Look-ahead for solving hard SAT problems

Oliver Kullmann

Computer Science Department
Swansea University

Dagstuhl Seminar: SAT and Interactions
September 23, 2016

Pythagorean triples I

Theorem (Heule, Kullmann, and Marek [10])

For every partition of $\mathbb{N} = \{1, 2, \ldots\}$ into two parts, one part contains a Pythagorean triple $a^2 + b^2 = c^2$.

- For example, decomposing $\mathbb{N}$ into even and odd natural numbers: Exercise for you.
- Open for more than 30 years (Croot and Lev [3]).

Pythagorean triples II

More precisely:

- $\{1,\ldots,7824\}$ can be partitioned into two parts such that no part contains a Pythagorean triple.
- In other words, the hypergraph of Pythagorean triples in $\{1,\ldots,7824\}$, i.e.,

$$\big\{\,\{3,4,5\},\{6,8,10\},\{5,12,13\},\ldots,\{1196,7728,7820\}\,\big\},$$

  with 9465 triples, is 2-colourable (can be coloured with two colours, such that no hyperedge is monochromatic).
- While the hypergraph of Pythagorean triples in $\{1,\ldots,7825\}$ (seven more triples) is not 2-colourable.

Pythagorean triples III

For the SAT-representation

use boolean variables $v_1, \ldots, v_{7825}$.

Now the clause-set is

$$\Big\{ \{v_3, v_4, v_5\}, \{\overline{v_3}, \overline{v_4}, \overline{v_5}\},$$
$$\ldots$$
$$\{v_{625}, v_{7800}, v_{7825}\}, \{\overline{v_{625}}, \overline{v_{7800}}, \overline{v_{7825}}\} \Big\}.$$

This is a 3-CNF, with $n = 7825$ and $c = 2 \cdot 9472 = 18944$.

Asymptotically, the number of clauses is $\frac{1}{\pi} n \ln(n)$.

Pythagorean triples IV

This result got a lot of media attention:

1. See `http://www.cs.utexas.edu/~marijn/ptn/` for links.
2. One aspect was that a long outstanding mathematical problem was solved with a super-computer.
3. Another aspect was that the extracted (DRAT) proof had the length of 200 terabytes ("longest proof ever").

Still

the story of SAT is mostly untold.

We solved the problem with the **Cube-and-Conquer** method, mixing old and new SAT solving.

This seems the best current method for solving hard problems.

Outline

Reminders

C&C is a hybrid method, using

look-ahead solvers to split the problem (CUBE)

and then apply CDCL-solvers

solve the sub-problems (CONQUER).

I use

- $\mathcal{CLS} = \mathcal{SAT} \cup \mathcal{USAT}$ for the set of clause-sets.
- $r_1 : \mathcal{CLS} \to \mathcal{CLS}$ for unit-clause propagation.
- $r_2 : \mathcal{CLS} \to \mathcal{CLS}$ for (complete) failed-literal elimination, that is, repeat the following until fixed point:

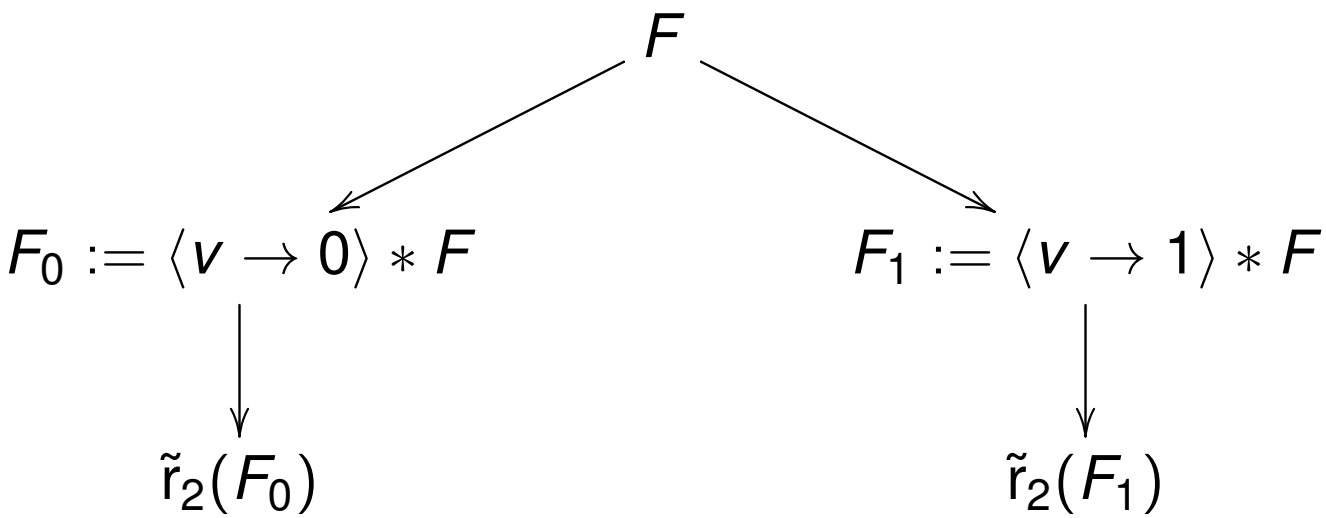
  Search for a literal x with $\bot \in r_1(\langle x \to 0\rangle * F)$,
  and reduce $F \rightsquigarrow \langle x \to 1\rangle * F$.

Look-ahead solvers I

For background see the two Handbook-chapters Heule and van Maaren [7], Kullmann [13]:

Split recursively, applying (strong) reductions.

That is, for input $F \in \mathcal{CLS}$, choose variable $v \in \mathrm{var}(F)$ and split



for some reduction $\tilde{r}_2 : \mathcal{CLS} \to \mathcal{CLS}$ (e.g., elimination of failed literals).

Look-ahead solvers II

Remarks:

- Application of partial assignments is done “eagerly”, since otherwise computation of $\tilde{r}_2$ becomes too expensive.
- Since we are interested only in UNSAT here, we ignore the question of the choice of the first branch.

Look-ahead solvers III

History:

1. Freeman [5] introduced the idea of look-ahead into the literature with his solver `Posit`.
2. Li and Anbulagan [14] refined this (now also partially using r_3, and introducing the product-rule) with the solver `satz` (code maintained at `https://github.com/OKullmann/oklibrary/blob/master/Satisfiability/Solvers/Satz/satz215.2.c`.
3. The `OKsolver` ([12]), successful in the first SAT-competition 2002, a "theoretical" look-ahead solver, used (complete) r_2 and autarky search, and, based on the worst-case 3-SAT upper bound [11], introduced the idea of counting *new clauses*; maintained at `https://github.com/OKullmann/oklibrary/tree/master/Satisfiability/Solvers/OKsolver/SAT2002`.
4. The `march` solvers Heule [8] extended these developments.

   `http://www.st.ewi.tudelft.nl/~marijn/sat/download.php`

Look-ahead solvers IV

5. The `tawSolver` (Ahmed, Kullmann, and Snevily [1]) finally implemented the original DLL-algorithm Davis, Logemann, and Loveland [4], with a modern heuristics, and some form of lazy data-structure (zero look-ahead); available at `https://github.com/OKullmann/oklibrary/blob/master/Satisfiability/Solvers/TawSolver/tawSolver.cpp`.

Even the `tawSolver` is best on some (combinatorial) instances.

The ideal heuristics

Here (different from CDCL) the ideal heuristics is actually productive:

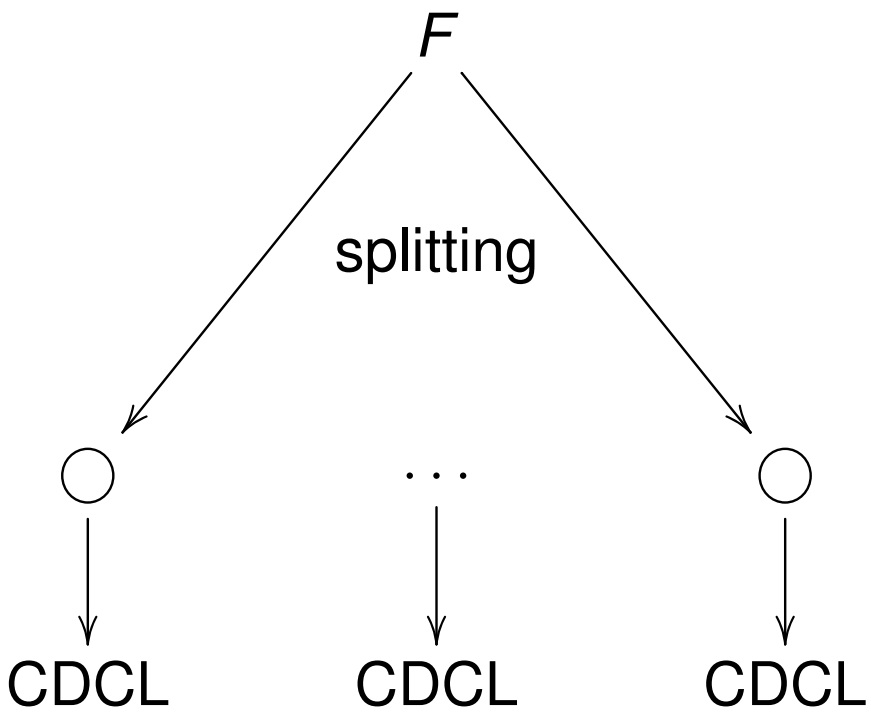
Choose a variable such that
the sum of the tree-sizes for $\tilde{r}_2(F_0)$ and $\tilde{r}_2(F_1)$
is minimal.

We will see schemes to “approximate” this.

A hybrid scheme

The **C&C paradigm** ([9]) has two phases:

1. First a look-ahead solver is employed to split the problem — the splitting tree is cut off appropriately.
2. At the leaves of the tree, CDCL solvers are employed.



First goal: parallelisation

The number N of leaves for the cube-phase is roughly

- in the thousands for relatively easy problems (say one day total run-time);
- in the millions for hard problems (say a month total run-time);
- in the billions for very hard problems.

The sub-problems should be at most one minute.

C&C achieves a good equal splitting
(that's what look-ahead is good at!).
The sub-problems (for CDCL) are scheduled independently.

- So a great **linear speed-up** for a large number of processors.
- The cube-phase has also **controlled run-time**.
- And the sub-problems can be **easily uniformly sampled**.

That's it?

So well, that's something:

- Hard problems need distributed solving.
- C&C delivers this, scaling very well.
- That's also quite natural:

The **tree-structure** is optimal for this.
Look-ahead heuristics prefer **equal splittings**.

But that's not the end of the story ...

Cube and Conquer: The discovery

For experiments with (hard) instances from Ramsey theory (van-der-Waerden; Ahmed et al. [1]), I made the following observation:

1. I just wanted to be able to easily monitor progress, and possibly do parallelisation.
2. So I took my own look-ahead solver, the `OKsolver` ([12]), using it to split the instances into a *large number N* of sub-instances, cutting off the splitting tree, and at the leaves I ran a CDCL-solver.
3. When the splitting was done *reasonably*, so that the leaf-instances are roughly of the same hardness, then the total run time, even with a very simple implementation,

   was **MUCH LOWER** than
   what any single solver could achieve.

Something's going on I

Consider again N (the number of leaves in the cube-phase):

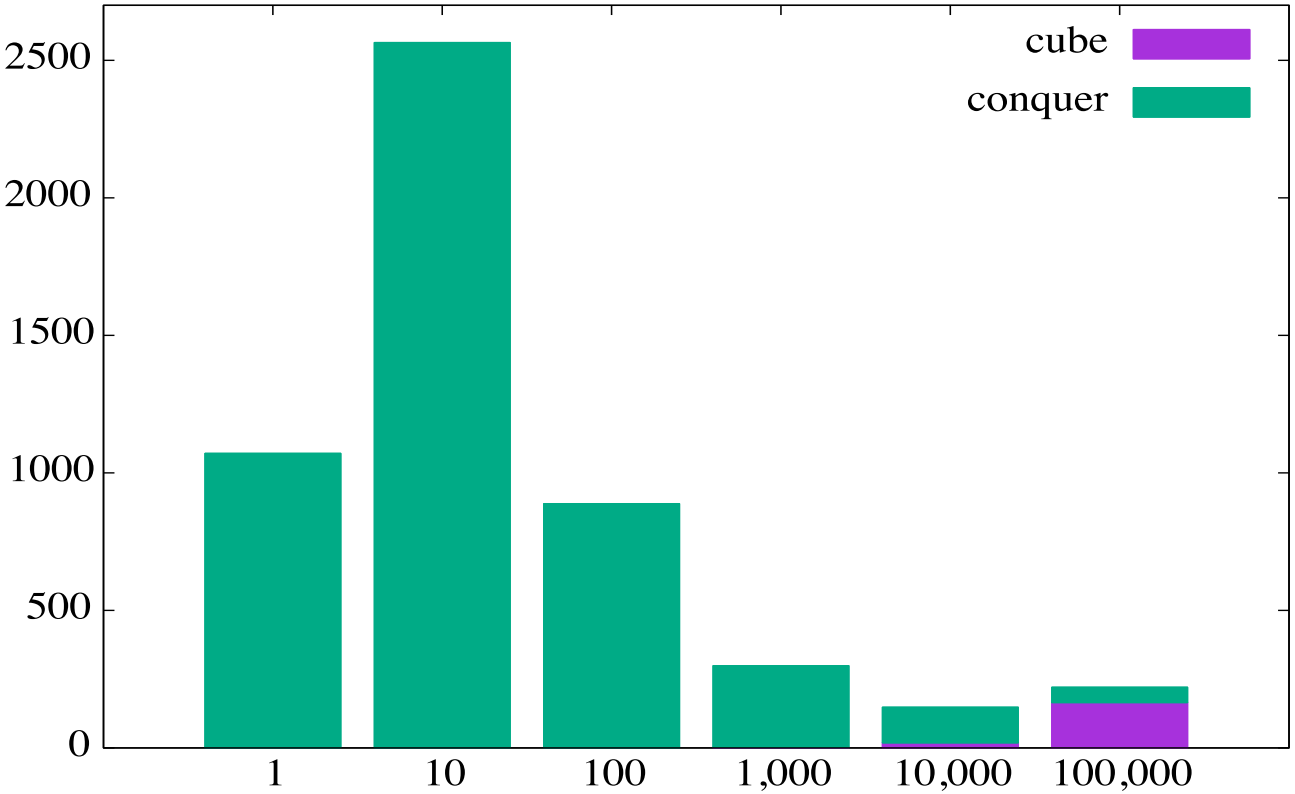
1. $N = 1$ means pure CDCL.
2. Very large N means pure look-ahead.

Now consider the total run-time in dependency on N:

1. Typically, first it increases,
2. then it **decreases** (only for a **large** number of sub-problems!),
3. then it stays for some time at a plateau,
4. and finally it typically increases again (often dramatically, but not for the Pythagorean triples problem).

In the area of optimal N,
the total run-time can be several orders of magnitudes faster
than any single method!!

Something's going on II



Example with Schur triples $a + b = c$
and 5 colours: a clause-set with
708 variables and 22608 clauses.

Why are CDCL solvers often better than look-ahead?

Three approaches to explain the advantage of CDCL:

- Look-ahead is basically tree-like (recursive splitting), while CDCL is dag-like (can *reuse* "lemmas").
- CDCL is more "optimistic", looks out for a "weakness", while look-ahead assume the worst-case.
- CDCL is "less intelligent", but "much faster".

It seems the instances where look-ahead is better are

"consistently hard",

(like random formulas), while for CDCL there must be "soft spots".

None of these approaches seems to be able
to explain the C&C phenomenon.

Open Problems I

Although not the main topic here:

> Explain (theoretically and practically) where look-ahead is best.

Two directions

Two basic opposite hypothesis' about the C&C phenomenon:

I It's a **weakness** of CDCL (resp. current implementation): these solvers have a "point of competence" — you can't run CDCL solvers for a long time.

II It's a **strength** of look-ahead: look-ahead "understands" better the "global structure".

Cube and Conquer: Global versus Local

Our current approach for explaining the success is as follows:

1. In some sense, the heuristic of look-ahead is “global”, the heuristic for CDCL is “local”.
2. The worst-case approach of look-ahead is good for splitting (globally), but not for solving (exploiting local structures).
3. The dag-like structures, exploited by CDCL, are somewhat of a “local” phenomenon.

In any case, this motivates to look again at the

branching heuristics (splitting heuristics)
for look-ahead solvers.

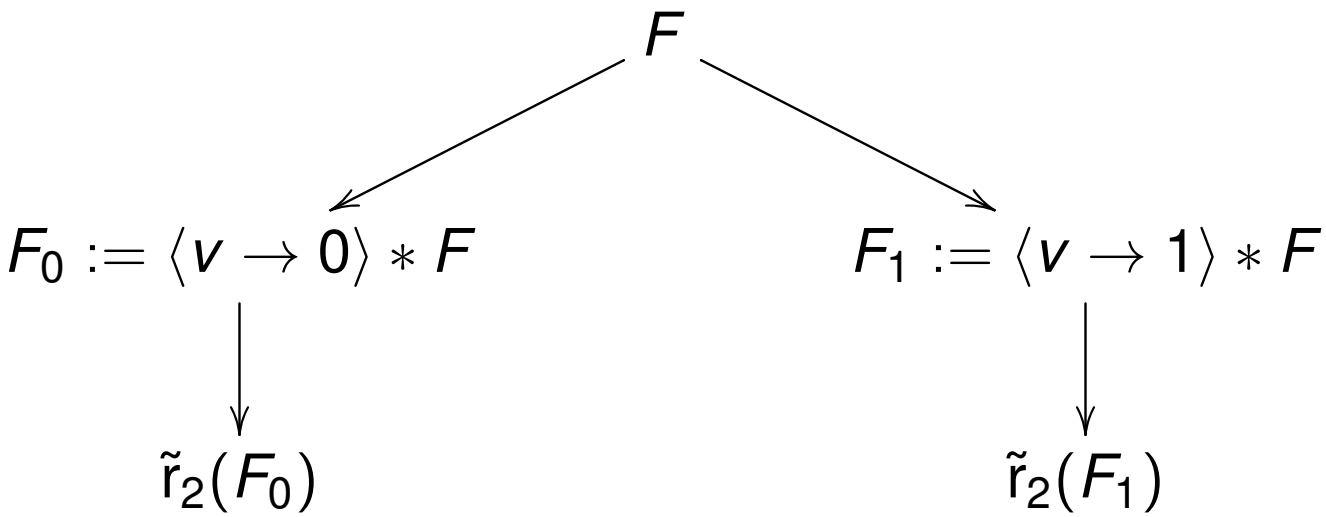
Open Problems II

Explain (theoretically and practically) why and where C&C is best.

It seems some form of “hybrid” proof theory is needed.

Where's the look-ahead? I

Recall



The "look-ahead" means that:

- for the choice of v,
- the effect of the reduction after splitting
- is partially considered (by actually *running* the reductions).

Where's the look-ahead? II

Now you can't run the full reduction:

and so a simpler version
$\tilde{r}_1 : \mathcal{CLS} \to \mathcal{CLS}$
is used (and run).

For example

- $\tilde{r}_1$ is UCP (r_1), while $\tilde{r}_2$ is failed-literal elimination (r_2).
- If we use $\tilde{r}_1$ the identity, while $\tilde{r}_2$ is UCP, then we get original DLL (Davis et al. [4]). A modern implementation is `tawSolver` ([1]), which can be fastest on selected benchmarks.

Thus for the heuristic

look-ahead runs through all splittings
$\big(\tilde{r}_1(\langle v \to 0\rangle * F),\ \tilde{r}_1(\langle v \to 1\rangle * F)\big)$
for $v \in \mathrm{var}(F)$,
and determines the best splitting.

A general theory

The following theory of branching heuristics has been developed (see Handbook chapter [13]):

1. Considered are **branchings** $F \rightsquigarrow (F_1, \ldots, F_m)$.
2. A notion of **distance** $d(F, F') \in \mathbb{R}_{>0}$ is needed: the larger, the more progress.
3. We obtain **branching tuples**

$$\big(d(F, F_1), \ldots, d(F, F_m)\big) \in \mathcal{BT} := \bigcup_{m \in \mathbb{N}} \mathbb{R}^m_{>0}.$$

4. Finally a **projection** $\rho : \mathcal{BT} \to \mathbb{R}$ is needed.

Choose a branching with minimal projection value.

Examples

Please sort ("$\prec$" means "better"):

- $(3, 6)$
- $(4, 6)$
- $(4, 5)$
- $(2, 8)$
- $(3, 9, 13)$

Clearly:

- $(4, 6) \prec (3, 6)$
- $(4, 6) \prec (4, 5)$

Symmetry is preferred:

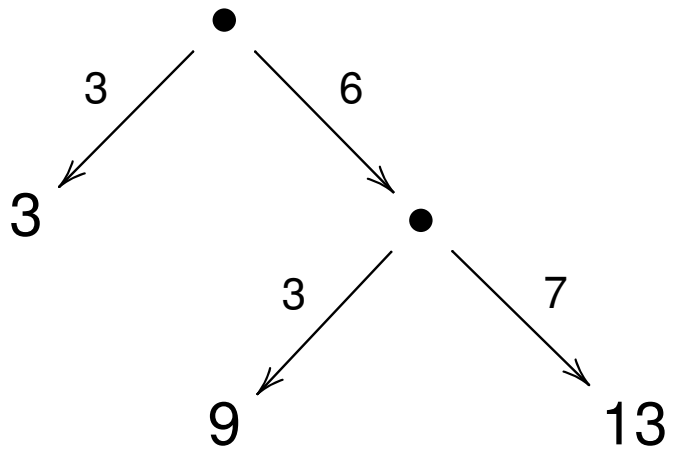
- $(4, 5) \prec (3, 6)$
- $(4, 6) \prec (2, 8)$

Composition of branching tuples

We furthermore have

$$(3, 9, 13) \prec (3, 6)$$

since



We can compare branching tuples by composition (including expansion)!

Canonical projection

It is shown ([13]) that under rather general (**axiomatic**) conditions

there is exactly one **canonical linear order** $\preceq$ on $\mathcal{BT}$.

The naturally associated **canonical projection** is

$$\tau((d_1, \ldots, d_m)) = \text{ that } x > 1 \text{ with } \sum_{i=1}^{m} x^{-d_i} = 1.$$

(To show uniqueness, tuples of *arbitrary width* are required.)

Evaluating the examples

- $(3, 6)$: 1.1739
- $(4, 6)$: 1.1509
- $(4, 5)$: 1.1673
- $(2, 8)$: 1.1748
- $(3, 9, 13)$: 1.1695

- Via composition we can not decide all cases.
- In general the decidability of the theory of $(\mathbb{R}, +, \cdot, \leq)$ can be employed, when the entries are roots of polynomials with integer coefficients, yielding actually polytime decision here.
- But that is still **far** too slow for practice.

Open Problems III

Questions related to the τ-function:

- Faster τ-comparisons (for the basics see the `tawSolver`).
- Apply it to **practical** non-boolean(!) algorithms (here it really shines).
- For the boolean case a good approximation is the *product rule* — are there other “approximations”?

Open Problems IV

Questions related to the canonical order:

- Canonicity needs wide branchings — what about bounded branchings?
- Especially is there a general theory about binary branchings?

Enabling shortcuts

The main remaining question is the choice of the distance $d(F, F')$.

When is look-ahead successful?

When branches are cut off early!

- So $d(F, F')$ should be large if F' has many more *future* reductions.
- In practice that means if F' has many more *expected* UCPs.

Now certain theoretical and all practical evidence says that the

weighted number of new clauses

is a good measure (the more the better).

All direct measure (number of eliminated variables) fail
(they are too pessimistic).

The weighting

The shorter a clause, the closer to unit.

Thus, an exponential decay of the weight with length is the basis.

Especially for **random** k**-SAT**,

- more sophisticated schemes have been developed.
- They treat every literal differently.
- The basic idea is to “estimate” how “likely” it is that the literal becomes `false`.
- From that one can “estimate” how “likely” a clause becomes unit.

Behaves like random

Various heuristic schemes for look-ahead solvers have been developed.

The Pythagorean Problems are far best attacked by schemes especially successful on random instances.

(But using different parameter values.)

Some remarks

The number of clauses for Pythagorean triples is asymptotically $\frac{1}{\pi} n \cdot \ln n$.

In some sense a "randomisation" takes place:

1. The original proof van der Waerden [16] for the existence of van-der-Waerden numbers (hyperedges: arithmetic progressions of fixed length) is purely combinatorial.
2. The refinement Green and Tao [6] to arithmetic progressions in the *prime numbers* uses some randomisation (to make the prime numbers look random).
3. Similarly, the basic proof of Schur [15] on the triples $x + y = z$ is purely combinatorial (a simple application of Ramsey's theorem).
4. Accordingly, for the refinement to *square numbers* (our case) one would expect that some randomisation should be appropriate.

Open Problems V

A theory of “distances” is needed:

- Can the existing schemes be unified?
- I believe the tools of statistical physics are appropriate here (I believe that “random formulas” is a kind of bogeyman, in the sense that randomness in the input is not required to apply these tools).

Summary and outlook

I C&C is to the best of our knowledge the strongest approach for hard SAT problems.

II The theory of heuristics for look-ahead solvers plays a crucial role.

III Now the task is to fully develop these pioneering efforts.

End

(references on the remaining slides).

For my papers see
http://cs.swan.ac.uk/~csoliver/papers.html.

Bibliography I

[1] Tanbir Ahmed, Oliver Kullmann, and Hunter Snevily. On the van der Waerden numbers $\mathrm{w}(2;3,t)$. *Discrete Applied Mathematics*, 174:27–51, September 2014. doi:10.1016/j.dam.2014.05.007.

[2] Armin Biere, Marijn J.H. Heule, Hans van Maaren, and Toby Walsh, editors. *Handbook of Satisfiability*, volume 185 of *Frontiers in Artificial Intelligence and Applications*. IOS Press, February 2009. ISBN 978-1-58603-929-5.

[3] Ernie Croot and Vsevolod F. Lev. Open problems in additive combinatorics. In Andrew Granville, Melvyn B. Nathanson, and József Solymosi, editors, *Additive Combinatorics*, CRM Proceedings & Lecture Notes, pages 207–234. American Mathematical Society, 2006. ISBN 978-0-8218-4351-2. URL http://people.math.gatech.edu/~ecroot/E2S-01-11.pdf.

Bibliography II

[4] Martin Davis, George Logemann, and Donald Loveland. A machine program for theorem-proving. *Communications of the ACM*, 5(7):394–397, July 1962. doi:10.1145/368273.368557.

[5] Jon William Freeman. *Improvements to propositional satisfiability search algorithms*. PhD thesis, University of Pennsylvania, 1995. URL http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.43.255.

[6] Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions. *Annals of Mathematics*, 167(2):481–547, 2008. doi:10.4007/annals.2008.167.481.

[7] Marijn J. H. Heule and Hans van Maaren. Look-ahead based SAT solvers. In Biere, Heule, van Maaren, and Walsh [2], chapter 5, pages 155–184. ISBN 978-1-58603-929-5. doi:10.3233/978-1-58603-929-5-155.

Bibliography III

[8] Marijn J.H. Heule. March: Towards a lookahead Sat solver for general purposes. Master's thesis, Delft University of Technology, Faculty of Electrical Engineering, Mathematics and Computer Science, March 2004. URL http://www.st.ewi.tudelft.nl/sat/theses/marijn.pdf.

[9] Marijn J.H. Heule, Oliver Kullmann, Siert Wieringa, and Armin Biere. Cube and conquer: Guiding CDCL SAT solvers by lookaheads. In Kerstin Eder, João Lourenço, and Onn Shehory, editors, *Hardware and Software: Verification and Testing (HVC 2011)*, volume 7261 of *Lecture Notes in Computer Science (LNCS)*, pages 50–65. Springer, 2012. doi:10.1007/978-3-642-34188-5_8. URL http://cs.swan.ac.uk/~csoliver/papers.html#CuCo2011.

Bibliography IV

[10] Marijn J.H. Heule, Oliver Kullmann, and Victor W. Marek. Solving and verifying the boolean Pythagorean Triples problem via Cube-and-Conquer. In Nadia Creignou and Daniel Le Berre, editors, *Theory and Applications of Satisfiability Testing - SAT 2016*, volume 9710 of *Lecture Notes in Computer Science*, pages 228–245. Springer, 2016. ISBN 978-3-319-40969-6. doi:10.1007/978-3-319-40970-2_15.

[11] Oliver Kullmann. New methods for 3-SAT decision and worst-case analysis. *Theoretical Computer Science*, 223(1-2):1–72, July 1999. doi:10.1016/S0304-3975(98)00017-6.

[12] Oliver Kullmann. Investigating the behaviour of a SAT solver on random formulas. Technical Report CSR 23-2002, Swansea University, Computer Science Report Series, October 2002. URL http://www-compsci.swan.ac.uk/reports/2002.html. 119 pages.

Bibliography V

[13] Oliver Kullmann. Fundaments of branching heuristics. In Biere et al. [2], chapter 7, pages 205–244. ISBN 978-1-58603-929-5. doi:10.3233/978-1-58603-929-5-205.

[14] Chu Min Li and Anbulagan. Heuristics based on unit propagation for satisfiability problems. In *Proceedings of 15th International Joint Conference on Artificial Intelligence (IJCAI'97)*, pages 366–371. Morgan Kaufmann Publishers, 1997. URL http://users.cecs.anu.edu.au/~anbu/papers/IJCAI97Anbulagan.pdf.

[15] Issai Schur. Über die Kongruenz $x^m + y^m = z^m \pmod{p}$. *Jahresbericht der Deutschen Mathematikervereinigung*, 25: 114–117, 1917. URL https://eudml.org/doc/145475.

[16] B.L. van der Waerden. Beweis einer Baudetschen Vermutung. *Nieuw Archief voor Wiskunde*, 15:212–216, 1927.