Zero-sum square matrices

Paul Balister * Yair Caro† Cecil Rousseau ‡ Raphael Yuster§

Abstract

Let A be a matrix over the integers, and let p be a positive integer. A submatrix B of A is *zero-sum* mod p if the sum of each row of B and the sum of each column of B is a multiple of p. Let $M(p,k)$ denote the least integer m for which every square matrix of order at least m has a square submatrix of order k which is zero-sum mod p. In this paper we supply upper and lower bounds for $M(p,k)$. In particular, we prove that $\limsup M(2,k)/k \leq 4$, $\liminf M(3,k)/k \leq 20$, and that $M(p,k) \geq \frac{k\sqrt{2}}{2e}\exp(1/\mathrm{e})^{p/2}$. Some nontrivial explicit values are also computed.

1 Introduction

Let A be a matrix over the integers, and let p be a positive integer. A submatrix B of A is called *zero-sum* mod p if the sum of each row of B and the sum of each column of B is a multiple of p.

Let $M(p,k)$ denote the least integer m for which every integer square matrix of order at least m has a square submatrix of order k which is zero-sum mod p. As usual in zero-sum problems, we assume that k is a multiple of p, since otherwise $M(p,k)$ may not exist, as any matrix whose elements all equal one has no square submatrix of order k which is zero-sum mod p. On the other hand, if k is a multiple of p, then $M(p,k)$ is finite by the following standard Ramsey-type argument: We may consider the elements of our matrices as taken from Z_p^+, thus, we have a coloring of an $m \times m$ grid with p colors, so, for sufficiently large m, there is a $k \times k$ sub-grid which is monochromatic. This translates to a (very specialized) submatrix of order k that is zero-sum mod p.

The case $p = 2$ has an interesting graph-theoretic interpretation. A zero-one $m \times n$ matrix A can be interpreted as the adjacency matrix of a bipartite graph $G = (X \cup Y, E)$, where $X = \{x_1, \ldots, x_m\}$ and $Y = \{y_1, \ldots, y_n\}$. In this interpretation, $A(i,j) = 1$ if and only if x_i is adjacent to y_j. Hence, $M(2,k)$ is the least integer m which guarantees that every bipartite graph with equal vertex classes

*Department of Mathematical Sciences, The University of Memphis, Memphis, TN 38152-3240. e–mail: balistep@msci.memphis.edu

†Department of Mathematics, University of Haifa-ORANIM, Tivon 36006, Israel. e–mail: yairc@macam98.ac.il

‡Department of Mathematical Sciences, The University of Memphis, Memphis, TN 38152-3240. e–mail: ccrousse@memphis.edu

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

having cardinality m, has an induced subgraph with equal vertex classes (one subclass from each original class) having cardinality k, such that all degrees are even. By the Ramsey-type argument mentioned above, it is obvious that $M(2,k) \leq B(k)$ where $B(k)$ is the *bipartite Ramsey number*, namely, the least integer m which guarantees that in any two-coloring of the edges of $K_{m,m}$ there exists a monochromatic copy of $K_{k,k}$. The best upper bound [6] and lower bound [4] for $B(k)$ are currently:

$$\sqrt{2}\mathrm{e}^{-1}k2^{k/2} < B(k) \leq 2^k(k-1)+1. \tag{1}$$

Thus, in particular, we obviously get $M(2,k) \leq 2^k(k-1)+1$.

In this paper we determine several upper and lower bounds for $M(p,k)$. We begin with the specific cases $p=2$ and $p=3$. Unlike the exponential lower bound for $B(k)$, we can show that $M(2,k)$ is linear in k. We can also show that $M(3,k)$ is linear in k for infinitely many values of k.

Theorem 1.1

1. $\limsup M(2,k)/k \leq 4$.
2. $\liminf M(3,k)/k \leq 20$. *In particular, for every positive integer s, $M(3,3^s) \leq 20 \cdot 3^s(1+o(1))$.*

The proof of Theorem 1.1 is based partly on a theorem of Olson [5] concerning the Davenport constant of certain abelian groups, another theorem of Enomoto et al [3], together with a tricky counting argument. In light of Theorem 1.1, the following conjecture seems plausible:

Conjecture 1.2 *For every positive integer p, there exists a constant c_p such that* $\limsup M(p,k)/k \leq c_p$.

Theorem 1.1 implies Conjecture 1.2 for $p=2$ with $c_2 \leq 4$. It is not difficult to construct examples showing $M(2,k) \geq 2k+1$ for all even k. A construction showing this appears in the proof of Theorem 1.4. Thus, we cannot have $c_2 < 2$.

It seems extremely difficult to compute $M(2,k)$ (moreover $M(p,k)$ for $p>2$) even for relatively small values of k. It is an easy exercise to show that $M(2,2)=5$. In fact, $5 \leq M(2,2) \leq B(2) \leq 5$ from (1) and from the fact that $M(2,k) \geq 2k+1$. A naive approach for computing $M(2,4)$ with a computer program which generates all possible 0-1 matrices and testing them would fail. By using, once again, the fact that $M(2,k) \geq 2k+1$, we know that $M(2,4) \geq 9$. Even generating all 0-1 matrices of order 9 is not feasible as there are 2^{81} such matrices (and even then, maybe the correct value is larger than 9). Using a sophisticated computer search that enables us to narrow down the checks considerably we can show:

Proposition 1.3 $M(2,4)=10$. *A binary matrix of order 9 which demonstrates $M(2,4)>9$ is the following:*

$$\begin{bmatrix} 1&1&1&0&0&0&1&0&0 \\ 1&1&1&0&0&0&0&1&0 \\ 1&1&1&0&0&0&0&0&1 \\ 1&0&0&1&1&1&0&0&0 \\ 0&1&0&1&1&1&0&0&0 \\ 0&0&1&1&1&1&0&0&0 \\ 0&0&0&1&0&0&1&1&1 \\ 0&0&0&0&1&0&1&1&1 \\ 0&0&0&0&0&1&1&1&1 \end{bmatrix}$$

In fact, this matrix and its complement are the only matrices of order 9 with the desired property, up to permutations of rows and columns.

The exact value of $M(2,k)$ for $k \geq 6$ is an open problem. A description of the computer search that leads to Proposition 1.3 is available upon request from the authors.

For general p, we can show that $M(p,k)/k$ grows exponentially with p. For fixed p, our lower bound only supplies a growth which is linear w.r.t. k; this is consistent with Conjecture 1.2. More precisely, we show the following:

Theorem 1.4

1. $M(p,p) \geq B(p) > \sqrt{2}\mathrm{e}^{-1}p2^{p/2}$.
2. $M(p,k) \geq \frac{k\sqrt{2}}{2e}\exp(1/\mathrm{e})^{p/2}$. *For* $p = 2$ *we have* $M(2,k) \geq 2k+1$.

The rest of this paper is organized as follows. In Section 2 we present the proof of Theorem 1.1. The proof of Theorem 1.4 is given in Section 3.

2 Upper and lower bounds for $M(2,k)$

In order to prove the first part of Theorem 1.1 we need the following special case of the main theorem in [3] proved by Enomoto et al. Recall that a linear binary code of length t contains the distance k if it contains as a codeword a vector with k ones and $t-k$ zeroes.

Lemma 2.1 ([3]) *Let k be even, and let A be a binary matrix with $k-1$ rows and $2k$ columns. Then, A is a parity-check matrix of a (linear) code which contains the distance k.* □

In order to prove the second part of Theorem 1.1 we need to state a theorem of Olson concerning the *Davenport constant* of certain abelian p-groups. Let G be a finite abelian group. The Davenport constant of G, denoted $D(G)$, is the least positive integer t such that in any sequence of t elements of G there is a (nonempty) subsequence whose sum is zero. Now, let p be a prime, and let G be a p-group. Then, $G = Z_{p^{\alpha_1}} \times \ldots \times Z_{p^{\alpha_k}}$. Olson [5] proved the following:

Lemma 2.2 *If* $G = Z_{p^{\alpha_1}} \times \ldots \times Z_{p^{\alpha_k}}$ *then* $D(G) = 1 + \sum_{i=1}^{k}(p^{\alpha_i} - 1)$. $\square$

An *even* vector is a binary vector whose number of nonzero coordinates is even. More generally, a *p-divisible* vector is a vector from $(Z_p)^k$ whose sum of coordinates is divisible by p. We use Lemmas 2.1 and 2.2 to prove the following two lemmas:

Lemma 2.3 *Let k be an even positive integer. Then, every sequence of $2k$ even vectors of length k each, contains a subsequence of exactly k vectors whose sum* mod 2 *is the zero vector. Moreover, if k is a power of 2, then every sequence of $2k-1$ even vectors of length k each contains a subsequence of exactly k vectors whose sum* mod 2 *is the zero vector.*

Proof: Consider the matrix A whose columns are the elements of the sequence of $2k$ even vectors of length k. Ignoring the last row of A, we have, by Lemma 2.1, a parity check matrix of a linear code that contains the distance k. By the definition of a parity check matrix, this means that we can choose k columns whose sum mod 2 is zero. Adding back the last coordinate to these columns still gives a zero sum mod 2, since the columns of A are even vectors.
Now, let k be a power of 2, and let $a_1, \ldots, a_{2k-1}$ be a sequence of even binary vectors, where $a_i \in (Z_2)^k$. Let b_i be the same as a_i, except that the last coordinate of b_i is always one. Note that b_i may not be even any more. We consider the b_i as elements of $G = (Z_2)^{k-1} \times Z_k$. Since k is a power of 2, G is a p-group for $p = 2$. According to Lemma 2.2, $D(G) = 1+(k-1)+(k-1) = 2k-1$. Hence, there is a nonempty subsequence of $\{b_1, \ldots, b_{2k-1}\}$ whose sum is zero. Since the last coordinate of b_i is the element 1 of Z_k, such a subsequence must contain *exactly* k elements. Thus, if $b_{i_1}, \ldots, b_{i_k}$ are the elements of such a subsequence we have $b_{i_1} + \ldots + b_{i_k} = 0$. Now, since the a_i's are even vectors we immediately get $a_{i_1} + \ldots + a_{i_k} = 0$. $\square$

Lemma 2.4 *Let k be a power of 3. Every sequence of $5k-2$ vectors of length k each that are 3-divisible, contains a subsequence of exactly k vectors whose sum is the zero vector (in $(Z_3)^k$).*

Proof: Let $a_1, \ldots, a_{5k-2}$ be a sequence of 3-divisible vectors, where $a_i \in (Z_3)^k$. Let b_i be the same as a_i, except that the last coordinate of b_i is always one. Note that b_i may not be 3-divisible any more. We consider the b_i as elements of $G = (Z_3)^{k-1} \times Z_{3k}$. Since k is a power of 3, G is a p-group for $p = 3$. According to Lemma 2.2, $D(G) = 1 + 2(k-1) + (3k-1) = 5k-2$. Hence, there is a nonempty subsequence of $\{b_1, \ldots, b_{5k-2}\}$ whose sum is zero. Since the last coordinate of b_i is the element 1 of Z_{3k}, such a subsequence must contain *exactly* $3k$ elements. Thus, if $b_{i_1}, \ldots, b_{i_{3k}}$ are the elements of such a subsequence we have $b_{i_1} + \ldots + b_{i_{3k}} = 0$. Now let us consider $b_{i_1}, \ldots, b_{i_{3k}}$ as elements of $G' = (Z_3)^{k-1} \times Z_k$. Again, G' is a p-group for $p = 3$, so by Lemma 2.1, $D(G') = 1 + 2(k-1) + (k-1) = 3k-2$. Hence, there is a nonempty subsequence of $\{b_{i_1}, \ldots, b_{i_{3k}}\}$ whose sum is zero. Since the last coordinate of b_i is the element 1 of Z_k, such a subsequence must contain either *exactly* k or $2k$ elements. In case it contains $2k$ elements, then the sum of the

remaining k vectors not in the subsequence is also zero, since the sum of all $3k$ vectors is zero. Thus, we have proved there is always a subsequence of k elements $b_{j_1}, \ldots, b_{j_k}$ whose sum is zero in G'. Now, since the a_i's are 3-divisible vectors we immediately get $a_{j_1} + \ldots + a_{j_k} = 0$. $\Box$

Let x be a vector. A *k-subset* of x is taken by selecting k coordinates of x. Clearly, if $x \in (Z_p)^t$ then the vector corresponding to a k-subset is a member of $(Z_p)^k$, and x has exactly $\binom{t}{k}$ k-subsets. Let $e_k(x)$ denote the number of p-divisible k-subsets of x (a k-subset is p-divisible if the vector corresponding to it is p-divisible). We shall always assume that k is divisible by p. If $x = (1, \ldots, 1) \in (Z_p)^t$ then $e_k(x) = \binom{t}{k}$, but, in general, $e_k(x)$ may be a lot smaller. For example, if $x = (1, 1, 1, 0, 0) \in (Z_2)^5$ then $e_2(x) = 4 < 10 = \binom{5}{2}$. Now, put

$$f(p, k, t) = \min_{x \in (Z_p)^t} e_k(x).$$

Lemma 2.5

1. *Let k be an even positive integer, and let t satisfy*

$$f(2, k, t) > \binom{t}{k} \frac{2k-1}{t}$$

   Then, $M(2, k) \leq t$.

2. *Let k be a power of 2, and let t satisfy*

$$f(2, k, t) > \binom{t}{k} \frac{2k-2}{t}$$

   Then, $M(2, k) \leq t$.

3. *Let k be a power of 3, and let t satisfy*

$$f(3, k, t) > \binom{t}{k} \frac{5k-3}{t}$$

   Then, $M(3, k) \leq t$.

Proof: We prove the first part. Let A be a square 0-1 matrix of order t. We must show that A has a square submatrix A' of order k, such that all rows and all columns of A' are even vectors. The condition $f(2, k, t) > \binom{t}{k} \frac{2k-1}{t}$ implies that the rows of A contain more than $\binom{t}{k}(2k-1)$ even k-subsets, counting multiplicity. Thus, there exists a set $X = \{i_1, \ldots, i_k\}$ of k columns of A, such that the set of vectors $a_j = (A_{j,i_1}, \ldots, A_{j,i_k})$ for $j = 1, \ldots t$ contains more than $2k-1$ even vectors. Let $Y = \{j_1, \ldots, j_{2k}\}$ be a set such that a_{j_q} is even for $q = 1, \ldots, 2k$. According to the first part of Lemma 2.3, there exists $Y' \subset Y$ such that $|Y'| = k$ and $\sum_{s \in Y'} a_s = 0$. Thus, the submatrix A' of A restricted to the columns X and the rows Y' is the required one. The proof of the second part

of the lemma is identical, except that we use the second part of Lemma 2.3, and the proof of the third part uses Lemma 2.4 where A is a square matrix of order t over $GF(3)$. $\Box$

It is not difficult to compute explicit small values of $f(p,k,t)$. Clearly, if x and y are two binary vectors having the same length, and the same number of zero coordinates, then $e_k(x) = e_k(y)$. More generally, if r denotes the number of zeroes in a binary vector of length t then,

$$f(2,k,t) = \min_{r=0}^{t} \left\{ \sum_{j=0}^{k/2} \binom{r}{k-2j} \binom{t-r}{2j} \right\}.$$

Similarly, for the case $p = 3$, if r denotes the number of zeroes and s denotes the number of ones in a 3-ary vector of length t then,

$$f(3,k,t) = \min_{r=0}^{t} \min_{s=0}^{t-r} \left\{ \sum_{j=0}^{k} \sum_{a+b=j} \sum_{a+2b \equiv 0 \bmod 3} \binom{r}{k-j} \binom{s}{a} \binom{t-r-s}{b} \right\}.$$

Example: $f(2,4,13) = 343$. The minimum is obtained when $r = 9$ (or $r = 4$). We can use the second part of Lemma 2.5 and see that $343 > \binom{13}{4} \frac{6}{13}$. Thus, we immediately get $M(2,4) \leq 13$.

Computing lower bounds for $f(p,k,t)$ in the general case is a more complicated task. The next two lemmas give a bound for every $p \geq 2$, in case $k = O(t)$ and $t \to \infty$.

Before we state the lemma, we need to define a particular constant. For a sequence of integers $a_1, \ldots, a_m$ let $w_p(a_1, \ldots, a_m)$ be the complex number defined as

$$w_p(a_1, \ldots, a_m) = 2^{-m} \sum_{\zeta^p = 1} \prod_{j=1}^{m} (1 + \zeta^{a_j})$$

where the sum is over the p distinct pth roots ζ of 1.

It is easy to see that this number is a real (indeed rational) number. Now, define $z_p = \inf w_p(a_1, \ldots, a_m)$ where the infimum is taken over all finite sequences $a_1, \ldots, a_m$ of all lengths $m \geq 0$. If all $a_i = 1$ and $\zeta \neq 1$ then $|(1 + \zeta^{a_j})/2| \leq \cos(\pi/p) = \eta < 1$ and so $w_p \leq 1 + (p-1)\eta^m$. Letting $m \to \infty$ we see that $z_p \leq 1$.

Lemma 2.6 *For all integers $p \geq 1$, $z_p = p2^{1-p}$.*

Proof: The sum $\sum_{\zeta^p=1} \zeta^j$ is p if $p \mid j$ and 0 otherwise, hence $w_p(a_1, \ldots, a_m)$ is just $p2^{-m}$ times the number of subsets X of $\{1, \ldots, m\}$ such that $\sum_{i \in X} a_i \equiv 0 \bmod p$. If $m = p - 1$ and all $a_i = 1$ then the only such subset X is $X = \emptyset$. Hence $z_p \leq p2^{1-p}$ and the result will follow if we can show the number of subsets X is always at least 2^{m+1-p}. We prove this by induction on m. Let S_m be the set of residue classes mod p that can be written in the form $\sum_{i \in X} a_i$ for some $X \subseteq \{1, \ldots, m\}$ and assume that for each element of S_m there are at least 2^{s_m} such subsets X. Now $S_m = S_{m-1} \cup (S_{m-1} + a_m)$. We consider two cases.

1) $S_m \neq S_{m-1}$. Then $|S_m| > |S_{m-1}|$ and $s_m \geq s_{m-1}$.
2) $S_m = S_{m-1}$. Then $S_{m-1} + a_m = S_{m-1}$ and so if $x \in S_m$ then both x and $x - a_m$ lie in S_{m-1}. Thus x can be written as a sum of the a_i's in at least $2^{s_{m-1}}$ ways which do not involve a_m and $2^{s_{m-1}}$ ways that do involve a_m. Thus $s_m \geq s_{m-1} + 1$.
In all cases $|S_m| + s_m \geq |S_{m-1}| + s_{m-1} + 1$. Now $S_0 = \{0\}$ and $s_0 = 0$, so by induction $|S_m| + s_m \geq m + 1$. Since $|S_m| \leq p$ we have $s_m \geq m + 1 - p$. Thus $0 \in S_m$ can be written as a sum of a_i mod p in at least 2^{m+1-p} ways. $\Box$

Lemma 2.7 *Let $k \leq t/2$. Then for any fixed prime p,*

$$f(p,k,t) \geq \frac{z_p}{p}\binom{t}{k}(1 - o_k(1)) = 2^{1-p}\binom{t}{k}(1 - o_k(1)).$$

In particular,

$$f(2,k,t) \geq \frac{1}{2}\binom{t}{k}(1 - o_k(1)),$$

$$f(3,k,t) \geq \frac{1}{4}\binom{t}{k}(1 - o_k(1)).$$

Proof: Let $T = \{1, \ldots, t\}$ and let $x = (x_1, \ldots, x_t) \in (Z_p)^t$ be a fixed vector for which $e_k(x) = f(p,k,t)$. Assume $p \mid k$ and $k \leq t/2$. We wish to estimate the number $f(p,k,t)$ of sets $K \subseteq T$, $|K| = k$, with $\sum_{i \in K} x_i \equiv 0 \bmod p$. Fix the k-element subset $K = \{1, \ldots, k\}$ of T and instead count the number p_k of permutations $\sigma \in S_t$ such that $\sum_{i=1}^{k} x_{\sigma(i)} \equiv 0 \bmod p$. It is clear that $p_k = f(p,k,t)k!(t-k)!$, so that $f(p,k,t)/\binom{t}{k} = p_k/t!$. Define

$$\hat{p}_k(\zeta) = \frac{1}{t!}\sum_{\sigma}\prod_{i=1}^{k}\zeta^{x_{\sigma(i)}} \tag{2}$$

where ζ is any pth root of 1. Then $\hat{p}_k(1) = 1$, $|\hat{p}_k(\zeta)| \leq 1$, and $p_k/t! = \frac{1}{p}\sum_{\zeta^p=1}\hat{p}_k(\zeta)$.

Let π be a partition of T into k pairs $S_i = \{a_i, b_i\}$, $i = 1, \ldots, k$, and a remaining set S_0 of $t - 2k$ numbers. We also regard π as the set of permutations σ such that $\{\sigma(i), \sigma(i+k)\} = S_i$ for all $i = 1, \ldots, k$. For each π there are exactly $2^k(t-2k)!$ choices for $\sigma \in \pi$ given by a choice of $(\sigma(i), \sigma(i+k)) = (a_i, b_i)$ or (b_i, a_i) for each i and a choice for the permutation of the remaining $t-2k$ elements of T. Let $\hat{p}_k(\zeta, \pi) = \prod_{i=1}^{k}(\zeta^{x_{a_i}} + \zeta^{x_{b_i}})/2$ and let $\mathbb{E}_\pi[\hat{p}_k(\zeta,\pi)]$ denote the expectation of $\hat{p}_k(\zeta,\pi)$ taken over a uniform random choice of π. Then,

$$\hat{p}_k(\zeta) = \frac{1}{t!}\sum_{\pi}\sum_{\sigma\in\pi}\prod_{i=1}^{k}\zeta^{x_{\sigma(i)}} = \frac{(t-2k)!}{t!}\sum_{\pi}\prod_{i=1}^{k}(\zeta^{x_{a_i}} + \zeta^{x_{b_i}}) = \mathbb{E}_\pi[\hat{p}_k(\zeta,\pi)].$$

In the last equality we use (2) and the fact that there are exactly $t!/(2^k(t-2k)!)$ choices for π.

Assume now $\zeta^p = 1$, $\zeta \neq 1$. If $a \not\equiv b \bmod p$ then $|(\zeta^a + \zeta^b)/2| \leq \cos \pi/p = \eta < 1$. Thus $|\hat{p}_k(\zeta, \pi)| \leq \eta^{n_\pi}$ where n_π is the number of $i = 1, \ldots, k$ such that $x_{a_i} \not\equiv x_{b_i} \bmod p$. Hence $|\hat{p}_k(\zeta)| \leq \mathbb{E}_\pi[\eta^{n_\pi}]$.

Let r_s be the number of coordinates with $x_i \equiv s \bmod p$. Then $\mathbb{E}_\pi[n_\pi] = \mu = k \sum_{i<j} \frac{2r_i r_j}{t(t-1)}$. It is not hard to show that $\mathrm{Var}_\pi[n_\pi] = O(\mu)$. Indeed, note that $n_\pi = \sum_{j=1}^{k} n_\pi^{(j)}$ where $n_\pi^{(j)}$ are indicator random variables that are equal to 1 in case $x_{a_j} \not\equiv x_{b_j} \bmod p$. Since $\mathrm{Cov}[n_\pi^{(j_1)}, n_\pi^{(j_2)}] = O(\mu^2/(k^2 t))$ and since $\mu \leq k < t$ we have

$$\mathrm{Var}_\pi[n_\pi] \leq \mu + k^2 O(\mu^2/(k^2 t)) = O(\mu).$$

Hence, by Tchebychev's Inequality, if $\mu \to \infty$ then n_π is almost surely large as well and $\hat{p}_k(\zeta) = o(1)$. In this case

$$\frac{f(p,k,t)}{\binom{t}{k}} = \frac{1}{p} \sum_{\zeta^p=1} \hat{p}_k(\zeta) = \frac{1}{p} \hat{p}_k(1) - o(1) \geq \frac{z_p}{p} - o(1).$$

Now assume μ is bounded and $k \to \infty$. Let $r = t - \max r_i$ be the number of coordinates of x not equal to the most common value. Then $\mu \geq k \frac{2r(t/p)}{t^2}$, so $r = O(t/k)$ and $kr^2/t^2 = o_k(1)$. By adding a constant vector to x and using $p \mid k$ we can assume the most common coefficient in x is 0. Let m_π be the number of S_i with both x_{a_i} and x_{b_i} non-zero. Then, $\Pr[m_\pi > 0] \leq E_\pi[m_\pi] = O(kr^2/t^2) = o(1)$. If $m_\pi = 0$ then $\hat{p}_k(\zeta, \pi)$ is a product of n_π terms of the form $(1 + \zeta^{a_i})/2$. Hence, the sum over all roots of unity of $\hat{p}_k(\zeta, \pi)$ is at least z_p. It follows that

$$\frac{f(p,k,t)}{\binom{t}{k}} = \frac{1}{p} \sum_{\zeta^p=1} \hat{p}_k(\zeta) \geq \frac{z_p}{p} - o(1).$$

□

Concluding the proof of Theorem 1.1: Let $\delta > 0$. Let $0 < \epsilon < \delta/(1+\delta)$. Let k be an even integer sufficiently large such that $f(2, k, 4k(1+\delta)) \geq 0.5\binom{4k(1+\delta)}{k}(1-\epsilon)$. This holds for all sufficiently large k by Lemma 2.7 (we assume, w.l.o.g., that $4k(1+\delta)$ is an integer). Now, since $0.5(1-\epsilon) > (2k-1)/(4k(1+\delta))$ we get by Lemma 2.5 that $M(2,k) \leq 4k(1+\delta)$. Similarly, by using the third part of Lemma 2.5 and Lemma 2.7 we get that for k sufficiently large which is a power of 3, $f(3, k, 20k(1+\delta)) \geq \binom{20k(1+\delta)}{k} \frac{5k-3}{20k(1+\delta)}$, and so $M(3,k) \leq 20k(1+\delta)$. □

In case k is not a power of 3, the proof of Theorem 1.1 does not supply a linear $O(k)$ upper bound for $M(3,k)$. We can, however, use the following idea to supply an $O(k)$ upper bound when k is only slightly larger than a power of three. This is an immediate consequence of the next proposition. Recall that $B_r(p)$, the bipartite Ramsey number with r colors, is the minimum integer s for which in every r-coloring of the edges of $K_{s,s}$ there is a monochromatic $K_{p,p}$.

Proposition 2.8 *Let $k \geq B_p(p^2 - p + 1)$. Then,*

$$M(p, k+p) \leq \binom{p^2 - p + 1}{p} p(M(p,k) - 1) + p^2 - p.$$

Proof: Let $t = \binom{p^2-p+1}{p}p(M(p,k)-1)+p^2-p$. Clearly, $t \geq k \geq B_p(p^2-p+1)$. Let A be a square matrix of order t over $GF(p)$. Hence, A has a monochromatic square submatrix of order p^2-p+1. Since permuting columns and rows does not change the set of submatrices of A (up to permutations of columns and rows), we may assume that $A(i,j) = A(i',j')$ for all $i,j,i',j' = 1,\ldots,p^2-p+1$. Consider the set of $t-p^2+p-1$ vectors $a_i = (A_{1,i}, A_{2,i}, \ldots, A_{p^2-p+1,i})$ for $i = p^2-p+2,\ldots,t$. Each a_i contains some element of Z_p at least p times. Since $(t-p^2+p-1)/(\binom{p^2-p+1}{p}p) > M(p,k)-1$, there exists a subset of $s = M(p,k)$ vectors, $a_{i_1},\ldots,a_{i_s}$, and an element $q \in Z_p$, where each a_{i_x} contains q at least p times, in the same coordinates. The same idea can be applied on the $t-p^2+p-1$ partial row vectors $b_j = (A_{j,1}, A_{j,2}, \ldots, A_{j,p^2-p+1})$ for $j = p^2-p+2,\ldots,t$. Again, we obtain that there is a subset of s vectors $b_{j_1},\ldots,b_{j_s}$, and an element $q' \in Z_p$, where each b_{j_y} contains q' at least p times, in the same coordinates. Consider the square submatrix of order s which is defined by taking the columns $i_1,\ldots,i_s$ and the rows $j_1,\ldots,j_s$. By definition of $s = M(p,k)$ this submatrix contains another square submatrix of order k that is zero sum. Denote this submatrix by R and assume, w.l.o.g, that the columns of R are $i_1,\ldots,i_k$ and the rows are $j_1,\ldots,j_k$. Now, add the p rows corresponding to p common coordinates of the a_{i_x} which contain q, and add the p columns corresponding to the p common coordinates of the b_{j_y} which contain q'. The new matrix is a square matrix of order $k+p$ and is easily seen to be zero sum, since we added p identical elements to each previous row or column, and the $2p$ new rows and columns are also p-divisible. $\Box$

3 Lower bounds for $M(p,k)$

Proof of Theorem 1.4: We first show that $M(p,p) \geq B(p)$. Consider any square matrix of order t over $GF(p)$ whose entries are only zeroes and ones. Notice that in this case, any square submatrix of order p that is zero-sum mod p must be monochromatic. As mentioned in the introduction, there is a one-to-one correspondence between 0-1 square matrices and red-blue colorings of the edges of $K_{t,t}$, and thus, a square submatrix of order p is equivalent to a monochromatic copy of $K_{p,p}$ in the corresponding coloring of $K_{t,t}$. Thus, if $t \geq B(p)$, this implies the existence of such a submatrix. Hence, $M(p,p) \geq B(p)$. By (1) we have $B(p) > \sqrt{2}\mathrm{e}^{-1}p2^{p/2}$.

We now show that $M(2,k) \geq 2k+1$ for every positive even integer k. Consider the square binary matrix A of order $2k$ which is defined as follows: $A(i,i) = 1$ for $i = 1,\ldots,2k$ and $A(i,i+1) = 1$ for $i = 1,\ldots,2k-1$ and $A(2k,1) = 1$. All other entries are zero. It is an easy exercise to check that A has no square submatrix of order k all of whose rows and columns are even vectors.

Finally, we show that $M(p,k) \geq \frac{k\sqrt{2}}{2e}\exp(1/\mathrm{e})^{p/2}$. We shall need the following simplified form of the Chernoff bound (cf. [1] Appendix A): if X is a random variable with Bernoulli distribution $B(k,q)$ and $\mu \geq 1$, then

$$\Pr[X \geq \mu kq] < \left(\frac{\mathrm{e}^{\mu-1}}{\mu^\mu}\right)^{kq}.$$

Let A be a random 0-1 matrix of order t over $GF(p)$, where $\Pr[a_{ij} = 1] = p/ke$ independently for each element a_{ij}. If I is a set of k elements $(i,j) \in [n] \times [n]$, then $X = \sum_I a_{ij}$ is a random variable with Bernoulli distribution $B(k, p/ke)$. It follows that $\Pr[X = 0] = (1 - p/ke)^k < \exp(-p/e)$, and by the Chernoff bound mentioned above (with $\mu = e$), $\Pr[X \geq p] < \exp(-p/e)$. If $X \equiv 0 \pmod p$ then either $X = 0$ or $X \geq p$. Hence $\Pr[X \equiv 0 \pmod p] \leq 2\exp(-p/e)$. Thus for any fixed choice of k rows and k columns of A, the probability that each row sum is divisible by p in the resulting $k \times k$ submatrix is less than $(2\exp(-p/e))^k$. If A has a $k \times k$ submatrix that is zero-sum mod p, then it also has a submatrix in which each row sum is divisible by p. It follows that the probability $\Pr[E]$ that A has a $k \times k$ submatrix that is zero-sum mod p satisfies

$$\Pr[E] < \binom{t}{k}^2 (2\exp(-p/e))^k < \left(\left(\frac{te}{k} \right)^2 2\exp(-p/e) \right)^k .$$

Hence $\Pr[E] < 1$ provided

$$\frac{te}{k} \sqrt{2} \exp(-1/\mathrm{e})^{p/2} \leq 1,$$

and this gives the desired result. □

Acknowledgment

The authors thank Noga Alon for fruitful discussions.

References

[1] N. Alon and J. H. Spencer, *The Probabilistic Method*, John Wiley and Sons Inc., New York, 1991.

[2] B. Bollobás, *Extremal Graph Theory*, Academic Press, 1978.

[3] H. Enomoto, P. Frankl, N. Ito and N. Nomura, Codes with given distances, Graphs and Combinatorics 3 (1987).

[4] J. H. Hattingh and M. A. Henning, Bipartite Ramsey theory, Utilitas Math. 53 (1998), 217-230.

[5] J. E. Olson, *A combinatorial problem on finite abelian groups, I, II.* J. Number Theory 1 (1969), 8-10, 195-199.

[6] A. Thomason, *On finite Ramsey numbers*, European J. Combin. 3 (1982), 263-273.