Lower bounds on some van der Waerden numbers based on quadratic residues

Meilian Liang
School of Mathematics and Information Science,
Guangxi University, Nanning 530004, China

Xiaodong Xu
Guangxi Academy of Sciences,
Nanning 530007, China

Zehui Shao*
Key Laboratory of Pattern Recognition and
Intelligent Information Processing,
School of Information Science & Technology,
Chengdu University, Chengdu 610106, China
kidszh_mail@163.com

Baoxin Xiu
College of Information System and Management,
National University of Defense Technology,
Changsha 410073, China

Abstract. The van der Waerden number $W(r,k)$ is the least integer N such that every r-coloring of $\{1,2,\cdots,N\}$ contains a monochromatic arithmetic progression of length at least k. Rabung gave a method to obtain lower bounds on $W(2,k)$ based on quadratic residues, and performed computations on all primes no greater than 20117. By improving the efficiency of the algorithm of Rabung, we perform the computation for all primes up to 6×10^7, and obtain lower bounds on $W(2,k)$ for k between 11 and 23.

*Corresponding author

1 Introduction

The van der Waerden number $W(r,k)$ is the least integer N such that every r-coloring of $\{1,2,\cdots,N\}$ contains a monochromatic arithmetic progression of length at least k. Van der Waerden's theorem states that $W(r,k)$ exists for any positive integers r and k.

We only consider lower bounds on $W(2,k)$ for k no greater than 25 in this paper.

In [1], Berlekamp proved that for any prime p, $W(2,p+1) > p \cdot 2^p$. On the other hand, in [2], T. Gowers proved the general upper bound that

$$W(r,k) \leq 2^{2^{r^{2^{2^{k+9}}}}}.$$

Rabung [3] followed Berlekamp's observation by constructing r-coloring using power residues and thereby gave some improved lower bounds on particular $W(r,k)$. He obtained lower bounds on some small van der Waerden numbers $W(2,k)$, by computing all primes no greater than 20117. The known values and the best known lower bounds on some van der Waerden numbers $W(2,k)$ are listed in Table 1 with their references. Rabung also obtained that $W(2,10) > 103474$, $W(2,11) > 196811$ and $W(2,12) > 220518$, among which his computation result for $W(2,11)$ was not correct.

Table 1: Known values and best known lower bounds on $W(2,k)$

k	3	4	5	6	7	8	9
$W(2,k)$	9	35	178	1,132	$> 3,703$	$> 11,495$	$> 41,265$
reference	[4]	[4]	[5]	[6]	[3]	[7]	[7]

Because that Rabung conducted his search only for primes no greater than 20117, he need not look for many new ideas to improve the efficiency of his algorithm. On the other hand, to obtain interesting lower bounds on $W(2,k)$ for k greater than 10, we need to do so.

By improving the efficiency of Rabung's method through avoiding unnecessary computation, we perform the computation for all primes up to 6×10^7, much larger than 20117 that Rabung reached. We also perform the computation for some primes between 6×10^7 and 5×10^8. Lower bounds on $W(2,k)$ are obtained in this paper for k between 11 and 23.

The rest of the paper is organized as follows. After the preliminaries in Section 2, a new method based on the one of Rabung is given in Section 3, based on which an efficient algorithm is designed in Section 4. Computation results are shown in Section 5.

2 The preliminaries

For a large prime p, we need compute quadratic residues through its primitive root. The following algorithm is the fastest algorithm to compute the least primitive root, which can be found in [8].

Algorithm 0 (Primitive Root). Given an odd prime p, this algorithm finds a primitive root modulo p.

1.[Initialize a] Set $a \leftarrow 1$ and let $p-1 = p_1^{v_1} p_2^{v_2} \cdots p_k^{v_k}$ be the complete factorization of $p-1$.

2.[Initialize check] Set $a \leftarrow a+1$ and $i \leftarrow 1$.

3.[Check p_i] Compute $e \leftarrow a^{(p-1)/p_i} (\mathrm{mod}\, p)$. If $e = 1$ go to step 2. Otherwise, set $i \leftarrow i+1$.

4.[finished?] If $i > k$ output a and terminate the algorithm, otherwise go to step 3.

To compute $a^{(p-1)/p_i} (\mathrm{mod}\, p)$ faster, in particular for a large prime p, repeated squaring algorithm (see [9]) is used in this paper.

3 New method based on that of Rabung

Denote $\{m, \ldots, n\}$ by $[m, n]$. Let Z be the set of integers. For any odd prime p, let $R(p)$ in $[1, p-1]$ be the set of all quadratic residues modulo p, and $NR(p)$ in $[1, p-1]$ be the set of all quadratic non-residues modulo p.

Let $f_0(p) = \min\{NR(p)\}$ be the smallest quadratic non-residues modulo p.

Let $f_1(p) = 2f_0(p) - 1$ for $p \equiv 1 (\mathrm{mod}\, 4)$, and $f_1(p) = f_0(p)$ for $p \equiv 3 (\mathrm{mod}\, 4)$.

Let $f_2(p)$ be the length of the longest arithmetic progression with common difference 1 in $R(p)$, and $f_3(p)$ be the length of the longest arithmetic progression with common difference 1 in $NR(p)$, respectively.

Let $f(p)$ be $\max\{f_i(p) \mid 1 \leq i \leq 3\}$. By the definition of $f(p)$, it is not difficult to obtain the following lemma.

Lemma 3.1 *For any odd prime p, if all quadratic non-residues in Z_p are in color blue, and other elements in Z_p are in color red, then the maximum length of any monochromatic arithmetic progression with common difference 1 in Z_p is $f(p)$.*

Proof. Suppose x is the maximum length of any monochromatic arithmetic progression with common difference 1 in Z_p, and $A_1 = \{a_i \mid 1 \leq i \leq x\}$ is a monochromatic arithmetic progression with common difference 1 in Z_p. Therefore $x \geq \max\{f_2(p), f_3(p)\}$ by their definitions. Note that $f_0(p) = \min\{NR(p)\}$ be the smallest quadratic non-residues modulo p. If $p \equiv 1(\bmod 4)$, then -1 is a quadratic residue modulo p, and $x \geq 2f_0(p) - 1$

because that $\{-(f_0(p)-1),\cdots,0,\cdots,f_0(p)-1\}$ is a red arithmetic progression with common difference 1, where both $f_0(p)$ and $-f_0(p)$ are quadratic non-residues and in color blue; if $p \equiv 3(\text{mod}\,4)$, then -1 is a quadratic non-residue modulo p, and $x \geq f_0(p)$ because that $\{0,\cdots,f_0(p)-1\}$ is a red arithmetic progression with common difference 1, where both $f_0(p)$ and -1 are quadratic non-residues and in color blue. So $x \geq f_1(p)$. Since $x \geq \max\{f_2(p), f_3(p)\}$, $x \geq f(p)$.

On the other hand, if $0 \notin A_1$, then $x = \max\{f_2(p), f_3(p)\}$; if $0 \in A_1$, then $x = f_1(p)$. So $x \leq f(p)$.

Therefore $x = f(p)$. □

Now we will prove the following theorem that Rabung used in [3], only for $W(2,k)$.

Theorem 3.1 *For any odd prime p, let $k = f(p)$, then*

$$W(2,k+1) > 1 + kp.$$

Proof. Let $A = [0,kp]$. For any $i \in A - \{jp \mid 0 \leq j \leq k, j \in Z\}$, we color i with color red if and only if i is a quadratic residue modulo p, and color i with color blue if and only if i is a quadratic non-residue modulo p. We color all integers in $\{jp \mid 0 \leq j < k, j \in Z\}$ with color red, and color kp with color blue.

Now we will prove that there is no monochromatic arithmetic progression of length $k+1$ in such a coloring of A. Suppose there is a monochromatic arithmetic progression $I = \{a_0 + di \mid 0 \leq i \leq k\}$ in such a coloring of A, with length $k+1$ and common difference d. It is not difficult to see that $d \leq p$. Moreover, d can not be p, because that $\{jp \mid 0 \leq j \leq k, j \in Z\}$ is the unique arithmetic progression of length $k+1$ in A, which is not monochromatic in the given coloring. Therefore $d \in [1, p-1]$.

Since $d \in [1,p-1]$ and p is a prime, there is $d' \in [1,p-1]$ such that $dd' \equiv 1(\text{mod}\,p)$. Let $I' = \{(d'i) \bmod p \mid i \in I\}$. Since I is an arithmetic progression with length $k+1$, I' is an arithmetic progression with length $k+1$ and common difference 1 in Z_p. By Lemma 3.1, the maximum length of any monochromatic arithmetic progression with common difference 1 in Z_p is $f(p)$. This contradicts with that I' is an arithmetic progression with length $k+1$ in Z_p.

Thus $W(2,k+1) > 1 + kp$. □

Let $h_2(p)$ be the length of the longest arithmetic progression with common difference 1 in $R(p)\bigcap[1,(p-1)/2+100]$, and $h_3(p)$ be the length of the longest arithmetic progression with common difference 1 in $NR(p)\bigcap[1,(p-1)/2+100]$. Let $h(p) = \max\{f_1(p), h_2(p), h_3(p)\}$. We can see that $h(p) \leq f(p)$. It is easier to compute $h(p)$ than $f(p)$.

Theorem 3.2 *Suppose p is a prime no less than 200. If $p \equiv 1 (\mathrm{mod}\, 4)$ and $f(p) \leq 100$, then $h(p) = f(p)$; if $p \equiv 3(\mathrm{mod}\, 4)$, then $h(p) = f(p)$.*

Proof. (i) For $p \equiv 1(\mathrm{mod} 4)$, -1 is a quadratic residue modulo p. If $h_2(p) < f_2(p)$, then there is an arithmetic progression $\{a_i \in R(p) | i = 1, \cdots, f_2(p)\}$ of length $f_2(p)$ with common difference 1, among which the greatest number is greater than $(p-1)/2 + 100$, and the least one smaller than $(p-1)/2$. Thus $f_2(p) > 100$. Similarly, if $h_3(p) < f_3(p)$, then $f_3(p) > 100$. Because that $f(p) \leq 100$, both $f_2(p) \leq 100$ and $f_3(p) \leq 100$ hold. Thus $h_2(p) = f_2(p)$ and $h_3(p) = f_3(p)$. So $h(p) = f(p)$.

(ii) If $p \equiv 3(\mathrm{mod} 4)$, then -1 is a quadratic non-residue modulo p. Since $(p-1)/2 \equiv -(p+1)/2(\mathrm{mod} p)$, one among $\{(p-1)/2, (p+1)/2\}$ is a quadratic residue and the other is a quadratic non-residue modulo p. Therefore the longest arithmetic progression with common difference 1 in $R(p)$ is either in $[1, (p-1)/2]$ or in $[(p+1)/2, p-1]$. So is the longest one in $NR(p)$.

If $\{a_i \in R(p) \cap [(p+1)/2, p-1] | i = 1, \cdots, f_2(p)\}$ is an arithmetic progression of length $f_2(p)$ with common difference 1, then $\{p - a_i \in NR(p) \cap [1, (p-1)/2] | i = 1, \cdots, f_2(p)\}$ is too. So $f_2(p) \leq h_3(p)$. We can prove $f_3(p) \leq h_2(p)$ similarly. So $h(p) = f(p)$ for $p \equiv 3(\mathrm{mod}\, 4)$. □

4 The algorithm

Algorithm 1 shows an implementation of the computation of pairs $(p, h(p))$ ($h(p)$ is defined in Section 3) for primes $p \equiv 1(\mathrm{mod}\, 4)$ in a given computational range. It should be pointed out that for two primes p_1 and p_2, if $p_1 > p_2$ and $h(p_1) \leq h(p_2)$, we need not use the pair $(p_2, h(p_2))$ to obtain a lower bound for $W(2, k)$. Therefore, the computation starts from the maximum prime in the range, and a variable *bkn* acting as a reference value is initialized before the computation (line 2 of Algorithm 1) by a file on the disk, in which previously obtained pairs $(p, h(p))$ are saved.

For a prime p, we need a primitive root modulo p to compute quadratic non-residues modulo p efficiently. After the primitive root is obtained, the set of quadratic non-residues is computed. By Theorem 3.2, only quadratic non-residues no greater than $(p-1)/2 + 100$ are saved to an array E (line 6). Then numbers in E are sorted into ascending order, with the smallest one being e_1.

Finally $h(p)$ is computed. Lines 10 to 26 demonstrate the computation of $h_2(p)$ and $h_3(p)$, for which traversing once E is sufficient. For consecutive elements e_i and e_{i+1} in E, let $d = e_{i+1} - e_i$. If $d = 1$, then it implies that e_i and e_{i+1} are part of an arithmetic progression with common difference 1 in $NR(p)$; otherwise, there exists an arithmetic progression with common

Algorithm 1 AlgoBoundsM4R1

Require:

The lower bound *lb* and upper bound *ub* of the computing range.

```
n ← max{s|s ≤ ub, s ≡ 1(mod 4)};
Initialize bkn according to known pairs (p, h(p)) and n;
for p ← n; p ≥ lb; p ← p − 4 do
  if p is a prime then
    g ← PrimitiveRoot(p);
    E ← SmallNR(p, g, (p − 1)/2 + 100);
    Sort the numbers in E into ascending order;
    max ← 2 × e_1;
    if max ≤ bkn then
      h_3 ← 2;
      for i ← 1 to |E| − 1 do
        h_2 ← e_{i+1} − e_i;
        if h_2 = 1 then
          h_3 ← h_3 + 1;
        else
          for each j ∈ [2, 3] do
            if h_j > max then
              if h_j > bkn then
                break out of the middle loop;
              end if
              max ← h_j;
            end if
          end for
          h_3 ← 2;
        end if
      end for
    end if
    hp ← max − 1;
    if hp < bkn then
      bkn ← hp;
      Print p, g, hp;
    end if
  end if
end for
```

Table 2: The values of $f(p)$ for some primes

the prime	the root	the length
198749009	3	22
98311009	19	21
55034921	3	20
27700919	7	19
13919273	3	18
5357603	2	17
2899861	2	16
1091339	2	15
608789	2	14
239873	3	13
136859	2	12
58013	2	11
17863	6	10

difference 1 of length $d-1$ in $R(p)$. Additionally, note that the traversal procedure will stop when $h_j > bkn$ (line 18), avoiding unnecessary computation, where h_j stores the maximum length of the arithmetic progressions processed.

We transform Algorithm 1 to the form suitable for primes $p \equiv 3 (\bmod\ 4)$ without difficulty, and use it together with Algorithm 1 to compute $f(p)$ for all primes in a given range.

5 Computation

By computing $f(p)$ for all primes between 10^4 and 6×10^7, and some primes between 6×10^7 and 5×10^8, we obtain the results in Table 2, by which we obtain lower bounds on some van der Waerden numbers, as shown in Theorem 5.1.

Theorem 5.1 $W(2,11) \geq 178632$, $W(2,12) \geq 638145$, $W(2,13) \geq 1642310$, $W(2,14) \geq 3118351$, $W(2,15) \geq 8523048$, $W(2,16) \geq 16370087$, $W(2,17) \geq 46397778$, $W(2,18) \geq 91079253$, $W(2,19) \geq 250546916$, $W(2,20) \geq 526317463$, $W(2,21) \geq 1100698422$, $W(2,22) \geq 2064531191$, $W(2,23) \geq 4372478200$.

We also obtain that $f(280014869) = 23$ and $f(470017417) = 24$, based on which the lower bounds on van der Waerden numbers obtained seem not good.

Note that Rebung gave a mistaken result $W(2,11) > 196811$ for $p = 19681$. We obtain $f(19681) = 21$. Now we only show that the minimum quadratic non-residue of 19681 is at least 11. All we need is to show that 2,3,5,7 are all quadratic residue of 19681. By computation we obtain that $1954^2 \equiv 2(\mathrm{mod}\, 19681)$, $1239^2 \equiv 3(\mathrm{mod}\, 19681)$, $3634^2 \equiv 5(\mathrm{mod}\, 19681)$, and $4815^2 \equiv 7(\mathrm{mod}\, 19681)$.

Some interesting open problems can be found in some references such as [10] and [11]. We may ask the following question based on the lower bounds obtained in this paper, which seems not easy to answer.

Question: Is $W(2, k+1) > 2W(2, k)$ true for any integer $k > 7$?

Acknowledgment

The authors wish to thank an anonymous referee for his or her helpful suggestions leading to the present form of this paper. This work is partially supported by the Guangxi Natural Science Foundation (2011GXNSFA018142, 0991027), the Scientific Research Foundation of GuangXi University (X081059), Science and Technology Project of Chengdu (10RKYB041ZF-023), Sichuan Youth Science & Technology Foundation (2010JQ0032).

References

[1] E.A. Berlekamp, Constructions for partitions which avoid long arithmetic progressions, Canad. Math. Bull 11 (1968) 409-414.

[2] T. Gowers, A new proof of Szemerédi's theorem, Geometric and Functional Analysis 11(2) (2001) 465-588.

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

[4] V. Chvátal, Some unknown van der Waerden numbers, Combinatorial Structures and Their Applications (R.Guy et al., eds.), Gordon and Breach, New York, 1970.

[5] R. Stevens, R. Shantaram, Computer-generated van der Waerden partitions, Mathematics of Computation 32 (142) (1978) 635-636.

[6] M. Kouril, J.L.Paul, The Van der Waerden Number W(2,6) is 1132, Experimental Mathematics, 17(1) (2008) 53-61.

[7] M. Heule, Improving the odds- New lower bounds for van der Waerden numbers, (2010),

`http://www.st.ewi.tudelft.nl/sat/slides/waerden.pdf`

[8] H. Cohen, A course in computational number theory, third edition, Springer-Verlag, 1996.

[9] T. H. Cormen, C. E. Leiserson, R. L. Rivest, Introduction to Algorithms, The MIT Press, 1990.

[10] P. Erdős and R. L. Graham, Old and New Problems and Results in Combinatorial Number Theory, L'Enseignement Mathématique, Geneva, 1980.

[11] B. Landman and A. Robertson, Ramsey Theory on the Integers, AMS Publications, 2004.