

## ON $(n, k, l, \Delta)$ -SYSTEMS

by STEPHEN D. COHEN and NIKOLAI N. KUZJURIN

(Received 13th January 1993)

The paper is devoted to studying one generalization of Steiner systems  $S(n, k, l)$  closely related to packings and coverings of  $l$ -tuples by  $k$ -tuples of an  $n$ -set. One necessary and one sufficient condition for the existence of such designs are obtained.

1980 Mathematics subject classifications: 05B07, 11T06.

### 1. Introduction

We consider  $(n, k, l, \Delta)$ -systems which are the generalization of Steiner systems  $S(n, k, l)$ .

**Definition.** A system  $P$  of  $k$ -tuples of an  $n$  element set  $S$  is called an  $(n, k, l, \Delta)$ -system iff every  $l$ -tuple of  $S$  is contained in at most one  $k$ -tuple from  $P$  and every  $(l - \Delta)$ -tuple of  $S$  is contained in at least one  $k$ -tuple from  $P$ .

Obviously, every  $(n, k, l, 0)$ -system is a Steiner system  $S(n, k, l)$ , i.e. a system of  $k$ -tuples of an  $n$ -element set such that every  $l$ -tuple is contained in exactly one  $k$ -tuple from the system. It is well known that the problem of finding the values  $(n, k, l)$  such that Steiner systems  $S(n, k, l)$  exist is a very difficult problem. Until now such values  $n > k > l > 5$  are still unknown. Only for  $l = 2, l = 3$  are infinite sequences of Steiner systems known (see [6, 16, 20, 21, 22, 4, 9–11, 17, 8]).

On the other hand  $(n, k, l, \Delta)$ -systems are also related to packings and coverings of  $l$ -tuples of an  $n$ -set by its  $k$ -tuples [6]. Recall that a system  $Q$  of  $k$ -tuples of an  $n$ -element set  $S$  is called an  $(n, k, l)$ -packing iff every  $l$ -tuple of  $S$  is contained in at most one  $k$ -tuple from  $Q$ , and a system  $P$  of  $k$ -tuples of an  $n$  element set  $S$  is called an  $(n, k, l)$ -covering iff every  $l$ -tuple of  $S$  is contained in at least one  $k$ -tuple from  $P$ . By definition an  $(n, k, l, \Delta)$ -system is simultaneously an  $(n, k, l)$ -packing and an  $(n, k, l - \Delta)$ -covering.

There are well-known simple inequalities which restrict the domain of values  $k - l$  for which Steiner systems can exist: for example, if  $l \geq 2$  and  $n > k$  then

$$(k - l + 1)(k - l + 2) \leq n - l + 1 \tag{1.1}$$

and a generalized Fisher's inequality holds (see, for example, [16]). To prove (1.1) we can fix  $l - 1$  elements of an  $n$  element set and consider all  $k$ -tuples from the Steiner system that contain these  $l - 1$  elements. If we delete from such  $k$ -tuples these  $l - 1$  elements we obtain the partition of the  $(n - l + 1)$ -set into  $(k - l + 1)$ -subsets. We consider

now the  $k$ -tuple from the Steiner system that intersects our  $l-1$  elements at  $l-2$  elements. The inequality (1.1) follows now from the fact that this  $k$ -tuple must intersect each  $(k-l+1)$ -subset of partition in at most one element.

From (1.1) it immediately follows that non-trivial Steiner systems  $S(n, k, l)$  can exist only if

$$k - l < \sqrt{n} \tag{1.2}$$

holds.

The  $(n, k, l-\Delta)$ -systems seem a much wider class of combinatorial objects than the Steiner systems  $S(n, k, l)$ . However, as we show in this paper, for  $(n, k, l, \Delta)$ -systems a necessary condition similar to (1.1) also holds. As we noted above it is very difficult to obtain sufficient conditions for the existence of  $(n, k, l, 0)$ -systems for arbitrary values  $l$  because  $(n, k, l, 0)$ -systems are simply Steiner systems  $S(n, k, l)$ . Using a result of S. D. Cohen on the number of solutions of one algebraic system over a finite field we obtain a sufficient condition for the existence of  $(n, k, l, \Delta)$ -systems for  $\Delta \geq 2$ .

The paper is organized as follows. In Section 2 we prove the necessary condition for the existence of  $(n, k, l, \Delta)$ -systems. In Section 3 we give the sufficient conditions for the existence of  $(n, k, l, \Delta)$ -systems for  $\Delta=2$  and  $\Delta \geq 3$ . For the sake of completeness in Section 4 we give the brief description of S. D. Cohen’s algebraical result which is the key to obtain these sufficient conditions.

**2. Necessary condition for the existence of  $(n, k, l, \Delta)$ -systems**

Here and in the sequel we suppose that  $n > k > l \geq \Delta + 2$ . In this section the following necessary condition will be formulated and proved.

**Theorem 1.** *If the inequality*  

$$(k - l + \Delta + 2)(k - l + 1) > (\Delta + 1)(n - l + \Delta + 1) \tag{2.1}$$

*holds, then  $(n, k, l, \Delta)$ -systems do not exist.*

**Proof.** We can use now the fact that an  $(n, k, l, \Delta)$ -system is a packing of  $l$ -tuples of an  $n$  element set by its  $k$ -tuples. For the maximal cardinality  $m(n, k, t)$  of an  $(n, k, t)$ -packing Johnson’s bound [14] holds. So

$$m(n, k, t) \leq \frac{n(k-t+1)}{n(k-t+1) - k(n-k)} \tag{2.2}$$

provided the denominator is positive; that is  $k^2 > (t-1)n$ .

Now we will show that  $(n, k, l, \Delta)$ -systems do not exist if (2.1) holds. This is a corollary from the inequality (2.2) and the recurrent inequality [14]:

$$m(n, k, l) \leq \frac{n}{k} m(n-1, k-1, l-1).$$

Actually this inequality immediately implies

$$m(n, k, l) \leq \frac{\binom{n}{l-\Delta-2}}{\binom{k}{l-\Delta-2}} m(n-l+\Delta+2, k-l+\Delta+2, \Delta+2). \tag{2.3}$$

We apply (2.2) to the last term of (2.3), i.e. to  $m(n-l+\Delta+2, k-l+\Delta+2, \Delta+2)$ . The denominator is positive if

$$(k-l+\Delta+2)^2 > (\Delta+1)(n-l+\Delta+2) \tag{2.4}$$

holds or equivalently

$$(k-l+\Delta+2)(k-l+1) > (\Delta+1)(n-k).$$

If this inequality does not hold then nothing need be proved. So assume that (2.4) holds. Under this condition we can derive the following:

$$\begin{aligned} & m(n-l+\Delta+2, k-l+\Delta+2, \Delta+2) \\ & \leq \frac{(n-l+\Delta+2)(k-l+1)}{(n-l+\Delta+2)(k-l+1) - (k-l+\Delta+2)(n-k)} \\ & \leq \frac{(n-l+\Delta+2)(k-l+1)}{(k-l+1)(k-l+2+\Delta) - (\Delta+1)(n-k)} \\ & \leq \frac{1}{1 - \frac{(\Delta+1)(n-k)}{(k-l+1)(k-l+\Delta+2)}} \frac{n-l+2+\Delta}{k-l+2+\Delta}. \end{aligned}$$

From this inequality and (2.3) we can derive the following inequality:

$$m(n, k, l) \leq \frac{\binom{n}{l-\Delta-1}}{\binom{k}{l-\Delta-1}} \frac{1}{1 - \frac{(\Delta+1)(n-k)}{(k-l+1)(k-l+\Delta+2)}}. \tag{2.5}$$

On the other hand any  $(n, k, l, \Delta)$ -system is an  $(n, k, l-\Delta)$ -covering. This implies that the cardinality of an  $(n, k, l, \Delta)$ -system is at least  $\binom{n}{l-\Delta} / \binom{k}{l-\Delta}$  and for the existence of such systems (see 2.5) the inequality

$$\frac{\binom{n}{l-\Delta-1}}{\binom{k}{l-\Delta-1}} \frac{1}{1 - \frac{(\Delta+1)(n-k)}{(k-l+1)(k-l+\Delta+2)}} \geq \frac{\binom{n}{l-\Delta}}{\binom{k}{l-\Delta}}$$

must hold. But this implies that

$$1 - \frac{(\Delta+1)(n-k)}{(k-l+1)(k-l+\Delta+2)} \leq \frac{k-l+\Delta+1}{n-l+\Delta+1}$$

and after routine simplifications we obtain the inequality

$$(k-l+\Delta+2)(k-l+1) \leq (\Delta+1)(n-l+\Delta+1).$$

Combining this inequality with (2.4) we obtain the desired bound. The proof is complete.

To compare this result with (1.2) we can use the rougher estimate:

**Corollary.** *If  $(n, k, l, \Delta)$ -systems exist then*

$$k-l \leq \sqrt{(\Delta+1)n}. \tag{2.6}$$

This inequality is a direct generalization of the necessary condition (1.2).

### 3. Sufficient conditions for the existence of $(n, k, l, \Delta)$ -systems

In Section 2 we noted that if  $\Delta=0$  then it is very difficult to obtain sufficient conditions for the existence of  $(n, k, l, \Delta)$ -systems for arbitrary values  $l$  because  $(n, k, l, \Delta)$ -systems are simply Steiner systems  $S(n, k, l)$  in this case. In this section we give sufficient conditions for the existence of  $(n, k, l, \Delta)$ -systems for  $\Delta \geq 3$  and  $\Delta=2$ . Let  $s=k-l$ .

**Theorem 2.** *Let  $k \leq cn/(s+3)$  and  $s \leq c_1 \log n / \log \log n$  for some constants  $c < 1$  and  $c_1 < 1/2$ . Then for all  $\Delta \geq 3$  and sufficiently large  $n$  there exist  $(n, k, l, \Delta)$ -systems.*

**Proof.** Let  $l=k-s$ . We consider as  $k$ -tuples of an  $(n, k, k-s, \Delta)$ -system for  $\Delta \geq 3$  all solutions of the system of equations:

$$\sum_{i=1}^k x_i^t \equiv a_t \pmod p, \quad t = 1, \dots, s. \tag{3.1}$$

where  $x_i \neq x_j, x_i \in \{0, 1, \dots, n-1\}, 1 \leq i < j \leq k$  and  $p$  is the minimal prime such that  $p \geq n$ .

It is not difficult to see that the  $k$ -tuples corresponding to all the solutions of such a

system form an  $(n, k, k-s)$ -packing (see, for example, [7, 15]). One  $k$ -tuple corresponds to  $k!$  solutions because all functions in our system are symmetric. Our goal now is to prove that it is an  $(n, k, k-s-3)$ -covering. Let us fix the first  $k-s-3$  variables in the system (3.1), say  $x_i = j_i, i = 1, \dots, k-s-3$ . We obtain a system of  $s$  equations with  $s+3$  variables. The number of possibilities to fix the first  $k-s-3$  variables such that

$$x_i \neq x_j, x_i \in \{0, 1, \dots, n-1\}, 1 \leq i < j \leq k-s-3$$

is  $(n)_{k-s-3} = n(n-1) \cdots (n-k+s+4)$ . We wish to estimate now the number of solutions of the system (3.1) under fixed values  $j_1, \dots, j_{k-s-3}$  of the first  $k-s-3$  variables and the conditions:

$$x_i \neq x_j, i \neq j \text{ and } x_i \notin \{j_1, \dots, j_{k-s-3}\}, i = k-s-2, \dots, k$$

for some fixed set  $\{j_1, \dots, j_{k-s-3}\}$ .

In order to do this we use the result of S. D. Cohen (see [2, 3] and the next section) which shows that for the number  $T$  of solutions of the system (3.1) without the restrictions  $x_i \in \{0, 1, \dots, n-1\}$  for  $k-s=2$  or 3 the following inequality holds:

$$|T - p^{k-s}| \leq \frac{k}{2} k! p^{k-s-1/2}. \tag{3.2}$$

If  $k-s \geq 4$ , at worst the right side of (3.2) needs to be doubled. Using this result for  $k-s=3$  we obtain that for this case the number of solutions is  $p^3 + (c(s+3)/2)(s+3)!p^{5/2}$  for some constant  $c, |c| < 1$ . So the total number of solutions with the first  $k-s-3$  variables arbitrarily fixed can be represented in the form

$$p^3 + c \frac{s+3}{2} (s+3)! p^{5/2}. \tag{3.3}$$

In order to obtain only solutions with restrictions:

$$x_i \neq x_j, 1 \leq i < j \leq k \text{ and } x_i \in \{0, 1, \dots, n-1\}$$

we must subtract from the value (3.3) two terms corresponding to the following cases:

(1) the number of solutions satisfying the condition  $x_i \in \{j_1, \dots, j_{k-s-3}\}$  for some  $i \in \{k-s-2, \dots, k\}$  and fixed set  $\{j_1, \dots, j_{k-s-3}\}$ .

This number is at most

$$(s+3)(k-s-3) \left( p^2 + \frac{s+2}{2} (s+2)! p^{3/2} \right). \tag{3.4}$$

(2) the number of solutions satisfying the condition  $x_i \in \{n, \dots, p-1\}$  for some  $i \in \{k-s-2, \dots, k\}$ .

This number is at most

$$(s+3)(p-n) \left( p^2 + \frac{s+2}{2}(s+2)!p^{3/2} \right). \tag{3.5}$$

So if the sum of the last two terms ((3.4 and (3.5)) is smaller than (3.3) then there exists at least one solution of (3.1) such that  $x_i \neq x_j, 1 \leq i < j \leq k$  and  $x_i \in \{1, \dots, n\}$  for  $1 \leq i \leq k$ . Because known results on the difference between consecutive primes (see, for example, [13]), imply that  $p-n \leq n^c$  for some constant  $c < 1$ , it is not difficult to check that this inequality holds under the conditions of Theorem 2.

This means that the set of  $k$ -tuples corresponding to all the solutions of such a system is an  $(n, k, k-s-3)$ -covering and so it is an  $(n, k, l, \Delta)$ -system for  $\Delta \geq 3$ . The proof of Theorem 2 is complete.

For the case  $\Delta=2$  we can prove the sufficient condition in the following form.

**Theorem 3.** *Let  $k \leq cn/(s+2)!$  and  $s \leq c_1 \log n / \log \log n$  for some constants  $c < 1$  and  $c_1 < 1/2$ . Then for  $\Delta=2$  and all sufficiently large  $n$  there exist  $(n, k, l, \Delta)$ -systems.*

The proof is quite similar to the proof of Theorem 2 with one difference: we fix values not of  $k-s-3$  but of the first  $k-s-2$  variables and for the system of  $s$  equations with  $s+1$  indeterminates we use the trivial upper bound  $p(s+1)!$  for the number of its solutions.

**Remark 1.** The assertions of Theorems 2 and 3 can be easily reformulated as sufficient conditions not for sufficiently large  $n$  only but for all  $n$ . The form of these conditions can be derived from the proof of Theorem 2.

**Remark 2.** For  $\Delta=1$  in [15] it was shown that  $(n, k, k-1, \Delta)$ -systems exist if  $k \leq (n/2) + 1$ .

**4. Bounds for the number of solutions of one algebraic system**

For the sake of completeness we give in this section a brief description of the result of S. D. Cohen on the number of solutions of one system of algebraic equations over a finite field. As it was shown above this result is the key to obtain the sufficient conditions for the existence of  $(n, k, l, \Delta)$ -systems for the case  $\Delta \geq 2$ .

Let  $\mathbb{F}_p = GF(p), p$  prime. Let  $k, s$  be positive integers with  $1 \leq s \leq k \leq p$ . Let  $l = k - s$  and assume  $l \leq 2$ . Write  $N(k, s)$  for the number of solutions of the system:

$$\sum_{i=1}^k x_i^t \equiv a_t \pmod p, t = 1, \dots, s, \tag{4.1}$$

where  $x_i \neq x_j, 1 \leq i < j \leq k$ .

We shall give a brief description of the following result of S. . Cohen ([2, 3]).

**Theorem 4.** *Let  $l = k - s \geq 2$ . Then*

$$|N(k, s) - p^l| \leq (k/2)k!p^{l-1/2},$$

except perhaps if  $l \geq 4$  and  $k^2/2 < p^{1/2} < k^2$ , in which case the right hand side should be doubled.

**Proof.** We give only a sketch of the proof which should be read along with [2], [3]. Fairly trivial estimates suffice unless  $k < p^{1/4}$  which can therefore be assumed. Let  $s_j$  be the  $j$ th symmetric function of  $x_1, \dots, x_k$ . Then the set of all solutions of (4.1) (with distinct components) is the subset of  $\mathbb{F}_p^k$  comprising those  $x$  with distinct components such that  $(-1)^j s_j$  has a prescribed value  $b_j$  for  $j = 1, \dots, s$ . Here  $b_1 = -a_1, b_2 = (1/2)(a_1^2 - a_2), \dots$

Let

$$f(x) = x^k + b_1 x^{k-1} + \dots + b_{k-1} x \in \mathbb{F}_p[x],$$

where  $b_1, \dots, b_s$  are the prescribed values and  $b = (b_{s+1}, \dots, b_{k-1}) \in \mathbb{F}_p^{l-1}$  is arbitrary. Then

$$N(k, s) = k! \sum_{b \in \mathbb{F}_p^{l-1}} M(b) \tag{4.2}$$

where  $M(b)$  denotes the number of  $a$  in  $\mathbb{F}_p$  such that  $f(x) + a$  splits completely into a product of  $k$  distinct linear factors over  $\mathbb{F}_p$ .

Rather than estimate  $M(b)$  in every case, we restrict ourselves to those  $b$  in the set

$$\mathbf{B} = \{b \in \mathbb{F}_p^{l-1} : f' \text{ has } k-1 \text{ distinct roots in } \overline{\mathbb{F}}_p \text{ all giving rise to distinct values}\}.$$

Here  $\overline{\mathbb{F}}_p$  is the algebraic closure of  $\mathbb{F}_p$ .

By Lemma 5 of [2],  $|\mathbf{B}| \geq p^{l-1} - cp^{l-2}$ , where  $c = c(k, s)$  is independent of  $p$ . The arguments of Lemmas 6 and 7 of [2] show that none of the polynomial equations which arise are identities and we can routinely bound their number of solutions. More specifically, but briefly, as regards Lemma 6 of [2], the relevant polynomials can be totally composite only if they are polynomials in  $x^d$  for some  $d > 1$  and this excludes at most  $lp^{l-2}$  elements ( $(l-1)$ -tuples) of  $\mathbf{B}$ . On the other hand, solutions of (5.4) and (5.6) exclude, between them, for each  $j$  (with  $1 \leq j \leq l-1$ ) at most  $3kp^{l-2}$  elements, and so a total of at most  $3lkp^{l-2}$  elements. Further, using the bound in Bezout's theorem, for each  $j \leq l-1$ , (5.8) of [2] excludes  $(k+j-3)(k-1)$  elements from  $\mathbf{B}$  and so  $(l-1)(k-1)(k+l/2-3)$  altogether. This gives the following lemma;

**Lemma.** *The size of  $\mathbf{B}$  satisfies*

$$|\mathbf{B}| \geq p^{l-1} - c(k, l)p^{l-2},$$

where

$$\begin{aligned}
 c(k, 2) &= k^2 + 3k + 4, \\
 c(k, 3) &= 2k^2 + 4k + 6, \\
 c(k, l) &\leq lk \binom{l}{k + \frac{l}{2}}, \quad l \geq 4.
 \end{aligned}$$

Now for  $b \in \mathbf{B}$ ,  $M(b)$  can be interpreted as the number of  $a$  in  $\mathbb{F}_p$  such that  $t+a$  is unramified and splits completely into first degree primes in  $E$ , the splitting field of  $f(x)+t$  over  $\mathbb{F}_p(t)$ . Since the Galois group of  $f(x)+t$  over  $\mathbb{F}_p(t)$  is  $S_k$  [1] and so has order  $k!$  we conclude that  $k!M(b)$  is exactly the number of first degree prime divisors of  $E$  which divide a finite unramified first degree prime  $t+a$  of  $\mathbb{F}_p(t)$ . On the other hand, by Weil’s theorem (which applies since  $\mathbb{F}_p$  is algebraically closed in  $E$ ), the total number of first degree prime divisors of  $E$  differs from  $p$  by at most  $2g\sqrt{p}$ , where  $g$  is the genus of  $E$ . So we obtain for  $b \in \mathbf{B}$

$$|k!M(b) + T - p| \leq 2g\sqrt{p}, \tag{4.3}$$

where  $T$  is the number of first degree prime divisors in  $E$  which are infinite or ramified.

Moreover, by Proposition 5.15 of [5], the ramification index of every finite ramified prime in  $E$  is 2 and the ramification index of the infinite prime is  $k$ . Using the definition of  $\mathbf{B}$ , this means that the relative different of  $E$  over  $\mathbb{F}_p(t)$  has degree

$$d = \frac{(k-1)k!}{2} + (k-1)(k-1)!. \tag{4.4}$$

Let  $g$  be the genus of  $E$ . By the Hurwitz formula and (4.4)

$$2g - 2 = -2k! + d = \frac{1}{2}(k^2 - 3k - 2)(k-1)!$$

From the above there are at most  $((k-1)k!/2)$  finite ramified first degree prime divisors of  $E$  and at most  $(k-1)!$  infinite first degree prime divisors of  $E$ . Thus

$$T \leq \frac{1}{2}(k^2 - k + 2)(k-1)!$$

and from (4.3)

$$|k!M(b) - p| \leq (\frac{1}{2}(k^3 - 3k - 2)(k-1)! + 2)\sqrt{p} + \frac{1}{2}(k^2 - k + 2)(k-1)!, \tag{4.5}$$

where for the upper bound for  $k!M(b)$ , we can disregard the last term.

For  $b \notin \mathbf{B}$  we can use “almost” trivial estimate

$$M(b) \leq \frac{p}{k}$$

which is arrived at by assuming, in the worst case, that (all but one of) the members of



$\mathbb{F}_p$  can be grouped in classes of size  $k$ , all giving the same value to  $f$ . Combining this bound with (4.5) and the lemma we can obtain the result of Theorem 4.

## 5. Resume

For  $(n, k, l, \Delta)$ -systems the notion of  $\Delta$  is similar to the notion of a covering radius of a code with given distance (or packing radius) [12, 16, 18, 19]. It is known that for BCH-codes the covering radius is roughly speaking twice the packing radius [12, 18, 19]. In contrast with these results, for our case the covering radius (i.e. the value of  $k-l+\Delta$ ) is equal to the packing radius plus a constant (2 or 3).

One interesting question arises if we compare the necessary condition with the sufficient one. Roughly speaking the necessary condition is:  $k-l < \sqrt{n(\Delta+1)}$  but the sufficient one is:  $k-l < c \log n / \log \log n$  (with some additional restriction on the size  $k$ ). It is not difficult to see that the bound for  $k-l$  is determined by the value of coefficient  $K$  in S. D. Cohen's bound (5.1) (see Theorem 4) for the number of solutions of the above system with  $k$  indeterminates and  $s$  equations (in S. D. Cohen's formula  $K = (k/2)k!$ ):

$$|N(k, s) - p^{k-s}| \leq K p^{k-s-1/2}. \quad (5.1)$$

From the necessary condition (Theorem 1) it is not difficult to prove that  $K > ck$ . If anybody can decrease the value of  $K$  in (5.1) then we can increase the upper bound for  $k-l$  in our sufficient condition.

## 6. Acknowledgements

The first author is grateful to the British Council for a grant for the visit to Moscow during which discussions on this paper took place. We also wish to thank Igor Shparlinski for many helpful discussions.

## REFERENCES

1. B. J. BIRCH and H. P. F. SWINNERTON-DYER, Note on a problem of Chowla, *Acta Arith.* **5** (1959), 417–423.
2. S. D. COHEN, Uniform distribution of polynomials over finite fields, *J. London Math. Soc.* **6** (1972), 93–102.
3. S. D. COHEN, Regular directed graphs with small diameter constructed by polynomial factorization, submitted.
4. P. DEMBOWSKI, *Finite Geometries* (Springer, Berlin 1968).
5. G. W. EFFINGER, A Goldbach theorem for polynomials of low degree over odd finite fields, *Acta Arith.* **42** (1983), 324–365.
6. P. ERDÖS and J. SPENCER, *Probabilistic methods in combinatorics* (Akademi Kiado, Budapest, 1974).

7. R. L. GRAHAM and N. J. A. SLOANE, Lower bounds for equal weight error correcting codes, *IEEE Trans. Inform. Theory* **26** (1980), 37–43.
8. M. J. GRANNELL and T. S. GRIGGS, A Steiner System (5, 6, 108), *Discrete Math.*, to appear.
9. H. HANANI, On quadruple systems, *Canad. J. Math.* **12** (1960), 145–157.
10. H. HANANI, On some tactical configurations, *Canad. J. Math.* **15** (1963), 702–722.
11. H. HANANI, On balanced incomplete block designs and related designs, *Discrete Math.* **11** (1975), 255–369.
12. T. HELLESETH, On covering radius of cyclic linear codes and arithmetic codes, *Discrete Appl. Math.* **11** (1985), 157–173.
13. A. E. INGHAM, On the difference between consecutive primes, *Quart. J. Oxford* **8** (1937), 255–266.
14. S. M. JOHNSON, A new upper bound for error-correcting codes, *IEEE Trans. Inf. Theory* **8** (1962), 203–207.
15. N. N. KUZJURIN, On some asymptotically optimal packings. *Algebraical and combinatorial methods in applied mathematics*, Gor'ky (1979), 57–65 (in Russian).
16. F. J. MACWILLIAMS and N. J. A. SLOANE, *The theory of error-correcting codes* (North-Holland, 1977).
17. N. V. SEMAKOV and V. A. ZINOV'EV, Balanced codes and tactical configurations, *Problems Inform. Transmission* **5** (3) (1969), 22–28.
18. A. TIETÄVÄINEN, On the covering radius of long binary BCH codes, *Discrete Appl. Math.* **16** (1987), 75–77.
19. S. G. VLADUTZ and A. N. SKOROBOGATOV, Covering radius of long BCH-codes, *Problemi peredachi informasii* **25** (1989), 38–45 (in Russian).
20. R. M. WILSON, An existence theory for pairwise balanced designs, *J. Combin. Theory Ser. A* **13** (1972), 220–273.
21. R. M. WILSON The necessary conditions for  $t$ -designs are sufficient for something, *Utilitas Math.* **4** (1973), 207–215.
22. R. M. WILSON, An existence theory for pairwise balanced designs: III—Proof of the existence conjectures, *J. Combin. Theory Ser. A* **18** (1975), 71–79.

DEPARTMENT OF MATHEMATICS  
UNIVERSITY OF GLASGOW  
GLASGOW G12 8QW  
SCOTLAND

INSTITUTE FOR CYBERNETICS PROBLEMS  
ACADEMY OF SCIENCE  
VAVILOVA 37, MOSCOW, 117312  
RUSSIA