Article Author: Berlekamp

Article Title: A construction for partitions which avoid long arithmetic progressions
A CONSTRUCTION FOR PARTITIONS WHICH AVOID LONG ARITHMETIC PROGRESSIONS

E. R. Berlekamp

(received January 2, 1968)

For \( k \geq 2, \ t \geq 2 \), let \( W(k, t) \) denote the least integer \( m \) such that in every partition of \( m \) consecutive integers into \( k \) sets, at least one set contains an arithmetic progression of \( t+1 \) terms. This paper presents a construction which improves the best previously known lower bounds on \( W(k, t) \) for small \( k \) and large \( t \).

1. Introduction. For \( k \geq 2, \ t \geq 2 \), let \( W(k, t) \) denote the least integer \( m \) such that in every partition of \( m \) consecutive integers into \( k \) sets, at least one set contains an arithmetic progression of \( t+1 \) terms. According to a well-known theorem of van der Waerden (1925), \( W(k, t) \leq \infty \). It is obvious that

\[
W(k, t) \leq W(k, t+1) \tag{1}
\]

Using random coding arguments, Erdős and Rado (1952) have shown that

\[
W(k, t) \geq [2t \cdot k^t]^{1/2} \tag{2}
\]

By a more refined nonconstructive argument, Schmidt (1962) has shown that

\[
W(k, t) \geq k^{(t+1)} - c[(t+1)\log(t+1)]^{1/2} \tag{3}
\]

where \( c \) is an absolute constant. The major result of this paper is

**THEOREM 1.** If \( k \) is a prime-power, and if \( \tilde{w} \) is an integer such that

\[
\tilde{w} \leq t(k^t-1)/k^{d-1} \tag{4}
\]

for all \( d \) which are proper divisors of \( t \), and if

\[
\tilde{w} \leq t(k^t-1)/D \tag{5}
\]

for all \( D < t \) which are divisors of \( k-1 \), then

\[
W(k, t) > \tilde{w} \tag{6}
\]

The proof consists of a construction, based on the Galois field
$GF(k^t)$, which partitions $W$ consecutive integers into $k$ sets, none
of which contains any arithmetic progression longer than $t$. In some
cases this construction can be extended by special arguments, to give

**THEOREM 2.** If $t$ is prime, $W(2, t) > t 2^t$.

The bound of Theorem 2 is stronger than equation (3). If $t$ is
the square of a prime or the product of two large primes whose
difference is small, then Theorem 1 again represents a slight
improvement over equation (3). However, for most values of $t$, the
bound of Theorem 1 can be improved by decreasing $t$ to the next
smaller prime and invoking equation (1). Although this technique
gives the best known bound for small $k$ and large $t$, the construction
of L. Moser (1960) still gives the best known bound for small $t$ and
large $k$, namely,

$$W(k, t) > t k^c \log k$$  \hspace{1cm} (7)

The bound of Theorem 2 is also disappointing for small values
of $t$. Theorem 2 shows only that $W(2, 3) > 24$, yet J. Folkman (1967)
has shown that $W(2, 3) > 34$ by the following construction: For
$i = 0, 1, 2, \ldots, 33$, let $i \in S_0$ if $i = 0, 11$, or a quadratic nonresidue
mod 11. It is believed that Folkman's partition is the best possible,
and that $W(2, 3) = 35$. Similar constructions using quadratic
residues modulo certain larger primes may be used to obtain other
lower bounds on $W(2, t)$, but the general form of these bounds is
unknown for large values of $t$.

2. **Proof of Theorem 1.** Let $a$ be a primitive element in
$GF(k^t)$. Then every nonzero element in $GF(k^t)$ is a power of $a$, and
$a^i = a^j$ if and only if $i \equiv j \mod k^t - 1$. Let $\beta_1, \beta_2, \ldots, \beta_t$ be a set of
elements in $GF(k^t)$ which are linearly independent over $GF(k)$. Since
these elements form a basis of $GF(k^t)$ over $GF(k)$, there exist
elements $A_{i, j} \in GF(k)$ such that

$$a^j = \sum_{i=1}^{t} A_{i, j} \beta_i$$

The field element $a^j$ is the root of some irreducible monic
polynomial, $f(j)(x) = \sum_{n=0}^{t} f_n x^n$, where $f_n \in GF(k)$. The degree of
$f(j)(x)$ is a divisor of $t$.  

410
For each $\xi \in GF(k)$, we define the set of integers $S_{\xi}$ by the rule
\[ i \in S_{\xi} \text{ if and only if } 0 \leq i < \tilde{W} \text{ and } A_{1,i} = \xi. \]
Similarly, for each $\xi \in GF(k)$, we define the set of nonzero field elements, $T_{\xi}$, by the rule $\alpha^i \in T_{\xi}$ for each $i \in S_{\xi}$.

We now claim that no $S_{\xi}$ contains any arithmetic progression of length $> t$. Let us suppose that for some $b \neq 0$,
\[(8) \quad \{a, a+b, a+2b, \ldots, a+tb\} \subset S_{\xi}.\]

Since $0 \leq a < a+tb < \tilde{W}$, we have
\[(9) \quad b < (k^t-1)/(k^d-1)\]
and
\[(10) \quad b < (k^t-1)/D\]
from equations (4) and (5). We now consider separately the cases $\xi \neq 0$ and $\xi = 0$.

**Case 1:** $\xi \neq 0$. Since $x_1(b) (\alpha^b) = 0$, we have $0 = \sum_{n=0}^{t} f_n(b) a+bn = \sum_{n=0}^{t} f_n(b) \sum_{j=1}^{t} A_j, a+bn \beta_j$. Since $\beta_1, \beta_2, \ldots, \beta_t$ are linearly independent, this implies that for every $j$,
\[(11) \quad \sum_{n=0}^{t} f_n(b) A_j, a+bn = 0.\]

In particular, since $A_1, a+bn = \xi$ for $n = 0, 1, \ldots, t$, we may set $j = 1$ in equation (11) and obtain $\xi \sum_{n=0}^{t} f_n(b) = 0$. If $\xi \neq 0$, this implies that $0 = \sum_{n=0}^{t} f_n(b) = f_n(b)(1)$. Therefore, $f_n(b)(x)$ is divisible by $x-1$.

Since $f_n(b)(x)$ is irreducible, $f_n(b)(x) = x-1$, $a = 1$, and $b \equiv 0 \mod k^t-1$, contradicting both equations (9) and (10).
Case 2: $\xi = 0$. A weakened form of equation (8) is

\[(a+b, a+2b, \ldots, a+tb) \subset S_0.\]

By definition of $T_0$, equation (12) implies that $T_0$ contains the elements $a+b, a+2b, \ldots, a+tb$. We claim that these elements are distinct, for if $a+nb = a+mb$, then $(n-m)b \equiv 0 \mod k-1$, contradicting equation (10). Since $T_0$ is a subspace of dimension $t-1$ over $GF(k)$, any $t$ distinct elements in $T_0$ must be linearly dependent. Therefore, there exist $B_1, B_2, \ldots, B_t \in GF(k)$ such that

\[\sum B_a a^n = 0.\]

This implies that $\alpha^b$ is a root of the polynomial

\[\sum_{n=1}^{t} B_a x^{n-1}.\]

Since the degree of this polynomial is less than $t$, $\alpha^b \in GF(k^d)$, where $d$ is a proper divisor of $t$. Thus, $(\alpha^b)^{(k^d-1)} = 1$, so $b(k^d-1) \equiv 0 \mod k-1$, contradicting equation (9). We conclude that equation (12) is possible only if $b$ is larger than the bounds of equation (9) or equation (10).

Proof of Theorem 2. If $p$ and $t$ are odd primes, then Fermat's theorem shows that $2^{(p-1)} \equiv 1 \mod p$ so $2^t \not\equiv 1 \mod p$ unless $p \equiv 1 \mod t$. In other words, if $D$ is any divisor of $2^t-1$, then $D \geq t+1$, so Theorem 1 asserts that $W(2,t) > \tilde{W}$, where $\tilde{W} = t(2^t-1)$. We shall now show that the construction of Theorem 1 can be extended to include additional consecutive integers.

The construction of Theorem 1 is valid for any choice of $\beta$'s, so we may now choose these basis elements as follows:

\[(13) \quad \beta_1 = 1, \quad \beta_2 = 1+\alpha, \ldots, \beta_{(t+1)/2} = 1+\alpha^{(t-1)/2};\]

\[\beta_{(t+3)/2} = 1+\alpha^{-1}, \beta_{(t+5)/2} = 1+\alpha^{-2}, \ldots, \beta_t = 1+\alpha^{-(t-1)/2}.\]

If these $\beta$'s were linearly dependent, then $\alpha$ would be a root of a polynomial of degree $\leq t-1$, contradicting the assumption that $\alpha$ is a primitive element in $GF(2^t)$.

With the basis chosen by equation (13), the proof of Theorem 1 partitions \{0, 1, 2, \ldots, \tilde{W}-1\} into disjoint sets $S_0$ and $S_1$, with the property that
(14) \( \{0, 1, 2, \ldots, (t-1)/2\} \subseteq S_t \)

and

(15) \( \{\bar{W}-1, \bar{W}-2, \ldots, \bar{W}-(t-1)/2\} \subseteq S_1 \).

We set \( S_0^+ = S_0 \cup S_0^- \cup S_0^u \) where

\[ S_0^+ = \{-1, -2, \ldots, -(t-1)/2\} \]

\[ S_0^- = \{\bar{W}, \bar{W}+1, \ldots, \bar{W}+(t-1)/2\} \).

Any arithmetic progression of length \( t+1 \) in \( S_0^+ \) would have to be of one of the following types:

1) Including an element in \( S_0^+ \) and another element in \( S_0^- \). This is impossible because the difference between any two such numbers is not divisible by \( t \).

2) Including two or more elements in \( S_0^+ \) (or \( S_0^- \)). This is blocked by equation (14) (or equation (15)).

3) Including one element in \( S_0^+ \) (or \( S_0^- \)) and an arithmetic progression of length \( t \) is \( S_0^- \). According to the proof of Theorem 1, the only arithmetic progressions of length \( t \) in \( S_0^- \) are those in which \( b \geq 2^t - 1 \). The total span of the extension of such a progression would be \( \geq t(2^t - 1) \), contradicting equation (15) (or equation (14)).

Therefore, \( S_0^+ \) and \( S_1^- \) partition the integers from \(-(t-1)/2\) to \( W+(t-1)/2 \) into two sets, neither of which contains any arithmetic progression longer than \( t \). This partition can be translated to a partition of the integers from 0 to \( t2^t - 1 \) (or from 1 to \( t2^t \)) by adding \((t-1)/2\) (or \((t+1)/2\)) to each element in \( S_0^+ \) and \( S_1^- \).

The construction of Theorem 1 may also be extended slightly for other values of \( t \) and \( k \), but the improvement is always relatively small.

3. **Example.** Let \( k = 2, t = 3, \bar{W} = 24 \). Take \( \omega \) as a root of \( x^3 + x + 1; \beta_1 = 1, \beta_2 = 1 + \omega + \omega^3; \beta_3 = 1 + \omega^2 = \omega \). For \( i = 1, 2, 3 \):

\[ j = 0, 1, 2, \ldots, 24 \text{. \( A_{i,j} \) is given by} \]
\[ S_1 = \{ 0, 1, 1, 6, 7, 8, 11, 13, 14, 15, 18, 20 \}; \quad S_2 = \{ 2, 3, 3, 9, 10, 12, 16, 17, 19 \}; \quad S_0 = S_1 \cup \{-1, 21, 22\} . \]

REFERENCES


J. Folkman, private communication (1967).


Bell Telephone Laboratories Incorporated
Murray Hill, New Jersey