



# On the size of partial block designs with large blocks

András Sárközy<sup>a,1</sup>, Gábor N. Sárközy<sup>b,c,2</sup>

<sup>a</sup>*Department of Algebra and Number Theory, Eötvös University, Pázmány Péter sétány 1/c, H-1117 Budapest, Hungary*

<sup>b</sup>*Computer Science Department, Worcester Polytechnic Institute, Worcester, MA 01609, USA*

<sup>c</sup>*Computer and Automation Research Institute, Hungarian Academy of Sciences, Budapest, P.O. Box 63, H-1518 Budapest, Hungary*

Received 28 September 2005; accepted 28 September 2005

Available online 16 November 2005

---

## Abstract

A  $t - (n, k, \lambda)$  design is a  $k$ -uniform hypergraph with the property that every set of  $t$  vertices is contained in exactly  $\lambda$  of the edges (blocks). A partial  $t - (n, k, \lambda)$  design is a  $k$ -uniform hypergraph with the property that every set of  $t$  vertices is contained in *at most*  $\lambda$  edges; or equivalently the intersection of every set of  $\lambda + 1$  blocks contains fewer than  $t$  elements. Let us denote by  $f_\lambda(n, k, t)$  the maximum size of a partial  $t - (n, k, \lambda)$  design. We determine  $f_\lambda(n, k, t)$  as a fundamental problem in design theory and in coding theory. In this paper we provide some new bounds for  $f_\lambda(n, k, t)$ .

© 2005 Elsevier B.V. All rights reserved.

*Keywords:* Partial block designs

---

## 1. Introduction

### 1.1. Notation and definitions

A *hypergraph*  $H$  is a set  $V(H)$ , whose elements are called vertices, and a set  $E(H)$  of subsets of  $V(H)$ , whose elements are called edges. A hypergraph is  *$k$ -uniform* if each of its edges contains exactly  $k$  vertices.

---

*E-mail addresses:* [sarkozy@cs.elte.hu](mailto:sarkozy@cs.elte.hu) (A. Sárközy), [gsarkozy@cs.wpi.edu](mailto:gsarkozy@cs.wpi.edu) (G.N. Sárközy).

<sup>1</sup> Research supported in part by the Hungarian National Foundation for Scientific Research, Grant no. T043623.

<sup>2</sup> Research supported in part by the National Science Foundation under Grant no. DMS-0456401.

A  $t - (n, k, \lambda)$  design is a  $k$ -uniform hypergraph on  $n$  vertices with the property that every set of  $t$  vertices is contained in exactly  $\lambda$  of the edges (blocks). A *partial*  $t - (n, k, \lambda)$  design is a  $k$ -uniform hypergraph on  $n$  vertices with the property that every set of  $t$  vertices is contained in *at most*  $\lambda$  edges; or equivalently the intersection of every set of  $\lambda + 1$  blocks contains fewer than  $t$  elements. (Partial)  $t - (n, k, 1)$  designs are often called (partial) *Steiner systems*. Let us denote by  $f_\lambda(n, k, t)$  the maximum size of a partial  $t - (n, k, \lambda)$  design.

A *binary code*  $C$  consists of bit vectors (codewords) of length  $m$ , where the *weight*  $w(\mathbf{e})$  of a vector  $\mathbf{e}$  is equal to the number of ones in  $\mathbf{e}$ . If  $\mathbf{x}$  and  $\mathbf{y}$  are codewords, then their *distance*  $d(\mathbf{x}, \mathbf{y})$  is the number of places where they differ, i.e.  $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$ . Then the *minimum distance* of code  $C$  is the minimal value of  $d(\mathbf{x}, \mathbf{y})$  for all pairs of distinct codewords.

In this paper  $\log n$  denotes the natural logarithm. We will also use the standard notation  $e(\alpha) = e^{2\pi i \alpha}$ .

### 1.2. On the size of block designs

Determine  $f_\lambda(n, k, t)$  as a fundamental problem; it is studied in various forms. It is sometimes also referred to as the packing problem for hypergraphs. It is also related to the Turán problem for hypergraphs, the lottery problem, the football pool problem, etc. It is also a fundamental problem in coding theory. Determine  $f_1(n, k, t)$  as equivalent to finding the maximum size  $A(n, d, k)$  of a binary code with word length  $n$ , constant weight  $k$  and minimum distance  $d \geq 2(k - t + 1)$ .

Since this is such a fundamental question, there is a vast literature on results concerning  $f_\lambda(n, k, t)$  (see e.g. [2,7] or [9]). The majority of the results concentrate on the case when  $k$  and  $t$  are “small”. For example, simple counting shows that for the number of edges in any partial Steiner system we have

$$f_1(n, k, t) \leq \frac{\binom{n}{k}}{\binom{k}{t}}.$$

In a breakthrough paper [10], Rödl developed the nibble technique in order to prove the conjecture of Erdős and Hanani [3], which asserts that for every fixed  $k \geq t > 0$  and  $n \rightarrow \infty$  we have

$$f_1(n, k, t) = (1 - o(1)) \frac{\binom{n}{k}}{\binom{k}{t}}.$$

In this paper we are interested in the other extreme, namely when  $k$  is large:  $\varepsilon n < k \leq (1 - \varepsilon)n$  for some  $\varepsilon > 0$ . We will define  $c$  by  $k = cn$  so that  $0 < c < 1$ . In particular, we are interested in what happens when  $t$  is around the “expected value” of the intersection of  $\lambda + 1$  blocks. Assuming that we selected the  $\lambda + 1$  blocks randomly, this expected value is  $c^{\lambda+1}n$ .

Fundamental results in coding theory (see [6]) imply that for  $k = cn$ , the function  $f_1(n, k, t)$  is polynomial in  $n$  for  $t \leq c^2n + 1$ , and exponential for  $t \geq (c^2 + \varepsilon)n$  for any  $\varepsilon > 0$ . In addition, the well-known Johnson bound (see [5] or [6]) gives the following upper

bound for this polynomial:

$$f_1(n, k, t) \leq \frac{k - (t - 1)n}{k^2 - (t - 1)n}, \quad (1)$$

assuming that the denominator is positive. Thus for  $k = cn$ , assuming that  $t < c^2n + 1$ , we get a linear upper bound

$$f_1(n, k, t) \leq \frac{cn - (t - 1)}{c^2n - (t - 1)}. \quad (2)$$

It is known that the Johnson bound (1) is sometimes sharp. For example, in an old (and somewhat forgotten) paper, answering a question of Erdős, et al. [11] determine exactly this function  $f_1(n, k, t)$  for infinitely many  $n$ 's in the special case  $k = n/2$  and  $t = n/4$ . More precisely, they give infinitely many  $m$ 's for which

$$f_1(4m, 2m, m) = m + 1; \quad (3)$$

indeed, they show that if  $m = (p - 1)/2$  where  $p$  is a prime with  $p \equiv -1 \pmod{4}$  then (3) holds. Here the upper bound comes from (1), and for the lower bound they construct a design using quadratic residues and non-residues. Since we will use this construction here as well, for the sake of completeness, we give the construction in Section 2.2.

In this paper we give some new (to the best of our knowledge) bounds for  $f_\lambda(n, k, t)$  for  $k = cn$ . We think of  $c$  and  $\lambda$  as constants and we let  $n \rightarrow \infty$ . First we prove a general upper bound, which is a generalization of the Johnson bound for  $\lambda \geq 1$ .

**Theorem 1.** *Let  $1 \leq k < n$ ,  $\lambda \geq 1$ ,  $t$  positive integers and  $c = k/n$ . Then we have*

$$f_\lambda(n, k, t) \leq \frac{c^\lambda n - (t - 1)}{c^{\lambda+1}n - (t - 1)} \binom{\lambda + 1}{2}, \quad (4)$$

*provided that the denominator is positive.*

Note that in the  $\lambda = 1$  special case this gives the Johnson bound (2).

Then we prove some lower bounds. First we examine for the special case  $\lambda = 1$ ,  $k = n/2$ , how close to the truth the Johnson bound is if we let  $t$  to be smaller than the expected value,  $n/4$ . The next construction shows that the Johnson bound is sharp in this case as well for infinitely many  $n$ 's.

**Theorem 2.** *For every integer  $d \geq 0$  there are infinitely many integers  $m > 0$ , for which*

$$f_1(4(d + 1)m, 2(d + 1)m, (d + 1)m - d) = m + 1,$$

*and, indeed, this holds if  $m = (p - 1)/2$  where  $p$  is a prime with  $p \equiv -1 \pmod{4}$ .*

Again here the upper bound comes from the Johnson bound, the lower bound uses an iterated version of the quadratic residue construction from (3).

In the next construction we let  $\lambda = 1$ ,  $\varepsilon n \leq k \leq n/2$  for some constant  $\varepsilon > 0$ ,  $c = k/n$  and  $t = \lfloor c^2n \rfloor$  (the expected value).

**Theorem 3.** Let  $\varepsilon > 0$  be a fixed constant, and  $\varepsilon n \leq k \leq n/2$ ,  $t = \lfloor c^2 n \rfloor$  positive integers, where  $c = k/n$ . Then there exists an integer  $n_0 = n_0(\varepsilon)$  such that for  $n \geq n_0$  we have

$$f_1(n, k, t) \geq \frac{\varepsilon^2}{16} \frac{\sqrt{n}}{\log n}. \quad (5)$$

Here, unfortunately there is a significant gap between this lower bound and the Johnson upper bound (2).

In the next construction we will consider any  $\lambda \geq 1$ , but, on the other hand,  $t$  will be slightly greater than the expected value.

**Theorem 4.** Let  $n = p$  be a prime number,  $\lambda, d, r$  positive integers with  $\lambda < n$ ,  $d \mid (p-1)$  and  $r < d$ , and write  $k = r((p-1)/d)$ . Then there is a number  $C_1 = C_1(\lambda, d, r)$  (to be computed later) so that writing  $c = k/n$  and  $t = \lfloor c^{\lambda+1} n + C_1 \sqrt{n} \rfloor$  we have

$$f_\lambda(n, k, t) = f_\lambda\left(p, r \frac{p-1}{d}, t\right) \geq n = p. \quad (6)$$

In the next section we provide the tools including some general tools and the quadratic residue construction from (3). Then in Section 3 we give the proofs.

## 2. Tools

### 2.1. General tools

Our first tool is the well-known Chernoff bound from probability theory. Let  $X_1, \dots, X_N$  be  $N$  independent random variables which are equal to one with probability  $\bar{p}$ , and zero with probability  $1 - \bar{p}$ . The random variable  $X = X_1 + \dots + X_N$  is called the binomial random variable (or the random variable with binomial distribution), and is denoted by  $\text{BIN}(N, \bar{p})$ . It is clear that the expected value of  $\text{BIN}(N, \bar{p})$  is  $N\bar{p}$ . The Chernoff bound estimates the probability of large deviation from the expected value.

**Lemma 1.** For any  $0 \leq r \leq N\bar{p}$ , we have

$$\Pr(|\text{BIN}(N, \bar{p}) - N\bar{p}| > r) < 2e^{-r^2/3N\bar{p}}.$$

The proof can be found in [1].

Our next tool is a theorem for multiplicative characters due to Weil [12], see also [4,8].

**Lemma 2.** Let  $p$  be a prime number, let  $\chi$  be a nontrivial character of order  $d$  (so that  $d \mid (p-1)$ ), and let  $f \in \mathbf{F}_p[x]$  be a polynomial of positive degree which is not a constant multiple of the  $d$ th power of a polynomial. Let  $m$  be the number of distinct roots of  $f$ . Then we have

$$\left| \sum_{x \in \mathbf{F}_p} \chi(f(x)) \right| \leq (m-1)\sqrt{p}.$$

## 2.2. The quadratic residue construction

For the lower bound in (3) it is sufficient to construct a design with blocks  $A_1, A_2, \dots, A_{m+1}$  that are subsets of  $\{1, 2, \dots, 4m\}$  and satisfy

$$|A_i| = 2m, \quad i = 1, 2, \dots, m + 1, \quad (7)$$

and

$$|A_i \cap A_j| < m, \quad 1 \leq i < j \leq m + 1. \quad (8)$$

Let  $p$  be a prime number with  $p \equiv -1 \pmod{4}$  (note that by Dirichlet's Theorem there are infinitely many primes with this property) and let  $n = 2p - 2 = 4m$ .

Recall that the Legendre symbol  $(n/p)$  is equal to  $+1$ , if  $n$  is a quadratic residue modulo  $p$ , and  $-1$  if  $n$  is a quadratic non-residue, while for  $p|n$  it is undefined. First we define by using the Legendre symbol a  $p \times p$  matrix  $C = [c_{ik}]$ ,  $1 \leq i \leq p$ ,  $1 \leq k \leq p$  in the following way:

$$c_{ik} = \begin{cases} 1 & \text{if } \left(\frac{i+k}{p}\right) = +1, \\ 0 & \text{if } \left(\frac{i+k}{p}\right) = -1 \text{ or } p|(i+k), \end{cases}$$

for  $i = 1, 2, \dots, p$ ;  $k = 1, 2, \dots, p$ .

Next we modify the matrix  $C$  in the following way. First we remove from  $C$  those  $(p-1)/2$  columns whose last entry is a one (note that the last row of  $C$ , as any row, contains  $(p+1)/2$  zeros and  $(p-1)/2$  ones). Then from the obtained  $p \times ((p+1)/2)$  matrix we remove the last row (consisting of zeros only). Denote the resulting  $(p-1) \times ((p+1)/2)$  matrix by  $D = d_{ik}$ ,  $1 \leq i \leq p-1$ ,  $1 \leq k \leq (p+1)/2$ .

Finally, let us define the  $(2p-2) \times ((p+1)/2) = n \times (m+1)$  matrix  $E = e_{ik}$ ,  $1 \leq i \leq 2p-2$ ,  $1 \leq k \leq (p+1)/2$  in the following way.

$$e_{ik} = \begin{cases} d_{ik} & \text{if } 1 \leq i \leq p-1, \\ d_{(i-p+1)k} & \text{if } p \leq i \leq 2p-2, \end{cases}$$

for  $i = 1, 2, \dots, (2p-2) = n$ ;  $k = 1, 2, \dots, (p+1)/2 = m+1$ . Thus we get the matrix  $E$  by writing  $D$  under itself again.

Now we are ready to give the construction of the blocks  $A_1, A_2, \dots, A_{m+1}$ :

$$i \in A_k \quad \text{if and only if } e_{ik} = 1.$$

It is not hard to check that for this construction both (7) and (8) hold.

## 3. Proofs

### 3.1. Proof of Theorem 1

Let  $1 \leq k \leq n/2$ ,  $\lambda \geq 1$ ,  $t < c^{\lambda+1}n + 1$  be positive integers, where  $c = k/n$ , so  $c \leq \frac{1}{2}$ . Let us consider a  $t - (n, k, \lambda)$  design with blocks  $A_1, A_2, \dots, A_N$  from the set  $\{a_1, a_2, \dots, a_n\}$ .

We will prove by contradiction; assume indirectly that in contrary to (4) we have

$$N > \frac{c^\lambda n - (t - 1)}{c^{\lambda+1} n - (t - 1)} \binom{\lambda + 1}{2}. \tag{9}$$

For a given  $l$  let us denote by  $N_l$  the number of those blocks  $A_1, A_2, \dots, A_N$  that contain  $a_l$ .

Let us start with the following equation:

$$\sum_{1 \leq i_1 < i_2 < \dots < i_{\lambda+1} \leq N} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_{\lambda+1}}| = \sum_{l=1}^n \binom{N_l}{\lambda + 1}. \tag{10}$$

Indeed, we get (10) by counting in two different ways for each vertex the number of  $(\lambda + 1)$ -set intersections it is contained in.

Furthermore, we clearly have

$$\sum_{l=1}^n N_l = kN = cnN,$$

and thus by the Jensen inequality we get

$$\sum_{l=1}^n \binom{N_l}{\lambda + 1} \geq n \binom{\frac{\sum_{l=1}^n N_l}{n}}{\lambda + 1} = n \binom{cN}{\lambda + 1}. \tag{11}$$

Combining (10) and (11) and using the  $(t - 1)$  upper bound for the size of the  $(\lambda + 1)$ -set intersections we get

$$n \binom{cN}{\lambda + 1} \leq (t - 1) \binom{N}{\lambda + 1}.$$

From this we obtain

$$ncN(cN - 1)(cN - 2) \dots (cN - \lambda) \leq (t - 1)N(N - 1)(N - 2) \dots (N - \lambda).$$

Multiplying this out results in

$$N^{\lambda+1}(c^{\lambda+1}n - (t - 1)) \leq (c^\lambda n - (t - 1)) \binom{\lambda + 1}{2} N^\lambda + \sum_{i=1}^{\lambda-1} c_i N^{\lambda-i}, \tag{12}$$

where we have

$$c_i = (-1)^i (c^{\lambda-i} n - (t - 1)) \sum_{1 \leq j_1 < j_2 < \dots < j_{i+1} \leq \lambda} j_1 j_2 \dots j_{i+1},$$

for  $i = 1, 2, \dots, \lambda - 1$ .

Next we claim that the terms in the summation in (12) are alternating in sign starting with a negative term, and their absolute values are non-increasing. For this purpose we only have to show

$$|c_i|N \geq |c_{i+1}| \quad \text{for } i = 1, 2, \dots, \lambda - 2 \tag{13}$$

or

$$\begin{aligned}
 & (c^{\lambda-i}n - (t-1))N \sum_{1 \leq j_1 < j_2 < \dots < j_{i+1} \leq \lambda} j_1 j_2 \dots j_{i+1} \\
 & \geq (c^{\lambda-i-1}n - (t-1)) \sum_{1 \leq j_1 < j_2 < \dots < j_{i+2} \leq \lambda} j_1 j_2 \dots j_{i+2} \\
 & \text{for } i = 1, 2, \dots, \lambda - 2.
 \end{aligned} \tag{14}$$

Since we have

$$\begin{aligned}
 \sum_{1 \leq j_1 < j_2 < \dots < j_{i+2} \leq \lambda} j_1 j_2 \dots j_{i+2} & \leq \sum_{1 \leq j_1 < j_2 < \dots < j_{i+1} \leq \lambda} j_1 j_2 \dots j_{i+1} \sum_{j=1}^{\lambda} j \\
 & = \sum_{1 \leq j_1 < j_2 < \dots < j_{i+1} \leq \lambda} j_1 j_2 \dots j_{i+1} \binom{\lambda+1}{2},
 \end{aligned}$$

in order to show (14), it is sufficient to show

$$(c^{\lambda-i}n - (t-1))N \geq (c^{\lambda-i-1}n - (t-1)) \binom{\lambda+1}{2}$$

or

$$N \geq \frac{c^{\lambda-i-1}n - (t-1)}{c^{\lambda-i}n - (t-1)} \binom{\lambda+1}{2}. \tag{15}$$

Note that

$$\frac{c^{\lambda}n - (t-1)}{c^{\lambda+1}n - (t-1)} \geq \frac{c^{\lambda-i-1}n - (t-1)}{c^{\lambda-i}n - (t-1)}. \tag{16}$$

Indeed, this simplifies to

$$1 \geq c + c^{i+1} - c^{i+2},$$

which is always true for  $c < 1$ ,  $i \geq 1$ .

But then (15) follows from (9) and (16).

The above implies that in (12) the negative terms “cancel” the positive terms, and thus (12) simplifies to

$$N^{\lambda+1}(c^{\lambda+1}n - (t-1)) \leq (c^{\lambda}n - (t-1)) \binom{\lambda+1}{2} N^{\lambda},$$

which contradicts (9) and this completes the proof of the theorem.

(Our proof also shows that in (4) equality can only be obtained for  $\lambda = 1$ .)

### 3.2. Proof of Theorem 2

We get the upper bound from the Johnson bound

$$\frac{2(d+1)m - ((d+1)m - d - 1)}{(d+1)m - ((d+1)m - d - 1)} = m + 1.$$

For the lower bound we iterate the quadratic residue construction from Section 2.2. Indeed, we do the following. Let  $d \geq 0$  be an arbitrary integer and let  $p$  be a prime number with  $p \equiv -1 \pmod{4}$  and let  $n = (d + 1)(2p - 2) = 4(d + 1)m$ . We divide the integers  $\{1, 2, \dots, n\}$  into  $(d + 1)$  intervals  $I_i = [4(i - 1)m + 1, 4im]$ ,  $1 \leq i \leq d + 1$ , and in each interval  $I_i$  we use the quadratic residue construction. More precisely, we define the blocks  $B_1, B_2, \dots, B_{m+1}$  from  $\{1, 2, \dots, n\}$  in the following way. Let

$$B_j \cap [4(i - 1)m + 1, 4im] = A_j + 4(i - 1)m, \quad 1 \leq i \leq d + 1,$$

for all  $1 \leq j \leq m + 1$ . Here  $A_j$  denote the blocks from the quadratic residue construction, and  $A_j + 4(i - 1)m$  means that we add  $4(i - 1)m$  to every element of  $A_j$ .

Thus we get blocks  $B_1, B_2, \dots, B_{m+1}$  from  $\{1, 2, \dots, n\}$  such that

$$|B_j| = 2(d + 1)m, \quad j = 1, 2, \dots, m + 1$$

and

$$|B_i \cap B_j| \leq (d + 1)m - (d + 1), \quad 1 \leq i < j \leq m + 1,$$

implying the lower bound in the theorem.

### 3.3. Proof of Theorem 3

Let  $\varepsilon > 0$  be a fixed constant, and  $\varepsilon n \leq k \leq n/2$ ,  $t = \lfloor c^2 n \rfloor$  positive integers, where  $c = k/n$ , so  $\varepsilon \leq c \leq 1/2$ . Let us assume that  $n$  is sufficiently large.

The proof will start out similarly to the proof of Theorem 2, we will iterate the quadratic residue construction. Let  $p$  be a prime number such that  $p \equiv -1 \pmod{4}$  and

$$\frac{\varepsilon^2}{8} \frac{\sqrt{n}}{\log n} \leq p - 1 \leq \frac{\varepsilon^2}{4} \frac{\sqrt{n}}{\log n}. \tag{17}$$

The prime number theorem for arithmetic progressions guarantees that there is a prime with these properties for sufficiently large  $n$ . Let  $m = (p - 1)/2$  and  $l = \lfloor n/4m \rfloor$ . Thus from (17) we get

$$\frac{\varepsilon^2}{16} \frac{\sqrt{n}}{\log n} \leq m \leq \frac{\varepsilon^2}{8} \frac{\sqrt{n}}{\log n} \tag{18}$$

and

$$\frac{1}{\varepsilon^2} \sqrt{n} \log n \leq l \leq \frac{4}{\varepsilon^2} \sqrt{n} \log n. \tag{19}$$

We divide the integers  $\{1, 2, \dots, n\}$  into  $(l + 1)$  intervals  $I_i$ ,  $1 \leq i \leq l + 1$ , such that  $I_i = [4(i - 1)m + 1, 4im]$ ,  $1 \leq i \leq l$ , and  $I_{l+1} = [4lm + 1, n]$  if  $4lm < n$ , and  $I_{l+1} = \emptyset$  otherwise.

First, again in each interval  $I_i$ ,  $1 \leq i \leq l$ , we do the quadratic residue construction. More precisely, we define the blocks  $B_1, B_2, \dots, B_{m+1}$  from  $\{1, 2, \dots, 4lm\}$  in the following

way. Let

$$B_j \cap [4(i-1)m+1, 4im] = A_j + 4(i-1)m, \quad 1 \leq i \leq l,$$

for all  $1 \leq j \leq m+1$ , where again  $A_j$  denote the blocks from the quadratic residue construction. Thus we get blocks  $B_1, B_2, \dots, B_{m+1}$  that are subsets of  $\{1, 2, \dots, 4lm\}$  such that

$$|B_j| = 2lm, \quad j = 1, 2, \dots, m+1$$

and

$$|B_j \cap B_{j'}| \leq l(m-1), \quad 1 \leq j < j' \leq m+1. \quad (20)$$

To get the final design consisting of blocks  $C_1, C_2, \dots, C_{m+1}$  we do the following.  $C_j^1$  will be a random subset of size  $\lfloor 4clm \rfloor$  from  $B_j$ .  $C_j^2$  will be a random subset of size  $k - \lfloor 4clm \rfloor$  from  $I_{l+1}$  assuming that  $I_{l+1} \neq \emptyset$ , otherwise  $C_j^2 = \emptyset$ . Let  $C_j = C_j^1 \cup C_j^2$ , and thus

$$|C_j| = k, \quad j = 1, 2, \dots, m+1,$$

as desired. In view of (18), in order to prove the theorem it only remains to estimate the pairwise intersections  $|C_j \cap C_{j'}|$  for  $1 \leq j < j' \leq m+1$ .

Using the Chernoff bound (Lemma 1) with  $r = \sqrt{n} \log n$  and (20) we get

$$\Pr \left( \left| |C_j^1 \cap B_j \cap B_{j'}| - |C_j^1| \frac{|B_j \cap B_{j'}|}{|B_j|} \right| > r \right) \leq 2e^{-r^2/3lm} \leq 2e^{-r^2/n} \leq 2n^{-\log n}.$$

Fix a choice of  $C_j^1$  for which we have

$$\left| |C_j^1 \cap B_j \cap B_{j'}| - |C_j^1| \frac{|B_j \cap B_{j'}|}{|B_j|} \right| \leq r.$$

Again by the Chernoff bound we get

$$\Pr \left( \left| |C_{j'}^1 \cap C_j^1| - |C_{j'}^1| \frac{|C_j^1 \cap B_j \cap B_{j'}|}{|B_{j'}|} \right| > r \right) \leq 2e^{-r^2/3lm} \leq 2e^{-r^2/n} \leq 2n^{-\log n}.$$

Finally, if  $I_{l+1} \neq \emptyset$ , we get by the Chernoff bound

$$\Pr \left( \left| |C_{j'}^2 \cap C_j^2| - |C_{j'}^2| \frac{|C_j^2|}{|I_{l+1}|} \right| > r \right) \leq 2e^{-r^2/n} \leq 2n^{-\log n}.$$

Thus for sufficiently large  $n$  we get that with high probability we have for every pair  $1 \leq j < j' \leq m + 1$  (assuming  $I_{l+1} \neq \emptyset$  and using (19), (20))

$$\begin{aligned} |C_j \cap C_{j'}| &= |C_j^1 \cap C_{j'}^1| + |C_j^2 \cap C_{j'}^2| \\ &\leq \frac{|C_{j'}^1|}{|B_{j'}|} \left( \frac{|C_j^1|}{|B_j|} |B_j \cap B_{j'}| + r \right) + r + \frac{|C_{j'}^2|}{|I_{l+1}|} |C_j^2| + r \\ &\leq 2c(2cl(m-1) + r) + r + \frac{cn - 4clm + 1}{n - 4lm} (cn - 4clm + 1) + r \\ &= c^2 4ml - 4c^2 l + 2cr + r + \left( c + \frac{1}{n - 4ml} \right) (c(n - 4ml) + 1) + r \\ &\leq c^2 n - 4c^2 l + 3r + 2 < c^2 n - 4c^2 l + 4r - 1 \leq \lfloor c^2 n \rfloor - 1 = t - 1, \end{aligned}$$

as desired.

### 3.4. Proof of Theorem 4

We have to show that there are  $p$  blocks  $A_1, \dots, A_p$  which are subsets of the vertex set  $V = \{1, 2, \dots, p\}$  so that

$$|A_l| = k = r \frac{p-1}{d} \quad \text{for } l = 1, 2, \dots, p \tag{21}$$

and

$$\begin{aligned} |A_{l_1} \cap A_{l_2} \cap \dots \cap A_{l_{\lambda+1}}| &< t = \lfloor c^{\lambda+1} p + C_1 \sqrt{p} \rfloor \\ &\text{for } 1 \leq l_1 < l_2 < \dots < l_{\lambda+1} \leq p. \end{aligned} \tag{22}$$

Let  $\chi$  be a (multiplicative) character of order  $d$  modulo  $p$ ; e.g. if  $g$  is a primitive root modulo  $p$ , then we may define such a character  $\chi$  by

$$\chi(g^k) = e\left(\frac{k}{d}\right) \quad \text{for } k = 1, 2, \dots$$

Let  $E$  be a set consisting of  $r$  distinct  $d$ th roots of unity, e.g. we may take  $E = \{e(1/d), e(2/d), \dots, e(r/d)\}$ . Then we define the blocks  $A_1, \dots, A_p \subset V$  by

$$\text{for } 1 \leq i, l \leq p \text{ we have } i \in A_l \text{ if and only if } \chi(l+i) \in E. \tag{23}$$

Clearly, we have

$$\begin{aligned} |A_l| &= |\{i : 1 \leq i \leq p, \chi(l+i) \in E\}| = |\{j : 1 \leq j \leq p, \chi(j) \in E\}| \\ &= \sum_{\varepsilon \in E} |\{j : 1 \leq j \leq p, \chi(j) = \varepsilon\}| = \sum_{\varepsilon \in E} \frac{p-1}{d} = |E| \frac{p-1}{d} = r \frac{p-1}{d}, \end{aligned}$$

which proves (21).

Now we will prove (22). Write  $\phi(z) = 1 + z + z^2 + \dots + z^{d-1}$ . Observe that if  $\varepsilon$  is a  $d$ th root of unity then we have

$$\phi(\varepsilon) = \begin{cases} d & \text{if } \varepsilon = 1, \\ 0 & \text{if } \varepsilon \neq 1. \end{cases}$$

By (23), it follows that

$$\sum_{\varepsilon \in E} \frac{1}{d} \phi(\bar{\varepsilon} \chi(l+i)) = \sum_{\substack{\varepsilon \in E \\ \chi(l+i)=\varepsilon}} 1 = \begin{cases} 1 & \text{if } i \in A_l, \\ 0 & \text{if } i \notin A_l. \end{cases}$$

Hence

$$\begin{aligned} & \prod_{j=1}^{\lambda+1} \sum_{\varepsilon_j \in E} \frac{1}{d} \phi(\bar{\varepsilon}_j \chi(l_j+i)) \\ &= \frac{1}{d^{\lambda+1}} \prod_{j=1}^{\lambda+1} \sum_{\varepsilon_j \in E} \sum_{h_j=0}^{d-1} (\bar{\varepsilon}_j \chi(l_j+i))^{h_j} \\ &= \frac{1}{d^{\lambda+1}} \sum_{h_1=0}^{d-1} \cdots \sum_{h_{\lambda+1}=0}^{d-1} s(h_1, \dots, h_{\lambda+1}) \chi((l_1+i)^{h_1} \cdots (l_{\lambda+1}+i)^{h_{\lambda+1}}) \\ &= \begin{cases} 1 & \text{if } i \in A_{l_1} \cap \cdots \cap A_{l_{\lambda+1}}, \\ 0 & \text{if } i \notin A_{l_1} \cap \cdots \cap A_{l_{\lambda+1}}, \end{cases} \end{aligned}$$

where

$$s(h_1, \dots, h_{\lambda+1}) = \sum_{\varepsilon_1 \in E} \cdots \sum_{\varepsilon_{\lambda+1} \in E} \varepsilon_1^{-h_1} \cdots \varepsilon_{\lambda+1}^{-h_{\lambda+1}},$$

so that

$$s(0, \dots, 0) = |E|^{\lambda+1} = r^{\lambda+1} \quad (24)$$

and

$$|s(h_1, \dots, h_{\lambda+1})| \leq s(0, \dots, 0) = r^{\lambda+1}, \quad (25)$$

for all  $h_1, \dots, h_{\lambda+1}$ .

Thus we have

$$\begin{aligned} & |A_{l_1} \cap \cdots \cap A_{l_{\lambda+1}}| \\ &= \sum_{i=1}^p \frac{1}{d^{\lambda+1}} \sum_{h_1=0}^{d-1} \cdots \sum_{h_{\lambda+1}=0}^{d-1} s(h_1, \dots, h_{\lambda+1}) \chi((l_1+i)^{h_1} \cdots (l_{\lambda+1}+i)^{h_{\lambda+1}}) \\ &= \frac{1}{d^{\lambda+1}} \sum_{h_1=0}^{d-1} \cdots \sum_{h_{\lambda+1}=0}^{d-1} s(h_1, \dots, h_{\lambda+1}) \sum_{i=1}^p \chi((l_1+i)^{h_1} \cdots (l_{\lambda+1}+i)^{h_{\lambda+1}}). \quad (26) \end{aligned}$$

By (24), the contribution of the  $h_1 = \cdots = h_{\lambda+1} = 0$  term is

$$\frac{r^{\lambda+1}}{d^{\lambda+1}} \sum_{i=1}^p 1 = \left(\frac{r}{d}\right)^{\lambda+1} p,$$

and by Lemma 2 for every other  $h_1, \dots, h_{\lambda+1}$  we have

$$\left| \sum_{i=1}^p \chi((l_1 + i)^{h_1} \cdots (l_{\lambda+1} + i)^{h_{\lambda+1}}) \right| \leq (h_1 + \cdots + h_{\lambda+1} - 1)\sqrt{p} < ((\lambda + 1)(d - 1) - 1)\sqrt{p} < 2\lambda d\sqrt{p}.$$

Thus separating the  $h_1 = \cdots = h_{\lambda+1} = 0$  term in (26), by (25) it follows from (26) that

$$\begin{aligned} |A_{l_1} \cap \cdots \cap A_{l_{\lambda+1}}| &\leq \left(\frac{r}{d}\right)^{\lambda+1} p + \frac{1}{d^{\lambda+1}} \sum_{\substack{0 \leq h_1, \dots, h_{\lambda+1} < d \\ (h_1, \dots, h_{\lambda+1}) \neq (0, \dots, 0)}} r^{\lambda+1} 2\lambda d\sqrt{p} \\ &= \left(\frac{r}{d}\right)^{\lambda+1} p + 2\lambda r^{\lambda+1} d\sqrt{p}. \end{aligned} \tag{27}$$

Observing that, by Bernoulli’s inequality, now

$$\begin{aligned} c^{\lambda+1} n &= \left(\frac{k}{n}\right)^{\lambda+1} n = \left(\frac{r(p-1)}{dp}\right)^{\lambda+1} p = \left(\frac{r}{d}\right)^{\lambda+1} \left(1 - \frac{1}{p}\right)^{\lambda+1} p \\ &> \left(\frac{r}{d}\right)^{\lambda+1} \left(1 - \frac{\lambda+1}{p}\right) p > \left(\frac{r}{d}\right)^{\lambda+1} p - (\lambda+1). \end{aligned} \tag{28}$$

(22) follows from (27) and (28) with  $C_1 = 3\lambda r^{\lambda+1} d$ , and this completes the proof of Theorem 4.

### References

- [1] N. Alon, J.H. Spencer, *The Probabilistic Method*, Wiley, New York, 1992.
- [2] A.E. Brouwer, Block designs, *Handbook of Combinatorics*, Elsevier, Amsterdam, 1995, pp. 693–745 (Chapter 14).
- [3] P. Erdős, H. Hanani, On a limit theorem in combinatorial analysis, *Publ. Math. Debrecen* 10 (1963) 10–13.
- [4] I. Honkala, A. Tietäväinen, Codes and number theory, *Handbook of Coding Theory*, Elsevier, Amsterdam, 1998, pp. 1141–1194 (Chapter 13).
- [5] S.M. Johnson, A new upper bound for error correcting codes, *IRE Trans. Inform. Theory* IT-8 (1962) 203–207.
- [6] V.I. Levenshtein, Universal bounds for codes and designs, *Handbook of Coding Theory*, Elsevier, Amsterdam, 1998, pp. 449–648 (Chapter 6).
- [7] J.H. van Lint, Codes, *Handbook of Combinatorics*, Elsevier, Amsterdam, 1995, pp. 773–807 (Chapter 16).
- [8] C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences, I., Measure of pseudorandomness, the Legendre symbol, *Acta Arith.* 82 (1997) 365–377.
- [9] V. Pless, W.C. Huffman (Eds.), *Handbook of Coding Theory*, Elsevier, Amsterdam, 1998.
- [10] V. Rödl, On a packing and covering problem, *European J. Combin.* 6 (1985) 69–78.
- [11] A. Sárközy, E. Szemerédi, On the intersections of subsets of finite sets, *Mat. Lapok* 21 (3–4) (1970) 269–278 (in Hungarian with an English abstract).
- [12] A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci. USA* 34 (1948) 204–207.