Canad. Math. Bull. Vol. 22 (1), 1979

SOME PROGRESSION-FREE PARTITIONS CONSTRUCTED USING FOLKMAN'S METHOD

BY
JOHN R. RABUNG*

Almost from the day that B. L. van der Waerden [10] proved his now famous theorem on arithmetic progressions, mathematicians have been working to find a new or an improved constructive proof of that result, but without much success. The theorem, which asserts the existence of an integer $N(k, l)$ such that every k-coloring of the integers $\{1, 2, \ldots, N(k, l)\}$ yields a monochromatic l-progression, may have far-reaching applications (see [3] or [7] for discussions of some of these) if $W(k, l)$, the least $N(k, l)$, can be determined. It is generally felt that the $N(k, l)$ constructed in van der Waerden's proof is very far from being $W(k, l)$. Consequently, much effort has been devoted to finding upper and lower bounds for $W(k, l)$. (See, for example, [1], [5], [6], [8])

Here we shall concentrate on finding lower bounds for some particular $W(k, l)$. This naturally involves constructing k-colorings of long segments of consecutive integers which avoid monochromatic l-progressions. The best general constructions to date are those given by Berlekamp [1] and Moser [6]. Moser shows

$$W(k, l) > (l-1)k^{c \log k}, \; c \text{ a fixed constant,} \tag{1}$$

while Berlekamp displays the bound

$$W(k, l) > \min_{\delta \in \Delta} \{(l-1)(k^{l-1}-1)/\delta\} \tag{2}$$

where Δ is the set of all positive integers of the form $k^d - 1$ with d a proper divisor of $l-1$ or of the form D where D is any divisor of $k^{l-1}-1$ such that $D < l-1$. Inequality (1) gives the better bound for large k and small l while (2) is superior when l is large and k is small. It should be noted that the bound

$$W(k, l) > k^{l-1}/4l$$

which improves on (2) in many cases can be obtained as a consequence of a local theorem of Lovász which may be found in [4] or [9]. However, Berlekamp's method is still superior in the case where $l-1$ is prime and $k=2$ in which he finds

$$W(2, l) > (l-1)2^{l-1}. \tag{3}$$

Received by the editors November 7, 1977 and, in revised form, April 19, 1978.
* Research supported by the Virginia Commonwealth University Faculty Grants-In-Aid Program.

Nonetheless he expresses disappointment that in the case $l=4$ the construction which gives (3) is inferior to a construction by J. Folkman which yields a 2-coloring of the integer segment $[0,33]$ free of monochromatic 4-progressions. Folkman's construction, based on quadratic residues modulo 11, thus shows $W(2,4)>34$. Since it is now known that $W(2,4)=35$ (see [2]), Folkman's bound is best possible. Berlekamp notes that similar constructions of l-progression-free 2-colorings using quadratic residues are possible, but that no general means for determining the required modulus for given l is known. In this paper we follow Berlekamp's observation by constructing k-colorings using power residues and thereby give some improved lower bounds for particular $W(k,l)$, but we still cannot make the desired general constructions.

Let k and l be positive integers and suppose p is a prime of the form $kt+1$ with $p>l$. We take ζ to be a primitive k^{th} root of unity and let G_k denote the group of k^{th} roots of unity. If $N_p=\{n\in\mathbb{Z}:(n,p)=1\}$, then $\nu(n)$ for $n\varepsilon N_p$ will represent the index of n modulo p relative to some fixed primitive root. Also, an l-progression with common difference one will be called an l-string.

Define: $\mathscr{X}:N_p\to G_k$ such that $\mathscr{X}(n)=\zeta^{\nu(n)}$. We see that the effect of $\mathscr{X}$ is to partition N_p into k classes, and note that $\mathscr{X}(nm)=\mathscr{X}(n)\mathscr{X}(m)$. Also observe that $\mathscr{X}$ has period p so that viewing $\mathscr{X}$ modulo p we have a character defined on the reduced residue system modulo p. At times we shall use the character properties of $\mathscr{X}$ in what follows.

THEOREM. *Let $\mathscr{X}':[0,(l-1)p]\to G_k$ such that $\mathscr{X}'(n)=\mathscr{X}(n)$ if $(n,p)=1$ and such that $\mathscr{X}'$ is not constant on $\{0,p,2p,\ldots,(l-1)p\}$. Then the k-partition imposed by $\mathscr{X}'$ on $[0,(l-1)p]$ is free of single-class l-progressions if and only if the following hold*:

(a) *no single-class l-string occurs in $[1,p-1]$; and*

(b) *if $\mathscr{X}(-1)=1$, the integers $1,2,\ldots,[(l-1)/2]$ are not in the same class; while if $\mathscr{X}(-1)=-1$ the integers $1,2,\ldots,(l-1)$ are not in the same class.*

Proof. If condition (a) does not hold, clearly the partition is not free of single-class l-progressions. Suppose condition (b) does not hold, and say $\mathscr{X}'(0)=\zeta^c$. If $\mathscr{X}(-1)=1$, we multiply the elements of $\{-[(l-1)/2],\ldots,-2,-1,0,1,2,\ldots,[(l-1)/2]\}$ by m, the least positive integer such that $\mathscr{X}(m)=\zeta^c$. (Note $m<p$.) This results in an l-progression contained in class ζ^c. Because of the periodicity of $\mathscr{X}$, we must have under these circumstances a single-class l-progression involving any multiple of p in $[p,(l-2)p]$. A similar argument applies when $\mathscr{X}(-1)=-1$.

Conversely, suppose $a, a+d,\ldots,a+(l-1)d$ is a single-class l-progression under the partition imposed by $\mathscr{X}'$. First, if $(d,p)=1$ and no multiple of p is involved in the progression, then ad^{-1}, $ad^{-1}+1,\ldots,ad^{-1}+(l-1)$ where

https://doi.org/10.4153/CMB-1979-012-1 Published online by Cambridge University Press

$dd^{-1} \equiv 1 \pmod p$ is a single-class l-string under $\mathscr{X}$ and, by periodicity, there exists a single-class l-string in $[0, (l-1)p]$ which contradicts condition (a).

Now suppose $(d, p) = 1$ and a multiple of p is contained in the given l-progression. Then we may assume that either this multiple lies in the middle or at one of the ends of this progression according as $\mathscr{X}(-1) = 1$ or $\mathscr{X}(-1) = -1$, respectively. Then multiplication by d^{-1} as before shows that condition (2) cannot hold.

Finally if $(d, p) \neq 1$, then the progression in question must be $0, p, \ldots, (l-1)p$ since this is the only such l-progression contained in $[0, (l-1)p]$. But this violates the condition that $\mathscr{X}'$ is not constant on the multiples of p. Q.E.D.

Thus a search for a prime p whose k^{th} power character yields a lower bound for $W(k, l)$ involves only observing that conditions (a) and (b) are met. If so, $W(k, l) > (l-1)p + 1$. We have conducted such a search for all primes up to 20,117. Obtaining primitive roots from [11] and [12] and using an IBM 370/145 we searched the classes imposed by k^{th}-power characters ($k = 2, 3, 4, 5, 6$) of these primes to produce a table listing lengths of longest single-class strings as well as lengths of longest single-class strings containing the number 1 and the class of -1 modulo p. Then a scan of the table gave us the following results which easily exceed the corresponding bounds given by Berlekamp, except in the case $W(2, 3)$.

l \ k	2	3	4	5	6
3	7 (3)		75 (37)		207 (103)
4	34 (11)	292 (97)	1048 (349)	2,254 (751)	9,778 (3,259)
5	149 (37)	965 (241)	10,437 (2,609)	24,045 (6,011)	52,637 (13,159)
6	696 (139)	8,886 (1,777)	90,306* (18,061)	93,456* (18,691)	100,566* (20,113)
7	3703 (617)	43,855 (7,309)	119,839 (19,973)	120,307* (20,051)	
8	7484 (1069)	132,812* (18,973)			
9	27,113 (3,389)	160,857* (20,107)			
10	103,474 (11,497)				
11	196,811* (19,681)				
12	220,518* (20,047)				

Lower bounds for particular $W(k, l)$. Numbers in parentheses show primes used to achieve the bounds shown. Asterisks (*) indicate bounds which are felt to be improvable through further computer searching.

It is interesting to note that the l-progression-free k-partitions constructed in this way are laden with single-class $(l-1)$-progressions. Suppose for some k and l we have p and $\mathscr{X}'$ satisfying the conditions of the theorem. We view $\mathscr{X}$ as a character modulo p and call $a, a+d, \ldots, a+(l-1)d$, where operations are taken modulo p, an l-progression $(\bmod p)$. Then if there are s single-class $(l-1)$-strings in the reduced residue system modulo p, it can be shown that:

(a) Every element in the reduced residue system belongs to exactly $\left\lceil \frac{s}{2} \right\rceil \times (l-1)$ single-class $(l-1)$-progressions $(\bmod p)$. (Here $\lceil a \rceil$ denotes the smallest integer greater than a.)

(b) There are exactly $\left\lceil \frac{s}{2} \right\rceil (p-1)$ distinct single-class $(l-1)$-progressions $(\bmod p)$ contained in the reduced residue system modulo p.

In the language of combinatorics, the elements of the reduced residue system modulo p and the single-class $(l-1)$-progressions $(\bmod p)$ form a $1-\left(p-1, l-1, \left\lceil \frac{s}{2} \right\rceil (l-1)\right)$ design.

Also, we point out that the bounds given here for $W(k, l)$ are not generally best possible. Using the computer we have found a 2-partition of $[1, 176]$ which is 5-progression-free. Although this partition does not arise from the method of this paper, it does display quite similar multiplicative properties and suggests generalization of the method.

ACKNOWLEDGMENT. The author wishes to thank the referee and Professor Joel Spencer for providing information concerning the theorem of Lovász cited in this paper.

REFERENCES

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

2. V. Chvátal, *Some unknown van der Waerden numbers, Combinatorial Structures and Their Applications*, R. K. Guy et al. (editors) Gordon and Breach, 1970, 31–33.

3. P. Erdös, *Some recent advances and current problems in number theory*, Lectures on Modern Mathematics, Vol. **3**, T. L. Saaty (editor), Wiley, New York, 1965, 196–244.

4. P. Erdös and L. Lovász, *Problems and results on 3-chromatic hypergraphs and some related questions*, Infinite and finite sets, Colloqu. Math. Soc. Janos Bolyai lo, Hajnol, Rado, and Sos (eds), North Holland, Amsterdam, 1975, 609–627.

5. P. Erdös and R. Rado, *Combinatorial theorems on classifications of subsets of a given set*, Proc. London Math. Soc., **2** (1952), 417–439.

6. L. Moser, *On a theorem of van der Waerden*, Canad. Math. Bull. **3** (1960), 23–25.

7. J. R. Rabung, *On applications of van der Waerden's theorem*, Math. Mag. **48** (1975), 142–148.

8. W. M. Schmidt, *Two combinatorial theorems on arithemtic progressions*, Duke Math. J. **29** (1962), 129–140.

9. Joel Spencer, *Ramsey's Theorem — a new lower bound*, J. Combinatorial Theory **18** (1975), 108–115.

10. B. L. van der Waerden, *Beweis einer Baudet'schen Vermutung*, Nieuw Arch. Wisk., **15** (1927) 212–216.

11. E. Vegh, H. Hauptman, and J. Fisher, *Tables of all Primitive Roots for Primes Less than 5000*, Mathematics Research Center Report **70-5,** Naval Research Laboratory, Washington, D.C. 1970.

12. A. E. Western and J. C. P. Miller, *Tables of Indices and Primitive Roots*, Royal Society Mathematical Tables, Vol. **9,** 1968, (University Press Cambridge).

DEPARTMENT OF MATHEMATICAL SCIENCES
VIRGINIA COMMONWEALTH UNIVERSITY
901 WEST FRANKLIN STREET
RICHMOND, VIRGINIA 23284

https://doi.org/10.4153/CMB-1979-012-1 Published online by Cambridge University Press