Erdös Dream

SAT, Extremal Combinatorics and Experimental Mathematics

V.W. Marek [1]

Department of Computer Science
University of Kentucky

October 2013

[1] *Discussions with J.B. Remmel and M. Truszczynski are acknowledged*

What it is about?

- Recent progress in *computation* of van der Waerden numbers (specifically Kouril's results and also Ahmed's results) obtained using SAT raises hope that more results of this sort can be found
- How did it arise?
- What are possible uses?
- Experimental Mathematics
- And what Paul Erdös, thinks about it now, that he has the access to *The Book*?

Plan

- How did it all start?
- How is it used now?
- Mathematics behind it
- How will SAT community contribute and what is there for that community

Like most things in modern Math...

- Quite a lot of things started or got clarified in 19th century Europe
- And many things started with David Hilbert
- While he was studying irreducibility of rational functions (i.e. functions that are fractions where both denominator and numerator are polynomials with integer coefficients, (denumerator non-zero)) he proved a lemma
- (Notation: $[n] = \{0, \ldots, n-1\}$)
- We define an *n-dimensional affine cube* as

$$\{a + \Sigma_{i \in X} b_i : X \subseteq [n]\}$$

- (Why is it an affine cube?)

Hilbert Lemma

- *For every positive integers r and n there is an integer h such that every coloring in r colors of $[h]$ results in a monochromatic n-dimensional affine cube*
- Thus there is a function $H(\cdot,\cdot)$ that assigns to r and n the least such h
- Of course if $h' > h$ then h' has has the desired property *because* we could limit to $[h]$, get the cube and claim it for h'

Not that anyone paid attention

- Like many other meaningful results, nobody paid any attention to it at the time
- That is, there were no follow up papers relating to this lemma
- (Later on things changed, but I am not aware of computation of specific values))

Then there was Schur...

- Issai Schur was a Berlin mathematician (story is quite tragic, b.t.w.)
- An algebrist, in 1916 he found the following fact while looking for solution to Fermat Last Problem
  - Let k be a positive integer. Then there is a positive integer s such that if $[s]$ is partitioned into k parts then at least one of the parts is not sum-free, that is it contains $a, b, a+b$
  - (with small extra effort, you can make them all different)
- As before this property of n inherits upward

And then van der Waerden...

- In 1927, the algebraist Bartel L. van der Waerden proved the following
  - Let k, l be positive integers, $l \geq 3$. Then there is w such that if we partition $[w]$ into k blocks then at least one of these blocks contains at least one arithmetic progression of length l
- This was generalized by Schur's student Brauer so we can have the difference also of same color!

Ramsey comes in...

- In 1928, Frank Ramsey proved the following theorem: Let k be a positive integer. Then there is n such that when a complete graph on $[n]$ is colored with two colors (say red, and blue) then there is a complete red graph on k vertices, or a complete blue graph on k vertices
- There are all sort of presentations of this theorem
- Since each human hand has (in principle) five fingers we can check that for $k = 3$, the "large enough" n is six

Ramsey, cont'd

- Of course, if you have more vertices same holds
- (We can also talk about a clique and independent set)
- So, in this case really the corresponding formal sentence of arithmetic looks like this:

$$\forall_k \exists_m \forall_n (n > m \Rightarrow \ldots)$$

- Here $\ldots$ is an expression that tells us that there is a red copy of K_k, or blue copy of K_k
- Generally, the fact that we are dealing with Π_3 formula is relevant, but we will not discuss it here

There is more...

- An h-dimensional $[n]$ cube is the Cartesian product of h copies of $[n]$
- (Straight lines in such cube are ...)
- In 1963 Alfred Hales and Robert Jewett proved the following theorem:
  - Given a positive n and k, there is an integer h such that h-dimensional cube is colored with k colors then there is a monochromatic straight line
- So, again we have this function $h(n, k)$, namely the least h for n and k

Hales-Jewett, cont'd

- One can code cubes as segments of integers so that lines become arithmetic progressions
- Therefore Hales-Jewett theorem entail van der Waerden theorem
- (And of course there is this tick-tack-toe game ...)

Strange thing about these functions

- For none of functions whose existence is implied by the five theorems above a “closed form” is known, i.e. an elementary function that describes it
- (There is an notion of elementary function that we are taught, say, at differential equations course)
- The mathematicians of, say, 17th century would be deeply worried
- More generally, they believed that a function had to have a recipe to compute it

Functions, cont'd

- To some people this is deeply disturbing because quite a number of mathematicians believe that elementary problems (and *each* of these problems is, kind of, Olympiad-style problem, that is hard, but with clever elementary proof) have elementary solutions
- Also, it looks like these functions grow quite fast
- Original bounds, obtained from the proofs looked ridiculous, originally, in case of v.d.W. numbers not even primitive recursive

Functions, cont’d

- This changed with Shelah’s proof of Hales-Jewett theorem (thus v.d. Waerden Theorem as well)
- (Generally, analysts got involved in getting upper bounds, and a reasonable bound in case of v.d. Waerden numbers was found by Timothy Gowers)
- Paul Erdös who was significantly involved in Extremal Combinatorics and bounds on functions we discuss here, was certainly surprised by the fact that no closed forms were found
- But many combinatorists are *not* surprised

These professional mathematicians...

- What do they do? They go for a generalization
- Let us discuss a couple of these
- We will generalize Ramsey, Schur, and van der Waerden theorems

Generalizing Ramsey's theorem

- Introduce more colors:
  - Let n, k be positive integers. Then there is r such that when a complete graph K_r is colored with k colors then there is a monochromatique clique of size n
- Obviously follows from Ramsey theorem by induction on k
- But now we have this function $r(n, k)$
- But wait, here is another generalization
  - Let k be a positive integer, $\langle i_1, \ldots, i_k \rangle$ a sequence of positive integers of length k. Then there is r such that if K_r is colored with k colors, then for some $j, 1 \leq j \leq k$ there is a clique of size i_j colored with the color j
- Follows from the previous generalization

Straight from Wikipedia

Table of $R(r, s)$

r,s	1	2	3	4	5	6	7	8	9
1	1	1	1	1	1	1	1	1	1
2	1	2	3	4	5	6	7	8	9
3	1	3	6	9	14	18	23	28	36
4	1	4	9	18	25	36-41	49-61	56-84	73-115
5	1	5	14	25	43-49	58-87	80-143	101-216	126-316
6	1	6	18	36-41	58-87	102-165	113-298	132-495	169=178
7	1	7	23	49-61	80-143	113-298	205-540	217-1031	241-1713
8	1	8	28	56-84	101-216	132-495	217-1031	282-1870	317-3583
9	1	9	36	73-115	126-316	169-780	241-1713	317-3583	581-12677

(More data available on Wolfram MathWorld)

Early contributions

- Actually, McKay and Radziszowski in 1995 established (?) that $R(4, 5) = 25$
- (And it made New York Times...)
- How was it done?
- First they had to have a counterexample on 24 vertices and then they had to show that there is no counterexample on 25
- Excellent combinatorists as they are, they cleverly pruned the search space
- Still it took them over half-year of continuous work on over 150 workstations (but see the timeline)
- *To the best of my knowledge their experiment was never repeated, but maybe nobody cared*

Since then

- Plenty of specific values of $R(k, m)$ has been established
- Stan Radziszowski publishes a kind of mathematical irregular blog, called *Small Ramsey Numbers*
- This blog/review is published as one of reviews at *Electronic Journal of Combinatorics*
- Everything I said above **and much more** can be found one way or another there
- (We will talk about resources later)

Generalizing van der Waerden

- We can use the second generalization of Ramsey Theorem to point us to a generalized version of van der Waerden Theorem
  - Let k be a positive integer and $\langle m_1, \ldots, m_k \rangle$ a sequence of positive integers, each bigger equal than 3. Then there is a number w such that any partition $\mathcal{P}$ of $[w]$ into k blocks has the property that for some $i, 1 \leq i \leq k$, the i^{th} block of the partition $\mathcal{P}$ has an arithmetic progression of length m_i
  - $w(k, m_1, \ldots, m_k)$ is (you guess...)

What about Schur...

- We can think about colorings of a segment of integers and integers $a_0, a_1, a_0 + a_1$ are colored with same colors
- So, *three* non-empty sums are monochromatic (which ones?)
- Why not have three integers a_0, a_1, a_2 and all seven sums over nonempty subsets $\emptyset \neq I \subseteq [3]$, $\Sigma_{i \in I} a_i$ monochromatic?
- Indeed, Arnautov-Folkman-Sanders Theorem (usually called Folkman Theorem) says exactly this:
  - For every m and n there is an integer a that for any m-coloring of $[a]$ there is an n element subset $A = \{k_1, \ldots, k_n\}$ of $[a]$ so that all sums of nonempty subsets $\emptyset \neq I \subseteq A$, $\Sigma_{i \in A} a_i$, are monochromatic
- There are other generalizations by Rado (in terms of so-called regular equations on integers) and we will see them below

Excursions into infinite - Ramsey

- There is a couple of species of combinatorists that deal with infinite sets
  - For instance we may want to color K_N, the complete graph on the set N of all natural numbers with a finite number of colors
  - Then there is a monochromatic infinite clique
- Then you may want to have same kind of properties on cardinals larger than $|N|$ (if you believe that something like this exists)
- This has serious metamathematical consequences (and I will not be talking about it)
- More generally, Ramsey properties on infinite sets relate to issues such as consistency of Peano arithmetic, and like

Excursions into infinite - Schur

- Here is the infinite version of Schur theorem
  - Every coloring of N with a finite number of colors has a monochromatic triple $a_0, a_1, a_0 + a_1$
- In other words the equation $x_0 + x_1 - x_2 = 0$ has a monochromatic solution
- What about a more general equation:

$$a_0 x_0 + \ldots + a_n x_n = 0$$

- First, we need to get an appropriate definition

Excursions into infinite - Schur, cont'd

- An equation $E := a_0x_0 + \ldots + a_nx_n = 0$ is called *regular* if for any positive integer k, and any coloring of N with k colors, there is a monochromatic solution to E
- (Schur Theorem says that the equation $x_0 + x_1 - x_2 = 0$ is regular)
- Rado proved that an equation E as above is regular if and only if it possesses a nontrivial 0-1 solution
- That is, for some $\emptyset \neq I \subseteq [n]$, $\Sigma_{i \in I} a_i = 0$

Now fun starts

- So we have no *closed* form for any of these functions (Hilbert, Schur, v.d. Waerden, Ramsey, Hales-Jewett, you name it)
- This does not mean that there is none; maybe humanity did not found it
- Since 17th century mathematicians learned (slowly) to live with functions that have no closed form (an example of such strange animal is solution to Riccati differential equation)
- What about approximations?

Fun continues

- There is one case where approximate solution is known. Specifically, the rate of growth of the function $k(n) = R(3, n)$ is known
- In 1995, J-H. Kim proved that

$$k(n) = \Theta(\frac{n^2}{ln^2(n)})$$

  That is the ratio of $R(3, n)$ and $\frac{n^2}{ln^2(n)}$ is bound from both sides by constants
- In fact $k(n) \sim c\frac{n^2}{ln^2(n)}$, but the constant c is not exactly known!
- This is, certainly, a great achievement, obtained by probabilistic methods

And then there was Doug Wiedemann

- Dedekind number $d(n)$ is the number of antichains in $\mathcal{P}([n])$
- Dedekind introduced it in 1897
- $d(n)$ is the number of monotone Boolean functions on n variables
- Only 8 are known. $d(8)$ was computed(?) by D.H. Wiedemann (with Thinking Machines Corp. at the time). It is:
$$56130437228687557907788$$
- (The original result is confirmed in Wikipedia, unclear what it means)
- I am not aware of this result recomputed

So what now?

- Say we believe that there is a closed form for one of these functions (call it Erdös *dream* for such function)
- What would be needed to really prove it?
  - First, data
  - Then someone with an idea and audacity to try it
- What would be data?
- Enough of values of the function in question
- Then maybe, just maybe, someone would figure it out

What about the data?

- Could we find some values?
- Sometimes fingers of two hands are enough; this is certainly the case of $R(3,3)$ or $w(2,3)$
- What is normally done by mathematicians?
- They would find a lower bound (i.e. a counterexample below) and upper bound
- In upper bound case the situation is conceptually harder because one needs to show that something happens *always* above some integer
- In the lower bound case they would find a *certificate*, a configuration where there is a counterexample

Logic and solutions to problems

- When we have a finite domain (for instance [25] or [44]) and a problem P (for instance existence existence of a graph with some properties on that domain) then we can write a *propositional theory* T_P on a suitably chosen set of propositional variables so that there is *one-to-one* correspondence between the solutions to the problem P and satisfying assignments for T_P
- It is easy to do something of this sort for any specific n (say 19) and the coloring of of complete graph in two colors without a clique of size 5
- When such satisfying assignment codes an example we talk about *certificate* kind)

Certificates and Ramsey number

- When an integer is strictly smaller than, say $R(k)$ then there is a certificate to this fact
- When we are at Ramsey number or above - there is none
- In other words, for each n we can write a clausal theory $T_{n,k}$ with the following properties:
  - When $n < R(k)$, $T_{n,k}$ is satisfiable (and in fact we can read off the satisfying assignment the certificate)
  - When $n \geq R(k)$, $T_{n,k}$ is not satisfiable
- There is a difference between these two situations - in the first case we just need to find one certificate, in the other we have to search the entire search space and fail to find one

But this is general

- In other cases (and variations that we provided) the same property holds
- In each case we can write a parameterized propositional theory $T_{\mathcal{P},P,n}$ (here $\mathcal{P}$ is a problem, P appropriate sequence of parameters, n an integer) with the desired properties
- (Let me be a bit imprecise)
  - When n is smaller than $f_{\mathcal{P},P,n}$ then $T_{\mathcal{P},P,n}$ is satisfiable and a satisfying assignment for $T_{\mathcal{P},P,n}$ determines a suitable certificate
  - When n is larger or equal than $f_{\mathcal{P},P,n}$ then $T_{\mathcal{P},P,n}$ is not satisfiable

Example

- Say, we want to write the theory (actually *two* theories) needed to deal with the McKay and Radziszowski result that $R(4,5) = 25$
  - We need to write a theory $T = T_{R,\langle 4,5\rangle,24}$ so that satisfying assignments for T describe graphs on [24] with no red clique of size 4, and no blue clique of size 5
  - We also need a theory $T' = T_{R,\langle 4,5\rangle,25}$ that does the same for the number 25
- Then with our superfast solver, we find solution for T
- Next, we run our solver on T' and, eventually, get the answer “UNSAT”

How to build theories for our example

- We do it for T (T' is quite similar)
- We need $\binom{24}{2} = 276$ atoms
- The atoms are labeled with pairs x, y where $0 \leq x < y < 24$
- Then, for every four element-subset S of [24] we generate the formula φ_S which is the conjunction of 6 atoms corresponding to the red complete graph on S
- Next, for every five element-subset S' of [24] we generate the formula $\psi_{S'}$ which is the conjunction of negations of 10 atoms (which describes blue complete graph on S')
- Then we take the disjunction consisting of all φ_S and $\psi_{S'}$ (over four-element Ses, five-element S's)
- (T' has 300 variables, the rest is similar)

The main point

- We have techniques for building T and T' because we can systematically generate all four-element subsets and all five-element subsets
- We can generate similar theories $T_{R,\langle k_1,\ldots,k_m\rangle,n}$ for more complex Ramsey numbers (we need to be a bit careful, but not much more, except that the number of atoms grows more significantly with the number of colors)

Building theories

- For each other case (Schur, van der Waerden, but also Rado) we can also build theories (there will be differences because we partition nodes, not edges)
- The “main point” above applies - we can systematically generate Schur triples, arithmetic progressions, solutions to another regular equation, etc
- (Fortunately we do not do this by hand)

To sum it up

- Building theories is relatively simple
- (Optimizing these theories to reduce work is another matter)
- The key is, of course, the solvers which carry the work and the whole “under-the-hood” mechanics of SAT; restarts, partial closure under resolution (a.k.a. learning from conflicts), heuristics
- But we can successfully do Knowledge Representation in SAT and so we can build these theories

But what about v.d. Waerden numbers?

- Some colleagues and I noticed that quite a lot of lower bounds can be found using solvers (SAT solvers, ASP solvers)
- But there is more to that
- Imagine you not only want a certificate showing your number is below (whatever function you are looking at) but you want to find *all counterexamples* at this place
- We did that for the old result of Beeler and O'Neil and computed all certificates at the critical number
- Specifically, Beeler and O'Neil found that w(4,3,3,3,3) is 76; we found all critical configurations on 75

The argument of McKay

- McKay argued *against* applications of solvers in the search for specific numbers
- His argument was like this: if there is anything useful in the search methods used by (say) SAT community, then we (the combinatorists) can strip the details related to SAT and add number-theoretic improvements and do an even better job
- But it turns out that the general-purpose solvers *and* proper knowledge representation can provide advantage in computation of v.d. Waerden numbers

Kouril's work

- Mihal Kouril computed $w(2,6)$ (two colors, arithmetic progression of length 6)
- This number is 1132
- The work was done using special purpose solver, actually a massively parallel solver on a reconfigurable hardware, specifically a number of FPGA circuits
- Again, the time needed was of the order of years, and the result was not repeated by others
- Since then Mihal computed other v.d. Waerden numbers and lower bounds
- Mihal used some vdW-numbers specific heuristics, so maybe McKay was not 100% wrong

But there is more

- In the past couple of years Kullmann and collaborators, esp. Ahmed, obtained numerous additional results showing both specific v.d. Waerden numbers and lower bounds
- In fact the results found in their work lead to new research in the area of v.d. Waerden numbers, for instance showing that a natural conjecture on the bounds of numbers $w(2,3,s)$ is false and many other specific results
- Availability of many certificates (an obvious benefit of using SAT technology) allows to classify them and as the result introduce new classes of v.d. Waerden numbers for instance not admitting certificates of certain kind
- (Analogous concepts occur in the area of Schur numbers)

Few things changed in the meanwhile

- Modern Experimental Mathematics started with the work by Haken and Appel on Four-Color Theorem
- Clearly it is now a recognized area of Mathematics (?) with its own journals
- One of these, called *Integers, Electronic Journal of Combinatorial Number Theory* publishes results related to specific values of functions of our interest
- This is a significant change to, say, 10 years ago when there were no reasonable venues for such work, or rather results of this sort were not really often found
- (Actually, *Integers* has a quite prominent editorial board)

But is it just a one-way street?

- We can use the *families* of problems to test solvers
- Specifically $\langle T_{\mathcal{P},P,n} : n < m \rangle$ for suitably chosen problem $\mathcal{P}$, parameters P and the length of the family of test cases m
- Thus we can use extremal combinatorics both for testing solvers and for finding new publishable results
- And then maybe, just maybe, we could contribute to the Erdös Dream

Some worries

- In other experimental sciences, for instance in molecular biology experiments are often repeated by independent groups of researchers
- Why?
- In molecular biology one sometimes finds in papers statements such as “Our results appear to conflict with ...”
- We did not see anything like this in experimental science associated with Erdös dream
- Will we?

Proof systems

- When we search the space of assignments and do not find solution we implicitly *prove* a formula
- That formula is a universal formula over (for instance) Z_2
- But that proof is of monstrous size
- That proof is another certificate, but of something else, namely unsatisfiability that is a prof of $\perp$
- If we have it in its entirety checking that indeed it is a proof is easy
- Thus, maybe, more efforts related to proof systems are needed

Future will take care of my worries?

- I guess, when instead of half-year to repeat McKay-Radziszowski we will be able to do it in 10 minutes the issue of their repeatability will disappear
- (This is suggested by Oliver Kullmann)
- But the cosmic sizes of the search spaces appear to suggest that unless someone figures out the closed forms, there will be NO final frontiers in Erdös Dream
- I do not know whether the quantum computing will help
- In case of ASP Remmel and collaborators were able to get a quantum algorithm for computation of answer sets
- So, who knows, maybe SAT and related problems will be solved in a multiverse?

Conclusions

- There is a two-way street between SAT (and related formalisms) and extremal combinatorics
- There is plenty to be done on SAT side
- The books (see *Resources* slide below) are full of specific problems waiting to be solved, and specific configurations to be found or (better yet) not to be found
- (I focused on 5 specific and best known problems, but there are many others, for instance generalizations I discussed above)
- Generally, the books on Combinatorics have plenty of topics where specific numbers are not known

Message to be taken home

- SAT promotes experimental aspects of Mathematics
- In the process *some* aspects of Mathematics change
- But Mathematics provides us with problems to be used in testing SAT, too
- I feel that we can be proud of taking part in the development of this novel branch of Mathematics

Resources

- When you want gossip, look up introduction by Alexander Soifer to *Ramsey Theory, Yesterday, Today, and Tomorrow*, Birkhäuser, 2011
- This book contains presentations of the Rutgers University 2010 workshop with the same name
- Soifer also wrote a fantastic text on coloring in general: *The Mathematical Coloring Book: Mathematics of Coloring and the Colorful Life of its Creators*, Springer 2009
- There is Stan Radziszowski's "Dynamic Survey" called *Small Ramsey Numbers*. This survey (the current one is more than two years old) contains all that Stan knows, and he knows everything in this area

Resources, cont'd

- The *Electronic Journal of Combinatorics* and also *Integers* (mentioned above) and of course *JSAT*
- The book by B.M. Landman and A. Robertson, *Ramsey Theory on the Integers*, AMS, 2004. Contains proofs of all basic theorems
- The book by S. Jukna, *Extremal Combinatorics*, Springer, 2001 contains plenty of proofs related to the area
- (And there are books on SAT)