Synthesis of Diophantine equations

Thibault Gauthier

February 17, 2020

Can we teach conceptualization (synthesis) to a computer?

$$2, 4, 6, 8, \ldots$$

$$2, 4, 6, 8, \ldots$$

$$0, 1$$

$$2, 4, 6, 8, \ldots$$

$$0, 1$$

$$2, 4, 6, 8, \ldots$$

$$k - 2x = 0$$

$$0, 1$$

$$2, 4, 6, 8, \ldots$$

$$k - 2x = 0$$

$$0, 1$$

$$k(k-1) = 0$$

Diophantine equation:

$$P(k_1, \dots, k_n, x_1, \dots, x_m) = 0$$

Diophantine set:

$$\{\{k_1, \dots, k_n\} \mid \exists x_1 \dots x_m.\ P(k_1, \dots, k_n, x_1, \dots, x_m) = 0\}$$

Given a computable (recursively enumerable) set, find the Diophantine equation corresponding to the set.

Given a computable (recursively enumerable) set, find the Diophantine equation corresponding to the set.

Solved by Yu. V. Matiyasevich in 1970.

Given a computable (recursively enumerable) set, find the Diophantine equation corresponding to the set.

Solved by Yu. V. Matiyasevich in 1970.

Given a subset S of $\mathbb{Z}/16\mathbb{Z}$, find a polynomial $P(k, x, y, z)$ with maximal exponent 4 such as:

$$S = \{k \mid \exists xyz.\ P(k, x, y, z) = 0 \bmod 16\}$$

Representation of polynomials

$$[[1, 2, 3], [2, 0, 0, 4]]$$

$$1 \times k^2 \times x^3 + 2 \times k^0 \times x^0 \times y^4$$

$$k^2 \times x^3 + 2 \times y^4$$

Synthesis of polynomials

- Move to the next monomial and choose its coefficient
- Choose the exponent of the next variable in the monomial

State:

$$\text{targeted set: } \{1, 3, 7, 15\}$$

$$2 \times k^3 + 5$$

Moves:

$$2 \times k^3 + 5 \times k^2$$

$$2 \times k^3 + 5 + 6$$

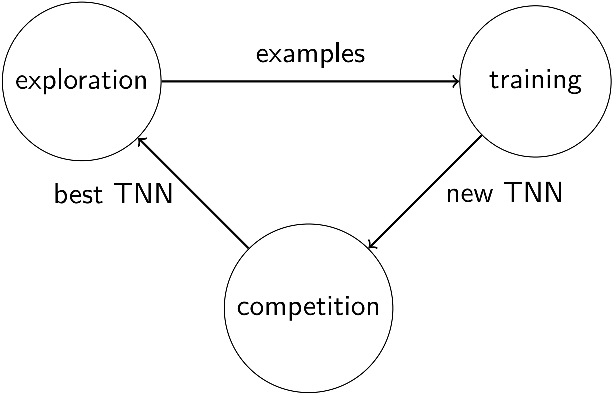
Winning condition:

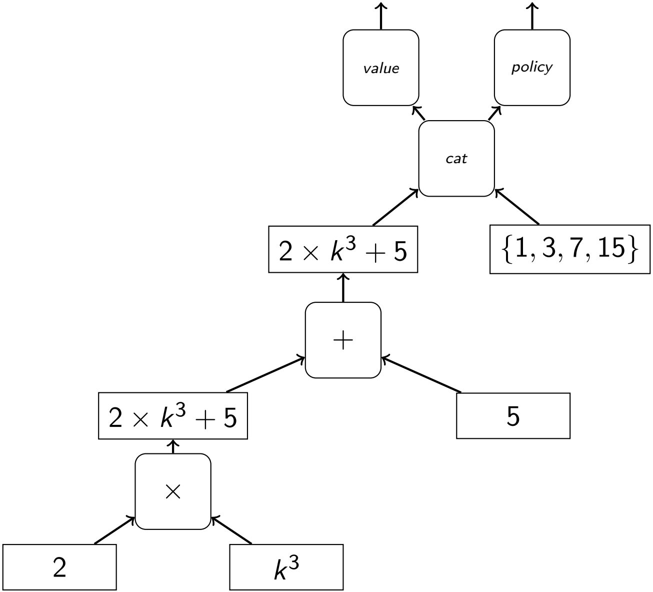
Diophantine set is equal to the targeted set.

A policy P is a function from $\mathbb{S}$ to $[0,1]^{cardinal(\mathbb{M})}$

A value V is a function from $\mathbb{S}$ to the interval $[0,1]$.

An example for the state s is a triple $(s, V(s), P(s))$.


exploration
examples
training
best TNN
new TNN
competition



value
policy
cat
$2 \times k^3 + 5$
$\{1, 3, 7, 15\}$
$+$
$2 \times k^3 + 5$
5
$\times$
2
k^3

How to get **balanced** and **adaptable** training examples?

From 2000 generated target sets, select 200:

- 100 positives and 100 negatives
- Probability: $\frac{1}{row(set)}$

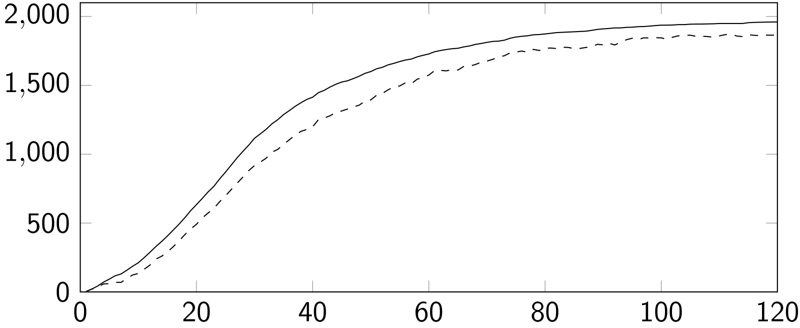


Figure: Number y of problems solved after generation x

Strategy	Train (2000)	Test (200)
breadth-first search	3.70	4.0
distance heuristic	3.05	2.0
TNN-guided	77.15	74.5

Table: Percentage of problems solved in 60 seconds

Demo

Bonus: Using combinators to do program synthesis?

$$(K\ x)\ y = x$$

$$((S\ x)\ y)\ z = (x\ y)(x\ z)$$

Problem:

$$\exists C.\ ((C\ x)\ y)\ z = (x\ z)\ y$$

Solution:

$$C = S\ (S\ (K\ (S\ (K\ S)\ K))\ S)\ (K\ K)$$

Training

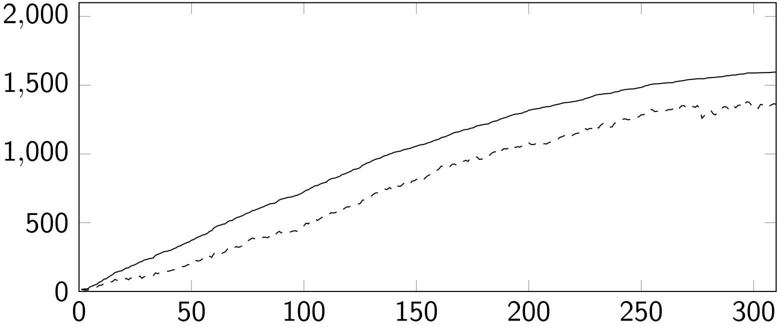


Figure: Number y of problems solved after generation x

Results

Prover	Strategy	Train (2000)	Test (200)
E prover	auto	38.80	36.0
	auto-schedule	50.35	48.5
Vampire	default	4.15	3.5
	mode casc	63.45	62.0
$\text{MCTS}_{combinators}$	breadth-first search	27.65	27.0
	TNN-guided	72.7	65.0

Table: Percentage of problems solved within 60 seconds