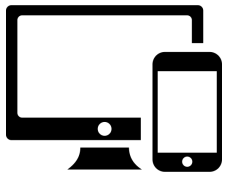
Spain: Succinct proofs for numerical computations

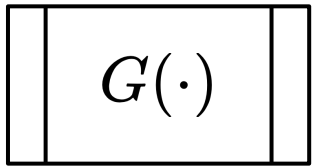
Zachary DeStefano, Noah Golub, Zile Huang,
Julius Zhang, Sam Frank, Michael Walfish



Succinct proof systems are powerful

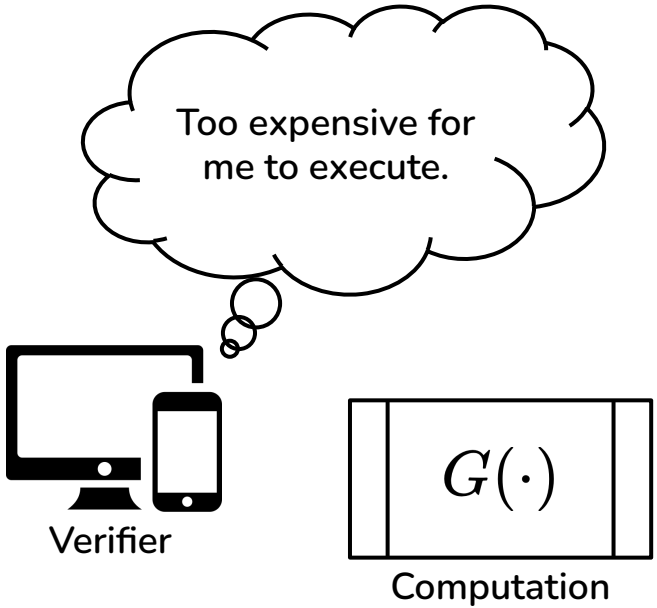


Verifier

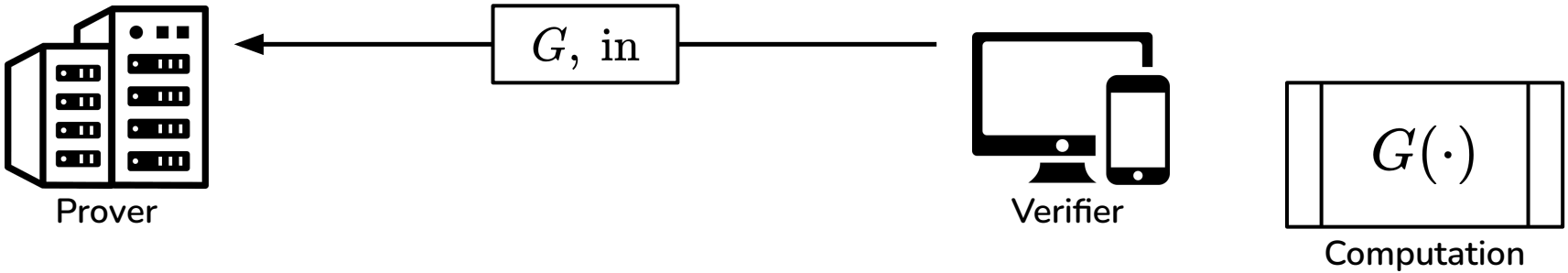


Computation

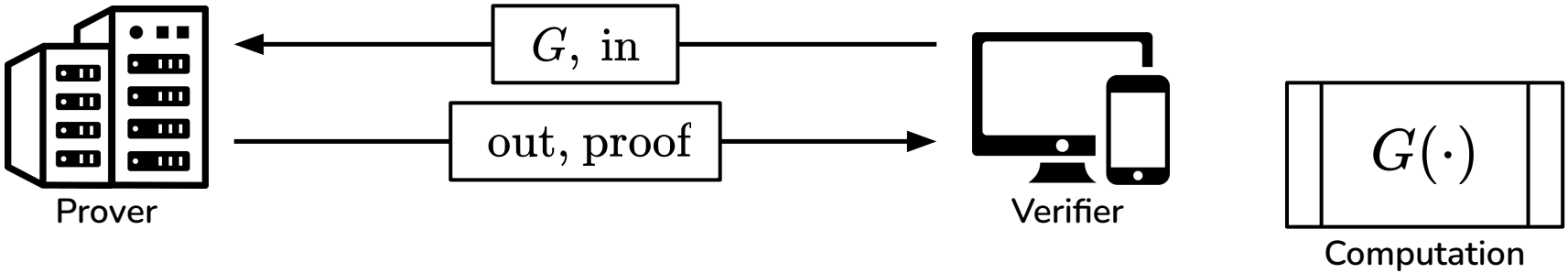
Succinct proof systems are powerful



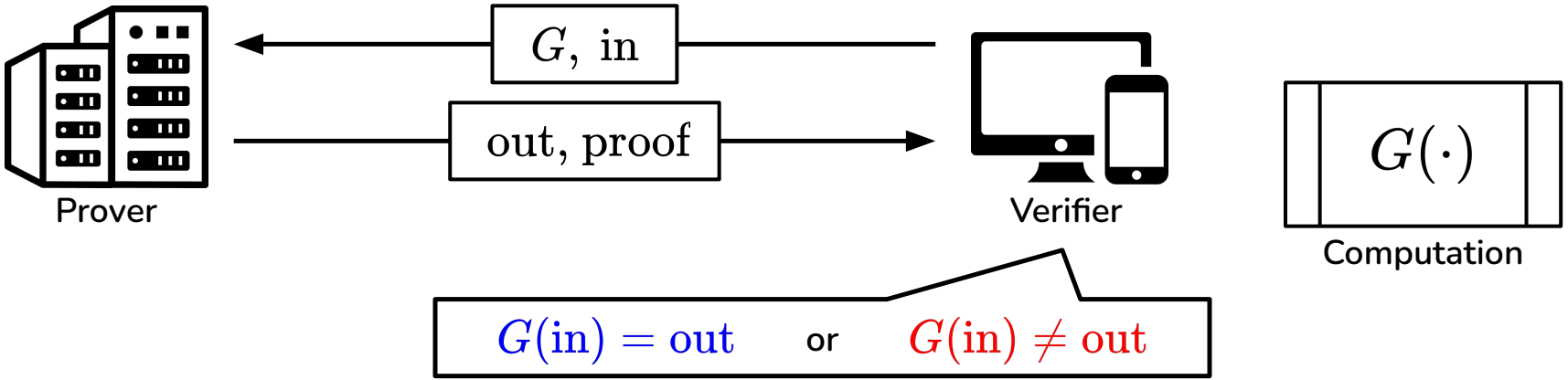
Succinct proof systems are powerful



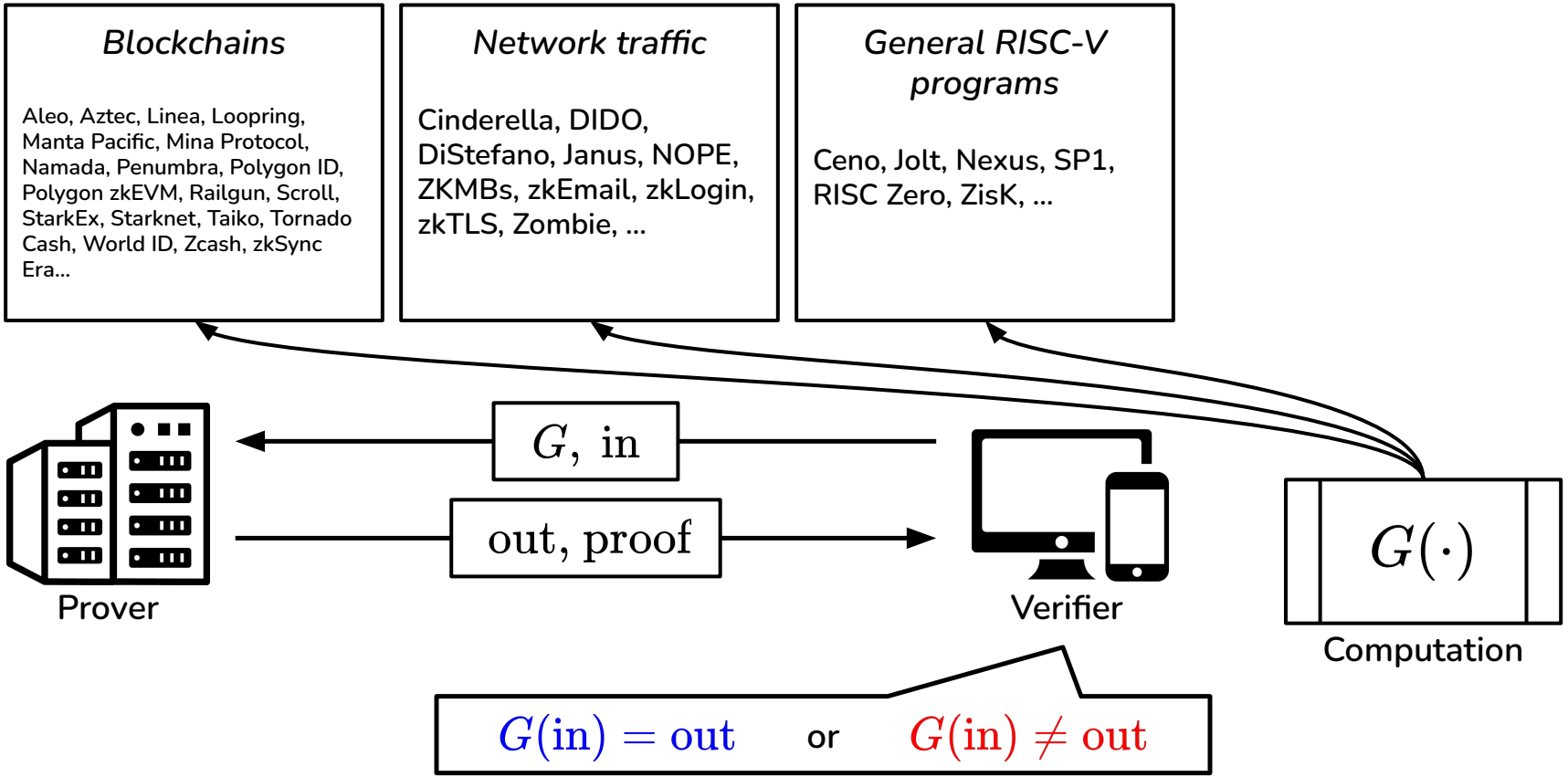
Succinct proof systems are powerful



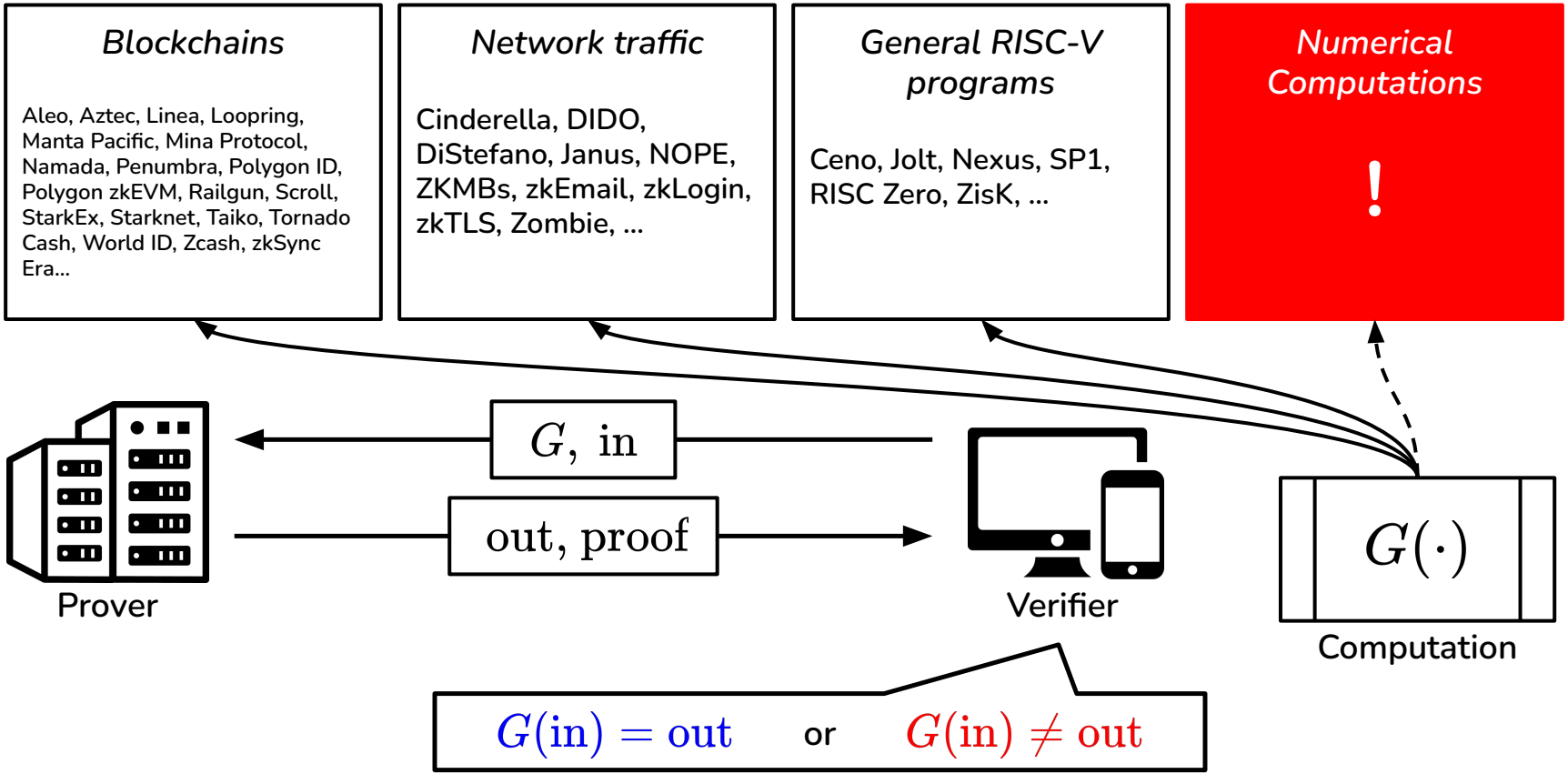
Succinct proof systems are powerful



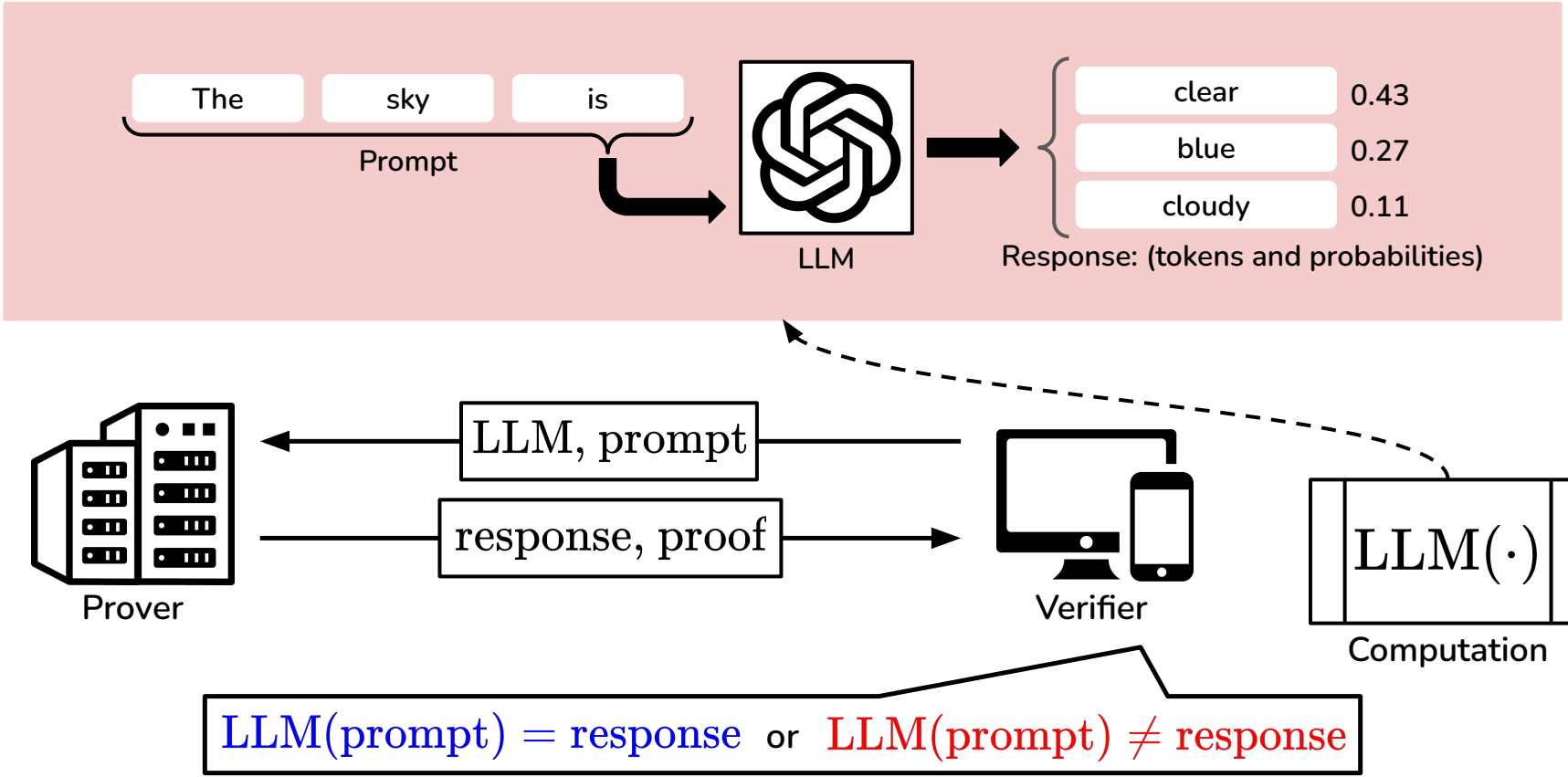
Succinct proof systems are powerful (and increasingly relevant in practice)



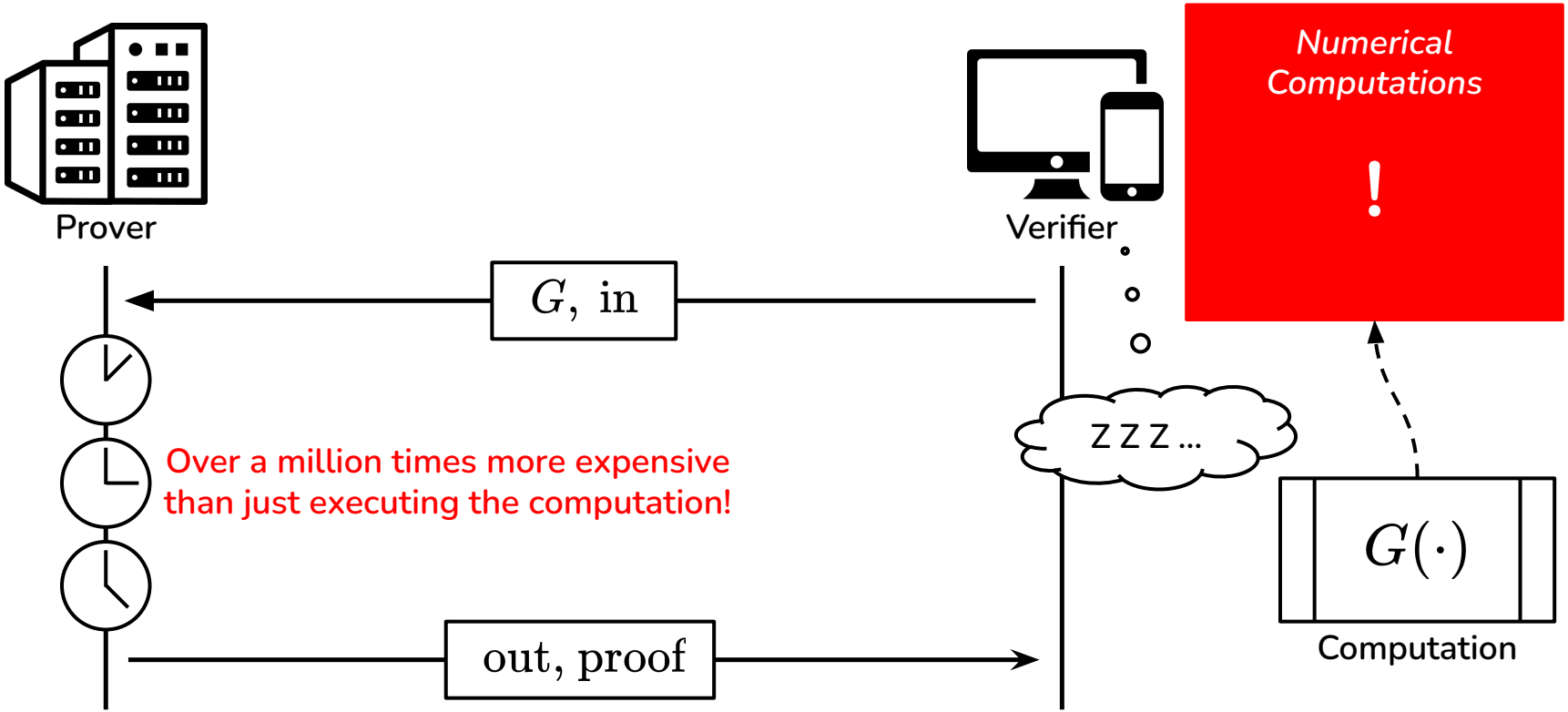
It is difficult to produce succinct proofs of numerical computations



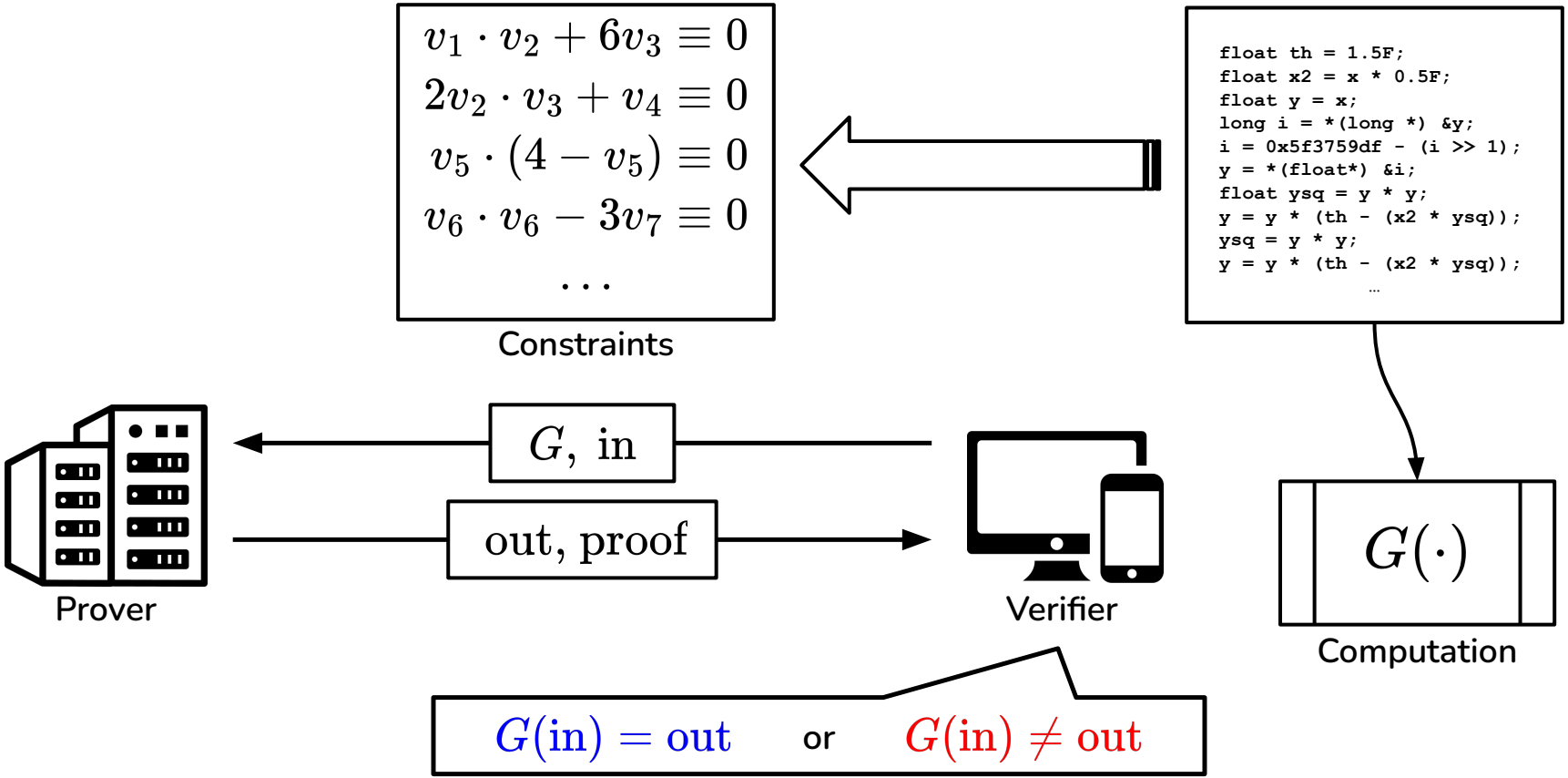
Succinct proofs of numerical programs enable new applications



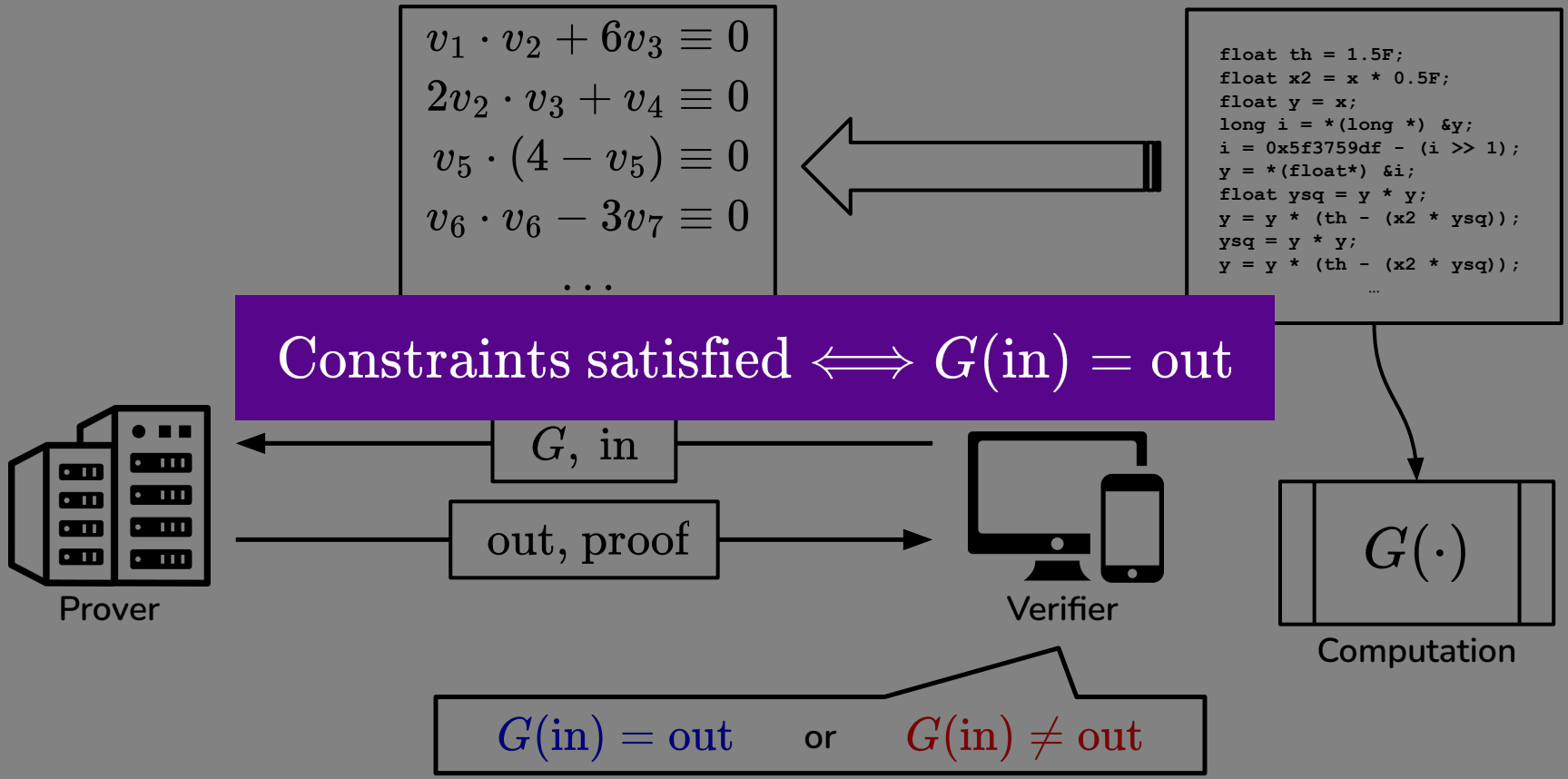
Succinct proof generation is expensive!



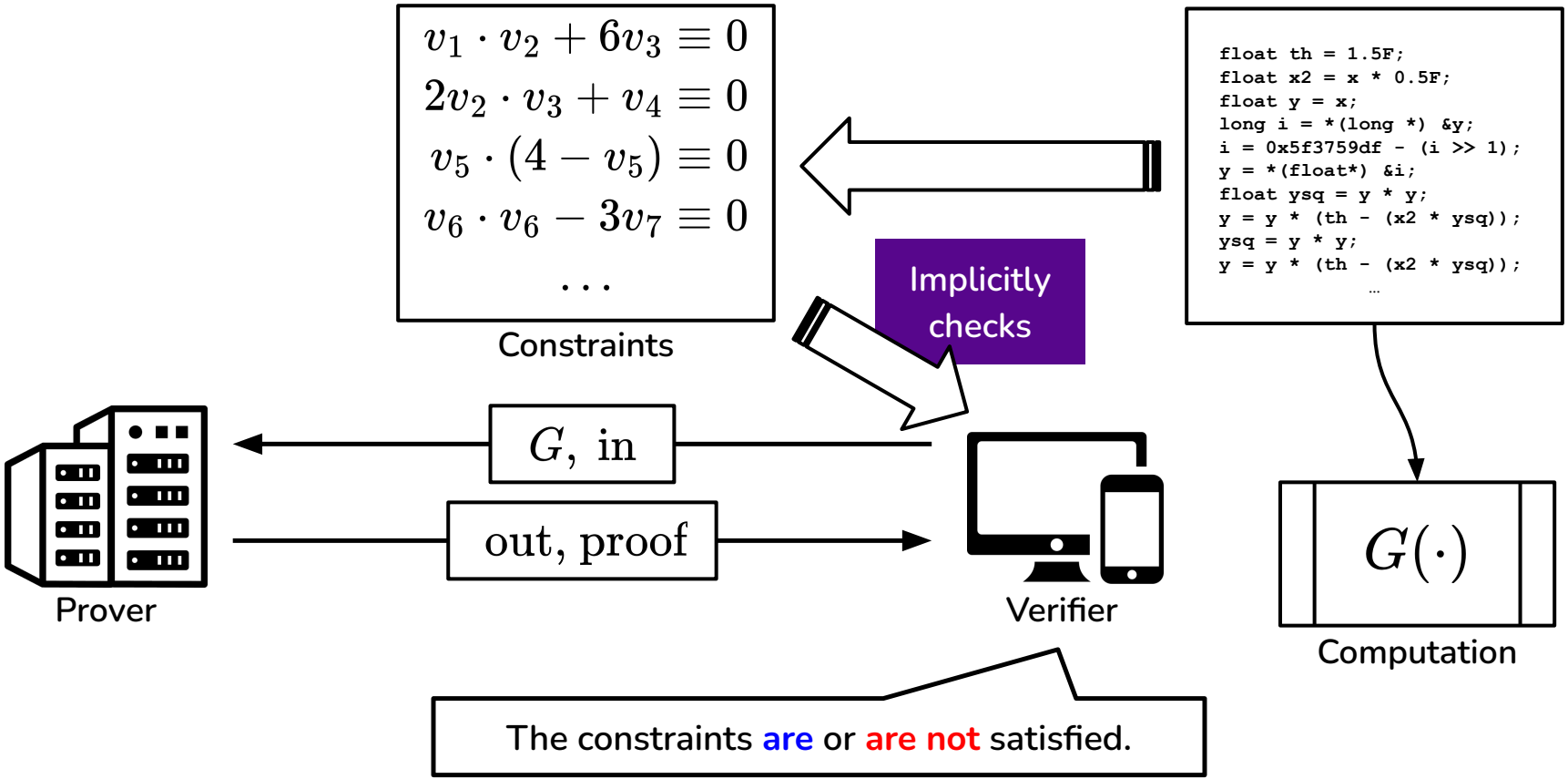
Constraints are the language of proof systems



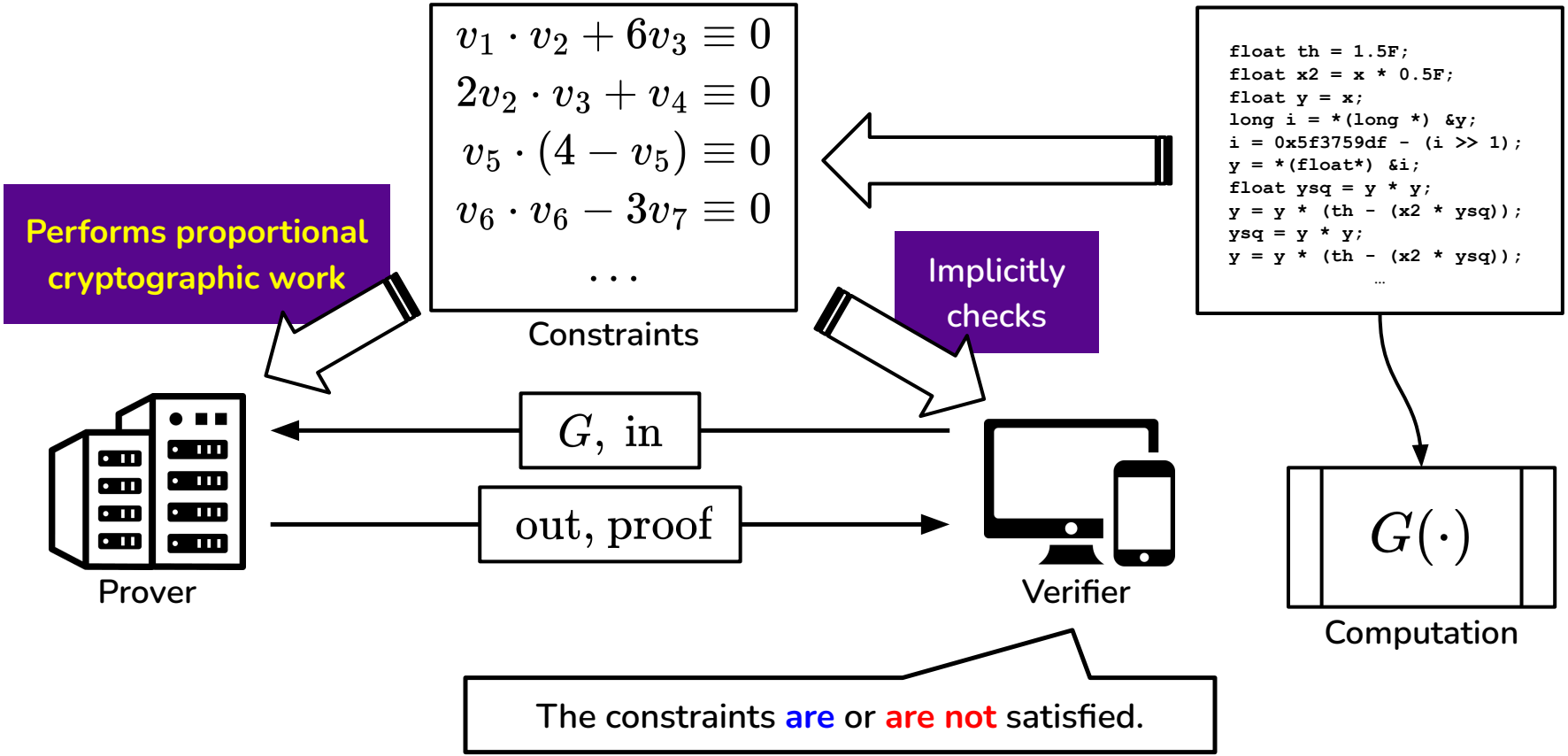
Constraints are the language of proof systems



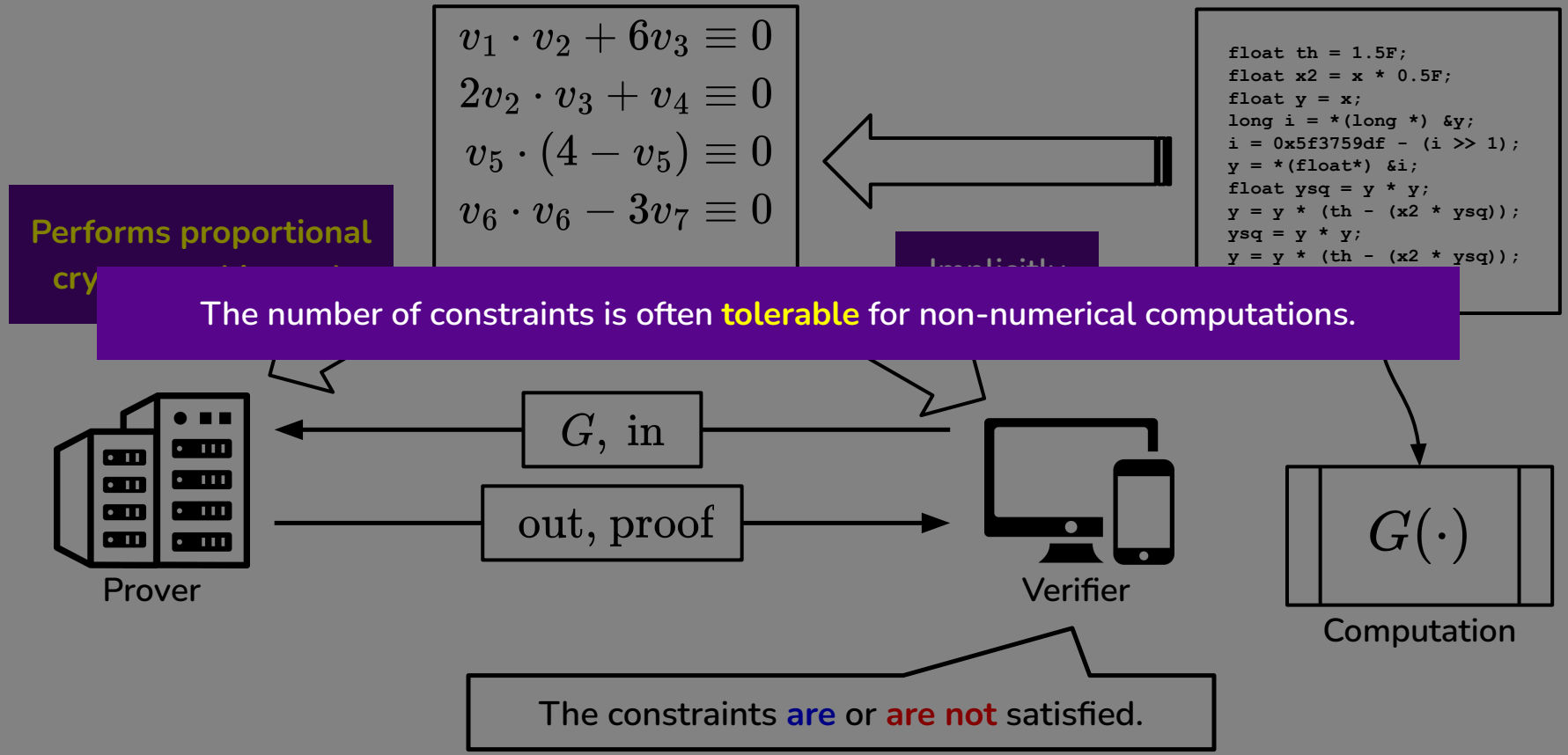
Constraints are the language of proof systems



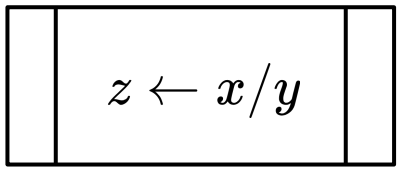
Constraints are the language of proof systems



Constraints are the language of proof systems

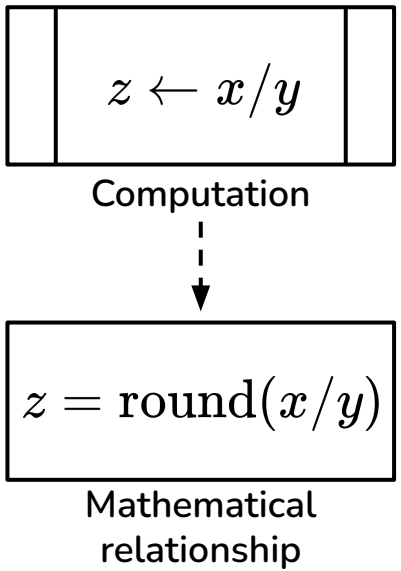


Every numerical operation requires a plethora of constraints

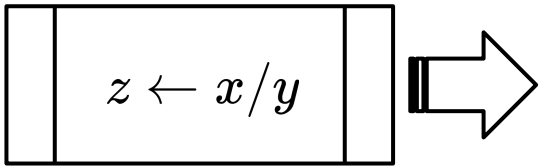


Computation

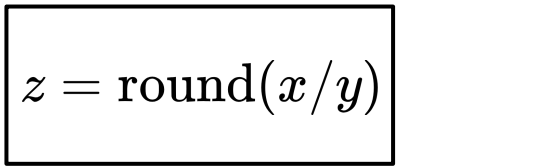
Every numerical operation requires a plethora of constraints



Every numerical operation requires a plethora of constraints



Computation

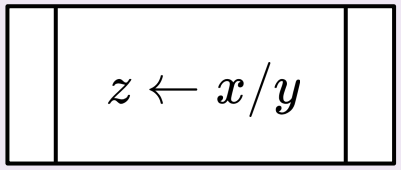


Mathematical relationship

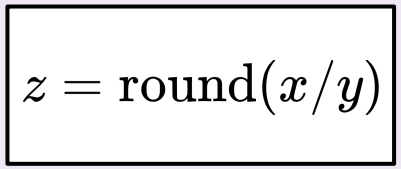
$$
\begin{array}{lllll}
y \cdot z - (x - r) \equiv 0 & s_{13} \cdot (1 - s_{13}) \equiv 0 & s_{27} \cdot (1 - s_{27}) \equiv 0 & t_8 \cdot (1 - t_8) \equiv 0 & t_{22} \cdot (1 - t_{22}) \equiv 0 \\
s_0 \cdot (1 - s_0) \equiv 0 & s_{14} \cdot (1 - s_{14}) \equiv 0 & s_{28} \cdot (1 - s_{28}) \equiv 0 & t_9 \cdot (1 - t_9) \equiv 0 & t_{23} \cdot (1 - t_{23}) \equiv 0 \\
s_1 \cdot (1 - s_1) \equiv 0 & s_{15} \cdot (1 - s_{15}) \equiv 0 & s_{29} \cdot (1 - s_{29}) \equiv 0 & t_{10} \cdot (1 - t_{10}) \equiv 0 & t_{24} \cdot (1 - t_{24}) \equiv 0 \\
s_2 \cdot (1 - s_2) \equiv 0 & s_{16} \cdot (1 - s_{16}) \equiv 0 & s_{30} \cdot (1 - s_{30}) \equiv 0 & t_{11} \cdot (1 - t_{11}) \equiv 0 & t_{25} \cdot (1 - t_{25}) \equiv 0 \\
s_3 \cdot (1 - s_3) \equiv 0 & s_{17} \cdot (1 - s_{17}) \equiv 0 & s_{31} \cdot (1 - s_{31}) \equiv 0 & t_{12} \cdot (1 - t_{12}) \equiv 0 & t_{26} \cdot (1 - t_{26}) \equiv 0 \\
s_4 \cdot (1 - s_4) \equiv 0 & s_{18} \cdot (1 - s_{18}) \equiv 0 & y - r - \sum_i 2^i s_i \equiv 0 & t_{13} \cdot (1 - t_{13}) \equiv 0 & t_{27} \cdot (1 - t_{27}) \equiv 0 \\
s_5 \cdot (1 - s_5) \equiv 0 & s_{19} \cdot (1 - s_{19}) \equiv 0 & t_0 \cdot (1 - t_0) \equiv 0 & t_{14} \cdot (1 - t_{14}) \equiv 0 & t_{28} \cdot (1 - t_{28}) \equiv 0 \\
s_6 \cdot (1 - s_6) \equiv 0 & s_{20} \cdot (1 - s_{20}) \equiv 0 & t_1 \cdot (1 - t_1) \equiv 0 & t_{15} \cdot (1 - t_{15}) \equiv 0 & t_{29} \cdot (1 - t_{29}) \equiv 0 \\
s_7 \cdot (1 - s_7) \equiv 0 & s_{21} \cdot (1 - s_{21}) \equiv 0 & t_2 \cdot (1 - t_2) \equiv 0 & t_{16} \cdot (1 - t_{16}) \equiv 0 & t_{30} \cdot (1 - t_{30}) \equiv 0 \\
s_8 \cdot (1 - s_8) \equiv 0 & s_{22} \cdot (1 - s_{22}) \equiv 0 & t_3 \cdot (1 - t_3) \equiv 0 & t_{17} \cdot (1 - t_{17}) \equiv 0 & t_{31} \cdot (1 - t_{31}) \equiv 0 \\
s_9 \cdot (1 - s_9) \equiv 0 & s_{23} \cdot (1 - s_{23}) \equiv 0 & t_4 \cdot (1 - t_4) \equiv 0 & t_{18} \cdot (1 - t_{18}) \equiv 0 & z - \sum_i 2^i t_i \equiv 0 \\
s_{10} \cdot (1 - s_{10}) \equiv 0 & s_{24} \cdot (1 - s_{24}) \equiv 0 & t_5 \cdot (1 - t_5) \equiv 0 & t_{19} \cdot (1 - t_{19}) \equiv 0 & \\
s_{11} \cdot (1 - s_{11}) \equiv 0 & s_{25} \cdot (1 - s_{25}) \equiv 0 & t_6 \cdot (1 - t_6) \equiv 0 & t_{20} \cdot (1 - t_{20}) \equiv 0 & \\
s_{12} \cdot (1 - s_{12}) \equiv 0 & s_{26} \cdot (1 - s_{26}) \equiv 0 & t_7 \cdot (1 - t_7) \equiv 0 & t_{21} \cdot (1 - t_{21}) \equiv 0 &
\end{array}
$$

Constraints

Every numerical operation requires a plethora of constraints



Computation



Mathematical relationship

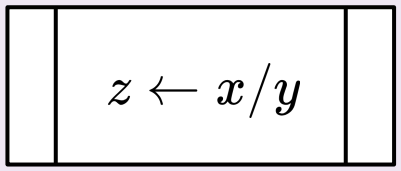
Approximate rational arithmetic: $\mathbb{Q}$

$$
\begin{array}{lllll}
y \cdot z - (x - r) \equiv 0 & s_{13} \cdot (1 - s_{13}) \equiv 0 & s_{27} \cdot (1 - s_{27}) \equiv 0 & t_8 \cdot (1 - t_8) \equiv 0 & t_{22} \cdot (1 - t_{22}) \equiv 0 \\
s_0 \cdot (1 - s_0) \equiv 0 & s_{14} \cdot (1 - s_{14}) \equiv 0 & s_{28} \cdot (1 - s_{28}) \equiv 0 & t_9 \cdot (1 - t_9) \equiv 0 & t_{23} \cdot (1 - t_{23}) \equiv 0 \\
s_1 \cdot (1 - s_1) \equiv 0 & s_{15} \cdot (1 - s_{15}) \equiv 0 & s_{29} \cdot (1 - s_{29}) \equiv 0 & t_{10} \cdot (1 - t_{10}) \equiv 0 & t_{24} \cdot (1 - t_{24}) \equiv 0 \\
s_2 \cdot (1 - s_2) \equiv 0 & s_{16} \cdot (1 - s_{16}) \equiv 0 & s_{30} \cdot (1 - s_{30}) \equiv 0 & t_{11} \cdot (1 - t_{11}) \equiv 0 & t_{25} \cdot (1 - t_{25}) \equiv 0 \\
s_3 \cdot (1 - s_3) \equiv 0 & s_{17} \cdot (1 - s_{17}) \equiv 0 & s_{31} \cdot (1 - s_{31}) \equiv 0 & t_{12} \cdot (1 - t_{12}) \equiv 0 & t_{26} \cdot (1 - t_{26}) \equiv 0 \\
s_4 \cdot (1 - s_4) \equiv 0 & s_{18} \cdot (1 - s_{18}) \equiv 0 & y - r - \sum_i 2^i s_i \equiv 0 & t_{13} \cdot (1 - t_{13}) \equiv 0 & t_{27} \cdot (1 - t_{27}) \equiv 0 \\
s_5 \cdot (1 - s_5) \equiv 0 & s_{19} \cdot (1 - s_{19}) \equiv 0 & t_0 \cdot (1 - t_0) \equiv 0 & t_{14} \cdot (1 - t_{14}) \equiv 0 & t_{28} \cdot (1 - t_{28}) \equiv 0 \\
s_6 \cdot (1 - s_6) \equiv 0 & s_{20} \cdot (1 - s_{20}) \equiv 0 & t_1 \cdot (1 - t_1) \equiv 0 & t_{15} \cdot (1 - t_{15}) \equiv 0 & t_{29} \cdot (1 - t_{29}) \equiv 0 \\
s_7 \cdot (1 - s_7) \equiv 0 & s_{21} \cdot (1 - s_{21}) \equiv 0 & t_2 \cdot (1 - t_2) \equiv 0 & t_{16} \cdot (1 - t_{16}) \equiv 0 & t_{30} \cdot (1 - t_{30}) \equiv 0 \\
s_8 \cdot (1 - s_8) \equiv 0 & s_{22} \cdot (1 - s_{22}) \equiv 0 & t_3 \cdot (1 - t_3) \equiv 0 & t_{17} \cdot (1 - t_{17}) \equiv 0 & t_{31} \cdot (1 - t_{31}) \equiv 0 \\
s_9 \cdot (1 - s_9) \equiv 0 & s_{23} \cdot (1 - s_{23}) \equiv 0 & t_4 \cdot (1 - t_4) \equiv 0 & t_{18} \cdot (1 - t_{18}) \equiv 0 & z - \sum_i 2^i t_i \equiv 0 \\
s_{10} \cdot (1 - s_{10}) \equiv 0 & s_{24} \cdot (1 - s_{24}) \equiv 0 & t_5 \cdot (1 - t_5) \equiv 0 & t_{19} \cdot (1 - t_{19}) \equiv 0 & \\
s_{11} \cdot (1 - s_{11}) \equiv 0 & s_{25} \cdot (1 - s_{25}) \equiv 0 & t_6 \cdot (1 - t_6) \equiv 0 & t_{20} \cdot (1 - t_{20}) \equiv 0 & \\
s_{12} \cdot (1 - s_{12}) \equiv 0 & s_{26} \cdot (1 - s_{26}) \equiv 0 & t_7 \cdot (1 - t_7) \equiv 0 & t_{21} \cdot (1 - t_{21}) \equiv 0 &
\end{array}
$$

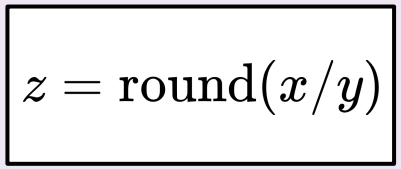
Constraints

Equations over a finite field: $\mathbb{F}_q$

Every numerical operation requires a plethora of constraints



Computation



Mathematical relationship

Approximate rational arithmetic: $\mathbb{Q}$

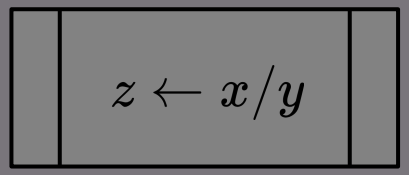
$$
\begin{array}{lllll}
y \cdot z - (x - r) \equiv 0 & s_{13} \cdot (1 - s_{13}) \equiv 0 & s_{27} \cdot (1 - s_{27}) \equiv 0 & t_8 \cdot (1 - t_8) \equiv 0 & t_{22} \cdot (1 - t_{22}) \equiv 0 \\
s_0 \cdot (1 - s_0) \equiv 0 & s_{14} \cdot (1 - s_{14}) \equiv 0 & s_{28} \cdot (1 - s_{28}) \equiv 0 & t_9 \cdot (1 - t_9) \equiv 0 & t_{23} \cdot (1 - t_{23}) \equiv 0 \\
s_1 \cdot (1 - s_1) \equiv 0 & s_{15} \cdot (1 - s_{15}) \equiv 0 & s_{29} \cdot (1 - s_{29}) \equiv 0 & t_{10} \cdot (1 - t_{10}) \equiv 0 & t_{24} \cdot (1 - t_{24}) \equiv 0 \\
s_2 \cdot (1 - s_2) \equiv 0 & s_{16} \cdot (1 - s_{16}) \equiv 0 & s_{30} \cdot (1 - s_{30}) \equiv 0 & t_{11} \cdot (1 - t_{11}) \equiv 0 & t_{25} \cdot (1 - t_{25}) \equiv 0 \\
s_3 \cdot (1 - s_3) \equiv 0 & s_{17} \cdot (1 - s_{17}) \equiv 0 & s_{31} \cdot (1 - s_{31}) \equiv 0 & t_{12} \cdot (1 - t_{12}) \equiv 0 & t_{26} \cdot (1 - t_{26}) \equiv 0 \\
s_4 \cdot (1 - s_4) \equiv 0 & s_{18} \cdot (1 - s_{18}) \equiv 0 & y - r - \sum_i 2^i s_i \equiv 0 & t_{13} \cdot (1 - t_{13}) \equiv 0 & t_{27} \cdot (1 - t_{27}) \equiv 0 \\
s_5 \cdot (1 - s_5) \equiv 0 & s_{19} \cdot (1 - s_{19}) \equiv 0 & t_0 \cdot (1 - t_0) \equiv 0 & t_{14} \cdot (1 - t_{14}) \equiv 0 & t_{28} \cdot (1 - t_{28}) \equiv 0 \\
s_6 \cdot (1 - s_6) \equiv 0 & s_{20} \cdot (1 - s_{20}) \equiv 0 & t_1 \cdot (1 - t_1) \equiv 0 & t_{15} \cdot (1 - t_{15}) \equiv 0 & t_{29} \cdot (1 - t_{29}) \equiv 0 \\
s_7 \cdot (1 - s_7) \equiv 0 & s_{21} \cdot (1 - s_{21}) \equiv 0 & t_2 \cdot (1 - t_2) \equiv 0 & t_{16} \cdot (1 - t_{16}) \equiv 0 & t_{30} \cdot (1 - t_{30}) \equiv 0 \\
s_8 \cdot (1 - s_8) \equiv 0 & s_{22} \cdot (1 - s_{22}) \equiv 0 & t_3 \cdot (1 - t_3) \equiv 0 & t_{17} \cdot (1 - t_{17}) \equiv 0 & t_{31} \cdot (1 - t_{31}) \equiv 0 \\
s_9 \cdot (1 - s_9) \equiv 0 & s_{23} \cdot (1 - s_{23}) \equiv 0 & t_4 \cdot (1 - t_4) \equiv 0 & t_{18} \cdot (1 - t_{18}) \equiv 0 & z - \sum_i 2^i t_i \equiv 0 \\
s_{10} \cdot (1 - s_{10}) \equiv 0 & s_{24} \cdot (1 - s_{24}) \equiv 0 & t_5 \cdot (1 - t_5) \equiv 0 & t_{19} \cdot (1 - t_{19}) \equiv 0 & \\
s_{11} \cdot (1 - s_{11}) \equiv 0 & s_{25} \cdot (1 - s_{25}) \equiv 0 & t_6 \cdot (1 - t_6) \equiv 0 & t_{20} \cdot (1 - t_{20}) \equiv 0 & \\
s_{12} \cdot (1 - s_{12}) \equiv 0 & s_{26} \cdot (1 - s_{26}) \equiv 0 & t_7 \cdot (1 - t_7) \equiv 0 & t_{21} \cdot (1 - t_{21}) \equiv 0 &
\end{array}
$$

Constraints

Equations over a finite field: $\mathbb{F}_q$

Arithmetic behaves differently over a finite field versus the rationals.
For example, over $\mathbb{F}_{103}$ it is the case that $3/2 \equiv 53$.

Every numerical operation requires a plethora of constraints



Computation

$z = \mathrm{round}(x/y)$

Mathematical relationship

Approximate rational arithmetic: $\mathbb{Q}$

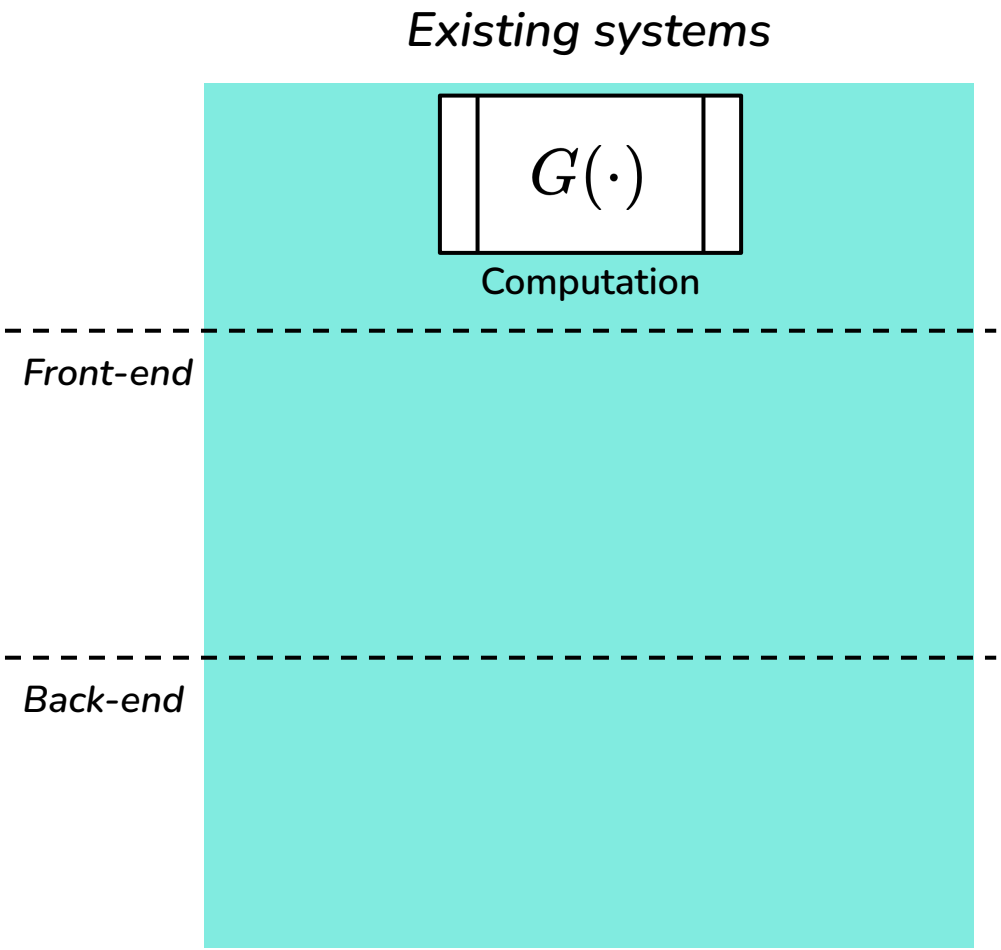
$$
\begin{array}{lllll}
y \cdot z - (x - r) \equiv 0 & s_{13} \cdot (1 - s_{13}) \equiv 0 & s_{27} \cdot (1 - s_{27}) \equiv 0 & t_8 \cdot (1 - t_8) \equiv 0 & t_{22} \cdot (1 - t_{22}) \equiv 0 \\
s_0 \cdot (1 - s_0) \equiv 0 & s_{14} \cdot (1 - s_{14}) \equiv 0 & s_{28} \cdot (1 - s_{28}) \equiv 0 & t_9 \cdot (1 - t_9) \equiv 0 & t_{23} \cdot (1 - t_{23}) \equiv 0 \\
s_1 \cdot (1 - s_1) \equiv 0 & s_{15} \cdot (1 - s_{15}) \equiv 0 & s_{29} \cdot (1 - s_{29}) \equiv 0 & t_{10} \cdot (1 - t_{10}) \equiv 0 & t_{24} \cdot (1 - t_{24}) \equiv 0 \\
s_2 \cdot (1 - s_2) \equiv 0 & s_{16} \cdot (1 - s_{16}) \equiv 0 & s_{30} \cdot (1 - s_{30}) \equiv 0 & t_{11} \cdot (1 - t_{11}) \equiv 0 & t_{25} \cdot (1 - t_{25}) \equiv 0 \\
s_3 \cdot (1 - s_3) \equiv 0 & s_{17} \cdot (1 - s_{17}) \equiv 0 & s_{31} \cdot (1 - s_{31}) \equiv 0 & t_{12} \cdot (1 - t_{12}) \equiv 0 & t_{26} \cdot (1 - t_{26}) \equiv 0 \\
s_4 \cdot (1 - s_4) \equiv 0 & s_{18} \cdot (1 - s_{18}) \equiv 0 & y - r - \sum_i 2^i s_i \equiv 0 & t_{13} \cdot (1 - t_{13}) \equiv 0 & t_{27} \cdot (1 - t_{27}) \equiv 0 \\
s_5 \cdot (1 - s_5) \equiv 0 & s_{19} \cdot (1 - s_{19}) \equiv 0 & t_0 \cdot (1 - t_0) \equiv 0 & t_{14} \cdot (1 - t_{14}) \equiv 0 & t_{28} \cdot (1 - t_{28}) \equiv 0 \\
s_6 \cdot (1 - s_6) \equiv 0 & s_{20} \cdot (1 - s_{20}) \equiv 0 & t_1 \cdot (1 - t_1) \equiv 0 & t_{15} \cdot (1 - t_{15}) \equiv 0 & t_{29} \cdot (1 - t_{29}) \equiv 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
s_{11} \cdot (1 - s_{11}) \equiv 0 & s_{25} \cdot (1 - s_{25}) \equiv 0 & t_6 \cdot (1 - t_6) \equiv 0 & t_{20} \cdot (1 - t_{20}) \equiv 0 & \\
s_{12} \cdot (1 - s_{12}) \equiv 0 & s_{26} \cdot (1 - s_{26}) \equiv 0 & t_7 \cdot (1 - t_7) \equiv 0 & t_{21} \cdot (1 - t_{21}) \equiv 0 &
\end{array}
$$

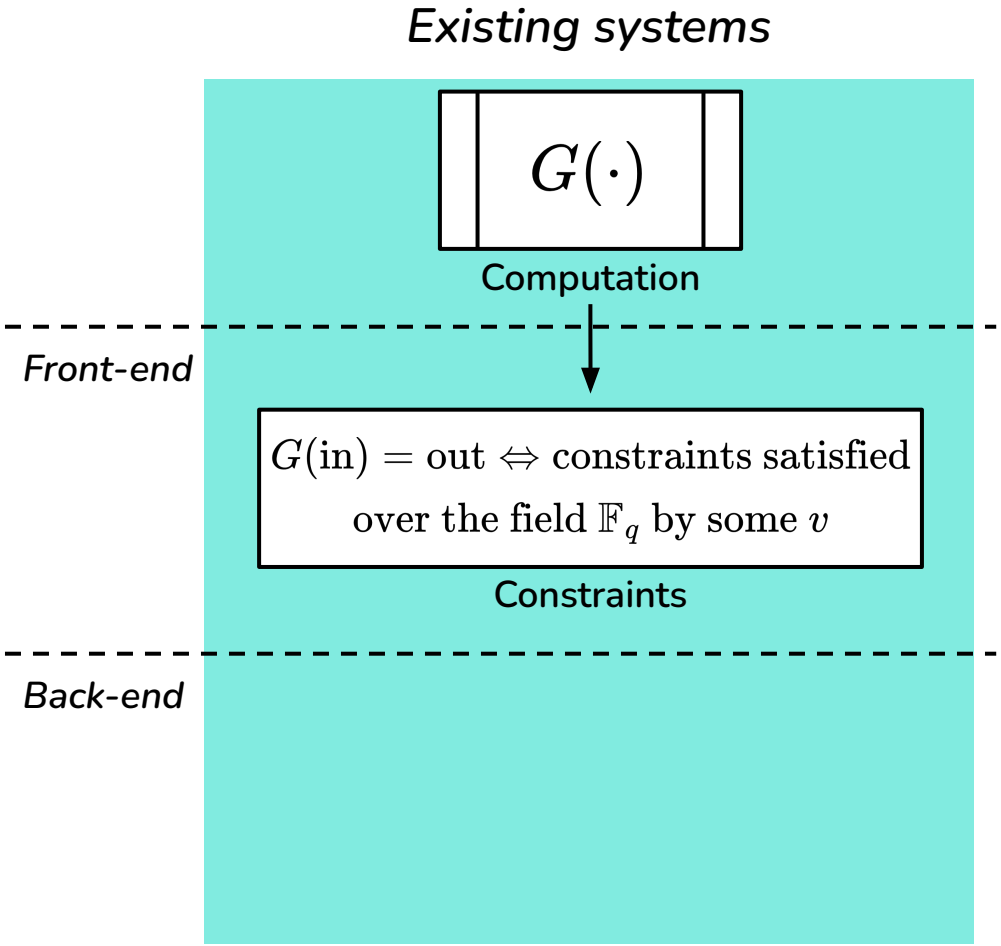
Constraints

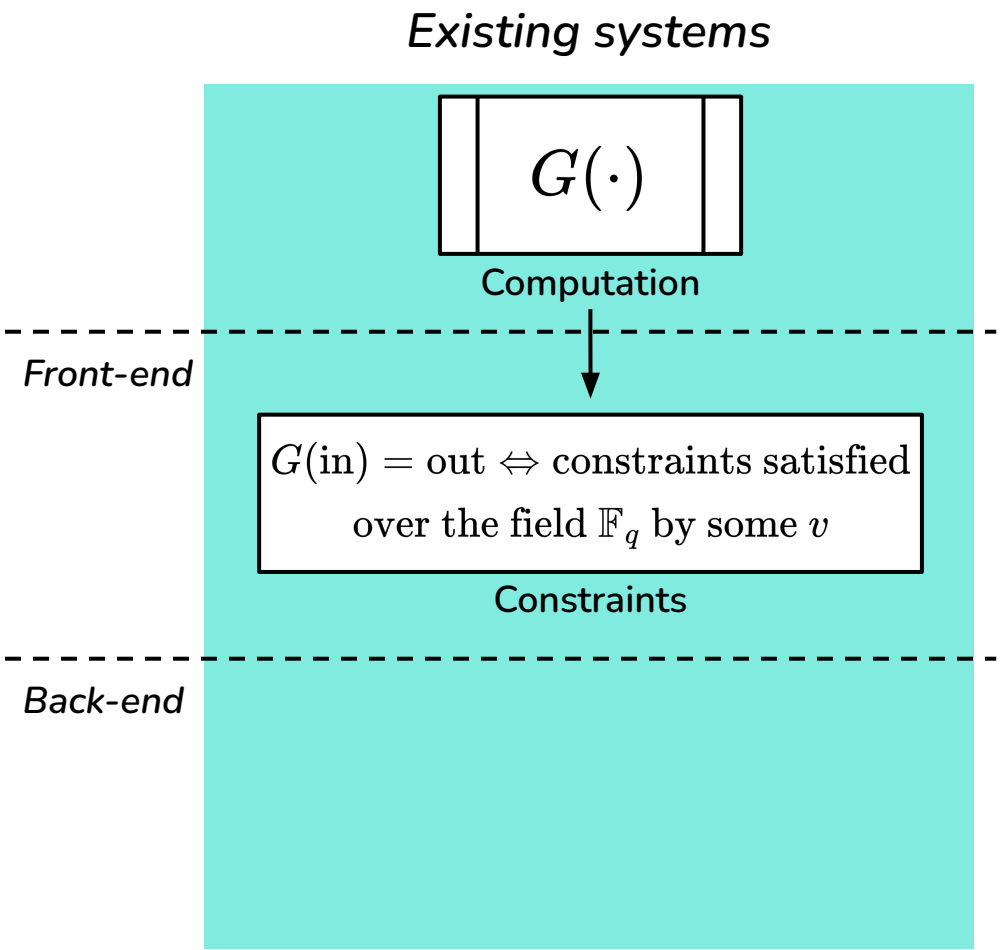
Equations over a finite field: $\mathbb{F}_q$

Our goal: make **constraints** for numerical computations **more concise**

Arithmetic behaves differently over a finite field versus the rationals.
For example, over $\mathbb{F}_{103}$ it is the case that $3/2 \equiv 53$.


Existing systems
$G(\cdot)$
Computation
Front-end
Back-end


Existing systems
$G(\cdot)$
Computation
Front-end
$G(\text{in}) = \text{out} \Leftrightarrow \text{constraints satisfied}$
over the field $\mathbb{F}_q$ by some v
Constraints
Back-end

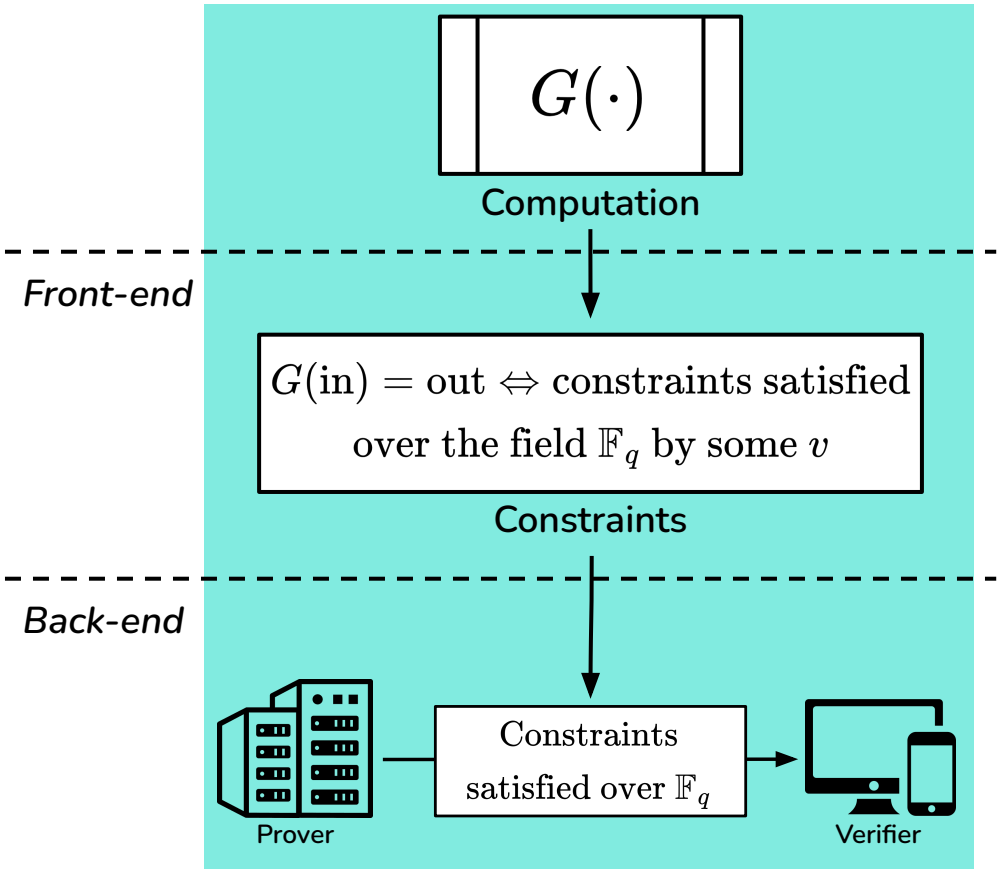


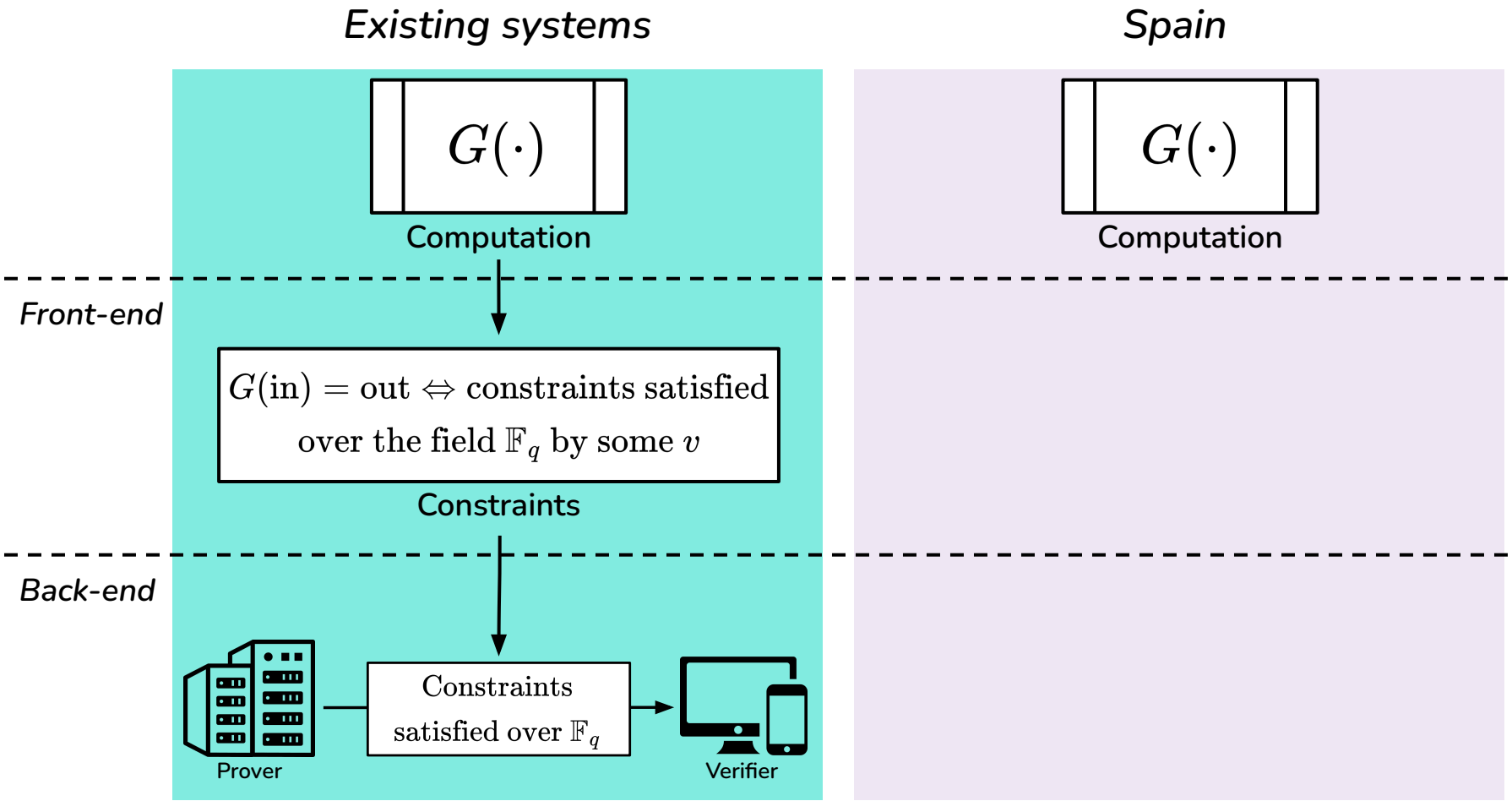
Let v be a vector of program variables.

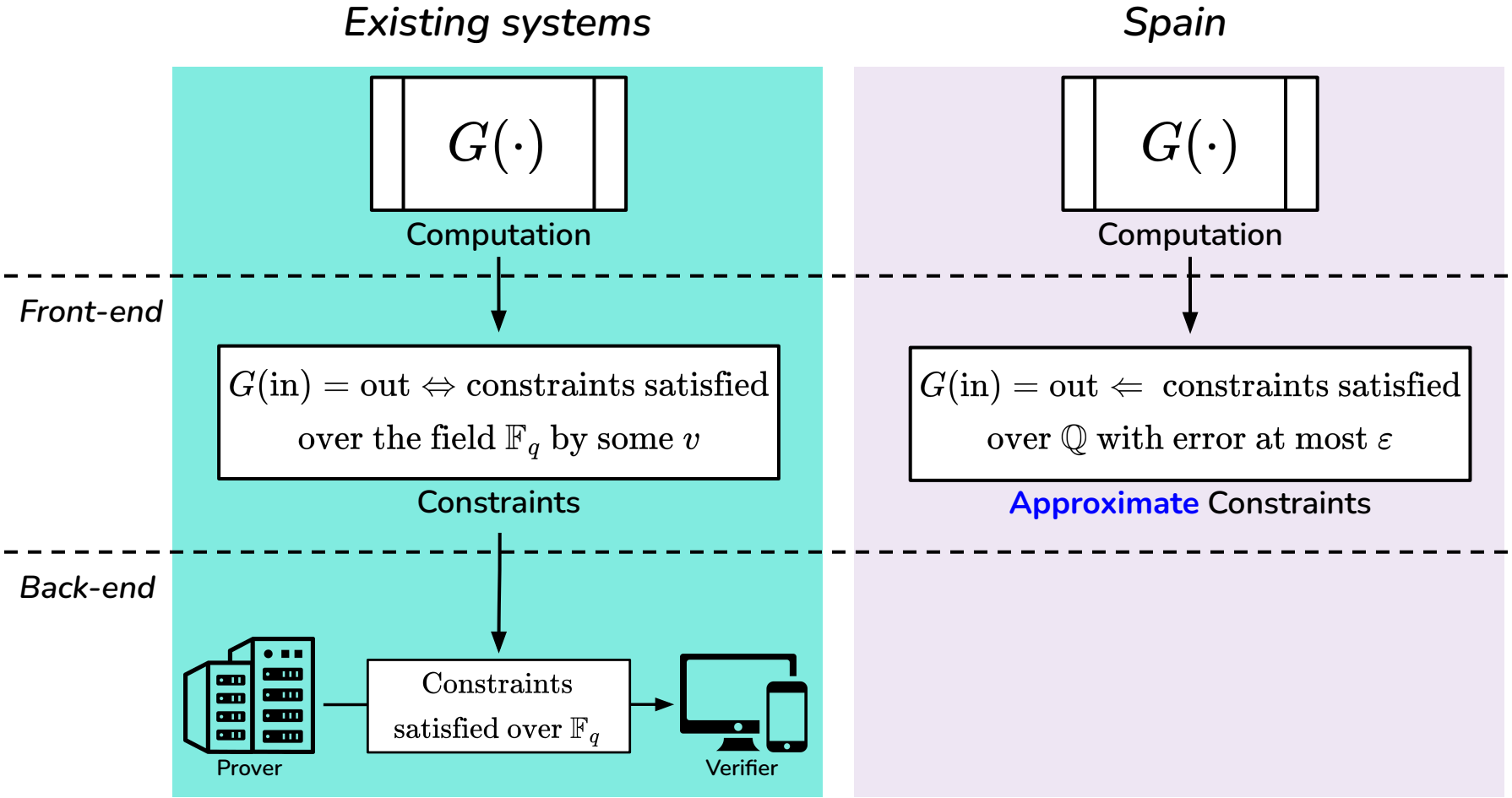
Constraints are equations over these variables of the form:

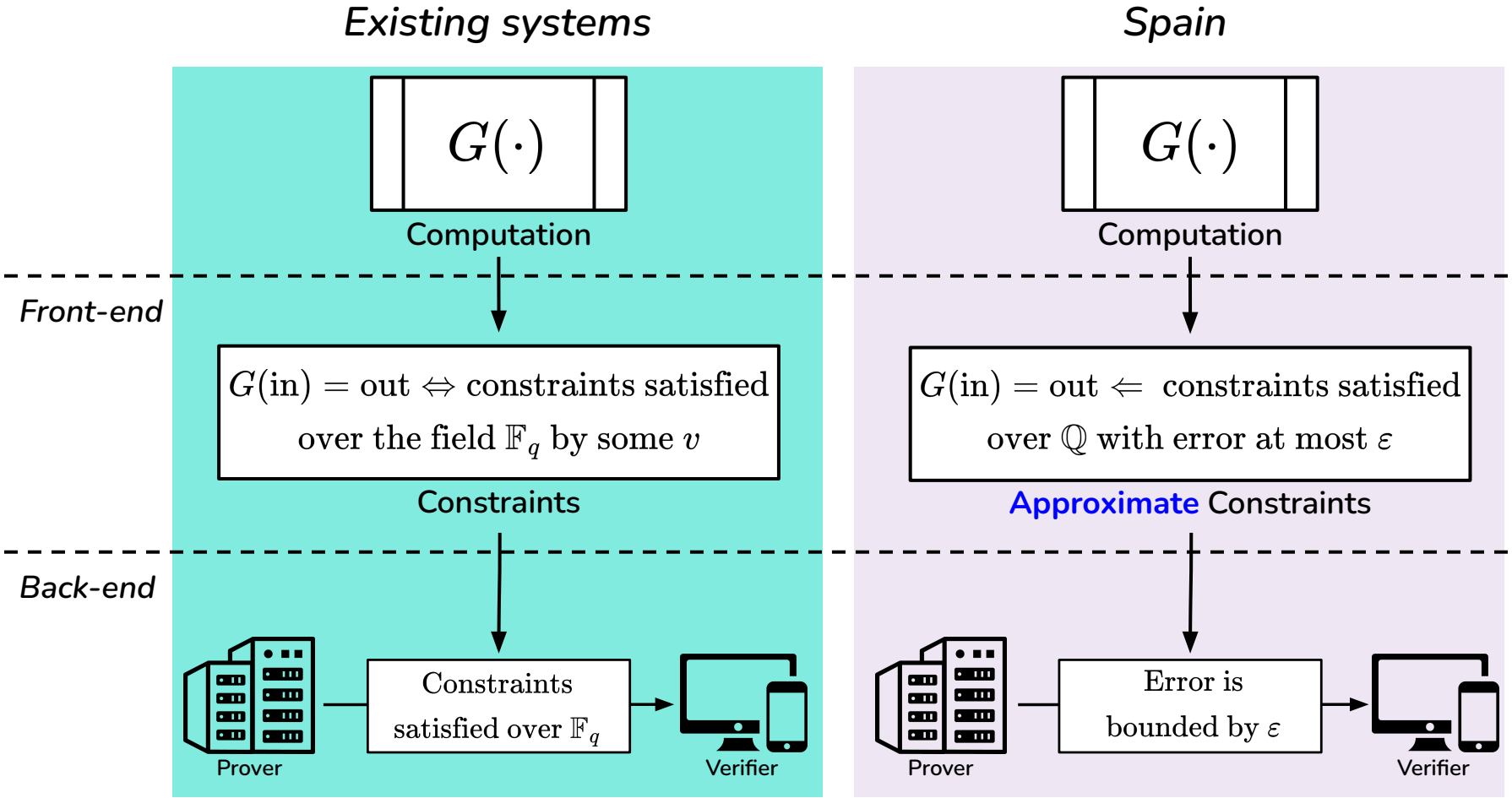
$$\text{expr} \cdot \text{expr} - \text{expr} \equiv 0$$

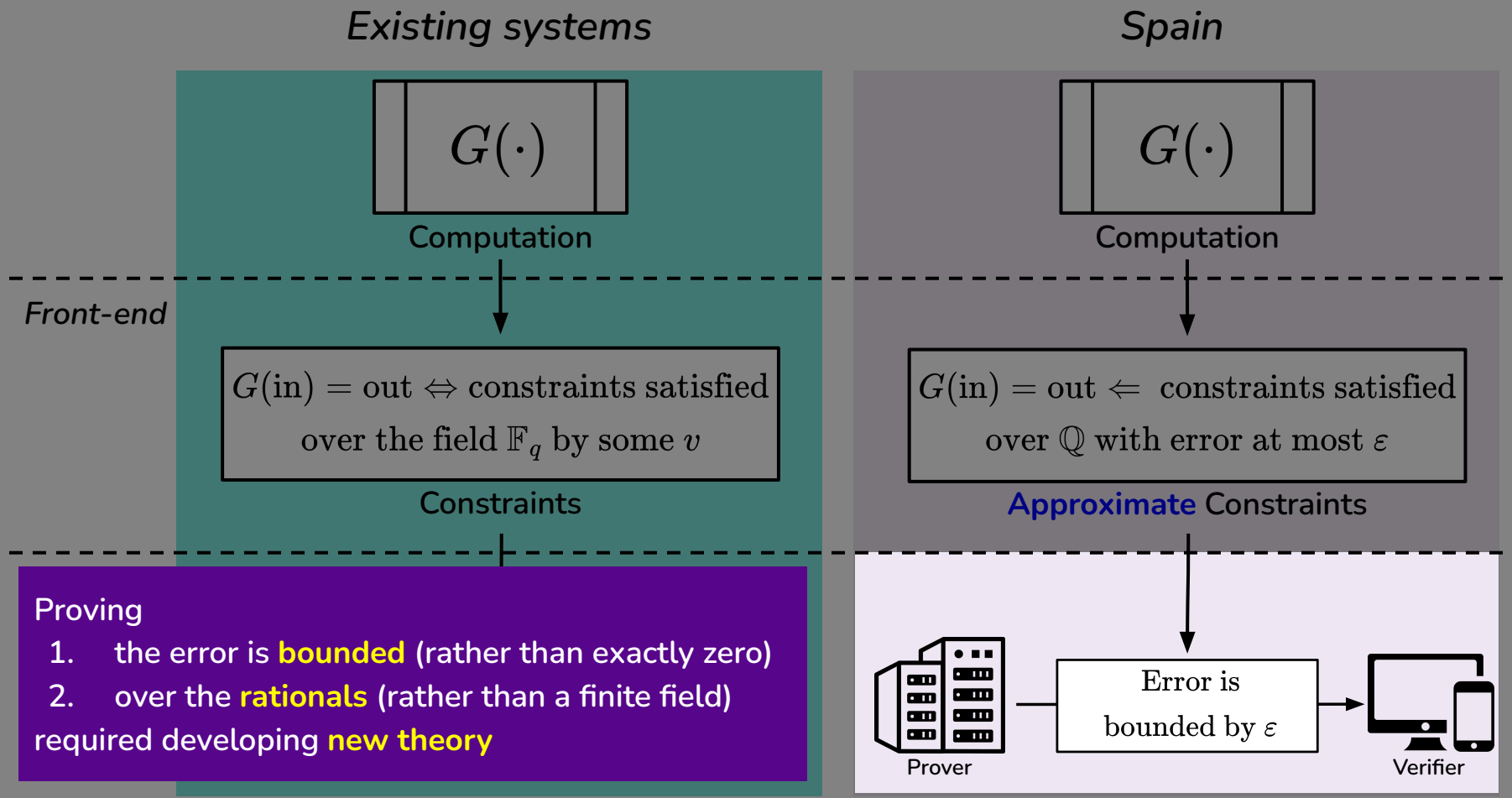
Existing systems

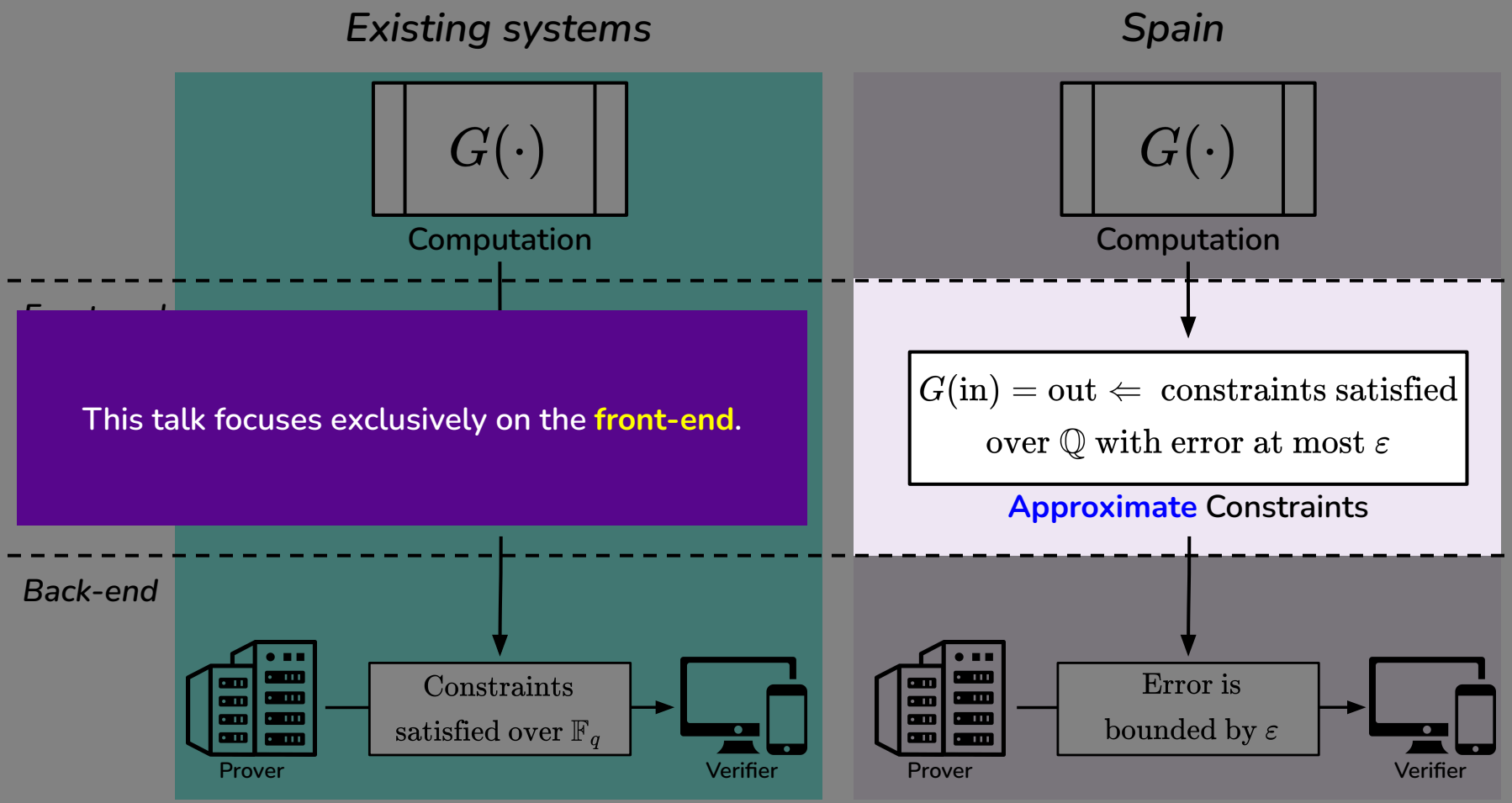



Existing systems
Spain
$G(\cdot)$
Computation
$G(\cdot)$
Computation
Front-end
$G(\text{in}) = \text{out} \Leftrightarrow$ constraints satisfied over the field $\mathbb{F}_q$ by some v
Constraints
Back-end
Constraints satisfied over $\mathbb{F}_q$
Prover
Verifier


Existing systems
Spain
$G(\cdot)$
Computation
$G(\cdot)$
Computation
Front-end
$G(\text{in}) = \text{out} \Leftrightarrow$ constraints satisfied over the field $\mathbb{F}_q$ by some v
Constraints
$G(\text{in}) = \text{out} \Leftarrow$ constraints satisfied over $\mathbb{Q}$ with error at most ε
Approximate Constraints
Back-end
Constraints satisfied over $\mathbb{F}_q$
Prover
Verifier


Existing systems
Spain
$G(\cdot)$
Computation
$G(\cdot)$
Computation
Front-end
$G(\text{in}) = \text{out} \Leftrightarrow$ constraints satisfied over the field $\mathbb{F}_q$ by some v
Constraints
$G(\text{in}) = \text{out} \Leftarrow$ constraints satisfied over $\mathbb{Q}$ with error at most ε
Approximate Constraints
Back-end
Prover
Constraints satisfied over $\mathbb{F}_q$
Verifier
Prover
Error is bounded by ε
Verifier


Existing systems
Spain
$G(\cdot)$
Computation
$G(\cdot)$
Computation
Front-end
$G(\text{in}) = \text{out} \Leftrightarrow$ constraints satisfied over the field $\mathbb{F}_q$ by some v
Constraints
$G(\text{in}) = \text{out} \Leftarrow$ constraints satisfied over $\mathbb{Q}$ with error at most ε
Approximate Constraints
Proving
1. the error is bounded (rather than exactly zero)
2. over the rationals (rather than a finite field)
required developing new theory
Error is bounded by ε
Prover
Verifier


Existing systems
Spain
$G(\cdot)$
Computation
$G(\cdot)$
Computation
This talk focuses exclusively on the front-end.
$G(\text{in}) = \text{out} \Leftarrow$ constraints satisfied over $\mathbb{Q}$ with error at most ε
Approximate Constraints
Back-end
Constraints satisfied over $\mathbb{F}_q$
Prover
Verifier
Error is bounded by ε
Prover
Verifier

A new formalism: approximate constraints

Rather than equations over a finite field:

$$\text{expr} \cdot \text{expr} - \text{expr} \equiv 0$$

we define **approximate** constraints over the **rationals**:

$$\left|\text{expr} \cdot \text{expr} - \text{expr}\right| \leq \varepsilon$$

A new formalism: approximate constraints

Rather than equations over a finite field:

$$\mathrm{expr} \cdot \mathrm{expr} - \mathrm{expr} \equiv 0$$

we define **approximate** constraints over the **rationals**:

$$\left|\mathrm{expr} \cdot \mathrm{expr} - \mathrm{expr}\right| \leq \varepsilon$$

This parameter depends on the allowed error in the original numerical computation

A new formalism: approximate constraints

Rather than equations over a finite field:

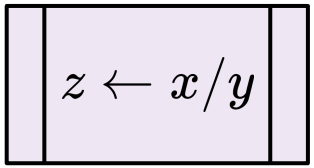
$$\text{expr} \cdot \text{expr} - \text{expr} \equiv 0$$

we define **approximate** constraints over the **rationals**:

$$\left|\text{expr} \cdot \text{expr} - \text{expr}\right| \leq \varepsilon$$

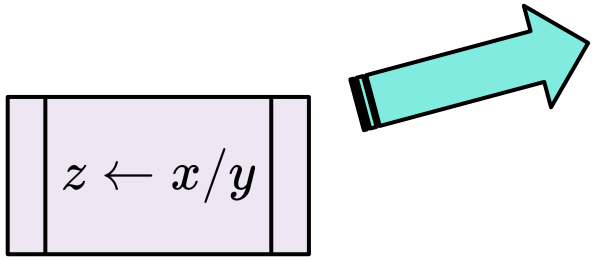
Claim: Approximate constraints better represent numerical computations

In Spain, division is dramatically fewer constraints



Computation

In Spain, division is dramatically fewer constraints



Computation

$$
\begin{array}{lllll}
y \cdot z - (x - r) \equiv 0 & s_{13} \cdot (1 - s_{13}) \equiv 0 & s_{27} \cdot (1 - s_{27}) \equiv 0 & t_8 \cdot (1 - t_8) \equiv 0 & t_{22} \cdot (1 - t_{22}) \equiv 0 \\
s_0 \cdot (1 - s_0) \equiv 0 & s_{14} \cdot (1 - s_{14}) \equiv 0 & s_{28} \cdot (1 - s_{28}) \equiv 0 & t_9 \cdot (1 - t_9) \equiv 0 & t_{23} \cdot (1 - t_{23}) \equiv 0 \\
s_1 \cdot (1 - s_1) \equiv 0 & s_{15} \cdot (1 - s_{15}) \equiv 0 & s_{29} \cdot (1 - s_{29}) \equiv 0 & t_{10} \cdot (1 - t_{10}) \equiv 0 & t_{24} \cdot (1 - t_{24}) \equiv 0 \\
s_2 \cdot (1 - s_2) \equiv 0 & s_{16} \cdot (1 - s_{16}) \equiv 0 & s_{30} \cdot (1 - s_{30}) \equiv 0 & t_{11} \cdot (1 - t_{11}) \equiv 0 & t_{25} \cdot (1 - t_{25}) \equiv 0 \\
s_3 \cdot (1 - s_3) \equiv 0 & s_{17} \cdot (1 - s_{17}) \equiv 0 & s_{31} \cdot (1 - s_{31}) \equiv 0 & t_{12} \cdot (1 - t_{12}) \equiv 0 & t_{26} \cdot (1 - t_{26}) \equiv 0 \\
s_4 \cdot (1 - s_4) \equiv 0 & s_{18} \cdot (1 - s_{18}) \equiv 0 & y - r - \sum_i 2^i s_i \equiv 0 & t_{13} \cdot (1 - t_{13}) \equiv 0 & t_{27} \cdot (1 - t_{27}) \equiv 0 \\
s_5 \cdot (1 - s_5) \equiv 0 & s_{19} \cdot (1 - s_{19}) \equiv 0 & t_0 \cdot (1 - t_0) \equiv 0 & t_{14} \cdot (1 - t_{14}) \equiv 0 & t_{28} \cdot (1 - t_{28}) \equiv 0 \\
s_6 \cdot (1 - s_6) \equiv 0 & s_{20} \cdot (1 - s_{20}) \equiv 0 & t_1 \cdot (1 - t_1) \equiv 0 & t_{15} \cdot (1 - t_{15}) \equiv 0 & t_{29} \cdot (1 - t_{29}) \equiv 0 \\
s_7 \cdot (1 - s_7) \equiv 0 & s_{21} \cdot (1 - s_{21}) \equiv 0 & t_2 \cdot (1 - t_2) \equiv 0 & t_{16} \cdot (1 - t_{16}) \equiv 0 & t_{30} \cdot (1 - t_{30}) \equiv 0 \\
s_8 \cdot (1 - s_8) \equiv 0 & s_{22} \cdot (1 - s_{22}) \equiv 0 & t_3 \cdot (1 - t_3) \equiv 0 & t_{17} \cdot (1 - t_{17}) \equiv 0 & t_{31} \cdot (1 - t_{31}) \equiv 0 \\
s_9 \cdot (1 - s_9) \equiv 0 & s_{23} \cdot (1 - s_{23}) \equiv 0 & t_4 \cdot (1 - t_4) \equiv 0 & t_{18} \cdot (1 - t_{18}) \equiv 0 & z - \sum_i 2^i t_i \equiv 0 \\
s_{10} \cdot (1 - s_{10}) \equiv 0 & s_{24} \cdot (1 - s_{24}) \equiv 0 & t_5 \cdot (1 - t_5) \equiv 0 & t_{19} \cdot (1 - t_{19}) \equiv 0 & \\
s_{11} \cdot (1 - s_{11}) \equiv 0 & s_{25} \cdot (1 - s_{25}) \equiv 0 & t_6 \cdot (1 - t_6) \equiv 0 & t_{20} \cdot (1 - t_{20}) \equiv 0 & \\
s_{12} \cdot (1 - s_{12}) \equiv 0 & s_{26} \cdot (1 - s_{26}) \equiv 0 & t_7 \cdot (1 - t_7) \equiv 0 & t_{21} \cdot (1 - t_{21}) \equiv 0 &
\end{array}
$$

Constraints in existing systems

In Spain, division is dramatically fewer constraints

$$z \leftarrow x/y$$

Computation

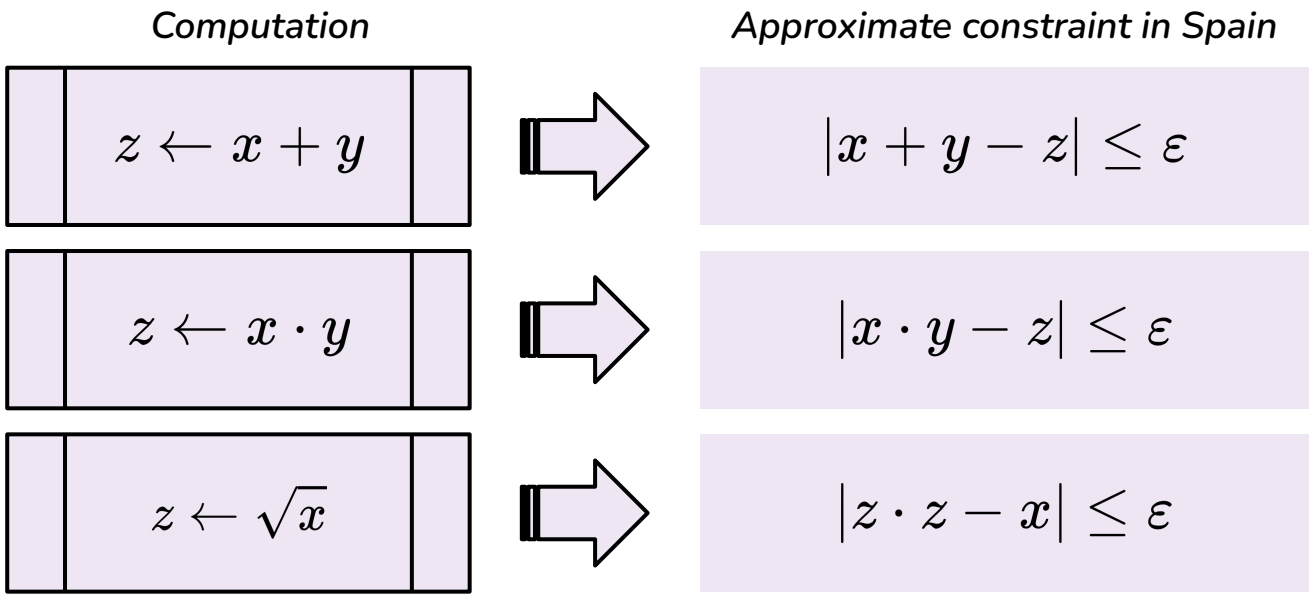
$$
\begin{array}{lllll}
y \cdot z - (x - r) \equiv 0 & s_{13} \cdot (1 - s_{13}) \equiv 0 & s_{27} \cdot (1 - s_{27}) \equiv 0 & t_8 \cdot (1 - t_8) \equiv 0 & t_{22} \cdot (1 - t_{22}) \equiv 0 \\
s_0 \cdot (1 - s_0) \equiv 0 & s_{14} \cdot (1 - s_{14}) \equiv 0 & s_{28} \cdot (1 - s_{28}) \equiv 0 & t_9 \cdot (1 - t_9) \equiv 0 & t_{23} \cdot (1 - t_{23}) \equiv 0 \\
s_1 \cdot (1 - s_1) \equiv 0 & s_{15} \cdot (1 - s_{15}) \equiv 0 & s_{29} \cdot (1 - s_{29}) \equiv 0 & t_{10} \cdot (1 - t_{10}) \equiv 0 & t_{24} \cdot (1 - t_{24}) \equiv 0 \\
s_2 \cdot (1 - s_2) \equiv 0 & s_{16} \cdot (1 - s_{16}) \equiv 0 & s_{30} \cdot (1 - s_{30}) \equiv 0 & t_{11} \cdot (1 - t_{11}) \equiv 0 & t_{25} \cdot (1 - t_{25}) \equiv 0 \\
s_3 \cdot (1 - s_3) \equiv 0 & s_{17} \cdot (1 - s_{17}) \equiv 0 & s_{31} \cdot (1 - s_{31}) \equiv 0 & t_{12} \cdot (1 - t_{12}) \equiv 0 & t_{26} \cdot (1 - t_{26}) \equiv 0 \\
s_4 \cdot (1 - s_4) \equiv 0 & s_{18} \cdot (1 - s_{18}) \equiv 0 & y - r - \sum_i 2^i s_i \equiv 0 & t_{13} \cdot (1 - t_{13}) \equiv 0 & t_{27} \cdot (1 - t_{27}) \equiv 0 \\
s_5 \cdot (1 - s_5) \equiv 0 & s_{19} \cdot (1 - s_{19}) \equiv 0 & t_0 \cdot (1 - t_0) \equiv 0 & t_{14} \cdot (1 - t_{14}) \equiv 0 & t_{28} \cdot (1 - t_{28}) \equiv 0 \\
s_6 \cdot (1 - s_6) \equiv 0 & s_{20} \cdot (1 - s_{20}) \equiv 0 & t_1 \cdot (1 - t_1) \equiv 0 & t_{15} \cdot (1 - t_{15}) \equiv 0 & t_{29} \cdot (1 - t_{29}) \equiv 0 \\
s_7 \cdot (1 - s_7) \equiv 0 & s_{21} \cdot (1 - s_{21}) \equiv 0 & t_2 \cdot (1 - t_2) \equiv 0 & t_{16} \cdot (1 - t_{16}) \equiv 0 & t_{30} \cdot (1 - t_{30}) \equiv 0 \\
s_8 \cdot (1 - s_8) \equiv 0 & s_{22} \cdot (1 - s_{22}) \equiv 0 & t_3 \cdot (1 - t_3) \equiv 0 & t_{17} \cdot (1 - t_{17}) \equiv 0 & t_{31} \cdot (1 - t_{31}) \equiv 0 \\
s_9 \cdot (1 - s_9) \equiv 0 & s_{23} \cdot (1 - s_{23}) \equiv 0 & t_4 \cdot (1 - t_4) \equiv 0 & t_{18} \cdot (1 - t_{18}) \equiv 0 & z - \sum_i 2^i t_i \equiv 0 \\
s_{10} \cdot (1 - s_{10}) \equiv 0 & s_{24} \cdot (1 - s_{24}) \equiv 0 & t_5 \cdot (1 - t_5) \equiv 0 & t_{19} \cdot (1 - t_{19}) \equiv 0 & \\
s_{11} \cdot (1 - s_{11}) \equiv 0 & s_{25} \cdot (1 - s_{25}) \equiv 0 & t_6 \cdot (1 - t_6) \equiv 0 & t_{20} \cdot (1 - t_{20}) \equiv 0 & \\
s_{12} \cdot (1 - s_{12}) \equiv 0 & s_{26} \cdot (1 - s_{26}) \equiv 0 & t_7 \cdot (1 - t_7) \equiv 0 & t_{21} \cdot (1 - t_{21}) \equiv 0 &
\end{array}
$$

Constraints in existing systems

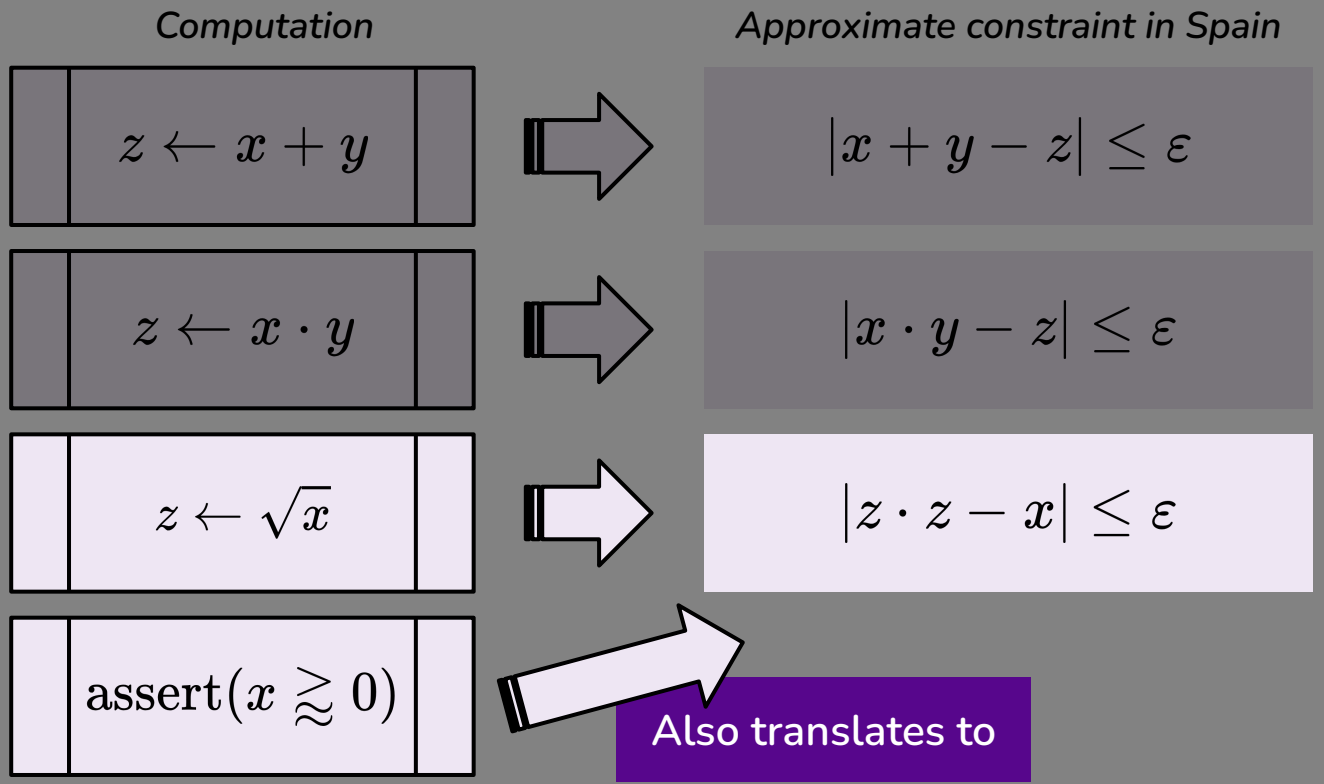
$$|z \cdot y - x| \leq \varepsilon$$

A single approximate constraint in Spain

In Spain, primitive numerical operations have concise representations

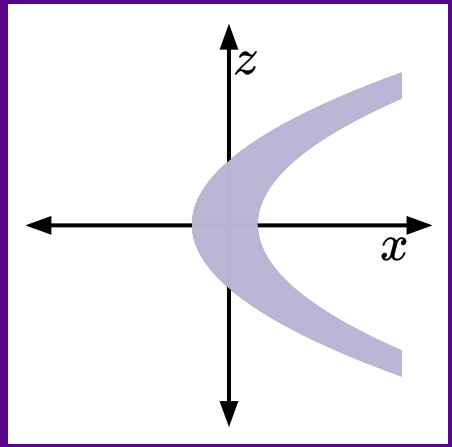


In Spain, primitive numerical operations have concise representations



In Spain, primitive numerical operations have concise representations

This graph contains all satisfying pairs (x, z).



$z \leftarrow \sqrt{x}$

$|z \cdot z - x| \leq \varepsilon$

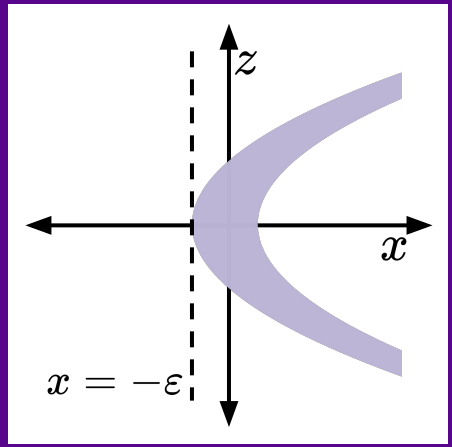
$\mathrm{assert}(x \gtrapprox 0)$

Also translates to

In Spain, primitive numerical operations have concise representations

This graph contains all satisfying pairs (x, z).

Observe that there are **no satisfying pairs** when $x < -\varepsilon$.



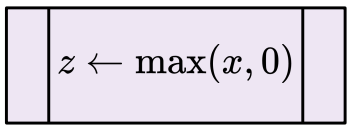
$z \leftarrow \sqrt{x}$

$\text{assert}(x \gtrapprox 0)$

Also translates to

$|z \cdot z - x| \leq \varepsilon$

In Spain, more complex numerical operations have concise representations

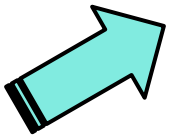


Computation

In Spain, more complex numerical operations have concise representations

$$z \leftarrow \max(x, 0)$$

Computation



$$\begin{aligned}
x \cdot (s+1) - 2z &\equiv 0 \\
s \cdot s - 1 &\equiv 0 \\
t_0 \cdot (1 - t_0) &\equiv 0 \\
t_1 \cdot (1 - t_1) &\equiv 0 \\
t_2 \cdot (1 - t_2) &\equiv 0 \\
t_3 \cdot (1 - t_3) &\equiv 0 \\
t_4 \cdot (1 - t_4) &\equiv 0 \\
t_5 \cdot (1 - t_5) &\equiv 0 \\
t_6 \cdot (1 - t_6) &\equiv 0 \\
t_7 \cdot (1 - t_7) &\equiv 0 \\
t_8 \cdot (1 - t_8) &\equiv 0 \\
t_9 \cdot (1 - t_9) &\equiv 0 \\
t_{10} \cdot (1 - t_{10}) &\equiv 0 \\
t_{11} \cdot (1 - t_{11}) &\equiv 0 \\
t_{12} \cdot (1 - t_{12}) &\equiv 0 \\
t_{13} \cdot (1 - t_{13}) &\equiv 0 \\
t_{14} \cdot (1 - t_{14}) &\equiv 0 \\
t_{15} \cdot (1 - t_{15}) &\equiv 0 \\
t_{16} \cdot (1 - t_{16}) &\equiv 0 \\
t_{17} \cdot (1 - t_{17}) &\equiv 0 \\
t_{18} \cdot (1 - t_{18}) &\equiv 0 \\
t_{19} \cdot (1 - t_{19}) &\equiv 0 \\
t_{20} \cdot (1 - t_{20}) &\equiv 0 \\
t_{21} \cdot (1 - t_{21}) &\equiv 0 \\
t_{22} \cdot (1 - t_{22}) &\equiv 0 \\
t_{23} \cdot (1 - t_{23}) &\equiv 0 \\
t_{24} \cdot (1 - t_{24}) &\equiv 0 \\
t_{25} \cdot (1 - t_{25}) &\equiv 0 \\
t_{26} \cdot (1 - t_{26}) &\equiv 0 \\
t_{27} \cdot (1 - t_{27}) &\equiv 0 \\
t_{28} \cdot (1 - t_{28}) &\equiv 0 \\
t_{29} \cdot (1 - t_{29}) &\equiv 0 \\
t_{30} \cdot (1 - t_{30}) &\equiv 0 \\
t_{31} \cdot (1 - t_{31}) &\equiv 0 \\
s \cdot \sum_i 2^i t_i - x &\equiv 0
\end{aligned}$$

Constraints in existing systems

In Spain, more complex numerical operations have concise representations

$$
\begin{array}{rrrr}
x \cdot (s+1) - 2z \equiv 0 & t_7 \cdot (1-t_7) \equiv 0 & t_{16} \cdot (1-t_{16}) \equiv 0 & t_{25} \cdot (1-t_{25}) \equiv 0 \\
s \cdot s - 1 \equiv 0 & t_8 \cdot (1-t_8) \equiv 0 & t_{17} \cdot (1-t_{17}) \equiv 0 & t_{26} \cdot (1-t_{26}) \equiv 0 \\
t_0 \cdot (1-t_0) \equiv 0 & t_9 \cdot (1-t_9) \equiv 0 & t_{18} \cdot (1-t_{18}) \equiv 0 & t_{27} \cdot (1-t_{27}) \equiv 0 \\
t_1 \cdot (1-t_1) \equiv 0 & t_{10} \cdot (1-t_{10}) \equiv 0 & t_{19} \cdot (1-t_{19}) \equiv 0 & t_{28} \cdot (1-t_{28}) \equiv 0 \\
t_2 \cdot (1-t_2) \equiv 0 & t_{11} \cdot (1-t_{11}) \equiv 0 & t_{20} \cdot (1-t_{20}) \equiv 0 & t_{29} \cdot (1-t_{29}) \equiv 0 \\
t_3 \cdot (1-t_3) \equiv 0 & t_{12} \cdot (1-t_{12}) \equiv 0 & t_{21} \cdot (1-t_{21}) \equiv 0 & t_{30} \cdot (1-t_{30}) \equiv 0 \\
t_4 \cdot (1-t_4) \equiv 0 & t_{13} \cdot (1-t_{13}) \equiv 0 & t_{22} \cdot (1-t_{22}) \equiv 0 & t_{31} \cdot (1-t_{31}) \equiv 0 \\
t_5 \cdot (1-t_5) \equiv 0 & t_{14} \cdot (1-t_{14}) \equiv 0 & t_{23} \cdot (1-t_{23}) \equiv 0 & s \cdot \sum_i 2^i t_i - x \equiv 0 \\
t_6 \cdot (1-t_6) \equiv 0 & t_{15} \cdot (1-t_{15}) \equiv 0 & t_{24} \cdot (1-t_{24}) \equiv 0 &
\end{array}
$$

Constraints in existing systems

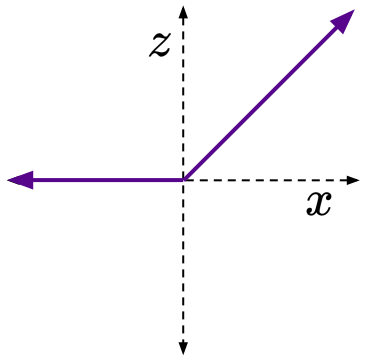
$$z \leftarrow \max(x, 0)$$

Computation

$$
\begin{aligned}
|s \cdot s - (z - x)| &\leq \varepsilon \\
|t \cdot t - z| &\leq \varepsilon \\
|(z - x) \cdot z| &\leq \varepsilon
\end{aligned}
$$

Three approximate constraints in Spain

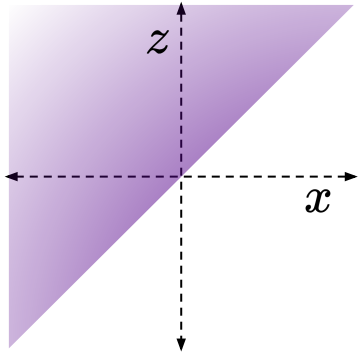
In Spain, more complex numerical operations have concise representations



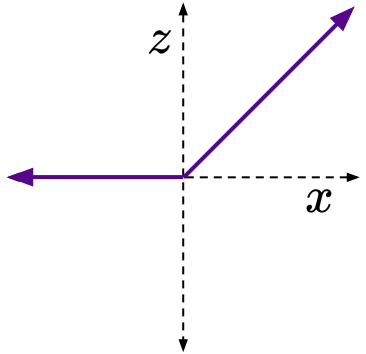
$$z \leftarrow \max(x, 0)$$

Computation

In Spain, more complex numerical operations have concise representations



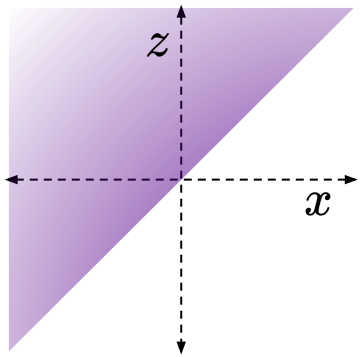
$$z \geq x$$



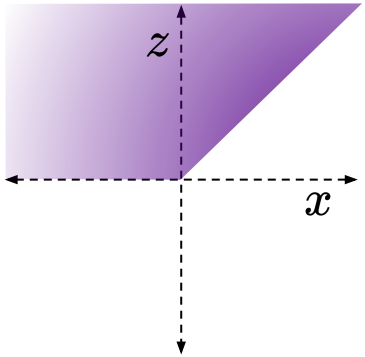
$$z \leftarrow \max(x, 0)$$

Computation

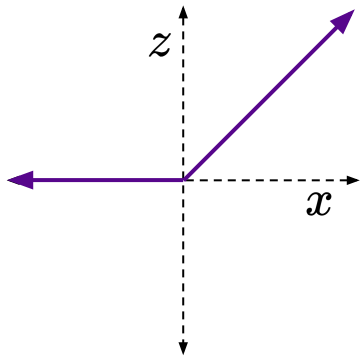
In Spain, more complex numerical operations have concise representations



$$z \geq x$$



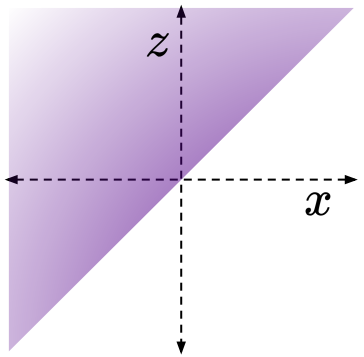
$$z \geq x$$
$$z \geq 0$$



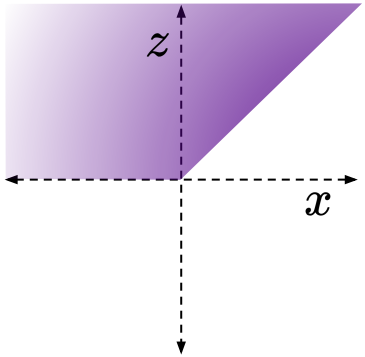
$$z \leftarrow \max(x, 0)$$

Computation

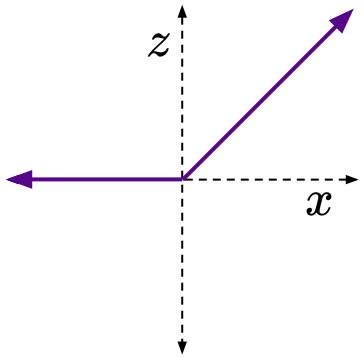
In Spain, more complex numerical operations have concise representations



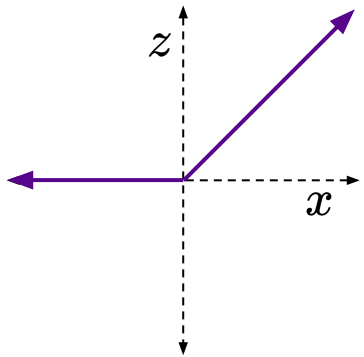
$$z \geq x$$



$$z \geq x$$
$$z \geq 0$$



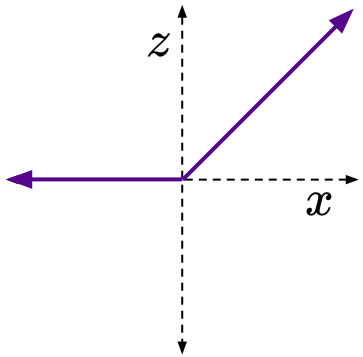
$$z \geq x$$
$$z \geq 0$$
$$z = x \text{ or } 0$$



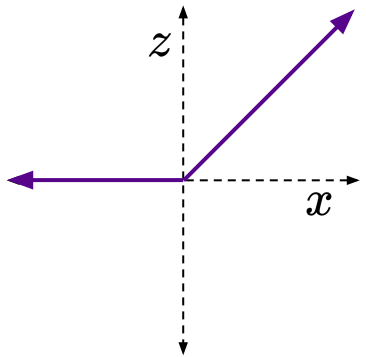
$$z \leftarrow \max(x, 0)$$

Computation

In Spain, more complex numerical operations have concise representations



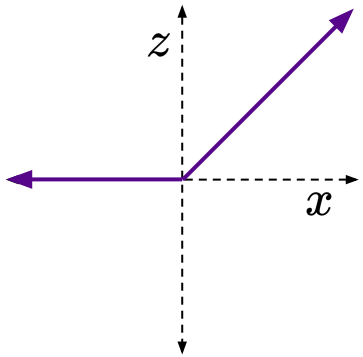
$$z \geq x$$
$$z \geq 0$$
$$z = x \text{ or } 0$$



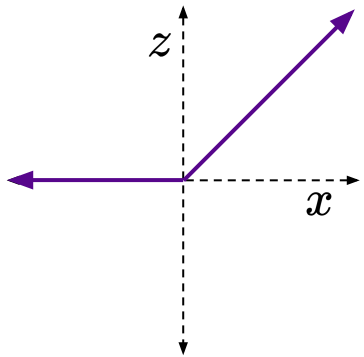
$$z \leftarrow \max(x, 0)$$

Computation

In Spain, more complex numerical operations have concise representations



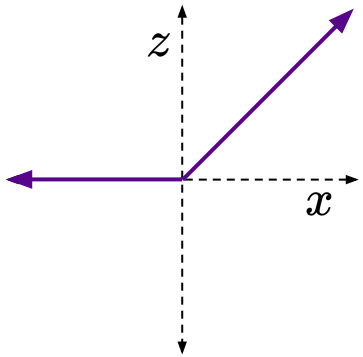
$$\text{assert}(z \gtrapprox x)$$
$$\text{assert}(z \gtrapprox 0)$$
$$\text{assert}(z \approx x \text{ or } 0)$$



$$z \leftarrow \max(x, 0)$$

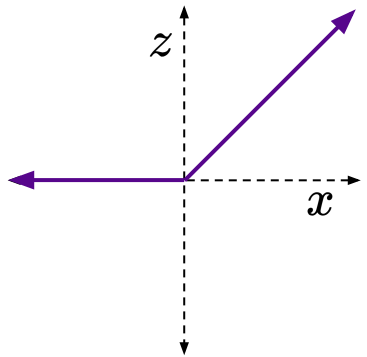
Computation

In Spain, more complex numerical operations have concise representations



$$|s \cdot s - (z - x)| \leq \varepsilon$$
$$|t \cdot t - z| \leq \varepsilon$$
$$|(z - x) \cdot z| \leq \varepsilon$$

Approximate constraints



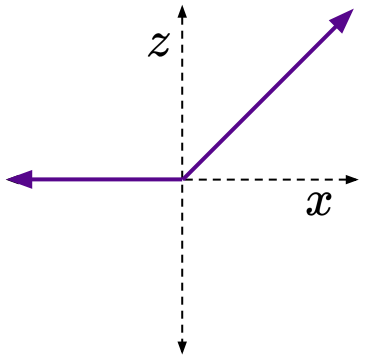
$$z \leftarrow \max(x, 0)$$

Computation

In Spain, more complex numerical operations have concise representations

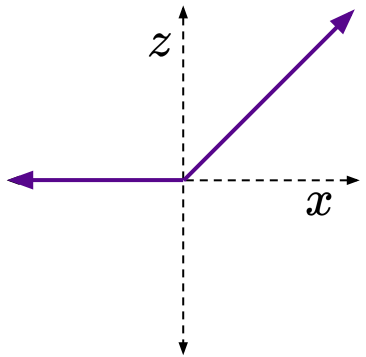
$$
\begin{array}{rrrr}
x \cdot (s+1) - 2z \equiv 0 & t_7 \cdot (1-t_7) \equiv 0 & t_{16} \cdot (1-t_{16}) \equiv 0 & t_{25} \cdot (1-t_{25}) \equiv 0 \\
s \cdot s - 1 \equiv 0 & t_8 \cdot (1-t_8) \equiv 0 & t_{17} \cdot (1-t_{17}) \equiv 0 & t_{26} \cdot (1-t_{26}) \equiv 0 \\
t_0 \cdot (1-t_0) \equiv 0 & t_9 \cdot (1-t_9) \equiv 0 & t_{18} \cdot (1-t_{18}) \equiv 0 & t_{27} \cdot (1-t_{27}) \equiv 0 \\
t_1 \cdot (1-t_1) \equiv 0 & t_{10} \cdot (1-t_{10}) \equiv 0 & t_{19} \cdot (1-t_{19}) \equiv 0 & t_{28} \cdot (1-t_{28}) \equiv 0 \\
t_2 \cdot (1-t_2) \equiv 0 & t_{11} \cdot (1-t_{11}) \equiv 0 & t_{20} \cdot (1-t_{20}) \equiv 0 & t_{29} \cdot (1-t_{29}) \equiv 0 \\
t_3 \cdot (1-t_3) \equiv 0 & t_{12} \cdot (1-t_{12}) \equiv 0 & t_{21} \cdot (1-t_{21}) \equiv 0 & t_{30} \cdot (1-t_{30}) \equiv 0 \\
t_4 \cdot (1-t_4) \equiv 0 & t_{13} \cdot (1-t_{13}) \equiv 0 & t_{22} \cdot (1-t_{22}) \equiv 0 & t_{31} \cdot (1-t_{31}) \equiv 0 \\
t_5 \cdot (1-t_5) \equiv 0 & t_{14} \cdot (1-t_{14}) \equiv 0 & t_{23} \cdot (1-t_{23}) \equiv 0 & s \cdot \sum_i 2^i t_i - x \equiv 0 \\
t_6 \cdot (1-t_6) \equiv 0 & t_{15} \cdot (1-t_{15}) \equiv 0 & t_{24} \cdot (1-t_{24}) \equiv 0 &
\end{array}
$$

Constraints in existing systems



$$
\begin{gathered}
|s \cdot s - (z - x)| \leq \varepsilon \\
|t \cdot t - z| \leq \varepsilon \\
|(z - x) \cdot z| \leq \varepsilon
\end{gathered}
$$

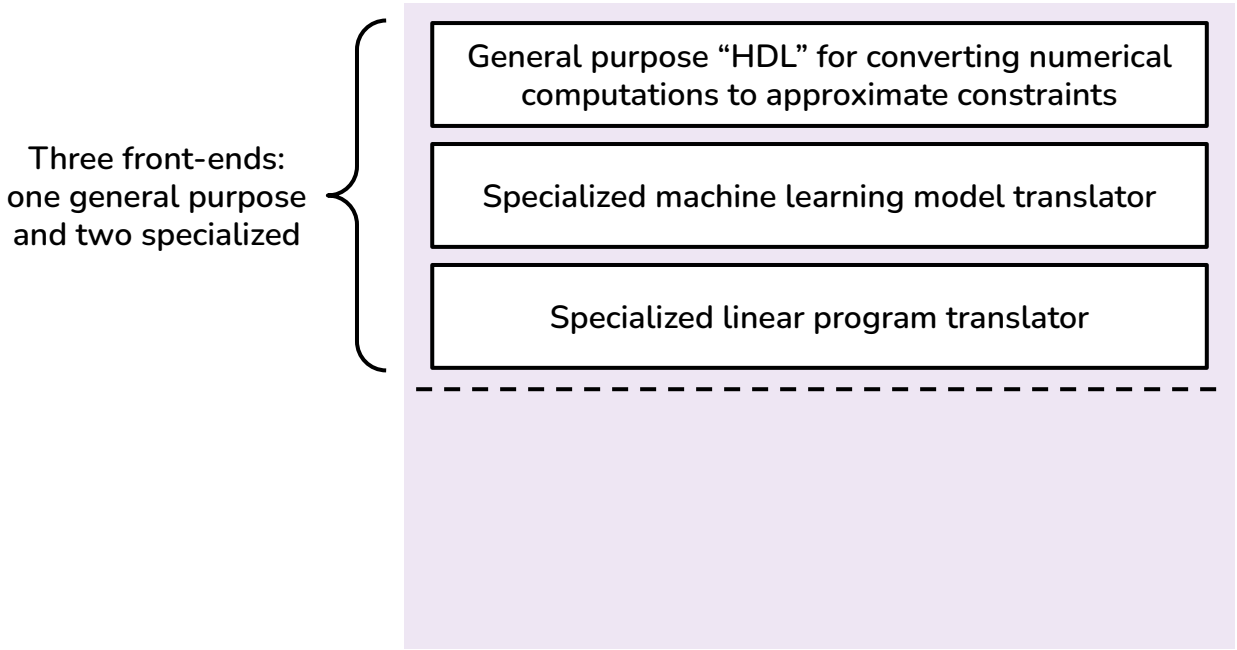
Approximate constraints



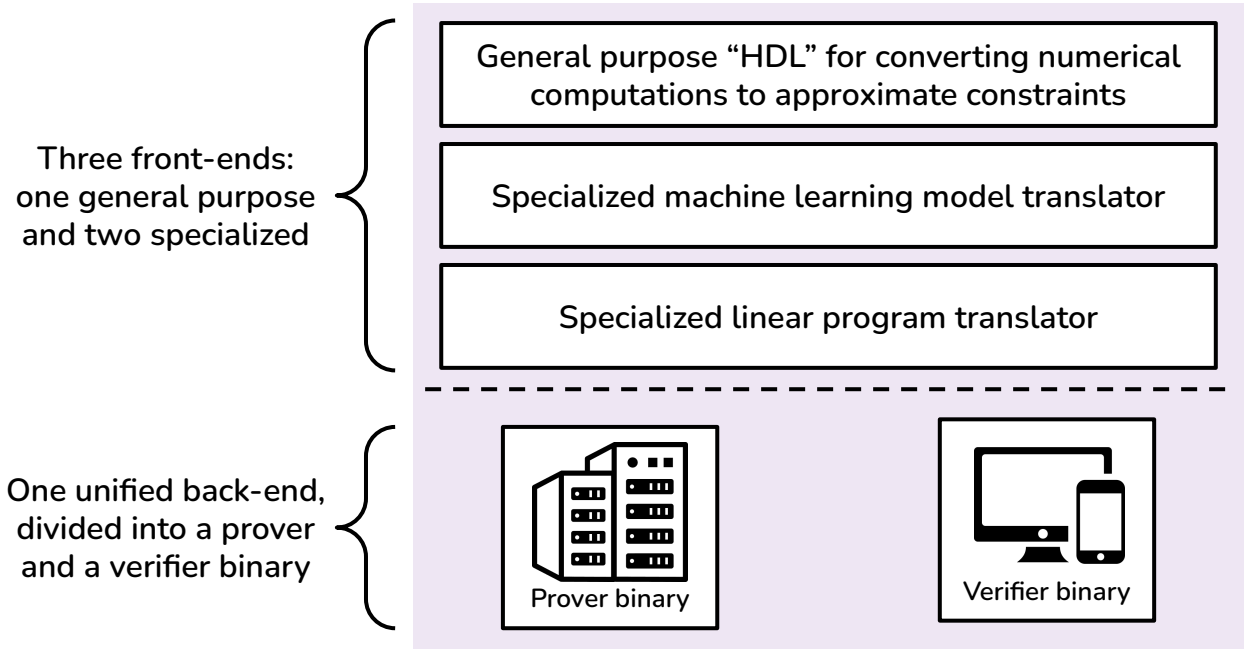
$$z \leftarrow \max(x, 0)$$

Computation

Spain was implemented and applied to several real-world computations



Spain was implemented and applied to several real-world computations

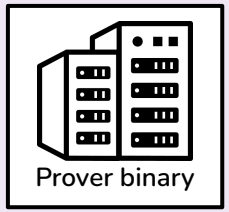


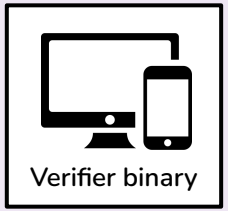
Spain was implemented and applied to several real-world computations

Three front-ends: one general purpose and two specialized

- General purpose “HDL” for converting numerical computations to approximate constraints
- Specialized machine learning model translator
- Specialized linear program translator

One unified back-end, divided into a prover and a verifier binary





- High-precision rational arithmetic
- Custom ML runtime
- Constraint gadget library
- Polynomial commitment
- Sum-check
- And more...

The system required a variety of custom **cryptographic** and **non-cryptographic** components

Spain's evaluation method

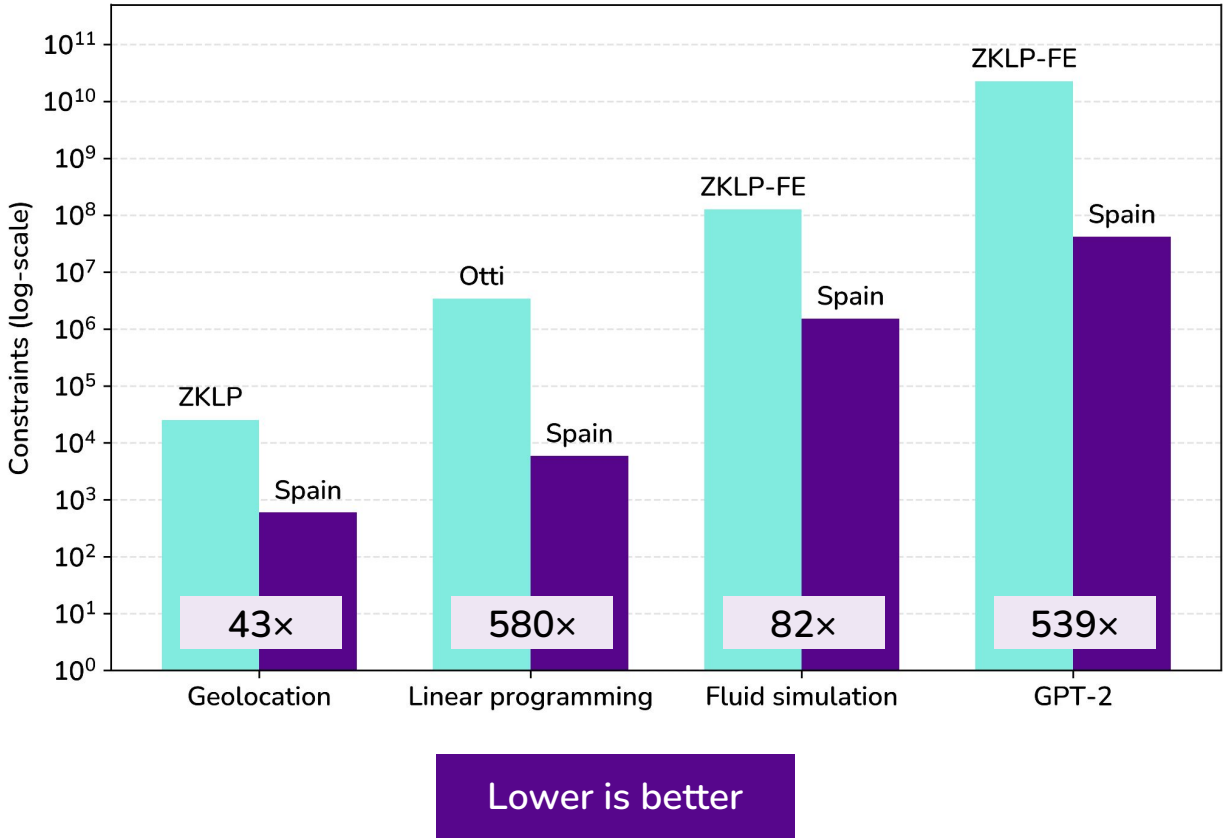
We compare Spain to **Otti** [‘22] and **ZKLP** [‘24], two state of the art systems for applying succinct proofs to numerical computations.

We benchmark Spain on four applications of different sizes.

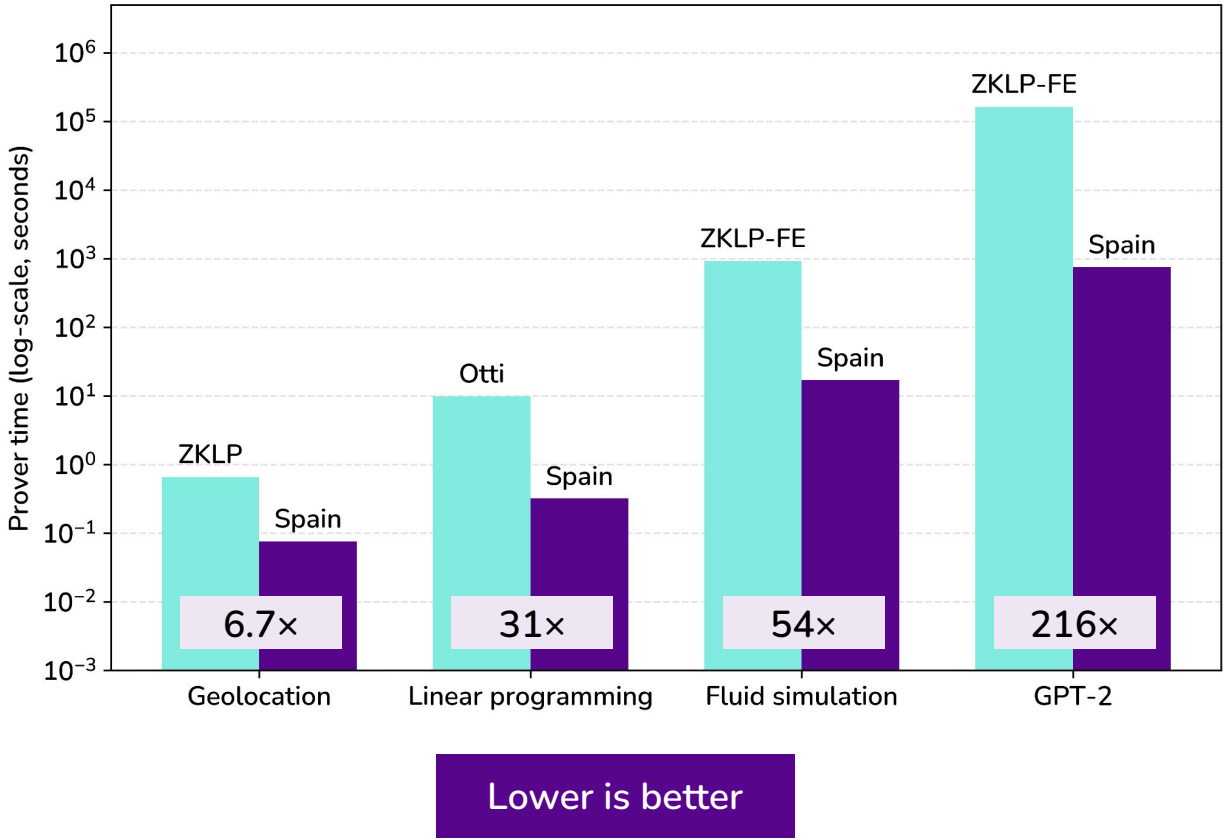
1. **Geolocation**: ZKLP's headline computation (for direct comparison)
2. **Linear programming**: Otti's headline computation (for direct comparison)
3. **Fluid simulation**: A Stable-Fluids-style incompressible fluid simulation
4. **GPT-2 inference**: execution of an open source LLM.

For larger computations, we developed a cost model of ZKLP and **estimated** performance. In the following slides, we label such baselines as **ZKLP-FE** to distinguish them.

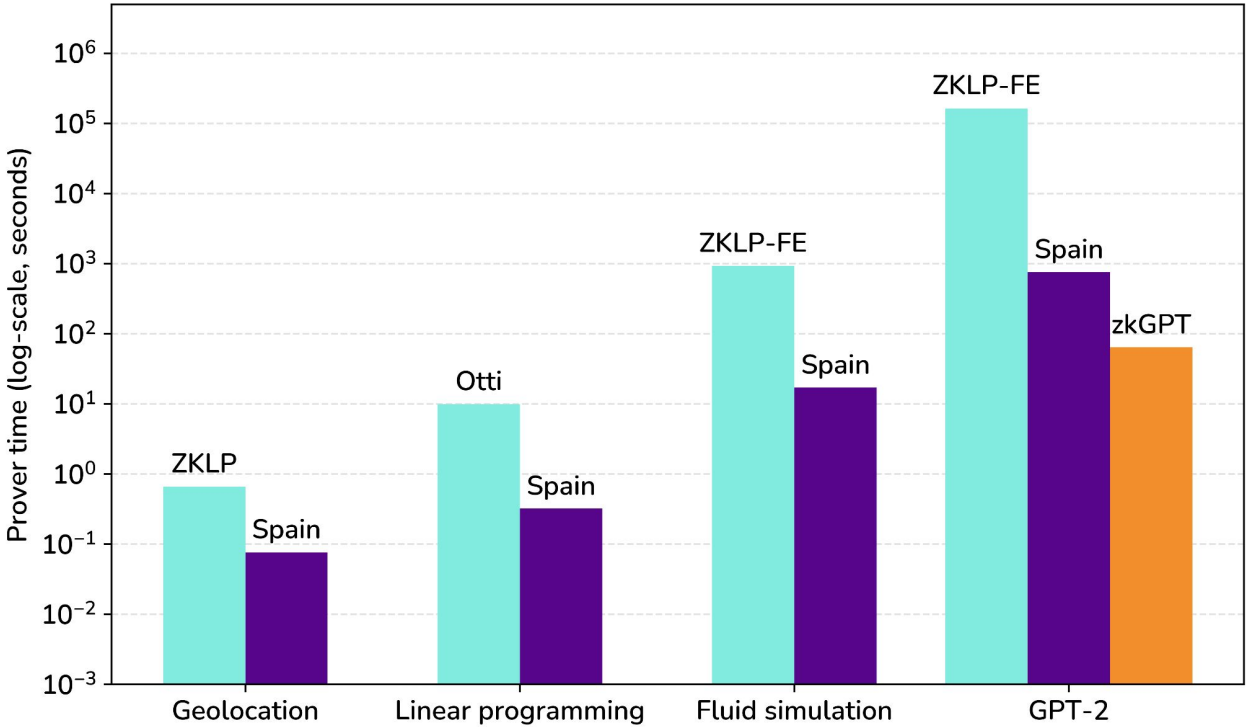
Spain results in dramatically more concise constraint representations



Spain proves numerical computations faster than the state of the art



Spain proves numerical computations faster than the (general-purpose) state of the art



zkGPT avoids the translation to constraints and directly encodes GPT-2 using custom cryptographic machinery

Related work generally falls into one of three categories

1. **Translation to constraints**: general but at the cost of prover runtime.

Ginger [‘12], Otti [‘22], Garg et al. [‘22], zkQMC [‘22], ZKLP [‘24], Kurik et al. [‘25]

Related work generally falls into one of three categories

1. **Translation to constraints**: general but at the cost of prover runtime.

Ginger [‘12], Otti [‘22], Garg et al. [‘22], zkQMC [‘22], ZKLP [‘24], Kurik et al. [‘25]

2. **Computation-specific proof systems**: very fast, at the cost of generality.

SafetyNets [‘17], zkCNN [‘21], ezkl [‘24], vCNN [‘24], ZKML [‘24], zkLLM [‘24], zkDL [‘24], zkGPT [‘25], and many more…

Related work generally falls into one of three categories

1. **Translation to constraints**: general but at the cost of prover runtime.

Ginger [‘12], Otti [‘22], Garg et al. [‘22], zkQMC [‘22], ZKLP [‘24], Kurik et al. [‘25]

2. **Computation-specific proof systems**: very fast, at the cost of generality.

SafetyNets [‘17], zkCNN [‘21], ezkl [‘24], vCNN [‘24], ZKML [‘24], zkLLM [‘24], zkDL [‘24], zkGPT [‘25], and many more…

3. **Approximate cryptographic machinery**: promising but currently slow

Chen et al. [‘22], Bitan et al. [‘26]

Spain’s takeaways and next steps

Spain is a succinct proof system that encodes **numerical computations** using **approximate constraints**.

This new formalism allows for proving the execution of numerical computations **significantly faster** than prior work.

Future work includes:

- applying Spain to a wider variety of numerical computations
- improving Spain's performance by combining with emerging cryptographic machinery