ISCAS 中国科学院软件研究所学术年会’2023
暨计算机科学国家重点实验室开放周

学术论文

ACM SIGSOFT DISTINGUISHED PAPER

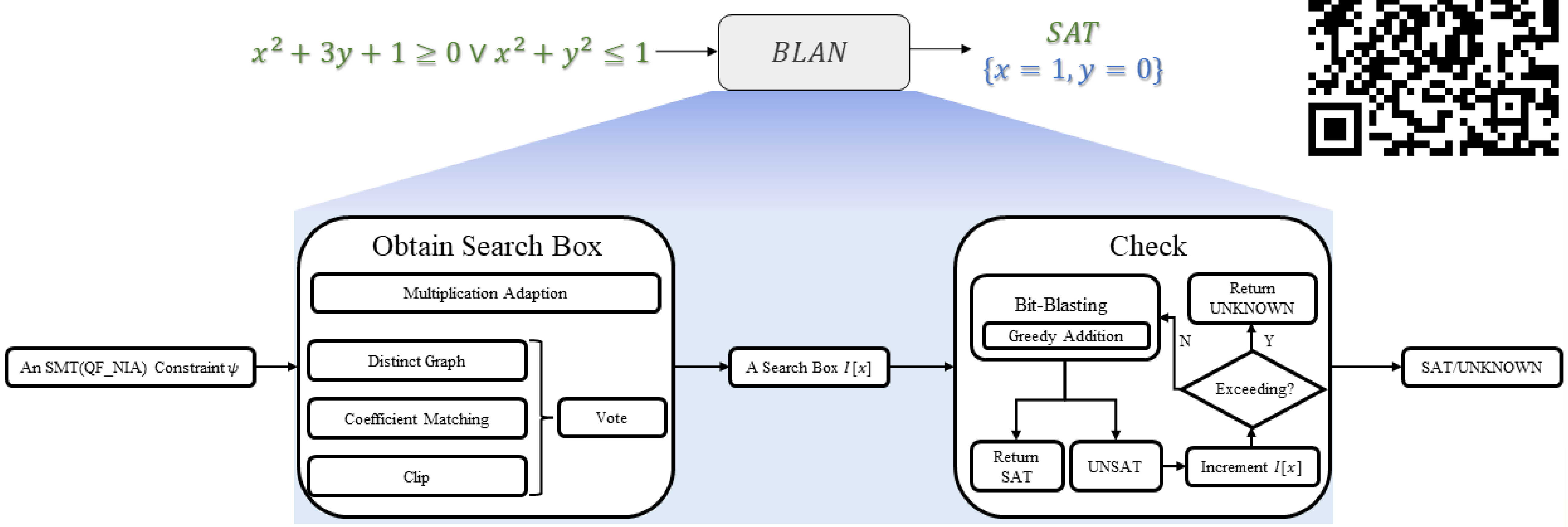
Improving Bit-Blasting for Nonlinear Integer Constraints

Fuqi Jia, Rui Han, Pei Huang, Minghao Liu, Feifei Ma, Jian Zhang
32nd International Symposium on Software Testing and Analysis (ISSTA ’23)
Contact: Feifei Ma, maff@ios.ac.cn

Introduction

The paper focuses on solving a general form of nonlinear integer arithmetic constraint: (SMT(QF_NIA)). It is the boolean combination (logic operators: ∧,∨,¬) of nonlinear integer arithmetic constraints, involving equations and inequalities. As they often appear in software/hardware verification and analysis, a practical algorithm for the problem is still highly desirable.

BLAN Solver



Heuristics for obtaining a proper search box

Multiplication Adaptation: $B_{MA} = \max(\beta - \lceil \alpha m \rceil, L)$;
Distinct Graph: $W_{DG}(x) = \lceil \log_2(\deg(x) + 1) \rceil$;
Coefficient Matching: $W_{CM}(x) = \left\lceil \log_2 \frac{\max_i |c_i|}{|c_x|} \right\rceil + 1$;
Clip: $W(x) = \min\big(K, \max\big(W_{DG}(x), W_{CM}(x)\big)\big)$;
Vote: $p(w) = \frac{\#(W(x)=w)}{|\mathcal{V}_{int}|}, x \in \mathcal{V}_{int}$;
$B_{VO} = \max(\{w | p(w) > \gamma\} \cup \{0\})$.

Algorithm 1 Greedy Addition (GA)

Input : X: a set of bit vectors.
Output: $\bar{z}$: the resulting bit vector.

```
while Size of X > 1 do
    $\bar{s}, \bar{t}$ ← the two bit-vectors with smallest bit-widths.
    remove $\bar{s}$ and $\bar{t}$ from $X$.
    $\bar{y}$ ← $\bar{s} + \bar{t}$ and add $\bar{y}$ into $X$.
end while
$\bar{z}$ ← $X[0]$.
return $\bar{z}$.
```

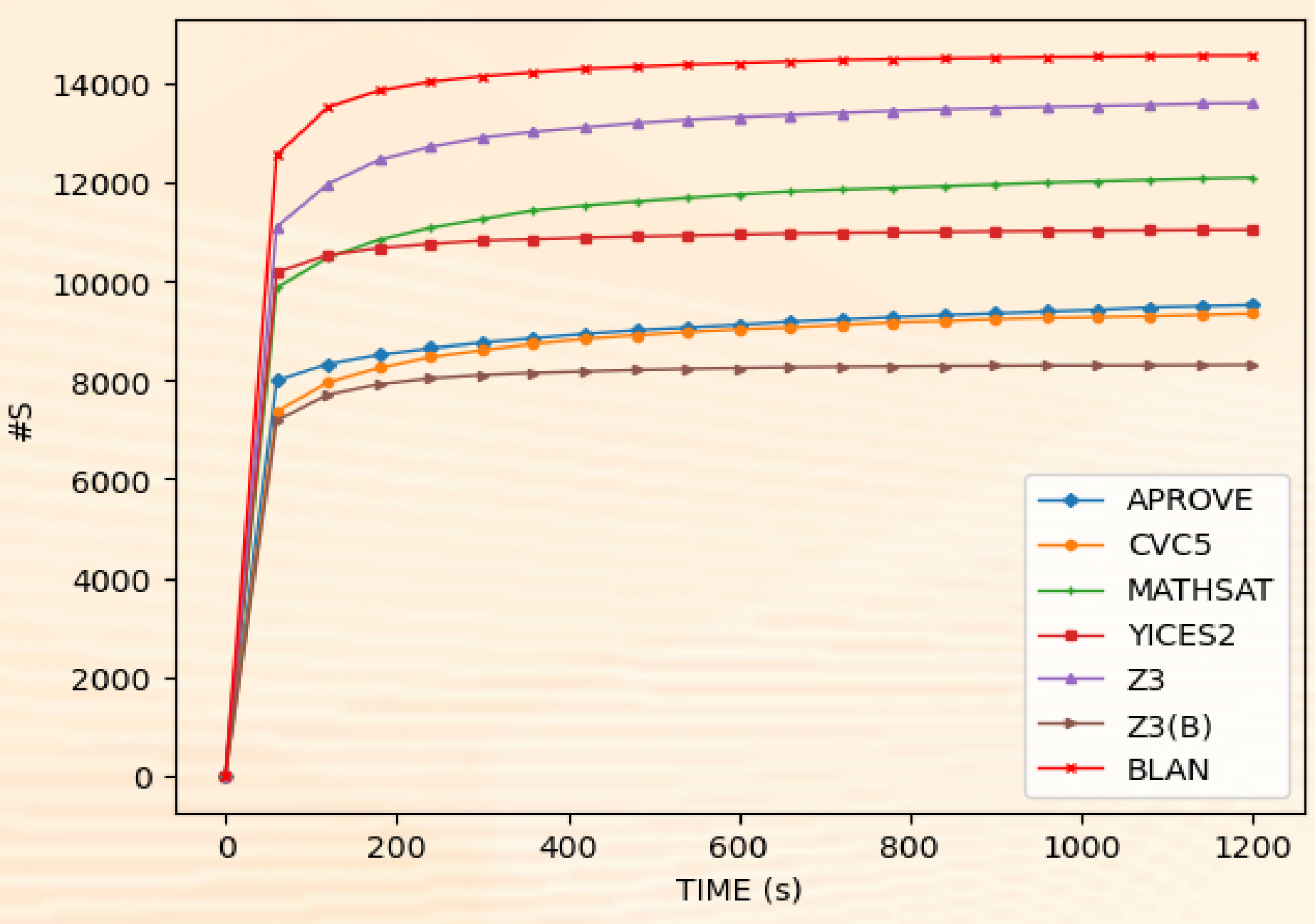
Optimal bit-vector addition algorithm (Greedy Addition)

Theorem 1: *Given a set of bit vectors X, B(X, GA) is minimal for a successive addition on X.*
Theorem 2: *For a successive addition on X, Algorithm 1 will produce a resulting bit vector z with the smallest bit-width.*

Experiments

- We compare other state-of-the-art SMT solvers: APROVE,CVC5, MATHSAT, YICES2 and Z3. The experiments show the advantages both in solving ability and speed.

Solvers	AProVE	calypto	Dartagnan	LassoRanker	Leipzig	MCM	CInteger	ITS	SAT14	MathProblems	Total	#U
APROVE	**1663**	77	0	9	**161**	0	667	6291	0	647	9515	8
CVC5	1354	79	**7**	**10**	94	13	320	5448	1788	230	9343	0
MATHSAT	1639	79	**7**	**10**	128	13	707	7553	1770	193	12099	16
YICES2	1591	79	6	**10**	101	10	511	6783	1837	112	11040	9
Z3	1658	**80**	**7**	**10**	159	15	760	8397	**1852**	659	13597	15
Z3(B)	1630	59	0	**10**	**161**	0	678	4878	244	658	8318	0
BLAN(ours)	1662	**80**	**7**	**10**	**161**	**29**	**837**	**9243**	1845	**688**	**14562**	**422**


#S
TIME (s)
APROVE
CVC5
MATHSAT
YICES2
Z3
Z3(B)
BLAN