# Improving the Use of Cyclic Zippers in Finding Lower Bounds for van der Waerden Numbers

John Rabung, Mark Lotts

Department of Computer Science
Randolph-Macon College

Ashland, VA 23005

jrabung@rmc.edu, marklotts@rmc.edu

Submitted: Nov 2, 2011; Accepted: May 19, 2012; Published: Jun 6, 2012

**Abstract**

For integers $k$ and $l$, each greater than 1, suppose that $p$ is a prime with $p \equiv 1 \pmod{k}$ and that the $k^{th}$-power classes $\bmod\, p$ induce a coloring of the integer segment $[0,\, p-1]$ that admits no monochromatic occurrence of $l$ consecutive members of an arithmetic progression. Such a coloring can lead to a coloring of $[0,\, (l-1)p]$ that is similarly free of monochromatic $l$-progressions, and, hence, can give directly a lower bound for the van der Waerden number $W(k,l)$. P. R. Herwig, M. J. H. Heule, P. M. van Lambalgen, and H. van Maaren have devised a technique for splitting and "zipping" such a coloring of $[0,\, p-1]$ to yield a coloring of $[0,\, 2p-1]$ which, for even values of $k$, is sometimes extendable to a coloring of $[0,\, 2(l-1)p]$ where both new colorings still admit no monochromatic $l$-progressions. Here we derive a fast procedure for checking whether such a zipped coloring remains free of monochromatic $l$-progressions, effectively reducing a quadratic-time check to a linear-time check. Using this procedure we find some new lower bounds for van der Waerden numbers.

## Introduction

For given positive integers $k$ and $l$, the van der Waerden number $W(k,l)$ is the smallest of the integers $N(k,l)$ such that any $k$-coloring of the integer segment $[1,\, N(k,l)]$ is sure to yield a monochromatic set of $l$ consecutive members of some arithmetic progression. That these numbers $N(k,l)$ exist was demonstrated constructively by B. L. van der Waerden [17] in 1927, but his construction, using double induction, was so loose as to be unhelpful in any attempt to determine either the size or the growth rate of $W(k,l)$.

Efforts to locate the numbers $W(k,l)$ have yielded few general results and a number of computational results for particular values of $k$ and $l$. Shelah [15] and Gowers [6] have shown general primitive recursive upper bounds for $W(k, l)$, while general results for lower bounds are attributable to Berlekamp [3] and Moser [13]. Because these upper and lower bounds still do not put very tight constraints on the values of $W(k, l)$, computational approaches have been used either to determine some $W(k, l)$ exactly by exhaustive search (see [4, 16, 2, 11]) or to improve on a lower bound for some $W(k, l)$ by finding ever-larger values of $n$ for which the integer segment $[1, n]$ can be $k$-colored so that there is no monochromatic instance of $l$ consecutive members of an arithmetic progression (see, for example, [14, 5, 10, 7]).

For convenience we use the term *$l$-progression* to mean a sequence of $l$ consecutive members of an arithmetic progression, and we use *$l$-string* to mean $l$ consecutive integers. For given $k$, $l$, and $n$, we follow Herwig et al. [10] in referring to a $k$-coloring of $[1, n]$ that is devoid of monochromatic $l$-progressions as a *van der Waerden certificate* and use the notation $W(k, l, n)$ to represent such a certificate. Of course, the existence of a certificate $W(k, l, n)$ implies $W(k, l) > n$.

Several recent works have encoded the construction of a van der Waerden certificate as a constraint satisfiability problem and have used fast satisfiability-checking algorithms to find improved lower bounds for van der Waerden numbers. This approach is well explained in a number of papers (see, for example, [5, 12, 1, 9]). Herwig et al. [10] used both satisfiability checking and coloring by $k^{th}$-power classes modulo a prime $p$ (the latter being a technique introduced in [14]) to devise a clever method for extending some certificates, $W(k, l, n)$, to certificates $W(k, l, 2n)$, thus doubling a lower bound for $W(k, l)$. Referring to this method as *zipping*, they were able to substantially improve lower bounds for seven van der Waerden numbers.

In this paper we follow Herwig et al. by starting with certificates generated, as in [14], via $k^{th}$-power-class coloring modulo a prime $p$ and then investigating what arithmetic properties might be preserved through the zipping technique. These arithmetic properties lead to a certificate-checking technique that is both very fast and quite reminiscent of checking techniques used in finding power-class-based certificates. Using this approach we are able to provide some new lower bounds for van der Waerden numbers.

# Zipping viewed arithmetically

Herwig et al. [10] define a *cyclic certificate* as a van der Waerden certificate $W(k, l, n)$ that preserves its certificate property under cyclic translation of its $k$-coloring mod $n$. Given a cyclic certificate $W(k, l, n)$ they attempt to extend it to a certificate $W(k, l, 2n)$ by applying their *zipping procedure.* Because every application of this procedure in [10] begins with a cyclic certificate $W(k, l, p)$ derived from the $k^{th}$-power classes of a prime, $p$, where $p = km + 1$ for some integer $m > 0$, we shall focus our discussion on the zipping of such certificates noting particular arithmetic properties of zipped colorings that yield a fast mechanism for checking whether the zipping of a certificate $W(k, l, p)$ does or does not yield a certificate $W(k, l, 2p)$. As indicated in both [14] and [10], once such a cyclic certificate is in hand, one can join $l - 1$ copies of it to generate an even longer van der Waerden certificate and a better lower bound for $W(k, l)$.

Let $\mathbb{Z}_p$ represent the ring of integers modulo $p$. That the non-zero elements of $\mathbb{Z}_p$ form a cyclic group under multiplicaton allows us to use the powers of any fixed generator of this group to generate the $k^{th}$-power classes mod $p$. We use $\mathbb{Z}_p^*$ to represent this cyclic group, and we use $g$ to represent a generator of that group (that is, $g$ is a primitive root mod $p$). Because $p$ is of the form $km+1,$ the set $C_0 = \left\{g^{\mathrm{jk}} \operatorname{mod} p : j = 1, 2, ..., m\right\}$ forms a subgroup of $\mathbb{Z}_p^*$ known as the *$k^{th}$-power residues* mod $p$. The $k-1$ cosets of $C_0$ are $C_i = \left\{g^{\mathrm{jk}+i} \operatorname{mod} p : j = 1, 2, ..., m\right\}$ with $i = 1, 2, ..., k-1$. Together this collection $\{C_i : i = 0, 1, ..., k-1\}$ gives the *$k^{th}$-power classes* mod $p$. Indeed, we can view these classes as inducing a $k$-coloring on $[1,\, p-1]$ by considering any element $h \in [1,\, p-1]$ to have color $i$ if $h \in C_i$ with $i \in [0,\, k-1]$. We extend this $k$-coloring to $[0,\, p-1]$ by coloring 0 with any of the given $k$ colors. In the context of devising a cyclic certificate $W(k, l, p)$, the only constraint on coloring 0 is that it must be done so as to avoid forming a monochromatic $l$-progression, even in a cyclic sense.

Given an even integer $k$, a prime $p \equiv 1 \, mod \; k,$ and a certificate $W(k, l, p)$ derived from a coloring of $[0,\, p-1]$ via the $k^{th}$-power classes mod $p$ as determined by some fixed generator $g_0$ of $\mathbb{Z}_p^*,$ the following describes the steps of the zipping procedure as given in [10] as they apply to the zipping of *W(k,l,p)*. With each step we give our arithmetic interpretation of that step's action:

1. **Spreading:** Use the given $k$-coloring of the segment $[1,\, p]$ to color the odd numbers in $[1,\, 2p]$ so that the color of $2j-1$ in $[1,\, 2p]$ is the same as the color of $j$ in the original coloring of $[1,\, p]$ for $j = 1,\, 2, \ldots,\, p$. Call this *partial coloring 1* of $[1,\, 2p]$.

   *Comment*: Here we note some minor awkwardness. Although we have been viewing colorings of integer segments $[1,\, n]$ that begin at 1, it is arithmetically convenient to translate such a coloring down by one to the segment $[0,\, n-1]$. We transit between these two views as we describe the steps of zipping and then interpret them arithmetically.

   *Arithmetic equivalent*: Use the given $k$-coloring of the segment $[0,\, p-1]$ to color the even numbers in $[0,\, 2p-1]$ by multiplying the elements of $\mathbb{Z}_p^*$ by 2 and assigning each number, $2m$ mod $2p$, to class $C_{(i+t) \operatorname{mod} k}$, where $C_i$ is the class to which $m$ was assigned in the given certificate and $C_t$ is the class to which 2 was assigned in the given certificate. (This is, of course, the class to which $2m$ belongs as a member of $\mathbb{Z}_p^*$.) Once again we choose to color 0 arbitrarily. Call this *partial arithmetic coloring 1* of $[0,\, 2p-1]$.

   Apart from shifting the underlying segment of $p$ numbers from $[1,\, p]$ to $[0,\, p-1]$ and the consequent interchange of the terms "odd" and "even" as the coloring is extended to the doubled segment, this multiplicative step is equivalent to spreading. Note, though, that the addition of $t$, the index of the $k^{th}$-power class to which 2 belongs, relabels the colors without altering the coloring pattern. This is not part of the original spreading step.

2. **Turning:** Because power-class-based certificates $W(k, l, p)$ display certain symmetries ([10] discusses both point symmetry and reflection symmetry), Herwig et al. highlight these by way of a grid representation of the certificate wherein rows represent colors, columns represent the numbers in the segment [1, $n$] or [1, $2n$], and rows have been arranged so as to clearly demonstrate the symmetry of the coloring. With this arrangement of rows and the resulting subscript relabeling of colors (away from power-class labeling), the authors suggest that partial coloring 1 now be "turned upside down". That is, under the symmetry-imposed labeling of the $k$ colors of our certificate as $c_1$, $c_2, \ldots,$ $c_k$, alter partial coloring 1 by substituting color $c_{k+1-i}$ for each occurrence of color $c_i$ for $i = 1,$ $2, \ldots,$ $k$. Call this *partial coloring 2* of [1, $2p$].

   *Arithmetic equivalent*: Noting that $k$ is even and that $p$ is a prime of the form $km + 1$, we observe that the $k^{th}$-power class to which $p - 1$ belongs determines whether our $k$-coloring is point symmetric or reflection symmetric. Given that $p - 1 \in C_h$, we have that $p - 1 \equiv g_0^{ki+h} \, mod \, p$, for some $i$ and our chosen generator, $g_0$, of $\mathbb{Z}_p^*$, so that for any number $n \in [1,\, p-1]$ if $n \in C_j$, then $n \equiv g_0^{ks+j} \, mod \, p$ for some s and $p - n \equiv (p-1)n \equiv g_0^{k(i+s)+h+j} \, mod \, p$. That is, if $p - 1 \in C_h$ and $n \in C_j$, then $p - n \in C_{(h+j) \, mod \, k}$. Observing that $p - 1 \equiv -1 \equiv g_0^{\frac{p-1}{2}} \equiv g_0^{\frac{km}{2}}$ $(mod\ p)$, we have that if $m$ is even, then $h = 0$, and we get reflection symmetry. If $m$ is odd, then $h = \frac{k}{2}$, and we get point symmetry. The "turn upside down" action, then, amounts to interchanging color classes according to the underlying symmetry. Here it amounts to shifting class indices by $h$ mod $k$. That is, if in partial arithmetic coloring 1 a number is colored with color $j$, change the color of that number to color $(j + h) \, mod \, k$, where $h$ is either 0 or $\frac{k}{2}$ according as $m$ is even or odd in the expression of $p$ as $km + 1$. Call the resulting coloring *partial arithmetic coloring 2.*

3. **Shifting:** Use partial coloring 2 to produce a coloring of the even numbers of [1, $2p$] by applying the color of $2j-1$ in partial coloring 2 to the number $2j-1-p \, (mod \, 2p)$ for $j = 1,$ $2, \ldots, p$. Call this *partial coloring 3* of [1, $2p$]. (Note that this step depends on $p$ being odd and that any attempt to do a second zipping–a zipping of a coloring of [1, $2p$]–will shift by $p$ in this step, not by $2p$.)

   *Arithmetic equivalent*: Noting that the odd numbers of $[0,\, 2p-1] - \{p\}$, a reduced residue system $mod \, 2p$, form a cyclic group under multiplication $mod \, 2p$ (we denote this group $\mathbb{Z}_{2p}^*$) and that if $g$ is a generator of $\mathbb{Z}_p^*$, then either $g$ or $g + p$, whichever is odd, is a generator of $\mathbb{Z}_{2p}^*$, we use $g_0$ (or, if $g_0$ is not odd, use $g_0 + p$) to determine the $k^{th}$-power classes of $\mathbb{Z}_{2p}^*$ and use those class assignments and an arbitrary coloring of $p$ to induce a $k$-coloring of the odd numbers in $[0,\, 2p-1]$. Call this *partial arithmetic coloring 3* of $[0,\, 2p-1]$.

   A reduced residue system mod $2p$ can be obtained through a doubling of each element of $[1,\, p-1]$, a reduced residue system mod $p$. If the doubled result, when reduced mod $p$ to an integer $r$ in $[1,\, p-1]$, is even, view it as the integer $r + p$

in the reduced residue system $\bmod 2p$. If $r$ is odd, view it directly as a member of a reduced residue system $\bmod 2p$. This doubling action maps the integers of $[1,\, \frac{p-1}{2}]$ consecutively to the odd integers of $[p+2,\, 2p-1]$ and maps the integers of $[\frac{p+1}{2},\, p-1]$ consecutively to the odd integers of $[1,\, p-2]$. Given that we use the same generator $g_0$ (or $g_0+p$), this is nothing more than a cyclic shifting by $p$ units within $[0,\, 2p-1]$ of the $k$-coloring imposed by doubling action taken in step 1, the spreading step, under our arithmetic view.

4. **Merging:** Do a full $k$-coloring of $[1,\, 2p]$ by coloring the odd numbers of $[1,\, 2p]$ as in partial coloring 1 and coloring the even numbers of $[1,\, 2p]$ as in partial coloring 3.

   *Arithmetic equivalent*: Do a full $k$-coloring of $[0,\, 2p-1]$ by coloring the even numbers of $[0,\, 2p-1]$ as in partial coloring 2 and coloring the odd numbers of $[0,\, 2p-1]$ as in partial coloring 3. The careful reader will note that we merge colorings 2 and 3 here while the original zipping procedure merged colorings 1 and 3. If we had shifted partial coloring 2 to get partial coloring 3, we would have done the original merge. Rather we prefer to use the turning step on the even numbers because it will allow us to see directly the arithmetic structure of the power classes in the coloring of the odd numbers and because it yields the same color labeling as that shown in [10] rather than a simple translation of color labels mod $k$.

# Validation of a zipped cyclic certificate

Given a cyclic certificate $W(k,l,p)$ whose coloring of $[0,\, p-1]$ (equivalently, $[1,\, p]$) arises from the distribution of $k^{th}$-power classes modulo the prime $p$, the zipping procedure will yield a $k$-coloring of $[0,\, 2p-1]$, but that coloring may or may not be free of monochromatic $l$-progressions; that is, it may or may not be a certificate $W(k,l,2p)$. Certifying that a zipped coloring is still $l$-progression free requires checking each of approximately $\frac{(2p-1)^2}{2(l-1)}$ $l$-progressions in $[0,\, 2p-1]$. Using arithmetic properties of the zipped coloring, however, allows us to cut this to little more than a check of at most $2p-l-1$ $l$-strings, essentially a reduction from a quadratic-time process to a linear-time process, since we shall be dealing with large values of $p$ and small values of $l$.

A similar speed-up was used in [14] to find certificates $W(k,l,p)$ based on $k^{th}$-power classes modulo a prime $p$. This speed-up depended heavily on the following simple *observations* (using $k^{th}$-power-class notation introduced in the preceding section):

1. For any $a$, $b$ in $\mathbb{Z}_p^*$, if $a \in C_i$ for some $i$ and $b \in C_j$ for some $j$, then $ab \in C_{(i+j)\, mod\, k}$. That is, because indices of $k^{th}$-power classes mod $p$ are based on exponents of a fixed generator of $\mathbb{Z}_p^*$, a product of elements of two classes resides in the class whose index is the sum of the indices of the original two classes.

2. If the members of the $l$-progression $a,\, a+d, \ldots,\, a+(l-1)d$ are all in the same $k^{th}$-power class mod $p$, then so are the members of the $l$-string $ad^{-1},\, ad^{-1}+1, \ldots, ad^{-1}+$

$(l-1)$, where $d^{-1}$ represents the inverse of $d$ in $\mathbb{Z}_p^*$. This is just an invocation of observation 1.

A zipped $k$-coloring of $\mathbb{Z}_{2p}$ has a property similar to, but weaker than, that mentioned in observation 1 above, but even in this weaker form it allows application of essentially the same simple criterion for checking whether the coloring is $l$-progression-free. Noting that the two observations above apply equally well in the cyclic group $\mathbb{Z}_{2p}^*$, we establish the following claims.

**Claim 1.** *Given that $k^{th}$-power classes $\bmod p$ and $\bmod 2p$ are formed relative to the same primitive root $g$, if $a$ is in class $C_i \bmod 2p$, then $a$ is also in class $C_i$ mod $p$.*

*Proof.* $a \in C_i \bmod 2p \Rightarrow a \equiv g^{jk+i} \bmod 2p \Rightarrow a \equiv g^{jk+i} \bmod p \Rightarrow a \in C_i \bmod p$. □

**Claim 2.** *Given that $k^{th}$-power classes $\bmod p$ and $\bmod 2p$ are formed relative to the same primitive root $g$, if $a \in C_i \, mod \, p$, then also $a \in C_i \, mod \, 2p$ if $a$ is odd, and $a+p \in C_i \, mod \, 2p$ if $a$ is even.*

*Proof.* If $a$ is even and $a \in C_i \, mod \, p$, then $a = g^{jk+i} + np$ with $n$ odd. (Here, since $g$ must be odd to be a primitive root $mod \, 2p$, if $g$ mod $p$ is even, we take $g+p$, an odd number, as the generator of $\mathbb{Z}_{2p}^*$.) Thus, $a+p = g^{jk+i} + (n+1)p \equiv g^{jk+i} \, mod \, 2p$ (since $n+1$ is even), and $a+p \in C_i \bmod 2p$. And if $a$ is odd and $a \in C_i \bmod p$, then $a = g^{jk+i} + np$ with $n$ even (since $g$ is odd), and we get immediately $a \equiv g^{\mathrm{jk+i}} \bmod 2p$ and $a \in C_i \, mod \, 2p$. □

**Claim 3.** *For any $a$, $b \in [0,\, 2p-1]$ with neither $a$ nor $b$ divisible by $p$, if $a$ and $b$ are in the same class, say $C_j$, under the zipped $k$-coloring of $[0,\, 2p-1]$ as defined above, then $ca$ and $cb$ $mod \, 2p$ are in the same class if $c$ is any odd integer not divisible by $p$.*

*Proof.* We consider 3 cases: $a$ and $b$ both odd, $a$ and $b$ both even, and $a$ odd with $b$ even. The first case follows directly from observation 1 above, since $a, b$, and $c$ are all in $\mathbb{Z}_{2p}^*$, whose $k^{th}$-power classes color the odd numbers in $[0,\, 2p-1]$. In the second case, let $a = 2m$ and $b = 2n$. Here we note that $m$ and $n$, taken $mod \, p$, are both in $\mathbb{Z}_p^*$, and, by the manner in which even numbers are placed in classes in the zipped $k$-coloring of $[0,\, 2p-1]$, $m$ and $n$ are in the same $k^{\mathrm{th}}$-power class mod $p$. So, by observation 1 above, $ca$ and$cb$ are in the same $k^{\mathrm{th}}$-power class mod $p$, and, as a consequence, $ca$ and$cb$ are placed in the same class in the zipped $k$-coloring of $[0,\, 2p-1]$.

It remains only to show that the claim holds for $a$ odd and $b$ even. In this case, suppose $c \in C_i \, mod \, 2p$. Then from observation 1 above (applied to $\mathbb{Z}_{2p}^*$) $ca \in C_{(i+j) \bmod k} \bmod 2p$, and, so, in $C_{(i+j) \bmod k}$ in the zipped coloring as well. Suppose, $b = 2m$ with $m \in \mathbb{Z}_p^*$. Because $b \in C_j$ in the zipped coloring, $m$ must be in $C_{(j-t-\frac{k}{2}) \bmod k}$ among the $k^{\mathrm{th}}$-power classes $mod \, p$. And since $c \in C_i \, mod \, 2p$ implies $c \in C_i \, mod \, p$ (see *Claim 2*), observation 1 indicates that $cm \in C_{(i+j-t-\frac{k}{2}) \bmod k)} \, mod \, p$ so that $cb = 2cm \in C_{(i+j) \bmod k}$ in the zipped coloring. Hence, in this zipped coloring $ca$ and $cb$ are in the same class, as claimed. □

(That *Claim 3* does not hold when $c$ is even is evidenced by using $p{=}113$, noting that in the zipped coloring of $\mathbb{Z}_{226}$ we have $a{=}9$ in $C_0$, $b = 10$ in $C_0$ and multiplying by $c = 10$ we find $ca = 90$ in $C_0$ and $cb{=}100$ in $C_1$.)

**Claim 4.** *If $a$ and $a+d$ are in the same class $C_i$ under the zipped $k$-coloring of $[0,\, 2p-1]$ with $d$ odd and not divisible by $p$, then $ad^{-1}$ and $ad^{-1}+1$ are in the same class of the extended partition of $\mathbb{Z}_{2p}$, where $d^{-1}$ is the multiplicative inverse of $d$ in $\mathbb{Z}^*_{2p}$.*

*Proof.* This follows immediately from *Claim 3* by multiplying both $a$ and $a+d$ by $d^{-1}$. □

It follows from *Claim 4* that if under the zipped coloring of $\mathbb{Z}_{2p}$ there is a single-class arithmetic progrression of $l$ terms beginning at $a$ and having odd common difference $d$, multiplying each member of the progression by $d^{-1} \bmod 2p$ yields a set that forms a single-class $l$-string beginning at $ad^{-1}$. The contrapositive of this—and the aid in checking whether $k$-colorings of long sequences are free of monochromatic $l$-progressions—is that if there is no single-class $l$-string found in the extended partition of $\mathbb{Z}_{2p}$, then there is no single-class $l$-progression with odd common difference.

**Claim 5.** *If $a$ and $a+d$ are in the same class $C_i$ under the zipped $k$-coloring of $[0,\, 2p-1]$ with $d$ even and not divisible by $p$, then $ad^{-1}$ and $ad^{-1}+1$ are in the same $k^{th}$-power classes $\bmod\, p$, where $d^{-1}$ is the multiplicative inverse of $d$ in $\mathbb{Z}^*_p$.*

*Proof.* This follows directly from observation 1 at the beginning of this section. For, an $l$-progression of even common difference will consist either entirely of odd numbers or entirely of even numbers. In the first case note that in the zipped $k$-coloring odd numbers are placed in their $k^{\text{th}}$-power classes *mod* $2p$, but taking these placements *mod* $p$ we still see a single-class $l$-progression and can quickly deduce the existence of a single-class $l$-string in $\mathbb{Z}^*_p$. Likewise, if in the zipped $k$-coloring all members of a single-class $l$-progression are even, we need only note that the classes assigned to the even numbers in the zipped coloring are just relabelings (i.e., shifted labelings) of the $k^{\text{th}}$-power classes mod $p$ so that any $l$-progression can quickly be associated with a single-class $l$-string in $\mathbb{Z}^*_p$. □

As a consequence of *Claim 5*, the existence of single-class $l$-progressions of even common difference within the zipped $k$-coloring of $\mathbb{Z}_{2p}$ will be signaled by the existence of single-class $l$-strings within $\mathbb{Z}^*_p$.

***Criteria for validating that a zipped k-coloring is l-progression free.*** For $k$ even, $p$ a prime of the form $km+1$, and $l > 2$, let *W(k,l,p)* be a van der Waerden certificate whose coloring of $[0,\, p-1]$ (equivalently, $[1,\, p]$) arises from the distribution of $k^{th}$-power classes modulo $p$ and a properly chosen color for 0. The zipping procedure applied to *W(k,l,p)* produces a van der Waerden certificate *W(k,l,2p)* if the zipped $k$-coloring of $[0,\, 2p-1]$ meets the following criteria:

- the $k^{th}$-power coloring of $\mathbb{Z}^*_p$ is free of monochromatic $l$-strings (if $W(k,l,p)$ is a certificate, we already know this);
- the zipped $k$-coloring of $[0,\, 2p-1]$ is likewise free of monochromatic $l$-strings; and
- 0 and $p$ are colored without introducing a monochromatic $l$-string, even in the cyclic sense.

Given that the zipping of a coloring based on $k^{th}$-power classes mod $p$ yields a certificate $W(k, l, 2p)$, we may be able to join $l-1$ of these certificate colorings together to get a certificate $W(k, l, 2(l-1)p+1)$. The following indicates when this joining effort will succeed.

***Criteria for validating an extension of a zipped, cyclic, power-class-based certificate, W(k,l,2p) to a certificate W(k,l,2(l-1)p+1).*** Given a zipped, $k^{th}$-power-class-based certificate, *W(k,l,2p)*, a coloring of $[0, 2(l-1)p]$ done so that

- any $a$ not divisible by $p$ is placed in class $C_j$ where $C_j$ is the class in which $b \equiv a \bmod 2p$ has been placed under $W(k, l, 2p)$ and
- the $2(l-1)+1$ multiples of $p$ in $[0, 2(l-1)p]$ are placed in any of the $k$ color classes so that no monochromatic $l$-progression occurs among these multiples

results in a coloring that is free of monochromatic $l$-progressions providing that:

- if $p-1$ is in $k^{\text{th}}$-power class $C_0 \mod p$, then the integers $1, 2, \ldots, [(l-1)/2]$ are not all in the same class under the coloring of $W(k, l, 2p)$;
- if $p-1$ is not in $k^{\text{th}}$-power class $C_0 \bmod p$, then the integers $1, 2, \ldots, (l-1)$ are not all in the same class under the coloring of $W(k, l, 2p)$; and
- there are no single-class $l$-progressions having common difference divisible by $p$.

# Computations

The above criteria yield a mechanism for a fast search for van der Waerden certificates $W(k, l, 2(l-1)p+1)$. We begin by establishing $k$-coloring profiles of prime numbers up to some reasonable computational limit. For each prime $p$ and a small range of values for $k$ and $l$ with $k$ even our procedure is:

1. Find a generator $g$ of $\mathbb{Z}_p^*$
2. For each of the values of $k$, if $p \equiv 1 \, mod \, k$, record the $k$-coloring profile of $p$ as follows:
    - use $g$ to determine the $k^{th}$-power classes (our basic $k$-coloring) of $\mathbb{Z}_p^*$;
    - record whether $p-1$ is in class $C_0$;
    - record the minimum value of $s \in [1,\, p-1]$ such that the number $s+1 \notin C_0$;
    - record the length of the longest monochromatic string of integers in $[1,\, p-1]$.
3. With a table of $k$-coloring profiles of primes, it is a simple (and quick) matter to search the table and apply the criteria given in [14] to find among the profiled primes those that yield cyclic certificates $W(k, l, p)$.

4. Apply the zipping technique to certificates $W(k, l, p)$ and subject the resulting colorings to inspection for monochromatic $l$-strings, monochromatic $l$-progressions with common difference $p$, and end conditions given by the criteria listed at the end of the previous section. If no such monochromatic $l$-strings or $l$-progressions are found and if the end conditions are met, then the coloring of $[0,\ 2(l-1)p]$ is free of monochromatic $l$-progressions—it gives a certificate $W(k, l, 2(l-1)p+1)$.

We applied this procedure to all primes less than 10,000,000, getting $k$-coloring profiles for $k = 2, 3, 4, 5, 6$, and then searching these profiles for fits to $l$-progression-free colorings with $l = 3, 4, 5, \ldots, 12$. Table 1 shows the known exact values of van der Waerden numbers and gives the best known lower bounds as well as new lower bounds that our procedure has revealed. With each of these new values we show in parentheses the prime number $p$ whose $k^{th}$-power classes formed the basis for the cyclic certificate $W(k, l, p)$ from which can arise a certificate $W(k, l, (l-1)p+1)$. We denote with “Z” in an entry where a single zip procedure was applied to extend successfully to a cyclic certificate $W(k, l, 2p)$ from which arises a certificate $W(k, l, 2(l-1)p+1)$. In one table entry we use “ZZ” to denote that double zipping was used to gain a certificate $W(k, l, 4(l-1)p+1)$.

Table 1: *Van der Waerden numbers W(k,l)–some exact and some lower bounds. New lower bounds are shown as 2-line entries with the acting prime in parentheses, “Z” indicating a single zipping was applied, and “ZZ” indicating a double zipping was applied.*

| $l \backslash k$ | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| 3 | 9 | 27 | 76 | >170 | >223 |
| 4 | 35 | >292 | >1048 | >2254 | >9778 |
| 5 | 178 | >2173 | >17705 | >98740 | >98740 |
| 6 | 1132 | >11191 | >91331 | >540025 | >816981 |
| 7 | >3703 | >48811 | >420217 | >1381687<br>(230281) | 7465909<br>(622159)Z |
| 8 | >11495 | >238400 | >2388317<br>(85297)ZZ | >10743258<br>(1534751) | >57445718<br>(8206531) |
| 9 | >41265 | >932745<br>(116593) | >10898729<br>(1362341)Z | >79706009<br>(9963251) | >159986609<br>(9999163)Z |
| 10 | >103474<br>(11497) | >4173724<br>(463747) | >760492218<br>(8449913) | >89999920<br>(9999991) | >179998975<br>(9999943)Z |
| 11 | >193941*<br>(9697)Z | >18603731<br>(1860373) | >198841541<br>(9942077)Z | >99999711<br>(9999971) | >199998621<br>(9999931)Z |
| 12 | >638727<br>(29033)Z | >79134144<br>(7194013) | >219988319<br>(9999469)Z | >109999242<br>(9999931) | >219996107<br>(9999823)Z |

Some of the entries in Table 1 deserve comments:

- Because our procedure went only through the primes less than 10,000,000, table entries associated with primes in the vicinity of 10,000,000 are very likely improvable by more extensive search.

- That our bound for $W(4, 12)$ exceeds that shown for $W(5, 12)$ is essentially a product of our limiting the search to primes less than 10,000,000. In our attempt to find a bound for $W(5, 12)$, for example, we searched only prime profiles for $k = 5$, not considering those for $k = 4$. Had our search gone far enough beyond the 10,0000,000 limit, we conjecture that a larger prime would have yielded a bound for $W(5, 12)$ that is larger than the bound given here for $W(4, 12)$. Rather than replicate the bound for $W(4, 12)$ as a bound also for $W(5, 12)$, which it clearly is, we preferred to show the prime and zipping results directly. The same comment applies to some entries for $l = 11$ as well.

- The asterisk (*) on the entry for $W(2, 11)$ highlights a new value that corrects an error in [14] where a bound for $W(2, 11)$was misreported. This error was discovered during our recent computations.

- There is only one double zipping reported in this table. That is not because no other double zippings would work, but rather that computional power needed to fully check double-zipped colorings is formidable. We have not found a shortcut for verifying that a $k$-coloring resulting from a double zipping is $l$-progression free.

# References

[1] T. Ahmed, Some new van der Waerden numbers and some van der Waerden-type numbers, *Integers* **9**, pp. 65-70, 2009.

[2] M. Beeler and P. O'Neil, Some new van der Waerden numbers, *Discrete Mathematics* **28**, pp. 135-146, 1979.

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

[4] V. Chvtal, Some unknown van der Waerden numbers, *Combinatorial Structures and Their Applications*, R. K. Guy et al. (editors), Gordon and Breach, pp. 31-33, 1970.

[5] M, R. Dransfield, L. Liu, V. W. Marek and M. Truszczynski, Satisfiability and computing van der Waerden numbers, *The Electronic Journal of Combinatorics* **11** (1) R41, pp. 1-15, 2004.

[6] T. Gowers, A new proof of Szemerdi's theorem, *Geometric and Functional Analysis* **11**, pp. 465-588, 2001.

[7] M. J. H. Heule, Improving the odds: New lower bounds for van der Waerden numbers, *http://www.st.ewi.tudelft.nl/sat/slides/waerden.pdf,* 2009.

[8] M. J. H. Heule, Van der Waerden numbers, *http://www.st.ewi.tudelft.nl/sat/waerden.php*, 2011.

[9] M. J. H. Heule and T. Walsh, Symmetry within solutions, *Proc. of the Twenty-Fourth AAAI Conference on Artificial Intelligence (AAAI '10)*, pp. 77-82, AAAI Press., 2010.

[10] P. R. Herwig, M. J. H. Heule, P. M. van Lambalgen, and H. van Maaren, A method to construct lower bounds for van der Waerden numbers, *The Electronic Journal of Combinatorics* **14** R6, pp. 1-15, 2007.

[11] M. Kouril and J. L. Paul, The van der Waerden number W(2,6) is 1132, *Experimental Mathematics* **17**, pp. 53–61, 2008.

[12] M. Kouril and J. Franco, Resolution tunnels for improved SAT solver performance, *Proc. of 8th International Conference on Theory and Applications of Satisfiability Testing,* pp. 143-157, 2005.

[13] L. Moser, On a theorem of van der Waerden, *Canad. Math. Bull.* **3**, pp. 23-25, 1960.

[14] J. R. Rabung, Some progression-free partitions constructed using Folkman's method, *Canad. Math. Bull.* **22** (1), pp. 87-91, 1979.

[15] S. Shelah, Primitive recursive bounds for van der Waerden numbers, *J. Amer. Math. Soc.* **1**, pp. 683-697, 1988.

[16] R. S. Stevens and R. Shantaram, Computer-generated van der Waerden partitions, *Math. Comp.* **32** (142), pp. 635-636, 1978.

[17] B. L. van der Waerden, Beweis einer Baudet'schen Vermutung, *Nieuw Archief voor Wiskunde* **15**, pp. 212-216, 1927.