Determinare la terminazione di programmi con il Teorema di Ramsey

Silvia Steila,
joint work with Stefano Berardi

Università degli studi di Torino

SELP - Università degli studi di Salerno
6 Giugno 2014

Teorema di Ramsey Finito

Quante persone devo invitare a una festa per avere che almeno n di loro si conoscono mutualmente oppure almeno n non si conoscono affatto?

Se in una festa ci sono almeno 6 persone allora 3 di loro si conoscono oppure 3 di loro non si conoscono.

Se in una festa ci sono almeno 18 persone allora 4 di loro si conoscono oppure 4 di loro non si conoscono.

Teorema di Ramsey Finito

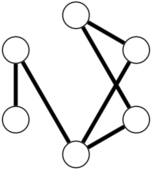
Quante persone devo invitare a una festa per avere che almeno n di loro si conoscono mutualmente oppure almeno n non si conoscono affatto?

Come possiamo sapere che tale numero esiste per ogni n?

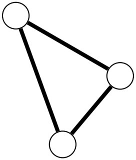
Grazie a F.P. Ramsey!

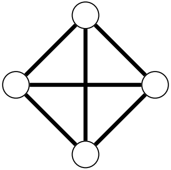
Qualche definizione in Teoria dei Grafi

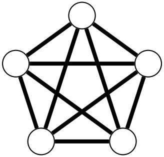
Un grafo è una coppia ordinata $G = (V, E)$ composta da un insieme V dei vertici e dall'insieme E dei lati, che sono sottoinsiemi di V composti da due elementi distinti.



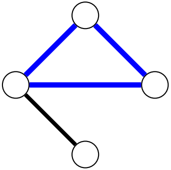
Un grafo è completo se per ogni coppia di vertici distinti esiste un lato che li connette. Per ogni $n \in \mathbb{N}$, K_n è il grafo completo con n vertici.

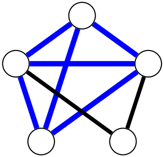






Una cricca in un grafo è un sottoinsieme V' di V tale che ogni coppia di vertici in V' è connessa da un lato.

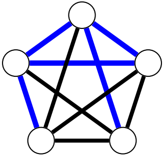




Sia $r \in \mathbb{N}$. Una colorazione dei lati di un grafo con r colori è una funzione

$$c : E \to r.$$

Una colorazione dei lati con r colori è una partizioni dell'insieme dei lati in r classi.



Teorema di Ramsey Finito

Quante persone devo invitare a una festa per avere che almeno n di loro si conoscono mutualmente oppure almeno n non si conoscono affatto?

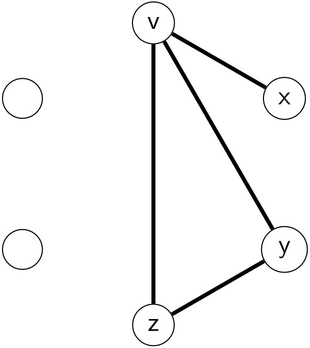
Theorem (Teorema di Ramsey Finito per coppie in due colori)

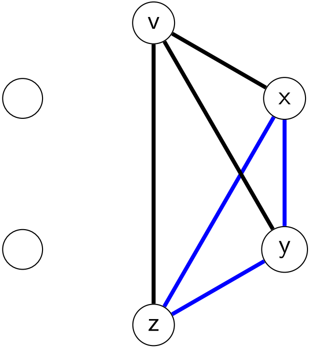
Per ogni $n, m \in \omega$ esiste un $t \in \omega$ tale che per ogni 2-colorazione sui lati del grafo completo con t vertici esiste una n-cricca omogenea nel colore 0 oppure una m-cricca omogenea nel colore 1.

Un insieme omogeneo è un sottoinsieme dei vertici tale che ogni lato che connette due di loro nello stesso colore.

Esempio

Se in una festa ci sono almeno 6 persone allora 3 di loro si conoscono oppure 3 di loro non si conoscono.





Teorema di Ramsey Infinito

Se in una festa ci sono ω invitati allora ω di loro si conoscono oppure ω di loro non si conoscono.

Theorem (Teorema di Ramsey Infinito per grafi)

Sia K_ω il grafo completo con ω vertici. Per ogni $n \in \omega$ e per ogni n-colorazione di K_ω, esiste un insieme infinito omogeneo.

Complete disorder is impossible

Theodore Samuel Motzkin

Overview I

Problem: Given a program we want to prove it terminates no matter what user does (called TERM problem).

1. Impossible in general- Harder than Halting.
2. But can do this on some simple progs. (We will.)

Notation

1. Will use psuedo-code progs.
2. KEY: If A is a set then the command

   ```
   x = input(A)
   ```

   means that x gets some value from A that the user decides.
3. Note: we will want to show that no matter what the user does the program will halt.
4. The code

   ```
   (x,y) = (f(x,y),g(x,y))
   ```

   means that simultaneously x gets f(x,y) and y gets g(x,y).

Easy Example of Traditional Method

```
(x,y,z) = (input(INT), input(INT), input(INT))
While x>0 and y>0 and z>0
        control = input(1,2,3)
        if control == 1 then
                (x,y,z)=(x+1,y-1,z-1)
        else
        if control == 2 then
                (x,y,z)=(x-1,y+1,z-1)
        else
                (x,y,z)=(x-1,y-1,z+1)
```

Sketch of Proof of termination:
Whatever the user does $x+y+z$ is decreasing.
Eventually $x+y+z=0$ so prog terminates there or earlier.

What is Traditional Method?

General method due to Floyd: Find a function f(x,y,z) from the values of the variables to N such that

1. in every iteration f(x,y,z) decreases
2. if f(x,y,z) is every 0 then the program must have halted.

Note: Method is more general- can map to a well founded order such that in every iteration f(x,y,z) decreases in that order, and if f(x,y,z) is ever a min element then program must have halted.

Hard Example of Traditional Method

```
(x,y,z) = (input(INT),input(INT),input(INT))
While x>0 and y>0 and z>0
        control = input(1,2)
        if control == 1 then
                (x,y) =(x-1,input(y+1,y+2,...))
        else
                (y,z)=(y-1,input(z+1,z+2,...))
```

Sketch of Proof of termination:
Use Lex Order: $(0,0,0) < (0,0,1) < \cdots < (0,1,0) \cdots$.
Note: $(4, 10^{100}, 10^{10!}) < (5,0,0)$.
In every iteration (x, y, z) decreases in this ordering.
If hits bottom then all vars are 0 so must halt then or earlier.

```
(x,y,z) = (input(INT),input(INT),input(INT))
While x>0 and y>0 and z>0
        control = input(1,2)
        if control == 1 then
                (x,y) =(x-1,input(y+1,y+2,...))
        else
                (y,z)=(y-1,input(z+1,z+2,...))
```

Begin Proof of termination:
If program does not halt then there is infinite sequence $(x_1, y_1, z_1), (x_2, y_2, z_2), \ldots,$ representing state of vars.

Reasoning about Blocks

```
control = input(1,2)
if control == 1 then
        (x,y) =(x-1,input(y+1,y+2,...))
else
        (y,z)=(y-1,input(z+1,z+2,...))
```

Look at $(x_i, y_i, z_i), \ldots, (x_j, y_j, z_j)$.

1. If control is ever 1 then $x_i > x_j$.
2. If control is never 1 then $y_i > y_j$.

Upshot: For all $i < j$ either $x_i > x_j$ or $y_i > y_j$.

Use Ramsey

If program does not halt then there is infinite sequence $(\mathrm{x}_1, \mathrm{y}_1, \mathrm{z}_1), (\mathrm{x}_2, \mathrm{y}_2, \mathrm{z}_2), \ldots,$ representing state of vars.
For all $i < j$ either $\mathrm{x}_i > \mathrm{x}_j$ or $\mathrm{y}_i > \mathrm{y}_j$.
Define a 2-coloring of the edges of K_ω:

$$COL(i,j) = \begin{cases} X \text{ if } \mathrm{x}_i > \mathrm{x}_j \\ Y \text{ if } \mathrm{y}_i > \mathrm{y}_j \end{cases} \tag{1}$$

By Ramsey there exists homog set $i_1 < i_2 < i_3 < \cdots$.
If color is X then $\mathrm{x}_{i_1} > \mathrm{x}_{i_2} > \mathrm{x}_{i_3} > \cdots$
If color is Y then $\mathrm{y}_{i_1} > \mathrm{y}_{i_2} > \mathrm{y}_{i_3} > \cdots$
In either case will have eventually have a var ≤ 0 and hence program must terminate. Contradiction.

Compare and Contrast

1. Trad. proof used lex order on N^3–complicated!
2. Ramsey Proof used only used the ordering N.
3. Traditional proof only had to reason about single steps.
4. Ramsey Proof had to reason about blocks of steps.

A More Compelling Example

```
(x,y) = (input(INT),input(INT))
While x>0 and y>0
       control = input(1,2)
       if control == 1 then
              (x,y)=(x-1,x)
       else
       if control == 2 then
              (x,y)=(y-2,x+1)
```

Reasoning about Blocks

If program does not halt then there is infinite sequence $(x_1, y_1), (x_2, y_2), \ldots,$ representing state of vars. Need to show that in any if $i < j$ then either $x_i > x_j$ or $y_i > y_j$. Can show that one of the following must occur:

1. $x_j < x_i$ and $y_j \le x_i$ (x decs),
2. $x_j < y_i - 1$ and $y_j \le x_i + 1$ (x+y decs so one of x or y decs),
3. $x_j < y_i - 1$ and $y_j < y_i$ (y decs),
4. $x_j < x_i$ and $y_j < y_i$ (x and y both decs).

Now use Ramsey argument.

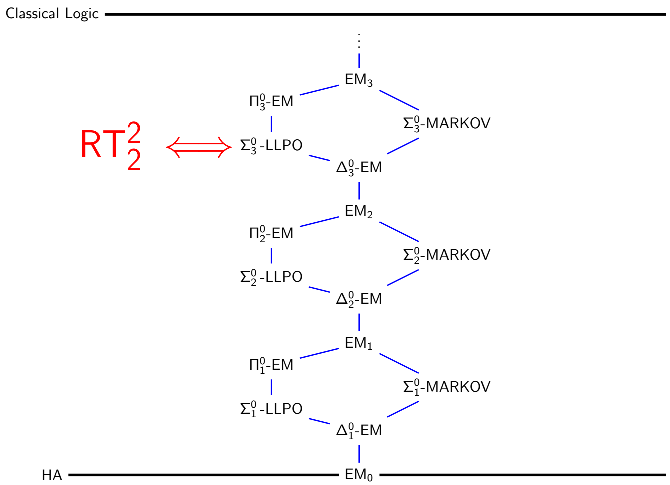
Termination Theorem

- La condizione dell'ultima prova è detta transition invariant. I transition invariants sono stati usati Podelski and Rybachenko per provare la terminazione di alcuni programmi.
- Un transition invariant di un programma è una relazione binaria sugli stati del programma che contiene la chiusura transitiva della relazione di transizione del programma, cioè $T \supseteq R^{+} \cap \mathrm{Acc} \times \mathrm{Acc}$.
- Una relazione è disjunctively well-founded se è unione finita di relazioni ben fondate.

Theorem (Termination Theorem)

Il programma P termina se e solo se esiste un disjunctively well-founded transition invariant per P.

Quanti passi sono necessari prima che il progamma P termini? Difficile da dire, perché il Teorema di Ramsey è un risultato classico.



Teorema di H-chiusura

Per analizzare i bound impliciti nel Termination Theorem dobbiamo sostituire Ramsey con qualche risultato intuizionista.

Sia R una relazione binaria su I.

- $H(R)$ è l'insieme delle sequenze R-decrescenti transitive e finite su I:

$$\langle x_1, \dots, x_n \rangle \in H(R) \iff \forall i, j \in [1, n](i < j \implies x_j R x_i).$$

- R è H-ben fondato se $H(R)$ è $\succ$-ben fondato.

Theorem (H-chiusura)

Le relazioni H-ben fondate sono chiuse per unioni finite:

$$(R_1, \dots, R_n \text{ } H\text{-well-founded}) \implies ((R_1 \cup \dots \cup R_n) \text{ } H\text{-well-founded}).$$

- Il teorema di H-chiusura è vero classicamente; esiste una dimostrazione semplice dell'equivalenza tra il Teorema di Ramsey e il Teorema di H-chiusura

- Il teorema di H-chiusura è provabile intuizionisticamente (usando la definizione induttiva di well-foundedness), e da questo possiamo provare intuizionisticamente il Teorema di Terminazione.

- Quindi spezza la dimostrazione del Teorema di Ramsey in due parti, una intuizionistica e l'altra classica (semplice: può essere provata usando il principio classico Σ^0_3-LLPO).

Una dimostrazione intuizionista alternativa del Teorema di Terminazione: le relazioni Almost full

Nel 1990 Veldman e Bezem provarono, usando l'Assioma della Scelta e la tesi di Brouwer, la prima versione intuizionista negation-free di Ramsey.

Una relazione binaria R su un insieme I è almost full se per ogni sequenza infinita $x_0, x_1, x_2, \ldots, x_n, \ldots$ su I estistono due indici $i < j$ tali che $x_i R x_j$.

Theorem (Almost Full Theorem)

Le relazioni almost full sono chiuse per intersezioni finite.

Coquand mostrò che possiamo evitare di usare sia la scelta che la tesi di Brouwer per provare l' Almost Full Theorem, usando la definizione induttiva di ben fondato al posto della definizione classica.

H-chiusura vs Almost Full

- Il Teorema di H-chiusura e Almost Full Theorem sono classicamente equivalenti.

- Non possiamo trovare una dimostrazione intuizionistica per dedurre uno dall'altro a causa dell'uso delle leggi di de' Morgan usate per tradurre la definizione di almost full nella definizione di H-ben fondato.

- H-chiusura è in un certo senso più simile al Teorema di Ramsey originale, perché è ottenuto con un solo passo classico, una contrapposizione; mentre almost fullness richiede un'applicazione della legge di de' Morgan, seguito da una contrapposizione.

Cosa stiamo facendo ora?

Theorem

Un funzione ha almeno un'implementazione con un disjunctively well-founded transition invariant in cui ogni relazione è primitiva ricorsiva e ha altezza ω *se e solo se è primitiva ricorsiva.*

La prova di questo risultato è basata sullo schema della dimostrazione del Teorema di H-chiusura.

Cosa stiamo facendo ora?

Poiché dal Teorema di Terminazione Podelski, Rybachenko e Cook hanno prodotto un algoritmo, speriamo che il Teorema di H-chiusura possa essere utile per trovare dei bound.

Conjecture

Una funzione ha almeno un'implementazione che l'algoritmo di Terminator prova terminante se e solo se è primitiva ricorsiva.

Riferimenti bibliografici

English slides by courtesy of Prof. Gasarch.

- Ramsey. On a problem of formal logic. Proceedings London Mathematical Society, 1930
- W. Veldman, M. Bezem. Ramsey's Theorem and the Pigeonhole principle in Intuitionistic Mathematics. University of Utrecht, Dept of Philosophy, 1992
- A. Podelski, A. Rybalchenko. Transition Invariants. LICS, 2004
- Coquand. A direct proof of Ramsey's Theorem. Author's website, revised in 2011
- S. Berardi, S. Steila. Ramsey Theorem for pairs as a classical principle in Intuitionistic Arithmetic. Accepted in Types 2013 Post-proceedings
- S. Berardi, S. Steila. Ramsey Theorem as an intuitionistic property of well-founded relations. Accepted RTA-TLCA 2014