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.
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.)
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.
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:
(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.
(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.
(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) < · · · < (0,1,0) · · ·.

Note:
(4,10,100,10) < (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.

William Gasarch-U of MD
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) < ... < (0, 1, 0) ... 
Note: (4, 10^{100}, 10^{101}) < (5, 0, 0).
(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) < · · · < (0,1,0) · · ·
Note: (4,10^{100},10^{101}) < (5,0,0).
In every iteration (x, y, z) decreases in this ordering.
(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) < · · · < (0,1,0) · · ·.
Note: (4,10^{100},10^{101}) < (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.
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.
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 $2^{k-1}$ 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 (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.
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.
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 $K_{ck-c}$ 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.
\[(x,y,z) = (\text{input(INT)}, \text{input(INT)}, \text{input(INT)})\]
While \(x > 0\) and \(y > 0\) and \(z > 0\)
  \[
  \text{control} = \text{input}(1,2)
  \]
  \[
  \text{if control == 1 then}
  \]
  \[
  (x,y) = (x-1, \text{input}(y+1,y+2,...))
  \]
  \[
  \text{else}
  \]
  \[
  (y,z) = (y-1, \text{input}(z+1,z+2,...))
  \]

Begin Proof of termination:
\[(x,y,z) = (\text{input(INT)}, \text{input(INT)}, \text{input(INT)})\]
While \(x > 0\) and \(y > 0\) and \(z > 0\)
  \[
  \text{control} = \text{input}(1, 2)
  \]
  if \(\text{control} == 1\) then
  \[
  (x,y) = (x-1, \text{input}(y+1,y+2,...))
  \]
else
  \[
  (y,z) = (y-1, \text{input}(z+1,z+2,...))
  \]

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, ...))

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 $y_i > y_j$.
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 \(y_i > y_j\).
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 \(y_i > y_j\).
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 \(x_i \geq x_j\) or \(y_i \geq y_j\).
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.**
Compare and Contrast

1. Traditional proof used lexicographic 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. Stewart/Colbert in 2016!
A More Compelling Example

\[(x,y) = (\text{input}(\text{INT}),\text{input}(\text{INT}))\]
While \(x > 0\) and \(y > 0\)
  \[\text{control} = \text{input}(1,2)\]
  if \(\text{control} == 1\) then
    \[(x,y)=(x-1,x)\]
  else
    if \(\text{control} == 2\) then
      \[(x,y)=(y-2,x+1)\]
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 \(y_j \leq x_i\) (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.
1. The condition in the last proof is called a **Termination Invariant**. They are used to strengthened 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 Term Problem?
if control == 1 then (x,y) = (x-1,x)

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

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

Entry $(x,y)$ is difference between OLD $x$ and NEW $y$. Entry $(x,x)$ is most interesting - if neg then $x$ 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.
X = (input(INT),...,input(INT)
While x[1]>0 and x[2]>0 and ... x[n]>0
  control = input(1,2,3,...,m)
  if control==1
    X = F1(X,input(INT,...,input(INT))
  else
    if control==2
      X = F2(X,input(INT),...,input(INT))
    else...
  else
    if control==m
      X = Fm(X,input(INT),...,input(INT))
Definition

The **TERMINATION PROBLEM**: Given $F_1, \ldots, F_m$ can we determine if the following holds:

For all $\omega$-seq of inputs the program halts

1. This is **HARDER** than **HALT**. TERM is $\Pi_1^1$-complete.
2. **EASY** to show is **HARD**: use polynomials and Hilbert’s Tenth Problem.
3. **OPEN**: Determine which subsets of $F_i$ make this decidable? $\Pi_1^1$-complete? Other?
The colorings we applied Ramsey to were of a certain type:

**Definition**
A coloring of the edges of $K_n$ or $K_N$ is *transitive* if, for every $i < j < k$, if $\text{COL}(i, j) = \text{COL}(j, k)$ then both equal $\text{COL}(i, k)$.

1. Our colorings were transitive.
2. Transitive Ramsey Thm is weaker than Ramsey’s Thm.
TR is Transitive Ramsey, R is Ramsey.

1. Combinatorially: $R(k, c) = c^{\Theta(ck)}$, $TR(k, c) = (k - 1)^c + 1$. This may look familiar
TR is Transitive Ramsey, R is Ramsey.

1. Combinatorially: \( R(k, c) = c^{\Theta(ck)} \), \( TR(k, c) = (k - 1)^c + 1 \).
   This may look familiar \( TR(k, 2) = (k - 1)^2 + 1 \) is Erdős-Szekeres Theorem. More usual statement: For any sequence of \((k - 1)^2 + 1\) distinct reals there is either an increasing or decreasing subsequence of length \(k\).
TR is Transitive Ramsey, R is Ramsey.

1. **Combinatorially:** \( R(k, c) = c^{\Theta(ck)} \), \( TR(k, c) = (k - 1)^c + 1 \).
   This may look familiar \( TR(k, 2) = (k - 1)^2 + 1 \) is Erdős-Szekeres Theorem. More usual statement: For any sequence of \((k - 1)^2 + 1\) distinct reals there is either an increasing or decreasing subsequence of length \( k \).

2. **Computability:** There exists a computable 2-coloring of \( K_\omega \) with no computable homogeneous set (can even have no \( \Sigma_2 \) homogeneous set). For every transitive computable \( c \)-coloring of \( K_\omega \) there exists a \( \Pi_2 \) computable homogeneous set (folklore).
TR is Transitive Ramsey, R is Ramsey.

1. **Combinatorially:** $R(k, c) = c^{\Theta(c^k)}$, $TR(k, c) = (k - 1)^c + 1$. This may look familiar $TR(k, 2) = (k - 1)^2 + 1$ is Erdős-Szekeres Theorem. More usual statement: For any sequence of $(k - 1)^2 + 1$ distinct reals there is either an increasing or decreasing subsequence of length $k$.

2. **Computability:** There exists a computable 2-coloring of $K_\omega$ with no computable homogeneous set (can even have no $\Sigma^0_2$ homogeneous set). For every transitive computable $c$-coloring of $K_\omega$ there exists a $\Pi^0_2$ computable homogeneous set (folklore).

3. **Proof Theory:** Over the axiom system $RCA_0$, R implies TR, but TR does not imply R.
1. Ramsey Theory can be used to prove some simple programs terminate that seem harder to do my traditional methods. Interest to PL.

2. Some to subcases of TERMINATION PROBLEM are decidable. Of interest to PL and Logic.

3. Full strength of Ramsey not needed. Interest to Logicians and Combinatorists.