Il programma
"Univalent Foundations of Mathematics"
di Vladimir Voevodsky

Nicola Gambino

Università degli Studi di Palermo

17 maggio 2012

Vladimir Voevodsky

1989 Laurea, Moscow State University
1992 Dottorato, Harvard
1998 Dimostra la congettura di Milnor ($\mathbb{A}^1$-homotopy theory)
2002 Medaglia Fields
2009 Dimostra la congettura di Bloch-Kato

"While working on the completion of the Bloch-Kato conjecture I have thought a lot about what to do next.

Eventually I became convinced that the most interesting and important directions in current mathematics are the ones related to the transition into a new era which will be characterized by the widespread use of automated tools for proof construction and verification."

V. Voevodsky (2010)

Univalent Foundations of Mathematics

Caratteristiche principali:

- Assiomatizza la nozione di spazio
- Formalizzata utilizzando la teoria dipendente dei tipi
- Facilita la costruzione e la verifica della correttezza di dimostrazioni matematiche al calcolatore
- Pemette di identificare oggetti isomorfi

Tutti questi aspetti segnano differenze significative con le familiari fondazioni insiemistiche.

Organizzazione del seminario

- Parte I: Spazi
- Parte II: Teorie dipendenti dei tipi
- Parte III: Univalent Foundations

Parte I

Spazi

Spazi (in ZF)

Definizione. Uno **spazio topologico** è una coppia

$$(A, \mathcal{O}(A))$$

ove A è un insieme e $\mathcal{O}(A)$ è una famiglia di sottoinsiemi di A tale che ...

Idea. Un insieme di punti con una nozione di vicinanza.

Esempi: $\mathbb{R}$, $[0,1]$, $\{*\}$, ...

Nota. Ci sono molti modi per costruire nuovi spazi a partire da spazi dati, *e.g.*

$$A \times B\,, \quad A^{[0,1]}\,, \quad \ldots$$

Omotopia

Due spazi A, B sono detti **omotopicamente equivalenti** se esiste una deformazione continua che trasforma A in B.

Esempio

- Tazze (con un manico) e ciambelle (con un buco)
- Cerchio $\not\simeq$ circonferenza

Uno spazio A è detto **contrattile** se è omotopicamente equivalente a $\{*\}$.

Esempi

- $[0, 1]$
- $\mathbb{R}$

La gerarchia omotopica

Definizione.

- Uno spazio A ha livello omotopico 0 se è contrattile.
- Uno spazio A ha livello omotopico $n+1$ se per ogni $x, y \in A$, lo spazio dei cammini da x a y ha livello n.

Osservazione.

$$\begin{array}{lcl} A \text{ di livello } 0 & \Leftrightarrow & A = \{*\} \\ A \text{ di livello } 1 & \Leftrightarrow & A \in \{\top, \bot\} \\ A \text{ di livello } 2 & \Leftrightarrow & A \text{ insieme} \\ A \text{ di livello } 3 & \Leftrightarrow & A \text{ gruppoide} \\ & \vdots & \end{array}$$

Nota. Tipo di omotopia n = spazio di livello $n+2$.

Idea

Fondazioni insiemistiche

- Nozione primitive: proposizione, insieme
- Nozione definite: spazio, ...

Fondazioni univalenti

- Nozione primitiva: spazio
- Nozione definite: proposizione, insieme, ...

Problema. Come realizzare formalmente quest'idea?

Parte II

Teorie dei tipi

Le teorie dipendenti dei tipi

Origini

- Definire la nozione di dimostrazione costruttiva (Curry, Howard, de Bruijn, Scott, Martin-Löf, ...)
- Fondamenti dei linguaggi di programmazione funzionali

Forme di giudizio

$$A : \text{type}\,, \quad a : A\,, \quad A = B : \text{type}\,, \quad a = b : A$$

Esempio: tipi funzione

$$\frac{A : \text{type} \qquad B : \text{type}}{A \to B : \text{type}}$$

$$\frac{x : A \vdash f(x) : B}{(\lambda x : A) f(x) : A \to B}$$

$$\frac{f : A \to B \qquad a : A}{\text{app}(f, a) : B}$$

$$\frac{x : A \vdash f(x) : B \qquad a : A}{\text{app}((\lambda x : A) f(x), a) = f(a) : A \to B}$$

Esempio: tipi identità

$$\frac{A : \text{type} \qquad a : A \qquad b : A}{\mathrm{Id}_A(a, b) : \text{type}}$$

$$\frac{a : A}{\mathrm{refl}(a) : \mathrm{Id}_A(a, a)}$$

$$\frac{\begin{array}{l} p : \mathrm{Id}_A(a, b) \\ x : A, y : A, u : \mathrm{Id}_A(x, y) \vdash C(x, y, u) : \text{type} \\ x : A \vdash d(x) : C(x, x, \mathrm{refl}(x)) \end{array}}{\mathrm{J}(a, b, p, d) : C(a, b, p)}$$

$$\frac{\begin{array}{l} a : A \\ x : A, y : A, u : \mathrm{Id}_A(x, y) \vdash C(x, y, u) : \text{type} \\ x : A \vdash d(x) : C(x, x, \mathrm{refl}(x)) \end{array}}{\mathrm{J}(a, a, \mathrm{refl}(a), d) = d(a) : C(a, a, \mathrm{refl}(a))}$$

Teorie estensionali e teorie intensionali

Le teorie estensionali hanno anche la regola

$$\frac{p : \mathrm{Id}_A(a, b)}{a = b : A}$$

Problema

- Il problema di *type-checking*, ovvero decidere se

  $$\Gamma \vdash a : A$$

  è derivabile, diventa indecidibile.

Coq

Un software sviluppato all'INRIA che

- aiuta la costruzione di dimostrazioni, verificandone la correttezza
- aiuta la scrittura di programmi dimostrabilmente corretti.

Base teorica

- Calcolo delle Costruzioni (Coquand e Huet 1988)
- Calcolo delle Costruzioni Induttive (Coquand e Paulin-Mohring 1990)
- Calcolo Predicativo delle Costruzioni Induttive (2009)

Esempio di formalizzazione

- Teorema fondamentale dell'algebra

Parte III

Univalent Foundations

Dizionario tra teoria dell'omotopia e teoria dei tipi

Teoria dei tipi	**Topologia**
$A : \text{type}$	A spazio
$a : A$	$a \in A$
$x : A \vdash B(x) : \text{type}$	$\begin{array}{c} B \\ \downarrow \text{ fibrazione} \\ A \end{array}$
$x : A, y : A \vdash \mathrm{Id}_A(x, y)$	$\begin{array}{c} A^{[0,1]} \\ \downarrow \\ A \times A \end{array}$

Nota. Hofmann, Streicher, Awodey, Warren, Garner, van den Berg, Lumsdaine, Shulman, ...

La gerarchia omotopica in teoria dei tipi

Con questo dizionario, Voevodsky ha definito in teoria dei tipi

- la nozione di contrattibilità di un tipo A,
- una controparte della gerarchia omotopica,
- ...

Quest'idea permette un nuovo sviluppo della matematica:

- proposizione $\Leftrightarrow$ tipo di livello omotopico 1
- insieme $\Leftrightarrow$ tipo di livello omotopico 2

Nota. Formalizzabile in Coq

Alcune nozioni fondamentali

- Dati $A : \mathrm{type}$, $f : A \to B$ e $b : B$, definiamo

$$\mathrm{hfiber}(f, b) =_{\mathrm{def}} (\Sigma x : A)\mathrm{Id}_B(\mathrm{app}(f, a), b)$$

- Dato $A : \mathrm{type}$, definiamo

$$\mathrm{iscontr}(A) =_{\mathrm{def}} (\Sigma x : A)(\Pi y : A)\mathrm{Id}_A(x, y)$$

- Data $f : A \to B$, definiamo

$$\mathrm{isweq}(f) =_{\mathrm{def}} (\Pi y : B)\mathrm{iscontr}(\mathrm{hfiber}(f, y))$$

Nota. I tipi $\mathrm{iscontr}(A)$ e $\mathrm{isweq}(f)$ sono di livello 1, *i.e.* proposizioni.

L'Assioma di Univalenza

Fissato un universo U e $A, B : \mathsf{U}$, abbiamo

- $\mathrm{Weq}(A, B)$, il tipo delle equivalenze deboli tra A e B
- $\mathrm{Id}_{\mathsf{U}}(A, B)$, il tipo delle dimostrazioni che A e B sono uguali
- una funzione

$$w_{A,B} : \mathrm{Id}_{\mathsf{U}}(A, B) \to \mathrm{Weq}(A, B)$$

Assioma di Univalenza. La mappa $w_{A,B}$ è una equivalenza debole, per ogni $A, B : \mathsf{U}$.

Idea. Strutture isomorfe sono uguali.

Prospettive future

- Sviluppo della matematica, *e.g.*
  - Strutture algebriche su insiemi (livello 2)
  - Strutture categoriali su gruppoidi (livello 3)
  - ...
- Formulazione di controparti in teoria di tipi di spazi complessi
- Nuova versione di Coq?

Anno tematico all'Institute for Advanced Study nel 2012/13

Alcune risorse utili

`http://www.math.ias.edu/~vladimir`

`http://homotopytypetheory.org`