\quad (\varphi(0) \ \& \ \forall n(\varphi(n) \Rightarrow \varphi(n+1))) \Rightarrow \forall n \varphi(n)$

Axiomas de Comprensión: Para toda formula $\varphi(n)$
$CA(\varphi)$ $\quad \exists X \forall n \ (n \in X \Leftrightarrow \varphi(n))$

Base RCA_0 consiste en: Ax. de semi-anillo + Σ^0_1-IND+ Δ^0_1-CA.

Δ^0_1-CA: para todo programa p, existe un conjunto X tal que

$$n \in X \Leftrightarrow p(n) = \text{s}i$$

(donde p siempre para, y puede usar información de conjuntos que existen)

Ejemplos

Teorema

Los siguientes son equivalentes sobre RCA_0:

- Weak König's lemma (WKL): *Todo árbol binario infinito tiene un camino infinito.*
- *Toda función continua en $[0,1]$ se puede aproximar por polinomios.*
- *Toda función continua en $[0,1]$ es integrable de Riemann.*
- *Todo espacio vectorial de dim>1 tiene un sub-espacio propio.* *[DHKLMM 07]*
- *Todo anillo artiniano abeliano es noetheriano.* *[Conidis 11]*

Teorema

Los siguientes son equivalentes sobre RCA_0:

- Arithmetic Comprehension Ax. (ACA): *$CA(\varphi)$ para φ sin cuantificadores de conjuntos.*
- *El problema de la detención existe relativo a cualquier oráculo.*
- *Toda secuencia acotada de numero reales tiene una sub-secuencia convergente.*
- *Todo espacio vectorial tiene una base.*
- *Todo anillo artiniano abeliano tiene largo finito [Conidis 09]*

Más ejemplos

Teorema

Los siguientes son equivalentes sobre RCA_0:

- Arithmetic Transfinite Recursion (ATR_0).
- *Todo conjunto cerrado no numerable de $[0,1]$ tiene un subconjunto perfecto.*
- *En todo juego de terminación finita, con infinitos movimientos, uno de los jugadores tiene estrategia ganadora.* [Steel 78]

Def: C es *perfecto* si es cerrado y $C' = C$.

Teorema

Los siguientes son equivalentes sobre RCA_0:

- (Π^1_1-CA_0): *$CA(\psi)$ para $\psi \equiv \forall X \subseteq \mathbb{N}\ \varphi(X)$, y φ sin cuantificadores sobre conjuntos.*
- *Todo subconjunto cerrado de $[0,1]$ es la unión de un conjunto perfecto y uno numerable.*
- *Todo grupo abeliano numerable es la suma de un divisible y uno reducido.*

Def: Un grupo G es *divisible* $\forall a \in G \forall n \in \mathbb{N} \exists b(nb = a)$.

Def: Un grupo G es *reducido* si no tiene subconjuntos divisibles.

El fenómeno de los “cinco grandes”

Luego de algunas décadas, y muchos investigadores trabajando en este programa, se descubrió el siguiente fenómeno:

Hay *5* sistemas de axiomas tales que *la mayoría* de los teoremas en matemática son equivalentes a uno de ellos.

$$\begin{array}{c} \Pi^1_1\text{-CA}_0 \\ | \\ \text{ATR}_0 \\ | \\ \text{ACA}_0 \\ | \\ \text{WKL}_0 \\ | \\ \text{RCA}_0 \end{array}$$

El fenómeno de los "cinco grandes"!

Sin razón aparente, los cinco grandes:

1. están ordenados en *linea*,
2. son muy *pocos*,
3. tienen un *tope* muy bajo.

$$\begin{array}{c} \Pi^1_1\text{-}\mathsf{CA}_0 \\ | \\ \mathsf{ATR}_0 \\ | \\ \mathsf{ACA}_0 \\ | \\ \mathsf{WKL}_0 \\ | \\ \mathsf{RCA}_0 \end{array}$$

Ambición a largo plazo: *entender por qué.*

Consistencia

Sean S y T conjuntos de axiomas y sentencias. Definimos

$$S \preccurlyeq T \quad \Leftrightarrow \quad \mathsf{RCA}_0 \vdash \mathrm{Consistencia(T)} \rightarrow \mathrm{Consistencia(S)},$$

donde $\mathrm{Consistencia(T)} \equiv$ "ninguna contradicción se deriva de T."

Hecho empírico:

Entre **todos** los conjuntos de axiomas *naturales*,

$\preccurlyeq$ es linealmente ordenado.

La conjetura de Martin

Def: Dado $X, Y\colon \mathbb{N} \to \{0,1\}$, definimos $X \leqslant_T Y$ si
X puede ser computado a partir de Y.

Def: X y Y *tienen el mismo grado* si $X \leqslant_T Y$ y $Y \leqslant_T X$.

Def: $A \subseteq 2^{\mathbb{N}}$ *tiene medida de Martin 1* si $\exists X\ \forall Y \geqslant_T X\ (Y \in A)$.

Teo:[Martin] Para todo conjunto Borel $\mathcal{A} \subseteq 2^{\mathbb{N}}$ que preserva grado, o A, o $2^{\mathbb{N}} \setminus A$ tiene medida de Martin 1.

Conjetura de Martin: Si $f, g\colon 2^{\mathbb{N}} \to 2^{\mathbb{N}}$ son Borel y preservan grado, entonces o $f(X) \leqslant_T g(X)$ o $g(X) \leqslant_T f(X)$,
en un conjunto de medida de Martin 1, etc.

Teo:[Slaman, Steel] La conjetura de Martin’s es cierta para funciones Borel que preservan grado uniformemente.

Sistemas robustos

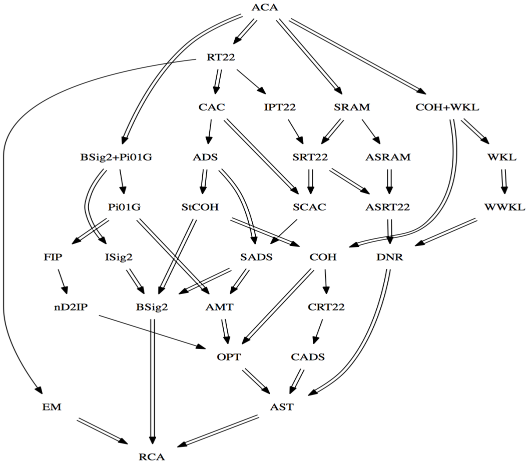
Def [M 05]: Decimos que un sistema de axiomas es *robusto* si es equivalente a toda perturbación pequeña de si mismo.

No tenemos una definición formal de sistema robusto

- Los cinco grandes son robustos.
- Casi ningún otro sistema es robusto.

Ejemplo 1: El zoológico debajo del teorema de Ramsey

RT^2_2: Todo 2-coloramiento de $[\mathbb{N}]^2$ tiene un conjunto infinito monocromático.



RT^2_2 **no** es robusto.

Diagrama robado de la pagina de Dzhafarov.

Conjetura de Fraïssé

Teorema [Conjetura de Fraïssé '48; Laver '71]
FRA: Los ordenes lineales forman un WQO con respecto a la inmersiones.
(i.e., no hay secuencias descendientes infinitas y no hay anti-cadenas infinitas.)

Conjetura:[Clote '90][Simpson '99][Marcone]
FRA es equivalente a ATR_0 sobre RCA_0.

$$\begin{tikzcd}
\Pi^1_2\text{-}CA_0 \arrow[d] \arrow[ddr] & \\
\Pi^1_1\text{-}CA_0 \arrow[dd] & \\
& \text{FRA} \arrow[dl] \\
ATR_0 \arrow[d] & \\
ACA_0 \arrow[d] & \\
WKL_0 \arrow[d] & \\
RCA_0 &
\end{tikzcd}$$

Ejemplo 2: Conjetura de Fraïssé

Postulado ([M 05])

RCA_0+FRA es el menor sistema donde es posible desarrollar una teoría razonable de ordenes lineales y la inmersiones.

[M 05] FRA es robusto.

Theorem ([M 05][Kach,Marcone,M,Weiermann 11])

Los siguientes son equivalentes sobre RCA_0

- *FRA;*
- *Para todo $\mathcal{L}$ numerable, existe $n_{\mathcal{L}} \in \mathbb{N}$, tal que: si $\mathcal{L}$ es coloreado con una cantidad finita de colores, hay una inmersión $\mathcal{L} \to \mathcal{L}$ cuya imagen tiene como máximo $n_{\mathcal{L}}$ colores.*
- *Todo ord. lin. disperso es una suma finita de indescomponibles;*
- *Todo ord. lin. indescomponible es una ω-suma o una ω^*-suma de indescomponibles menores;*
- *La caracterización de Jullien de ordenes extendibles;*
- *etc.*

El tope

Def: Π^1_n*-formula:* $\underbrace{\forall X_1\ \exists X_2 \cdots}_{n \text{ alternaciones}} \qquad \overbrace{\varphi(X_1,...,X_n)}^{\text{sin cuantificadores sobre conjuntos}}$

Def: Π^1_n-$CA_0 = RCA_0 +$ "$\{n \in \mathbb{N} : \psi(n)\}$ existe" para toda formula Π^1_n ψ.

Obs: $ASO = \bigcup_{n\in\mathbb{N}} \Pi^1_n$-$CA_0$.

No conocemos casi ningún ejemplo de teoremas más allá de Π^1_1-CA_0.

Determinación

Fijemos un conjunto A de secuencias en $\mathbb{N}^{\mathbb{N}}$.

Jugador I	a_0		a_2		$\cdots$	sea $\bar{a}$ =
Jugador II		a_1		a_3	$\cdots$	$(a_0, a_1, a_2, a_3, \ldots)$

El jugador I *gana* si $\bar{a} \in A$, y el jugador II *gana* si $\bar{a} \in \mathbb{N}^{\mathbb{N}} \setminus A$.

$A \subseteq \mathbb{N}^{\mathbb{N}}$ es *determinado*
si hay una estrategia ganadora uno de los jugadores.

Obs: No todo $A \subseteq \mathbb{N}^{\mathbb{N}}$ es determinado.

La fuerza de la determinación

Γ	complejidad de "Todo conjunto en Γ es determinado"	
abierto	ATR_0	[Steel 78]
F_σ	Σ^1_1-ID_0	[Tanaka 91]
$F_{\sigma\delta}$	Π^1_3-$\mathsf{CA}_0 \vdash$ .. $\quad \Delta^1_3$-$\mathsf{CA}_0 \nvdash$ ..	[Welch 09]
$F_{\sigma\delta\sigma}$	ASO$\nvdash$ ..	[Martin] [Friedman 71]
Borel	$\aleph_1$ iteraciones del axioma de la potencia	[Martin 75] [Friedman 71]
imagen Borel	$\forall x(x^\sharp$ existe)	[Martin 75] [Harrington 78]
Proyectivo	infinitos cardinales de Woodin	[Martin, Steel 88]

Determinación en ASO

Cuanta determinación se puede demostrar
sin usar objetos no numerables?

Teorema (esencialmente debido a Martin, [M,Shore 09])

Dado $n \in \mathbb{N}$, ASO puede demostrar que toda combinación Booleana de n conjuntos $F_{\sigma\delta}$ es determinada.

donde $F_{\sigma\delta}$ = intersección de uniones de conjuntos cerrados

Pero....
Mientras más grande es n, más axiomas se necesitan.

Teorema ([M,Shore 09])

ASO no puede probar que toda combinación Booleana de $F_{\sigma\delta}$ conjuntos es determinada.