SAT and Ramsey theory

Oliver Kullmann
Computer Science Department
Swansea University

RaTLoCC
Bertinoro, October 29, 2009

Introduction

- [Dransfield, Marek, Truszczyński, SAT 2003] introduced van der Waerden numbers into SAT: all existing numbers can easily be computed by (standard) SAT solvers, and new lower bounds.
- [Herwig, Heule, van Lambalgen, van Maaren, 2007] go far beyond these lower bounds by introducing special methods.
- [Kouril, Paul, 2008] compute $\mathrm{vdw}_2(6,6) = 1132$ by running specialised SAT solvers on clusters of conventional computers and FPGAs for altogether 6 months.

To map out the terrain.
Create a systematic field of benchmarks for solvers.
To find the best algorithms.
To understand.
Even perhaps the general problems.

Introduction

- [Dransfield, Marek, Truszczyński, SAT 2003] introduced van der Waerden numbers into SAT: all existing numbers can easily be computed by (standard) SAT solvers, and new lower bounds.
- [Herwig, Heule, van Lambalgen, van Maaren, 2007] go far beyond these lower bounds by introducing special methods.
- [Kouril, Paul, 2008] compute $\mathrm{vdw}_2(6,6) = 1132$ by running specialised SAT solvers on clusters of conventional computers and FPGAs for altogether 6 months.

To map out the terrain.

Create a systematic field of benchmarks for solvers.

To find the best algorithms.

To understand.

Even perhaps the general problems.

Introduction

- [Dransfield, Marek, Truszczyński, SAT 2003] introduced van der Waerden numbers into SAT: all existing numbers can easily be computed by (standard) SAT solvers, and new lower bounds.
- [Herwig, Heule, van Lambalgen, van Maaren, 2007] go far beyond these lower bounds by introducing special methods.
- [Kouril, Paul, 2008] compute $\mathrm{vdw}_2(6, 6) = 1132$ by running specialised SAT solvers on clusters of conventional computers and FPGAs for altogether 6 months.

To map out the terrain.

Create a systematic field of benchmarks for solvers.

To find the best algorithms.

To understand.

Even perhaps the general problems.

Introduction

- [Dransfield, Marek, Truszczyński, SAT 2003] introduced van der Waerden numbers into SAT: all existing numbers can easily be computed by (standard) SAT solvers, and new lower bounds.
- [Herwig, Heule, van Lambalgen, van Maaren, 2007] go far beyond these lower bounds by introducing special methods.
- [Kouril, Paul, 2008] compute $\mathrm{vdw}_2(6,6) = 1132$ by running specialised SAT solvers on clusters of conventional computers and FPGAs for altogether 6 months.

To map out the terrain.
Create a systematic field of benchmarks for solvers.
To find the best algorithms.
To understand.
Even perhaps the general problems.

Introduction

- [Dransfield, Marek, Truszczyński, SAT 2003] introduced van der Waerden numbers into SAT: all existing numbers can easily be computed by (standard) SAT solvers, and new lower bounds.
- [Herwig, Heule, van Lambalgen, van Maaren, 2007] go far beyond these lower bounds by introducing special methods.
- [Kouril, Paul, 2008] compute $\mathrm{vdw}_2(6, 6) = 1132$ by running specialised SAT solvers on clusters of conventional computers and FPGAs for altogether 6 months.

To map out the terrain.
Create a systematic field of benchmarks for solvers.
To find the best algorithms.
To understand.
Even perhaps the general problems.

Introduction

- [Dransfield, Marek, Truszczyński, SAT 2003] introduced van der Waerden numbers into SAT: all existing numbers can easily be computed by (standard) SAT solvers, and new lower bounds.
- [Herwig, Heule, van Lambalgen, van Maaren, 2007] go far beyond these lower bounds by introducing special methods.
- [Kouril, Paul, 2008] compute $\mathrm{vdw}_2(6,6) = 1132$ by running specialised SAT solvers on clusters of conventional computers and FPGAs for altogether 6 months.

To map out the terrain.
Create a systematic field of benchmarks for solvers.
To find the best algorithms.
To understand.
Even perhaps the general problems.

Overview

Overview

1. Van der Waerden numbers
2. What can be computed
3. Polynomial growth
4. Green-Tao numbers
5. What can be computed
6. Polynomial growth
7. Conclusions

Overview

Overview

Overview

Overview

Overview

1. Van der Waerden numbers
2. What can be computed
3. Polynomial growth
4. Green-Tao numbers
5. What can be computed
6. Polynomial growth
7. Conclusions

The general definition

Theorem [van der Waerden 1927] For every $m \in \mathbb{N}_0$ and all $a_1, \dots, a_m \in \mathbb{N}$ there exists a unique $n \in \mathbb{N}$ such that

- however $\{1, \dots, n\}$ is partitioned into m possibly empty parts P_i, there is one part P_i containing at least one arithmetic progression of size a_i;
- there exists a partitioning of $\{1, \dots, n-1\}$ into m (possibly empty) parts P_i such that no part contains an arithmetic progression of size a_i.

This n is denoted by $\mathbf{vdw}_m(a_1, \dots, a_m)$.

(For $a_1 = \dots a_m$ we obtain the (most prominent) "diagonal cases".)

The field of *Additive Number Theory* emerged.

Bounds

1. Van der Waerden's original proof (1927) yields the Ackerman function as upper bound.
2. Motivated by results from mathematical logic, it was conjectured that this upper bound is best-possible.
3. A break-through was achieved by Shelah in 1988, showing a primitive recursive upper bound.
4. Related to his fields medal (1998), Gowers showed
$$\mathrm{vdw}_m(k,\dots,k) \leq 2^{2^{m^{2^{2^{k+9}}}}}.$$
5. The best known general lower bounds are from Brown et al (2006, 2008) and from Berlekamp (1968), and are only single-exponential.
6. $k^{2-o(1)} < \mathrm{vdw}_2(3,k) < k^{c \cdot k^2}$.
7. Graham offers \$1000 for (dis)proving
$$\mathrm{vdw}_2(k,k) < 2^{k^2}?$$

Transversals

For $k, n \in \mathbb{N}$ let $\mathbf{ap}(k, n)$ be the hypergraph of arithmetic progressions of length k over the vertex-set $\{1, \ldots, n\}$. For example:

$$\operatorname{ap}(3,5) = (\{1, \ldots, 5\}, \\ \{ \{1,2,3\}, \{2,3,4\}, \{3,4,5\}, \{1,3,5\} \}).$$

For a hypergraph G let $\boldsymbol{\tau(G)}$ denote the **transversal number** of G, the minimum size of a transversal (or "hitting set").

$$\mathrm{vdw}_{m+1}(2, \ldots, 2, k) \text{ is the smallest } n \text{ such that } \\ \tau(\operatorname{ap}(k, n)) > m.$$

Obviously $\mathrm{vdw}_{m+1}(2, \ldots, 2, k) \leq k \cdot (m+1)$.

Szemerédi's theorem

A breakthrough was achieved by Szemerédi in 1975.

A subset $A \subseteq \mathbb{N}$ has **positive upper density** if there exists $a \in \mathbb{R}_{>0}$ such that the set of $n \in \mathbb{N}$ with

$$\frac{|A \cap \{1, \ldots, n\}|}{n} \geq a$$

is infinite.

Theorem *If $A \subseteq \mathbb{N}$ has positive upper density, then A contains arithmetic progressions of arbitrary size.*

It is not too hard to show, that Szemerédi's theorem is equivalent (by elementary means) to

$$\forall k \in \mathbb{N} : \lim_{n \to \infty} \frac{\tau(\mathrm{ap}(k, n))}{n} = 1.$$

k-free sequences of integers

$\boldsymbol{\alpha(G)}$ is the **independence number** of hypergraph G, the minimum size of an independent set (not containing any hyperedge). Obviously $\alpha(G) + \tau(G) = |V(G)|$.

So Szemerédi's theorem says

$$\forall k \in \mathbb{N} : \lim_{n \to \infty} \frac{\alpha(\mathrm{ap}(k,n))}{n} = 0.$$

For $k \in \mathbb{N}$ and $q \in \mathbb{N}$ let $\gamma_k(q) \in \mathbb{N}$ be the first $n \in \mathbb{N}$ with

$$\frac{\alpha(\mathrm{ap}(k,n))}{n} < \frac{1}{q}.$$

Now

$$\mathrm{vdw}_m(a_1, \ldots, a_m) \leq \max_{i \in \{1,\ldots,m\}} \gamma_{a_i}(m).$$

Translation into SAT

- The van-der-Waerden problems are just hypergraph colouring problems for $\mathrm{ap}(k, n)$, the SAT-translation is straight-forward (and canonical).
- That is, for boolean SAT; or using CNF with non-boolean values.

Example CNF for $k = 3, n = 9$

```
p cnf 9 32
-7 -8 -9 0
-5 -7 -9 0
-3 -6 -9 0
-1 -5 -9 0
-6 -7 -8 0
-4 -6 -8 0
-2 -5 -8 0
-5 -6 -7 0
-3 -5 -7 0
-1 -4 -7 0
-4 -5 -6 0
-2 -4 -6 0
-3 -4 -5 0
-1 -3 -5 0
-2 -3 -4 0
-1 -2 -3 0
1 2 3 0
1 3 5 0
1 4 7 0
1 5 9 0
2 3 4 0
2 4 6 0
2 5 8 0
3 4 5 0
3 5 7 0
3 6 9 0
4 5 6 0
4 6 8 0
5 6 7 0
5 7 9 0
6 7 8 0
7 8 9 0
```

Parameter tuples

A **parameter tuple** is an element of $\bigcup_{m \in \mathbb{N}} \mathbb{N}_{\geq 2}^{m}$. The set $\mathcal{PT}$ of all parameter tuples is a monoid together with the concatenation operation ";". So **vdw** : $\mathcal{PT} \to \mathbb{N}$.

- A parameter tuple is **simple** if its length is at most one, while otherwise it is **non-simple**.
- A **diagonal tuple** is a parameter tuple where all entries are the same, while otherwise it is called **non-diagonal**.
- A non-empty parameter tuple is **transversal** if all but possibly one entry equals 2.
- A **core tuple** is a non-simple parameter tuple not containing an entry equal to 2.
- A **standardised tuple** is a parameter tuple sorted in ascending order.

Binary core tuples

There are only $22 + 4 + 1 = 27$ standardised core tuples t for which $\text{vdw}(t)$ is known.

For $14 + 5 + 2 + 1 = 22$ binary standardised core tuples the values $\mathrm{vdw}_2(a, b)$ are known:

a \ b	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	9	18	22	32	46	58	77	97	114	135	160	186	218	238
4	-	35	55	73	109	146								
5	-	-	178	206										
6	-	-	-	1132										

Core tuples of length 3 and 4

For 4 ternary standardised core tuples the values $\mathrm{vdw}_3(a, b, c)$ are known:

a, b \ c	3	4	5
3, 3	27	51	80
3, 4	-	89	

Finally the value $\mathrm{vdw}_4(a, b, c, d)$ is known for one standardised core tuple:

a, b, c \ d	3
3, 3, 3	76

Transversal extensions

1. Calling the parameter tuple $((2, \ldots, 2); t)$ a **transversal extension** of t, we see that the transversal tuples are exactly the transversal extensions of simple tuples.
2. Every parameter tuple is either a transversal extension of a core tuple or is a transversal tuple.
3. Computation of $\text{vdw}(t)$ for transversal t can be done more efficient than for general t, and so here we cannot really draw a precise frontier of current capabilities for computing vdW-numbers.

Only $33 + 10 + 1 + 6 = 50$ non-trivial extensions of core tuples are known.

Extending $(3, k)$

Extending $(3, k)$ by $m \geq 1$ 2's, i.e., the numbers $\mathrm{vdw}_{m+2}((2, \ldots, 2); (3, k))$:

m \ k	3	4	5	6	7	8	9	10	11	12	13
0	9	18	22	32	46	58	77	97	114	135	160
1	14	21	32	40	55	72	90	108	129	150	171
2	17	25	43	48	65	83	99	119			
3	20	29	44	56	72	88					
4	21	33	50	60							
5	24	36									
6	25										
7	28										

Extending $(4, k)$

Extending $(4, k)$ by $m \geq 1$ 2's, i.e., the numbers $\mathrm{vdw}_{m+2}((2, \ldots, 2); (4, k))$:

m \ k	4	5	6	7	8
0	35	55	73	109	146
1	40	71	83	119	
2	53	75	93		
3	54	79			
4	56				

Extending $(5, k)$ and $(3, 3, k)$

Extending $(5, k)$ by $m \geq 1$ 2's, i.e., the numbers $\mathrm{vdw}_{m+2}((2, \ldots, 2); (5, k))$:

m \ k	5
0	178
1	180

Extending $(3, 3, k)$ by $m \geq 1$ 2's, i.e., the numbers $\mathrm{vdw}_{m+3}((2, \ldots, 2); (3, 3, k))$:

m \ k	3	4	5
0	27	51	80
1	40	60	86
2	41	63	
3	42		

A bold conjecture

For every (fixed) parameter tuple t the map

$$k \in \mathbb{N} \mapsto \mathrm{vdw}(t; k)$$

is polynomially bounded (where the polynomial depends on t).

- This says that all rows in the above table are polynomially bounded.
- Perhaps one should better speak of an “open question”.

$t = (3)$

The case $t = (3)$ has been conjectured by Landman et al, where more precisely $\mathrm{vdw}_2(3, k) \leq k^2$ has been conjectured. The numbers $\mathrm{vdw}_2(3, k)$ are known for $1 \leq k \leq 16$ (see above). Our experiments yield the following conjectured values:

1. $\mathrm{vdw}_2(3, 17) \geq 279$
2. $\mathrm{vdw}_2(3, 18) \geq 312$
3. $\mathrm{vdw}_2(3, 19) \geq 349$
4. $\mathrm{vdw}_2(3, 20) > 388$

which is well compatible with quadratic growth. Fitting the 19 data points $k \in \{1, \dots, 19\} \mapsto \mathrm{vdw}_2(3, k)$ yields $f(k) = 3.74303 - 1.11280 \cdot k + 1.01187 \cdot k^2$, which after rounding has a distance to the true values of at most 3 except for the exceptional point $k = 16$, where the distance is 7.

$t = (4)$

- For $t = (4)$ the bound $\mathrm{vdw}_2(4, 9) > 254$ is in the literature ([Ahmed 2009]).
- We can improve this to $\mathrm{vdw}_2(4, 9) \geq 309$, and furthermore $\mathrm{vdw}_2(4, 10) > 320$.
- So going from $k = 8$ to $k = 9$ we see a rather big jump.
- However possibly from $k = 9$ to $k = 10$ only a very small change might take place.

Transversal extensions

For a parameter tuple t of length $l \in \mathbb{N}_0$ and for $m \in \mathbb{N}_0$ we have

$$\mathrm{vdw}_{m+l}((2,\dots,2);t) \le (m+1)\cdot \mathrm{vdw}_l(t).$$

Proof: Let $n := (m+1)\cdot \mathrm{vdw}_l(t)$. Now for any $S \subseteq \{1,\dots,n\}$ with $|S| \le m$ the set $\{1,\dots,n\} \setminus S$ contains at least one interval $\{i,\dots,j\}$ for $1 \le i \le j \le n$ with $j - i + 1 = \mathrm{vdw}_l(t)$.
Use the invariance of linear progressions under translation. ∎

So in the tables for transversal extensions all columns grow linearly.

Remarks on transversal numbers

- Understanding for some (fixed) $k \geq 3$ the convergence rate of $n \mapsto \alpha(\mathrm{ap}(k, n))/n$ (against zero), we obtain upper bounds on $m \mapsto \mathrm{vdw}_m(k)$.
- It seems unknown how good such bounds can be; and apparently only applicable yet for $k = 3$.
- Algorithmically, it is more natural to consider $\tau(\mathrm{ap}(k, n))$ (the size of the smallest transversal, i.e., hitting all arithmetic progressions of length k).
- Due to the lack of dedicated hypergraph transversal implementations, fastest seems at this time to translate the problem into a SAT problem, using some translation of a *cardinality constraint* into CNF.

Transversal numbers for $k = 3$

- Via SAT we can handle (within a few days) $n \leq 102$.
- While actually precise values for $n \leq 194$ are known.
- A key observation (apparently!) exploited in these specialised computations is

$$\tau(\mathrm{ap}(k, n+m)) \geq \tau(\mathrm{ap}(k, n)) + \tau(\mathrm{ap}(k, m)).$$

- Yet we didn't incorporate this into our computations, focusing on completely uninformed computations at this stage.
- But handled as additional constraints, hopefully in this way we can handle large n than 194 via SAT.
- Here quite something is known, but the state of the literature is insufficient. (In the course of this project we shall change this.)

Transversal numbers for $k > 3$

- Data for $k \leq 6$ is available in the "Encyclopedia of Integer Sequences", not containing the better data for $k = 3$, but apparently otherwise containing all what is known (except of our data).
- For $4 \leq k \leq 6$ this can be easily covered by simple hypergraph transversal approaches for computing the set of all minimum transversals.
- One gets somewhat farther with the SAT approach, but not dramatically.
- Yet we considered $k \leq 11$ (where for $k = 11$ we reached $n = 131$).

A precise formula

[Landman, Robertson, Culver, 2005] actually provide a (precise) formula for

$$\mathrm{vdw}_{m+1}(2, \ldots, 2, k)$$

for "almost all k".

- Ironically this means "if k is large enough" for *fixed* m, and thus is actually not what we would like to have.
- From our computations we see that their approach likely can be enhanced and smoothed out.
- But very likely it won't cover $m > k$.

Ramsey properties as threshold phenomenons?!

A kind of "conjecture":

Ramsey problems are phase transitions
in structured spaces.

A riddle

How to get randomness into the picture?

Prime numbers!

A riddle

How to get randomness into the picture?

Prime numbers!

3-free sequences of primes

Let $\mathbf{ap_{pr}(k, n)}$ be the hypergraph with

- vertex set $\{p_1, \dots, p_n\}$, the first n prime numbers;
- hyperedges the arithmetic progressions of size k.

For example

$$\mathrm{ap_{pr}}(3,7) = (\{2,3,5,7,11,13,17\},\\ \{\{3,5,7\},\{3,7,11\},\{5,11,17\}\}).$$

So $\tau(\mathrm{ap_{pr}}(3,7)) = 2$ and $\alpha(\mathrm{ap_{pr}}(3,7)) = 5$.

An independent set here is for example $\{2,5,7,11,13\}$.

The Green-Tao theorem

Strongly involved in the Fields medal of Terence Tao (2006) was the Green-Tao Theorem (2004):

$$\forall k \in \mathbb{N} : \lim_{n \to \infty} \frac{\alpha(\mathrm{ap}_{\mathrm{pr}}(k, n))}{n} = 0.$$

Analogously to $\mathrm{vdw}_m(a_1, \ldots, a_m)$ we get $\mathbf{grt}_m(a_1, \ldots, a_m)$:

Now partitioning the first n prime numbers into m parts.

The Green-Tao theorem

Strongly involved in the Fields medal of Terence Tao (2006) was the Green-Tao Theorem (2004):

$$\forall k \in \mathbb{N} : \lim_{n \to \infty} \frac{\alpha(\mathrm{ap}_{\mathrm{pr}}(k, n))}{n} = 0.$$

Analogously to $\mathrm{vdw}_m(a_1, \dots, a_m)$ we get $\mathbf{grt}_m(a_1, \dots, a_m)$:

Now partitioning the first n prime numbers into m parts.

Efficient generation of Green-Tao hypergraphs

For $n \in \mathbb{N}_0$ let $\boldsymbol{\Pi(n)} \in \mathbb{N}$ be the product of all prime numbers p with $p \leq n$.
So $\Pi(0) = \Pi(1) = 1$, $\Pi(2) = 2$, and $\Pi(3) = \Pi(4) = 6$.

Consider an arithmetic progression

$$P = \{a + i \cdot d \mid i \in \{0, \ldots, k-1\}\}$$

for some $k \geq 2$ and $d \geq 1$ such that all elements of P are prime numbers:

1. *If $a \neq k$, then $\Pi(k) \mid d$.*
2. *If $a = k$, then $\Pi(k-1) \mid d$.*

“Simple” statistics

The number of hyperedges in $\mathrm{ap}(k, n)$ is $O(n^2)$, and can easily be computed precisely. For Green-Tao hypergraphs these are deep questions. The following numerical models yield very good approximations:

- For $n \le 30000$:
  $|E(\mathrm{ap}_{\mathrm{pr}}(3, n))| \approx 0.07487019 \cdot n^{1.90377210}$.
- For $n \le 40000$:
  $|E(\mathrm{ap}_{\mathrm{pr}}(4, n))| \approx 0.02317292 \cdot n^{1.81359675}$.
- For $n \le 80000$:
  $|E(\mathrm{ap}_{\mathrm{pr}}(5, n))| \approx 0.004561643 \cdot n^{1.739623162}$.
- For $n \le 160000$:
  $|E(\mathrm{ap}_{\mathrm{pr}}(6, n))| \approx 0.001491893 \cdot n^{1.671835433}$.
- For $n \le 10^6$:
  $|E(\mathrm{ap}_{\mathrm{pr}}(7, n))| \approx 0.0002054541 \cdot n^{1.6465780527}$.
- For $n \le 8 \cdot 10^6$:
  $|E(\mathrm{ap}_{\mathrm{pr}}(8, n))| \approx 4.218958 \cdot 10^{-5} \cdot n^{1.631506}$.

Simple parameter tuples

Already $\mathrm{grt}_1(k)$ for $k \in \mathbb{N}$ poses a non-trivial mathematical problem (while $\mathrm{vdw}_1(k) = k$), namely the question is to find the smallest $n \in \mathbb{N}$ such that the first n prime numbers contain an arithmetic progression of length k.

The following is known:

k	$\mathrm{grt}_1(k)$
1	1
2	2
3	4
4	9
5	10
6	37
7	155
8	263
9	289
10	316

k	$\mathrm{grt}_1(k)$
11	21,966
12	23,060
13	58,464
14	2,253,121
15	9,686,320
16	11,015,837
17	227,225,515
18	755,752,809
19	3,466,256,932
20	22,009,064,470
21	220,525,414,079

Core parameter tuples

For 5 standardised core tuples t we have been able to compute precise values for $\mathrm{grt}(t)$:

$a \backslash b$	3	4	5	6	7
3	23	79	528	≥ 2072	> 13750
4	-	512	$\gtrapprox 4232$		
5	-	-	≥ 34309		

$a, b \backslash c$	3	4	5
3, 3	137	$\gtrapprox 434$	> 1927
3, 4	-	> 1537	> 7000

$a, b, c \backslash d$	3	4
3, 3, 3	> 380	> 997
3, 3, 4	-	> 2750

Transversal extensions

Regarding transversal extensions of non-simple parameter tuples yet we only considered extending $(3, k)$ by $m \geq 1$ 2's, i.e., the numbers $\mathrm{grt}_{m+2}((2, \ldots, 2); (3, k))$:

k \ m	0	1	2	3	4	5	6	7	8	9	10
3	23	31	39	41	47	53	55	≥ 60	≥ 62	≥ 67	≥ 71

The following conjecture seems plausible, though it is no longer trivial as it was for van der Waerden:

For every (fixed) parameter tuple t of length l the map

$$m \in \mathbb{N}_0 \mapsto \mathrm{vdw}_{m+l}((2, \ldots, 2); t)$$

is polynomially bounded.

The goals

- Computing "all" numbers from Ramsey theory as far as possible.
- Making all the knowledge available, precise values, concrete bounds and general bounds.
- Understanding how SAT solvers work on these "benchmarks" — and how to make them faster.
- Especially interesting:
  1. Finding short tree-like resolution refutations.
  2. Comparing tree-like and dag-like resolution refutations.
- Making *everything* available in the open-source library `OKlibrary` (`http://www.ok-sat-library.org`)

Of course, I hope that all this leads also to insights into the mathematical structure of these problems.

End

References