

# Static Analysis and Verification in Databases

Victor Vianu  
U.C. San Diego

# What is it?

Reasoning about queries and applications to guarantee

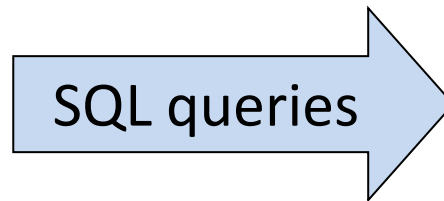
correctness

good performance

# Important to experts ...



Expert user



Database Server

# ... but also to the public at large

- Applications built on top of a database

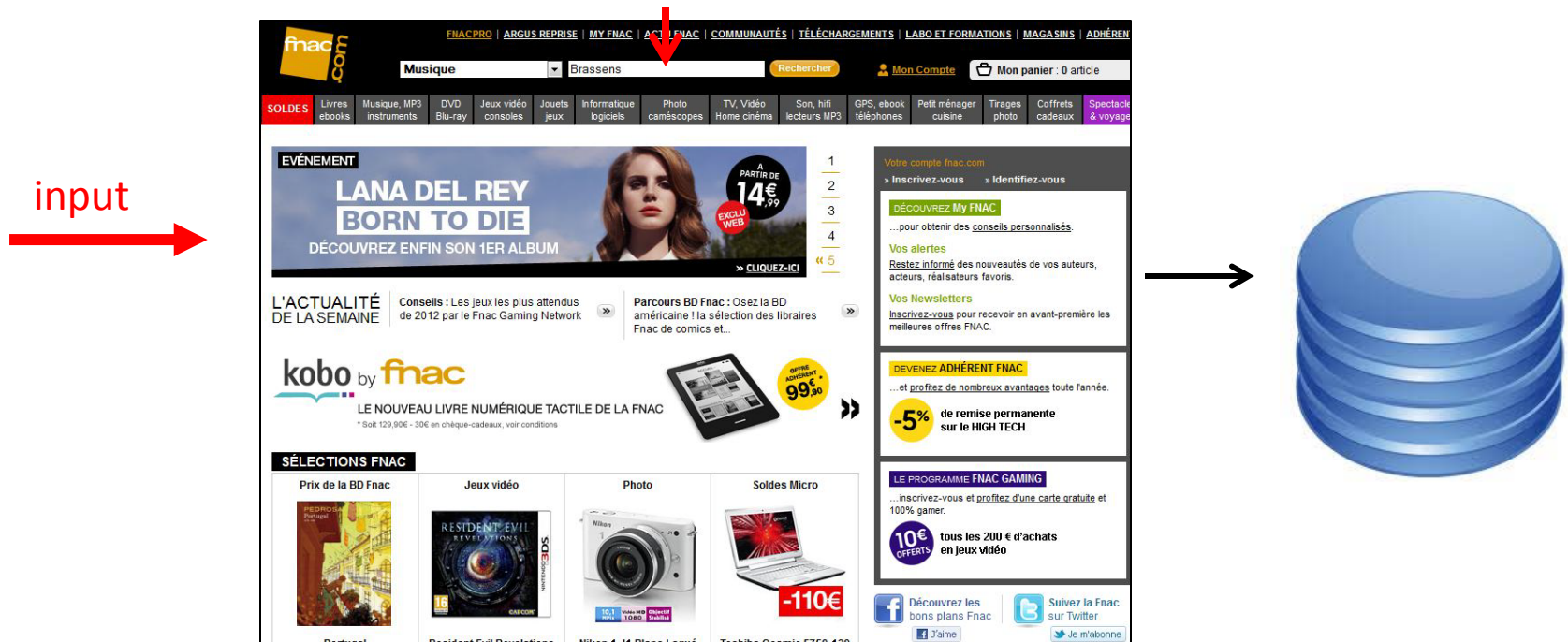
Web sites: **FNAC**, Amazon, SNCF, Opendo, Facebook,...

The screenshot displays the FNAC.com website interface. At the top, there is a navigation bar with the FNAC logo and a search bar containing the word "Musique". Below the search bar, a horizontal menu lists various product categories: Livres ebooks, Musique, MP3 instruments, DVD Blu-ray, Jeux vidéo consoles, Jouets jeux, Informatique logiciels, Photo caméscopes, TV, Vidéo Home cinéma, Son, hifi lecteurs MP3, GPS, ebook téléphones, Petit ménage cuisine, Tirages photo, Coffrets cadeaux, and Spectacle & voyage. The main content area features a large banner for Lana Del Rey's album "Born to Die", priced at 14€ (part of a 14.99€ offer). Below this, there are sections for "L'ACTUALITÉ DE LA SEMAINE" with gaming news, "kobo by fnac" promoting digital books, and "SÉLECTIONS FNAC" with sub-sections for "Prix de la BD Fnac", "Jeux vidéo" (featuring Resident Evil Revelations), "Photo" (featuring a Nikon camera), and "Soldes Micro" (featuring a Toshiba laptop with a -110€ discount). On the right side, a sidebar contains a "Votre compte fnac.com" section with links for registration and identification, a "DÉCOUVREZ My FNAC" section for personalized advice, "Vos alertes" for author updates, "Vos Newsletters" for offers, and a "DEVENEZ ADHÉRENT FNAC" section offering a 5% permanent discount on high-tech items. At the bottom of the sidebar, there is a "LE PROGRAMME FNAC GAMING" section offering 10€ off on video game purchases over 200€. Social media links for Facebook and Twitter are also present at the bottom.

# ... but also to the public at large

- Applications built on top of a database

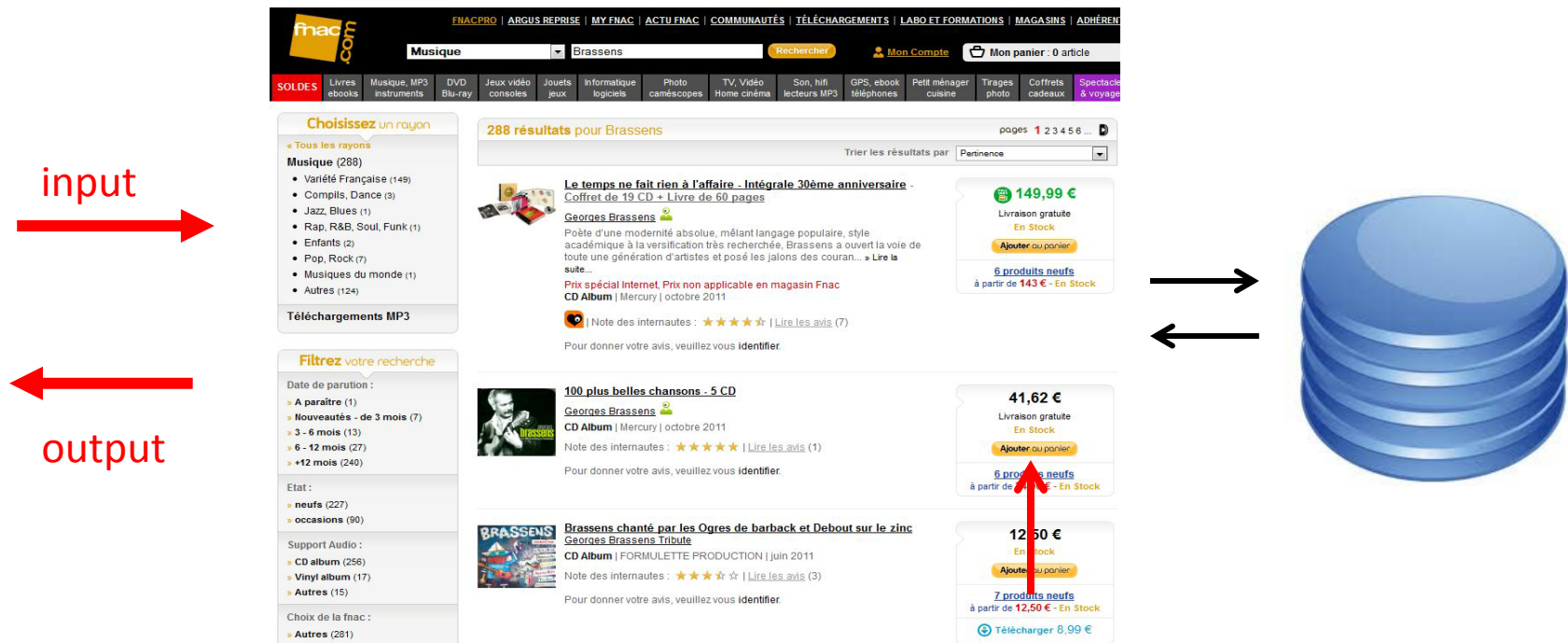
Web sites: **FNAC, Amazon, SNCF, Opendo, Facebook,...**



# ... but also to the public at large

- Applications built on top of a database

Web sites: **FNAC, Amazon, SNCF, Opendo, Facebook,...**



# ... but also to the public at large

- Applications built on top of a database

Web sites: **FNAC, Amazon, SNCF, Opodo, Facebook,...**

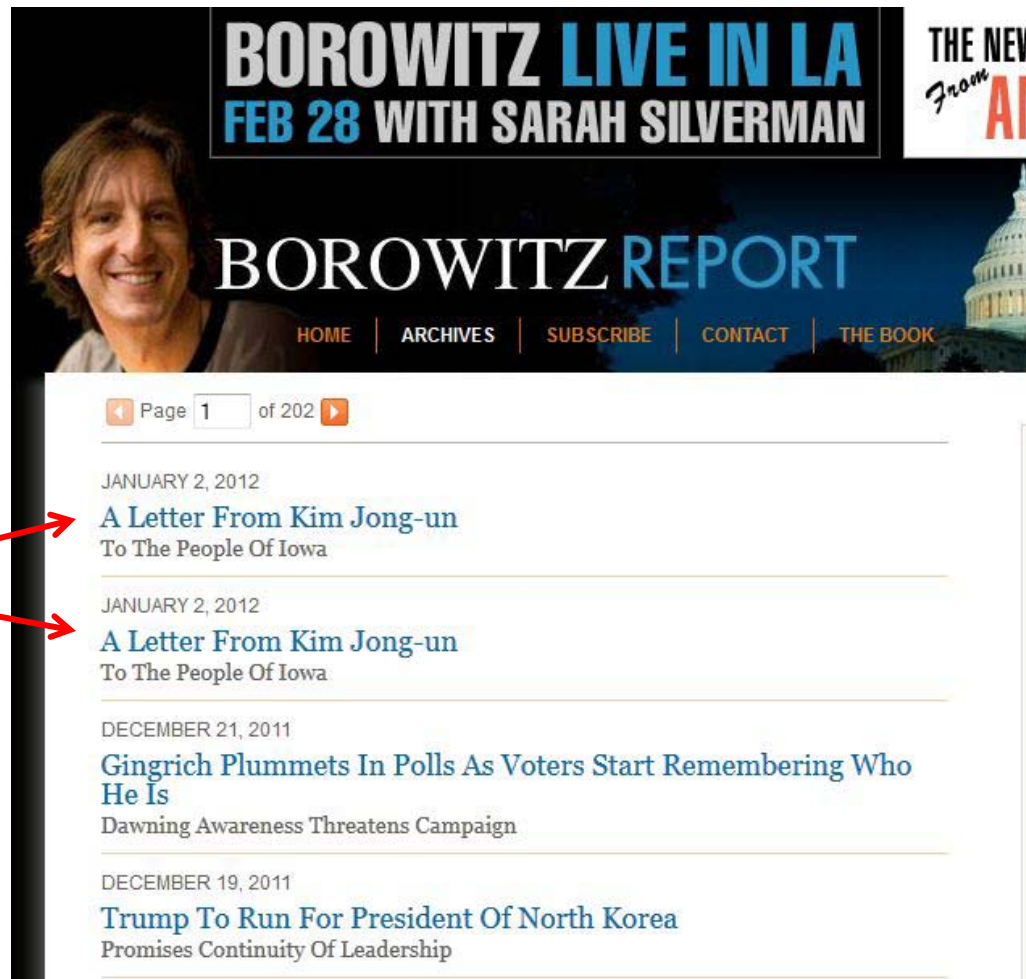
← output

The screenshot displays the FNAC.com website interface. At the top, there is a navigation bar with the FNAC logo and various menu items like 'Tous produits', 'Rechercher', 'Mon Compte', and 'Mon panier : 1 article'. Below this is a category bar with options such as 'SOLDES', 'Livres ebooks', 'Musique, MP3 instruments', 'DVD Blu-ray', 'Jeux vidéo consoles', 'Jouets jeux', 'Informatique logiciels', 'Photo caméscopes', 'TV Vidéo Home cinéma', 'Son, hifi lecteurs MP3', 'GPS, ebook téléphones', 'Petit ménage cuisine', 'Tirages photo', 'Coffrets cadeaux', and 'Spectacles & voyages'. The main content area is divided into several sections: 'Nous vous recommandons aussi :', 'Meilleures ventes Disques :', 'Continuez vos achats', and 'Votre panier'. The 'Meilleures ventes Disques' section features three album covers: Adele's '21' (10,99 €), Lana Del Rey's 'Born to die - Edition limitée' (16,99 €), and Leonard Cohen's 'Old ideas' (15,99 €). The 'Continuez vos achats' section lists various music collections and gift sets. The 'Votre panier' section shows a total of 41,62 € and a 'Passez la commande' button. A 'Votre sélection' section is also present, indicating that the selection is currently empty. At the bottom, there is a footer with the text 'Les + de Fnac.com', ' Paiement sécurisé + Suivi de commande + Satisfait ou remboursé', and contact information.



# Wide array of bugs

- Mildly annoying: duplicate news items





# Wide array of bugs

- Mildly annoying: duplicate news items

Mise à jour à 00h25 - Paris

# Le Monde.fr



Abonnez-vous au Monde à partir de 15 € / mois

Recherchez sur Le Monde.fr



Recevez les newsletters gratuites

S'identifier >

Le Monde.fr

Édu, santé, organisations,



ACTUALITÉS

ÉCONOMIE

SPORT

CULTURE

IDÉES

ÉDUCATION

M MAGAZINE

PRATIQUE

JOURNAL

ÉDITION ABONNÉS

S'abonner au Monde - 15 € / mois

▼ PUBLICITE

## "Ce qui devait être fait a été fait par le gouvernement"



Dans un discours résolument axé sur l'emploi et le contexte économique morose, Nicolas Sarkozy a présenté les derniers vœux de son quinquennat.

- Pour 2012, des vœux résolument politiques
-  Vœux : Sarkozy veut anticiper le volet emploi de son programme présidentiel
- Hollande adresse ses vœux par téléphone et promet "le changement"
- La fête de la Saint-Sylvestre ne sera pas "gâchée par des trublions"

### En continu

- 22:23 Face à la crise, Nicolas Sarkozy donne la priorité à l'emploi REUTERS
- 21:28 Face à la crise, Nicolas Sarkozy donne la priorité à l'emploi REUTERS
- 20:43 "Ce qui devait être fait a été fait par le gouvernement" LEMONDE.FR
- 20:21 Nicolas Sarkozy écarte un nouveau plan de rigueur REUTERS
- 19:54 Deux-tiers des Français contre un abandon de l'euro LEMONDE.FR

► L'actu en continu sur [Facebook](#), [Twitter](#) et [Mobile](#)

▼ PUBLICITE

# Wide array of bugs

- Possible reason: a query returns duplicates

Mise à jour à 00h25 - Paris

# Le Monde.fr



Abonnez-vous au Monde à partir de 15 € / mois

Recherchez sur Le Monde.fr

Recevez les newsletters gratuites

S'identifier >

Le Monde.fr

Eau, santé, organisations,



ACTUALITÉS

ÉCONOMIE

SPORT

CULTURE

IDÉES

ÉDUCATION

M MAGAZINE

PRATIQUE

JOURNAL

ÉDITION ABONNÉS

S'abonner au Monde - 15 € / mois

▼ PUBLICITE

## "Ce qui devait être fait a été fait par le gouvernement"



Dans un discours résolument axé sur l'emploi et le contexte économique morose, Nicolas Sarkozy a présenté les derniers vœux de son quinquennat.

- Pour 2012, des vœux résolument politiques
-  Vœux : Sarkozy veut anticiper le volet emploi de son programme présidentiel
- Hollande adresse ses vœux par téléphone et promet "le changement"
- La fête de la Saint-Sylvestre ne sera pas "gâchée par des trublions"

### En continu

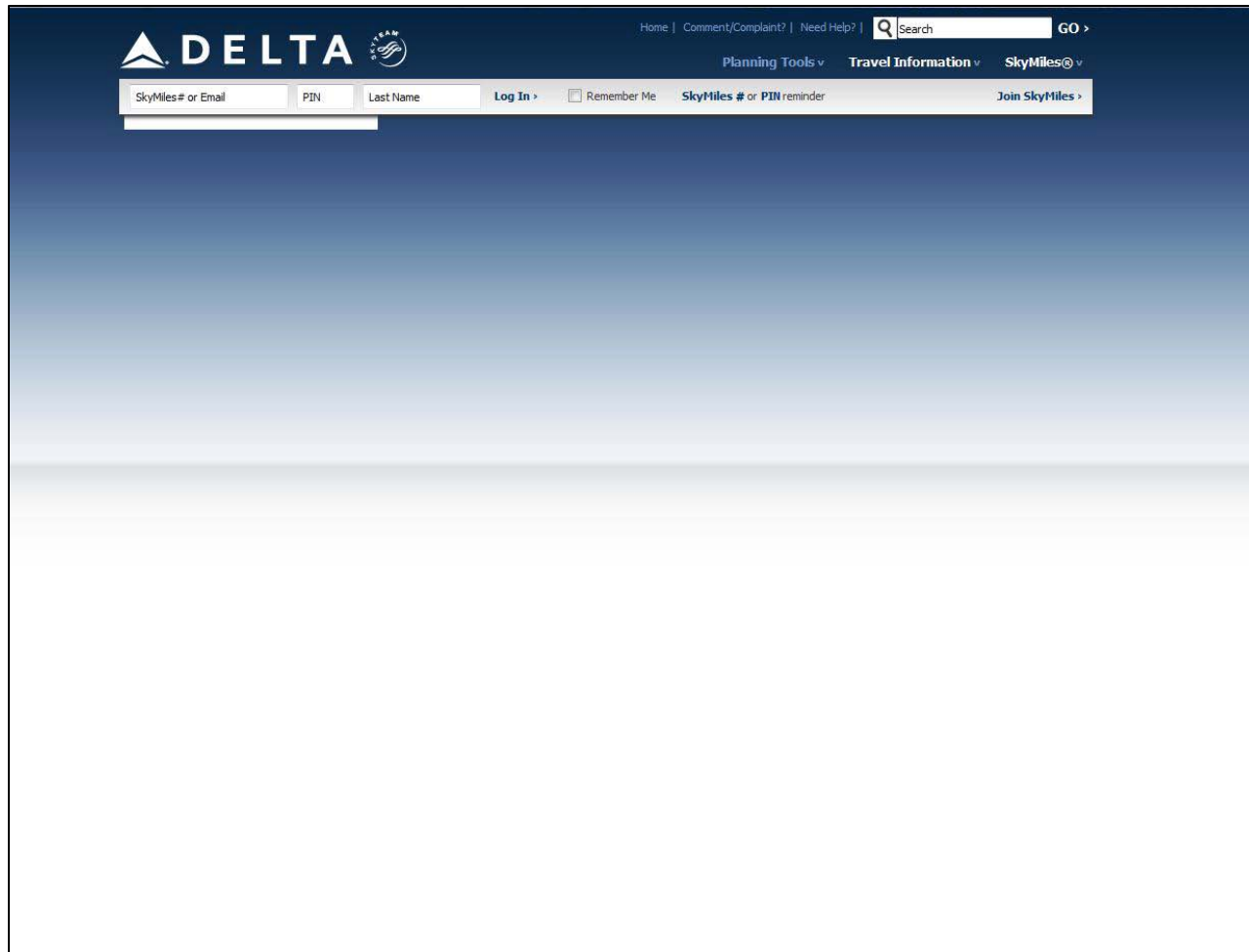
- 22:23 Face à la crise, Nicolas Sarkozy donne la priorité à l'emploi REUTERS
- 21:28 Face à la crise, Nicolas Sarkozy donne la priorité à l'emploi REUTERS
- 20:43 "Ce qui devait être fait a été fait par le gouvernement" LEMONDE.FR
- 20:21 Nicolas Sarkozy écarte un nouveau plan de rigueur REUTERS
- 19:54 Deux-tiers des Français contre un abandon de l'euro LEMONDE.FR

► L'actu en continu sur [Facebook](#), [Twitter](#) et [Mobile](#)

▼ PUBLICITE

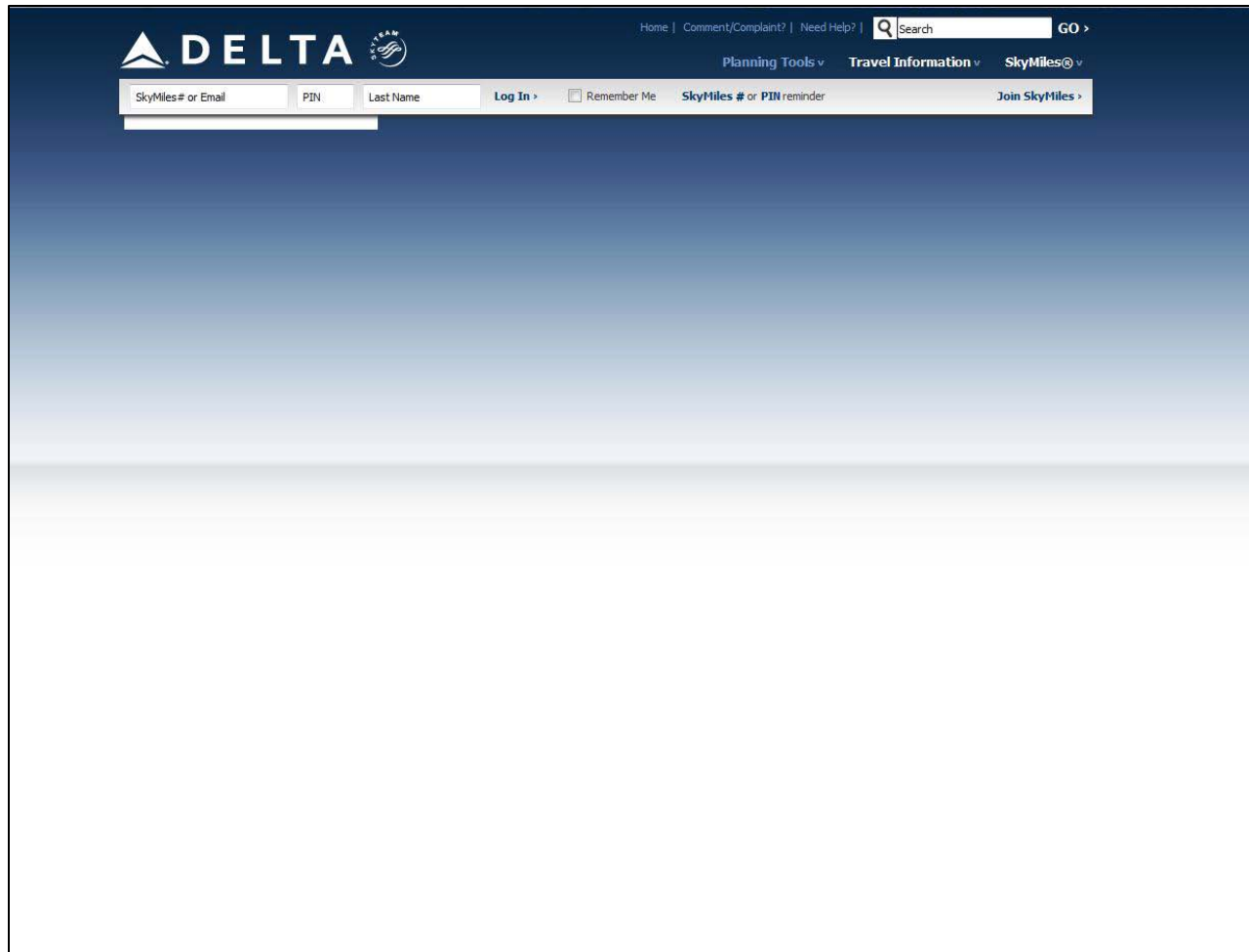
# Wide array of bugs

- Irritating: blank web page



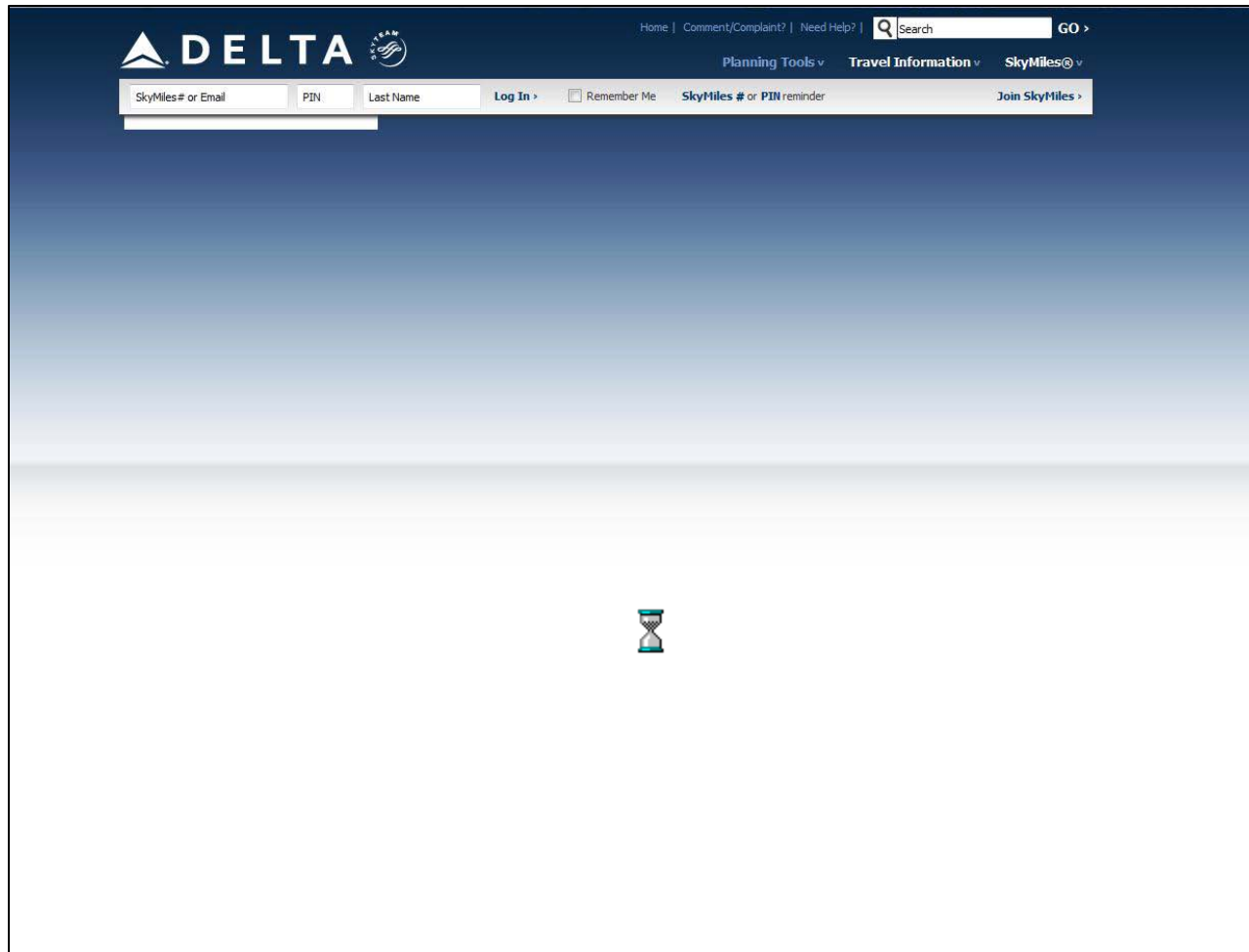
# Wide array of bugs

- Possible reason: a query returns empty answer



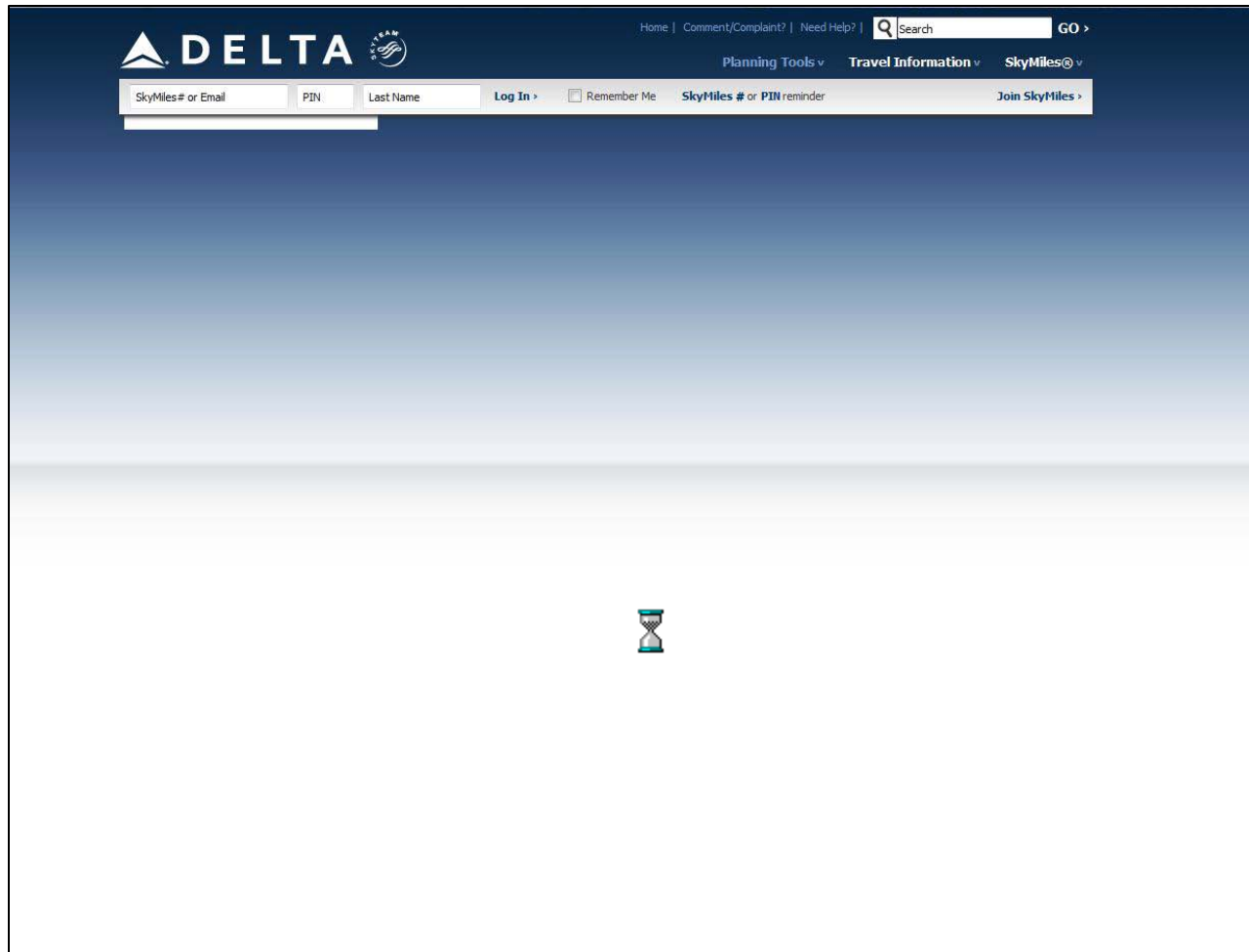
# Wide array of bugs

- Irritating: wait forever



# Wide array of bugs


- Possible reason: query processing is too slow



# Wide array of bugs

- Irritating: fail after long interaction

**RÉSERVEZ VOTRE BILLET DE TRAIN**

 Votre demande n'a pu aboutir. Veuillez la renouveler dans quelques instants.  
Pour plus d'informations, nos conseillers sont à votre disposition.  
Merci de votre compréhension.

Simplifiez vos réservations. [Connectez-vous](#) ou [Créez votre compte](#).

Précisez votre date retour et profitez de prix avantageux pour votre trajet Rome (Roma) - Moscou Oktiabrskaja (Moskva).

**- Où et quand souhaitez-vous partir ?**

Voyage \*  Aller Simple  Aller-Retour

Départ \*  Arrivée \*


Aller le \*  à partir de  Retour le  à partir de

Trajets directs uniquement ou trajet Via

# Wide array of bugs

- Possible reason: poorly designed workflow

**RÉSERVEZ VOTRE BILLET DE TRAIN**

 Votre demande n'a pu aboutir. Veuillez la renouveler dans quelques instants.  
Pour plus d'informations, nos conseillers sont à votre disposition.  
Merci de votre compréhension.

Simplifiez vos réservations. [Connectez-vous](#) ou [Créez votre compte](#).

Précisez votre date retour et profitez de prix avantageux pour votre trajet Rome (Roma) - Moscou Oktiabrskaja (Moskva).

**- Où et quand souhaitez-vous partir ?**

Voyage \*  Aller Simple  Aller-Retour

Départ \*  Arrivée \*

Aller le \*  à partir de  Retour le  à partir de

Trajets directs uniquement ou trajet Via



# Wide array of bugs

- Exhilarating/catastrophic: free ticket!

For a full list of Ryanair fees, please click [here](#)

### Going Out From Dublin - Cork

[« Previous Day](#) [Next Day »](#)

**Select A Flight**

<input checked="" type="radio"/>	Regular Fare	Adult	9.99 EUR	Sat , 21 Feb 09 Flight FR 9843	08:55 Depart 09:45 Arrive	<input checked="" type="radio"/> Going Out Regular Fare <b>Depart:</b> Dublin 08:55 <b>Arrive:</b> Cork 09:45 <b>Fare:</b> 0.00 EUR <b>Taxes / Fees:</b> 0.00 EUR <b>Total Price:</b> 0.00 EUR
<input type="radio"/>	Regular Fare	Adult	9.99 EUR	Sat , 21 Feb 09 Flight FR 9845	11:35 Depart 12:25 Arrive	
<input type="radio"/>	Regular Fare	Adult	9.99 EUR	Sat , 21 Feb 09 Flight FR 9857	14:00 Depart 14:50 Arrive	
<input type="radio"/>	Regular Fare	Adult	14.99 EUR	Sat , 21 Feb 09 Flight FR 9847	15:20 Depart 19:10 Arrive	
<input type="radio"/>	Regular Fare	Adult	9.99 EUR	Sat , 21 Feb 09 Flight FR 9849	20:50 Depart 21:40 Arrive	

### Coming Back From Cork - Dublin

[« Previous Day](#) [Next Day »](#)

**Select A Flight**

<input checked="" type="radio"/>	Regular Fare	Adult	0.99 EUR	Sun , 22 Feb 09 Flight FR 9844	10:10 Depart 11:00 Arrive	<input checked="" type="radio"/> Coming Back Regular Fare <b>Depart:</b> Cork 10:10 <b>Arrive:</b> Dublin 11:00 <b>Fare:</b> 0.00 EUR <b>Taxes / Fees:</b> 0.00 EUR <b>Total Price:</b> 0.00 EUR
<input type="radio"/>	Regular Fare	Adult	9.99 EUR	Sun , 22 Feb 09 Flight FR 9856	14:30 Depart 15:20 Arrive	
<input type="radio"/>	Regular Fare	Adult	9.99 EUR	Sun , 22 Feb 09 Flight FR 9846	17:05 Depart 17:55 Arrive	
<input type="radio"/>	Regular Fare	Adult	29.99 EUR	Sun , 22 Feb 09 Flight FR 9848	19:25 Depart 20:25 Arrive	

**Select Your Flights and Continue**  
If the flights you require are shown above, select them and click on "Select and Continue" to proceed.

**SELECT AND CONTINUE**

# Wide array of bugs


- Likely reason: flaw in workflow design

For a full list of Ryanair fees, please click [here](#)

### Going Out From Dublin - Cork

« Previous Day » Next Day »


**Select A Flight**

<input checked="" type="radio"/>	Regular Fare	Adult	9.99 EUR	Sat , 21 Feb 09 Flight FR 9843	08:55 Depart 09:45 Arrive	 Going Out Regular Fare <b>Depart:</b> Dublin 08:55 <b>Arrive:</b> Cork 09:45 <hr/> Fare: 0.00 EUR Taxes / Fees: 0.00 EUR Total Price: 0.00 EUR
<input type="radio"/>	Regular Fare	Adult	9.99 EUR	Sat , 21 Feb 09 Flight FR 9845	11:35 Depart 12:25 Arrive	
<input type="radio"/>	Regular Fare	Adult	9.99 EUR	Sat , 21 Feb 09 Flight FR 9857	14:00 Depart 14:50 Arrive	
<input type="radio"/>	Regular Fare	Adult	14.99 EUR	Sat , 21 Feb 09 Flight FR 9847	15:20 Depart 19:10 Arrive	
<input type="radio"/>	Regular Fare	Adult	9.99 EUR	Sat , 21 Feb 09 Flight FR 9849	20:50 Depart 21:40 Arrive	

### Coming Back From Cork - Dublin

« Previous Day » Next Day »

**Select A Flight**

<input checked="" type="radio"/>	Regular Fare	Adult	0.99 EUR	Sun , 22 Feb 09 Flight FR 9844	10:10 Depart 11:00 Arrive	 Coming Back Regular Fare <b>Depart:</b> Cork 10:10 <b>Arrive:</b> Dublin 11:00 <hr/> Fare: 0.00 EUR Taxes / Fees: 0.00 EUR Total Price: 0.00 EUR
<input type="radio"/>	Regular Fare	Adult	9.99 EUR	Sun , 22 Feb 09 Flight FR 9856	14:30 Depart 15:20 Arrive	
<input type="radio"/>	Regular Fare	Adult	9.99 EUR	Sun , 22 Feb 09 Flight FR 9846	17:05 Depart 17:55 Arrive	
<input type="radio"/>	Regular Fare	Adult	29.99 EUR	Sun , 22 Feb 09 Flight FR 9848	19:25 Depart 20:25 Arrive	

**Select Your Flights and Continue**  
If the flights you require are shown above, select them and click on "Select and Continue" to proceed.

**SELECT AND CONTINUE**

# How can static analysis and verification help?

**Static analysis**

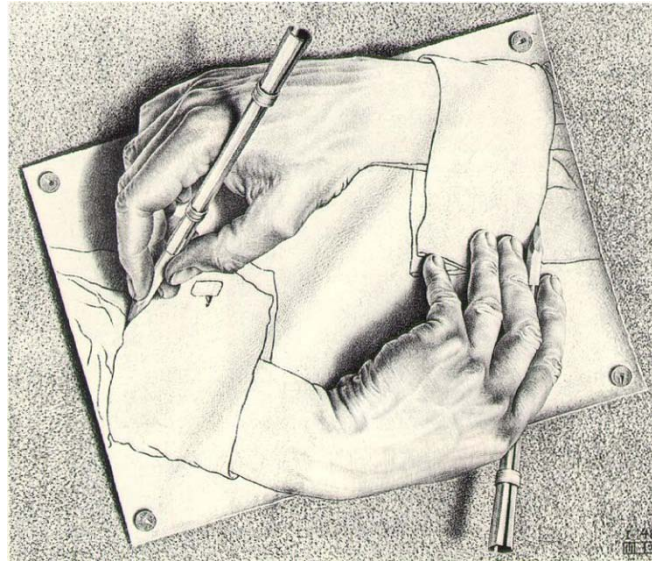
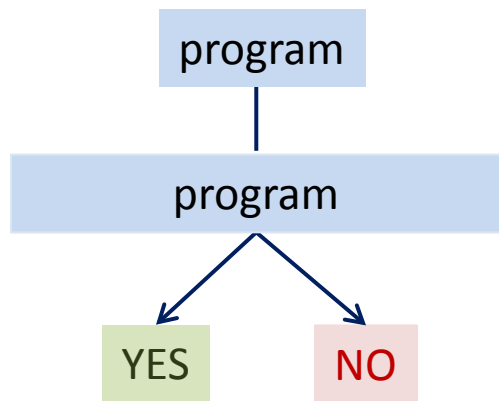
reasoning about queries

**Verification**

reasoning about workflow

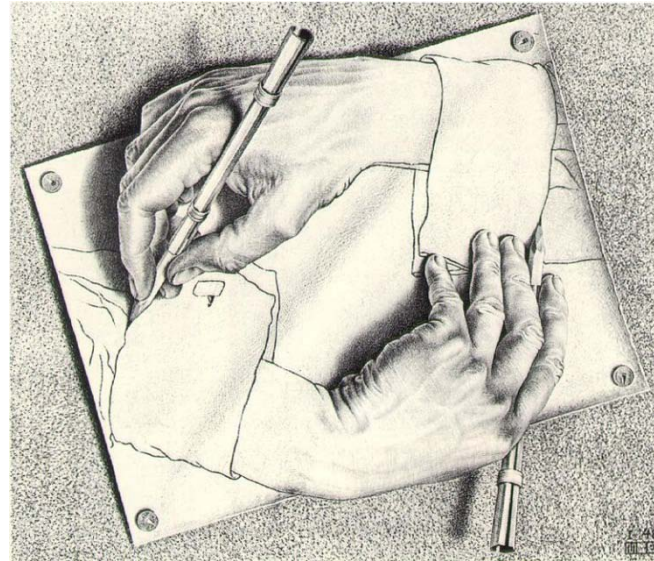
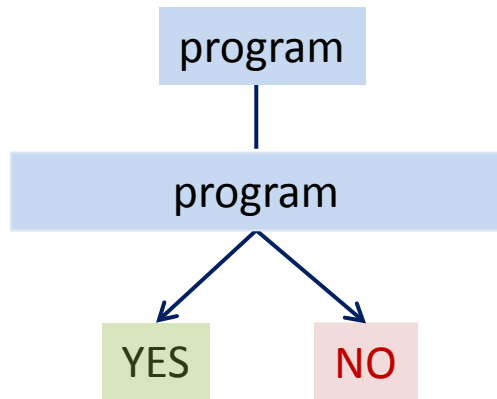
# Static analysis

- Query: “reasoning” about data
- Static analysis: “reasoning” about the “reasoner”



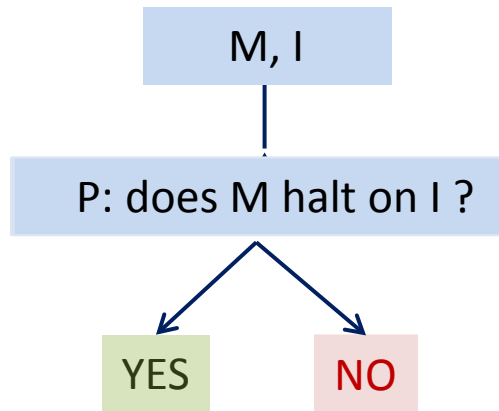
# Static analysis

- Self-reference: source of undecidability



# Static analysis

- Self-reference: source of undecidability



*Well, the truth is that  $P$  cannot possibly be, because if you wrote it and gave it to me, I could use it to set up a logical bind that would shatter your reason and scramble your mind.*

.....

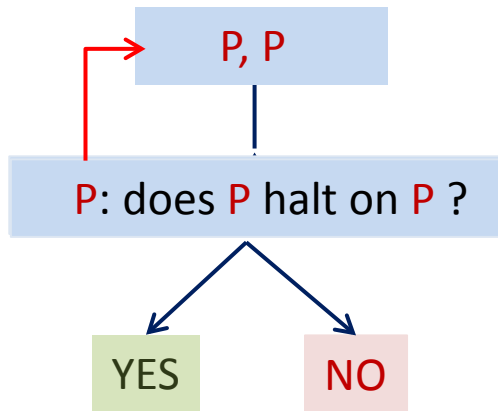
*You can never find general mechanical means for predicting the acts of computing machines; it's something that cannot be done. So we users must find our own bugs. Our computers are losers!*

Geoffrey K. Pullum, University of Edinburgh



# Static analysis

- Self-reference: source of undecidability

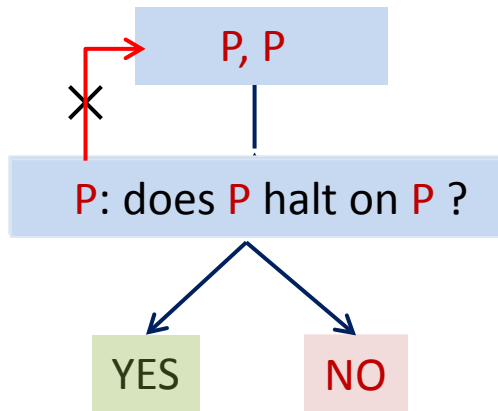


Flavor of the paradox

“This sentence is false”

# Static analysis

- Self-reference: source of undecidability



Is this really relevant to SQL ?



# Static analysis

“Simple”, fundamental question:  
Is the answer to Q always empty ?

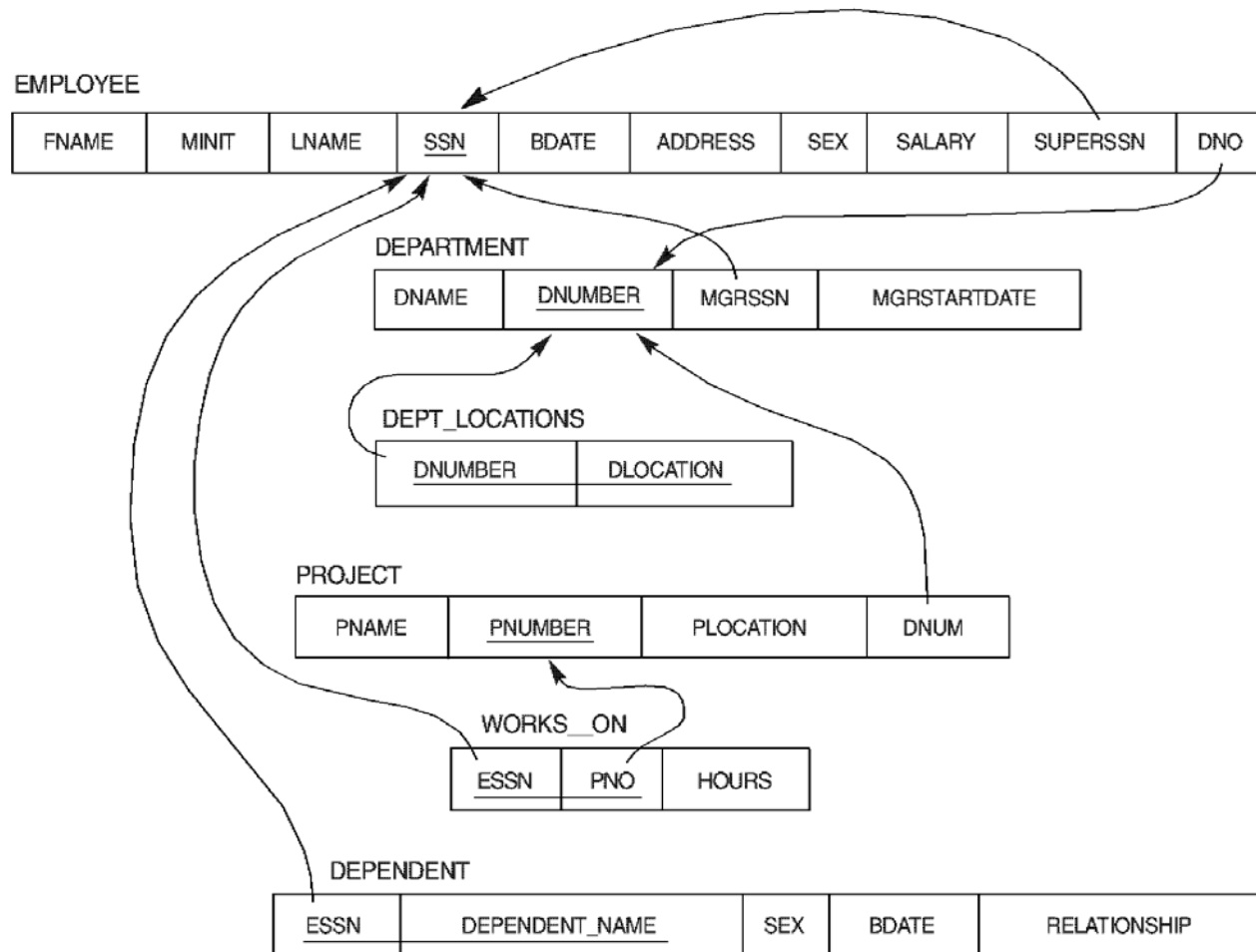
```
select title
from Schedule
where theater = 'Les Halles'
      and theater = 'Odeon'
```

'Les Halles' = 'Odeon'



Schedule	title	theater	time
----------	-------	---------	------

# Static analysis



# Static analysis

```
select PROJECT.PNAME, EMPLOYEE.LNAME  
from PROJECT, EMPLOYEE, WORKS_ON  
where PROJECT.PNUMBER = WORKS_ON.PNO  
       and WORKS_ON.ESSN = EMPLOYEE.SSN and  
       not exists  
       (select * from DEPARTMENT, EMPLOYEE  
        where PROJECT.DNUM = DNUMBER or MGRSSN = SSN)
```

Always empty?

# Static analysis

Surprise:

The Halting problem can be reduced to the SQL query emptiness problem!



M halts on I  
iff  
 $Q_{M,I}(DB) \neq \emptyset$  for some database DB

# Static analysis

Surprise:

The Halting problem can be reduced to the SQL query emptiness problem!

SQL query emptiness is undecidable

# Static analysis

## Also undecidable:

- Are two queries P and Q equivalent?
- Can Q be simplified (relative to various criteria)
- Does query Q ever return duplicate tuples?

Any non-trivial property!

Is there a class of **simpler but useful** SQL queries amenable to static analysis?

# Well-behaved case: Conjunctive Queries

select ... from ... where...

conjunction of equalities  
on attributes and constants



```
select theater
from Movie, Schedule
where director = 'Godard' and
      Movie.title = Schedule.title
```

Movie	title	director	actor
-------	-------	----------	-------

Schedule	title	theater	time
----------	-------	---------	------

# Well-behaved case: Conjunctive Queries

- Query emptiness: easy to check

```
select title  
from Schedule  
where theater = 'Les Halles'  
       and theater = 'Odeon'
```



'Les Halles' = 'Odeon'



# Well-behaved case: Conjunctive Queries

- Useful fact: if non-empty, can represent intuitively as a simple pattern of tuples using variables and constants

```
select theater
from Movie, Schedule
where director = 'Godard' and
      Movie.title = Schedule.title
```

Movie	title	director	actor
	t	Godard	

Schedule	title	theater	time
	t	a	

Answer	theater
	a

← Query result

# Well-behaved case: Conjunctive Queries

- Unsettling thought: **this query is a database!**

Can I apply a query to a query ?

Movie	title	director	actor
	t	Godard	

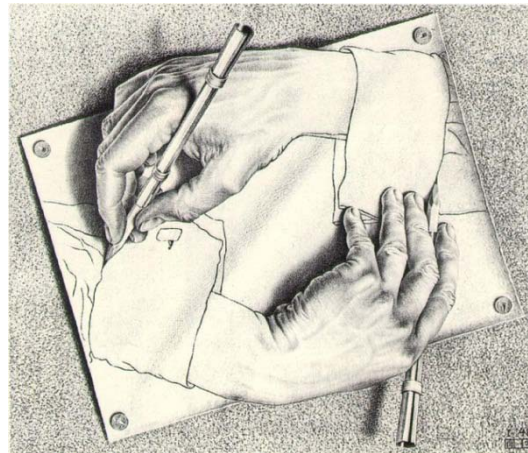
Schedule	title	theater	time
	t	a	

Answer	theater
	a

# Well-behaved case: Conjunctive Queries

- Unsettling thought: **this query is a database!**

Can I apply a query to a query ?

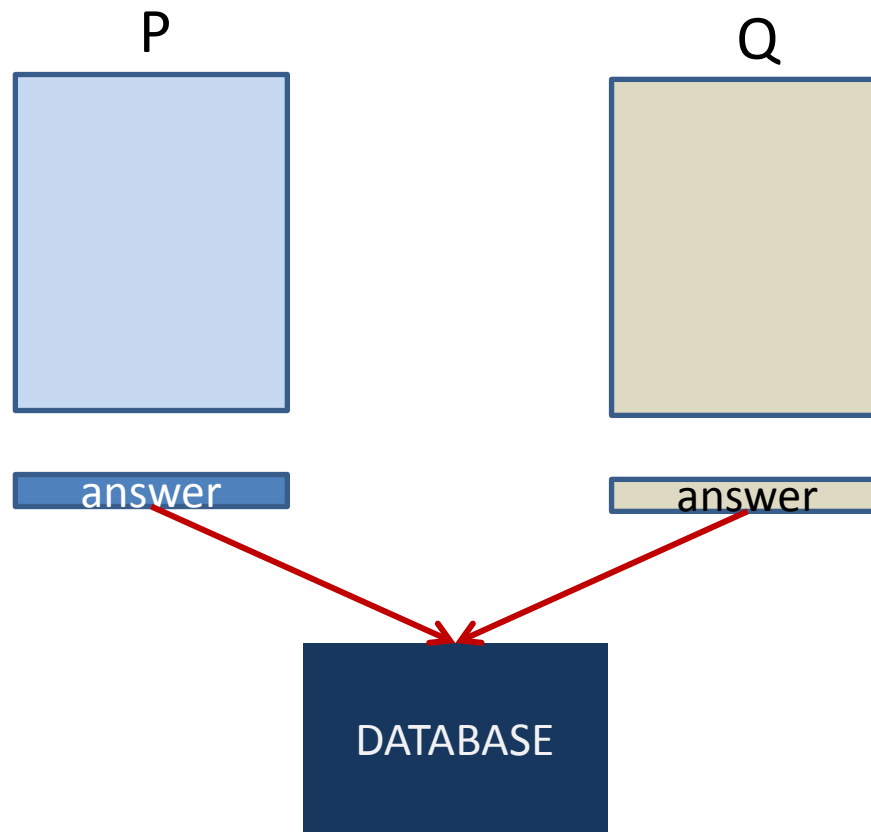


# Well-behaved case: Conjunctive Queries

- Good news: **powerful tool for static analysis!**

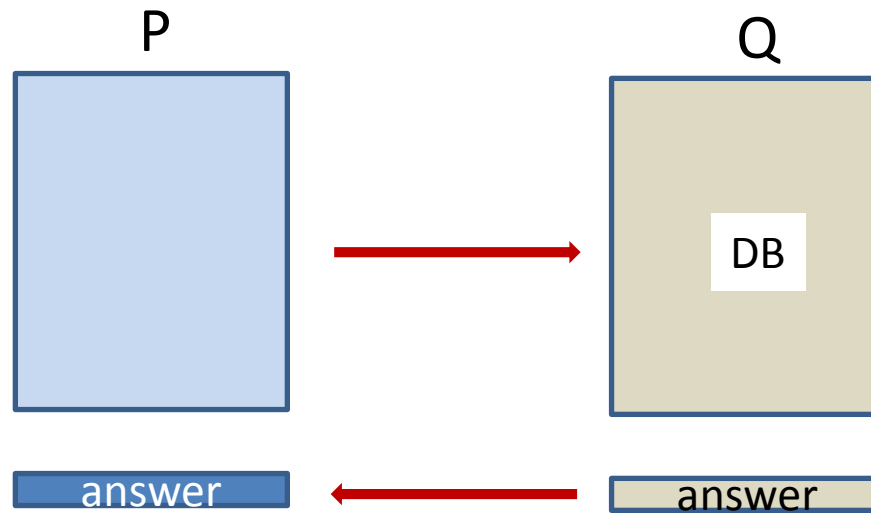
# Well-behaved case: Conjunctive Queries

- Query equivalence



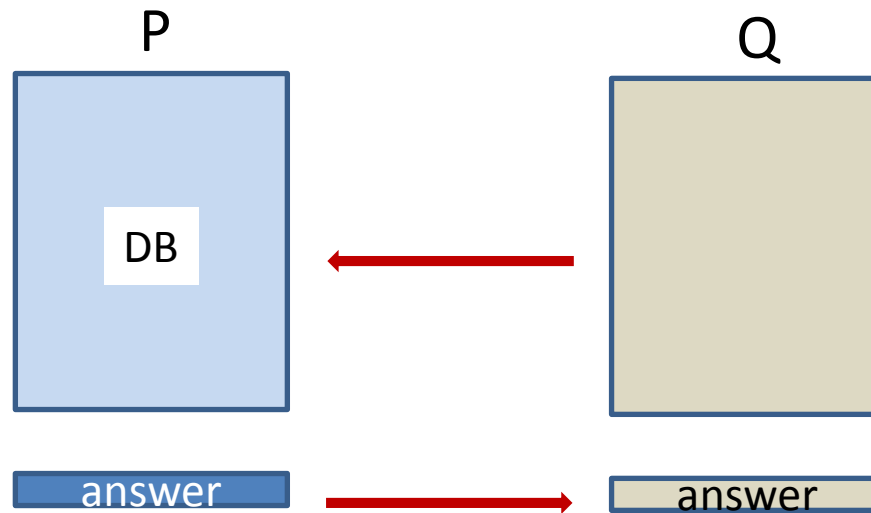
# Well-behaved case: Conjunctive Queries

- Query equivalence



# Well-behaved case: Conjunctive Queries

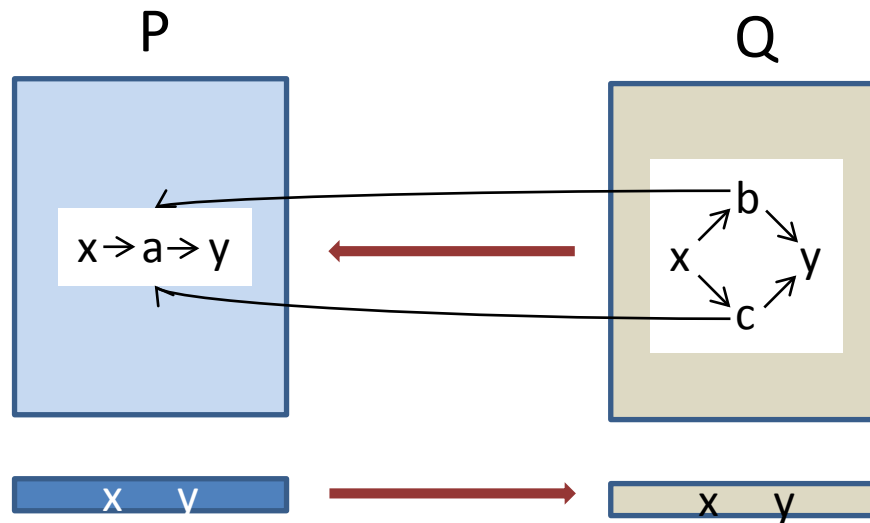
- Query equivalence



# Well-behaved case: Conjunctive Queries

- Query equivalence

Example: db is a binary relation (graph)

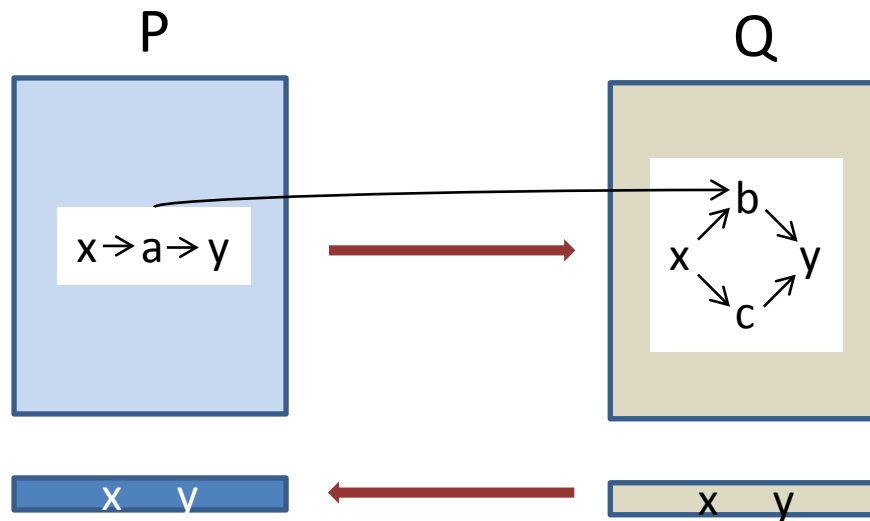




# Well-behaved case: Conjunctive Queries

- Query equivalence

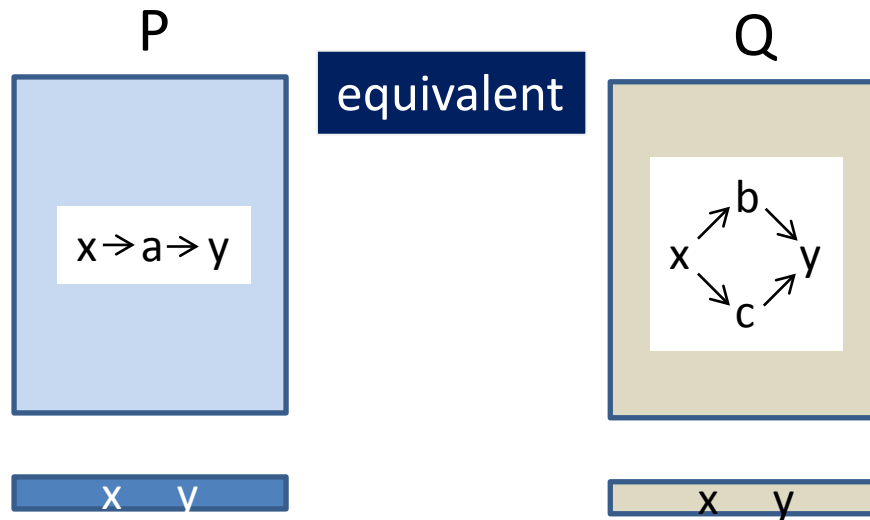
Example: db is a binary relation (graph)



# Well-behaved case: Conjunctive Queries

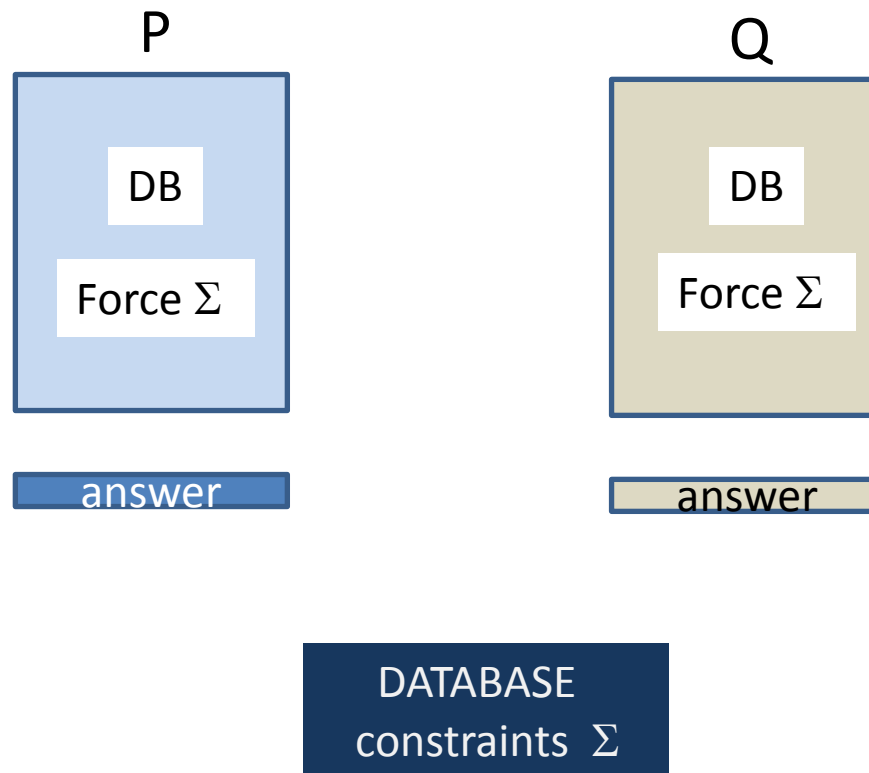
- Query equivalence

Example: db is a binary relation (graph)



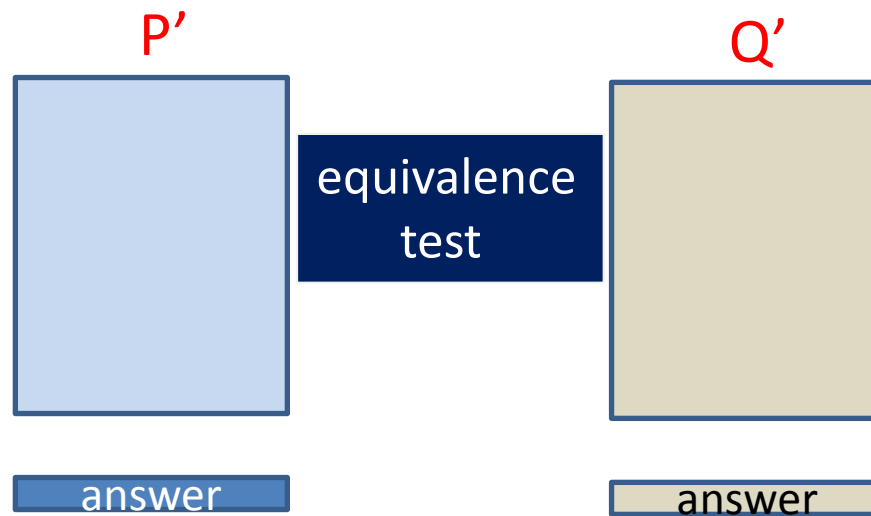
# Well-behaved case: Conjunctive Queries

- One step further: **taking into account constraints**



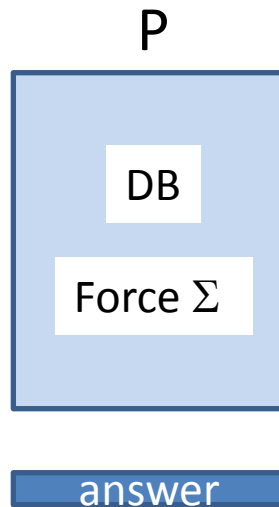
# Well-behaved case: Conjunctive Queries

- One step further: **taking into account constraints**



# Well-behaved case: Conjunctive Queries

- Forcing satisfaction of  $\Sigma$ : **the Chase**



# Well-behaved case: Conjunctive Queries

- Forcing satisfaction of  $\Sigma$ : **the Chase**

Movie	title	director	actor
	b	Godard	
	c		Bardot

Schedule	title	theater	time
	b	a	
	c	a	

Answer	theater
	a

$\Sigma$  theater  $\rightarrow$  title  
title  $\rightarrow$  director

# Well-behaved case: Conjunctive Queries

- Forcing satisfaction of  $\Sigma$ : **the Chase**

Movie	title	director	actor
	b	Godard	
	b		Bardot

Schedule	title	theater	time
	b	a	
	b	a	

Answer	theater
	a

$\Sigma$  theater  $\rightarrow$  title,  
title  $\rightarrow$  director

# Well-behaved case: Conjunctive Queries

- Forcing satisfaction of  $\Sigma$ : **the Chase**

Movie	title	director	actor
	b	Godard	
	b	Godard	Bardot

Schedule	title	theater	time
	b	a	
	b	a	

Answer	theater
	a

$\Sigma$  theater  $\rightarrow$  title  
title  $\rightarrow$  director



# Well-behaved case: Conjunctive Queries

- Forcing satisfaction of  $\Sigma$ : **the Chase**

Movie	title	director	actor
	b	Godard	Bardot

Schedule	title	theater	time
	b	a	

Answer	theater
	a

$\Sigma$  theater  $\rightarrow$  title  
title  $\rightarrow$  director

# Well-behaved case: Conjunctive Queries

- How far does the good news go?
- Trouble in paradise: **an undecidable question**

Implication of CQ inclusion

$$\begin{array}{l} P_1 \subseteq Q_1 \\ P_2 \subseteq Q_2 \\ \dots \\ P_n \subseteq Q_n \end{array}$$

implies

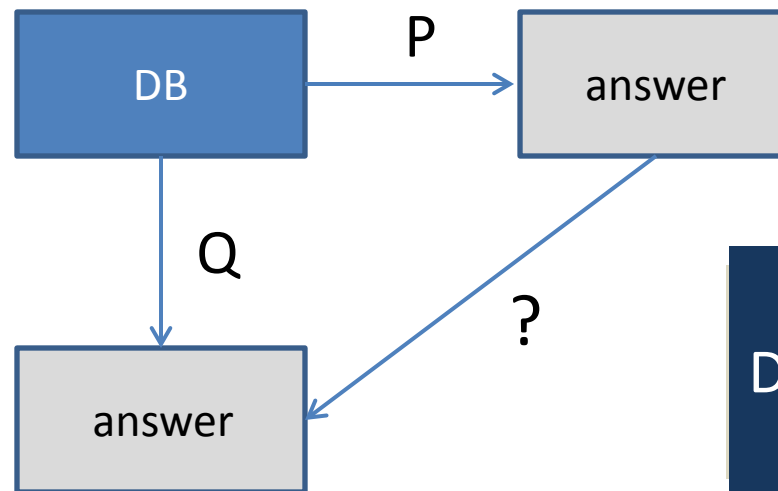
$$P \subseteq Q$$

reduction from word problem  
for finite monoids

# Well-behaved case: Conjunctive Queries

- How far does the good news go?
- Trouble in paradise: **an open question**

Does the answer to P determine the answer to Q?



Decidability is open!

# Summary so far

- **SQL:** too powerful for decidable static analysis
- **Conjunctive queries:** simple SQL queries, well behaved

**Not enough:**  
static analysis of complex queries  
is essential to performance!

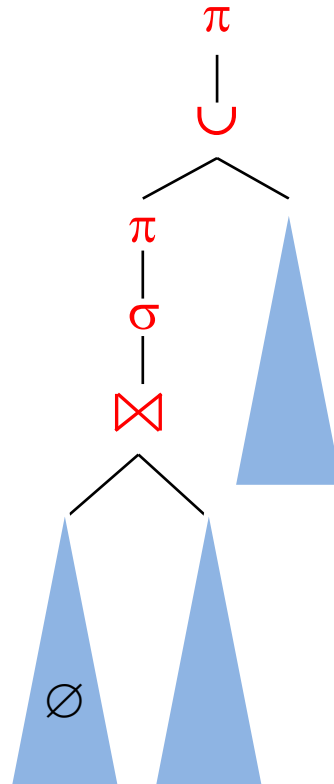
# What to do in practical query processing

- Static analysis on simple building blocks

Complex SQL query

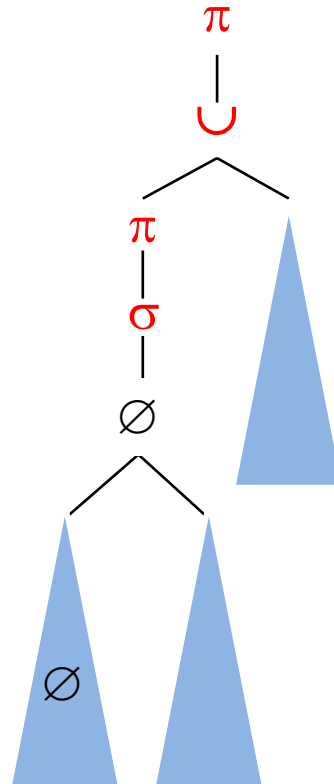
# What to do in practical query processing

- Static analysis on simple building blocks



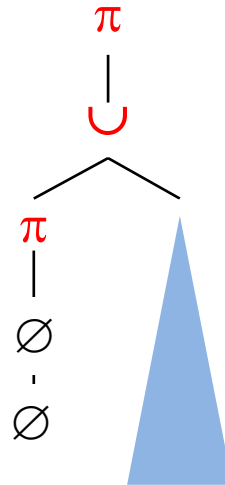
# What to do in practical query processing

- Static analysis on simple building blocks



# What to do in practical query processing

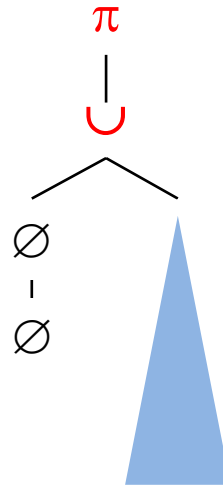
- Static analysis on simple building blocks





# What to do in practical query processing

- Static analysis on simple building blocks



# What to do in practical query processing

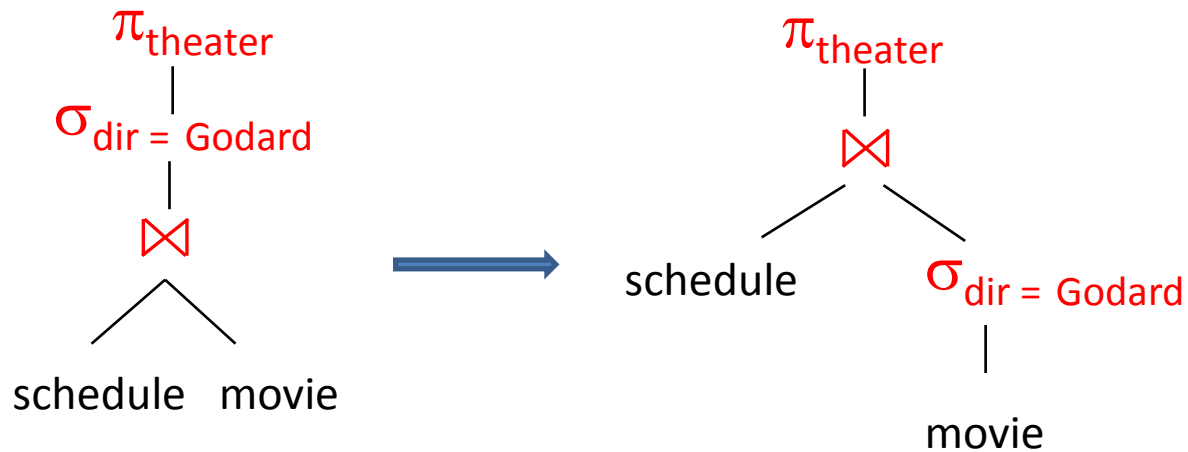
- Static analysis on simple building blocks



# What to do in practical query processing

- Rewrite rules for simplifying queries

early selection



# What to do in practical query processing

- Many other heuristics

More rewrite rules, subquery decorrelation,  
common subqueries, view unfolding ...

- Dramatic impact on complex queries

Example [Bill McKenna, *ParAccel*):  
23 000 lines “monster query”  
static analysis improved performance by 95%

# Static analysis for XML

- Questions: some similar, some new
- Different techniques
- XML Schema is closely related to tree automata
- XQuery is closely related to tree transducers

Techniques for XML:  
mix of logic and automata theory

Important twist due to data:  
**automata on infinite alphabets**

**Static analysis**

reasoning about queries

**Verification**

reasoning about workflow

# Verification of application workflows

- Example: verify that no free tickets can be sold

For a full list of Ryanair fees, please click [here](#)

### Going Out From Dublin - Cork

« Previous Day » Next Day »

Select A Flight

	<input type="radio"/>	Regular Fare	Adult	9,99 EUR	Sat , 21 Feb 09 Flight FR 9843	08:55 Depart 09:45 Arrive	Going Out Regular Fare <b>Depart:</b> Dublin 08:55 <b>Arrive:</b> Cork 09:45  Fare: 0,00 EUR Taxes / Fees: 0,00 EUR Total Price: 0,00 EUR
	<input type="radio"/>	Regular Fare	Adult	9,99 EUR	Sat , 21 Feb 09 Flight FR 9845	11:35 Depart 12:25 Arrive	
	<input type="radio"/>	Regular Fare	Adult	9,99 EUR	Sat , 21 Feb 09 Flight FR 9857	14:00 Depart 14:50 Arrive	
	<input type="radio"/>	Regular Fare	Adult	14,99 EUR	Sat , 21 Feb 09 Flight FR 9847	16:20 Depart 19:10 Arrive	
	<input type="radio"/>	Regular Fare	Adult	9,99 EUR	Sat , 21 Feb 09 Flight FR 9849	20:50 Depart 21:40 Arrive	

### Coming Back From Cork - Dublin

« Previous Day » Next Day »

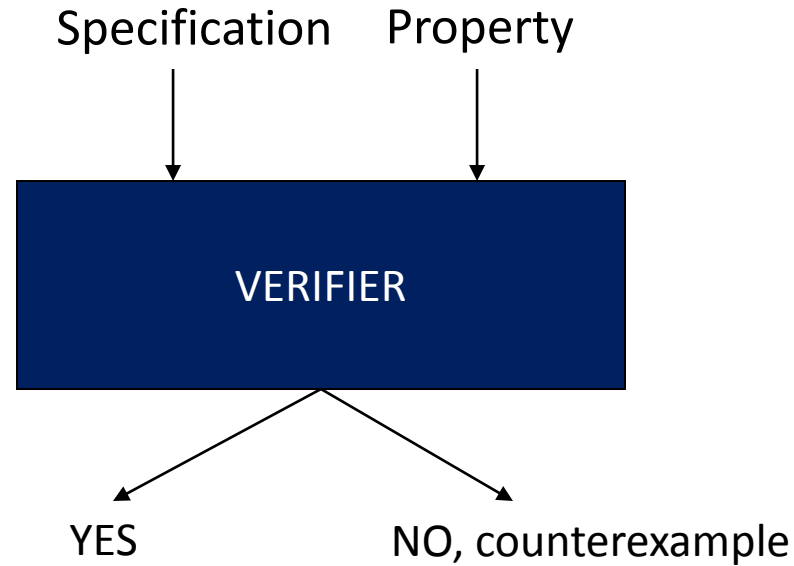
Select A Flight

	<input type="radio"/>	Regular Fare	Adult	0,99 EUR	Sun , 22 Feb 09 Flight FR 9844	10:10 Depart 11:00 Arrive	Coming Back Regular Fare <b>Depart:</b> Cork 10:10 <b>Arrive:</b> Dublin 11:00  Fare: 0,00 EUR Taxes / Fees: 0,00 EUR Total Price: 0,00 EUR
	<input type="radio"/>	Regular Fare	Adult	9,99 EUR	Sun , 22 Feb 09 Flight FR 9856	14:30 Depart 15:20 Arrive	
	<input type="radio"/>	Regular Fare	Adult	9,99 EUR	Sun , 22 Feb 09 Flight FR 9846	17:05 Depart 17:55 Arrive	
	<input type="radio"/>	Regular Fare	Adult	29,99 EUR	Sun , 22 Feb 09 Flight FR 9848	19:25 Depart 20:25 Arrive	

**Select Your Flights and Continue**  
If the flights you require are shown above, select them and click on "Select and Continue" to proceed.

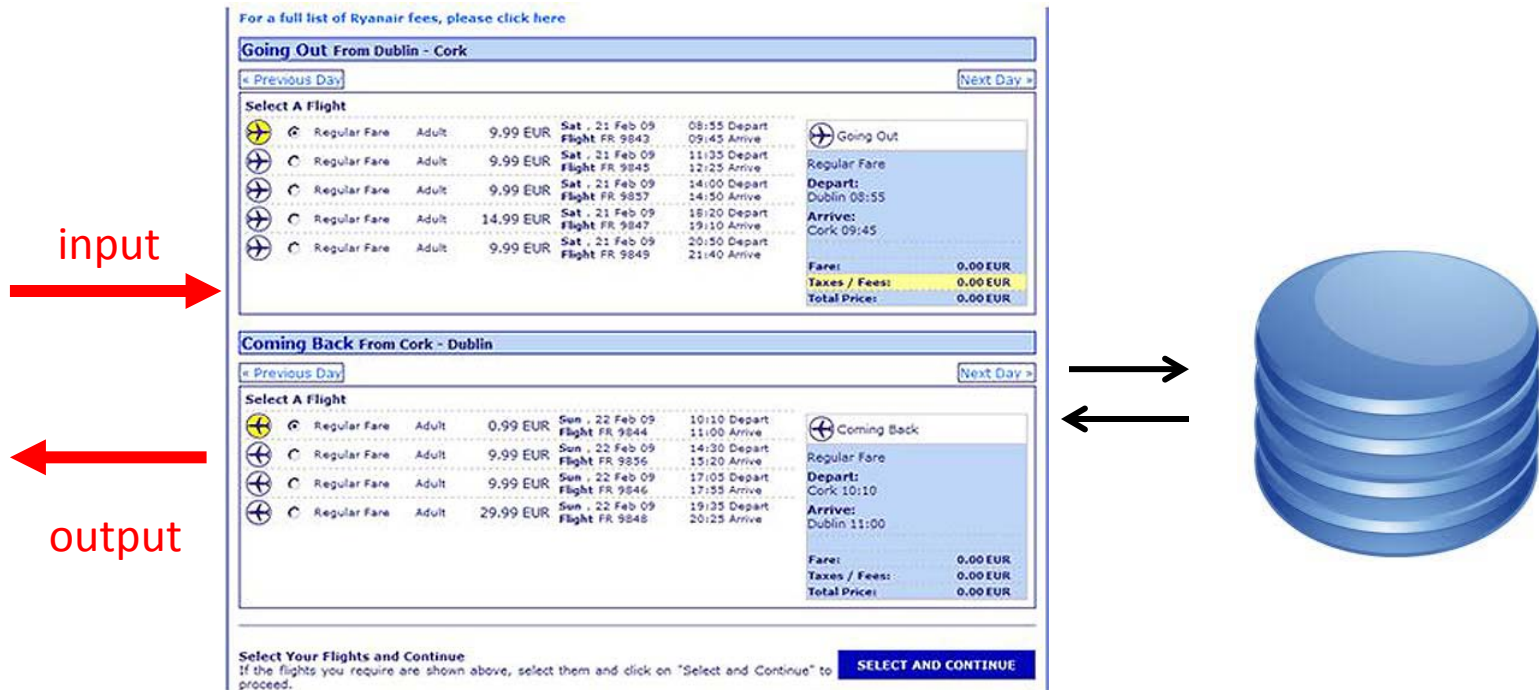
**SELECT AND CONTINUE**

# Automatic verification problem



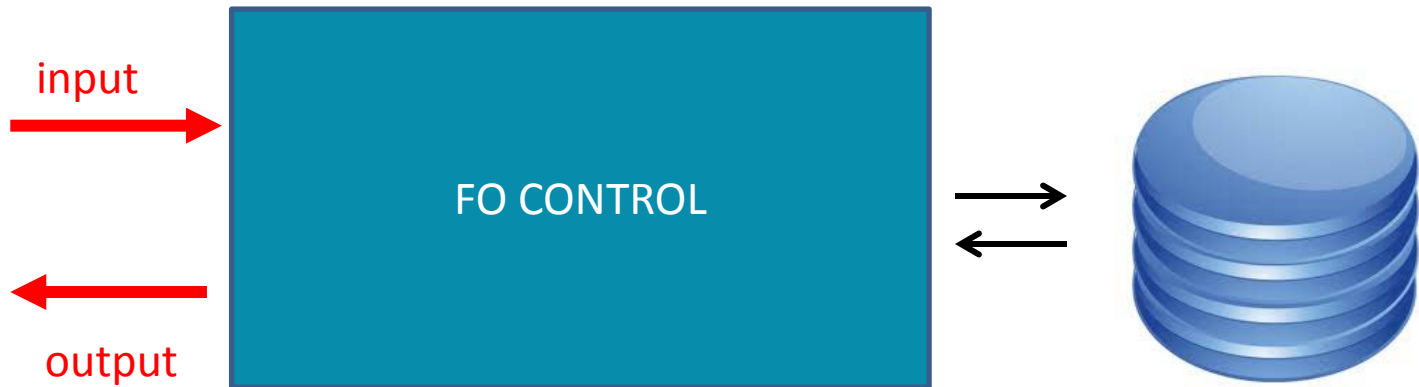


# Verification of application workflows



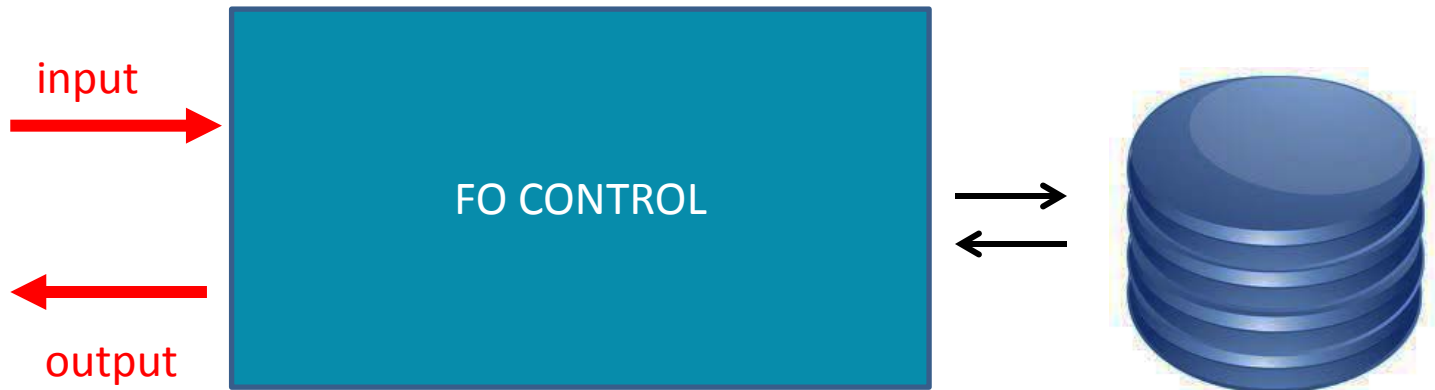
# Verification of application workflows

High-level specification: **First-Order logic (FO) control**



# Verification of application workflows

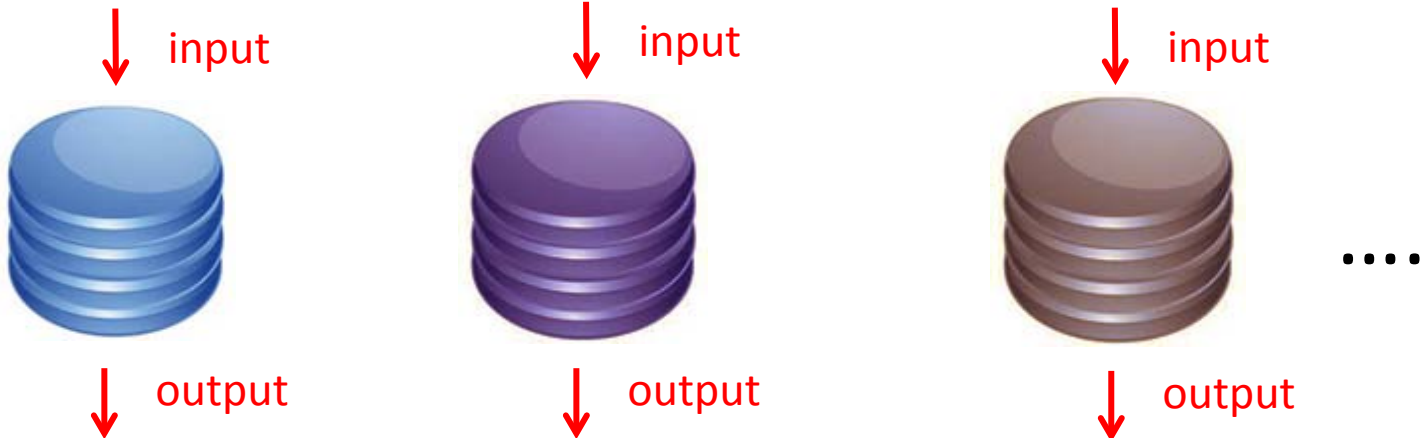
High-level specification: **FO control**



# Verification of application workflows

High-level specification: **FO control**

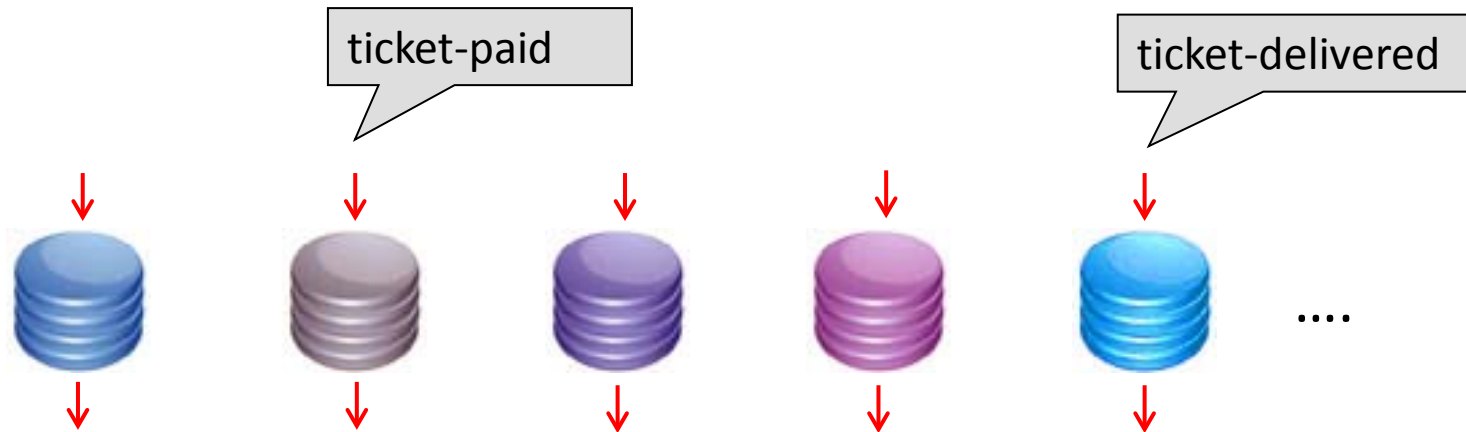
RUN



# Verification of application workflows

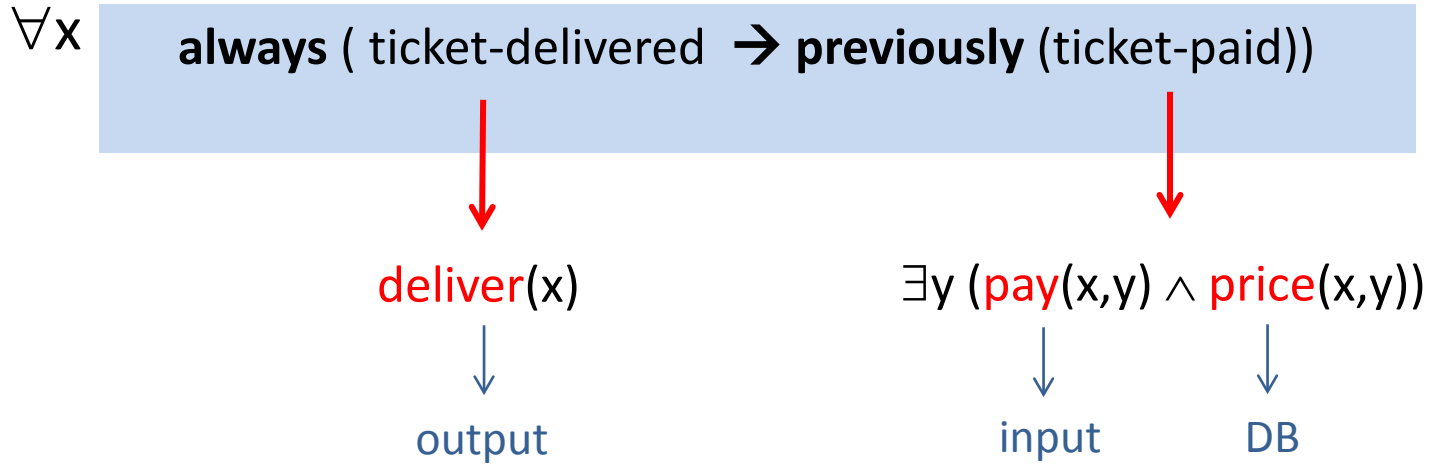
## *Specifying properties*

**always** ( ticket-delivered  $\rightarrow$  **previously** (ticket-paid))



# Verification of application workflows

## *Specifying properties*



# Verification of application workflows

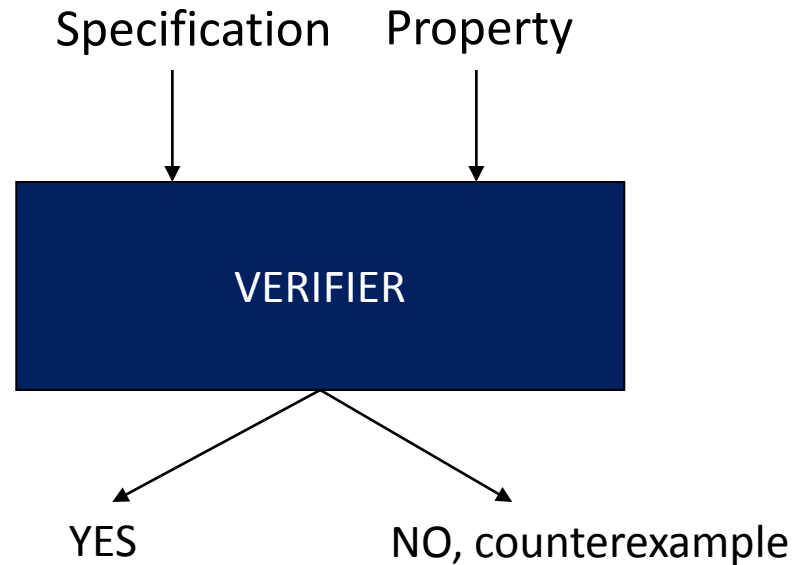
## *Specifying properties*

**always** ( ticket-delivered  $\rightarrow$  **previously** (ticket-paid))



Language for properties: FO + temporal operators

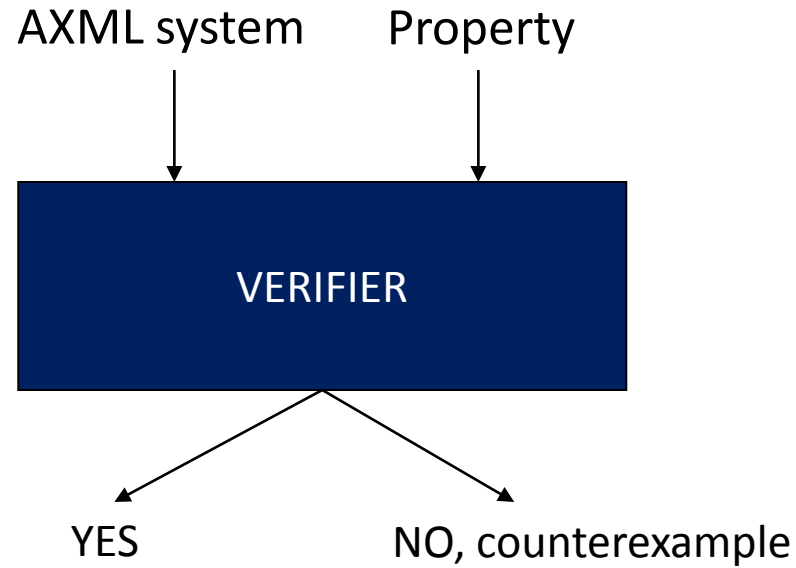
# Formal verification problem



Techniques:  
mix of logic and automata theory



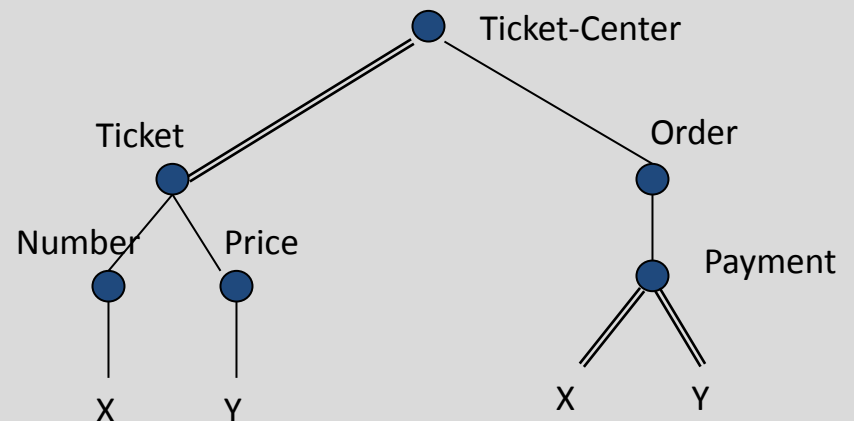
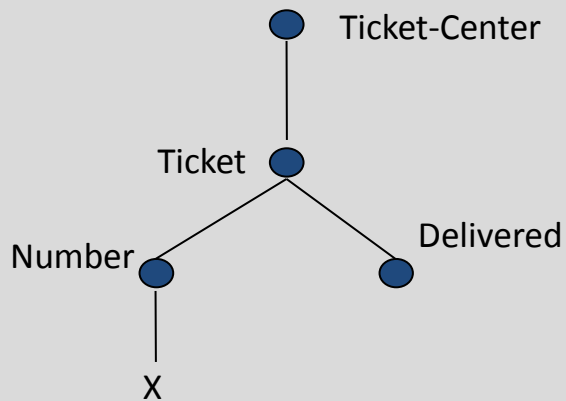
# Variant for AXML



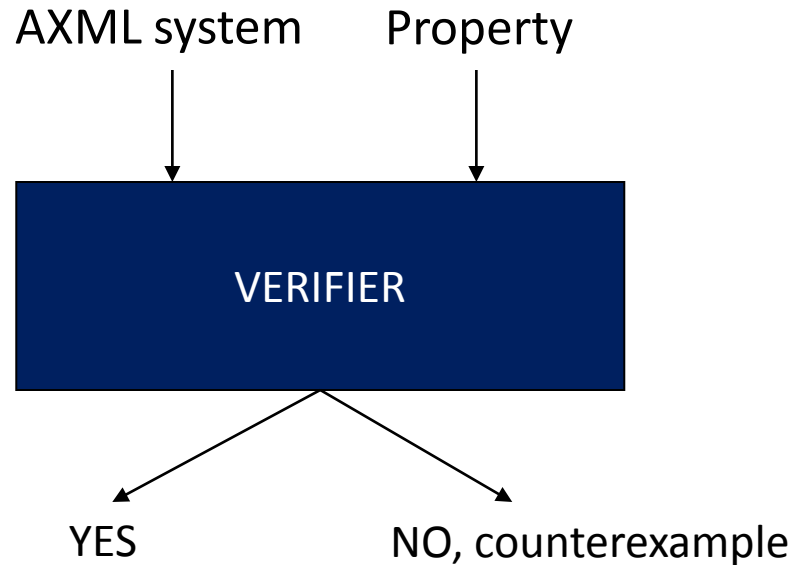
# Variant for AXML

$\forall x$

**always ( ticket-delivered  $\rightarrow$  previously (ticket-paid))**



# Variant for AXML



**Good news, again:** can automatically verify significant classes of applications

# Conclusions

## Static analysis and verification in databases:

- Practically essential, intellectually challenging
- Run against fundamental limitations of computing
- Deep mathematics, elegant mix of logic and automata theory
- **This talk:** limited overview of some basic questions and ideas
- **Just the tip of the iceberg:**

Many more static analysis and verification problems

Wide array of techniques to deal with limitations:  
**sophisticated heuristics, approximation, abstraction**

# Work on verification

UC San Diego:

Alin Deutsch & DB team

INRIA & ENS Cachan:

Serge Abiteboul and Luc Segoufin

Thank you!  
Merci!