An Application of Ramsey’s Theorem to Proving Programs Terminate: An Exposition

William Gasarch-U of MD
Who is Who

1. Work by
   1.1 Floyd,
   1.2 Byron Cook, Andreas Podelski, Andrey Rybalchenko,
   1.3 Lee, Jones, Ben-Amram
   1.4 Others

2. Pre-Apology: Not my area-some things may be wrong.

3. Pre-Brag: Not my area-some things may be understandable.
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.)
Overview II

In this talk I will:

1. Do example of traditional method to prove progs terminate.
2. Do harder example of traditional method.
3. DIGRESSION: A very short lecture on Ramsey Theory.
4. Do that same harder example using Ramsey Theory.
5. Compelling example with Ramsey Theory.
6. Do same example with Ramsey Theory and Matrices.
Notation

1. Will use psuedo-code progs.
2. **KEY:** If A is a set then the command
   \[ x = \text{input}(A) \]
   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 \( g(x,y) \).
(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:
Easy Example of Traditional Method

\[(x,y,z) = (\text{input(INT)}, \text{input(INT)}, \text{input(INT)})\]
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.
(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 ever 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.
(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, z) = (x-1, input(y+1, y+2, ...), z)
    else
        (x, y, z) = (x, y-1, input(z+1, z+2, ...))

Sketch of Proof of termination:
Hard Example of Traditional Method

\[(x,y,z) = (\text{input(INT)}, \text{input(INT)}, \text{input(INT)})\]  
While \(x > 0\) and \(y > 0\) and \(z > 0\)  
\[\text{control} = \text{input}(1, 2)\]  
if control == 1 then  
\[\text{(x,y,z)} = (x-1, \text{input}(y+1, y+2, \ldots), z)\]  
else  
\[\text{(x,y,z)} = (x, y-1, \text{input}(z+1, z+2, \ldots))\]  

Sketch of Proof of termination:  
Use Lex Order: \((0, 0, 0) < (0, 0, 1) < \cdots < (0, 1, 0) \cdots\).  
Note: \((4, 10^{100}, 10^{101}) < (5, 0, 0)\).
Hard Example of Traditional Method

\[(x,y,z) = (\text{input(INT)}, \text{input(INT)}, \text{input(INT)})\]
While \(x>0\) and \(y>0\) and \(z>0\)
  \[
  \text{control} = \text{input}(1,2)
  \]
  if control == 1 then
    \[
    (x,y,z) = (x-1, \text{input}(y+1, y+2, \ldots), z)
    \]
  else
    \[
    (x,y,z) = (x, y-1, \text{input}(z+1, z+2, \ldots))
    \]
Sketch of Proof of termination:
Use Lex Order: 
\[(0,0,0) < (0,0,1) < \ldots < (0,1,0) \ldots\]
Note: 
\[(4, 10^{100}, 10^{10!}) < (5, 0, 0).\]
In every iteration \((x, y, z)\) decreases in this ordering.
Hard Example of Traditional Method

\[ (x,y,z) = (\text{input}(\text{INT}), \text{input}(\text{INT}), \text{input}(\text{INT})) \]

While \( x > 0 \) and \( y > 0 \) and \( z > 0 \)

control = \text{input}(1,2)

if control == 1 then

\[ (x,y,z) = (x-1, \text{input}(y+1,y+2,...), z) \]

else

\[ (x,y,z) = (x,y-1, \text{input}(z+1,z+2,...)) \]

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.
Well Ordering is Key!

**Definition** An ordering \((X, \preceq)\) is a **well founded** if there are no infinite decreasing sequences. (Induction proofs can be done on such orderings.)

**Examples and Counterexamples**

- \(\mathbb{N}\) in its usual ordering is well founded.
- \(\mathbb{Z}\) in its usual ordering is NOT well founded.
- Lex order on \(\mathbb{N} \times \mathbb{N} \times \mathbb{N}\) is well founded. Discuss.
Notes about Proof

1. **Bad News**: We had to use a *funky* ordering. This might be hard for a proof checker to find. (*Funky* is not a formal term.)

2. **Good News**: We only had to reason about what happens in one iteration.

Keep these in mind- our later proof will use a *nice* ordering but will need to reason about a *block* of instructions.
Digression Into Ramsey Theory (Parties!)

The following are known:

1. If you have 6 people at a party then either 3 of them mutually know each other or 3 of them mutually don’t know each other.
Digression Into Ramsey Theory (Parties!)

The following are known:

1. If you have 6 people at a party then either 3 of them mutually know each other or 3 of them mutually don’t know each other.

2. If you have 18 people at a party then either 4 of them mutually know each other or 4 of them mutually do not know each other.
The following are known:

1. If you have 6 people at a party then either 3 of them mutually
   know each other or 3 of them mutually don’t know each other.
2. If you have 18 people at a party then either 4 of them
   mutually know each other or 4 of them mutually do not know
   each other.
3. If you have $2^{2k-1}$ people at a party then either $k$ of them
   mutually know each other or $k$ of them mutually do not know
   each other.
Digression Into Ramsey Theory (Parties!)

The following are known:

1. If you have 6 people at a party then either 3 of them mutually know each other or 3 of them mutually don’t know each other.

2. If you have 18 people at a party then either 4 of them mutually know each other or 4 of them mutually do not know each other.

3. If you have \(2^{2k-1}\) people at a party then either \(k\) of them mutually know each other or \(k\) of them mutually do not know each other.

4. If you have an infinite number of people at a party then either there exists an infinite subset that all know each other or an infinite subset that all do not know each other.
Digression Into Ramsey Theory (Math!)

Definition
Let $c, k, n \in \mathbb{N}$. $K_n$ is the complete graph on $n$ vertices (all pairs are edges). $K_\omega$ is the infinite complete graph. A $c$-coloring of $K_n$ is a $c$-coloring of the edges of $K_n$. A homogeneous set is a subset $H$ of the vertices such that every pair has the same color (e.g., 10 people all of whom know each other).

The following are known.

1. For all 2-colorings of $K_6$ there is a homog 3-set.
2. For all $c$-colorings of $K_c$ there is a homog $k$-set.
3. For all $c$-colorings of $K_\omega$ there exists a homog $\omega$-set.
Definition
Let $c, k, n \in \mathbb{N}$. $K_n$ is the complete graph on $n$ vertices (all pairs are edges). $K_\omega$ is the infinite complete graph. A $c$-coloring of $K_n$ is a $c$-coloring of the edges of $K_n$. A homogeneous set is a subset $H$ of the vertices such that every pair has the same color (e.g., 10 people all of whom know each other).

The following are known.
1. For all 2-colorings of $K_6$ there is a homog 3-set.
Definition
Let $c, k, n \in \mathbb{N}$. $K_n$ is the complete graph on $n$ vertices (all pairs are edges). $K_\omega$ is the infinite complete graph. A $c$-coloring of $K_n$ is a $c$-coloring of the edges of $K_n$. A homogeneous set is a subset $H$ of the vertices such that every pair has the same color (e.g., 10 people all of whom know each other).

The following are known.

1. For all 2-colorings of $K_6$ there is a homog 3-set.
2. For all $c$-colorings of $K_{c^{ck-c}}$ there is a homog $k$-set.
Definition
Let $c, k, n \in \mathbb{N}$. $K_n$ is the complete graph on $n$ vertices (all pairs are edges). $K_\omega$ is the infinite complete graph. A $c$-coloring of $K_n$ is a $c$-coloring of the edges of $K_n$. A homogeneous set is a subset $H$ of the vertices such that every pair has the same color (e.g., 10 people all of whom know each other).

The following are known.

1. For all 2-colorings of $K_6$ there is a homog 3-set.
2. For all $c$-colorings of $K_{ck-c}$ there is a homog $k$-set.
3. For all $c$-colorings of the $K_\omega$ there exists a homog $\omega$-set.
(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,z) = (x-1, input(y+1, y+2, ...), z)
    else
        (x,y,z) = (x, y-1, input(z+1, z+2, ...))
Begin Proof of termination:
(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, z) = (x - 1, input(y + 1, y + 2, ...), z)
    else
        (x, y, z) = (x, 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), ..., representing state of vars.
Reasoning about Blocks

control = input(1,2)
if control == 1 then
    \((x,y,z) = (x-1,\text{input}(y+1,y+2,...),z)\)
else
    \((x,y,z) = (x,y-1,\text{input}(z+1,z+2,...))\)
Reasoning about Blocks

control = input(1,2)
if control == 1 then
    (x,y,z) =(x-1,input(y+1,y+2,...),z)
else
    (x,y,z)=(x,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 \(y_i > y_j\).
Reasoning about Blocks

countrol = input(1,2)
if control == 1 then
    \((x,y,z) = (x-1, \text{input}(y+1,y+2,\ldots),z)\)
else
    \((x,y,z) = (x,y-1, \text{input}(z+1,z+2,\ldots))\)

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 
\((x_1, y_1, z_1), (x_2, y_2, z_2), \ldots\), representing state of vars.
For all \(i < j\) either \(x_i > x_j\) or \(y_i > y_j\).
Define a 2-coloring of the edges of \(K_\omega\):

\[
COL(i, j) = \begin{cases} 
X & \text{if } x_i > x_j \\
Y & \text{if } y_i > y_j 
\end{cases}
\]  

(1)

By Ramsey there exists homog set \(i_1 < i_2 < i_3 < \cdots\).
If color is \(X\) then \(x_{i_1} > x_{i_2} > x_{i_3} > \cdots\).
If color is \(Y\) then \(y_{i_1} > y_{i_2} > y_{i_3} > \cdots\).
In either case will have eventually have a var \(\leq 0\) and hence program must terminate. Contradiction.
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.
What do YOU think?

VOTE:

1. Traditional Proof!
2. Ramsey Proof!
3. Emily/Erika in 2020! (First Law: ban all gross functions.)
A More Compelling Example

\[(x,y) = (\text{input(INT)}, \text{input(INT)})\]

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 for all \(i < j\) 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 \(y_j \leq x_i\) (\(x\) decs),
2. \(x_j < y_i - 1\) and \(y_j \leq x_i + 1\) (\(x+y\) 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.
Comments

1. The condition in the last proof is called a **Termination Invariant**. They are used to strengthen the induction hypothesis.
2. The proof was found by the system of B. Cook et al.
3. Looking for a Termination Invariant is the hard part to automate but they have automated it.
4. Can we use these techniques to solve a fragment of the Termination Problem?
if control == 1 then (x, y) = (x-1, x)

Model as a matrix $A$ indexed by $x, y, x+y$.

$$
\begin{pmatrix}
-1 & 0 & \infty \\
\infty & \infty & \infty \\
\infty & \infty & \infty \\
\end{pmatrix}
$$

For $a, b \in \{x, y, x+y\}$

Entry $(a, b)$ is difference between NEW $b$ and OLD $a$.

Entry $(a, a)$ is most interesting- if neg then $a$ decreased.
if control == 2 then (x, y) = (y-2, x+1)

Model as a matrix $B$ indexed by $x, y, x+y$.

$$
\begin{pmatrix}
\infty & 1 & \infty \\
-2 & \infty & \infty \\
\infty & \infty & -1
\end{pmatrix}
$$
Redefine Matrix Mult

A and B matrices, \( C = AB \) defined by

\[
c_{ij} = \min_k \{a_{ik} + b_{kj}\}.
\]

Lemma

*If matrix A models a statement \( s_1 \) and matrix B models a statement \( s_2 \) then matrix \( AB \) models what happens if you run \( s_1; s_2 \).*
Matrix Proof that Program Terminates

- A is matrix for control=1. B is matrix for control=2.
- Show: any prod of A’s and B’s some diag is negative.
- Hence in any finite seg one of the vars decreases.
- Hence, by Ramsey proof, the program always terminates