Program termination · Lecture I

Berkeley · Spring ’09

Byron Cook

Introduction

→ The program termination problem *a.k.a.* (uniform) halting problem:

Given any computer program, decide whether the program will finish running or could run forever

→ Decide is used in the technical sense

- Use only a finite amount of time
- Return either “yes” or “no”

Introduction

- The program termination problem *a.k.a.* (uniform) halting problem:

  Given any computer program, decide whether its transition relation is well founded

- Decide is used in the technical sense
  - Use only a finite amount of time
  - Return either “yes” or “no”

Introduction

- Myth: It is *always impossible to* prove terminating programs terminating

- Truth: It is *impossible to always* prove terminating programs terminating

Introduction

```
while(n>1) {
    if (n % 2 == 0) {
        n = n/2;
    } else {
        n = 3*n +1;
    }
}
```

- Myth: It is *always* …
  programs terminati…

- Truth: It is *impossible to always* prove terminating programs terminating

Introduction

→ The program termination problem *a.k.a.* (uniform) halting problem:

Given any computer program, decide whether its transition relation is well founded

→ Decide is used in the technical sense

- Use only a finite amount of time
- Return either “yes” or “no”

Introduction

→ The program termination problem *a.k.a.* (uniform) halting problem:

try to

Given any computer program, try to *decide whether its transition relation is well founded*

Try to

→ Try to Decide is used in the technical sense

- Use only a finite amount of time
- Return either "yes" or "no" or "don't know"

Introduction

→ Automatically discovering abstraction is key to a solution.

→ <u>Try to decide with abstraction</u>

- Use only a finite amount of time
- Return either “yes”, “no”, or “don’t know”

Introduction

→ Automatically discovering abstraction is key to a solution.

→ Try to decide with abstraction

- Use only a finite amount of time
- Return either “yes”, “[illegible]”, or “don’t know”

Over approximation

Introduction

→ Automatically discovering abstraction is key to a solution.

→ <u>Try to decide with abstraction</u>

- Use only a finite amount of time
- Return either ~~“yes~~”, “no”, or “don’t know”

Underapproximation

Introduction

→ Termination is a matter of practical importance:

- Liveness: *Is every call to AcquireLock() followed by a call to ReleaseLock()?*

- Pure termination: *Does the mouse driver's dispatch routine always return control back to the OS?*

→ Recent advances allow us to prove termination in many practical cases

A Year Ticks Over, and Zunes Get the Hiccups - NYTimes.com - Windows Internet Explorer

http://www.nytimes.com/2009/01/01/technology/personaltech/01zune.html

microsoft zune new york times

A Year Ticks Over, and Zunes Get the Hiccups - N...

Page ▾ Tools ▾

The New York Times

Personal Tech

Search All NYTimes.com Go

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION | ARTS | STYLE | TRAVEL | JOBS | REAL ESTATE | AUTOS

Search Tech News & 8,000+ Products Go

Browse Products
-- Select a Product Category --

Personal Tech »
Cellphones, Cameras, Computers and more.

A Year Ticks Over, and Zunes Get Hiccups

By JENNA WORTHAM
Published: December 31, 2008

SIGN IN TO E-MAIL OR SAVE THIS
PRINT
REPRINTS
SHARE

ARTICLE TOOLS SPONSORED BY

It has been nine years since the Y2K computer glitch inspired apocalyptic fears. On Wednesday, another time-related bug created its own small-scale panic. For some owners of the Zune, the portable media player that is Microsoft's answer to the Apple iPod, it was a day without Kanye West and Girl Talk.

Related

Bits: The Day the Microsoft Zunes Stood Still

Owners of 30-gigabyte Zunes began flooding Zune-related Web sites with complaints early Wednesday morning. They said their players had suddenly stopped working, displaying only a frozen start-up screen.

After spending much of the day digging into the problem, Microsoft said that it had traced it to a software bug "related to the way the device handles a leap year." Apparently the Zune was expecting 2008 to have 365 days, not 366.

The fix for the glitch? Patience. The company said the internal clock on the players should reset itself at 7 a.m. Eastern time on Thursday. Microsoft advised Zune owners to drain the battery and then turn the players back on after that time. Those who were hoping to provide the soundtrack to New Year's Eve parties had no choice but to find a friend with an iPod.

Some Zune owners, like Geoffry Houze, a 53-year-old entrepreneur in Las Vegas, were frustrated by the breakdown. "It's inexcusable," Mr. Houze said. "It's surprising that

Product Categories

Camcorders »	Home Video »
Cameras »	Music »
Cellphones »	Peripherals »
Computers »	Video Games »
G.P.S. »	Wi-Fi »
Handhelds »	

ttp://www.nytimes.com/pages/jobs/index.html Internet | Protected Mode: On 100%

A Year Ticks Over, and Zunes Get Hiccups

By JENNA WORTHAM
Published: December 31, 2008

SIGN IN TO E-MAIL OR SAVE THIS
PRINT
REPRINTS
SHARE

It has been nine years since the Y2K computer glitch inspired apocalyptic fears. On Wednesday, another time-related bug created its own small-scale panic. For some owners of the Zune, the portable media player that is Microsoft's answer to the Apple iPod, it was a day without Kanye West and Girl Talk.

Related

Bits: The Day the Microsoft Zunes Stood Still

Owners of 30-gigabyte Zunes began flooding Zune-related Web sites with complaints early Wednesday morning. They said their players had suddenly stopped working, displaying only a frozen start-up screen.

After spending much of the day digging into the problem, Microsoft said that it had traced it to a software bug "related to the way the device handles a leap year." Apparently the

A Year Ticks Over, and Zunes Get Hiccups

By JENNA W

Published: D

It has be
apocalyp
own sma
media pl
without

Related

Bits: The
Zunes Sto

After spe
it to a so

Proc

Glitch freezes Microsoft Zune music devices

By Jessica Hodgson

Microsoft Corp.'s Zune digital music player was tripped up by leap year, causing thousands of the devices to freeze on Wednesday, presenting a year-end embarrassment for a gadget that's already had a hard enough time winning fans.

On Wednesday, Zune owners flooded blogs and Internet chat sites to complain they couldn't listen to music on the 30-gigabyte version of the Zune, an early version of the device, because it wouldn't start up properly. The postings noted that the players got stuck with the Zune logo screen and were unresponsive.

Microsoft initially acknowledged there was a problem with some Zunes and told customers it was working to address it. Later, the company said engineers had identified that the cause of the problem was an issue with the device's internal clock driver and how it handles a leap year, such as 2008.

The issue relates to a part of the Zune hardware, and only affects the 30-gigabyte Zunes, a Microsoft spokeswoman said.

The issue, Microsoft said, would resolve itself as the device moved to Jan. 1. Microsoft advised customers to let the battery run down on the devices before recharging and restarting.

A Microsoft spokeswoman said even those Zunes no longer covered by warranty should be able to be reset.

Zune Pass subscribers should sync the device to their personal computers, the company added.

The 30-gigabyte model, released in November 2006, was the first Zune player from Microsoft, which wanted to challenge Apple Inc.'s iPod. Microsoft said it had sold more than 1.2 million of the units when it released updated models the following holiday season.

The Zune devices appear to have started freezing early Wednesday, according to customers' complaints. Microsoft didn't say how many of the devices were affected, but a spokeswoman said that all 30-gigabyte Zunes were potentially affected. A forum on the Microsoft Zune support site, titled "Help-frozen zune," had registered more than 20,000 comments by 5:30 p.m. EST on Wednesday.

Some bloggers and users initially speculated that the issue may be caused by a "Y2K" problem, a reference to the issue that consumed computer experts at the end of 1999, when computer clocks had to switch to 2000. Many feared that the change of the millennium would interfere with the internal time settings in computers and potentially wreak havoc on systems around the globe. Companies spend thousands of dollars to protect themselves, largely unnecessarily.

Zune accounts for a very small proportion of Microsoft's roughly $60 billion in annual sales and its market share is dwarfed by that of Apple, whose iPods have more than 70% of the market, according to NPD figures.

Matt Rosoff, an analyst with Directions on Microsoft, a Seattle-based research firm that tracks the company, said the Zune snafu underscored the device's weakness in the market. Microsoft has "missed the boat" in the market for digital music players, Mr. Rosoff said. "That game is over."

He expects the company to shift its strategy early in 2009 to focus on improving the Zune software and service offerings, and joining with mobile-phone handset makers.

The Zune problem closes out a year in which Microsoft's problems had been more prominent than its successes. Microsoft shares lost around 45% in 2008. They closed Wednesday up 0.5% at $19.44.

The company is still struggling to excite customers about its latest operating system, Windows Vista. That may force the company to release Vista's successor, Windows 7, earlier than initially planned.

Microsoft has also failed to gain traction in building market share for its Internet-search advertising operations, an area Chief Executive Steve Ballmer has indicated is a priority for the company.

The 30-gigabyte model, released in November 2006, was the first Zune.

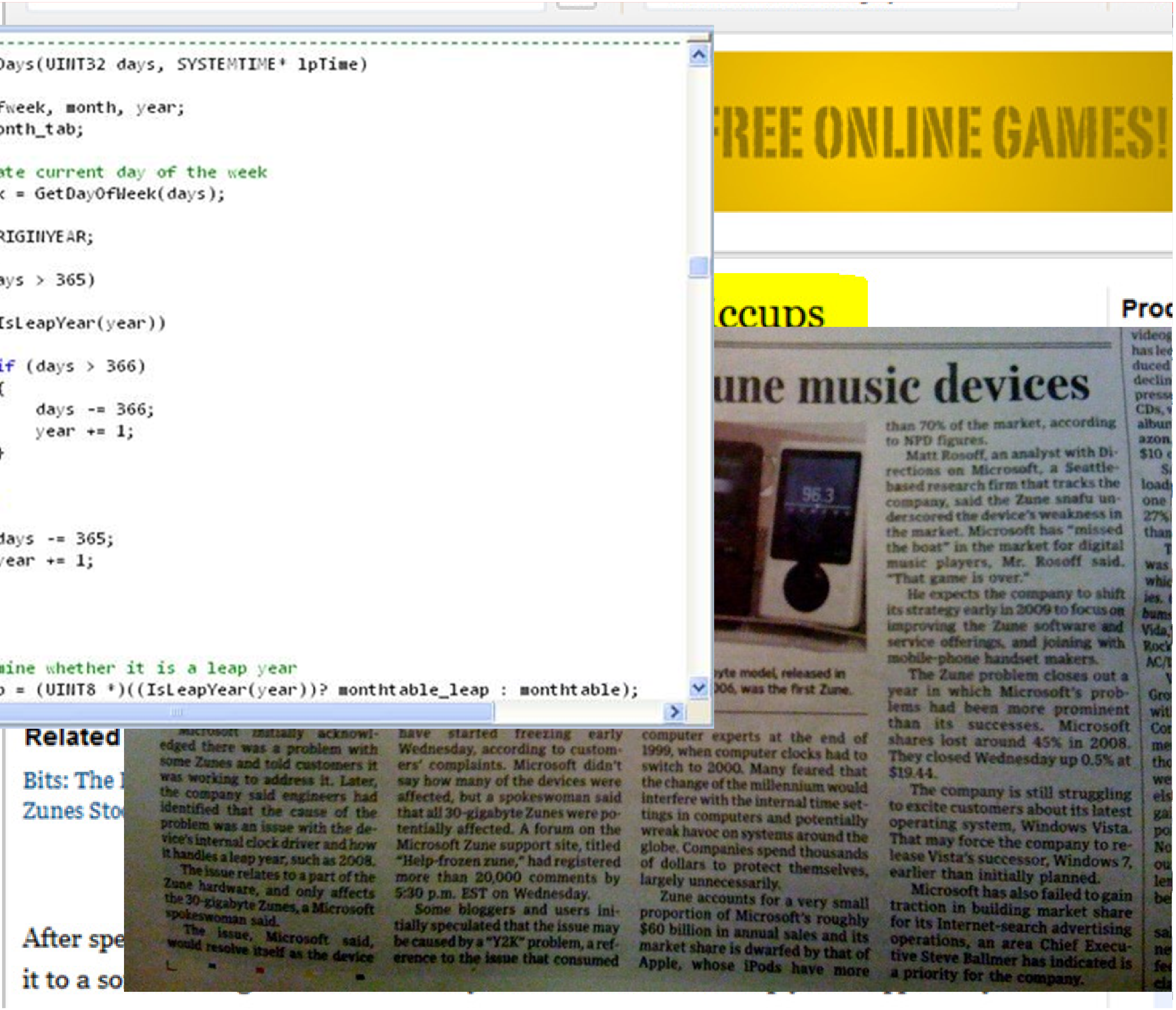
```
//----------------------------------------------------------------------
BOOL ConvertDays(UINT32 days, SYSTEMTIME* lpTime)
{
    int dayofweek, month, year;
    UINT8 *month_tab;

    //Calculate current day of the week
    dayofweek = GetDayOfWeek(days);

    year = ORIGINYEAR;

    while (days > 365)
    {
        if (IsLeapYear(year))
        {
            if (days > 366)
            {
                days -= 366;
                year += 1;
            }
        }
        else
        {
            days -= 365;
            year += 1;
        }
    }


    // Determine whether it is a leap year
    month_tab = (UINT8 *)((IsLeapYear(year))? monthtable_leap : monthtable);
```



une music devices

...byte model, released in ...006, was the first Zune.

Microsoft initially acknowledged there was a problem with some Zunes and told customers it was working to address it. Later, the company said engineers had identified that the cause of the problem was an issue with the device's internal clock driver and how it handles a leap year, such as 2008.

The issue relates to a part of the Zune hardware, and only affects the 30-gigabyte Zunes, a Microsoft spokeswoman said.

The issue, Microsoft said, would resolve itself as the device

have started freezing early Wednesday, according to customers' complaints. Microsoft didn't say how many of the devices were affected, but a spokeswoman said that all 30-gigabyte Zunes were potentially affected. A forum on the Microsoft Zune support site, titled "Help-frozen zune," had registered more than 20,000 comments by 5:30 p.m. EST on Wednesday.

Some bloggers and users initially speculated that the issue may be caused by a "Y2K" problem, a reference to the issue that consumed

computer experts at the end of 1999, when computer clocks had to switch to 2000. Many feared that the change of the millennium would interfere with the internal time settings in computers and potentially wreak havoc on systems around the globe. Companies spend thousands of dollars to protect themselves, largely unnecessarily.

Zune accounts for a very small proportion of Microsoft's roughly $60 billion in annual sales and its market share is dwarfed by that of Apple, whose iPods have more

than 70% of the market, according to NPD figures.

Matt Rosoff, an analyst with Directions on Microsoft, a Seattle-based research firm that tracks the company, said the Zune snafu underscored the device's weakness in the market. Microsoft has "missed the boat" in the market for digital music players, Mr. Rosoff said. "That game is over."

He expects the company to shift its strategy early in 2009 to focus on improving the Zune software and service offerings, and joining with mobile-phone handset makers.

The Zune problem closes out a year in which Microsoft's problems had been more prominent than its successes. Microsoft shares lost around 45% in 2008. They closed Wednesday up 0.5% at $19.44.

The company is still struggling to excite customers about its latest operating system, Windows Vista. That may force the company to release Vista's successor, Windows 7, earlier than initially planned.

Microsoft has also failed to gain traction in building market share for its Internet-search advertising operations, an area Chief Executive Steve Ballmer has indicated is a priority for the company.

```
//--------------------------------------------------------
BOOL ConvertDays(UINT32 days, SYSTEMTIME* lpTime)
{
    int dayofweek, month, year;
    UINT8 *month_tab;

    //Calculate current day of the week
    dayofweek = GetDayOfWeek(days);

    year = ORIGINYEAR;

    while (days > 365)
    {
        if (IsLeapYear(year))
        {
            if (days > 366)
            {
                days -= 366;
                year += 1;
            }
        }
        else
        {
            days -= 365;
            year += 1;
        }
    }

    // Determine whether it is a leap year
    month_tab = (UINT8 *)((IsLeapYear(year))? monthtable_leap : monthtable);
```

Do you see the bug?

Microsoft initially acknowledged there was a problem with some Zunes and told customers it was working to address it. Later, the company said engineers had identified that the cause of the problem was an issue with the device's internal clock driver and how it handles a leap year, such as 2008.

The issue relates to a part of the Zune hardware, and only affects the 30-gigabyte Zunes, a Microsoft spokeswoman said.

The issue, Microsoft said, would resolve itself as the device have started freezing early Wednesday, according to customers' complaints. Microsoft didn't say how many of the devices were affected, but a spokeswoman said that all 30-gigabyte Zunes were potentially affected. A forum on the Microsoft Zune support site, titled "Help-frozen zune," had registered more than 20,000 comments by 5:30 p.m. EST on Wednesday.

Some bloggers and users initially speculated that the issue may be caused by a "Y2K" problem, a reference to the issue that consumed computer experts at the end of 1999, when computer clocks had to switch to 2000. Many feared that the change of the millennium would interfere with the internal time settings in computers and potentially wreak havoc on systems around the globe. Companies spend thousands of dollars to protect themselves, largely unnecessarily.

Zune accounts for a very small proportion of Microsoft's roughly $60 billion in annual sales and its market share is dwarfed by that of Apple, whose iPods have more than 70% of the market, according to NPD figures.

Matt Rosoff, an analyst with Directions on Microsoft, a Seattle-based research firm that tracks the company, said the Zune snafu underscored the device's weakness in the market. Microsoft has "missed the boat" in the market for digital music players, Mr. Rosoff said. "That game is over."

He expects the company to shift its strategy early in 2009 to focus on improving the Zune software and service offerings, and joining with mobile-phone handset makers.

The Zune problem closes out a year in which Microsoft's problems had been more prominent than its successes. Microsoft shares lost around 45% in 2008. They closed Wednesday up 0.5% at $19.44.

The company is still struggling to excite customers about its latest operating system, Windows Vista. That may force the company to release Vista's successor, Windows 7, earlier than initially planned.

Microsoft has also failed to gain traction in building market share for its Internet-search advertising operations, an area Chief Executive Steve Ballmer has indicated is a priority for the company.

Harder example

Microsoft Development Environment [design] - mouclass.c [Read Only]

File Edit View Debug Tools Window Help

mouclass.c

```c
    for (entry = DeviceExtension->ReadQueue.Flink;
         entry != &DeviceExtension->ReadQueue;
         entry = entry->Flink) {

        irp = CONTAINING_RECORD (entry, IRP, Tail.Overlay.ListEntry);
        stack = IoGetCurrentIrpStackLocation (irp);
        if (stack->FileObject == FileObject) {
            RemoveEntryList (entry);

            oldCancelRoutine = IoSetCancelRoutine (irp, NULL);

            //
            // IoCancelIrp() could have just been called on this IRP.
            // What we're interested in is not whether IoCancelIrp() was called
            // (ie, nextIrp->Cancel is set), but whether IoCancelIrp() calle
            // is about to call) our cancel routine. To check that, check t
            // of the test-and-set macro IoSetCancelRoutine.
            //
            if (oldCancelRoutine) {
                //
                //  Cancel routine not called for this IRP.  Return this IRP.
                //
                return irp;
            }
            else {
                //
                // This IRP was just cancelled and the cancel routine was (or will
                // be) called. The cancel routine will complete this IRP as soon as
                // we drop the spinlock. So don't do anything with the IRP.
                //
                // Also, the cancel routine will try to dequeue the IRP, so make the
                // IRP's listEntry point to itself.
                //
                ASSERT (irp->Cancel);
                InitializeListHead (&irp->Tail.Overlay.ListEntry);
            }
        }
    }
```

Ready | Ln 2292 | Col 41 | Ch 41 | INS

Microsoft Development Environment [design] - mouclass.c [Read Only]

File Edit View Debug Tools Window Help

mouclass.c

```
for (entry = DeviceExtension->ReadQueue.Flink;
     entry != &DeviceExtension->ReadQueue;
     entry = entry->Flink) {

    irp = CONTAINING_RECORD (entry, IRP, Tail.Overlay.ListEntry);
    stack = IoGetCurrentIrpStackLocation (irp);
    if (stack->FileObject == FileObject) {
        RemoveEntryList (entry);

        oldCancelRoutine = IoSetCancelRoutine (irp, NULL);

        //
        // IoCancelIrp() could have just been called on this IRP.
        // What we're interested in is not whether IoCancelIrp() was called
        // (ie, nextIrp->Cancel is set), but whether IoCancelIrp() calle
        // is about to call) our cancel routine. To check that, check th
        // of the test-and-set macro IoSetCancelRoutine.
        //
        if (oldCancelRoutine) {
            //
            //  Cancel routine not called for this IRP.  Return this IRP.
            //
            return irp;
        }
        else {
            //
            // This IRP was just cancelled and the cancel routine was (or will
            // be) called. The cancel routine will complete this IRP as soon as
            // we drop the spinlock. So don't do anything with the IRP.
            //
            // Also, the cancel routine will try to dequeue the IRP, so make the
            // IRP's listEntry point to itself.
            //
            ASSERT (irp->Cancel);
            InitializeListHead (&irp->Tail.Overlay.ListEntry);
        }
    }
}
```

Ready | Ln 2292 | Col 41 | Ch 41 | INS

Harder example

Introduction

→ Perhaps recent advances will help unlock solutions to other problems

- Search for thread-scheduling that guarantees termination (operating systems)
- Wang's tiling problem (graphics)
- Synthesis of compounds that kill targeted cells (medicine)
- ………

Outline of lectures

- Lecture 1:
  - Principles
  - Rank function synthesis
- Lecture 2:
  - Checking & refinement
  - Termination analysis
- Lecture 3:
  - Recursion
  - WP synthesis
  - Non-termination
- Lecture 4:
  - Fair termination
  - Data structures
  - Concurrency

Outline

- Introduction
- Well-founded relations and ranking functions
- Disjunctive well foundedness
- Decomposition
- Notes on rank function synthesis

Outline

- Introduction

Cantor Turing

- Well-founded relations and ranking functions

Jones et al,

- Disjunctive well foundedness

Podelski & Rybalchenko

- Decomposition

Floyd

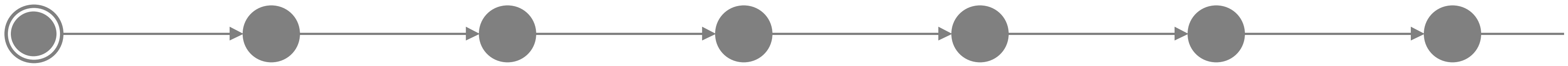
- Notes on rank function synthesis

Colon & Sipma

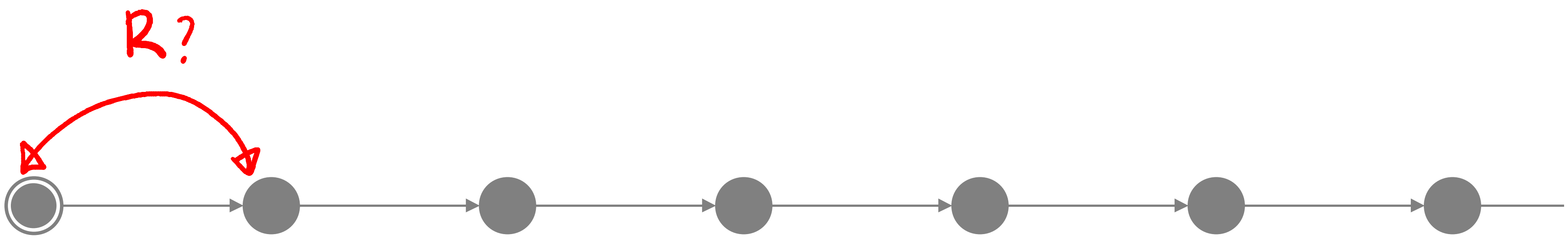
Outline

- Introduction
- Well-founded relations and ranking functions
- Disjunctive well foundedness
- Decomposition
- Notes on rank function synthesis

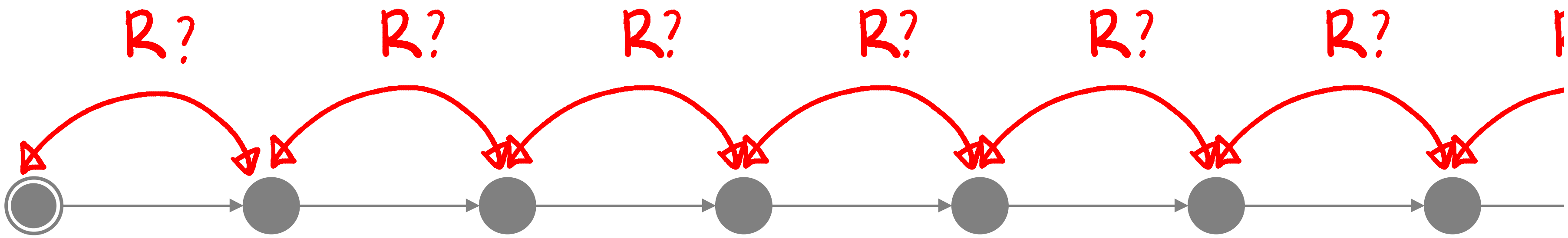
Well-founded relations



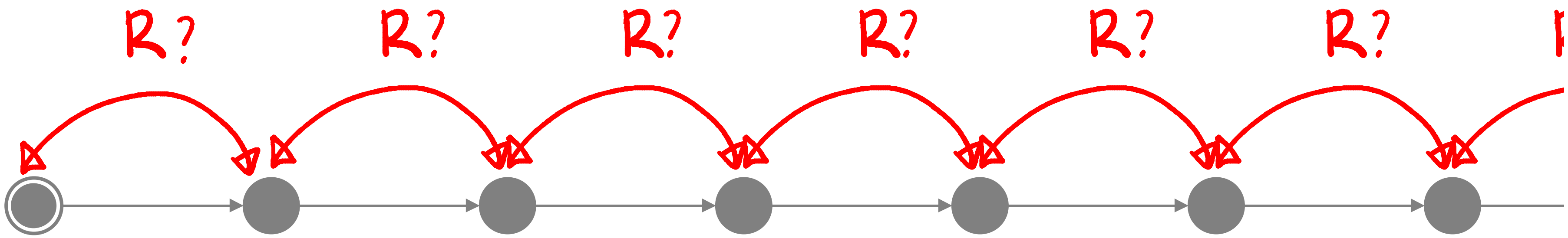
Well-founded relations



Well-founded relations



Well-founded relations



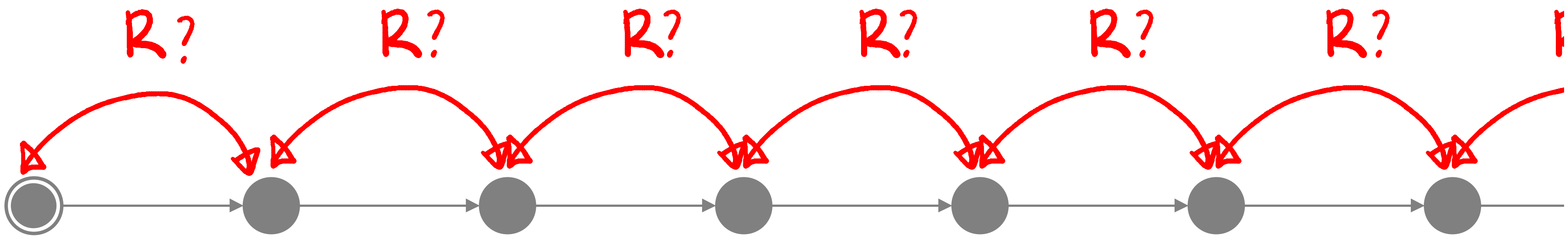
Well-founded relations do not permit infinite sequences

Well-founded relations

$R \subseteq S \times S$ is well-founded *iff* for any infinite S-sequence $s_0, s_1, \ldots$ there exists a j such that $(s_j, s_{j+1}) \notin R$.

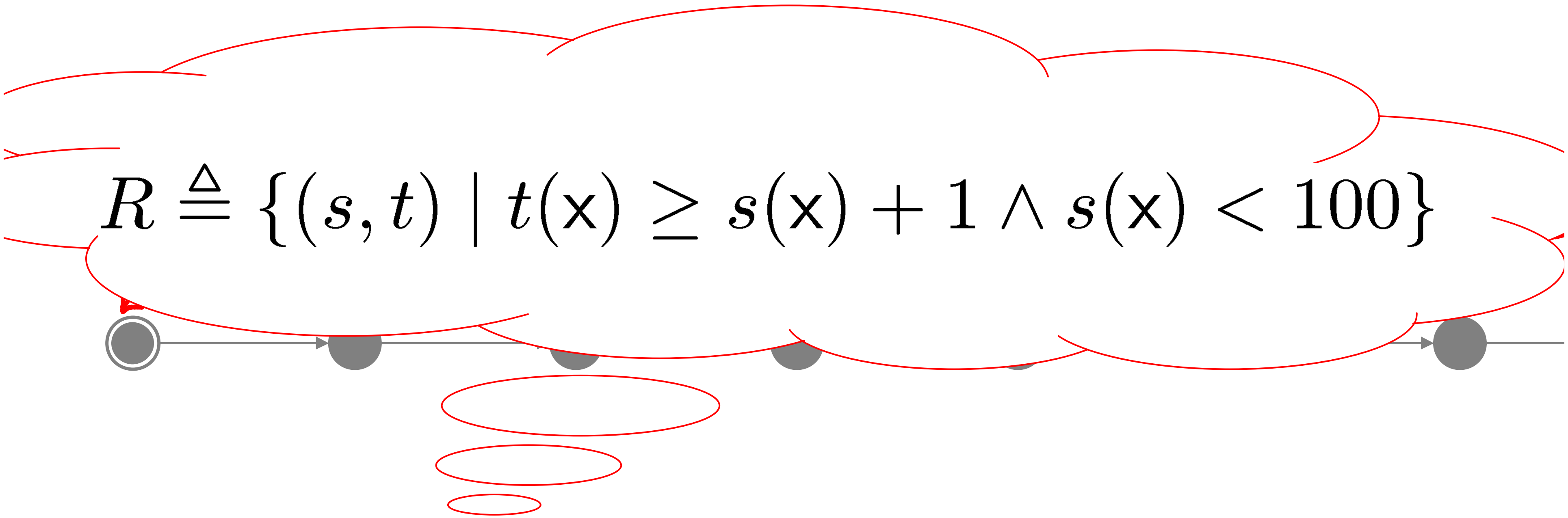
Well-founded relations do not permit infinite sequences

Well-founded relations



$$R \triangleq x' \geq x + 1 \land x < 100$$

Well-founded relations



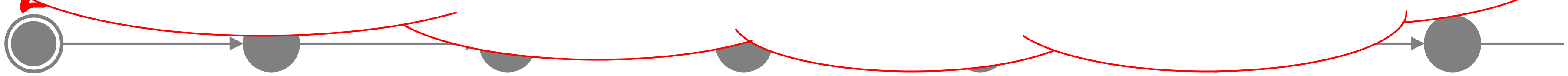
$$R \triangleq \{(s,t) \mid t(\mathsf{x}) \geq s(\mathsf{x}) + 1 \land s(\mathsf{x}) < 100\}$$

$$R \triangleq \mathsf{x}' \geq \mathsf{x} + 1 \land \mathsf{x} < 100$$

Well-founded relations

$$R \triangleq [\![\mathsf{x}' \geq \mathsf{x} + 1 \wedge \mathsf{x} < 100]\!]$$

$$R \triangleq \{(s,t) \mid t(\mathsf{x}) \geq s(\mathsf{x}) + 1 \wedge s(\mathsf{x}) < 100\}$$



$$R \triangleq \mathsf{x}' \geq \mathsf{x} + 1 \wedge \mathsf{x} < 100$$

Questions

- If R is WF, is $R;R$ WF?
- If $R;R$ is WF, is R WF?
- If R is WF and $R \subseteq R'$, is R WF?
- If R is WF and $R' \subseteq R$, is R WF?

Questions

$$R^n \triangleq \begin{cases} R; R^{n-1} & \text{if } n \geq 1 \\ \textsc{Id} & \text{otherwise} \end{cases}$$

$$R^+ \triangleq \{(s,t) \mid \exists n > 0.(s,t) \in R^n\}$$

$$R^* \triangleq R^+ \cup \textsc{Id}$$

Questions

If R is WF, is R^* WF? What about R^+?

$$R^n \triangleq \begin{cases} R; R^{n-1} & \text{if } n \geq 1 \\ \textsc{Id} & \text{otherwise} \end{cases}$$

$$R^+ \triangleq \{(s,t) \mid \exists n > 0.(s,t) \in R^n\}$$

$$R^* \triangleq R^+ \cup \textsc{Id}$$

Questions

If R^+ is WF, is R WF? What about R^*?

$$R^n \triangleq \begin{cases} R; R^{n-1} & \text{if } n \geq 1 \\ \textsc{Id} & \text{otherwise} \end{cases}$$

$$R^+ \triangleq \{(s,t) \mid \exists n > 0.(s,t) \in R^n\}$$

$$R^* \triangleq R^+ \cup \textsc{Id}$$

Outline

- Introduction
- Well-founded relations and ranking functions
- Disjunctive well foundedness
- Decomposition
- Notes on rank function synthesis

Well-ordered sets

$(S, \leq)$ is a well-ordered set *iff* it is

- reflexive $(a \leq a)$
- antisymmetric $(a \leq b \wedge b \leq a \Rightarrow a = b)$
- transitive $(a \leq b \wedge b \leq c \Rightarrow a \leq c)$
- comparable $(a \leq b \vee b \leq a)$
- every nonempty subset of S has a least element.

Well-ordered sets

- The natural numbers are a well-ordered set, as in the worst case 0 is the least element of the subset.
- The integers are not well-ordered because there is no least element.
- For any integer constant $b \in \mathbb{N}$, the set $\{x \mid x \in \mathbb{N} \wedge x \geq b\}$ is a well-ordered set.
- The non-negative real numbers are not a well-ordered set because there there is no least element in the open interval (0,1).

Ranking functions and ranking relations

- $f : S \to Y$ is a *ranking function* if Y is a well-ordered set.

- We define the *ranking relation* of f to be:

$$\trianglerighteq_f \quad \triangleq \quad \{(s,t) \mid f(s) > f(t)\}$$

- **Theorem.** $\mathsf{WF}(R)$ *iff* $\exists f.\ R \subseteq \trianglerighteq_f$

Ranking functions and ranking relations

- $f : S \to Y$ is a *ranking function* if Y is a well-ordered set.

always well founded

- We define the *ranking relation* of f to be:

$$\trianglerighteq_f \quad \triangleq \quad \{(s,t) \mid f(s) > f(t)\}$$

- **Theorem.** $\mathsf{WF}(R)$ *iff* $\exists f.\ R \subseteq \trianglerighteq_f$

Ranking functions and ranking relations

- $f : S \to Y$ is a *ranking function* if Y is a well-ordered set.

always well founded

- We define the *ranking relation* of f to be:

$$\begin{aligned}
\trianglerighteq_f &\triangleq \{(s,t) \mid f(s) > f(t)\} \\
\trianglerighteq_{f,b} &\triangleq \{(s,t) \mid f(s) > f(t) \wedge f(s) \geq b\} \\
\trianglerighteq_{f,b,d} &\triangleq \{(s,t) \mid f(s) \geq f(t) + d \wedge f(s) \geq b\}
\end{aligned}$$

- **Theorem.** $\mathsf{WF}(R)$ *iff* $\exists f.\ R \subseteq \trianglerighteq_f$

Example

Example:

$$R \triangleq \mathsf{x}' = \mathsf{x} - 1 \land \mathsf{x} > 0$$

Example

Example:

→ $R \triangleq \mathrm{x}' = \mathrm{x} - 1 \land \mathrm{x} > 0$

Is R well founded?

Example

Example:

- $R \triangleq \mathrm{x}' = \mathrm{x} - 1 \wedge \mathrm{x} > 0$
- $R \subseteq \trianglerighteq_{\mathrm{x},-1}$

Example

Example:

→ $R \triangleq \mathrm{x}' = \mathrm{x} - 1 \wedge \mathrm{x} > 0$

→ $R \subseteq \trianglerighteq_{\mathrm{x},-1}$

Shorthand for $f : S \to \mathbb{N}$
where $f(s) \triangleq s(\mathrm{x})$

Example

Example:

- $R \triangleq \mathsf{x}' = \mathsf{x} - 1 \land \mathsf{x} > 0$
- $R \subseteq \trianglerighteq_{\mathsf{x},-1}$

Example

$$\mathrm{x}' = \mathrm{x} - 1 \wedge \mathrm{x} > 0 \subseteq \mathrm{x}' > \mathrm{x} \wedge \mathrm{x} \geq -1$$

- $R \subseteq \unrhd_{\mathrm{x},-1}$

$$\forall x, x'.\ x' = x - 1 \wedge x > 0 \Rightarrow x' > x \wedge x \geq -1$$

$$\mathsf{x}' = \mathsf{x} - 1 \wedge \mathsf{x} > 0 \subseteq \mathsf{x}' > \mathsf{x} \wedge \mathsf{x} \geq -1$$

- $R \subseteq \trianglerighteq_{\mathsf{x},-1}$

$$\forall x, x'.\ x' = x - 1 \land x > 0 \Rightarrow x' > x \land x \geq -1$$

$$\mathsf{x}' = \mathsf{x} - 1 \land \mathsf{x} > 0 \subseteq \mathsf{x}' > \mathsf{x} \land \mathsf{x} \geq -1$$

→ $R \subseteq \trianglerighteq_{\mathsf{x},-1}$

Connection is made precise in the handout

Questions

(a) $1 < 0$

(b) $0 < 1$

(c) $x' > x \wedge x' < 1000$

(d) $x' > x \wedge x' > 1000$

(e) $x' \geq x + 1 \wedge x' < 1000$

(f) $x' \geq x - 1 \wedge x' < 1000$

(g) $y' \geq y + 1 \wedge z' = z \wedge z < 1000$

(h) $y' + 1 \geq y \wedge z' = z \wedge z < 1000$

(i) $(x' = x - 1 \vee x' = x + 1) \wedge x < 1000$

(j) $x' = x - z \wedge x > 0$

Questions

(a) $1 < 0$

(b) $0 < 1$

(c) $x' > x \wedge x' < 1000$

(d) $x' > x \wedge x' > 1000$

(e) $x' \geq x + 1 \wedge x' < 1000$

(f) $x' \geq x - 1 \wedge x' < 1000$

(g) $y' \geq y + 1 \wedge z' = z \wedge z < 1000$

(h) $y' + 1 \geq y \wedge z' = z \wedge z < 1000$

(i) $(x' = x - 1 \vee x' = x + 1) \wedge x < 1000$

(j) $x' = x - z \wedge x > 0$

Let's try to prove these with a decision procedure

Transition systems

Notation:

→ Transition system: $P = (I, R, S)$

→ Update relation: R

→ Initial states: I

→ Transition relation: $R\big|_I^{*} \triangleq R \cap (R^*(I) \times R^*(I))$

Transition systems

Notation:

- Transition system: $P = (I, R, S)$
- Update relatio
- Initial states: I
- Transition relation: $R\big|_I \triangleq R \cap (R^*(I) \times R^*(I))$

A transition system is terminating if its *transition relation* is *WF*

Notation:

→ Tr

$$R|_{\downarrow Q} \triangleq R \cap (Q \times Q)$$

$$R|_{\downarrow^* I} = R|_{\downarrow R^*(I)}$$

minating

is *WF*

→ Initia

→ Transition relation: $R|_{\downarrow^* I} \triangleq R \cap (R^*(I) \times R^*(I))$

Supporting invariants

- → Update relations are typically not well founded, even when the transition relation is

- → Computing a precise $R^*(I)$ is very hard (technically, undecidable)

Supporting invariants

- In practice, we must find a supporting invariant that is "computable" yet still powerful enough for termination:

$$Q \text{ is an invariant of iff } Q \supseteq R^*(I)$$

- Much of the hard part when proving WF is finding the right invariant

Example

$$R \triangleq \mathsf{x}' = \mathsf{x} + \mathsf{y} \wedge \mathsf{y}' = \mathsf{y} \wedge \mathsf{x} > 0$$

$$I \triangleq \mathsf{y}' < -1$$

→ Is the update relation well founded?

Example

$$R \triangleq \mathsf{x}' = \mathsf{x} + \mathsf{y} \wedge \mathsf{y}' = \mathsf{y} \wedge \mathsf{x} > 0$$

$$I \triangleq \mathsf{y}' < -1$$

- → Is the update relation well founded?
- → Is the transition relation well founded?

Example

$$R \triangleq \mathsf{x}' = \mathsf{x} + \mathsf{y} \land \mathsf{y}' = \mathsf{y} \land \mathsf{x} > 0$$

$$I \triangleq \mathsf{y}' < -1$$

- → Is the update relation well founded?
- → Is the transition relation well founded?
- → How would you prove this with a decision procedure?

Outline

- Introduction
- Well-founded relations and ranking functions
- Disjunctive well foundedness
- Decomposition techniques
- Rank function synthesis (if time permits)

Example

Is the following relation well founded?

$$\bigwedge \left\{ \begin{array}{l} \mathsf{x} > 0, \\ \mathsf{y} > 0, \\ (\mathsf{x}' = \mathsf{x} - 1 \wedge \mathsf{y}' = \mathsf{y} + 1) \vee (\mathsf{x}' = \mathsf{x} \wedge \mathsf{y}' = \mathsf{y} - 1) \end{array} \right\}$$

Yes? What's the ranking function?

No? Show me a counterexample

Example

Is the following relation well founded?

$$\bigwedge \left\{ \begin{array}{l} \mathsf{x} > 0, \\ \mathsf{y} > 0, \\ (\mathsf{x}' = \mathsf{x} - 1 \wedge \mathsf{y}' = \mathsf{y} + 1) \vee (\mathsf{x}' = \mathsf{x} \wedge \mathsf{y}' = \mathsf{y} - 1) \end{array} \right\}$$

Yes? What's the ranking function?

No? Show me a counterexample

$f(x,y) \triangleq$??

Example

Is the following relation well founded?

$$\bigwedge \left\{ \begin{array}{l} \mathsf{x} > 0, \\ \mathsf{y} > 0, \\ (\mathsf{x}' = \mathsf{x} - 1 \land \mathsf{y}' = \mathsf{y} + 1) \lor (\mathsf{x}' = \mathsf{x} \land \mathsf{y}' = \mathsf{y} - 1) \end{array} \right\}$$

Yes? What's the ranking function?

No? Show me a counterexample

$$f(x, y) \triangleq 2x + y$$

Example

Is the following relation well foun

$$\bigwedge \begin{cases} x > 0, \\ y > 0, \\ (x' = x - 1 \wedge y \end{cases}$$

Yes? What's the ran

No? Show me a coun

Static guess as to relative importance of variables

$f(x,y) \triangleq 2x + y$

Example

Is the following relation well founded?

$$\bigwedge \left\{ \begin{array}{l} \mathsf{x} > 0, \\ \mathsf{y} > 0, \\ (\mathsf{x}' = \mathsf{x} - 1) \vee (\mathsf{x}' = \mathsf{x} \wedge \mathsf{y}' = \mathsf{y} - 1) \end{array} \right\}$$

Yes? What's the ranking function?

No? Show me a counterexample

Example

Is the following relation well founded?

y := *

$$\bigwedge \left\{ \begin{array}{l} \mathsf{x} > 0, \\ \mathsf{y} > 0, \\ (\mathsf{x}' = \mathsf{x} - 1) \vee (\mathsf{x}' = \mathsf{x} \wedge \mathsf{y}' = \mathsf{y} - 1) \end{array} \right\}$$

Yes? What's the ranking function?

No? Show me a counterexample

Example

Is the following relation well founded?

y := *

$$\bigwedge \left\{ \begin{array}{l} \mathsf{x} > 0, \\ \mathsf{y} > 0, \\ (\mathsf{x}' = \mathsf{x} - 1) \vee (\mathsf{x}' = \mathsf{x} \wedge \mathsf{y}' = \mathsf{y} - 1) \end{array} \right\}$$

Yes? What's the ranking function?

No? Show me a counterexample

$f(x,y) \triangleq$???

Temptation!!!!!

- Its tempting to look for ranking functions by examining some cases

$$\bigwedge \left\{ \begin{array}{l} x > 0, \\ y > 0, \\ (x' = x - 1) \lor (x' = x \land y' = y - 1) \end{array} \right\}$$

Temptation!!!!!

- Its tempting to look for ranking functions by examining some cases

$$\bigwedge \left\{ \begin{array}{l} x > 0, \\ y > 0, \\ (x' = x - 1) \lor \cancel{(x' = x \land y' = y - 1)} \end{array} \right\}$$

Temptation!!!!!

- Its tempting to look for ranking functions by examining some cases

$$\bigwedge \left\{ \begin{array}{l} x > 0, \\ y > 0, \\ (x' = x - 1) \lor \cancel{(x' = x \land y' = y - 1)} \end{array} \right\}$$

Is this relation well founded?

Temptation!!!!!

- Its tempting to look for ranking functions by examining some cases

$$\bigwedge \left\{ \begin{array}{l} x > 0, \\ y > 0, \\ (x' = x - 1) \lor (\cancel{x' = x \land y' = y - 1}) \end{array} \right\}$$

Is this relation well founded?

$f(x,y) = x$

Temptation!!!!!

- Its tempting to look for ranking functions by examining some cases

$$\bigwedge \left\{ \begin{array}{l} x > 0, \\ y > 0, \\ (\cancel{x' = x - 1}) \vee (x' = x \wedge y' = y - 1) \end{array} \right\}$$

$f(x,y) = x$

Temptation!!!!!

→ Its tempting to look for ranking functions by examining some cases

$$\bigwedge \left\{ \begin{array}{l} x > 0, \\ y > 0, \\ (\cancel{x' = x - 1}) \vee (x' = x \wedge y' = y - 1) \end{array} \right\}$$

$f(x, y) = y$

$f(x, y) = x$

Temptation!!!!!

- Its tempting to look for ranking functions by examining some cases

$$\bigwedge \left\{ \begin{array}{l} \mathrm{x} > 0, \\ \mathrm{y} > 0, \\ \cancel{(\mathrm{x}' = \mathrm{x} - 1)} \vee (\mathrm{x}' = \mathrm{x} \wedge \mathrm{y}' = \mathrm{y} - 1) \end{array} \right\}$$

$f(x,y) = y$

$f(x,y) = x$

How can we combine these?

Temptation!!!!!

→ Its tempting to look for ranking examining some cases

$$R \subseteq \trianglerighteq_{\mathsf{x}} \cup \trianglerighteq_{\mathsf{y}} \ ?$$

$$\bigwedge \left\{ \begin{array}{l} \mathsf{x} > 0, \\ \mathsf{y} > 0, \\ \cancel{(\mathsf{x}' = \mathsf{x} - 1)} \vee (\mathsf{x}' = \mathsf{x} \wedge \mathsf{y}' = \mathsf{y} - 1) \end{array} \right\}$$

$f(x,y) = y$

$f(x,y) = x$

How can we combine these?

Temptation!!!!!

→ Its tempting to look for rankin
examining some cases

$\cancel{R \subseteq \rhd_x \cup \rhd_y\ ?}$

$$\bigwedge \left\{ \begin{array}{l} x > 0, \\ y > 0, \\ (\cancel{x' = x - 1}) \vee (x' = x \wedge y' = y - 1) \end{array} \right\}$$

$f(x,y) = y$

$f(x,y) = x$

How can we combine these?

Disjunctive well foundedness

If Q and R are well founded, is $Q \cup R$ well founded?

Disjunctive well foundedness

If Q and R are well founded, is $Q \cup R$ well founded?

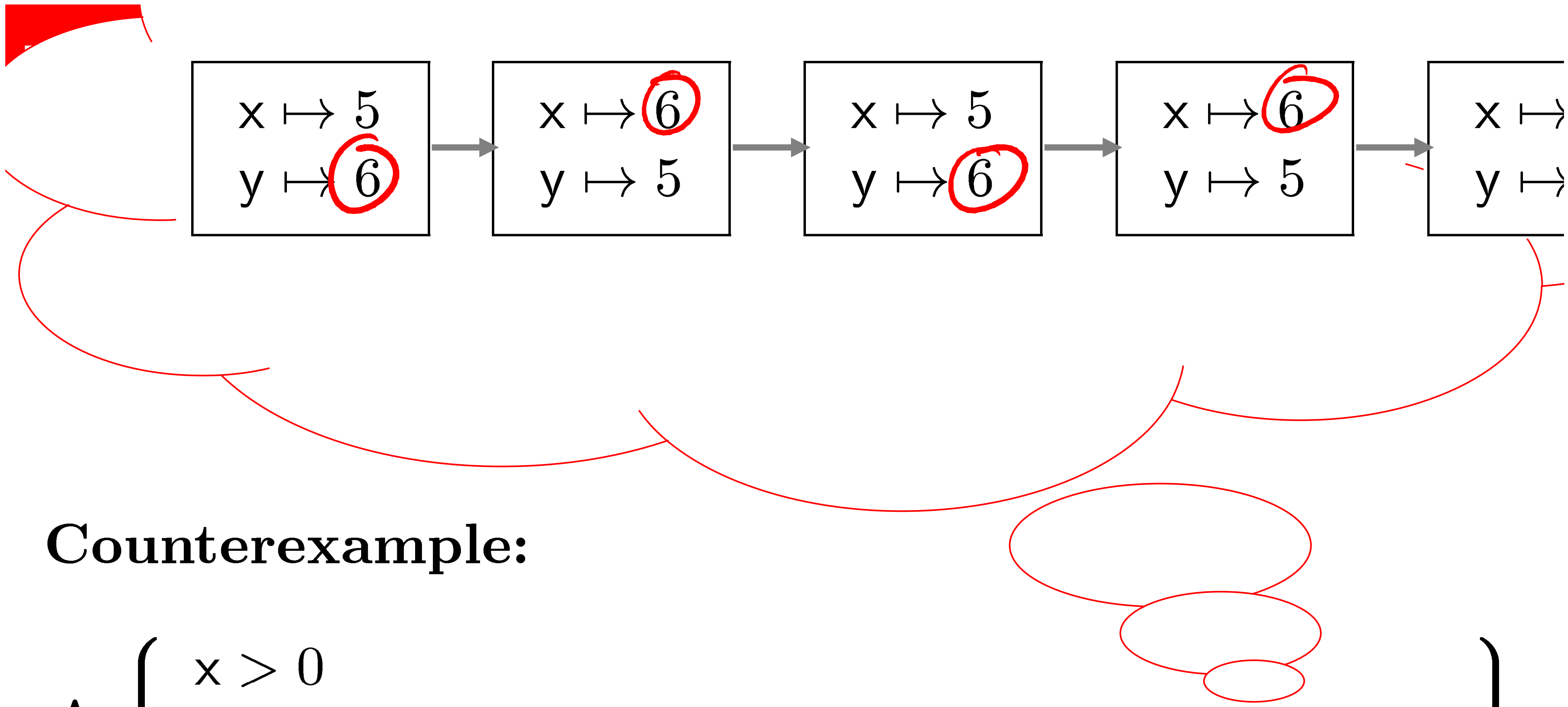
Counterexample:

$$\bigwedge \left\{ \begin{array}{l} \mathsf{x} > 0 \\ \mathsf{y} > 0 \\ (\mathsf{x}' = \mathsf{x} + 1 \wedge \mathsf{y}' = \mathsf{y} - 1) \vee (\mathsf{x}' = \mathsf{x} - 1 \wedge \mathsf{y}' = \mathsf{y} + 1) \end{array} \right\}$$

$$\boxed{\begin{array}{c} x \mapsto 5 \\ y \mapsto 6 \end{array}} \rightarrow \boxed{\begin{array}{c} x \mapsto 6 \\ y \mapsto 5 \end{array}} \rightarrow \boxed{\begin{array}{c} x \mapsto 5 \\ y \mapsto 6 \end{array}} \rightarrow \boxed{\begin{array}{c} x \mapsto 6 \\ y \mapsto 5 \end{array}} \rightarrow \boxed{\begin{array}{c} x \mapsto \\ y \mapsto \end{array}}$$

Counterexample:

$$\bigwedge \left\{ \begin{array}{l} x > 0 \\ y > 0 \\ (x' = x + 1 \land y' = y - 1) \lor (x' = x - 1 \land y' = y + 1) \end{array} \right\}$$



Counterexample:

$$\bigwedge \left\{ \begin{array}{l} x > 0 \\ y > 0 \\ (x' = x + 1 \land y' = y - 1) \lor (x' = x - 1 \land y' = y + 1) \end{array} \right\}$$

Theorem

- Assume that $Q_1, Q_2, \ldots Q_n$ are well-founded relations
- R is well-founded *iff* $R^+ \subseteq Q_1 \cup Q_2 \cup \ldots \cup Q_n$.

Theorem

- Assume that $Q_1, Q_2, \ldots Q_n$ are well-founded relations
- R is well-founded *iff* $R^+ \subseteq Q_1 \cup Q_2 \cup \ldots \cup Q_n$.

This is key!

Disjunctive well foundedness

- *Constructing* the argument is much easier
  - Simply union based on examples rather than a holistic synthesis
  - Many (hopefully) easier problems, rather than one big one

- *Checking* the argument is harder
  - Even checking WF without invariants is now no longer decidable

- Checking is something we know how to do
  - The check is a very difficult (but solvable) invariance property..........more later...........

Disjunctive well foundedness

→ *Constructing* the argument is much easier

- Simply union based on examples rather than a holistic synthesis
- Many (hopefully) easier problems, rather than one big one

→ *Checking* the argument is harder

- Even checking WF without invariants is now no longer decidable

→ Checking is something we know how to do

- The check is a very difficult (but solvable) invariance property……….more later…………

Lemma.

$$R^+ \subseteq Q \text{ if } R \subseteq Q \text{ and } (Q; R) \subseteq Q$$

$$
\begin{array}{rcl}
R & \triangleq & \mathsf{x} > 0 \wedge \mathsf{y} > 0 \wedge \mathsf{x}' = \mathsf{x} - 1 \wedge \mathsf{y}' = \mathsf{y} \\
& \vee & \mathsf{x} > 0 \wedge \mathsf{y} > 0 \wedge \mathsf{y}' = \mathsf{y} - 1
\end{array}
$$

$$Q \triangleq (\trianglerighteq_{\mathsf{y},0} \cap \trianglerighteq_{\mathsf{x},0}) \cup \trianglerighteq_{(\mathsf{y},0)}$$

$$R \subseteq Q,\ (Q; R) \subseteq Q,\ \text{thus } R^+ \subseteq Q\ \checkmark$$

Example

$$R \triangleq \mathsf{x} > 0 \land \mathsf{x}' = \mathsf{x} - \mathsf{y} \land \mathsf{y}' = \mathsf{y} + 1$$

Example

$$R \triangleq \mathsf{x} > 0 \wedge \mathsf{x}' = \mathsf{x} - \mathsf{y} \wedge \mathsf{y}' = \mathsf{y} + 1$$

Can you prove termination with induction?

Outline

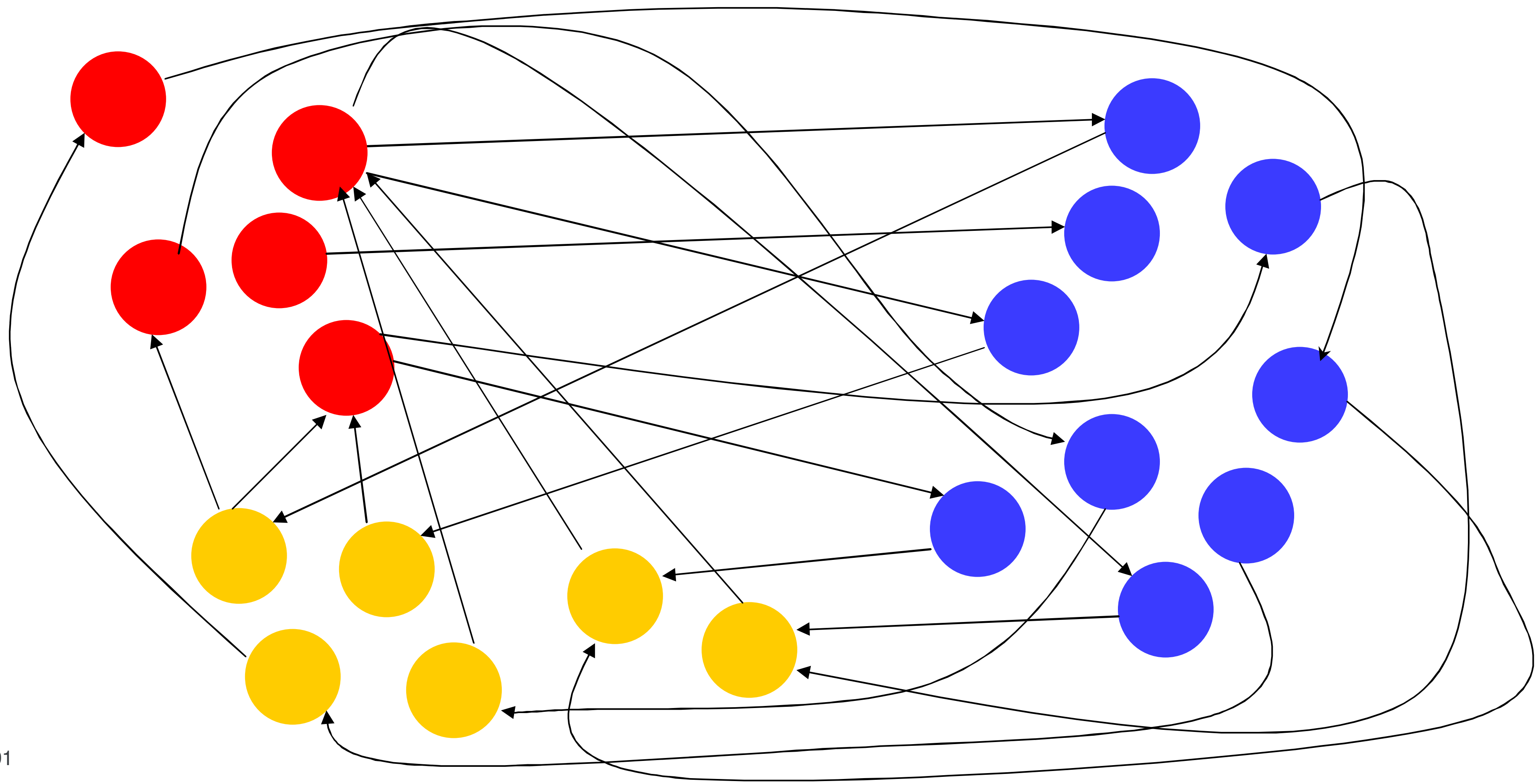
- → Introduction
- → Well-founded relations and ranking
- → Disjunctive well foundedness
- → Decomposition techniques
- → Rank function synthesis (if time permits)

Decomposition

- Most systems we're interested in proving terminating have at least some finite structure we can make use of

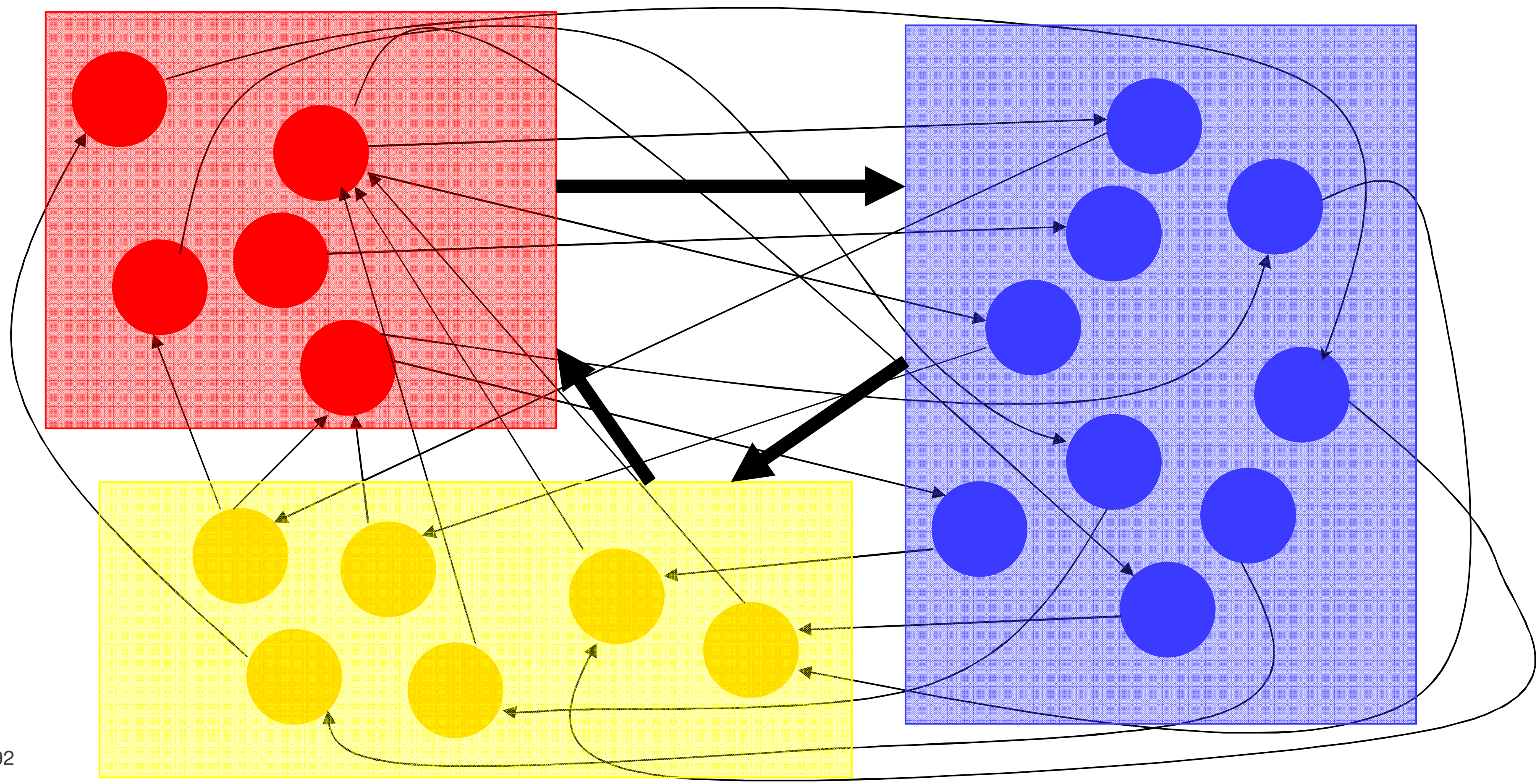
Decomposition

→ Most systems we're interested in proving terminating have at least some finite structure we can make use of



Decomposition

- Most systems we're interested in proving terminating have at least some finite structure we can make use of



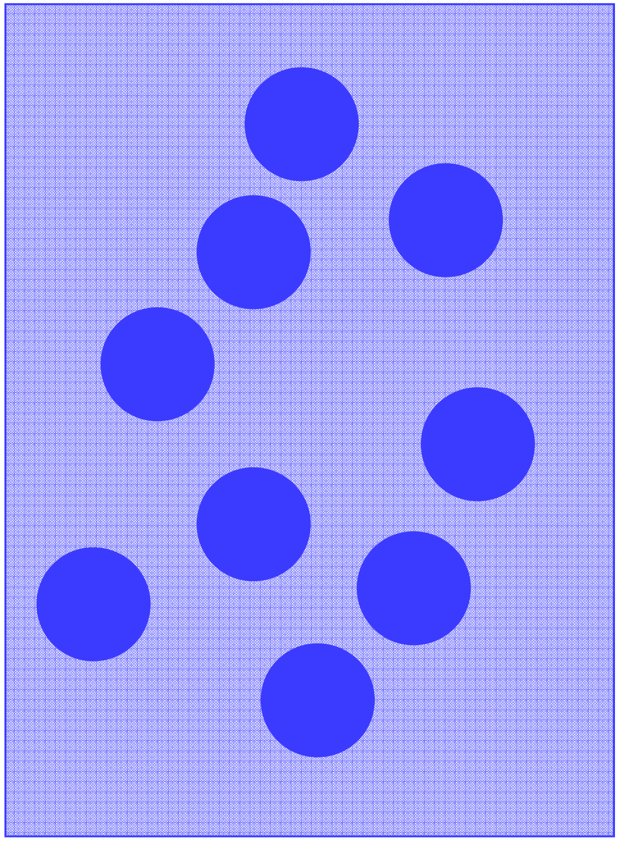
Decomposition

→ Most systems we're interested in proving terminating have at least some finite structure we can make use of

All states at location 10

or

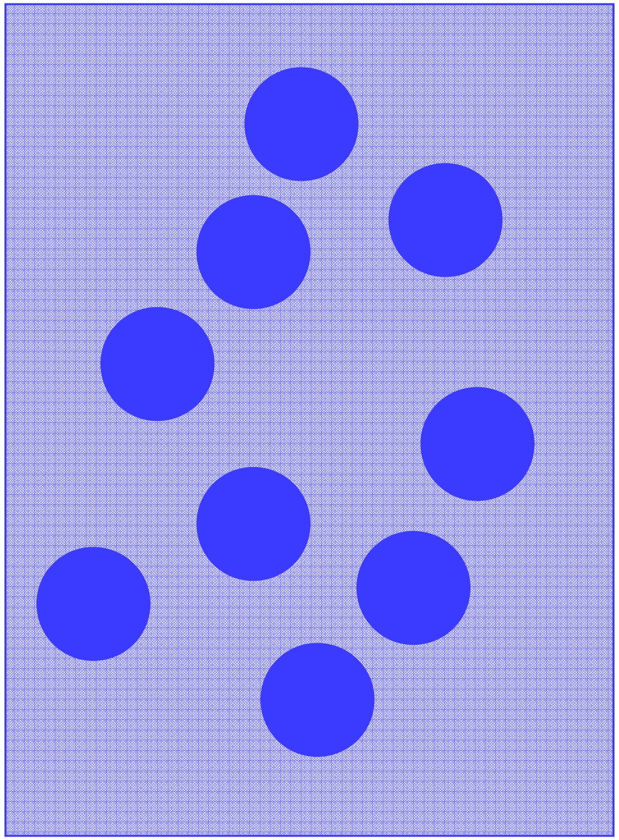
all states at circuit reset



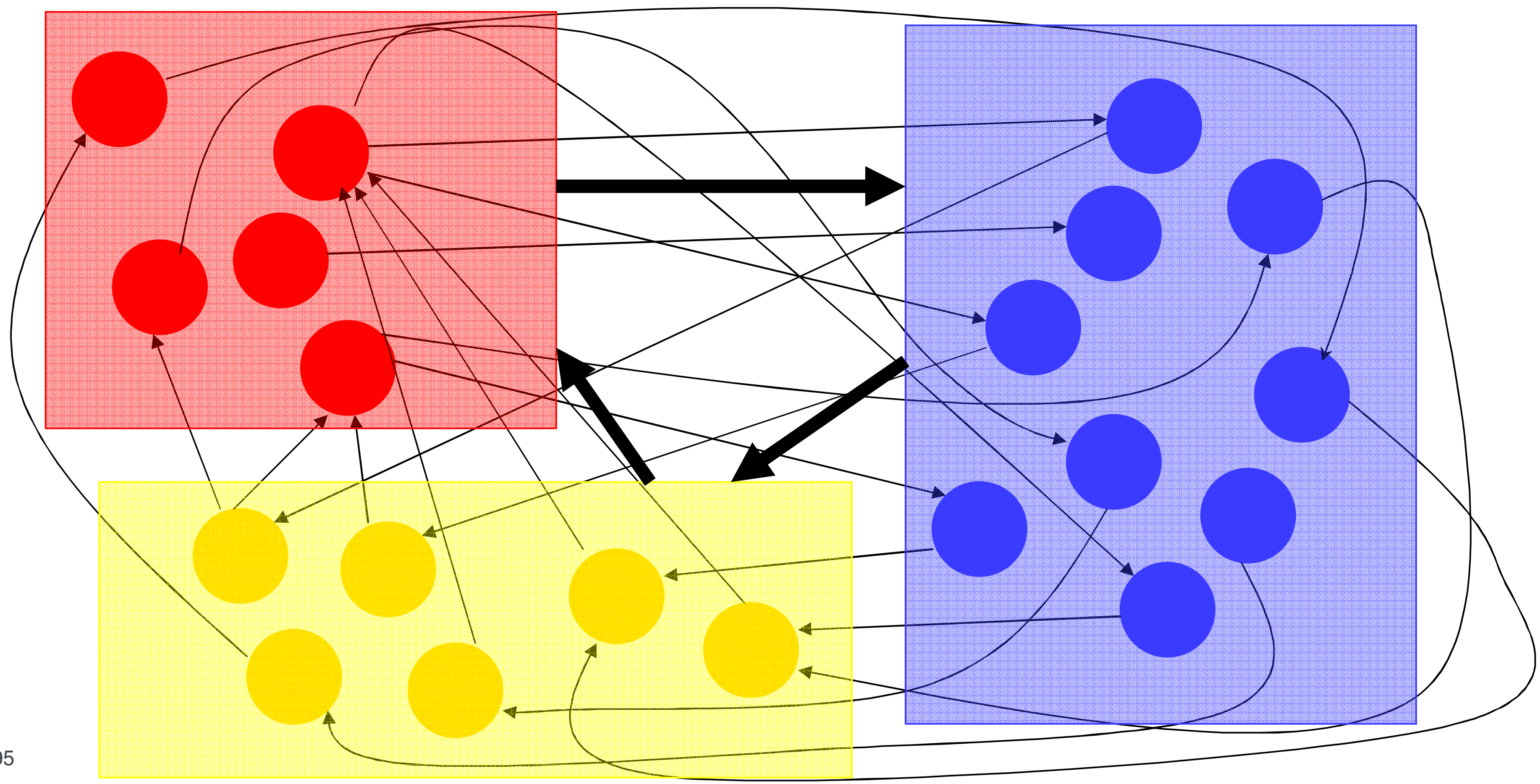
Decomposition

→ Most systems we're interested in proving terminating have at least some finite structure we can make use of

We can prove termination one slice at a time

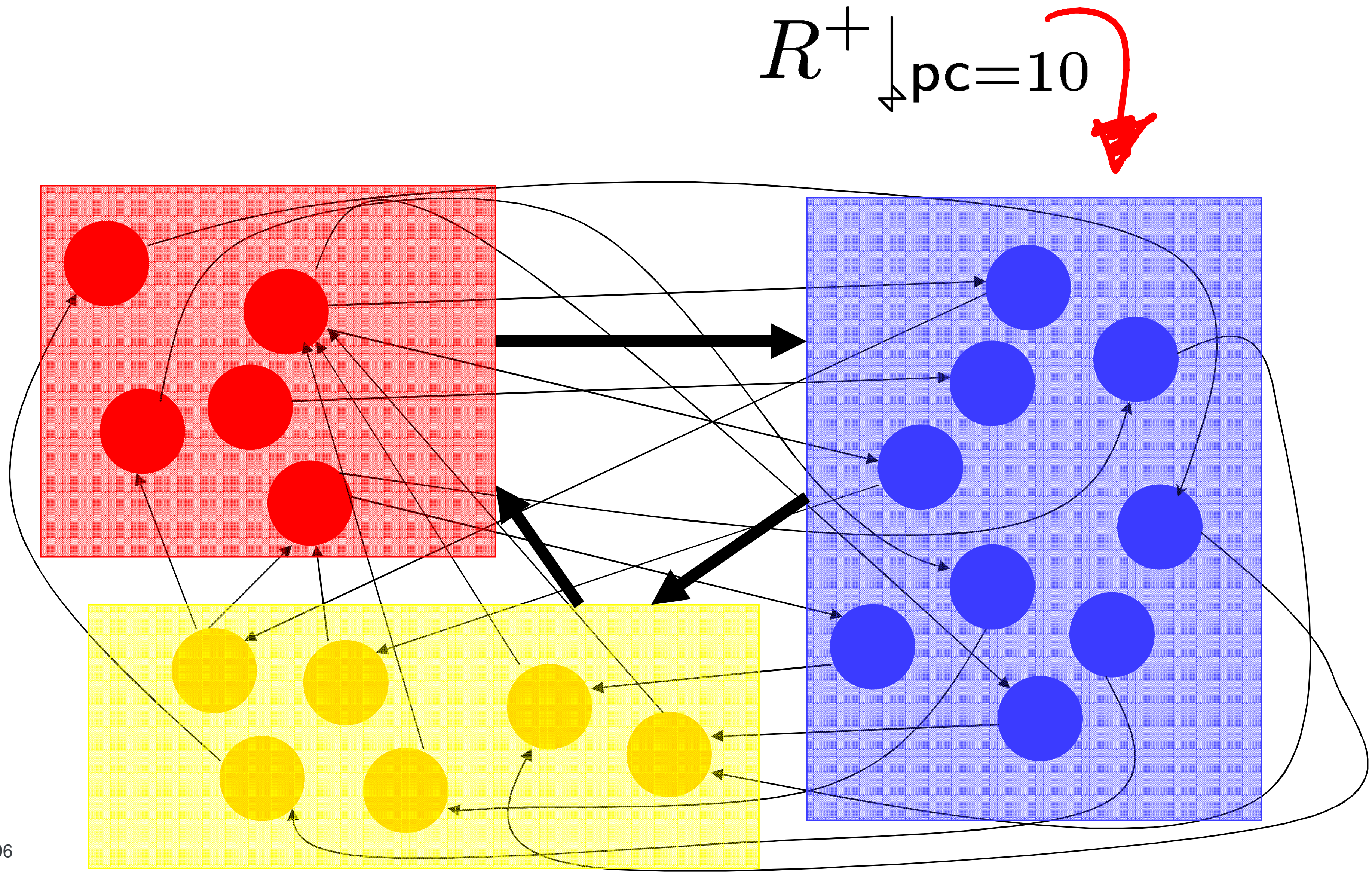


Decomposition



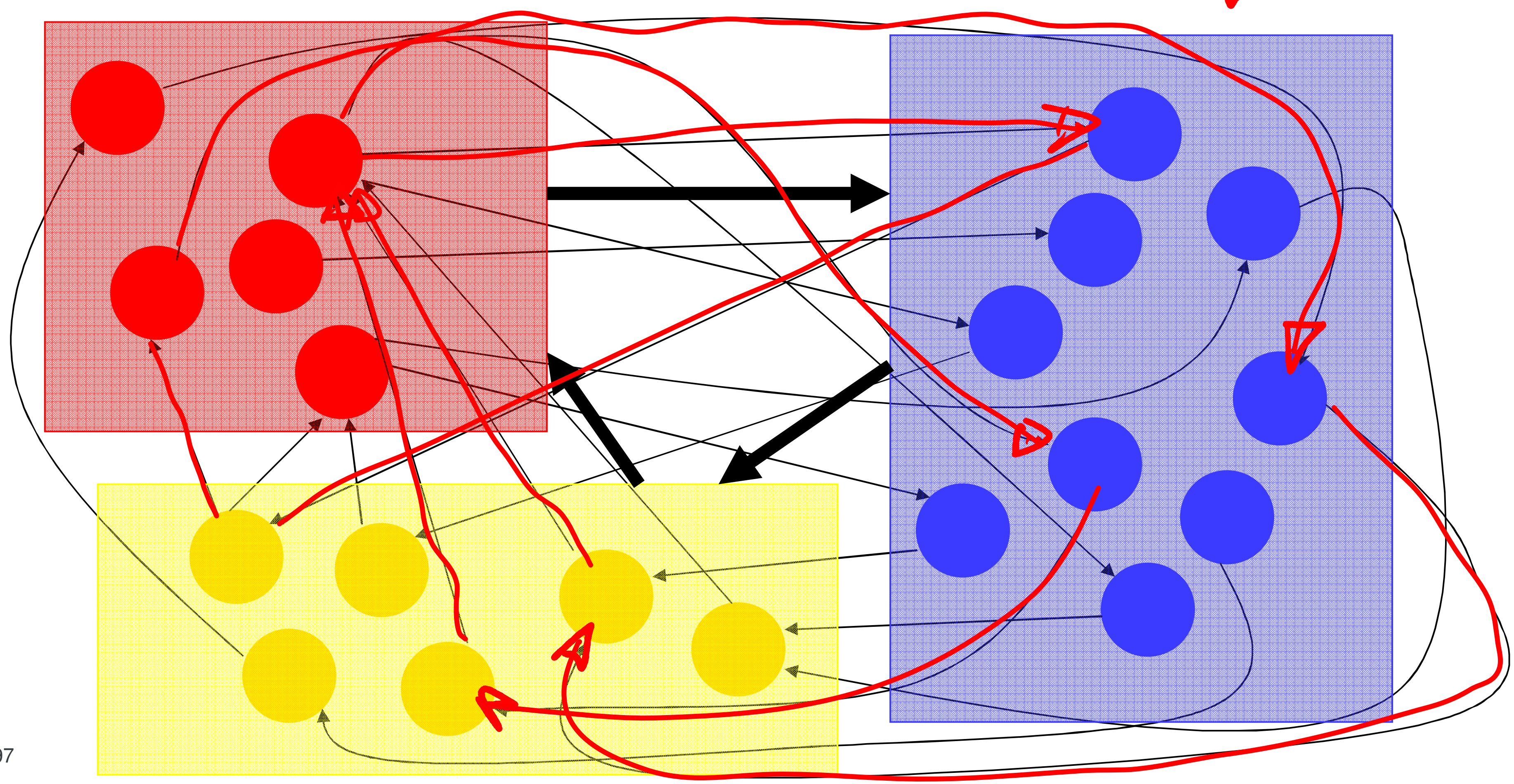
Decomposition

$$R^{+}\downarrow_{\mathrm{pc}=10}$$



Decomposition

$$R^{+}\downarrow_{\mathrm{pc}=10}$$



Decomposition

Theorem

- Assume $v \in \textsc{Var}$
- Assume $L = R^*(I)(v)$ is finite
- $R{\downarrow^*_I}$ is well-founded if for all $l \in L$, $(R{\downarrow^+_I}){\downarrow^\triangleleft_{v=l}}$ is well-founded.

Decomposition

- Assume $v \in \textsc{Var}$
- Assume $L = R^*(I)(v)$ is finite.
- Let k_1 and k_2 be constants from $\textsc{Val}$.
- Assume that, if $R(s,t)$ and $t(v) = k_2$ then $s(v) = k_1$.
- $\forall l \in L.(R{\downarrow}_{I}^{+}){\downarrow}_{v=l}$ is well founded *iff* $\forall l \in L - \{k_2\}.(R{\downarrow}_{I}^{+}){\downarrow}_{v=l}$ is well founded

Example

Is the following relation well founded?

$$
\begin{array}{rcl}
R & \triangleq & (\mathsf{b}' = 1 \land \mathsf{b} = 0) \lor (\mathsf{b}' = 0 \land \mathsf{b} = 1) \\
 & \land & (\mathsf{b} = 1 \land \mathsf{x}' = \mathsf{x} - 1 \land \mathsf{x} > 0) \lor (\mathsf{b} = 0 \land \mathsf{x}' = \mathsf{x})
\end{array}
$$

Yes? What's the ranking function?

No? Show me a counterexample

Example

$$R^+\downarrow_{\mathsf{b}=1} \subseteq Q_1$$

$$\wedge$$

$$R^+\downarrow_{\mathsf{b}=0} \subseteq Q_2$$

Is the following relation ounded?

$$
\begin{array}{rcl}
R & \triangleq & (\mathsf{b}' = 1 \wedge \mathsf{b} = 0) \vee (\mathsf{b}' = 0 \wedge \mathsf{b} = 1) \\
 & \wedge & (\mathsf{b} = 1 \wedge \mathsf{x}' = \mathsf{x} - 1 \wedge \mathsf{x} > 0) \vee (\mathsf{b} = 0 \wedge \mathsf{x}' = \mathsf{x})
\end{array}
$$

Yes? What's the ranking function?

No? Show me a counterexample

Example

$$R^+\!\downharpoonright_{\mathsf{b}=1} \subseteq Q_1$$

$$\wedge$$

$$\cancel{R^+\!\downharpoonright_{\mathsf{b}=0} \subseteq Q_2}$$

Is the following relation ounded?

$$\begin{array}{rcl} R & \triangleq & (\mathsf{b}' = 1 \wedge \mathsf{b} = 0) \vee (\mathsf{b}' = 0 \wedge \mathsf{b} = 1) \\ & \wedge & (\mathsf{b} = 1 \wedge \mathsf{x}' = \mathsf{x} - 1 \wedge \mathsf{x} > 0) \vee (\mathsf{b} = 0 \wedge \mathsf{x}' = \mathsf{x}) \end{array}$$

Yes? What's the ranking function?

No? Show me a counterexample

Example

$$R^+\downharpoonright_{\mathsf{b}=1} \subseteq Q_1$$

$$\wedge$$

$$\cancel{R^+\downharpoonright_{\mathsf{b}=0} \subseteq Q_2}$$

$$\begin{aligned} R^+\downharpoonright_{\mathsf{b}=1} &= \mathsf{b}' = 1 \wedge \mathsf{b} = 1 \wedge \mathsf{x}' < \mathsf{x} \wedge \mathsf{x} > 0 \\ &\subseteq \unrhd_{\mathsf{x},0} \end{aligned}$$

Outline

- → Introduction
- → Well-founded relations and ranking
- → Disjunctive well foundedness
- → Decomposition techniques
- → Notes on rank function synthesis

Rank function synthesis

Goal: find an f such that

$$\forall V, V'.\ R(V, V') \Rightarrow f(V) > f(V')$$

Rank function synthesis

We consider a search for affine functions over generic parameters, *e.g.* $f(g_1, g_2, g_3) = 1g_1 + 2g_2 + 0g_3 + 5$

Goal: find an f such that

$$\forall V, V'.\ R(V, V') \Rightarrow f(V) > f(V')$$

Rank function synthesis

Thus f is the vector of coeffecients $1, 2, 0, 5$, and $f(V)$ is $f_1V_1 + f_2V_2 + f_3V_3 + f_4$

$$\forall V, V'.\ R(V, V') \Rightarrow f(V) > f(V')$$

Rank function synthesis

The difficulty is that search for f_1, f_2, f_3, etc is a non-linear problem.

Thus f is the vector of coeffecients $1, 2, 0, 5$, and $f(V)$ is $f_1 V_1 + f_2 V_2 + f_3 V_3 + f_4$

$$\forall V, V'.\ R(V, V') \Rightarrow f(V) > f(V')$$

Farkas' lemma

Theorem. Assume that

- M is a matrix,
- v is a column vector,
- f is a row vector,
- and $Mv \leq 0$ is satisfiable.

Then:

$$Mv \leq 0 \Rightarrow fv \leq 0$$

$$\textit{iff}$$

$$\exists\lambda.\ \lambda M = f \wedge \lambda \geq 0$$

Farkas' lemma

Theorem. Assume that

- M is a matrix,
- v is a column vector,
- f is a row vector,
- and $Mv \leq 0$ is satisfiable.

Th

Linear system

$$Mv \leq 0 \Rightarrow fv \leq 0$$

iff

$$\exists \lambda.\ \lambda M = f \wedge \lambda \geq 0$$

Farkas' lemma

Theorem. Assume that

- M is a matrix,
- v is a column vector,
- f is a row vector,
- and $Mv \leq 0$ is satisfiable.

Validity

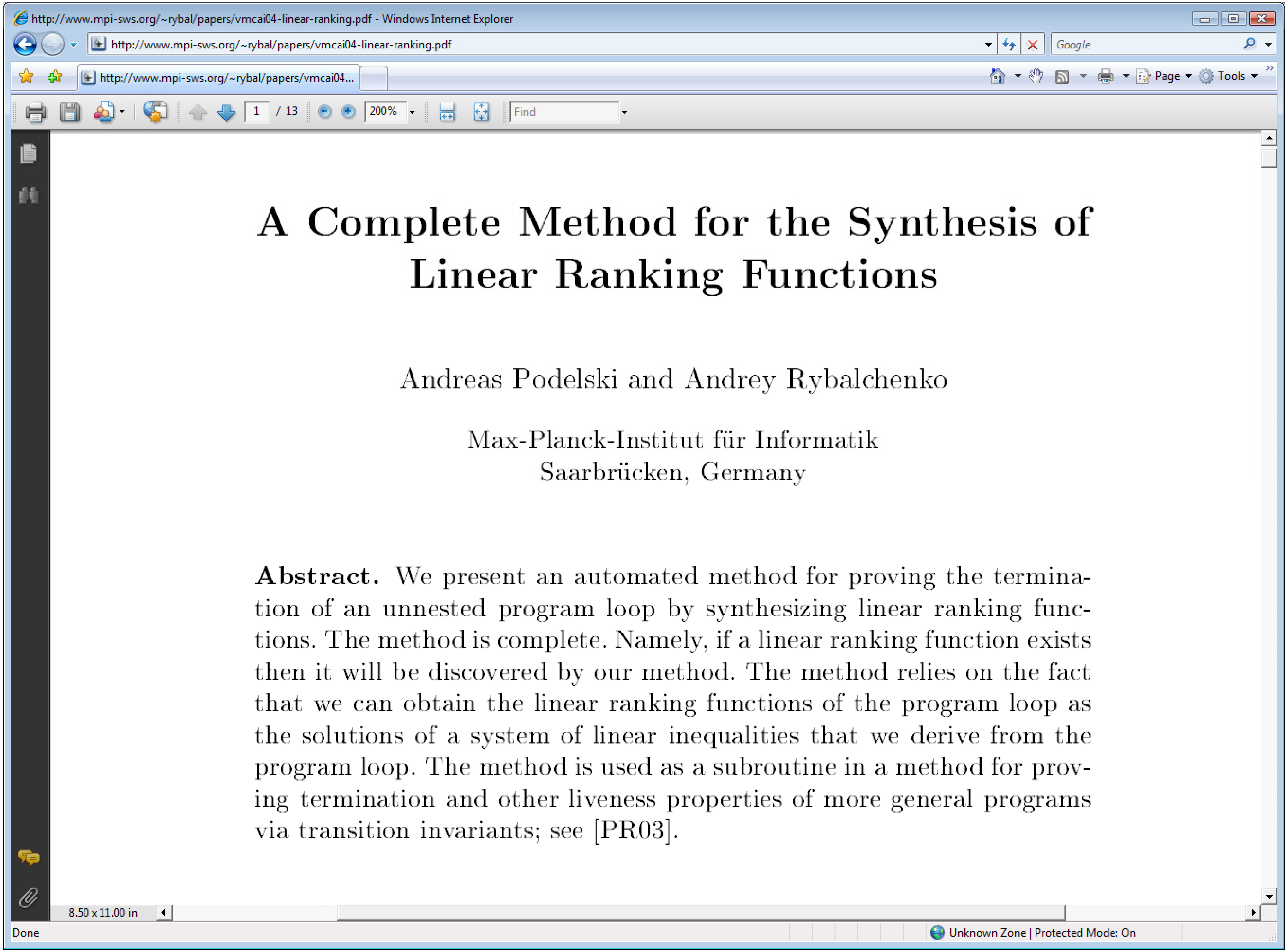
Th

satisfiability

$$Mv \leq 0 \Rightarrow fv \leq 0$$

iff

$$\exists \lambda.\ \lambda M = f \wedge \lambda \geq 0$$



A Complete Method for the Synthesis of Linear Ranking Functions

Andreas Podelski and Andrey Rybalchenko

Max-Planck-Institut für Informatik
Saarbrücken, Germany

Abstract. We present an automated method for proving the termination of an unnested program loop by synthesizing linear ranking functions. The method is complete. Namely, if a linear ranking function exists then it will be discovered by our method. The method relies on the fact that we can obtain the linear ranking functions of the program loop as the solutions of a system of linear inequalities that we derive from the program loop. The method is used as a subroutine in a method for proving termination and other liveness properties of more general programs via transition invariants; see [PR03].

Rank function synthesis

Goal: find an f such that

$$\forall V, V'.\ R(V, V') \Rightarrow f(V) > f(V')$$

Rank function synthesis

Goal: find an f such that

$$\forall V, V'.\ R(V, V') \Rightarrow f(V) > f(V')$$

or $-f(V) \leq -f(V')$, or $\boxed{-f(V) + f(V') \leq 0}$

Rank function synthesis

Goal: find an f such that

$$\forall V, V'.\ R(V, V') \Rightarrow \boxed{-f(V) + f(V') \leq 0}$$

or $-f(V) \leq -f(V')$, or $-f(V) + f(V') \leq 0$

Rank function synthesis

Goal: find an f such that

$$\forall V, V'.\ R(V, V') \Rightarrow -f(V) + f(V') \leq 0$$

Farkas' lemma

Theorem. Assume that

- M is a matrix,
- v is a column vector,
- f is a row vector,
- and $Mv \leq 0$ is satisfiable.

Then:

$$Mv \leq 0 \Rightarrow fv \leq 0$$

iff

$$\exists \lambda.\ \lambda M = f \wedge \lambda \geq 0$$

83

Goal: find an f such that

$$\forall V, V'.\ R(V, V') \Rightarrow -f(V) + f(V') \leq 0$$

Farkas' lemma

Theorem. Assume that

- M is a matrix,
- v is a column vector,
- f is a row vector,
- and $Mv \leq 0$ is satisfiable.

Then:

$$\boxed{Mv \leq 0} \Rightarrow fv \leq 0$$

iff

$$\exists \lambda.\ \lambda M = f \wedge \lambda \geq 0$$

83

Goal: find an f such that

$$\forall V, V'.\ \boxed{R(V, V')} \Rightarrow -f(V) + f(V') \leq 0$$

Farkas' lemma

Microsoft Research Cambridge

Theorem. Assume that

- M is a matrix,
- v is a column vector,
- f is a row vector,
- and $Mv \leq 0$ is satisfiable.

Then:

$$\boxed{Mv \leq 0} \Rightarrow \boxed{fv \leq 0}$$

iff

$$\exists \lambda.\ \lambda M = f \wedge \lambda \geq 0$$

83

Goal: find an f such that

$$\forall V, V'.\ \boxed{R(V, V')} \Rightarrow -f(V) + f(V') \leq 0$$

Farkas' lemma

Microsoft Research Cambridge

Theorem. Assume that

- M is a matrix,
- v is a column vector,
- f is a row vector,
- and $Mv \leq 0$ is satisfiable.

Then:

$$Mv \leq 0 \Rightarrow fv \leq 0$$

iff

$$\underline{\exists \lambda.\ \lambda M = f \wedge \lambda \geq 0}$$

83

Goal: find an f such that

$$\forall V, V'.\ R(V, V') \Rightarrow -f(V) + f(V') \leq 0$$

Now we can use SMT solvers (e.g. Z3)

Rank function synthesis

```
assume(x>0);
x := x - 1;
assume(y>0);
y : = y + pos();
```

Rank function synthesis

```
assume(x>0);
x := x - 1;
assume(y>0);
y : = y + pos();
```

$$
\begin{array}{rcl}
x & > & 0 \\
x' & = & x-1 \\
y & > & 0 \\
y' & > & y
\end{array}
$$

Rank function synthesis

```
assume(x>0);
x := x - 1;
assume(y>0);
y : = y + pos();
```

$$\begin{aligned} x &> 0 \\ x' &= x - 1 \\ y &> 0 \\ y' &> y \end{aligned}$$

$$\begin{aligned} x &> 0 \\ x' &\geq x - 1 \\ x' &\leq x - 1 \\ y &> 0 \\ y' &> y \end{aligned}$$

Rank function synthesis

```
assume(x>0);
x := x - 1;
assume(y>0);
y : = y + pos();
```

$$\begin{array}{rcl} x & > & 0 \\ x' & = & x-1 \\ y & > & 0 \\ y' & > & y \end{array}$$

$$\begin{array}{rcl} x & > & 0 \\ x' & \geq & x-1 \\ x' & \leq & x-1 \\ y & > & 0 \\ y' & > & y \end{array}$$

$$\begin{array}{rcrcrcrcrcl} 0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ 1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ -1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\ 0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\ 0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0 \end{array}$$

Rank function synthesis

$$
\begin{array}{ccccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0
\end{array}
$$

Rank function synthesis

$$
\begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0
\end{array}
$$

Rank function synthesis

$$\begin{array}{ccccccccccc} 0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ 1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ -1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\ 0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\ 0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0 \end{array}$$

$$\subseteq$$

$$\succeq_{f,b}$$

Rank function synthesis

$$\begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0
\end{array}$$

$$\subseteq$$

$$\trianglerighteq_{f,b}$$

Can we find
such an f and b?

Rank function synthesis

$$\begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0
\end{array}$$

$$\subseteq$$

$$\begin{array}{ccc}
f(x, y) & > & f(x', y') \\
f(x', y') & \geq & b
\end{array}$$

Can we find
such an f and b?

Rank function synthesis

$$
\begin{array}{rcrcrcrcrcl}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & & & & &
\end{array}
$$

$$
\begin{array}{rcl}
f(x,y) & > & f(x',y') \\
f(x',y') & \geq & b
\end{array}
$$

$$\subseteq$$

$$
\begin{array}{rcrcrcl}
f(x',y') & + & -f(x,y) & + & 1 & \leq & 0 \\
 & & -f(x',y') & + & b & \leq & 0
\end{array}
$$

Can we find such an f and b?

Rank function synthesis

$$
\begin{array}{rcrcl}
f(a,b) & \triangleq & c_1 a & + & c_2 b \\
-f(a,b) & \triangleq & c_3 b & + & c_4 b \\
c_1 & = & -1 c_3 & & \\
c_2 & = & -1 c_4 & &
\end{array}
$$

$$
\begin{array}{rrcl}
+ & 1 & \leq & 0 \\
+ & 1 & \leq & 0 \\
+ & -1 & \leq & 0 \\
+ & 1 & \leq & 0 \\
+ & 1 & \leq & 0
\end{array}
$$

$$
\begin{array}{rcrcrcl}
f(x',y') & + & -f(x,y) & + & 1 & \leq & 0 \\
 & & -f(x',y') & + & b & \leq & 0
\end{array}
$$

$$
\begin{array}{rcrcl}
f(a,b) & \triangleq & c_1 a & + & c_2 b \\
-f(a,b) & \triangleq & c_3 a & + & c_4 b \\
c_1 & = & -1c_3 & & \\
c_2 & = & -1c_4 & &
\end{array}
$$

$$
\begin{array}{rcrcl}
+ & 1 & \leq & 0 \\
+ & 1 & \leq & 0 \\
+ & -1 & \leq & 0 \\
+ & 1 & \leq & 0 \\
+ & 1 & \leq & 0
\end{array}
$$

$$\subseteq$$

$$
\begin{array}{ccccccccccccc}
c_1x' & + & c_2y' & + & c_3x & + & c_4y & + & 1 & \leq & 0 \\
 & & & & c_3x' & + & c_4y' & + & b & \leq & 0 \\
 & & & & 1c_1 & + & 1c_3 & + & 0 & \leq & 0 \\
 & & & & -1c_1 & + & -1c_3 & + & 0 & \leq & 0 \\
 & & & & 1c_2 & + & 1c_4 & + & 0 & \leq & 0 \\
 & & & & -1c_2 & + & -1c_4 & + & 0 & \leq & 0
\end{array}
$$

Rank function synthesis

$$
\begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \le & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \le & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \le & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \le & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \le & 0
\end{array}
$$

$$\subseteq$$

$$
\begin{array}{ccccccccccc}
c_1x' & + & c_2y' & + & c_3x & + & c_4y & + & 1 & \le & 0 \\
 & & & & c_3x' & + & c_4y' & + & b & \le & 0 \\
 & & & & 1c_1 & + & 1c_3 & + & 0 & \le & 0 \\
 & & & & -1c_1 & + & -1c_3 & + & 0 & \le & 0 \\
 & & & & 1c_2 & + & 1c_4 & + & 0 & \le & 0 \\
 & & & & -1c_2 & + & -1c_4 & + & 0 & \le & 0
\end{array}
$$

Rank function synthesis

$$\begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0
\end{array}$$

$$\Rightarrow$$

$$\begin{array}{ccccccccccc}
c_1 x' & + & c_2 y' & + & c_3 x & + & c_4 y & + & 1 & \leq & 0 \\
 & & & & c_3 x' & + & c_4 y' & + & b & \leq & 0 \\
 & & & & 1c_1 & + & 1c_3 & + & 0 & \leq & 0 \\
 & & & & -1c_1 & + & -1c_3 & + & 0 & \leq & 0 \\
 & & & & 1c_2 & + & 1c_4 & + & 0 & \leq & 0 \\
 & & & & -1c_2 & + & -1c_4 & + & 0 & \leq & 0
\end{array}$$

Rank function synthesis

$$
\begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0
\end{array}
$$

$$\Rightarrow$$

$$
\begin{array}{ccccccccccc}
c_1x' & + & c_2y' & + & c_3x & + & c_4y & + & 1 & \leq & 0 \\
 & & & & c_3x' & + & c_4y' & + & b & \leq & 0 \\
 & & & & 1c_1 & + & 1c_3 & + & 0 & \leq & 0 \\
 & & & & -1c_1 & + & -1c_3 & + & 0 & \leq & 0 \\
 & & & & 1c_2 & + & 1c_4 & + & 0 & \leq & 0 \\
 & & & & -1c_2 & + & -1c_4 & + & 0 & \leq & 0
\end{array}
$$

Nonlinear

Rank function synthesis

$$
\begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0
\end{array}
$$

$$\Rightarrow$$

$$
\begin{array}{ccccccccccc}
c_1 x' & + & c_2 y' & + & c_3 x & + & c_4 y & + & 1 & \leq & 0 \\
 & & & & c_3 x' & + & c_4 y' & + & b & \leq & 0 \\
 & & & & 1c_1 & + & 1c_3 & + & 0 & \leq & 0 \\
 & & & & -1c_1 & + & -1c_3 & + & 0 & \leq & 0 \\
 & & & & 1c_2 & + & 1c_4 & + & 0 & \leq & 0 \\
 & & & & -1c_2 & + & -1c_4 & + & 0 & \leq & 0
\end{array}
$$

Non convex

Rank function synthesis

$$\begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0
\end{array}$$

$$\Rightarrow$$

$$\begin{array}{ccccccccccc}
c_1 x' & + & c_2 y' & + & c_3 x & + & c_4 y & + & 1 & \leq & 0 \\
 & & & & c_3 x' & + & c_4 y' & + & b & \leq & 0 \\
 & & & & 1c_1 & + & 1c_3 & + & 0 & \leq & 0 \\
 & & & & -1c_1 & + & -1c_3 & + & 0 & \leq & 0 \\
 & & & & 1c_2 & + & 1c_4 & + & 0 & \leq & 0 \\
 & & & & -1c_2 & + & -1c_4 & + & 0 & \leq & 0
\end{array}$$

mixture of $\exists$
$\forall$ variables

Rank function synthesis

$$
\begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0
\end{array}
$$

$$\Rightarrow$$

$$
\begin{array}{ccccccccccc}
c_1x' & + & c_2y' & + & c_3x & + & c_4y & + & 1 & \leq & 0 \\
 & & & & c_3x' & + & c_4y' & + & b & \leq & 0 \\
 & & & & 1c_1 & + & 1c_3 & + & 0 & \leq & 0 \\
 & & & & -1c_1 & + & -1c_3 & + & 0 & \leq & 0 \\
 & & & & 1c_2 & + & 1c_4 & + & 0 & \leq & 0 \\
 & & & & -1c_2 & + & -1c_4 & + & 0 & \leq & 0
\end{array}
$$

mixture of $\exists$
$\forall$ variables

Rank function synthesis

$$
\begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \le & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \le & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \le & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \le & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \le & 0
\end{array}
$$

$$\Rightarrow$$

$$c_1x' \quad + \quad c_2y' \quad + \quad c_3x \quad + \quad c_4y \quad + \quad 1 \quad \le \quad 0$$

(for simplicity)

Rank function synthesis

$$
\begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0
\end{array}
$$

$$\Rightarrow$$

$$c_1x' \quad + \quad c_2y' \quad + \quad c_3x \quad + \quad c_4y \quad + \quad 1 \quad \leq \quad 0$$

Rank function synthesis

$$R \triangleq \begin{array}{ccccccccccccc} 0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ 1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ -1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\ 0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\ 0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0 \end{array}$$

$$\Rightarrow$$

$$\psi \triangleq c_1 x' + c_2 y' + c_3 x + c_4 y + 1 \leq 0$$

Farkas' lemma. $R \Rightarrow \psi$ *iff* there exist real multipliers $\lambda_1, \ldots, \lambda_5 \geq 0$ such that

$$c_1 = \sum_{i=1}^{5} \lambda_i a_{i,1} \quad \wedge \cdots \wedge \quad c_4 = \sum_{i=1}^{5} \lambda_i a_{i,4} \quad \wedge \quad 1 \leq \left(\sum_{i=0}^{5} \lambda_i b_i\right)$$

Rank function synthesis

$$R \triangleq \begin{array}{ccccccccccc} 0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ 1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ -1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\ 0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\ 0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0 \end{array}$$

$$\Rightarrow$$

$$\psi \quad \triangleq \quad c_1 x' \quad + \quad c_2 y' \quad + \quad c_3 x \quad + \quad c_4 y \quad + \quad 1 \quad \leq \quad 0$$

Farkas' lemma. $R \Rightarrow \psi$ *iff* there exist real multipliers $\lambda_1, \ldots, \lambda_5 \geq 0$ such that

$$c_1 = \sum_{i=1}^{5} \lambda_i a_{i,1} \quad \wedge \cdots \wedge \qquad c_4 = \sum_{i=1}^{5} \lambda_i a_{i,4} \quad \wedge \quad 1 \leq (\sum_{i=0}^{5} \lambda_i b_i)$$

Rank function synthesis

$$
R \triangleq \begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0
\end{array}
$$

$$\Rightarrow$$

$$\psi \triangleq c_1 x' + c_2 y' + c_3 x + c_4 y + 1 \leq 0$$

Farkas' lemma. $R \Rightarrow \psi$ *iff* there exist real multipliers $\lambda_1, \ldots, \lambda_5 \geq 0$ such that

$$c_1 = \sum_{i=1}^{5} \lambda_i a_{i,1} \quad \wedge \cdots \wedge \quad c_4 = \sum_{i=1}^{5} \lambda_i a_{i,4} \quad \wedge \quad 1 \leq (\sum_{i=0}^{5} \lambda_i b_i)$$

Rank function synthesis

$$
R \triangleq \begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0
\end{array}
$$

$$\Rightarrow$$

$$\psi \triangleq c_1 x' + c_2 y' + c_3 x + c_4 y + 1 \leq 0$$

Farkas' lemma. $R \Rightarrow \psi$ *iff* there exist real multipliers $\lambda_1, \ldots, \lambda_5 \geq 0$ such that

$$c_1 = \sum_{i=1}^{5} \lambda_i a_{i,1} \wedge \cdots \wedge \quad c_4 = \sum_{i=1}^{5} \lambda_i a_{i,4} \quad \wedge \quad 1 \leq \left(\sum_{i=0}^{5} \lambda_i b_i\right)$$

Rank function synthesis

$$R \triangleq \begin{array}{ccccccccccc} 0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ 1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ -1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\ 0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\ 0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0 \end{array}$$

$$\Rightarrow$$

$$\psi \triangleq c_1 x' + c_2 y' + c_3 x + c_4 y + 1 \leq 0$$

Farkas' lemma. $R \Rightarrow \psi$ *iff* there exist real multipliers $\lambda_1, \ldots, \lambda_5 \geq 0$ such that

$$c_1 = \sum_{i=1}^{5} \lambda_i a_{i,1} \quad \wedge \cdots \wedge \quad c_4 = \sum_{i=1}^{5} \lambda_i a_{i,4} \quad \wedge \quad 1 \leq (\sum_{i=0}^{5} \lambda_i b_i)$$

Rank function synthesis

$$R \triangleq \begin{array}{ccccccccccc} 0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ 1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ -1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\ 0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\ 0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0 \end{array}$$

$$\begin{array}{ccccccccccc} c_1 & = & 0\lambda_1 & + & 1\lambda_2 & + & -1\lambda_3 & + & 0\lambda_4 & + & 0\lambda_5 \\ c_2 & = & 0\lambda_1 & + & 0\lambda_2 & + & 0\lambda_3 & + & 0\lambda_4 & + & -1\lambda_5 \\ c_3 & = & -1\lambda_1 & + & -1\lambda_2 & + & 1\lambda_3 & + & 0\lambda_4 & + & 0\lambda_5 \\ c_4 & = & 0\lambda_1 & + & 0\lambda_2 & + & 0\lambda_3 & + & -1\lambda_4 & + & 1\lambda_5 \\ 1 & \leq & 1\lambda_1 & + & 1\lambda_2 & + & -1\lambda_3 & + & 1\lambda_4 & + & 1\lambda_5 \\ c_1 & = & -1c_3 & \wedge & \lambda_1 \geq 0 & \wedge & \lambda_2 \geq 0 & \wedge & \lambda_3 \geq 0 & & \\ c_2 & = & -1c_4 & \wedge & \lambda_4 \geq 0 & \wedge & \lambda_5 \geq 0 & & & & \end{array}$$

$\psi \triangleq$

Farkas' lem

$\lambda_1, \ldots, \lambda_5 >$

$$c_1 = \sum_{i=1}^{5} \lambda_i a_{i,1} \quad \wedge \cdots \wedge \quad c_4 = \sum_{i=1}^{5} \lambda_i a_{i,4} \quad \wedge \quad 1 \leq \left(\sum_{i=0}^{5} \lambda_i b_i\right)$$

Rank function synthe

Linear, convex, with only ∃ variables ....

$$
\begin{array}{lcccccccccc}
 & & & & & & & & & \leq & 0 \\
 & & & & & & & & 1 & \leq & 0 \\
R \triangleq & -1 & & & & + & 0y & + & -1 & \leq & 0 \\
 & 0x' & + & 0 & & 0x & + & -1y & + 1 & \leq & 0 \\
 & 0x' & + & -1 & + & 0x & + & 1y & + 1 & \leq & 0
\end{array}
$$

$$
\begin{array}{lcccccccccc}
c_1 & = & 0\lambda_1 & + & 1\lambda_2 & + & -1\lambda_3 & + & 0\lambda_4 & + & 0\lambda_5 \\
c_2 & = & 0\lambda_1 & + & 0\lambda_2 & + & 0\lambda_3 & + & 0\lambda_4 & + & -1\lambda_5 \\
c_3 & = & -1\lambda_1 & + & -1\lambda_2 & + & 1\lambda_3 & + & 0\lambda_4 & + & 0\lambda_5 \\
c_4 & = & 0\lambda_1 & + & 0\lambda_2 & + & 0\lambda_3 & + & -1\lambda_4 & + & 1\lambda_5 \\
1 & \leq & 1\lambda_1 & + & 1\lambda_2 & + & -1\lambda_3 & + & 1\lambda_4 & + & 1\lambda_5 \\
c_1 & = & -1c_3 & \wedge & \lambda_1 \geq 0 & \wedge & \lambda_2 \geq 0 & \wedge & \lambda_3 \geq 0 & & \\
c_2 & = & -1c_4 & \wedge & \lambda_4 \geq 0 & \wedge & \lambda_5 \geq 0 & & & &
\end{array}
$$

$\psi \triangleq$

Farkas' lem

$\lambda_1, \ldots, \lambda_5 \geq$

$$c_1 = \sum_{i=1}^{5} \lambda_i a_{i,1} \quad \wedge \cdots \wedge \quad c_4 = \sum_{i=1}^{5} \lambda_i a_{i,4} \quad \wedge \quad 1 \leq \left(\sum_{i=0}^{5} \lambda_i b_i\right)$$

Rank function synthesis

Satisfying assignment:

$$\begin{array}{lcllcl} c_1 & = & 1 & c_2 & = & 0 \\ c_3 & = & -1 & c_4 & = & 0 \\ \lambda_1 & = & 0 & \lambda_2 & = & 1 \\ \lambda_3 & = & 0 & \lambda_4 & = & 0 \\ \lambda_5 & = & 0 & & & \end{array}$$

$$R \triangleq \begin{array}{ccccccccc} 0x' & + & 0y' & + & -1x & & & & \\ 1x' & + & 0y' & + & -1x & & & & \\ -1x' & + & 0y' & + & 1x & & & & 0 \\ 0x' & + & 0y' & + & 0x & + & & \leq & 0 \\ 0x' & + & -1y' & + & 0x & + & & 1 & \leq 0 \end{array}$$

$$\begin{array}{lclclclclcl} c_1 & = & 0\lambda_1 & + & 1\lambda_2 & + & -1\lambda_3 & + & 0\lambda_4 & + & 0\lambda_5 \\ c_2 & = & 0\lambda_1 & + & 0\lambda_2 & + & 0\lambda_3 & + & 0\lambda_4 & + & -1\lambda_5 \\ c_3 & = & -1\lambda_1 & + & -1\lambda_2 & + & 1\lambda_3 & + & 0\lambda_4 & + & 0\lambda_5 \\ c_4 & = & 0\lambda_1 & + & 0\lambda_2 & + & 0\lambda_3 & + & -1\lambda_4 & + & 1\lambda_5 \\ 1 & \leq & 1\lambda_1 & + & 1\lambda_2 & + & -1\lambda_3 & + & 1\lambda_4 & + & 1\lambda_5 \\ c_1 & = & -1c_3 & \wedge & \lambda_1 \geq 0 & \wedge & \lambda_2 \geq 0 & \wedge & \lambda_3 \geq 0 & & \\ c_2 & = & -1c_4 & \wedge & \lambda_4 \geq 0 & \wedge & \lambda_5 \geq 0 & & & & \end{array}$$

$\psi \triangleq$

Farkas' lemma

$\lambda_1, \ldots, \lambda_5 \geq$

$$c_1 = \sum_{i=1}^{5} \lambda_i a_{i,1} \quad \wedge \cdots \wedge \quad c_4 = \sum_{i=1}^{5} \lambda_i a_{i,4} \quad \wedge \quad 1 \leq \left(\sum_{i=0}^{5} \lambda_i b_i\right)$$

Rank function synthesis

Satisfying assignment:

$$
\begin{array}{llllll}
c_1 & = & 1 & c_2 & = & 0 \\
c_3 & = & -1 & c_4 & = & 0 \\
\lambda_1 & = & 0 & \lambda_2 & = & 1 \\
\lambda_3 & = & 0 & \lambda_4 & = & 0 \\
\lambda_5 & = & 0 & & &
\end{array}
$$

$$
R \triangleq \begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & & & & & & \\
1x' & + & 0y' & + & -1x & & & & & & \\
-1x' & + & 0y' & + & 1x & & & & & & 0 \\
0x' & + & 0y' & + & 0x & + & & & & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & y & + & 1 & \leq & 0
\end{array}
$$

$$\Longrightarrow$$

$$\psi \triangleq c_1 x' + c_2 y' + c_3 x + c_4 y + 1 \leq 0$$

Farkas' lemma. $R \Rightarrow \psi$ *iff* there exist real multipliers $\lambda_1, \ldots, \lambda_5 \geq 0$ such that

$$c_1 = \sum_{i=1}^{5} \lambda_i a_{i,1} \quad \wedge \cdots \wedge \quad c_4 = \sum_{i=1}^{5} \lambda_i a_{i,4} \quad \wedge \quad 1 \leq (\sum_{i=0}^{5} \lambda_i b_i)$$

Rank f

$$
\begin{array}{rcccc}
f(a,b) & \triangleq & c_1 a & + & c_2 b \\
-f(a,b) & \triangleq & c_3 b & + & c_4 b \\
c_1 & = & -1 c_3 & & \\
c_2 & = & -1 c_4 & &
\end{array}
$$

Satisfying assignment:

$$
\begin{array}{ccccccc}
c_1 & = & 1 & & c_2 & = & 0 \\
c_3 & = & -1 & & c_4 & = & 0 \\
\lambda_1 & = & 0 & & \lambda_2 & = & 1 \\
\lambda_3 & = & 0 & & \lambda_4 & = & 0 \\
\lambda_5 & = & 0 & & & &
\end{array}
$$

$$
\begin{array}{ccccccc}
0x & + & & & & \leq & 0 \\
+ \; 0x & & 1y & + & 1 & \leq & 0
\end{array}
$$

$$\Rightarrow$$

$$\psi \;\triangleq\; c_1 x' \;+\; c_2 y' \;+\; c_3 x \;+\; c_4 y \;+\; 1 \;\leq\; 0$$

Farkas' lemma. $R \Rightarrow \psi$ *iff* there exist real multipliers $\lambda_1, \ldots, \lambda_5 \geq 0$ such that

$$c_1 = \sum_{i=1}^{5} \lambda_i a_{i,1} \quad \wedge \cdots \wedge \quad c_4 = \sum_{i=1}^{5} \lambda_i a_{i,4} \quad \wedge \quad 1 \leq \left(\sum_{i=0}^{5} \lambda_i b_i\right)$$

Rank f...

$$
\begin{array}{rcccc}
f(a,b) & \triangleq & c_1 a & + & c_2 b \\
-f(a,b) & \triangleq & c_3 b & + & c_4 b \\
c_1 & = & -1 c_3 & & \\
c_2 & = & -1 c_4 & &
\end{array}
$$

Satisfying assignment:

$$
\boxed{\begin{array}{lllllll}
c_1 & = & 1 & \quad & c_2 & = & 0 \\
c_3 & = & -1 & & c_4 & = & 0
\end{array}}
$$

$$
\begin{array}{lllllll}
\lambda_1 & = & 0 & \quad & \lambda_2 & = & 1 \\
\lambda_3 & = & 0 & & \lambda_4 & = & 0 \\
\lambda_5 & = & 0 & & & &
\end{array}
$$

$$0x \quad + \quad -1y \qquad \leq \quad 0$$

$$+ \quad 0x \qquad 1y \quad + \quad 1 \quad \leq \quad 0$$

$$\Rightarrow$$

$f(x,y) \triangleq 1x + 0y$

$-f(x,y) \triangleq -1x + 0y$

$$\psi \quad \triangleq \quad c_1 x' \quad + \quad c_2 y' \quad + \quad c_3 x \quad + \quad c_4 y \quad + \quad 1 \quad \leq \quad 0$$

Farkas' lemma. $R \Rightarrow \psi$ *iff* there exist real multipliers $\lambda_1, \ldots, \lambda_5 \geq 0$ such that

$$c_1 = \sum_{i=1}^{5} \lambda_i a_{i,1} \quad \wedge \cdots \wedge \quad c_4 = \sum_{i=1}^{5} \lambda_i a_{i,4} \quad \wedge \quad 1 \leq \left(\sum_{i=0}^{5} \lambda_i b_i\right)$$

Rank function synthesis

$$R \triangleq \begin{array}{ccccccccccc} 0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ 1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ -1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\ 0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\ 0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0 \end{array}$$

$$\Rightarrow$$

$f(x,y) \triangleq 1x + 0y$

$-f(x,y) \triangleq -1x + 0y$

$$\psi \triangleq c_1x' + c_2y' + c_3x + c_4y + 1 \leq 0$$

Rank function synthesis

$$R \triangleq \begin{array}{rcrcrcrcrcc} 0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ 1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ -1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\ 0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\ 0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0 \end{array}$$

$$\Rightarrow$$

$f(x,y) \triangleq 1x + 0y$

$-f(x,y) \triangleq -1x + 0y$

$$\begin{array}{rcrcrcc} f(x',y') & + & -f(x,y) & + & 1 & \leq & 0 \\ & & -f(x',y') & + & b & \leq & 0 \end{array}$$

Rank function synthesis

$$
R \triangleq \begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0
\end{array}
$$

$$\Rightarrow$$

$f(x,y) \triangleq 1x + 0y$

$-f(x,y) \triangleq -1x + 0y$

$b = -1$

$$
\begin{array}{ccccccc}
f(x', y') & + & -f(x, y) & + & 1 & \leq & 0 \\
 & & -f(x', y') & + & b & \leq & 0
\end{array}
$$

Rank function synthesis

$$
R \triangleq \begin{array}{ccccccccccc}
0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\
-1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\
0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\
0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0
\end{array}
$$

$$\Rightarrow$$

$f(x,y) \triangleq 1x + 0y$

$-f(x,y) \triangleq -1x + 0y$

$b = -1$

$$
\begin{array}{ccccccc}
x' & + & -x & + & 1 & \leq & 0 \\
 & & -x' & + & -1 & \leq & 0
\end{array}
$$

Rank function synthesis

$$R \triangleq \begin{array}{rcrcrcrcrcr} 0x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ 1x' & + & 0y' & + & -1x & + & 0y & + & 1 & \leq & 0 \\ -1x' & + & 0y' & + & 1x & + & 0y & + & -1 & \leq & 0 \\ 0x' & + & 0y' & + & 0x & + & -1y & + & 1 & \leq & 0 \\ 0x' & + & -1y' & + & 0x & + & 1y & + & 1 & \leq & 0 \end{array}$$

$$\subseteq$$

$$\unrhd_{x,0}$$

Rank function synthesis

$$0x' \quad + \quad 0y' \quad + \quad -1x \quad + \quad 0y \quad + \quad 1 \quad \leq \quad 0$$

$$R \triangleq$$

Cygwin

```
$ cat input.txt
relation( from(X,Y)
        , to(Xp,Yp)
        , constraint( [ X>0
                      , Xp=X-1
                      , Y>0
                      , Yp>Y
                      ])
        , dump('output.txt')
        ).
$ rankfinder -extrarank input.txt -primed
RankFinder: Synthesis of linear ranking functions.
Computing primed boundedness constraint rx' >= d_0
Ranking          r   =    [1,0]
Bounded by       d0  =    0
Min decrease     d   =    1

$ _
```

Rank function synthesis

$$0x' \quad + \quad 0y' \quad + \quad -1x \quad + \quad 0y \quad + \quad 1 \quad \le \quad 0$$

$R \triangleq$

Cygwin

```
$ cat input.txt
relation( from(X,Y)
        , to(Xp,Yp)
        , constraint( [ X>0
                      , Xp=X-1
                      , Y>0
                      , Yp>Y
                      ])
        , dump('output.txt')
        ).
$ rankfinder -extrarank input.txt -primed
RankFinder: Synthesis of linear ranking functions.
Computing primed boundedness constraint rx' >= d 0
Ranking          r  =    [1,0]
Bounded by       d0 =    0
Min decrease     d  =    1

$ _
```

Xp is x'

R

ranking function

bound

goes down by 1

(fixed in our formulation)

Rank function synthesis

→ Question: can we automatically synthesize *f*s if we limit their form?

- Linear ranking functions from linear convex relations: Yes, *always!*
- Linear ranking functions from linear non-convex relations: *Yes, sometimes……*
- Linear ranking functions from non-linear convex relations: *Yes, sometimes…..*
- Linear ranking functions with invariants from convex relations: *Yes, always…..*
- Non-linear ranking functions from non-linear convex relations: *Yes, sometimes…..*
- ………….

Linear ranking functions

- Not all WF linear relations have linear ranking functions

- Example 1: $R \triangleq \mathsf{x} \geq 0 \wedge \mathsf{x}' = -2\mathsf{x} + 10$
  - No linear f exists s.t. $R \subseteq \trianglerighteq_f$
  - $R^+ \subseteq \trianglerighteq_{\mathsf{x},0} \cup \trianglerighteq_{(-\mathsf{x},-10)}$

- Example 2: $R \triangleq \mathsf{x} > 0 \wedge \mathsf{x}' = \mathsf{x} - \mathsf{y} \wedge \mathsf{y}' = \mathsf{y} + 1$
  - No linear f exists s.t. $R \subseteq \trianglerighteq_f$
  - $R^+ \subseteq \trianglerighteq_{\mathsf{x},0} \cup \trianglerighteq_{(-\mathsf{y},0)}$

- Other examples: Ackermann's function and most programs with complex nested loops

Today

- → Introduction
- → Well-founded relations and ranking functions
- → Disjunctive well foundedness
- → Decomposition
- → Notes on rank function synthesis