Constraint Solvers for the Working PL Researcher

Nadia Polikarpova

UCSDCSE
Computer Science and Engineering

The SAT/SMT Revolution

hardware verification

KLEE

Dafny

LiquidHaskell

software verification

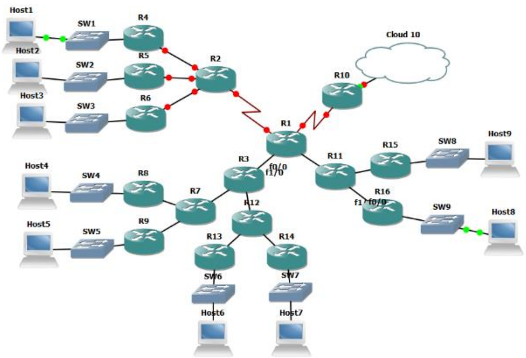
Rosette

Sketch

Leon

Synquid

software synthesis & repair



network configuration synthesis

biological modeling

architecture

Boolean SATisfiability

$$(\text{gin} \lor \text{tonic}) \land (\text{minor} \Rightarrow \neg\text{gin}) \land \text{minor}$$

Boolean SATisfiability

$$(\text{gin} \lor \text{tonic}) \land (\text{minor} \Rightarrow \neg\text{gin}) \land \text{minor}$$

Solution:

$\text{minor} \mapsto T$

$\text{gin} \mapsto F$

$\text{tonic} \mapsto T$

Satisfiability Modulo Theories

$$(\text{gin} \lor \text{tonic}) \land (\text{age} < 21 \Rightarrow \text{abv} = 0) \land (\text{age} = 20)$$

Satisfiability Modulo Theories

$(gin \lor tonic) \land (age < 21 \Rightarrow abv = 0) \land (age = 20)$

In the United States, "gin" is defined as an alcoholic beverage of no less than 40% ABV… Wikipedia

Satisfiability Modulo Theories

$$(\text{gin} \lor \text{tonic}) \land (\text{age} < 21 \Rightarrow \text{abv} = 0) \land (\text{age} = 20) \land (\text{gin} \Rightarrow \text{abv} \geq 40)$$

> In the United States, "gin" is defined as an alcoholic beverage of no less than 40% ABV…
>
> Wikipedia

Satisfiability Modulo Theories

$$(\text{gin} \lor \text{tonic}) \land (\text{age} < 21 \Rightarrow \text{abv} = 0) \land (\text{age} = 20) \land (\text{gin} \Rightarrow \text{abv} \geq 40)$$

$\text{age} \mapsto 20$

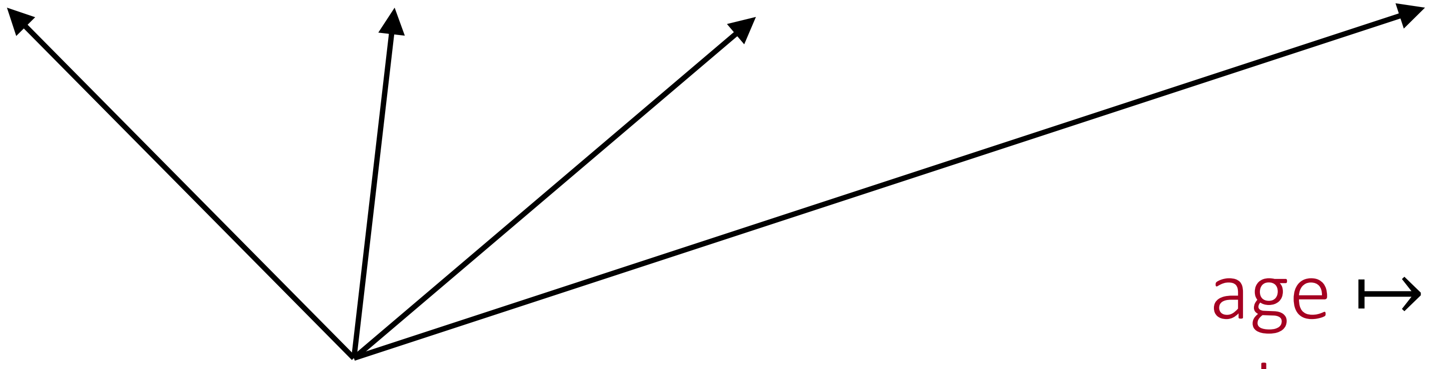
$\text{abv} \mapsto 0$

$\text{gin} \mapsto F$

$\text{tonic} \mapsto T$

Satisfiability Modulo Theories

$$(\text{gin} \lor \text{tonic}) \land (\text{age} < 21 \Rightarrow \text{abv} = 0) \land (\text{age} = 20) \land (\text{gin} \Rightarrow \text{abv} \geq 40)$$



theory of Linear Integer Arithmetic

$\text{age} \mapsto 20$

$\text{abv} \mapsto 0$

$\text{gin} \mapsto F$

$\text{tonic} \mapsto T$

Popular Solvers

Microsoft — Z3

Stanford — CVC4

SRI — Yices2

JKU Linz, Austria — Boolector

SMT competition: http://smtcomp.sourceforge.net

```
.smt2                // SMTLib format

(declare-fun (Int) age)
(declare-fun (Int) abv)
```

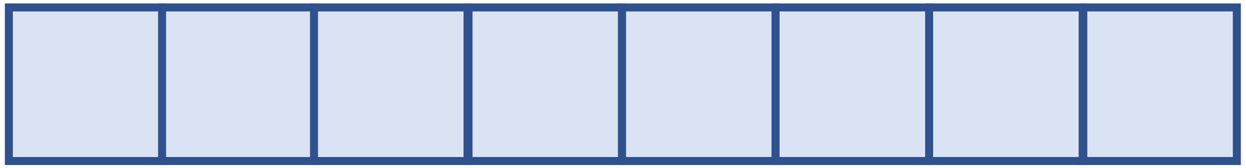
Plan for Today

How to use Z3 for:

1. Constraint programming
2. Program verification
3. Program synthesis

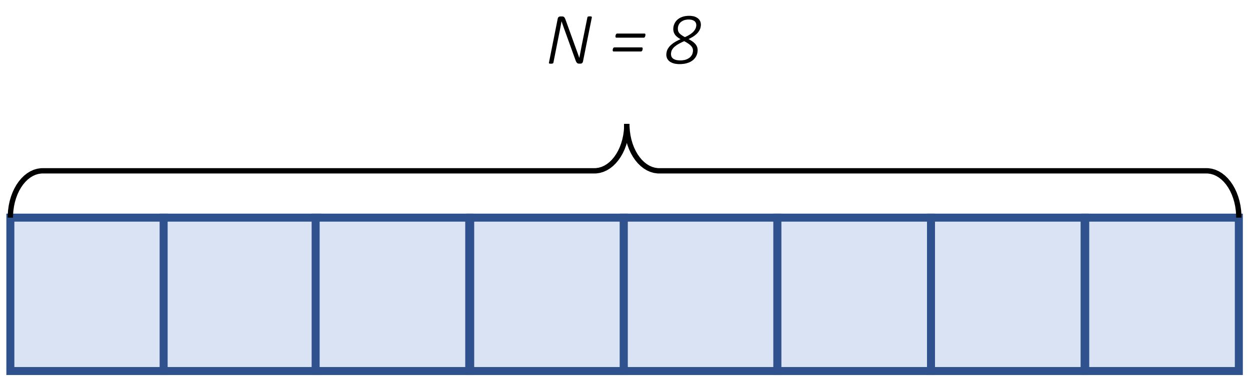
Problem: Array Partitioning

Partition an array of size *N* evenly into *P* sub-ranges



Problem: Array Partitioning

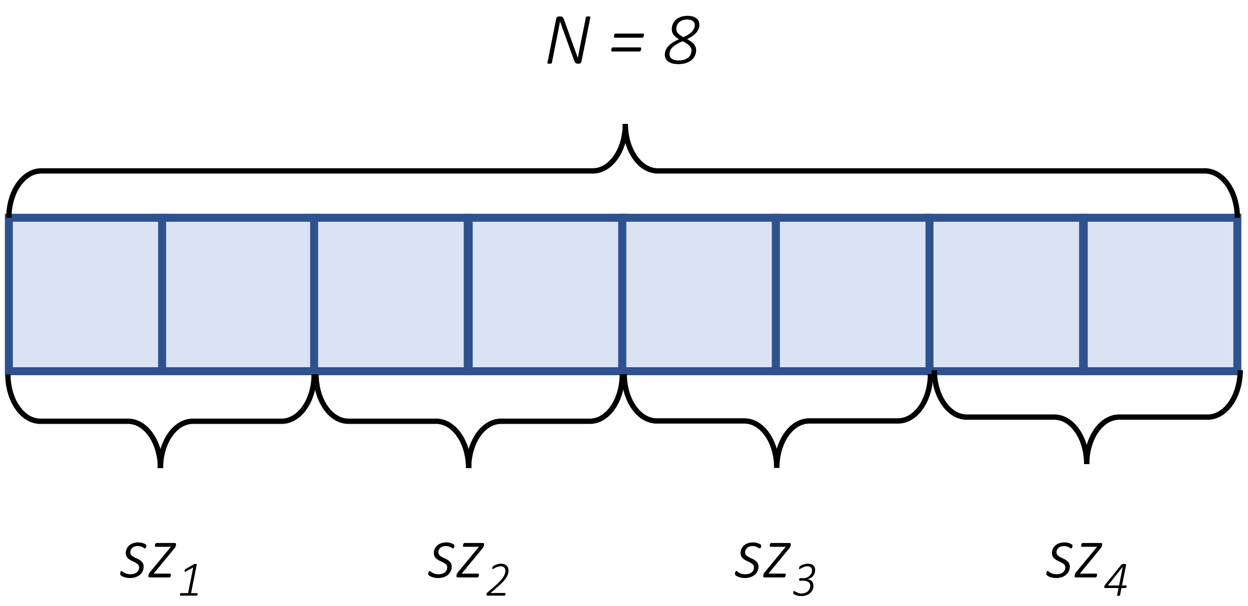
Partition an array of size *N* evenly into *P* sub-ranges



P = 4

Problem: Array Partitioning

Partition an array of size *N* evenly into *P* sub-ranges

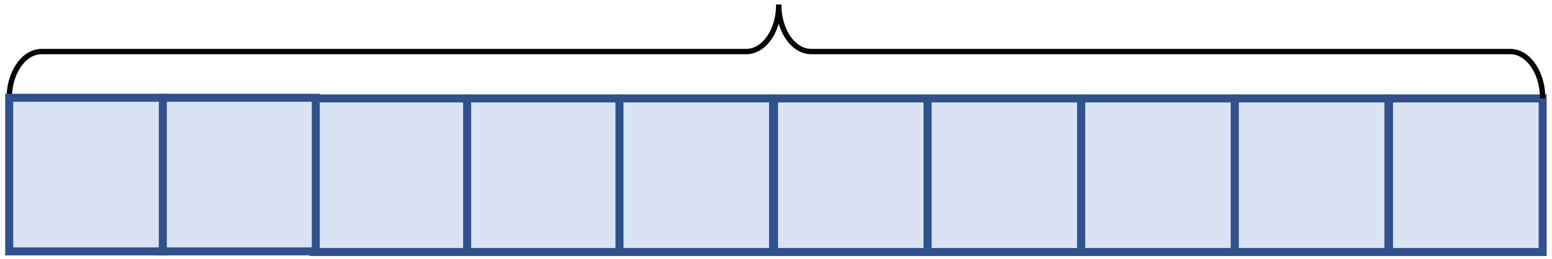


P = 4

Problem: Array Partitioning

Partition an array of size *N* evenly into *P* sub-ranges

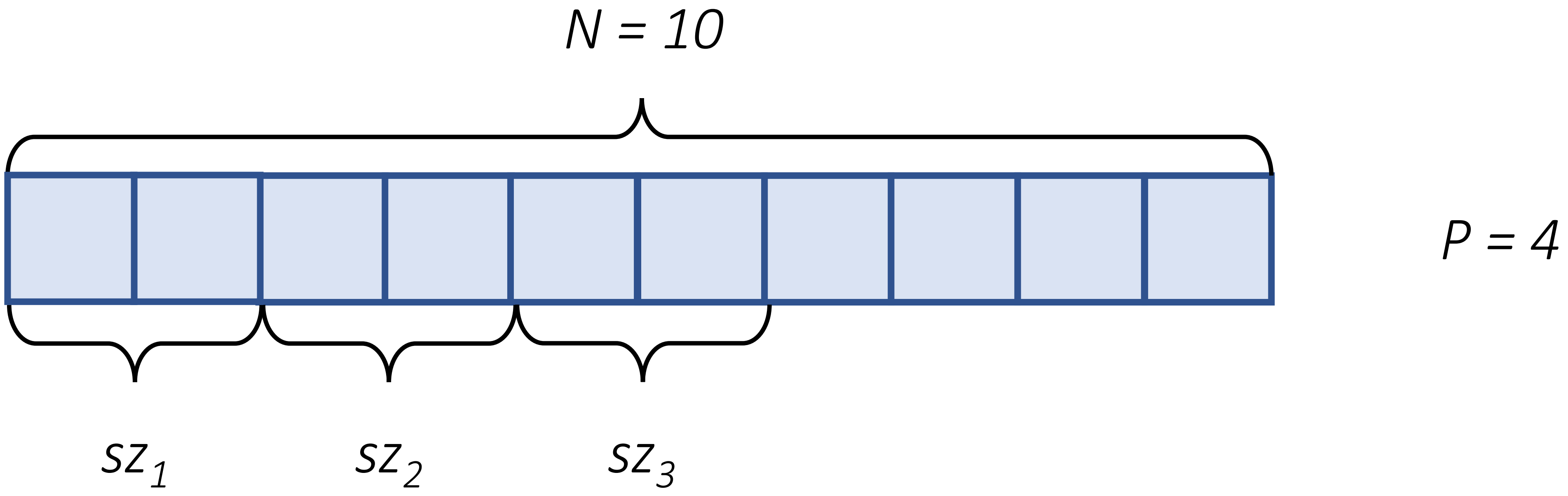
$N = 10$



$P = 4$

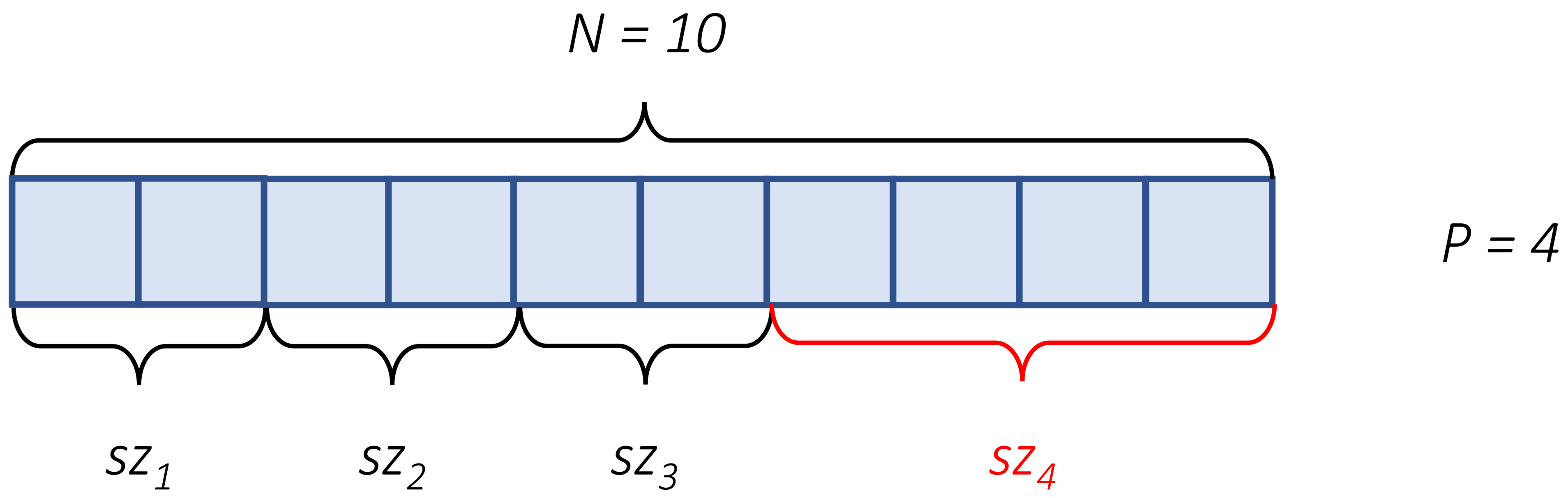
Problem: Array Partitioning

Partition an array of size *N* evenly into *P* sub-ranges



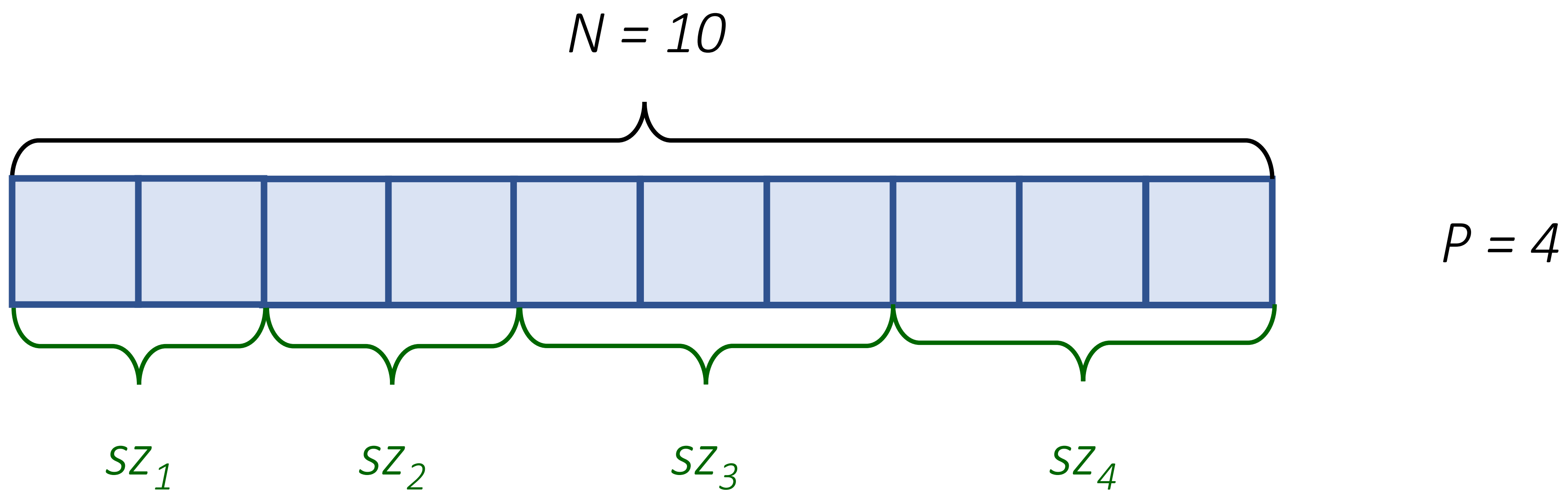
Problem: Array Partitioning

Partition an array of size *N* evenly into *P* sub-ranges



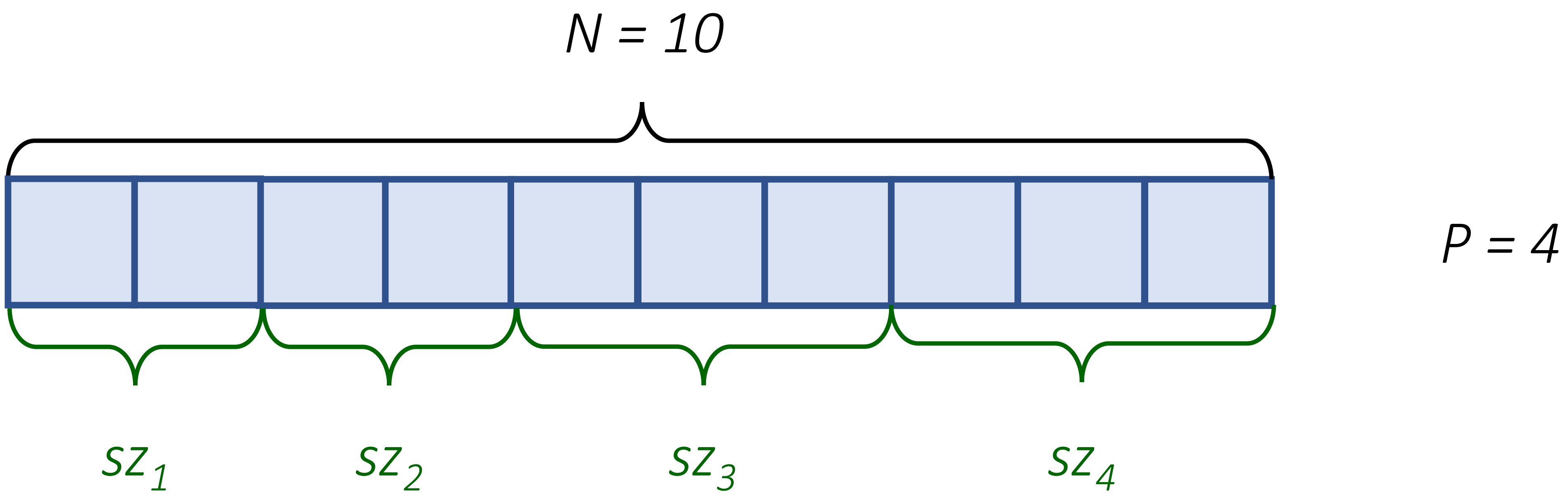
Problem: Array Partitioning

Partition an array of size N evenly into P sub-ranges



Problem: Array Partitioning

Partition an array of size *N* evenly into *P* sub-ranges



Can we always make them differ by at most 1?

Z3

to the rescue!

Plan for Today

How to use Z3 for:

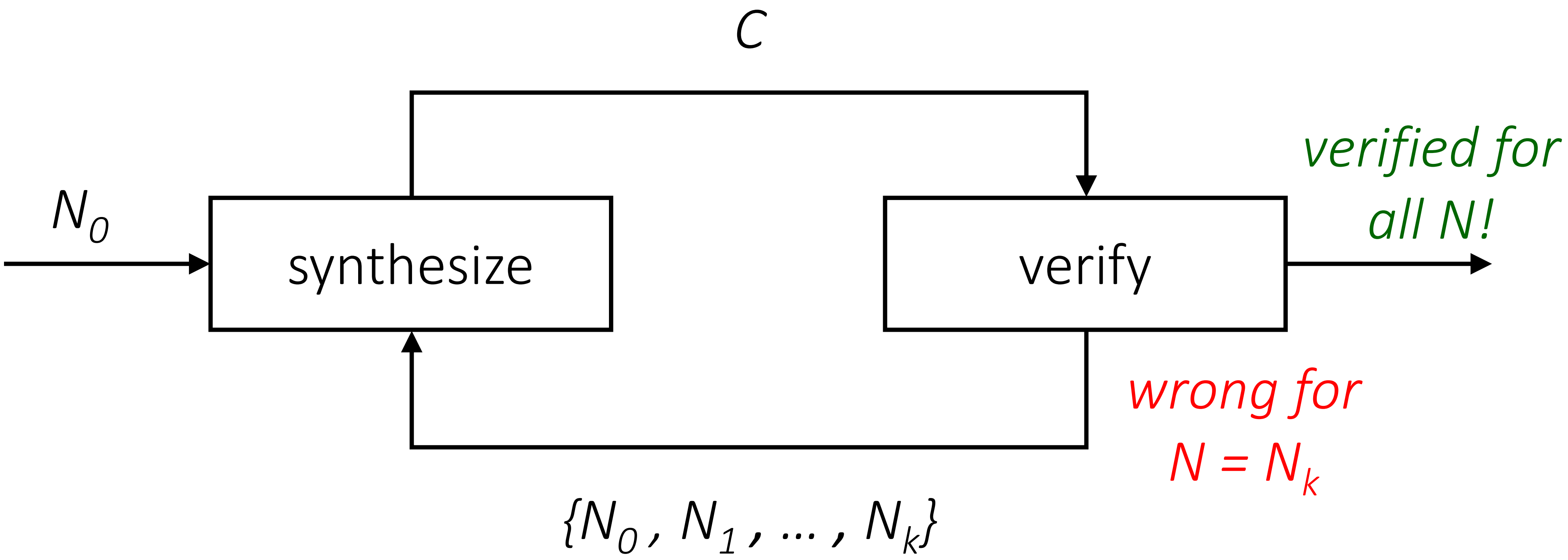
1. Constraint programming
2. Program verification
3. Program synthesis

Plan for Today

How to use Z3 for:

1. Constraint programming
2. Program verification
3. Program synthesis

CEGIS



C
N_0
synthesize
verify
verified for all N!
wrong for $N = N_k$
$\{N_0, N_1, \ldots, N_k\}$

What we have seen:

How to use Z3 for:

1. Constraint programming
2. Program verification
3. Program synthesis

You can find all the code from this talk here:

https://github.com/nadia-polikarpova/smt-talk