



# PTA-Viz

Siddharth Patil  
Guide: Prof. Uday Khedker

Department of Computer Science and Engineering, IIT Bombay



## What is PTA-Viz?

- **Points To Analysis Visualizer**
- A tool for **interactive visualization** of PTA algorithms
- Shows the **results** of the analysis at **each iteration** for **each statement/block**
- Entirely **GUI** based application with the ability to **load and export** the analysis' results

## How it works

- User types/loads his code in the **GUI's code editor**
- Input is **scanned+parsed** using **PLY** to get a **CFG**
- Analysis is performed on the **CFG** and the **results** are stored using **graphviz**
- **CFG** is displayed in the **GUI** which the **user interacts** with to view the specific analysis **results**

## Future Work

- Cover various **different** kinds of more **complex** analyses
- **Finer** analysis details along with verbose explanations
- **Custom** analysis creator

## Uses

- **Academic** tool to be accompanied with the book "**Excursions in Pointer Analysis**" by Prof. Uday P. Khedker and Pritam M. Gharat
- Helps to see the subtle nuances of the algorithm's specifications via **corner cases**

## Definitions

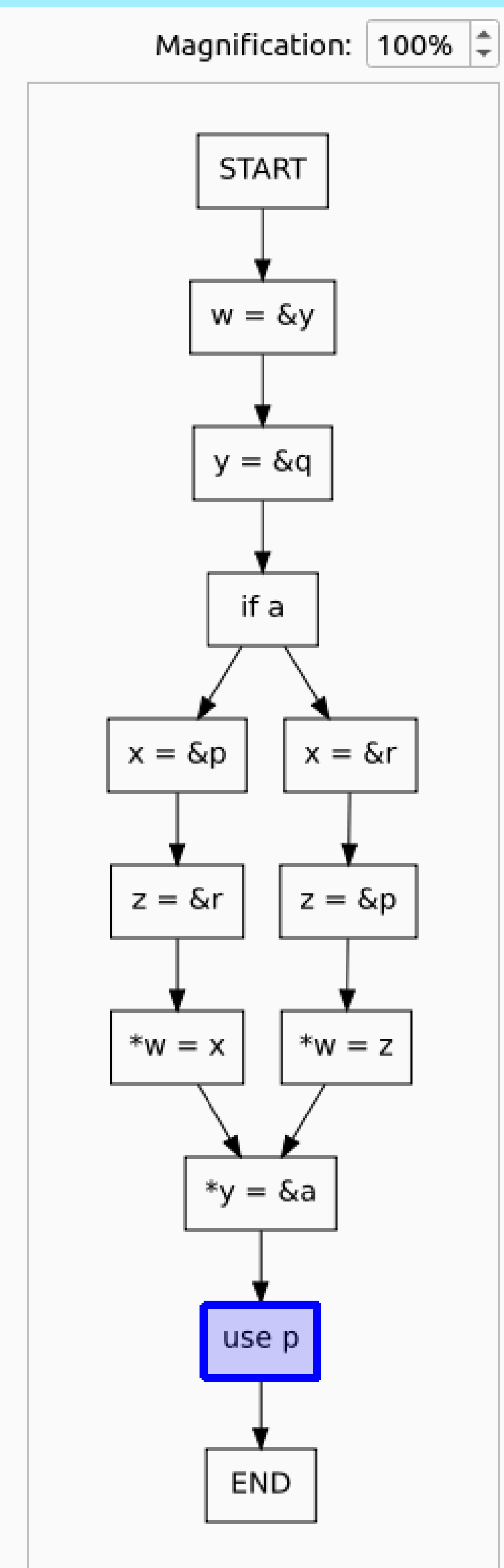
- **PTA**: Compile time technique to determine **potential pointer-pointee relationships** during program execution
- **FI-PTA** (Flow Insensitive): Analysis **ignores** the **control flow** of the program during execution
- **FS-PTA** (Flow Sensitive): **CFG** is used to analyze the program for **reasonable control flows** only
- **LFCPA** (Liveness based Flow and Context sensitive PTA): **Trimmed** version of **FS-PTA** where **liveness of variables** is considered and analysis is **performed separately** for each **calling context of methods**

## Example Code

```
1 structs:
2
3 funcs:
4
5 main:
6     scalar a
7     scalar* p,q,r
8     scalar** x,y,z
9     scalar*** w
10
11     w = &y
12     y = &q
13
14     if a goto 21
15
16     x = &p
17     z = &r
18     *w = x
19
20     goto 25
21
22     x = &r
23     z = &p
24     *w = z
25
26     *y = &a
27     use p
```

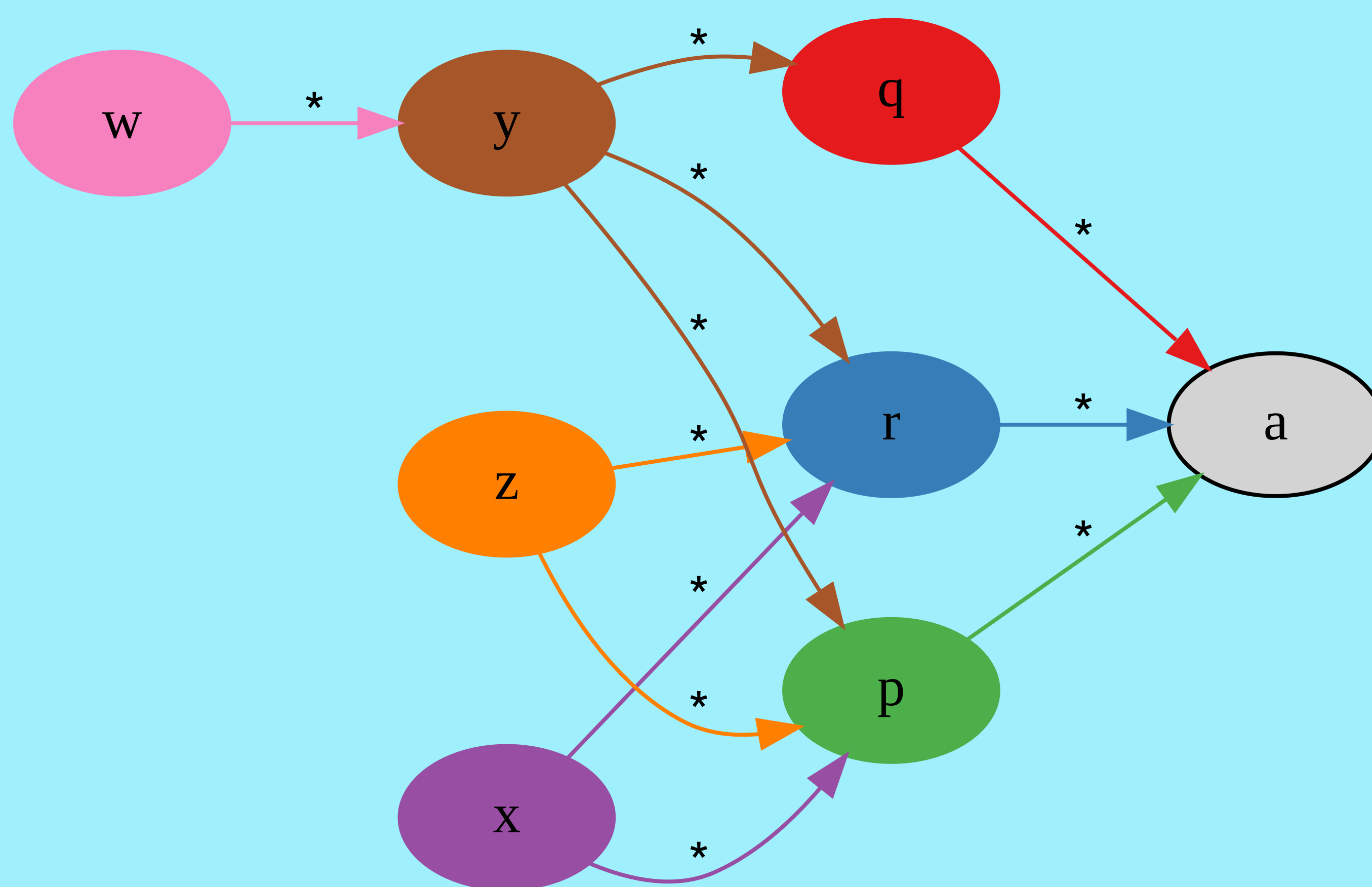
## CFG

Control Flow Graph

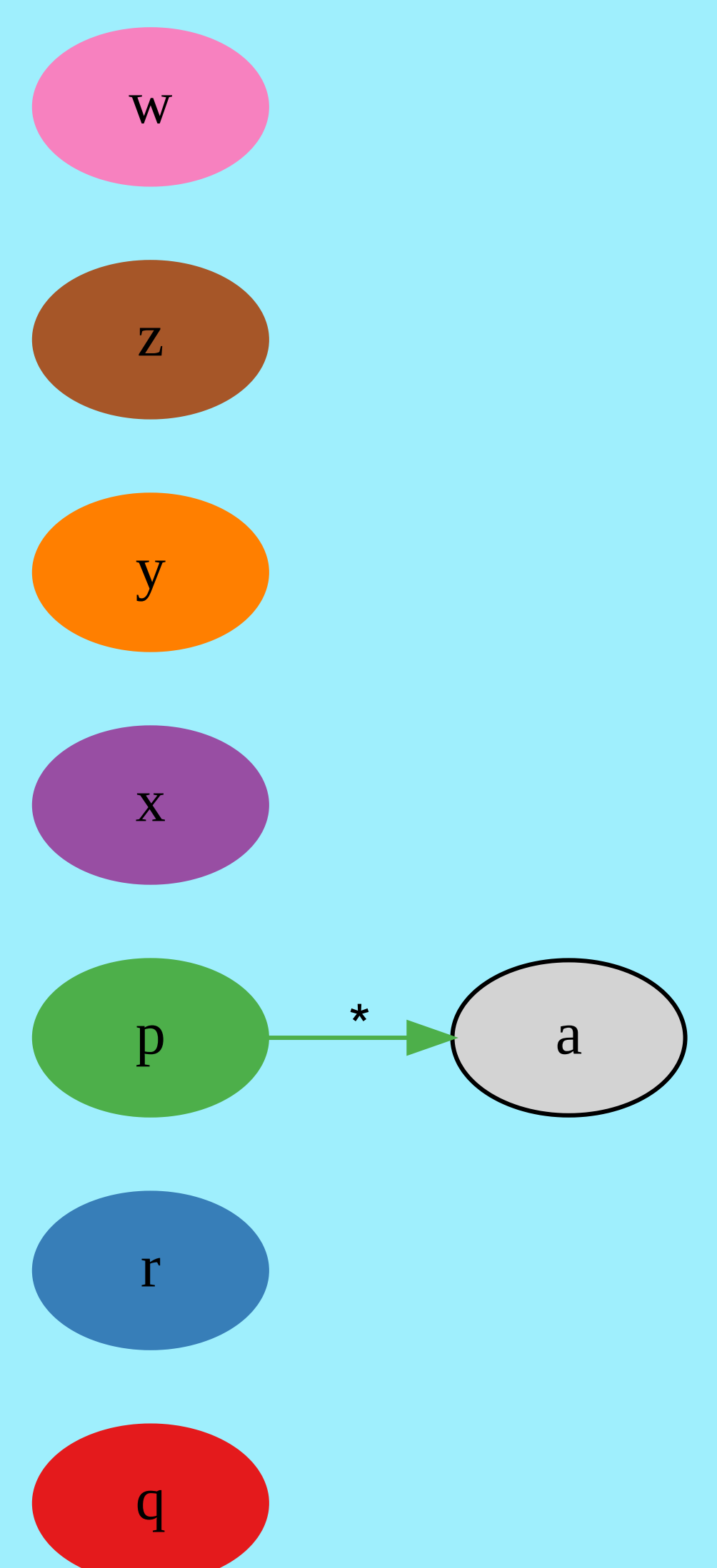


## Results

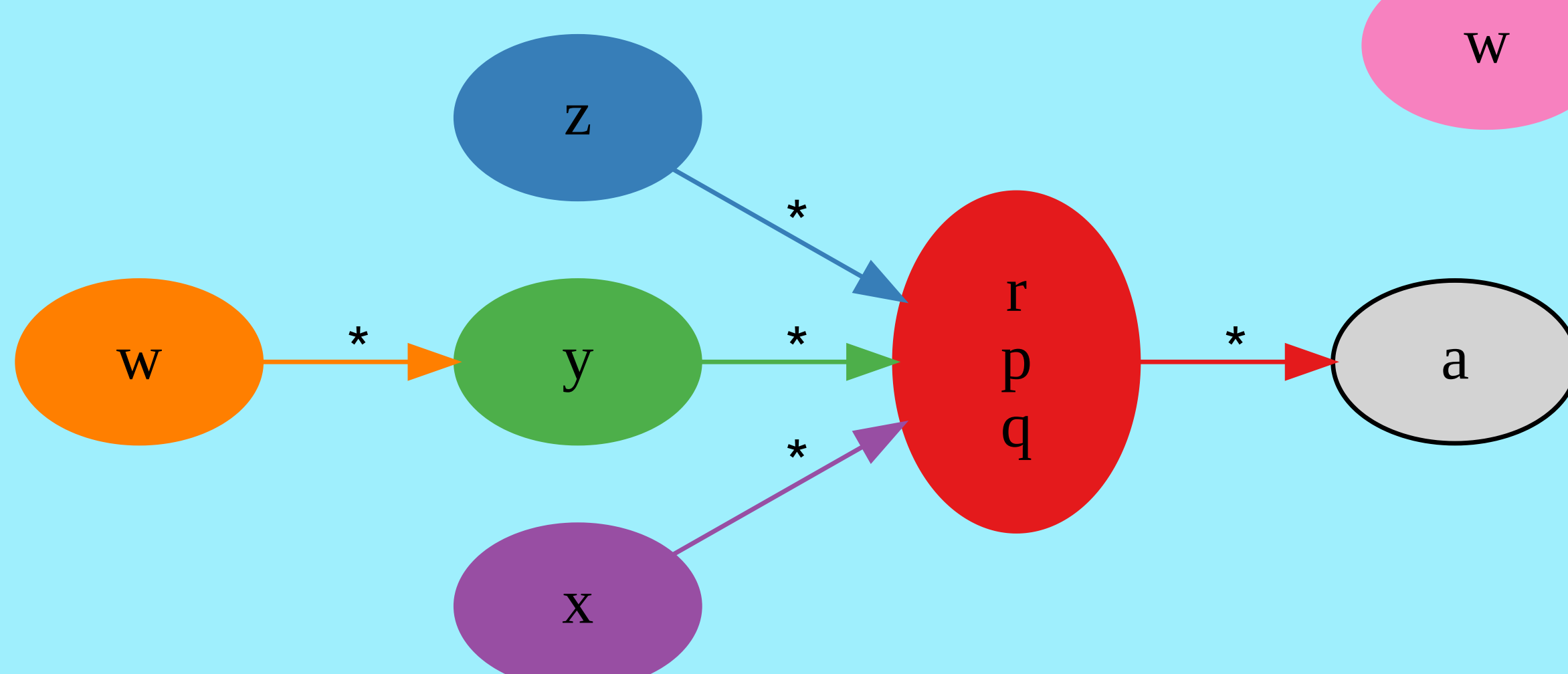
### • Andersen's FI-PTA



### • LFCPA



### • Steensgaard's FI-PTA



### • FS-PTA

