On the history of van der Waerden's theorem on arithmetic progressions

Tom C. Brown*and Peter Jau-Shyong Shiue†

Citation data: T.C. Brown and P.J.-S. Shiue, *On the history of van der Waerden's theorem on arithmetic progressions*, Tamkang J. Math. **32** (2001), no. 4, 335–341.

Abstract

In this expository note, we discuss the celebrated theorem known as "van der Waerden's theorem on arithemetic progressions," the history of work on upper and lower bounds for the function associated with this theorem, a number of generalizations, and some open problems.

1 van der Waerden's theorem, and the function $w(k)$

The famous theorem of van der Waerden on arithmetic progressions is usually stated in the following way.

Theorem 1. *(van der Waerden 1927 [24]). For every positive integer k, there exists a positive integer n such that if the set $[1, n = \{1, 2, \ldots, n\}]$ is partitioned into two subsets, then at least one of the subsets must contain an arithmetic progression of size k.*

(Recall that an arithmetic progression of size k is a set of the form $\{a, a+d, a+2d, \ldots, a + (k-1)d\}$, where $d > 0$.)

This latter statement (with r subsets instead of two subsets) is the statement given in van der Waerden's original proof, which used a double induction on k and r. Van der Waerden's original proof was found with the help of Artin and Schrier. See [25] for a nice description of how the proof was found, and of the proof itself.

Good expositions of this proof are given in the charming book by Khinchin [14], and in the book by Graham, Rothschild, and Spencer [13]. Other proofs of this statement can be found in [1, 7, 15, 22]. Perhaps the easiest of these to read is [15]. A very short proof is in [13]. A topological proof is in [9]. An algebraic proof is in [2].

For each positive integer k, we let $w(k)$ denote the *smallest* positive integer such that if the set $[1, w(k)]$ is partitioned into two subsets, then at least one of the subsets must contain an arithmetic progression of size k. The function $w(k)$ is often called the *van der Waerden function*.

*Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V3G 1G4. tbrown@sfu.ca

†Department of Mathematical Sciences, University of Nevada, Las Vegas, NV, USA 89154-4020. shiue@nevada.edu

One can use a simple backtrack procedure to find the exact value $w(k)$ for small values of k. The idea is, first of all, to replace a partition of $[1,n]$ by a binary sequence of length n. The sequence 00110011, for example, corresponds to the partition $\{1,2,5,6\},\{3,4,7,8\}$, as illustrated in this diagram:

1	2	3	4	5	6	7	8
0	0	1	1	0	0	1	1

An arithmetic progression of size k which is contained in one of the sets of the partition then corresponds to k equally space 0's or k equally spaced 1's. One then "grows" a maximal (i.e., non-extendable) binary sequence which does not contain k equally spaced 0's or 1's, by starting with a 0, then at each stage adding a 0 at the end of the sequence if possible (that is, if the addition of this 0 does not produce k equally spaced 0's). If adding a 0 is not possible, then one adds a 1, if possible. If neither 0 nor 1 are possible, the given sequence is maximal. In this case, one goes back and changes the latest 0 to a 1 (if this produces 3 equally spaced 1's, then one goes back to the next preceding 0 and changes that to a 1), and then continues to form another maximal sequence. This is repeated, until the procedure requires the initial 0 to be changed to a 1; by symmetry, one can stop at this point. The length of the longest binary sequence obtained in this way will be $w(k)-1$.

For example, with $k=3$ the first few maximal binary strings obtained in this way are listed below. Each line ends when neither a 0 nor a 1 can be added to the string. Then the latest 0 is changed to a 1, and the process continues on the next line. In the first line, a 0 cannot be added because of the 0's in positions 2 and 5. (Adding a 0 would produce 3 equally spaced 0's in positions 2,5,8.) A 1 cannot be added in the first line because of the 1's in positions 6 and 7. (Adding a 1 would produce 3 equally spaced 1's in the positions 6,7,8.) Then, the 0 in position 5 is changed to a 1, to begin the second line.

1	2	3	4	5	6	7	8
0	0	1	0	0	1	1	
0	0	1	0	1	1		
0	0	1	1	0	0	1	1
...							

This process will terminate in less than a page, to show that $w(3)=9$. a computer will find in a few seconds that $w(4)=35$. Unfortunately, this simple backtrack procedure takes far too long even for the case $k=5$. A refinement [19] was used to show $w(5)=178$; the CPU time used was about 6 months. These values, together with $w(2)=3$, are the only known values of $w(k)$. G. Mills has pointed out that for these known values, $w(k)$ is very close to $(3/2)k!$.

2 Upper bounds on the van der Waerden function

Every known proof of van der Waerden's theorem gives, at least implicitly, an upper bound for the function $w(k)$. For example, if we let $w(k,r)$ denote the smallest value of n such that in every partition of the interval $[1,n]$ into r subsets, at least one subset must contain an arithmetic progression of size k, then the proof found in Khinchin's book gives $w(3)=w(3,2)<5\cdot(2\cdot 2^5+1)$, $w(3,3)<7\cdot(2\cdot 3^7+1)(2\cdot 3^{7\cdot(2\cdot 3^7+1)}+1),\ldots$, and then $w(4)=w(4,2)<14\cdot(\frac{3}{2}w(3,2^{14})+\cdots)$.

We can see from the pattern of these bounds that the bound on $w(3, 2^{14})$, and hence the bound on $w(4)$, will involve a tower of exponents of height 2^{14}, very much larger indeed than $w(4) = 35$.

These bounds (and the bounds given by all other proofs prior to 1987) are in fact so large that it was not known until 1987 whether or not $w(k)$ was a primitive recursive function. R. L. Graham for many years had a standing offer of US \$1000 for a proof or disproof of the bound $w(k) < 2^{2^{\cdot^{\cdot^{2}}}}$, where there are k 2's in this tower of exponents.

In 1987 S. Shelah [18] gave a completely new combinatorial proof of van der Waerden's theorem which gave an upper bound for $w(k)$ which was tiny in comparison with earlier proofs. To describe the Shelah upper bound, first define the sequence of numbers $n_1, n_2, \dots$ by $n_1 = 2$, $n_2 = 2^2 = 4$, $n_3 = 2^{2^{2^2}} = 2^{16} = 65536$, $n_4 = 2^{2^{\cdot^{\cdot^{2}}}}$, where this is a tower of 65536 2's, $n_5 = 2^{2^{\cdot^{\cdot^{2}}}}$ where this is a tower of n_4 2's, and so on. Shelah showed that $w(k) < n_{k+2}$. Although this was far weaker than $w(k) < 2^{2^{\cdot^{\cdot^{2}}}}$, Graham awarded him US \$500, and the original prize was still available.

In 1999, at a meeting in Budapest, on "The Mathematics of Paul Erdős," Graham handed over a check for the full amount of US \$1000 to W. Timothy Gowers, who had proved that $w(k) < 2^{2^{2^{2^{2^{k+9}}}}}$. At the same time, Graham announced that he would now give US \$1000 for a proof or disproof of the bound $w(k) < 2^{k^2}$.

Brown [4] showed that if one chooses a *random* partition of the interval $[1, (\log k)^2 2^k]$ into two subsets, then the probability that at least one of these subsets contains an arithmetic progression of size k goes to 1 as $k \to \infty$. It is likely that this remains true for the interval $[1, 2^k]$.

3 Lower bounds on the function $w(k)$

A straightforward application of the "probabilistic method," using also the Lovász Local Lemma, gives a lower bound of $(1 + o(1))(2^k/2ek) < w(k)$, where $e = 2.718\dots$. Here $o(1)$ is a function on k which converges to 0 as $k \to \infty$. For details see [13]. Zoltán Szabó [20] improved this to: for every $\varepsilon > 0$, $2^k/k^\varepsilon < w(k)$ for all sufficiently large k.

By a constructive argument, Berlekamp [3] showed that for primes p, $p \cdot 2^p < w(p+1)$.

It follows from Berlekamp's result that $\limsup w(k)/2^k = \infty$ as $k \to \infty$. Paul Erdős offered US \$25 for a proof that $\lim w(k)/2^k = \infty$ as $k \to \infty$. This remains an attractive open question, and the US \$25 prize still stands.

4 Szemerédi's Theorem

Szemerédi's theorem is the following statement:

Theorem 2. *(Szemerédi 1974 [21]). For every $k \geq 1$ and every $\varepsilon > 0$ there exists n such that*

$$\begin{bmatrix} A \subseteq [1, n] \\ |A|/n \geq \varepsilon \end{bmatrix} \implies \begin{bmatrix} \textit{A contains an arithmetic} \\ \textit{progression of size } k \end{bmatrix}$$

This clearly implies van der Waerden's theorem, for if k is given and we partition $[1,n]$ into two subsets, then at least one of them, call it A, will have the property that $|A|/n \geq 1/2$. Taking $\varepsilon = 1/2$ in the above statement, if n is large enough then A must contain an arithmetic progression of size k.

This statement was conjectured by Paul Erdős and Paul Turán in 1936. It was first proved for the case $k = 3$ by Klaus Roth in 1952 [17], using trigonometric sums. Then in 1974, Erdős offered US $1000 for a proof of the general case. A proof for the general case was found by Szemerédi in 1974 [21]. (This proof was called "a masterpiece of combinatorial reasoning" by Graham, Rothschild, and Spencer [13].)

The US $1000 awarded to Szemerédi is the largest prize every collected for an Erdős problem.

In 1977 Furstenberg [10] found an entirely different proof, using ergodic theory.

In 1998 W. Timothy Gowers found another proof which (as mentioned above), resulted in a sensational improvement of Shelah's upper bound for the van der Waerden function $w(k)$. Gowers' proof used Fourier analysis and probability theory, as well as combinatorics. His proof for the case $k = 4$ is in [12]. The proof for the general case has not yet appeared.

Now for each positive integer k and each positive real number ε, we let $Sz(k,\varepsilon)$ denote the *smallest* positive integer such that

$$\left[\begin{array}{c} A \subseteq [1,n] \\ |A|/n \geq \varepsilon \end{array}\right] \Longrightarrow \left[\begin{array}{c} A \text{ contains an arithmetic} \\ \text{progression of size } k \end{array}\right]$$

The function $Sz(k,\varepsilon)$ is called the *Szemerédi function*.

Theorem 3. *(Gowers 1998). For every positive integer k and every positive real number* ε, $Sz(k,\varepsilon) < 2^{2^{(1/\varepsilon)^{2^{2^{k+9}}}}}$.

Since for every partition of $[1,n]$ into two subsets, at least one of the subsets, call it A, has $|A|/n \geq 1/2$, it follows from Theorem 3 that $w(k) \leq Sz(k,1/2) < 2^{2^{2^{2^{2^{k+9}}}}}$.

5 Other results and open questions

Erdős and Graham [8] observed that Szemerédi's theorem implies the following result: If the set of all positive integers is partitioned into arbitrarily many subsets (perhaps infinitely many), then for every k there is an arithmetic progression P of size k with the property that either P is completely contained in one of the subsets, or else P intersects each subset in at most one element. This result (called the *canonical form of van der Waerden's theorem*) is often stated in the following way: If f is an arbitrary function from the positive integers to the positive integers, then there are arbitrarily large arithmetic progressions P such that the restriction of f to P is either constant or one-to-one.

Deuber, Graham, Prömel and Voigt [6] proved the "multi-dimensional version" of the canonical version of van der Waerden's theorem. Their proof makes use of Furstenberg and Katznelson's multi-dimensional generalization of Szemerédi's theorem [11], for which no elementary proof is yet known. (Furstenberg and Katznelson's proof uses heavy ergodic tools.) Later, a combinatorial proof (of the multi-dimensional version of the canonical form of van der Waerden's theorem) was given by Prömel and Rödl [16] which did not use Szemerédi's theorem.

One of Erdős's most famous conjectures, for which he offered US \$3000, and later US \$5000, is the following. Let A be a set of positive integers such that $\sum_{n \in A} \frac{1}{n} = \infty$. Then for every k, A must contain an arithmetic progression of size k. This statement, if true, is stronger than Szemerédi's theorem. It still remains open, even for $k = 3$.

Erdős offered US \$10,000 for an explicit asymptotic formula for the function $g(n)$, where $g(n) = \max\{|A| : A \subseteq [1,n]$ and A contains no arithmetic progression of size $k\}$. Again, Szemerédi's theorem implies that $g(n,k)/n \to 0$ as $n \to \infty$.

One can also allow k to depend on n, and Erdős offered US \$100 to settle the question of whether or not $g(n, \log n)/n \to 1$ as $n \to \infty$. This was settled in the affirmative by Brown and Freedman [5], who proved that for all $k \geq 4$, $g(n,k) \geq n - (12n \log n)/(k \log k)$. With $k = \log n$, this gives $g(n, \log n) \geq n - (12n)/(\log \log n)$.

They also noted that the statement $g(n, \log \log n)/n \to 1$ as $n \to \infty$ implies Szemerédi's theorem, and showed that $Sz(p, 1/e) > p^p$ for every prime number $p \geq 7$.

It would be interesting to know the exact value of $g(n^2, n)$ It is known (see [5, 23] that $n^2 - n(1 + o(1)) < g(n^2, n) < n^2 - 2n(1 + o(1)))$.

See also

- `http://www.mathsoft.com/asolve` (an excellent site with many interesting links)
- `http://math.ucsd.edu/~fan` (Fan Chung Graham's web page)
- `http://www.integers-ejcnt.org` (Integers: the Electronic Journal of Combinatorial Number Theory)
- `http://www.combinatorics.org` (The Electronic Journal of Combinatorics)
- `http://can.dpmms.cam.ac.uk/~wtg10` (W. T. Gowers' home page)
- `http://www-groups.dcs.st-andrews.ac.uk/~history/Mathematicians/Erdos.html` (biography of Paul Erdős and links to other Erdős sites)

References

[1] Peter G. Anderson, *A generalization of Baudet's conjecture (van der waerden's theorem)*, Amer. Math. Monthly **83** (1976), 359–361.

[2] Vitaly Bergelson, Hillel Furstenberg, Neil Hindman, and Yitzhak Katznelson, *An algebraic proof of van der Waerden's theorem*, Enseign. Math. (2) **35** (1989), 209–215.

[3] E.R. Berlekamp, *A construction for partitions which avoid long arithmetic progressions*, Canad. Math. Bull. **11** (1968), 409–414.

[4] T.C. Brown, *A pseudo upper bound for the van der Waerden function*, J. Combin. Theory Ser. A **87** (1999), 233–238.

[5] T.C. Brown and Allen R. Freedman, *Small sets which meet all the $k(n)$-term arithmetic progressions in the interval* $[1,n]$, J. Combin. Theory Ser. A **51** (1989), 244–249.

[6] W. Deuber, R.L. Graham, H.J. Prömel, and B. Voigt, *A canonical portition theorem for equivalence relations on z^t*, J. Combin. Theory Ser. A **34** (1983), 331–339.

[7] Walter Deuber, *On van der Waerden's theorem on arithmetic progressions*, J. Combin. Theory Ser. A **32** (1982), 115–118.

[8] P. Erdős and R.L. Graham, *Old and new problems and results in combinatorial number theory*, Monographies de L'Enseignement Mathématique [Monographs of L'Enseignement Mathématique], vol. 28, Université de Genève, L'Enseignement Mathématique, Geneva, 1980.

[9] H. Furstenberg and Y. Katznelson, *Topological dynamics and combinatorial number theory*, J. Analyse Math. **34** (1978), 275–291.

[10] Harry Furstenberg, *Ergodic behavior of diagonal measures and a theorem of szemerédi on arithmetic progressions*, J. Analyze Math. **34** (1978), 61–85.

[11] Harry Furstenberg and Y. Katznelson, *An ergodic Szemerédi theorem for commuting transformations*, J. Analyse Math. **34** (1978), 61–85.

[12] W.T. Gowers, *A new proof of szemerédi's theorem for arithmetic progressions of length four*, Geom. Funct. Anal. **8** (1998), 529–551.

[13] Ronald L. Graham, Bruce L. Rothschild, and Joel H. Spencer, *Ramsey theory*, 2nd ed., Wiley-Interscience Series in Discrete Mathematics and Optimization. A Wiley-Interscience Publication., John Wiley & Sons, Inc., New York, 1990.

[14] A.Y. Khinchin, *Three pearls of number theory*, Dover Publications, Inc., Mineola, NY, 1998, Translated fro the Russian by F. Bagemihl, H. Komm, and W. Seidel. Reprint of the 1952 translation.

[15] George Mills, *A quintessential proof of van der Waerden's theorem on arithmetic progressions*, Discrete Math. **47** (1983), 117–120.

[16] Hans-Jürgen Prömel and Vojtek Rödl, *An elementary proof of the canonizing version of Gallai-Witt's theorem*, J. Combin. Theory Ser. A **42** (1986), 114–149.

[17] Klaus F. Roth, *Sur quelques ensumbles d'entiers*, C. R. Acad. Sci. Paris **234** (1952), 388–390, French.

[18] Saharon Shelah, *Primitive recursive bounds for van der Waerden numbers*, J. Amer. Math. Soc. **1** (1988), 635–636.

[19] R.S. Stevens and R. Shantaram, *Computer-generater van der Waerden numbers*, J. Combin. Theory Ser. A **33** (1982), 30–35.

[20] Zoltán Szabó, *An application of lovász' local lemma — a new lower bound for the van der Waerden number*, Random Structures Algorithms **1** (1990), 343–360.

[21] E. Szemerédi, *On sets of integers containing no k elements in an arithmetic progression*, Acta. Arith. **27** (1975), 199–245, Collection of articles in memory of Jurii Vladimirovic Linnik.

[22] Alan D. Taylor, *A note on van der Waerden's theorem*, J. Combin. Theory Ser. A **33** (1982), 215–219.

[23] J.K. Truss, *Small sets which meet all the n-term arithmetic progressions in the interval* $[1, n^2]$, Bull, London Math. Soc. **23** (1991), 123–127.

[24] B.L. van der Waerden, *Beweis einer baudetschen vermutung*, Nieuw Arch. Wisk. **15** (1927), 212–216.

[25] ———, *How the proof of baudet's conjecture was found*, Studies in Pure Mathematics (Presented to Richard Rado), Studies in Pure Mathematics, Academic Press, London, 1971, pp. 251–260.