On the strength of Sherali-Adams and Nullstellensatz as propositional proof systems

Ilario Bonacina Maria Luisa Bonet

UPC Barcelona Tech

LICS Haifa, August 4 2022

Context

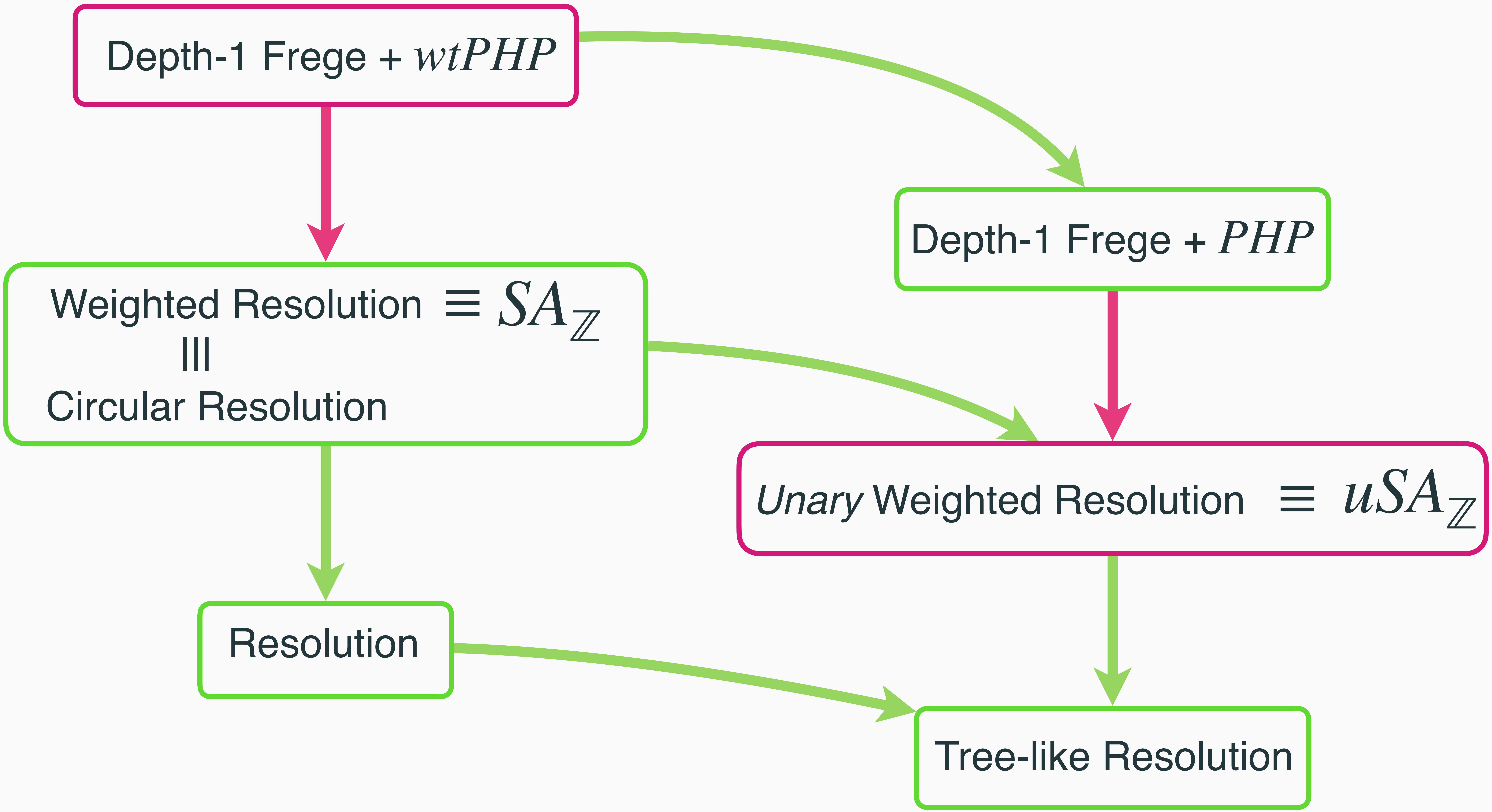
What area? Propositional proof complexity

What? New relations between well studied proof systems

How? Using a connection to proof systems studied in the context of maxSAT

Why? New insights on the strength of some systems

& connections to TFNP classes


Depth-1 Frege + $wtPHP$
Depth-1 Frege + PHP
Weighted Resolution $\equiv SA_{\mathbb{Z}}$
$\equiv$
Circular Resolution
Unary Weighted Resolution $\equiv uSA_{\mathbb{Z}}$
Resolution
Tree-like Resolution

Proof System

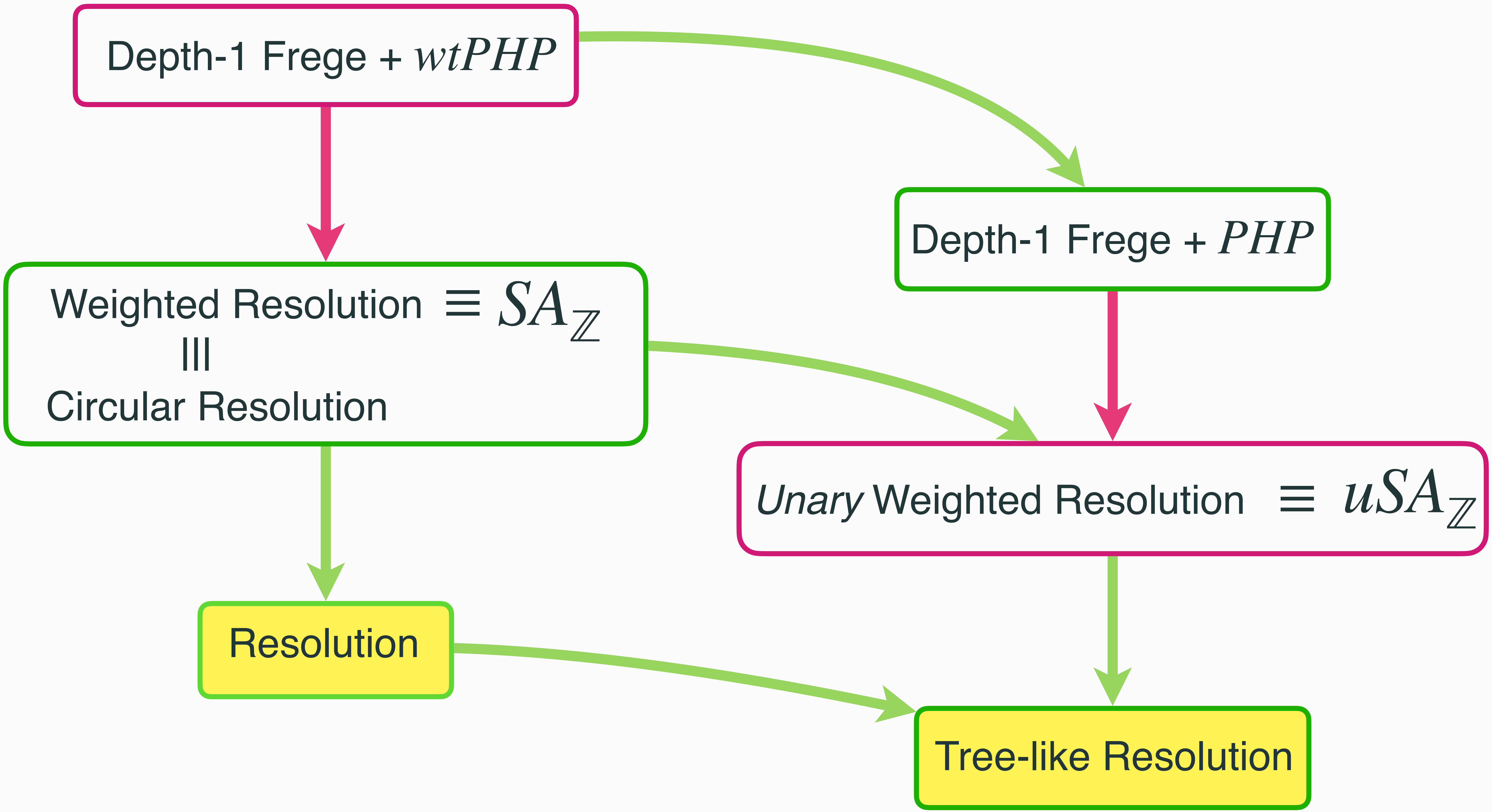
“A way to certify propositional tautologies/ contradictions”

Proof System 1

$\downarrow$

Proof System 2

“All the propositional tautologies certifiable efficiently in Proof System 2 are also efficiently certifiable in Proof System 1”


Depth-1 Frege + $wtPHP$
Depth-1 Frege + PHP
Weighted Resolution $\equiv SA_{\mathbb{Z}}$
$|||$
Circular Resolution
Unary Weighted Resolution $\equiv uSA_{\mathbb{Z}}$
Resolution
Tree-like Resolution

Resolution

$F = C_1 \wedge \ldots \wedge C_m$ where C_j are clauses (i.e. disj. of vars or negated vars)

Inference Rules

$$\frac{C \vee x \qquad C \vee \neg x}{C} \text{ (symmetric cut)}$$

$$\frac{C}{C \vee x \qquad C \vee \neg x} \text{ (symmetric weakening)}$$

$$\frac{}{x \vee \neg x} \text{ (excluded middle)}$$

Resolution

$F = C_1 \wedge \ldots \wedge C_m$ where C_j are clauses (i.e. disj. of vars or negated vars)

Inference Rules

$$\frac{C \vee x \qquad C \vee \neg x}{C} \text{ (symmetric cut)}$$

$$\frac{C}{C \vee x \qquad C \vee \neg x} \text{ (symmetric weakening)}$$

$$\frac{C \vee x \qquad C \vee \neg x}{C} \updownarrow$$

$$\frac{}{x \vee \neg x} \text{ (excluded middle)}$$

An example

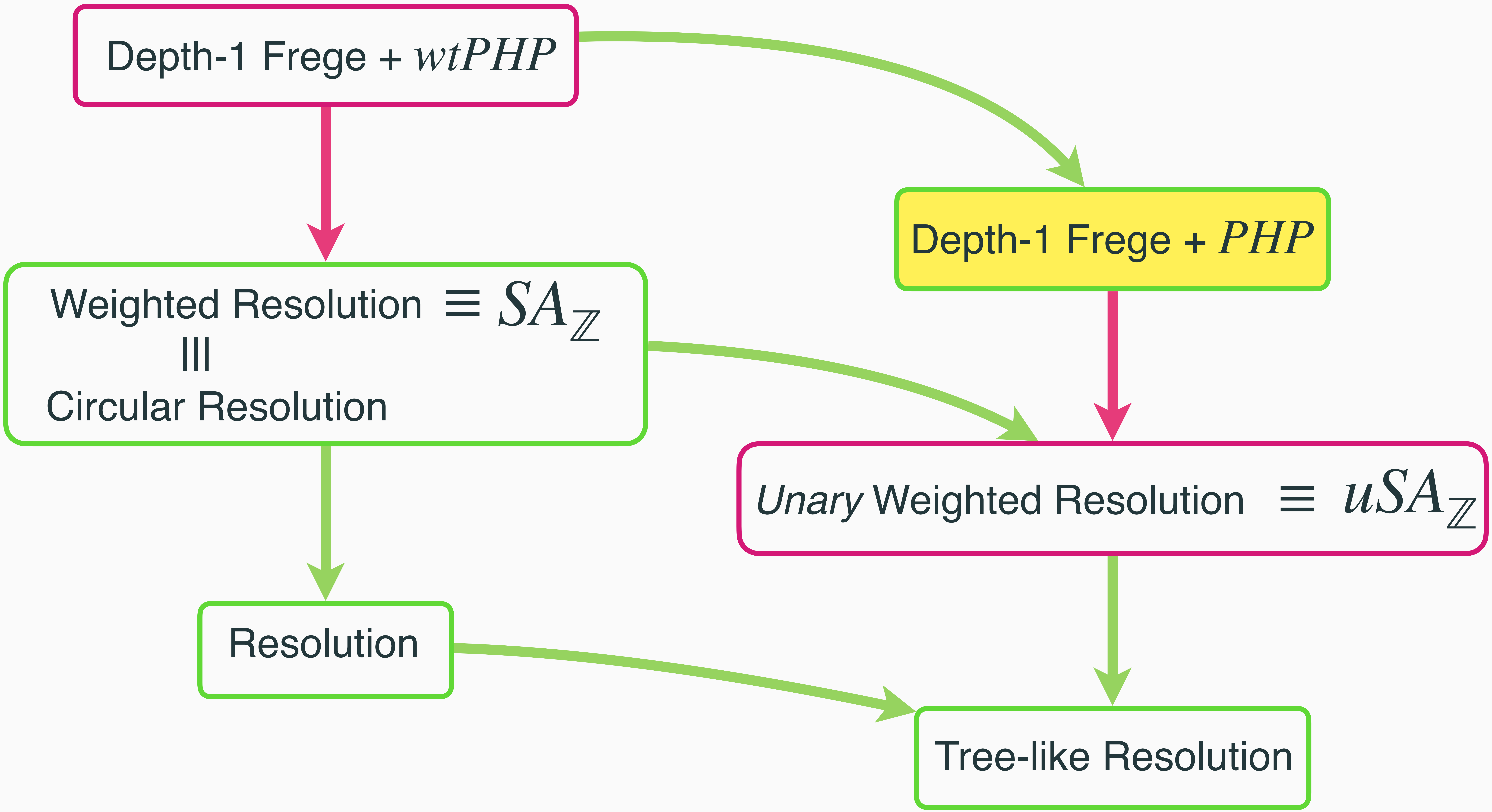
$x \vee y$ $\qquad$ $x \vee \neg y$ $\qquad$ $\neg x$

An example

$$
\begin{tikzcd}
x \lor y \arrow[dr, bend right] & & x \lor \neg y \arrow[dl, bend left] & \neg x \\
& x & &
\end{tikzcd}
$$

An example

$$
\begin{tikzcd}
x \vee y \arrow[dr] & & x \vee \neg y \arrow[dl] & \neg x \arrow[ddl, bend left] \\
& x \arrow[dr, bend right] & & \\
& & \bot &
\end{tikzcd}
$$


Depth-1 Frege + $wtPHP$
Depth-1 Frege + PHP
Weighted Resolution $\equiv SA_{\mathbb{Z}}$
|||
Circular Resolution
Unary Weighted Resolution $\equiv uSA_{\mathbb{Z}}$
Resolution
Tree-like Resolution

Depth-d Frege + Φ

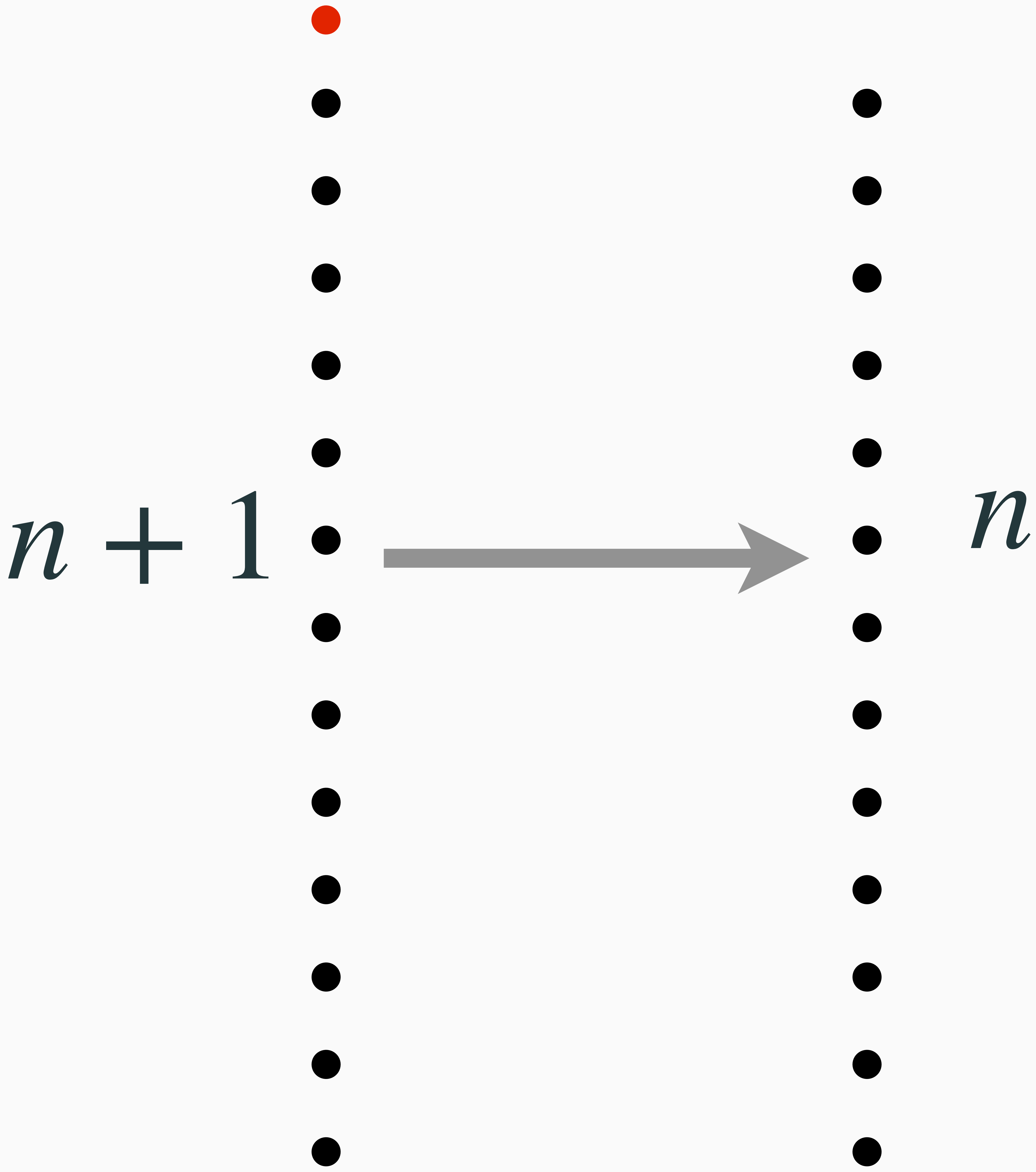
$F = C_1 \wedge \ldots \wedge C_m$ where C_j are clauses

Inference Rules similar to **Resolution** but for formulas of logical depth d.

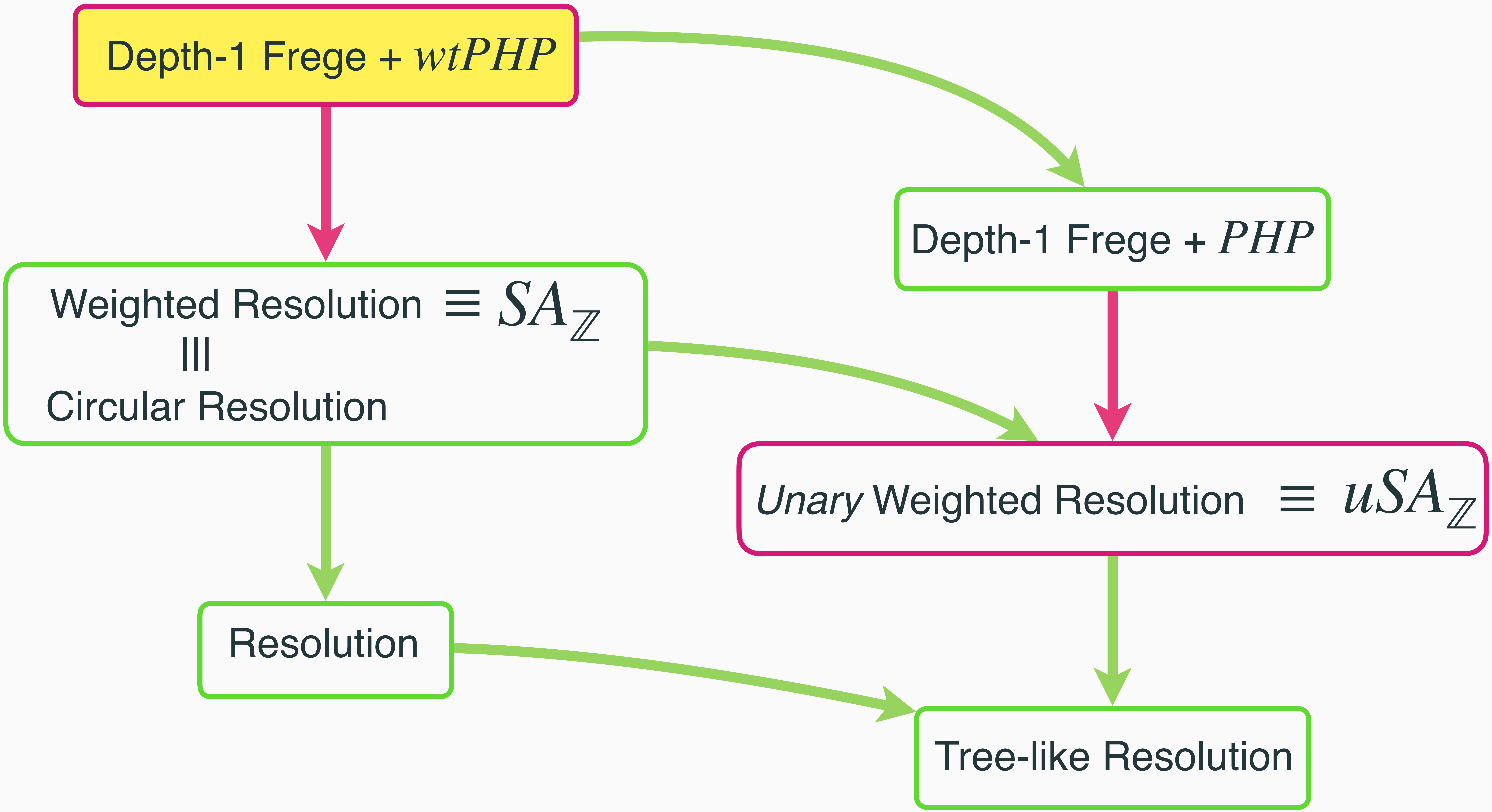
$\dfrac{}{A \vee \neg A}$ (excluded middle)

$\dfrac{}{\Phi}$

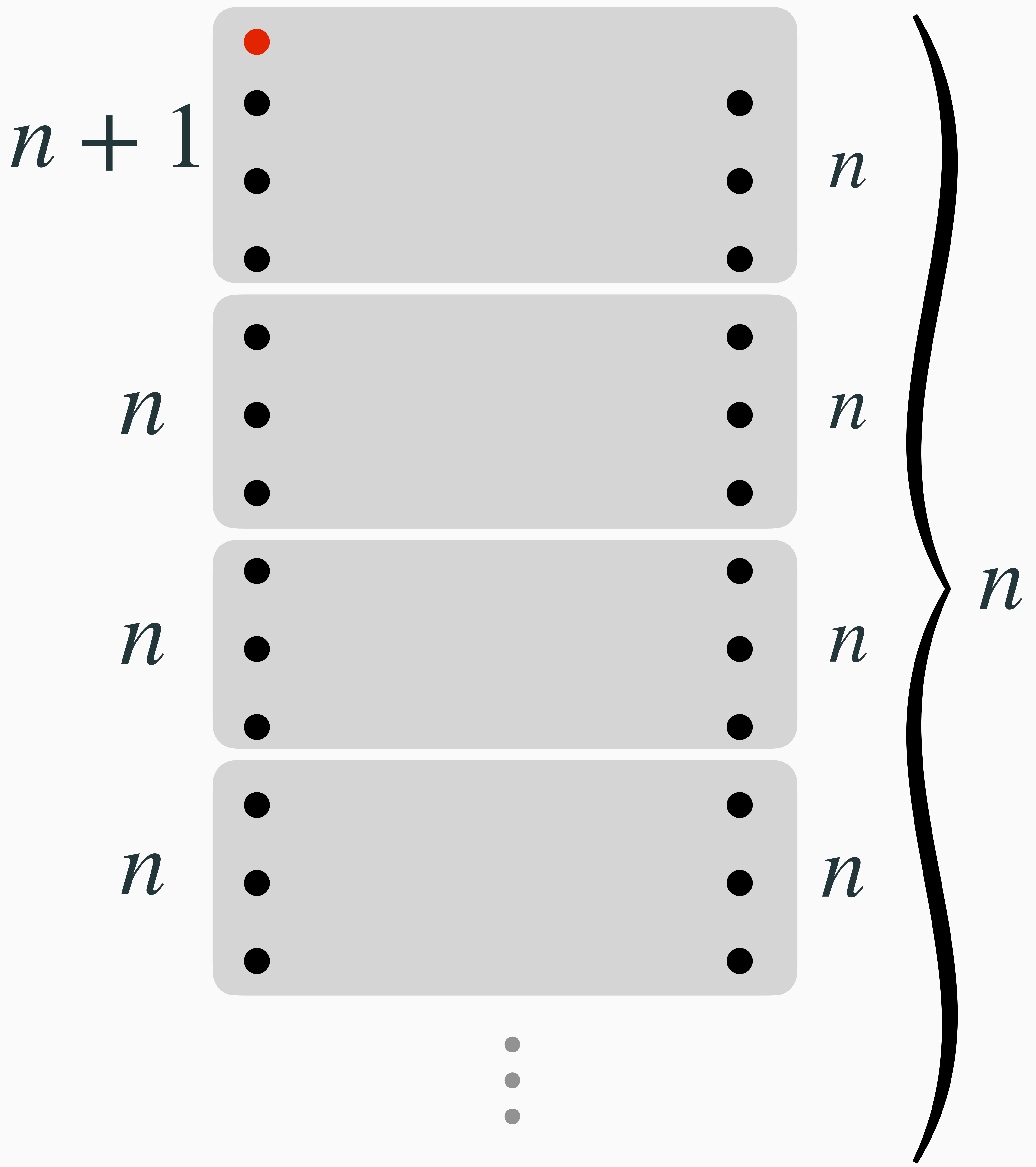
Pigeonhole Principle



- Pigeons fly to some hole
- Holes can accept at most 1 pigeon

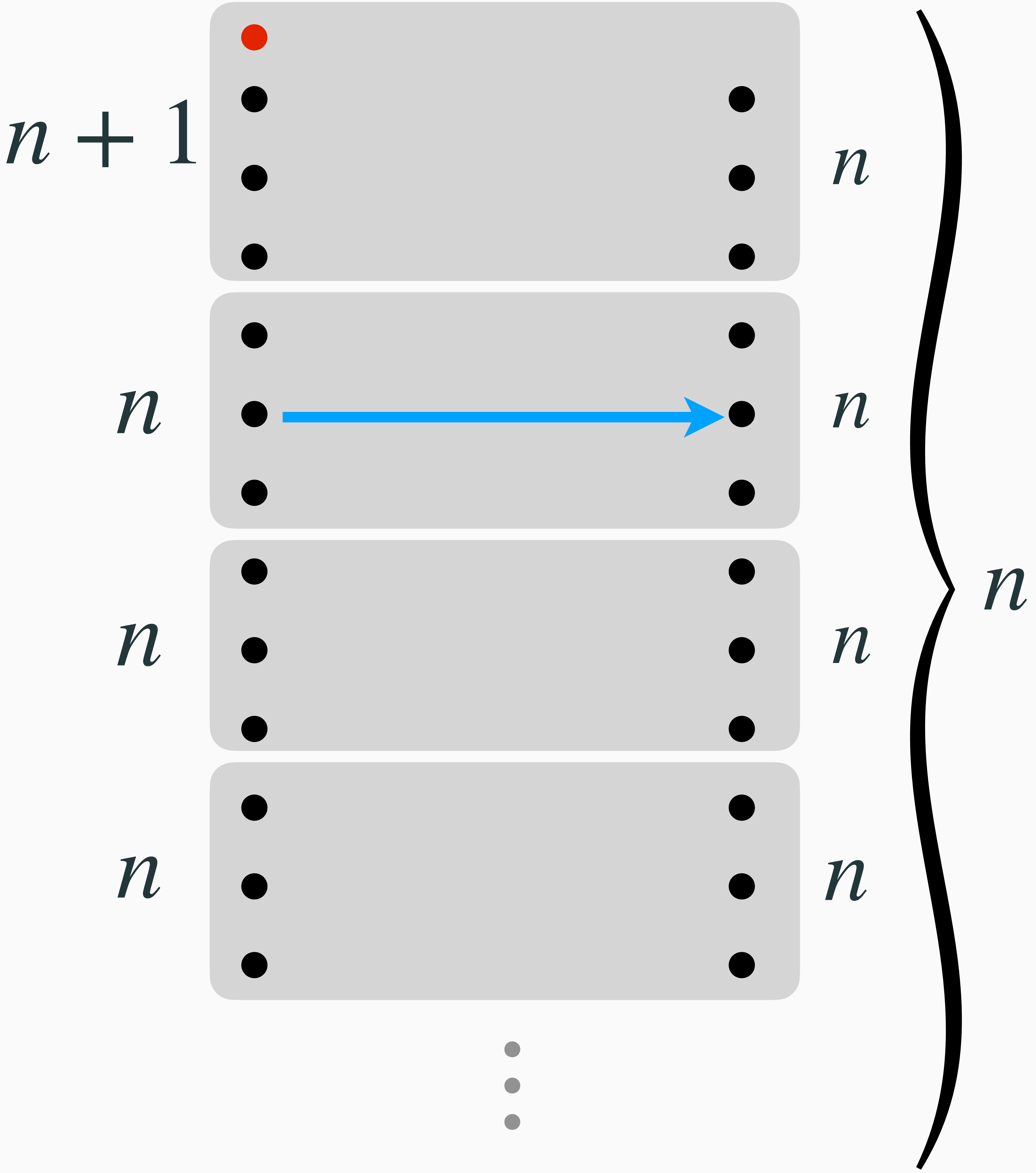

Depth-1 Frege + $wtPHP$
Depth-1 Frege + PHP
Weighted Resolution $\equiv SA_{\mathbb{Z}}$
$\equiv$
Circular Resolution
Unary Weighted Resolution $\equiv uSA_{\mathbb{Z}}$
Resolution
Tree-like Resolution

Weighted PHP (*wt*PHP)



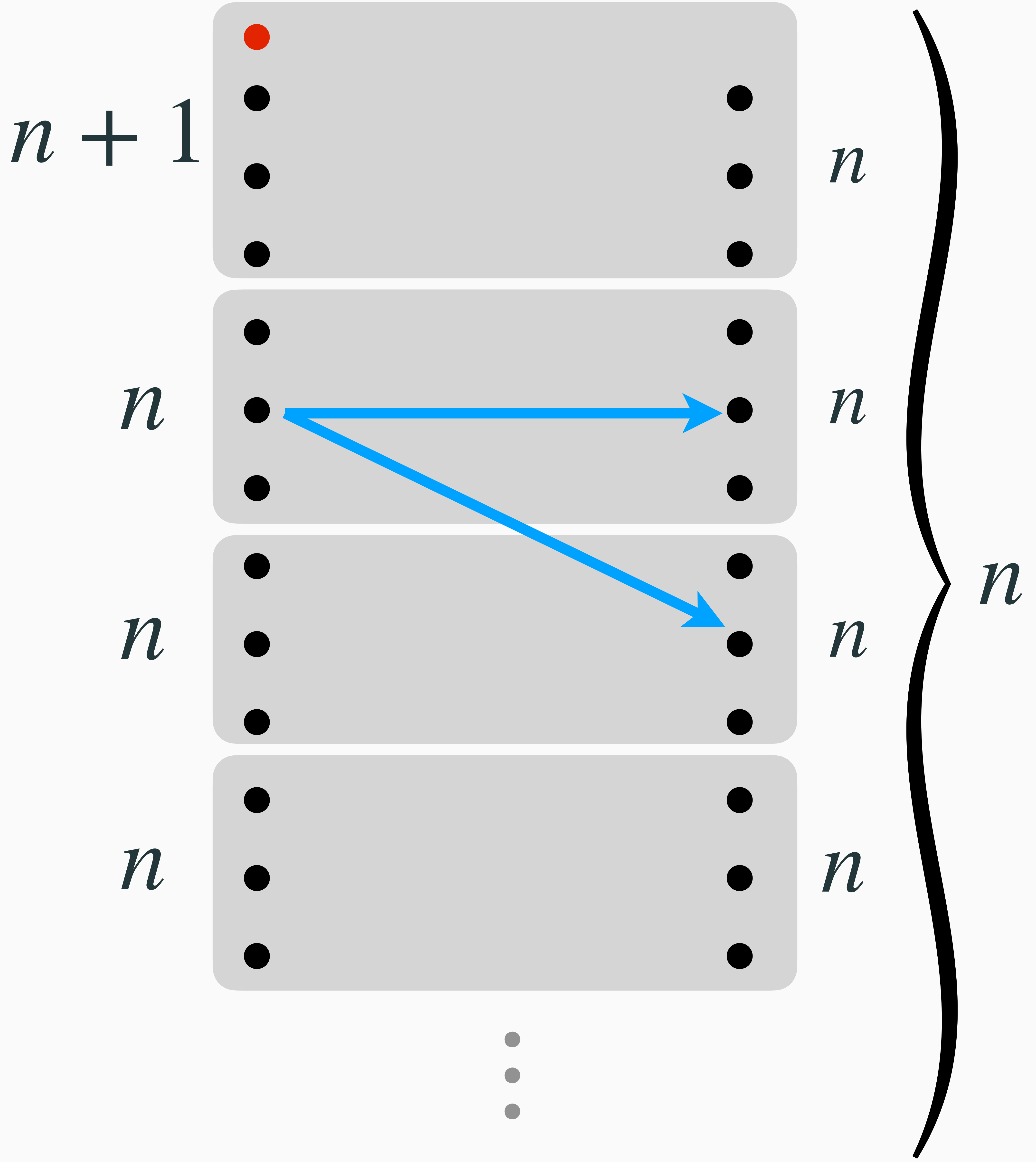
- Pigeons fly to holes in the same group or in some adjacent group.
- If a pigeon flies to the upper group it must fly twice.
- Holes can accept at most 1 pigeon coming from the same group or the lower group.
- Holes can accept at most 2 pigeons coming from the upper group.

Weighted PHP (*wt*PHP)



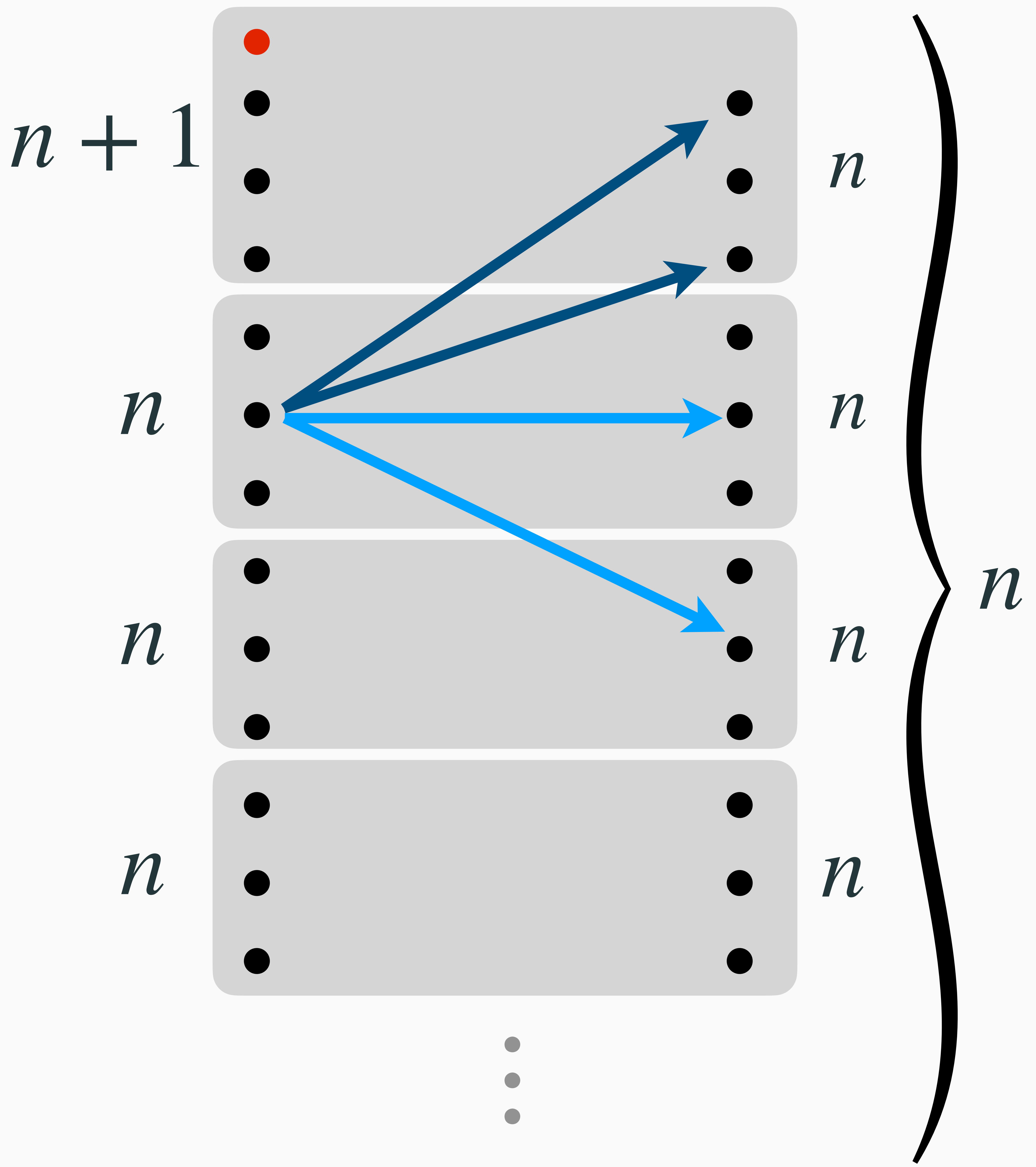
- Pigeons fly to holes in the same group or in some adjacent group.
- If a pigeon flies to the upper group it must fly twice.
- Holes can accept at most 1 pigeon coming from the same group or the lower group.
- Holes can accept at most 2 pigeons coming from the upper group.

Weighted PHP (*wt*PHP)



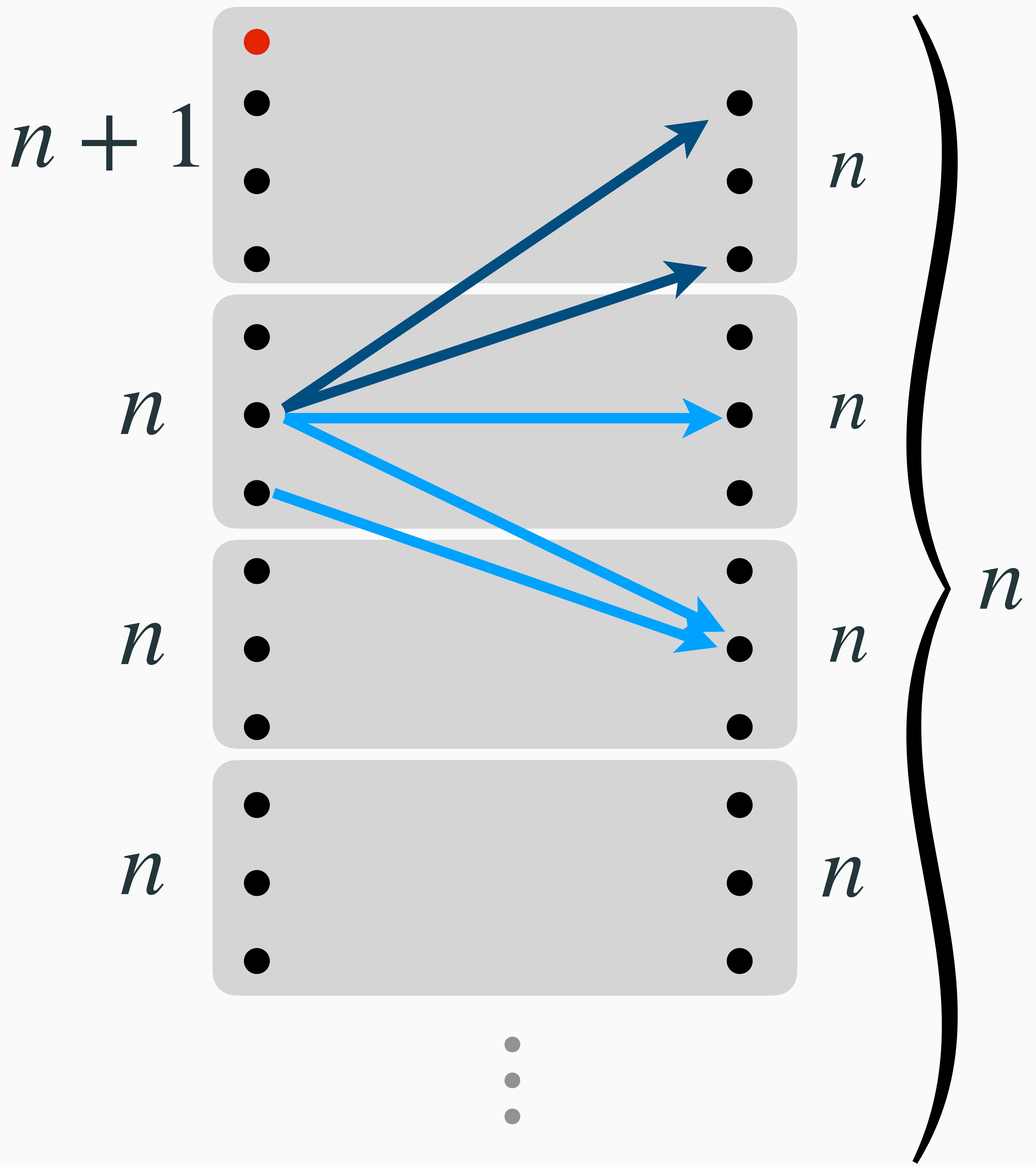
- Pigeons fly to holes in the same group or in some adjacent group.
- If a pigeon flies to the upper group it must fly twice.
- Holes can accept at most 1 pigeon coming from the same group or the lower group.
- Holes can accept at most 2 pigeons coming from the upper group.

Weighted PHP (*wt*PHP)



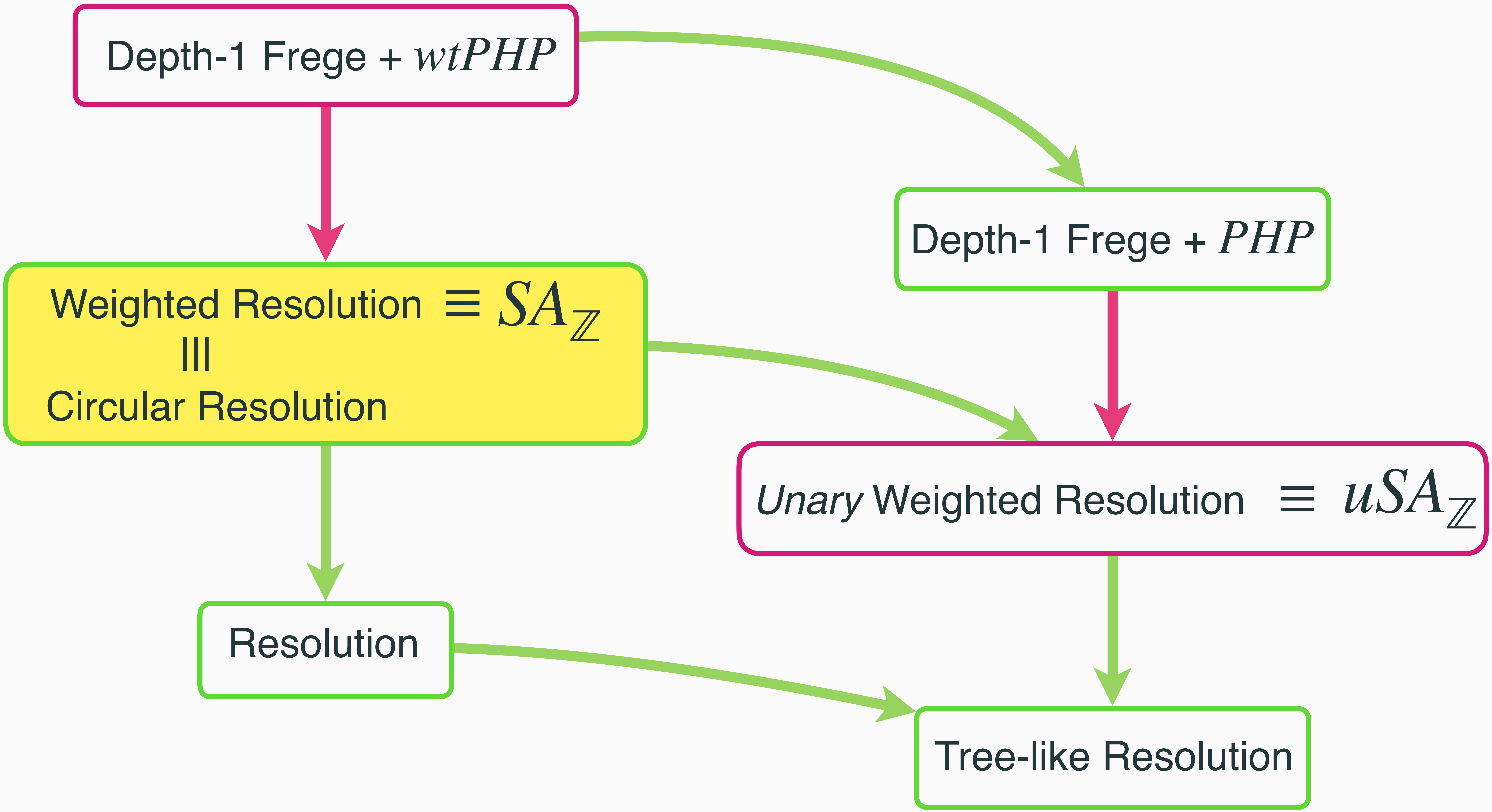
- Pigeons fly to holes in the same group or in some adjacent group.
- If a pigeon flies to the upper group it must fly twice.
- Holes can accept at most 1 pigeon coming from the same group or the lower group.
- Holes can accept at most 2 pigeons coming from the upper group.

Weighted PHP (*wt*PHP)



- Pigeons fly to holes in the same group or in some adjacent group.
- If a pigeon flies to the upper group it must fly twice.

- Holes can accept at most 1 pigeon coming from the same group or the lower group.
- Holes can accept at most 2 pigeons coming from the upper group.



Depth-1 Frege + $wtPHP$
Depth-1 Frege + PHP
Weighted Resolution $\equiv SA_{\mathbb{Z}}$
$\equiv$
Circular Resolution
Unary Weighted Resolution $\equiv uSA_{\mathbb{Z}}$
Resolution
Tree-like Resolution

Weighted Resolution Rules

$$F = \{(C_1, w_1),\ \ \ldots, (C_m, w_m)\} \text{ with } w_i \in \mathbb{Z}$$

Substitution Rules

$$\frac{(C \vee x, w) \qquad\qquad (C \vee \neg x, w)}{(C, w)} \updownarrow$$

$$\frac{}{(x \vee \neg x, w)} \text{ (excluded middle)}$$

Weighted Resolution Rules

$$F = \{(C_1, w_1), \ \ldots, (C_m, w_m)\} \text{ with } w_i \in \mathbb{Z}$$

Substitution Rules

$$\frac{(C \vee x, w) \qquad (C \vee \neg x, w)}{(C, w)} \updownarrow$$

$$\frac{(C, w_1 + w_2)}{(C, w_1) \qquad (C, w_2)} \updownarrow$$

$$\frac{}{(x \vee \neg x, w)} \text{ (excluded middle)}$$

$$\frac{}{(C, w) \qquad (C, -w)} \updownarrow$$

Weighted Resolution Rules

$$F = \{(C_1, w_1),\ \ldots, (C_m, w_m)\} \text{ with } w_i \in \mathbb{Z}$$

Substitution Rules

$$\frac{(C \vee x, w) \qquad (C \vee \neg x, w)}{(C, w)} \updownarrow$$

$$\frac{(C, w_1 + w_2)}{(C, w_1) \qquad (C, w_2)} \updownarrow$$

$$\frac{}{(x \vee \neg x, w)} \text{ (excluded middle)}$$

$$\frac{}{(C, w) \qquad (C, -w)} \updownarrow$$

The definition works equally well for bounded depth-Frege.

Weighted Resolution

$(C_1, w_1) \qquad (C_2, w_2) \qquad \dots \qquad (C_m, w_m)$

$(C_m \vee y, w_m) \qquad (C_m \vee \neg y, w_m)$

$(C \vee x, w) \qquad (C \vee \neg x, w)$

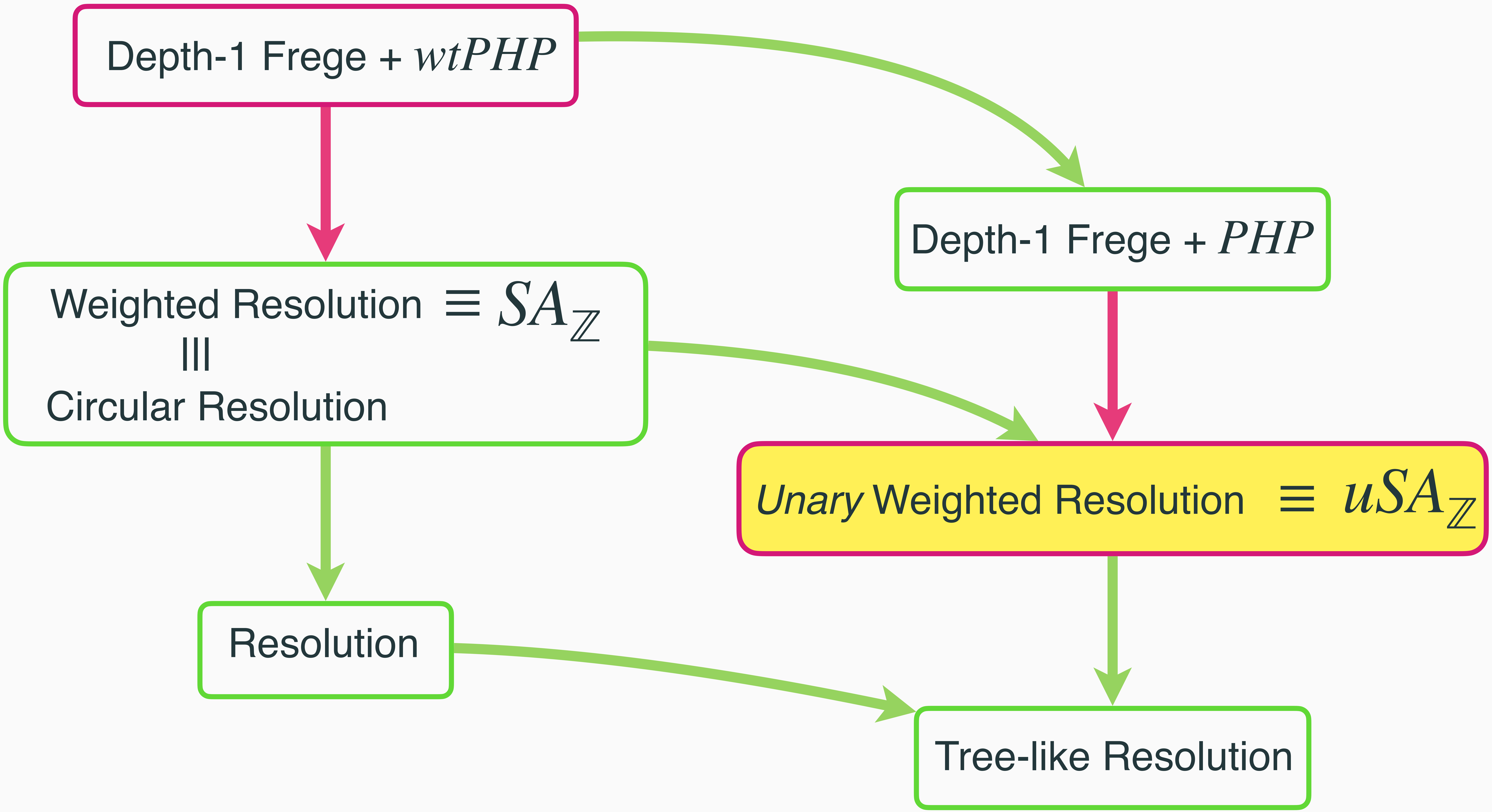
$(C, w) \qquad (C, -w)$

$(E, w) \qquad (E, -w)$

Only clauses with positive weights $\quad (\perp, m) \quad m > 0$

THM. $wtPHP$ is easy to refute in weighted resolution

THM. Weighted resolution is equivalent to circular resolution and $SA_{\mathbb{Z}}$, when clauses are encoded using the **multiplicative** encoding.


Depth-1 Frege + $wtPHP$
Depth-1 Frege + PHP
Weighted Resolution $\equiv SA_{\mathbb{Z}}$
$\equiv$
Circular Resolution
Unary Weighted Resolution $\equiv uSA_{\mathbb{Z}}$
Resolution
Tree-like Resolution

Unary Weighted Resolution

$(C_1, w_1) \quad (C_2, w_2) \quad \dots \quad (C_m, w_m)$

$(C_m \vee y, w_m) \quad (C_m \vee \neg y, w_m)$

$(C \vee x, w) \quad (C \vee \neg x, w)$

$(C, w) \quad (C, -w)$

No instances of the rule $\dfrac{(C, w_1 + w_2)}{(C, w_1) \qquad (C, w_2)} \updownarrow$

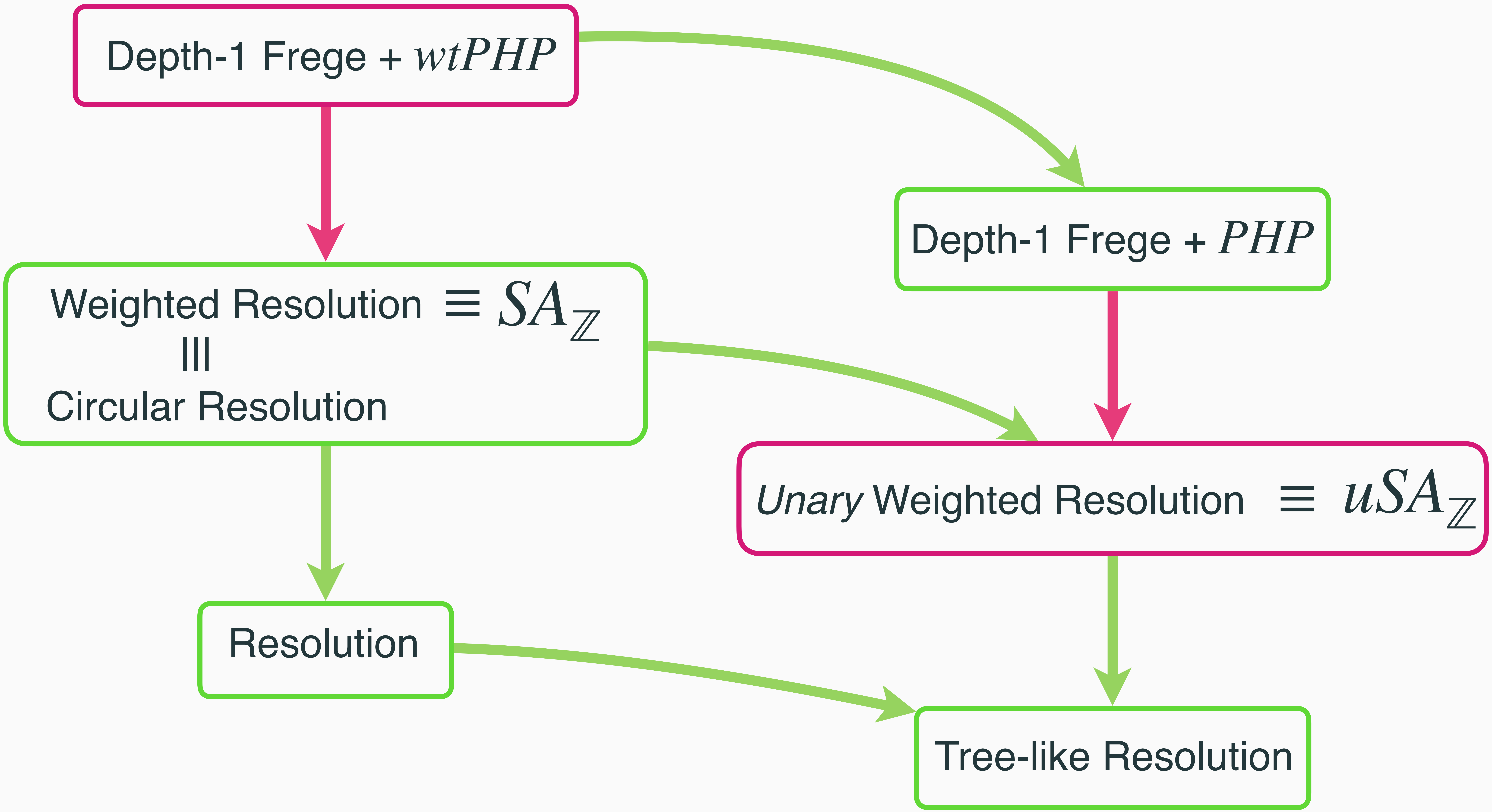
And weights in $\{\pm 1\}$

$(E, w) \quad (E, -w)$

Only clauses with positive weights $(\perp, 1) \dots (\perp, 1)$

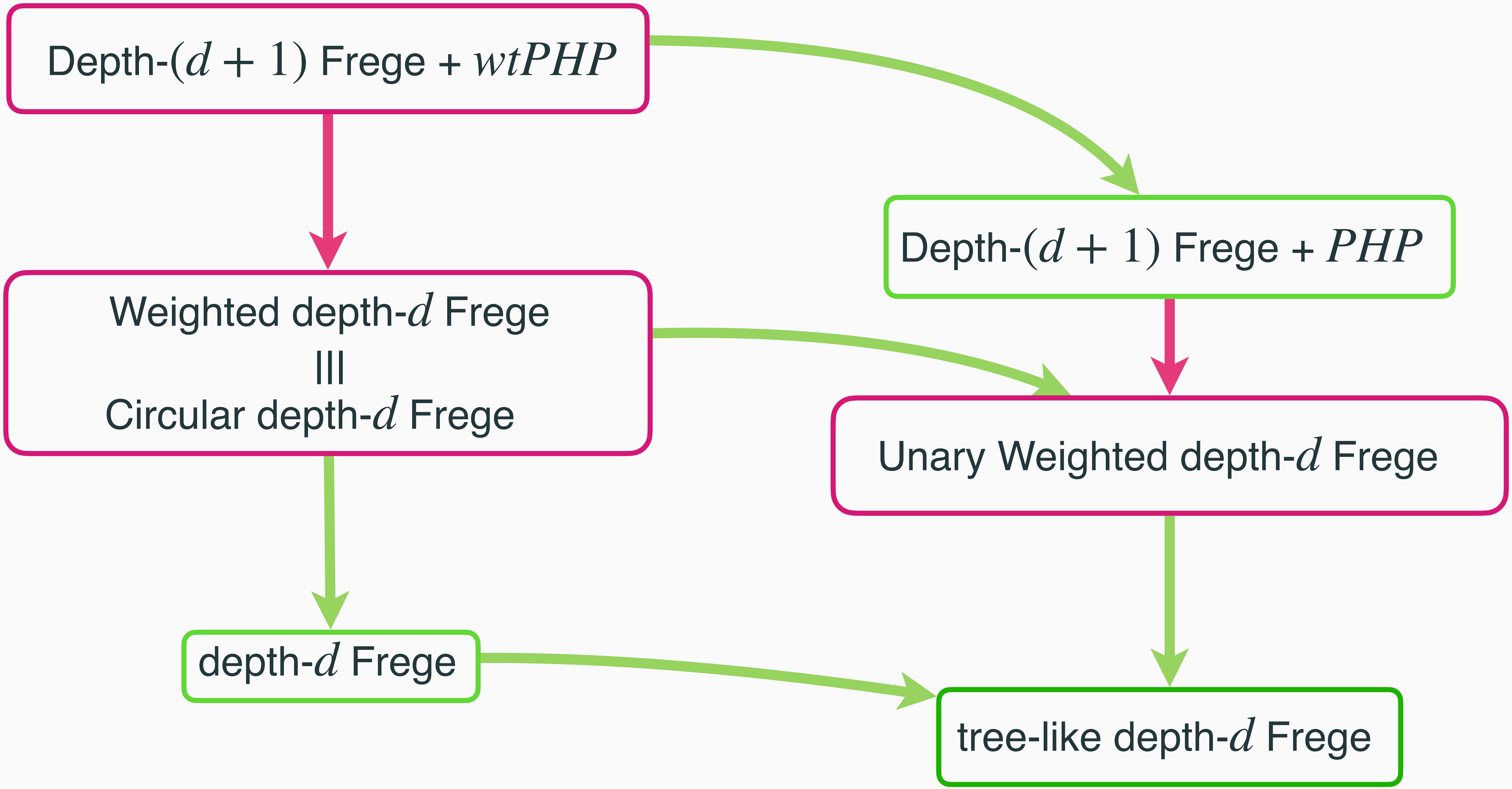
THM. PHP is easy to refute in unary weighted resolution

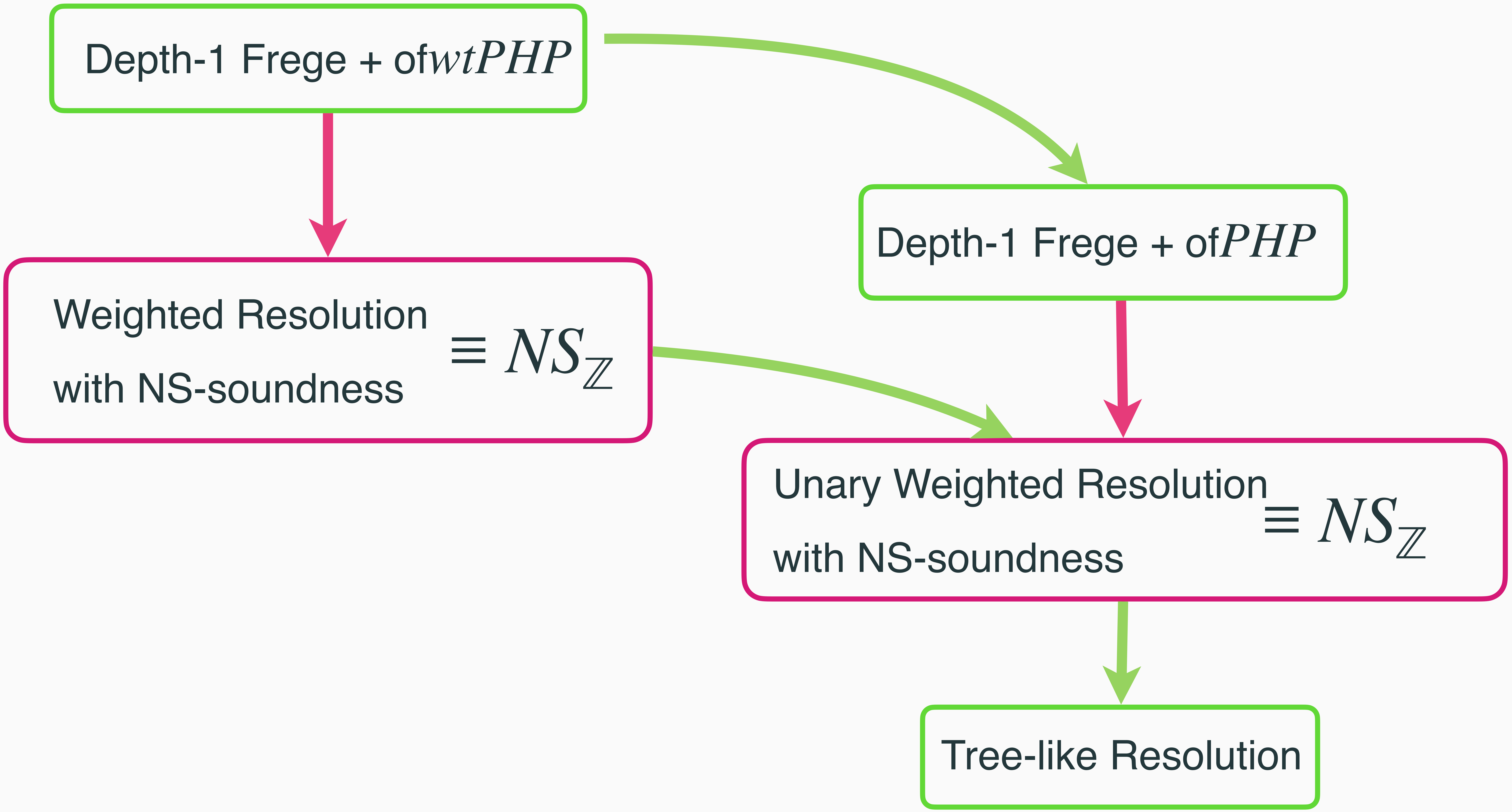
THM. Unary weighted resolution is equivalent to unary $SA_{\mathbb{Z}}$, when clauses are encoded using the **multiplicative** encoding.


Depth-1 Frege + $wtPHP$
Depth-1 Frege + PHP
Weighted Resolution $\equiv SA_{\mathbb{Z}}$
III
Circular Resolution
Unary Weighted Resolution $\equiv uSA_{\mathbb{Z}}$
Resolution
Tree-like Resolution

In the paper but not in this talk

- More detailed version of the simulations for SA (PHP over a graph, degree-width, etc)
- Analogous p-simulations for Nullstellensatz
- Analogous p-simulations for depth-d Frege


Depth-$(d+1)$ Frege + $wtPHP$
Depth-$(d+1)$ Frege + PHP
Weighted depth-d Frege
|||
Circular depth-d Frege
Unary Weighted depth-d Frege
depth-d Frege
tree-like depth-d Frege



Depth-1 Frege + of$wtPHP$
Depth-1 Frege + ofPHP
Weighted Resolution with NS-soundness $\equiv NS_{\mathbb{Z}}$
Unary Weighted Resolution with NS-soundness $\equiv NS_{\mathbb{Z}}$
Tree-like Resolution

Thanks!

Questions?

bonacina@cs.upc.edu