A coding theory bound and zero-sum square matrices

Noga Alon * Simon Litsyn † Raphael Yuster ‡

Abstract

For a code $C = C(n, M)$ the *level* k code of C, denoted C_k, is the set of all vectors resulting from a linear combination of precisely k distinct codewords of C. We prove that if k is any positive integer divisible by 8, and $n = \gamma k$, $M = \beta k \geq 2k$ then there is a codeword in C_k whose weight is either 0 or at most $n/2 - n(\frac{1}{8\gamma} - \frac{6}{(4\beta-2)^2}) + 1$. In particular, if $\gamma < (4\beta - 2)^2/48$ then there is a codeword in C_k whose weight is $n/2 - \Theta(n)$. The method used to prove this result enables us to prove the following: Let k be an integer divisible by p, and let $f(k, p)$ denote the minimum integer guaranteeing that in any square matrix over Z_p, of order $f(k, p)$, there is a square submatrix of order k such that the sum of all the elements in each row and column is 0. We prove that $\liminf f(k, 2)/k < 3.836$. For general p we obtain, using a different approach, that $f(k, p) \leq p^{(k/\ln k)(1+o_k(1))}$.

1 Introduction

For standard coding theory notations the reader is referred to [6]. The *minimum weight* of a code C is the smallest Hamming weight of a codeword of C other than zero. Coding theory bounds such as Plotkin's bound or the Linear Programming bound show that if the dimension of a binary code is large enough as a function of its length, then some linear combination has a small Hamming weight. In other words, the code spanned by the codewords of C has small minimum weight. In this paper we present an alternative coding theory bound for the code obtained by *fixed size* linear combinations. For a positive integer k, let C_k denote the code obtained by linear combinations of precisely k distinct codewords of C. In particular, $C_1 = C$, and if C is a linear code then $C_k \subset C$. We call C_k the *level k code of* C. Let $w(C_k)$ denote the minimum weight of C_k. Notice that if k is odd then $w(C_k)$ can be very large. Indeed, consider a code $C = C(n, M)$ where M is the size of the code and n is the length of the codewords, and assume the first $n - \lceil \log M \rceil$ coordinates of

*School of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel. E–mail: nogaa@post.tau.ac.il

†Department of Electrical Engineering – Systems, Tel Aviv University, Tel Aviv, Israel.
E–mail: litsyn@yarkon.eng.tau.ac.il

‡Department of Mathematics, University of Haifa at Oranim, Tivon 36006, Israel.
E–mail: raphy@research.haifa.ac.il

all codewords are one. We can still have all M codewords distinct, and clearly, for such a code, $w(C_k) \geq n - \lceil \log M \rceil$ for all odd k. (If we allow C to contain repeated words we can even have all coordinates of all its members being 1). Thus, to avoid this non-interesting case, we assume k is even. For $M \geq k$, let $w(k,n,M)$ denote the maximum possible value of $w(C_k)$ ranging over all codes of size M and length n. A theorem of Enomoto et al. [3] shows that $w(k,k-1,M) = 0$ for $M \geq 2k$ and the result is tight. In general, however, no nontrivial bound is known. It is interesting to find general cases which guarantee that $w(k,n,M)$ is significantly less than $n/2$. In this paper we present a nontrivial bound of this type. Our main result is the following:

Theorem 1.1 *Let k be divisible by 8. Let $C = C(n,M)$ be any code with $M \geq 2k$. Put $M = \beta k$ and $n = \gamma k$. Then, either $0 \in C_k$ or else*

$$w(C_k) \leq \frac{n}{2} - n\left(\frac{1}{8\gamma} - \frac{6}{(4\beta-2)^2}\right) + 1.$$

In particular, if $\gamma < (4\beta-2)^2/48$ then $w(C_k) = n/2 - \Theta(n)$.

The constants appearing in Theorem 1.1 are not optimal. It is not difficult to obtain somewhat better constants for specific values of β and γ, but we prefer a general statement at the price of some loss in the constants. For example, Theorem 1.1 gives $w(64,800,640) \leq 396$ and $w(64,640,640) \leq 315$. Theorem 1.1 is an application of a more general technical lemma, Lemma 2.2 proved in Section 2, whose proof has another interesting application. Let A be a matrix over Z_p. A submatrix B of A is called *zero-sum* if the sum of all elements in each row and in each column of B is zero. Consider the following Ramsey-type extremal problem: Let $f(k,p)$ denote the least integer such that any square matrix of order $f(k,p)$ over Z_p has a square submatrix of order k which is zero-sum. Standard Ramsey-type arguments show that $f(k,p)$ is finite for all $k = 0 \bmod p$. If p does not divide k then the all one matrix shows that $f(k,p)$ is infinite. The problem of determining $f(k,p)$ was first raised in [1]. It is proved there that $\liminf f(k,2)/k \leq 4$, $\liminf f(k,2)/k \geq 2$ and $\liminf f(k,3)/k \leq 20$ (in fact, the authors show that $f(k,2) \leq 4k(1+o_k(1))$ for all even k). It is conjectured there that for every prime p, $\liminf f(k,p)/k \leq c_p$ where c_p is a constant depending only on p. The conjecture is open for all primes except $p = 2,3$. Using the proof method of Lemma 2.2 and the theorem of Enomoto et al. mentioned above we are able to show that $\liminf f(k,2)/k < 3.836$. We also present a nontrivial upper bound for $f(k,p)$ (which is, however, still very far from the conjectured $O(k)$ upper bound).

The rest of this note is organized as follows: In Section 2 we prove Theorem 1.1 and the lemmas that are needed for its proof. In Section 3 we present the application to zero-sum square matrices.

2 The proof of the main result

The main tool in the proof of Theorem 1.1 is a more general lemma whose proof is presented next. Before we state the lemma we need some definitions and notations. An *r-subvector* of a vector v

is obtained by picking r (not necessarily consecutive) coordinates of v. Let s and r be positive integers where $s \geq r$. For $v \in (Z_2)^s$ let $z_v(r)$ denote the fraction of r-subvectors of v whose sum of coordinates is odd. Let $z(s,r)$ denote the maximum of $z_v(r)$ ranging over all $v \in (Z_2)^s$. This quantity can be expressed in terms of the minimum possible value of the corresponding Krawchouk polynomial (see., e.g., [6] for the definition and some properties of these polynomials). Trivially, if r is odd then $z(s,r) = 1$. However, when r is even it is not difficult to show that when $s \geq r/2$, $z(s,r)$ is close to 0.5 for large s. We shall be interested, however, in more precise approximations and in fixed values of r. An easy exercise gives that $z(s,2) = s/(2(s-1))$ when s is even and $z(s,2) = (s+1)/(2s)$ when s is odd. However, for $r \geq 4$ there seems to be no nice formula.

Another tool that we use is a theorem of Enomoto et al. [3] also mentioned in the introduction:

Lemma 2.1 *[[3]] Let t be an even integer. If $s \leq t-1$ then any sequence of at least $2t$ vectors from $(Z_2)^s$ contains a t-subsequence whose sum is zero.* $\Box$

We are now ready to prove the following lemma.

Lemma 2.2 *Let $k = 0 \bmod 4$ and let r be any positive integer dividing $k/4$. Suppose $C = C(n,M)$ is a binary code with $M \geq k + k/(2r)$. Then, either $0 \in C_k$ or else*

$$w(C_k) \leq (n - k/(2r) + 1)z(\lfloor 2rM/k \rfloor - 1, 2r).$$

Proof: Partition each $v \in C$ into two parts, v_a and v_b where v_a consists of the first $k/(2r)-1$ coordinates, and v_b consists of the remaining coordinates (if $n \leq k/(2r)-1$ take $v_a = v$ and there is no v_b). Let $A = \{v_a \ : \ v \in C\}$ (although the vectors in A are not necessarily distinct, we consider each v_a as labeled by the original vector v, and in this sense, they are distinct). Since $k/(2r)$ is even and since $M \geq k/r$, we have, by Lemma 2.1, that there exists $A_1 \subset A$ with $|A_1| = k/(2r)$ such that the sum of all vectors in A_1 is zero. Throwing the vectors of A_1 away from A we can repeat this process and find another set of $k/(2r)$ vectors whose sum is zero. We can repeat this process precisely $d = \lfloor 2rM/k \rfloor - 1$ times obtaining subsets of vectors $A_1, \ldots, A_d$, that correspond to disjoint subsets of vectors of C, such that the sum of the $k/(2r)$ vectors in A_i is zero for $i = 1, \ldots, d$. Since $M \geq k + k/(2r)$ we have $d \geq 2r$. If $n \leq k/(2r) - 1$ we have that the sum of the vectors in $A_1, \ldots, A_{2r}$ is a sum of k distinct vectors of C. Since this sum is zero, we have $0 \in C_k$ and we are done. We therefore assume $n \geq k/(2r)$. Let $B_i = \{v_b \ : \ v_a \in A_i\}$. For each $j = 1, \ldots, n - k/(2r) + 1$ let $u_j = \{u_j^1, \ldots, u_j^d\}$ be defined by $u_j^i = \sum_{v_b \in B_i} v_b^j$. Let U_j denote the family of $(2r)$-sets of $\{1, \ldots, d\}$ for which the corresponding $(2r)$-subvector of u_j has an odd number of ones. By definition, $|U_j| \leq z(d,2r)\binom{d}{2r}$. Hence, $\sum_{j=1}^{n-k/(2r)+1} |U_j| \leq (n - k/(2r) + 1)z(d,2r)\binom{d}{2r}$. It follows that there exists a $(2r)$-set U such that if $B' = \cup_{i \in U} B_i$ then $\sum_{v_b \in B'} v_b$ contains at most $(n - k/(2r) + 1)z(d,2r)$ ones. Notice that $|B'| = 2rk/2r = k$. Now let $C' = \{v \ : \ v_b \in B'\}$. Clearly $\sum_{v \in C'} v \in C_k$ and has at most $(n - k/(2r) + 1)z(d,2r)$ ones. $\Box$

It is interesting to obtain general cases where $w(C_k)$ is significantly less than $n/2$. If we use Lemma 2.2 with $r = 1$ we can obtain such a statement only when $n < M$.

Proposition 2.3 *Let $k = 0 \bmod 4$. Suppose $\beta \geq 2$ is an integer. Then, for any code $C = C(n, M)$ with $M \geq \beta k$ and $n < \beta k$, $0 \in C_k$ or else $w(C_k) \leq n/2 - (\beta k - n)/(4\beta - 2) + 1$.*

Proof: Clearly we may assume $M = \beta k$. Put $n = \gamma k$. We use Lemma 2.2 with $r = 1$. Using the fact that $z(2\beta - 1, 2) = 1/2 + 1/(2(2\beta - 1))$ we get that either $0 \in C_k$ or else $w(C_k) \leq (n - k/2 + 1)(1/2 + 1/(2(2\beta - 1)))$. Now,

$$\left(n - \frac{k}{2} + 1\right)\left(\frac{1}{2} + \frac{1}{2(2\beta - 1)}\right) \leq k\left(\gamma - \frac{1}{2}\right)\left(\frac{1}{2} + \frac{1}{2(2\beta - 1)}\right) + 1 =$$

$$\frac{\gamma}{2}k - k\frac{\beta - \gamma}{2(2\beta - 1)} + 1 = \frac{n}{2} - \frac{\beta k - n}{4\beta - 2} + 1. \qquad \square$$

The real power of Lemma 2.2 is demonstrated when $r \geq 2$. In this case we can show that even if $n > M$ we can still have $w(C_k) \leq n/2 - \Theta(n)$. In fact, we can have n/M as large as we want, assuming M is sufficiently large (but still $M = O(k)$). It turns out that using $r = 2$ already suffices for this purpose. Before we complete the proof of Theorem 1.1, we need to provide a tight upper bound for $z(s, 4)$.

Lemma 2.4 *For $s \geq 7$, $z(s, 4) \leq 0.5 + 6/s^2$.*

Proof: Consider a binary vector of length s. Let x denote its Hamming weight. The number of 4-subvectors with an odd number of ones is $(s - x)\binom{x}{3} + x\binom{s-x}{3}$. Hence, we need to show that for all $s \geq 7$,

$$\frac{(s - x)\binom{x}{3} + x\binom{s-x}{3}}{\binom{s}{4}} \leq \frac{1}{2} + \frac{6}{s^2}.$$

Consider the numerator of the left-hand-side of the last inequality as a real polynomial (of degree 4) of x (which can be expressed in terms of the corresponding Krawchouk polynomial). Its derivative is a polynomial of degree 3, and $x = n/2$ is a root of the derivative and is a local minimum. The other two roots are local maxima (yielding the same value, and hence each is also a global maxima) and they are $(s \pm \sqrt{3s - 4})/2$. The value at these maxima is $s^4/48 - s^3/8 + 17s^2/48 - s/2 + 1/3$. Hence,

$$\frac{(s - x)\binom{x}{3} + x\binom{s-x}{3}}{\binom{s}{4}} \leq \frac{s^4/48 - s^3/8 + 17s^2/48 - s/2 + 1/3}{\binom{s}{4}} = \frac{1}{2} + \frac{s^2/8 - 3s/8 + 1/3}{\binom{s}{4}}.$$

It follows that for $s \geq 7$,

$$z(s, 4) \leq \frac{1}{2} + \frac{s^2/8 - 3s/8 + 1/3}{\binom{s}{4}} = \frac{1}{2} + \frac{3(s - 1)(s - 2) + 2}{s(s - 1)(s - 2)(s - 3)} =$$

$$\frac{1}{2}+\frac{3}{s(s-3)}+\frac{2}{s(s-1)(s-2)(s-3)} \leq \frac{1}{2}+\frac{6}{s^2}. \qquad \square$$

Proof of Theorem 1.1: Since $k = 0 \bmod 8$ we can use $r = 2$ in Lemma 2.2. Let $C = C(n, M)$ be any code with $M \geq 2k$. $M = \beta k$ and $n = \gamma k$. By Lemma 2.2, either $0 \in C_k$ or else $w(C_k) \leq (n - k/4 + 1)z(\lfloor 4\beta \rfloor - 1, 4)$. Assuming the latter, and since $\beta \geq 2$, we have $\lfloor 4\beta \rfloor - 1 \geq 7$, so using Lemma 2.4 we get

$$w(C_k) \leq (n-k/4+1)\left(\frac{1}{2}+\frac{6}{(\lfloor 4\beta \rfloor -1)^2}\right) < k\left(\gamma-\frac{1}{4}\right)\left(\frac{1}{2}+\frac{6}{(4\beta-2)^2}\right)+1 =$$

$$\frac{n}{2}-\frac{n}{8\gamma}+\frac{6n}{(4\beta-2)^2}-\frac{6k}{4(4\beta-2)^2}+1 < \frac{n}{2}-n\left(\frac{1}{8\gamma}-\frac{6}{(4\beta-2)^2}\right)+1. \qquad \square$$

It is easy to see from Theorem 1.1, that when M grows, our upper bound for $w(C_k)$ approaches $n/2 - n/(8\gamma)$. When M becomes very large we can gain some more as demonstrated by the following simple example: Suppose $m \geq 9n2^{0.1n}$, $n = \gamma k$ with, say, $\gamma \geq 1$. We can find $9n$ vectors that agree on the first $0.1n$ coordinates. Putting $M' = 9n$ and $n' = 0.9n$ we have $M' = 10n'$, $\gamma' = 0.9\gamma$ and $\beta' = 9\gamma$. By Theorem 1.1 we have

$$w(C_k) \leq \frac{n'}{2}-n'\left(\frac{1}{8\gamma'}-\frac{6}{(36\gamma-2)^2}\right)+1 = 0.45n-n\left(\frac{1}{8\gamma}-\frac{5.4}{(36\gamma-2)^2}\right)+1 \leq 0.45n-\frac{n}{9\gamma}+1.$$

3 Zero sum square matrices

In the following upper bound for $\liminf f(k,2)/k$ we use Lemma 2.2 without change. In fact, the following theorem supplies an upper bound for $f(k,2)$ valid for all $k = 0 \bmod 12$.

Theorem 3.1 *Let $k = 0 \bmod 12$. Every square binary matrix of order at least $50447k/13008 + 2221/2168$ has a square submatrix of order k which is zero sum. In particular $\liminf f(k,2)/k < 3.879$.*

Proof: Let A be a square binary matrix of order $n \geq 50447k/13008 + 2221/2168$. Clearly we may assume $n - 1 < 4k$. We consider the first $n-1$ rows of A as codewords of an $(n, n-1)$ binary code. Since $k = 0 \bmod 12$ we can use Lemma 2.2 with $r = 3$. Since $23 < 6(n-1)/k < 24$ we have, by Lemma 2.2, that there are k rows of A whose sum contains at most $(n - k/6 + 1)z(22, 6)$ ones. The maximum number of 6-subvectors with an odd number of ones of a vector $v \in (Z_2)^{22}$ is obtained when v has 5 or 17 ones and it is 37757. Thus, $z(22,6) = 37757/74613 = 2221/4389$. It follows that there are k rows of A whose sum has at least

$$n-\frac{2221}{4389}(n-\frac{k}{6}+1) = \frac{2168}{4389}n+\frac{2221}{26334}k-\frac{2221}{4389} \geq \frac{2168}{4389}\left(\frac{50447k}{13008}+\frac{2221}{2168}\right)+\frac{2221}{26334}k-\frac{2221}{4389} = 2k$$

zeroes. Thus, A has a submatrix B with k rows and $2k$ columns, such that the sum of all rows of B is zero. Ignoring the last row of B, and using Lemma 2.1 with $t = k$ and $s = k - 1$ we have a submatrix B' of B with k columns and k rows such that sum of all rows of B' is zero and the sum of all columns is a vector whose first $k-1$ coordinates are zero. However, the last coordinate must also be zero since the total number of ones in B' is even. Hence B' is a zero sum square submatrix of order k. $\square$

The choice of $r=3$ in the proof of Theorem 3.1 is optimal. A similar approach using $r=2$ yields the constant $144/37 > 3.89$ instead of the constant $50447/13008 < 3.879$ that appears in Theorem 3.1. However, using $r=2$ applies to all $k = 0 \bmod 8$. Using values of $r \geq 4$ again yields inferior results. This is because $z(s,r) \geq 0.5$, by a simple probabilistic argument. Now if $r \geq 5$ take $n = 3.89k$ and then the number of ones in the sum of the k rows guaranteed by Lemma 2.2 is not less than $(3.9k - k/2r)/2 \geq 1.9k$ so there are less than $3.89k - 1.9k < 2k$ guaranteed zeroes and we cannot define B as in the proof of Theorem 3.1. Thus, even a constant of 3.89 cannot be guaranteed in this way. For $r=4$ one can check specifically that the obtained constant is inferior.

A slightly better upper bound for $\liminf f(k,2)/k$ is obtained using the following idea, that supplies an upper bound for $f(k,2)$ valid for large k that is of the form $k = 12q$ where q is a prime power. The following coding theory bound has been proved by Bassalygo et al. in [2] using a theorem of Frankl and Wilson [5]:

Lemma 3.2 *Let $\lambda \leq 0.5$. For every n sufficiently large, if λn is twice a prime power and C is a linear code of dimension dn that does not contain the weight λn then*

$$d \leq 1 - H(\lambda) + H(\lambda/2)$$

where $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy. $\square$

We therefore obtain the following corollary:

Corollary 3.3 *For every sufficiently large m for which $m/2$ is a prime power, the following holds: Every binary matrix with $\lceil 1.41m \rceil$ rows and $\lceil 5.95m \rceil$ columns has m columns whose sum is the zero vector of $(Z_2)^{\lceil 1.41m \rceil}$.*

Proof: Choose m sufficiently large such that $n = \lceil 5.95m \rceil$ is sufficiently large for the parameter $\lambda = m/n \leq 1/5.95$ in Lemma 3.2 and so that $\lambda > 1/5.9449$. Let A be a binary matrix with $\lceil 1.41m \rceil$ rows and n columns. Consider the linear code C whose parity check matrix is A. The dimension of C is at least $n - \lceil 1.41m \rceil > 4.54m - 1 > 0.763n$. Now, since

$$1 - H(\lambda) + H(\lambda/2) < 0.763$$

it follows from Lemma 3.2 that C contains the weight $\lambda n = m$. In particular, there are m columns whose sum is zero. $\square$

Corollary 3.3, together with (a slightly modified) version of Lemma 2.2 give the following:

Theorem 3.4 *For k sufficiently large for which $k/12$ is a prime power, $f(k,2) < 3.836k + 1$.*

Proof: Assume m is sufficiently large and chosen as in Corollary 3.3. Put $k = 6m$. Let A be a square matrix of order $t > 3.836k = 23.016m$. By Corollary 3.3 we can arrange the rows of A such that the sum of all m rows $sm+1, \ldots, (s+1)m$ is zero in the first $\lceil 1.41m \rceil$ coordinates, for each $s = 0, \ldots, 17$. For each of these 18 sums, let S_i denote the vector corresponding to the remaining $t - \lceil 1.41m \rceil$ coordinates of the corresponding sum vector. As in Lemma 2.2, we can find a set of 6 vectors of the S_i such that their sum has at most $z(18,6)(t - \lceil 1.41m \rceil)$ ones. This implies the existence of $6m = k$ rows of A whose sum has at least $t - z(18,6)(t - \lceil 1.41m \rceil)$ zeroes. Since $z(18,6) = 26/51$ we have $t - z(18,6)(t - \lceil 1.41m \rceil) \geq 12m = 2k$. Thus, A has a submatrix B with k rows and $2k$ columns, such that the sum of all rows of B is zero. As in Theorem 3.1 we get that there exists a zero sum square submatrix B' of order k. $\Box$

We note here that use of Lemma 3.2 allows improvement on the coding bound of Theorem 1.1. However, the conditions on the length are much more restrictive. We omit the details.

We conclude this section with an upper bound for $f(k,p)$. In fact, our upper bound follows from a proposition which is a (weak) analog of the theorem of Enomoto et al. for Z_p instead of Z_2. For k a multiple of p, let $g(k,p)$ be the minimum integer that guarantees that in any sequence of $g(k,p)$ elements of $(Z_p)^k$ there is a k-subsequence whose sum is zero. The theorem of Enomoto et al. gives, almost immediately, that $g(k,2) \leq 4k-1$ for all even k. In fact, using a theorem of Olson [7] we can get $g(k,2) \leq 2k+1$ whenever k is a power of 2. In [1] it is proved that $g(k,3) \leq 15k-8$ if k is a power of 3 (no linear bound is known for all k divisible by 3). For $p > 3$ there is no known linear bound for $g(k,p)$ which holds for infinitely many values of k. A trivial upper bound is obviously $(k-1)p^k + 1$. A much smaller upper bound (but still, a non polynomial one) is given in the following theorem:

Proposition 3.5 *Let p be a fixed prime. For infinitely many values of k, $g(k,p) \leq p^{(k/\ln k)(1+o_k(1))}$.*

Proof: Let r be a positive integer. Let k be the smallest integer such that k/p is divisible by all $1 \leq s \leq r$. Clearly, k/p is obtained by multiplying appropriate powers of all primes q up to r, where each prime q is raised to the maximum power x_q for which $q^{x_q} \leq r$. Hence $k/p < r^{\pi(r)}$ where $\pi(r)$ is the number of primes up to r. It is well known that $\pi(r) \leq (1+o(1))r/\ln r$, and hence $k/p < e^{r(1+o_r(1))}$. Now, suppose m satisfies $\binom{m-kr^2}{r} \geq p^k r^r p^{r+1}$. We claim that $g(k,p) \leq m$. Consider a sequence of m vectors from $(Z_p)^k$. By the pigeonhole principle, there is a family T of at least $t \geq p^{r+1}r^r$ r-subsequences, such that for each $U \in T$, the sum of all r vectors of U is the same. It is well-known that in any family of at least $(p-1)^{r+1}r! < t$ distinct (but non necessarily disjoint) sets, each with r elements, there is a delta system with p petals [4]. In other words, there are p sets in the family such that the common intersection of all of them is identical to the intersection of any two of them. Hence, there are $U_1, \ldots, U_p \in T$, where $\cap_{i=1}^{p} = S$ and $(U_i \setminus S) \cap (U_j \setminus S) = \emptyset$ for $i \neq j$. Putting $W_i = U_i \setminus S$ we have that the sum of all the vectors in W_i is the same for all $i = 1, \ldots, p$. Hence the sum of all vectors in $\cup_{i=1}^{p} W_i$ is zero (in Z_p). Now,

$r \geq |W_i| = r - |S| \geq 1$. Putting $r - |S| = q_1$ we have found $q_1 p$ distinct vectors whose sum is zero. Recall that k is divisible by $q_1 p$. Deleting these $q_1 p$ vectors and repeating this process kr/p times we have kr/p disjoint subsequences of $q_i p$ vectors for $i = 1, \ldots, kr/p$, such that the sum of the vectors in each subsequence is zero. There exist some $1 \leq s \leq r$ such that $q_i = s$ for at least k/p distinct values of i. As $k/(ps) < k/p$ is an integer, we can select $k/(ps)$ sequences of size sp each. The union of these sequences is a sequence of k vectors whose sum is zero, as required. Now, $m = p^{(k/\ln k)(1+o_k(1))}$ satisfies $\binom{m-kr^2}{r} \geq p^k r^r p^{r+1}$ and the result follows. $\square$

It remains to show the relation between $f(k,p)$ and $g(k,p)$. Let $z(s,k,p)$ denote the minimum possible fraction of k-subvectors of a vector $v \in (Z_p)^s$ whose sum is divisible by p. This generalizes the definition of $z(s,k) = 1 - z(s,k,2)$ appearing in Section 2. It is proved in [1] that $z(s,k,p) \geq 2^{1-p}(1-o_k(1))$ for $k \leq s/2$. This, together with an immediate counting argument, shows that in any matrix over Z_p with $s \geq 2k$ rows and t columns there is a submatrix with k rows and $t2^{1-p}(1-o_k(1))$ columns such that the sum of the rows is zero. By definition of $g(k,p)$, if $t2^{1-p}(1-o_k(1)) \geq g(k,p)$ then there is a square zero-sum submatrix of order k. Since $t > s$, it follows that any square matrix of order t over Z_p has a square submatrix of order k which is zero-sum. Hence $f(k,p) \leq 2^{p-1} g(k,p)(1+o_k(1))$. By Proposition 3.5 we have that for infinitely many values of k, $f(k,p) \leq 2^{p-1} p^{(k/\ln k)(1+o_k(1))} = p^{(k/\ln k)(1+o_k(1))}$.

References

[1] P. Balister, Y. Caro, C. Rousseau and R. Yuster, *Zero-sum square matrices*, European J. Combin. 23 (2002), 489–497.

[2] L. Bassalygo, G. Cohen and G. Zémor, *Codes with forbidden distances*, Discrete Mathematics 213 (2000), 3–11.

[3] H. Enomoto, P. Frankl, N. Ito and N. Nomura, Codes with given distances, Graphs and Combinatorics 3 (1987), 25–38.

[4] P. Erdős and R. Rado, *Intersection theorems for systems of sets*, J. London Math. Soc. 35 (1960), 85–90.

[5] P. Frankl and R.M. Wilson, *Intersection theorems with geometric consequences*, Combinatorica 1 (1981), 357–368.

[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, New York, 1977.

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