Arithmetic Progressions with Constant Weight

Raphael Yuster
Department of Mathematics
University of Haifa-ORANIM
Tivon 36006, Israel
e-mail: raphy@oranim.macam98.ac.il

Abstract

Let $k \le n$ be two positive integers, and let F be a field with characteristic p. A sequence $f : \{1, \ldots, n\} \to F$ is called k-constant, if the sum of the values of f is the same for every arithmetic progression of length k in $\{1, \ldots, n\}$. Let $V(n, k, F)$ be the vector space of all k-constant sequences. The constant sequence is, trivially, k-constant, and thus dim $V(n, k, F) \ge 1$. Let $m(k, F) = \min_{n=k}^{\infty} \dim\ V(n, k, F)$, and let $c(k, F)$ be the smallest value of n for which dim $V(n, k, F) = m(k, F)$. We compute $m(k, F)$ for all k and F and show that the value only depends on k and p and not on the actual field. In particular we show that if $p \not| k$ (in particular, if $p = 0$) then $m(k, F) = 1$ (namely, when n is large enough, only constant functions are k constant). Otherwise, if $k = p^r t$ where $r \ge 1$ is maximal, then $m(k, F) = k - t$. We also conjecture that $c(k, F) = (k-1)t + \phi(t)$, unless $p > t$ and p divides k, in which case $c(k, F) = (k-1)p + 1$ (in case $p \not| k$ we put $t = k$), where $\phi(t)$ is Euler's function. We prove this conjecture in case t is a multiple of at most two distinct prime powers. Thus, in particular, we get that whenever $k = q_1^{s_1} q_2^{s_2}$ where q_1, q_2 are distinct primes and $p \ne q_1, q_2$, then every k-constant sequence is constant *if and only if* $n \ge q_1^{2s_1} q_2^{2s_2} - q_1^{s_1-1} q_2^{s_2-1}(q_1 + q_2 - 1)$. Finally, we establish an interesting connection between the conjecture regarding $c(k, F)$ and a conjecture about the non-singularity of a certain $(0, 1)$-matrix over the integers.

1 Introduction

Consider any function $f : X \to G$ where X is an arbitrary set and G is an arbitrary abelian group. Given a family $\mathcal{F} \subset 2^X$ of subsets of X, we say that f is *uniform* on $\mathcal{F}$ if there exists $\alpha \in G$ such that for every $Y \in \mathcal{F}$ the sum (in G) of the values of f on the elements of Y is α. As a trivial example, one can take X to be any set, f being any constant function, and $\mathcal{F}$ being all the subsets of X with cardinality 7. Clearly, f is uniform on $\mathcal{F}$. When $G = F$ is a field, we can define $V(X, \mathcal{F}, F)$ to be the vector space of all uniform functions. (It is trivial to verify that V is, indeed, a vector space over F). V is called the *uniformity space* of $(X, \mathcal{F})$ over F. The dimension of V is called the *uniformity dimension* of $(X, \mathcal{F})$ over F. We can associate $V(X, \mathcal{F}, F)$ with a $(0,1)$-matrix H as follows. The columns of H are indexed by the elements of X, the rows by the elements of $\mathcal{F}$, and for $x \in X$ and $Y \in \mathcal{F}$ we have $H(Y, x) = 1$ if and only if $x \in Y$. Clearly, dim V can be computed from the rank of H since V is spanned by the union of the solutions to $Hx = J$ or $Hx = 0$ (J denotes the all-one column vector in $F^{|\mathcal{F}|}$, and dim V depends on whether J belongs to the column space of H). Note that H can be viewed as an incidence matrix of a hypergraph.

The problem of determining or computing the uniformity space of specific combinatorial structures has been studied by several researchers. For example, in [5] the problem of determining the Zero-Sum (mod 2) bipartite Ramsey numbers of a bipartite graph G was solved by determining the uniformity space of the family of all bipartite subgraphs of $K_{n,n}$ which are isomorphic to G, over the field Z_2 (in fact, over any field). See also [6] for a determination of the uniformity space of the family of all subgraphs of K_n isomorphic to a specific graph G over any field. Another recent application of uniformity space is the characterization of the Z_m-well-covered graphs of girth at least 6 [4]. A graph G is a *magic graph* if the uniformity space of all the maximal stars in G contains a one-to-one function from the edge-set of G to a field. Some papers considering magic graphs are [10, 11, 7, 13]. Computing the rank of incidence matrices of hypergraphs has been investigated by several researchers (cf. [2, 8, 14]) and these results may sometimes be helpful in solving combinatorial problems which rely on the characterization of an appropriate uniformity space. Weighted well-covered graphs are graphs with real-valued weights on the vertices such that all maximal (w.r.t. containment) independent sets have the same weight. In other words, the uniformity space (over the reals) of all maximal independent sets is non-trivial. These graphs have been studied in [3]. Other papers relating to uniformity space are [9] and [12].

In this paper we consider the uniformity aspects of fixed length arithmetic progressions in sequences. Consider a sequence of n elements $a_1, \ldots, a_n$ of some field F. The sequence is called k-constant (we assume $k \leq n$) if the sum of the values of all subsequences formed by an arithmetic progression of length k of $1, \ldots, n$ is the same. k-constant arithmetic progressions in the field Z_2 are discussed in [1]. Since every sequence corresponds to a function $f : \{1, \ldots, n\} \rightarrow F$, we have that the set of all k-constant sequences forms a vector space which is the uniformity space $V(X, \mathcal{F}, F)$ where $X = \{1, \ldots, n\}$ and $\mathcal{F}$ is the set of all arithmetic progressions of length k of X. Clearly, $V(X, \mathcal{F}, F)$ is only a function of n, k and F, so we shall use the notation $V(n, k, F)$. Since any constant sequence is k-constant, we trivially have dim $V(n, k, F) \geq 1$. Since, obviously

$f(i) = f(i+k)$, it is also immediate to verify that for every $n \geq k$

$$k = \dim V(k,k,F) \geq \dim V(n,k,F) \geq \dim V(n+1,k,F) \geq 1. \quad (1)$$

Thus, it is natural to define the following two parameters:

1. $m(k,F) = \min_{n=k}^{\infty} \dim V(n,k,F)$.

2. $c(k,F) = \min\{n \mid \dim V(n,k,F) = m(k,F)\}$.

The purpose of this paper is to determine $m(k,F)$ and $c(k,F)$. It turns out that these values are only functions of k and the *characteristic of* F and not of the actual field being used. Let p denote the characteristic of F. The value of $m(k,F)$ is determined in the following theorem:

Theorem 1.1 *If $p = 0$ or $gcd(p,k) = 1$ then $m(k,F) = 1$. Otherwise, let $k = p^r t$ where $r \geq 1$ is maximal, then $m(k,F) = k - t$.*

Note that Theorem 1.1 shows that if $p = 0$ or $gcd(p,k) = 1$ then, for $n \geq c(k,F)$ the only k-constant sequences are the constant sequences. On the other hand, if p is a prime factor of k then there always exist infinite non-constant sequences which are k-constant (except when $k = p = 2$), and, in fact, there are $k - t - 1$ such sequences which are linearly independent.

The problem of determining $c(k,F)$ turns out to be much harder. We are currently unable to determine it precisely for every k, but there is a wide spectrum of integers for which we can. If $p \neq 0$ put $k = p^r t$ where $gcd(p,t) = 1$, and if $p = 0$ put $t = k$ (Thus, $t = k$ if and only if p is not a prime factor of k). The following theorem determines $c(k,F)$ whenever t has at most two distinct prime factors:

Theorem 1.2 *If $t = q_1^{r_1} q_2^{r_2}$ where $r_1 \geq 0$ and $r_2 \geq 0$ and q_1, q_2 are primes, then:*

- *if $p < t$ or $gcd(p,k) = 1$ then $c(k,F) = (k-1)t + \phi(t)$, where ϕ denotes Euler's function*
- *otherwise, $c(k,F) = (k-1)p + 1$.*

Examples:

1. Theorem 1.2 holds for every $k < 30$, and for any field, since 30 is the smallest number which is a multiple of three distinct primes. In fact, there are exactly six numbers between 1 and 100 which are multiples of more than two distinct prime powers.

2. If F is any field with characteristic 2 then Theorem 1.2 holds for any $k < 105$.

3. If $k = q^s$ where $q \neq p$ is a prime then $c(k, F) = q^{2s} - q^{s-1}$. (Recall that $\phi(q^s) = q^s - q^{s-1}$). If, on the other hand, $k = p^s$, we have $c(k, F) = p^{s+1} - p + 1$.

4. If $k = q_1^{s_1} q_2^{s_2}$ where q_1, q_2 are distinct primes, which are distinct from p then we have, together with Theorem 1.1, that every k-constant function is constant if and only if $n \geq q_1^{2s_1} q_2^{2s_2} - q_1^{s_1-1} q_2^{s_2-1}(q_1 + q_2 - 1)$.

5. If $k = 6$ and $p = 3$ then $c(6, F) = 16$. If $p = 2$ then $c(6, F) = 17$. Otherwise, $c(6, F) = 32$.

We conjecture that Theorem 1.2 holds for every k:

Conjecture 1.3 *For every positive integer k, if $p < t$ or $gcd(p, k) = 1$ then $c(k, F) = (k-1)t + \phi(t)$. Otherwise, $c(k, F) = (k - 1)p + 1$.*

We establish an interesting connection between Conjecture 1.3 and a conjecture about $(0, 1)$-matrices over the integers. Let n and k be two positive integers where k divides n. We define the *divisor matrix* $A_{n,k}$ as follows: $A_{n,k}$ has n columns and $\phi(k)$ rows, and $A_{n,k}(i, j) = 1$ if and only if k divides $i - j$. Now define the *primary divisor matrix* A_n to be the union of the rows of all $A_{n,k}$ for every k which divides n (for uniqueness, we assume that if $k_1 < k_2$ are two divisors of n, the rows of A_{n,k_1} appear before the rows of A_{n,k_2}. Note that A_n is square since $\sum_{k \mid n} \phi(k) = n$. The following conjecture is simple to state (but, unfortunately, much harder to prove):

Conjecture 1.4 *$det(A_n) \in \{1, -1\}$. Namely, A_n is non-singular over any field.*

A slightly stronger version of this conjecture is that $det(A_n) = 1$ if n is odd and $det(A_n) = -1$ if n is even. Since A_n can be constructed easily, one can use a computer to verify the conjecture for small n. We have verified it for all $n < 180$. We can prove conjecture 1.4 for every n which has at most two distinct prime factors:

Theorem 1.5 *If n has at most two distinct prime factors then A_n is non-singular over any field.*

The relationship between A_n and $c(k, F)$ is established in the following theorem:

Theorem 1.6 *If A_t is non singular over F then:*

- *if $p < t$ or $gcd(p, k) = 1$ then $c(k, F) = (k - 1)t + \phi(t)$,*
- *otherwise, $c(k, F) = (k - 1)p + 1$.*

Thus, we see that Theorem 1.2 is a corollary of Theorems 1.5 and 1.6. Hence, we only need to prove the latter two theorems. Another interesting consequence of Theorem 1.6 is that if Conjecture 1.4

is true then so is Conjecture 1.3. This is rather intriguing since conjecture 1.4 bears no relevance to fields; it is only stated over the integers.

The rest of this paper is organized as follows. In section 2 we investigate the properties of the matrices A_n and prove Theorem 1.5. In Section 3 we prove Theorems 1.1 and 1.6.

2 Primary divisor matrices

In this section we consider the primary divisor matrix A_n and prove Theorem 1.5. We first need to recall a few definitions. For a square $(0,1)$-matrix B of order n, the *permanent* of B, denoted by $Perm(B)$ is the number of permutations σ of $1,\ldots,n$ for which $\Pi_{i=1}^{n} B(i,\sigma(i)) = 1$. The following observations are immediate:

1. If $Perm(B) = 1$ then $det(B) \in \{1,-1\}$. Thus, B is non-singular over every field.
2. $Perm(B)$ is odd if and only if $det(B)$ is odd. Thus, $Perm(B)$ is odd if and only if B is non-singular over each field with characteristic 2.

Note, however that for every odd prime p, there exist $(0,1)$-matrices with $det(B) = p$. Such a matrix has, of course, an odd permanent but is singular over every field with characteristic p. Unfortunately, primary divisor matrices may have permanents larger than 1. For example, the matrix A_{12} shown in Table 1 has $Perm(A_{12}) = 3$, while $det(A_{12}) = -1$. In fact, the permanent of A_n can get quite large if n has many divisors.

If $v = (v_1,\ldots,v_n) \in F^n$ is any vector, and $k > 0$ divides n, we say that v is *k-periodic* if for each $i = 1,\ldots,n-k$, $v_i = v_{i+k}$. Trivially, v is n-periodic, and the only vectors which are 1-periodic are the constant vectors. The *period* of v, denoted $\mu(v)$ is the smallest k for which v is k-periodic. For example, $v = (1,1,0,1,1,0,1,1,0)$ has $\mu(v) = 3$. Clearly, $\mu(v)$ is the *greatest common divisor* of all the periods of v. The following lemma highlights the role of Euler's function in the definition of the divisor matrix $A_{n,k}$.

Lemma 2.1 *Let F be a field. If v is the result of a non-trivial linear combination over F of the row vectors of $A_{n,k}$, then $\mu(v) = k$.*

Proof: If $k = 1$ the lemma is trivial, so we assume $k > 1$. By definition, the matrix $A_{n,k}$ has full row rank $\phi(k)$ over F. Since v results from a non-trivial linear combination over F of the rows of $A_{n,k}$ we have $v \neq 0$. Every row of $A_{n,k}$ is k-periodic. Thus, v is also k-periodic. Assume, for the sake of contradiction, that $\mu(v) = s < k$. Hence, s properly divides k. Let p be the smallest prime which divides k. Then $s \le k/p$. Also, $\phi(k) \le k - k/p$, and therefore $k - \phi(k) \ge k/p$. It follows that

$$A_{6,3} = \begin{vmatrix} 1\,0\,0\,1\,0\,0 \\ 0\,1\,0\,0\,1\,0 \end{vmatrix} \quad A_7 = \begin{vmatrix} 1\,1\,1\,1\,1\,1\,1 \\ 1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0 \end{vmatrix} \quad A_9 = \begin{vmatrix} 1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 1\,0\,0\,1\,0\,0\,1\,0\,0 \\ 0\,1\,0\,0\,1\,0\,0\,1\,0 \\ 1\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0\,0\,0 \end{vmatrix} \quad A_{12} = \begin{vmatrix} 1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0 \\ 1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0 \\ 0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0 \\ 1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,0 \\ 0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0 \\ 1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0 \\ 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0 \end{vmatrix}$$

Table 1: Some divisor matrices and primary divisor matrices

$k - \phi(k) \geq s$. The rows of $A_{n,k}$ have, simultaneously, $k - \phi(k)$ consecutive zeroes in the columns $\phi(k) + 1, \ldots, k$. Thus, v also has zeroes in these columns, and, in particular, v has s consecutive zeros. Since v is s-periodic, it follows that $v = 0$, a contradiction. □

We prove Theorem 1.5 in two stages. We first prove it for primes and prime powers (this part is rather easy) and we then prove it for multiples of two distinct prime powers (in this part the arguments are more complex).

Lemma 2.2 *If q is a prime and $s \geq 0$ then $Perm(A_{q^s}) = 1$.*

Proof: We prove the Lemma by induction on s. The case $s \leq 1$ is simple. The only permutation σ which gives $\Pi_{i=1}^{n} A_q(i, \sigma(i)) = 1$ is the permutation $\sigma = (q, 1, 2, \ldots, q-1)$ (cf. e.g. Table 1 for the case $q = 7$). Since the sign of this permutation is $sgn(\sigma) = (-1)^{q-1}$, we also get that $\det(A_q) = 1$ unless $q = 2$ in which case $det(A_2) = -1$. Assume the lemma holds for $s - 1$. We show it holds for s. The intersection between the last $\phi(q^s)$ rows and the first $\phi(q^s)$ columns of A_{q^s} is the identity matrix. Since $\phi(q^s) = q^s - q^{s-1}$, it suffices to show that the permanent of the matrix A' formed by the intersection of the first q^{s-1} rows and the last q^{s-1} columns of A_{q^s} has $perm(A') = 1$ (cf. e.g. Table 1 for the case $q = 3$ and $s = 2$). However, since each of the first q^{s-1} rows of A_{q^s} is q^{s-1} periodic, we have that $A' = A_{q^{s-1}}$. By the induction hypothesis we have $perm(A_{q^{s-1}}) = 1$, completing the proof. Note also that since the determinant of the identity matrix is 1, and since we are looking at consecutive rows whose number is even, we also have $det(A_{q^s}) = det(A_{q^{s-1}})$. Consequently, $det(A_{q^s}) = 1$ unless $q = 2$ in which case $det(A_{2^s}) = -1$. □

In order to complete the proof of Theorem 1.5 we need a lemma about semi-periodic vectors. A vector $w = (w_1, \ldots, w_z)$ of length z is called x *semi-periodic* if $w_i = w_{i+x}$ for $i = 1, \ldots, z - x$.

Note that in this definition we do not require that x divides z.

Lemma 2.3 *If $w = (w_1, \ldots, w_z)$ is both x semi-periodic,and y semi-periodic, where $z \geq x + y - gcd(x, y)$, then w is $gcd(x, y)$ periodic.*

Proof: We assume $x \leq y$ and x does not divide y (otherwise the lemma is trivial). Put $d = gcd(x, y)$, and let $x = ad$ and $y = bd$. Put $b = sa + r$ where $1 \leq r < a$. Clearly, $gcd(a, r) = gcd(a, b) = 1$. Denote $(w_1, \ldots, w_x)$ by $A_1 A_2 \cdots A_a$ where the A_i are vectors of length d. Since w is x semi-periodic it suffices to prove that $A_1 = \cdots = A_a$. Let $u = x + y - d \leq z$ and consider $w' = (w_{sx+1}, \ldots, w_y, w_{y+1}, \ldots, w_u)$. Note that $y = sx + rd$ and $u = y + (a - 1)d$. Since w' is x semi-periodic we have $w' = A_1 A_2 \cdots A_r A_{r+1} \cdots A_a A_1 \cdots A_{r-1}$. Since w' is y semi-periodic we have $w' = A_1 A_2 \cdots A_r A_1 \cdots A_{a-r} A_{a-r+1} \cdots A_{a-1}$. So, $A_i = A_{(i+r) \bmod a}$. From $gcd(a, r) = 1$ it follows that $A_1 = \cdots = A_a$. $\square$

We are now ready to complete the proof of Theorem 1.5.

Proof of Theorem 1.5: Let $n = q_1^{s_1} q_2^{s_2}$ where $q_1 < q_2$ are primes and s_1, s_2 are two nonnegative integers. Let F be an arbitrary field. We must show that A_n is non-singular over F. We prove the theorem by induction on s_2. If $s_2 = 0$ then $n = q_1^{s_1}$. If $s_1 = 0$ the result is trivial, and if $s_1 > 0$ then n is a prime power, and according to Lemma 2.2 $Perm(A_n) = 1$, so A_n is non-singular over F. We now assume that the theorem holds for $s_2 - 1$, and show that it holds for s_2. The proof will be established by showing that any nontrivial linear combination over F of the rows of A_n does not yield the vector 0. Each row of A_n belongs to some $A_{n,k}$, and is uniquely defined by k and j where $1 \leq j \leq \phi(k)$ is the first nonzero position in the row. The row corresponding to k and j is denoted by $v_{k,j}$. Clearly, $\mu(v_{k,j}) = k$. We partition the set of rows of A_n into two parts, Q_1 and Q_2 according to the following rule:

$$Q_1 = \{v_{k,j} \mid k \text{ divides } q_1^{s_1} q_2^{s_2 - 1}\}.$$

All other rows of A_n belong to Q_2. Thus,

$$Q_2 = \{v_{k,j} \mid q_2^{s_2} \text{ divides } k\}.$$

(For example, if $n = 36$ where $q_1 = 2$ and $q_2 = 3$, $s_1 = 2$ and $s_2 = 2$, we have that Q_1 is formed by the rows belonging to $A_{36,1}, A_{36,2}$,$A_{36,3}$, $A_{36,4}$,$A_{36,6}$ and $A_{36,12}$ while Q_2 contains the rows of $A_{36,9}$, $A_{36,18}$ and $A_{36,36}$). Consider any vector v which is the result of a nontrivial linear combination of the rows of A_n. We must show that $v \neq 0$. Put

$$v = \sum_{k \mid n} \sum_{j=1}^{\phi(k)} \lambda_{k,j} v_{k,j}.$$

We may write $v = u_1 + u_2$ where u_i is the part of the linear combination consisting of the rows of Q_i. Namely:

$$u_1 = \sum_{k \mid q_1^{s_1} q_2^{s_2-1}} \sum_{j=1}^{\phi(k)} \lambda_{k,j} v_{k,j} \qquad u_2 = \sum_{q_2^{s_2} \mid k} \sum_{j=1}^{\phi(k)} \lambda_{k,j} v_{k,j}.$$

Assume first that the linear combination forming u_2 is trivial. It suffices to show that $u_1 \neq 0$. The vectors forming u_1 all belong to Q_1, and hence they are all $q_1^{s_1} q_2^{s_2-1}$ periodic. Thus, considering only the first $q_1^{s_1} q_2^{s_2-1}$ columns in these vectors, we have a nontrivial linear combination of the rows of $A_{q_1^{s_1} q_2^{s_2-1}}$, which, by the induction hypothesis, results in a nonzero vector. Hence, u_1 has at least one nonzero component.

We may now assume that the linear combination forming u_2 is nontrivial. Since all the vectors belonging to Q_1 are $q_1^{s_1} q_2^{s_2-1}$ periodic, we have that u_1 is also $q_1^{s_1} q_2^{s_2-1}$ periodic. Therefore, it suffices to show that u_2 is *not* $q_1^{s_1} q_2^{s_2-1}$ periodic. Let i be the maximal integer such that $k = q_2^{s_2} q_1^i$, and $\lambda_{k,j} \neq 0$ for some $1 \leq j \leq \phi(k)$. Clearly, $i \geq 0$ exists. Let $k = q_2^{s_2} q_1^i$ and put $u^* = \sum_{j=1}^{\phi(k)} \lambda_{k,j} v_{k,j}$. Since u^* is a nontrivial linear combination of the rows of $A_{n,k}$, we have, by Lemma 2.1, $\mu(u^*) = k$. Consider first the case $i = 0$. In this case $u^* = u_2$. Since $k = q_2^{s_2}$, we have

$$k \not| \, q_1^{s_1} q_2^{s_2-1}$$

and, therefore, u^* cannot be $q_1^{s_1} q_2^{s_2-1}$ periodic, and we are done. We now assume that $i > 0$. Put $\overline{u} = u_2 - u^*$. Each vector in the linear combination forming $\overline{u}$ is $q_2^{s_2} q_1^{i-1}$ periodic, and therefore, putting $y = q_2^{s_2} q_1^{i-1}$, we also have that $\overline{u}$ is y periodic (it is possible that $\overline{u}$ has smaller periods, in fact, it is possible that $\overline{u} = 0$). Assume, for the sake of contradiction, that u_2 is $q_1^{s_1} q_2^{s_2-1}$ periodic. Since $u_2 = \overline{u} + u^*$ we have, by the maximality of i, that u_2 is also $q_2^{s_2} q_1^i$ periodic. Put $x = q_2^{s_2-1} q_1^i$. Since

$$gcd(q_1^{s_1} q_2^{s_2-1} \ , \ q_2^{s_2} q_1^i) = q_2^{s_2-1} q_1^i = x$$

we have that u_2 is also x-periodic. Now, put $z = k - \phi(k)$. In any linear combination of rows of $A_{n,k}$, and in particular, in u^*, there are $k - \phi(k) = z$ consecutive zeroes in columns $\phi(k)+1, \ldots, k$. Thus, u_2 coincides with $\overline{u}$ in these columns. Let w be the partial vector of length z of u_2 consisting of these columns. Since u_2 is x-periodic, we have that w is x semi-periodic. Since $\overline{u}$ is y-periodic, we have that w is also y semi-periodic. Recalling the definitions of x, y, z we see that

$$z = k - \phi(k) = q_2^{s_2-1} q_1^i + q_2^{s_2} q_1^{i-1} - q_2^{s_2-1} q_1^{i-1} = x + y - gcd(x, y)$$

We can therefore use lemma 2.3 and obtain that w is $gcd(x, y) = q_2^{s_2-1} q_1^{i-1}$ periodic. Since w is of length z, and since $z \geq y$, and since $\overline{u}$ contains w as an interval, we have that $\overline{u}$ is also

$gcd(x,y) = q_2^{s_2-1}q_1^{i-1}$ periodic. Since u_2 is x-periodic, and since $u^* = u_2 - \overline{u}$ we have that u^* is also x-periodic. This, however, is a contradiction since $\mu(u^*) = k$ while

$$gcd(x,k) = gcd(q_2^{s_2-1}q_1^{i}\ ,\ q_2^{s_2}q_1^{i}) = x < k. \qquad \square$$

3 Arithmetic progressions and primary divisor matrices

In this section we use the properties of primary divisor matrices to prove Theorem 1.6. We shall begin, however, with proving Theorem 1.1, which is easier. Let $f = (a_1,\ldots,a_n)$ be a sequence of a field F. Given positive integers i, d and k, where $i+(k-1)d \le n$, we let $f(i,d,k)$ denote the arithmetic subsequence (a.s. for short) of f which consists of the elements $a_i, a_{i+d}, a_{i+2d}, \ldots, a_{i+(k-1)d}$. Since k will usually be fixed, we shall use the notation $f(i,d)$ whenever there is no confusion. If f is k-constant, let $s(f)$ denote the common value of all a.s. of length k. Clearly $s(f) = a_1 + \ldots + a_k$. By considering $f(i,1)$ for $i = 2,\ldots,n-k+1$, we immediately obtain that if $i \equiv j \bmod k$ then $a_i = a_j$. Thus, f is k semi-periodic (we use "semi" here for consistency with the definition in Section 2, since k does not necessarily divide n), and is determined by its first k elements $a_1,\ldots,a_k$. In this section we shall, therefore, always assume that the sequences are k semi-periodic. Moreover, given a k semi-periodic sequence f, we do not need to test all the a.s. in order to determine if f is k-constant. It suffices to test only a.s. of the form $f(i,d)$ where $1 \le i \le k$ and $1 \le d < k$. We shall make use of these facts with no further mention.

Proof of Theorem 1.1: Let F be a field with characteristic p, and let k be a fixed positive integer. Throughout the proof we shall assume $n \ge k^2$. We consider first the simple case where $p = 0$ or $gcd(p,k) = 1$. Let f be a k-constant sequence of F, with n elements. We will show that f must be constant, thereby obtaining $m(k,F) = 1$. For each $i = 1,\ldots,k$ we have the a.s. $f(i,k)$ (the last element is $a_{i+k(k-1)}$ and $i + k(k-1) \le k^2 \le n$). Since all the elements of $f(i,k)$ are equal to a_i, we have that $s(f) = ka_i$ for each $i = 1,\ldots,k$. Since $k \ne 0$ in F, we have $a_1 = a_2 = \ldots = a_k$. It follows that f is constant and therefore $m(k,F) = 1$.

We now assume that $k = p^r t$ where $r \ge 1$ is maximal (i.e. $gcd(t,p) = 1$). We must show that $m(k,F) = k-t$. Our first claim is that every k-constant sequence f must have $s(f) = 0$. Indeed, since $n \ge k^2 > p(k-1)+1$ we may look at the a.s. $f(1,p)$. Since p divides k, this a.s. shows $s(f) = p(a_1 + a_{p+1} + \ldots + a_{k-p+1})$. However, since $p = 0$ in F, this gives $s(f) = 0$. Next, we show that $m(k,F) \le k-t$. Consider the a.s. $f(i,t)$ of an arbitrary k-constant sequence f, for all $i = 1,\ldots,t$. Since t divides k, and since $s(f) = 0$, these a.s. show that

$$t(a_i + a_{i+t} + \ldots + a_{k-t+i}) = 0 \qquad \forall\, i = 1,\ldots,t.$$

Since $gcd(t, p) = 1$, we have $t \neq 0$ in F. Thus, the last equation is equivalent to

$$a_i + a_{i+t} + \ldots + a_{k-t+i} = 0 \qquad \forall\, i = 1, \ldots, t. \tag{2}$$

(2) is a homogeneous system of t linear equations with k variables, whose corresponding matrix has full row rank (it contains the identity matrix I_t). Thus, the space of solutions of (2), which contains $V(n, k, F)$, has dimension $k - t$. It follows that $m(k, F) \leq k - t$. In order to show that $m(k, F) = k - t$ it suffices to show that if f is a k semi-periodic sequence which satisfies (2), then it is also k-constant. Consider $f(i, d)$ where $1 \leq i \leq k$ and $1 \leq d \leq k$. We must show that the sum of the elements of $f(i, d)$ is zero. Put $z = gcd(k, d)$ and put $x = i \bmod z$ where $1 \leq x \leq z$. Clearly, by periodicity, we have that the sum of the elements of $f(i, d)$ is:

$$z \cdot (a_x + a_{x+z} + a_{x+2z} + \ldots + a_{x+k-z}). \tag{3}$$

We distinguish two cases:

1. p divides d. In this case, $z = gcd(k, d)$ is a multiple of p, so $z = 0$ in F. Thus, (3) is zero.

2. p does not divide d. Hence, $z = gcd(k, d) = gcd(t, d)$. In this case (3) is a linear combination of the rows of system (2). This can be seen by taking the sum of the rows $x, x + z, x + 2z, \ldots, x + t - z$, and multiplying the result by the scalar $z \neq 0$ in F. $\Box$

Before we prove Theorem 1.6 we need the two following lemmas:

Lemma 3.1 *If A_t is non-singular over F, and z divides t, then the set of rows of A_t which are z-periodic span every z-periodic vector of length t over F.*

Proof: The rows of A_t which are z-periodic are the union of the rows belonging to the matrices $A_{t,x}$ where x divides z. There are, altogether, $\sum_{x \mid z} \phi(x) = z$ such rows. Since A_t is non-singular over F, this set of rows has full row rank, namely z. Since each of these z rows is z-periodic, we can restrict our attention to the first z columns, thereby obtaining a z by z non-singular matrix. Hence, the rows span every z-periodic vector over F. $\Box$

For three positive integers k, j, i where j divides k and $1 \leq i \leq j$, define the vector $v_{k,j,i}$ as follows: $v_{k,j,i} = (x_1, \ldots, x_k)$ where $x_s = j$ if $s = i \bmod j$. Otherwise, $x_s = 0$. For example, $v_{12,4,3} = (0, 0, 4, 0, 0, 0, 4, 0, 0, 0, 4, 0)$. Now, given t and k where t divides k we define three matrices as follows: $B_{k,t}$ is the matrix whose rows are all the $v_{k,j,i}$ where $1 \leq j < t$, j divides t and $i = 1, \ldots, j$, or $j = t$ and $i = 1, \ldots, \phi(t) - 1$. $C_{k,t}$ is the same as $B_{k,t}$ with one additional row, which is $v_{k,t,\phi(t)}$. $D_{k,t}$ is the same as $C_{k,t}$ with the additional rows $v_{k,t,i}$ for $i = \phi(t) + 1, \ldots, t$. Note that $B_{k,t}$, $C_{k,t}$ and $D_{k,t}$ all have k columns, while the number of rows of $B_{k,t}$ (and therefore also the number of rows of $C_{k,t}$ and $D_{k,t}$), may be substantially larger than k. For example, $B_{60,60}$ has 123 rows, $C_{60,60}$ has 124 rows and $D_{60,60}$ has 168 rows. However, the crucial observation is the following:

Lemma 3.2 *Let k be an integer and let F be a field with characteristic p. Assume that t divides k, and either $p = 0$ or $gcd(p,t) = 1$. If A_t is non-singular over F then the rank of $B_{k,t}$ over F is $t-1$ and the ranks of $C_{k,t}$ and $D_{k,t}$ over F are t.*

Proof: Each row of $D_{k,t}$ (and thus, of $C_{k,t}$ and $B_{k,t}$) is of the form $v_{k,j,i}$, and since j divides t, the rows are t-periodic. Hence, it suffices to prove that the matrix $B_{t,t}$ has rank $t-1$ and the matrices $C_{t,t}$ and $D_{t,t}$ have ranks t. Each row of $D_{t,t}$ is j-periodic for some j which divides t. Thus, according to Lemma 3.1, it is spanned by the rows of A_t. It follows that the rank of $D_{t,t}$ is at most t. On the other hand, each row of A_t belongs to some divisor matrix $A_{t,j}$, and is, therefore, equal to some $j^{-1}v_{t,j,i}$. Note that j^{-1} exists since $j \neq 0$ in F, as j divides t and either $p = 0$ or $gcd(p,t) = 1$. Hence, the rank of A_t (which is t by the assumption) is at most the rank of $C_{t,t}$. Consequently, the ranks of $C_{t,t}$ and $D_{t,t}$ are both t. Now, for $B_{t,t}$ the argument is the same except that we ignore the last row of A_t. □

Proof of Theorem 1.6: Let k be a positive integer, and let F be a field of characteristic p. $k = p^r t$, where $gcd(t,p) = 1$. If $p = 0$ then we define $t = k$. Assume that A_t is non-singular over F. We must show that if $t > p$ or $gcd(p,k) = 1$ then $c(k,F) = (k-1)t + \phi(t)$, and otherwise (namely, if $t < p \mid k$) then $c(k,F) = (k-1)p + 1$.

Consider first the case where $p = 0$ or $gcd(p,k) = 1$. In this case, we must show that $c(k,F) = (k-1)k + \phi(k)$, assuming A_k is non-singular over F. Recall that, by Theorem 1.1, $m(k,F) = 1$. We will show that if $n = (k-1)k + \phi(k) - 1$ then $\dim V(n,k,F) > 1$, and when $n = (k-1)k + \phi(k)$ then $\dim V(n,k,F) = 1$. Assume first that $n = (k-1)k + \phi(k) - 1$. Consider the homogeneous linear system of equations

$$B_{k,k}(a_1, \ldots, a_k)^T = 0. \tag{4}$$

According to Lemma 3.2, $B_{k,k}$ has rank $k-1$, and, therefore, the system (4) has a nontrivial solution $f = (a_1, \ldots, a_k) \in F^k$. We may identify f with a k semi-periodic sequence with n elements in the obvious manner. Note first that f is linearly independent with the all-one constant sequence of length n. This is because $a_1 + \ldots + a_k = 0$, while, in the constant sequence, the corresponding sum is k, and $k \neq 0$ in F. We now show that $f \in V(n,k,F)$. Indeed, consider any a.s. $f(i,d)$ where $1 \leq i \leq k$ and $1 \leq d \leq k$. We must show that in any such a.s. the sum of the elements is the same (in fact, it is zero). Put $z = gcd(k,d)$ and put $x = i \bmod z$ where $1 \leq x \leq z$. Then, the sum of the elements of $f(i,d)$ is given in (3). However, if $z < k$ then (3) corresponds to the expression

$v_{k,z,x}(a_1,\dots,a_k)^T$ which is the left hand side of one of the equations in the system (4). So, in this case, (3) is zero. Now, if $z = k$ this means that $z = d = k$, but since $n = (k-1)k + \phi(k) - 1$ we can only have $i = 1,\dots,\phi(k) - 1$. So, in this case, (3) corresponds to the equation $ka_i = 0$, which, once again, is one of the equations in the system (4). So, also here, (3) is zero. We have proved that dim $V(n,k,F) > 1$ since $V(n,k,f)$ contains f as well as the all-one constant sequence, and they are linearly independent.

We now assume that $n = (k-1)k + \phi(k)$. Consider the following linear system of equations over F

$$C_{k,k}(a_1,\dots,a_k)^T = \alpha J^T, \tag{5}$$

where J is the all-one vector, and $\alpha \in F$. According to Lemma 3.2, the rank of $C_{k,k}$ is k, and, therefore, the system (5) has at most one solution. In fact, it has exactly one solution since the constant assignment $a_i = \alpha/k$ for $i = 1,\dots,k$ solves it. On the other hand, given any k-constant sequence f with $s(f) = \alpha$, each equation in the system (5) corresponds to at least one a.s. of f. Namely, the equation $v_{k,z,x}(a_1,\dots,a_k)^T = \alpha$ corresponds to the a.s. $f(x,z)$. (Note that the last index of $f(x,z)$ is $x + (k-1)z$ and $x + (k-1)z \le \phi(k) + (k-1)k = n$ since either $z < k$ or $z = k$ but then $x \le \phi(k)$). It follows that f must be constant. Thus, dim $V(n,k,F) = 1$.

We now consider the case $p > 0$ and p divides k, but $p < t$. We must show $c(k,F) = (k-1)t + \phi(t)$. By theorem 1.1, $m(k,F) = k - t$. Assume first that $n = (k-1)t + \phi(t) - 1$. As in the proof of Theorem 1.1, if f is any k-constant sequence, the a.s. $f(1,p)$ shows that $s(f) = 0$. We use here the fact that the last index of $f(1,p)$ is $(k-1)p + 1 \le (k-1)t + \phi(t) - 1 = n$ so $f(1,p)$ is indeed an a.s. of f. Consider the linear system

$$B_{k,t}(a_1,\dots,a_k)^T = 0. \tag{6}$$

By Lemma 3.2, $B_{k,t}$ has rank $t-1$. Thus, the system (6) has $k-(t-1) = k-t+1$ linearly independent solutions. Each such solution $f = (a_1,\dots,a_k)$ is identified with a k semi-periodic sequence of length n. We show that f is k-constant, thereby obtaining that dim $V(n,k,F) \ge k-t+1$. Indeed, consider an a.s. $f(i,d)$, where $1 \le i \le k$ and $1 \le d \le k$. we must show that the sum of the elements of $f(i,d)$ (which is expressed in (3)) is zero. If d is a multiple of p we are done since $z = gcd(k,d) = 0$ in F so (3) is zero. Otherwise, $z = gcd(k,d) = gcd(t,d)$ and so the equation $v_{k,z,x}(a_1,\dots,a_k)^T = 0$ which is one of the equations in (6) shows that in this case (3) is zero (we use here that fact that z divides t and thus, either $z < t$ or $z = t$ but, if $z = t$ then also $z = t = d$ so the last index in $f(i,d)$ is $i + (k-1)t$ and since $n = (k-1)t + \phi(t) - 1$ we have $i \le \phi(t) - 1$ so $x = i$ in this case, and $v_{k,z,x}$ is, indeed, one of the lines of $B_{k,t}$). Now assume that $n = (k-1)t + \phi(t)$. We consider the linear system

$$C_{k,t}(a_1,\dots,a_k)^T = 0. \tag{7}$$

By lemma 3.2, $C_{k,t}$ has rank t, so there are exactly $k-t$ linearly independent solutions to (7). As in the previous case, we identify each solution with a k semi-periodic sequence of length n, and show, in the same way as before, that each such sequence is k-constant, and therefore, dim $V(n,k,F) \geq k-t$. On the other hand, in every k-constant sequence, the elements $(a_1, \ldots, a_k)$ of the sequence form a solution to (7), (same proof as the proof in the case $p = 0$ or $gcd(p,k) = 1$ above). Thus, dim $V(n,k,F) = k-t$.
The remaining case is when $p > t$ and p divides k. We must show that $c(k,F) = (k-1)p+1$. By theorem 1.1, $m(k,F) = k-t$. Assume first that $n = (k-1)p$. Consider the linear system over F

$$D_{k,t}(a_1, \ldots, a_k)^T = 0. \tag{8}$$

By Lemma 3.2, $D_{k,t}$ has rank t. Thus, the system (8) has $k-t$ linearly independent solutions. As before, each solution is identified with a k semi-periodic sequence of length n and, as shown in the above cases, each such sequence f is k-constant, and, in fact, $s(f) = 0$. However, there is another sequence which is also k-constant and is linearly independent of the solutions of (8). This sequence is the sequence with $a_1 = \ldots = a_t = 1$ while $a_{t+1} = \ldots = a_k = 0$. It is easy to check that the sum of each a.s. of the form $f(i,d)$ is exactly t and $t \neq 0$ in F. This is because we must have $d < p$ (since $n = (k-1)p$), and therefore, $z = gcd(k,d) = gcd(t,d)$ so in (3) there are exactly t/z elements in the interval $a_1, \ldots, a_t$ appearing there, and (3) gives that the sum is $z \cdot t/z = t$. We have proved that dim $V(n,k,F) \geq k-t+1$. However, when $n = (k-1)p+1$, each k-constant sequence also contains the a.s. $f(1,p)$ which, as already shown, forces $s(f) = 0$. Hence, the system (8) still shows that dim$V(n,k,F) \geq k-t$ but now, in every k-constant sequence, the elements $a_1, \ldots, a_k$ must also be a solution to (8), so dim $V(n,k,F) = k-t$. $\Box$

Acknowledgment

The author wishes to thank Yair Caro for many helpful references and discussions.

References

[1] N. Alon and Y. Caro, *On three zero-sum Ramsey-type problems*, J. Graph Theory 17 (1993), 177-192.

[2] A.E. Brouwer and C.A. van Eijl, *On the p-rank of the adjacency matrices of strongly regular graphs*, J. Alg. Combinatorics 1 (1992), 329-346.

[3] Y. Caro, M.N. Ellingham and J.E. Ramey, *Local structure when all maximal independent sets have equal weight*, SIAM J. Disc. Math., to appear.

[4] Y. Caro and B. Hartnell, *A characterization of Z_m well-covered graphs of girth 6 or more*, submitted.

[5] Y. Caro and R. Yuster, *The zero-sum mod 2 bipartite Ramsey numbers and the uniformity space of bipartite graphs*, J. Graph Theory, to appear.

[6] Y. Caro and R. Yuster, *The Uniformity Space of Hypergraphs and its Applications*, Discrete Math., to appear.

[7] M. Doob, *Generalizations of magic graphs*, J. Combin. Theory 17 (1974), 205-217.

[8] P. Frankl, *Intersection theorems and mod p rank of inclusion matrices*, J. Combin. Theory 15 (1973), 75-90.

[9] G. Gunther, B. Hartnell and C.A. Whitehead, *On 2-packings of graphs of girth at least 9*, Congressus Numerantium, to appear.

[10] R.H. Jeurissen, *The incidence matrix of labellings of a graph*, J. Combin. Theory, Ser. B. 30 (1981), 290-301.

[11] R.H. Jeurissen, *Magic graphs, a characterization*, Europ. J. Combin. 9 (1988), 363-368.

[12] M. Lesk, M.D. Plummer and W.R. Pulleyblank, *Equimatchable graphs*, *Graph Theory and Combinatorics*, ed. B. Bollobás, Academic Press, London, 1984.

[13] S. Jezny and M. Trenkler, *Characterization of magic graphs*, Czech. Math. J. 33 (1983), 435-438.

[14] R.M. Wilson, *A diagonal form for the incidence matrices of t-subsets vs. k-subsets*, Europ. J. Combin. 11 (1990), 609-615.