Towards Building A Scalable Bit-vector Model Counter

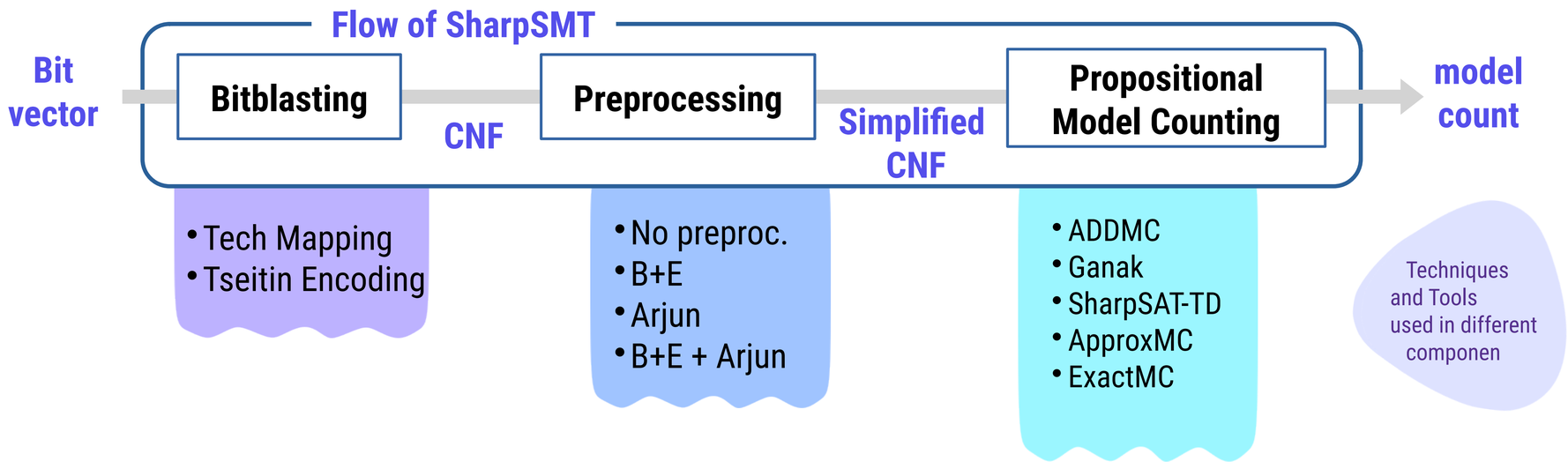
Arijit Shaw
Chennai Mathematical Institute
IAI, TCG-CREST
Kuldeep S. Meel
National University of Singapore

= vector of bits
A theory in SMT

MODEL = satisfying assignment to formula
Model Counter Counts Models

{ A **bitvector model counter** returns the number of model of a bitvector formula. }

We designed a bitvector model counting portfolio **SharpSMT,** that leverages the progress made in propositional model counting in last two decades. Given a formula, SharpSMT works in the following way:



MOTIVATING EXAMPLE

$$x_1 = 0$$
$$x_1 \leq x_2$$
$$x_2 \leq x_3$$
$$\dots$$
$$x_9 \leq x_{10}$$
$$x_{10} \leq x_1$$

Count the number of solutions of the formula,
each x_i is a 32 bit bitvector.

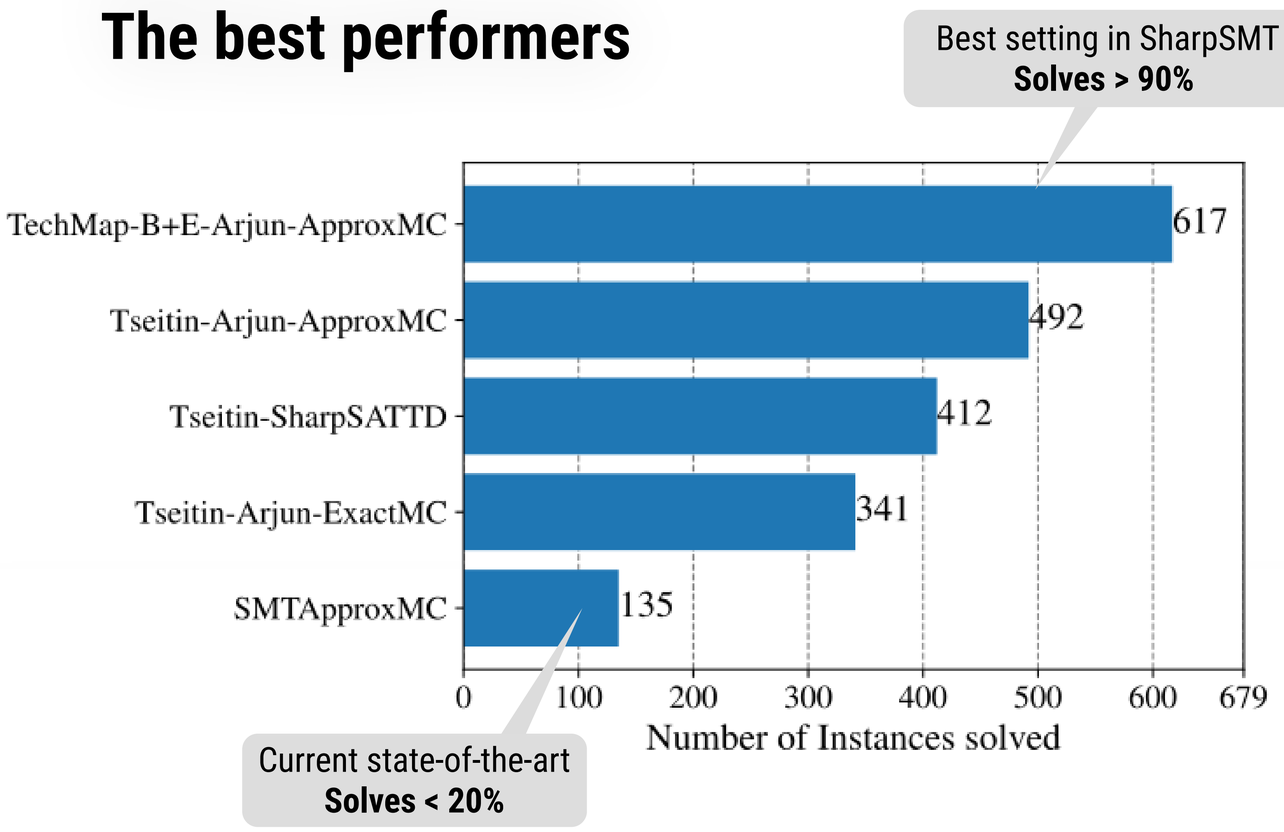
SharpSMT can be run in any of (2x4x5=) **40** possible combinations. We did experiments to find which combinations are the best! Experiments with **679 benchmarks** from cryptography, model checking, older literature. Timeout = 3600s

Applications:

1. Software model checking
– quantitative properties
2. Cryptography
3. Computational Biology

RESULTS

The best performers



TAKEAWAY

For bit-vector model counting, our portfolio performs 4X the current state of the art.

The best performing systems are as follows:

1. for **Approximate Count**:

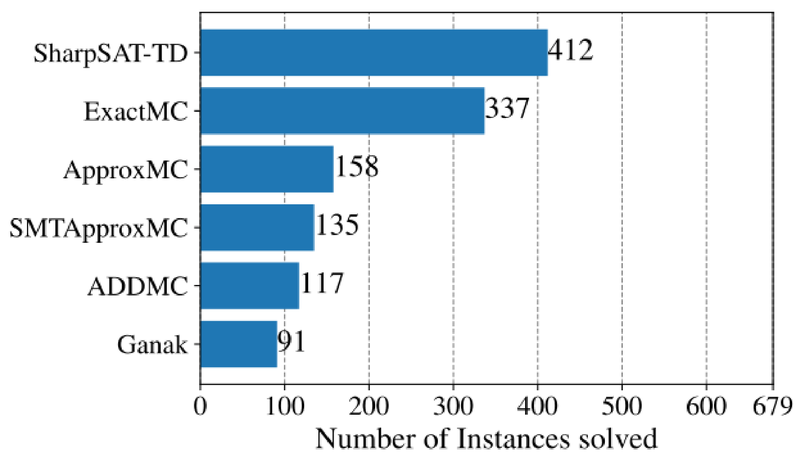
TechMap → B+E → Arjun → ApproxMC

2. for **Exact Count:**

Tseitin Encoding → SharpSAT-TD

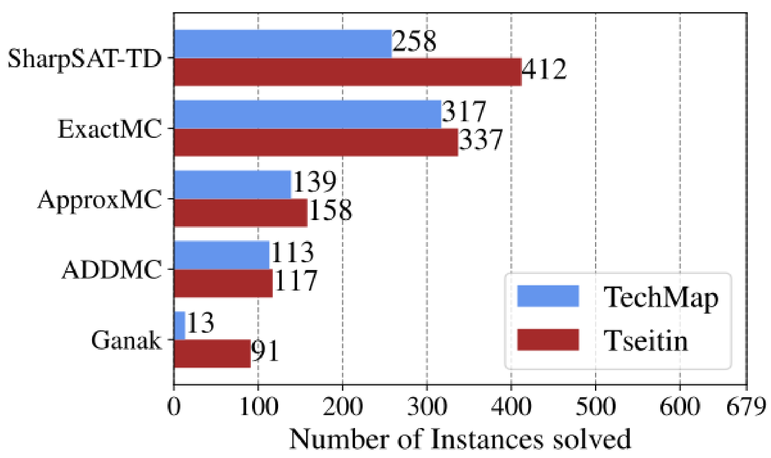
Comparison of Model Counters

Tseitin Encoding / No Preprocessing



Comparison of Bitblasting Methods

No Preprocessing



Comparison of Preprocssing Methods

Tseitin Encoding