Reprinted from JOURNAL OF COMBINATORIAL THEORY, Series A
Vol. 38, No. 2, March 1985
Printed in Belgium

On 2-Designs

P. ERDÖS

Hungarian Academy of Sciences

JOEL C. FOWLER*

California Institute of Technology, Pasadena, California 91125

VERA T. SÓS†

Bell Laboratories, Murray Hill, New Jersey 07974

AND

RICHARD M. WILSON*

California Institute of Technology, Pasadena, California 91125

Communicated by the Managing Editors

Received December 9, 1982

Denote by M_v the set of integers b for which there exists a 2-design (linear space) with v points and b lines. M_v is determined as accurately as possible. On one hand, it is shown for $v > v_0$ that M_v contains the interval $[v + v^{4/5}, \binom{v}{2} - 4]$. On the other hand for v of the form $p^2 + p + 1$ it is shown that the interval $[v+1, v+p-1]$ is disjoint from M_v; and if $v > v_0$ and p is of the form $q^2 + q$, then an additional interval $[v+p+1, v+p+q-1]$ is disjoint from M_v. © 1985 Academic Press, Inc.

Let S be a finite set, $|S| = v$, and let $\mathbf{A} = \{A_1, ..., A_b\}$ be a family of subsets of S. $\mathbf{A}$ is a *2-design* (or *pairwise balanced design*) or *linear space*) if every pair of elements of S occurs in exactly one A_i and $|A_i| > 1$ for $1 \leq i \leq b$. The elements of S are called the *points*, the subsets A_i are called the *lines* or *blocks* of the 2-design. Doyen asked what are the possible values of b for a given v? Let M_v be defined as the set of integers b for which there exists a 2-design with v points and b lines. So the problem is the determination of M_v.

* The work of these authors was supported in part by National Science Foundation Grant MCS-8217596.

† Permanent address: Eötvös University of Budapest, Hungary.

0097-3165/85 $3.00

Clearly

$$M_v \subset \left[1, \binom{v}{2}\right] \quad \text{and} \quad \binom{v}{2}-1, \binom{v}{2}-3 \notin M_v.$$

Also a well-known theorem of de Bruijn and Erdös [1] states that if $b>1$, then $b \geqslant v$. Thus min $M_v = v$.

Answering a question of Grünbaum, Erdös [2] proved the following: Let there be given n points in the plane. Join any two of them by a line. Denote by b the number of lines obtained. There is an absolute constant c so that every b with $cv^{3/2} < b \leqslant \binom{v}{2}$, $b \neq \binom{v}{2}-1$, $b \neq \binom{v}{2}-3$ can occur as the number of lines. (This result is best possible apart from the value of c.) This obviously gives that with the same c every $b \neq \binom{v}{2}-1$, $\binom{v}{2}-3$, $cv^{3/2} < b < \binom{v}{2}$ occurs in M_v. For an arbitrary 2-design the situation is different. Let $f(v)$ denote the largest integer $b < \binom{v}{2}-3$ for which there is no 2-design on v elements and b lines. We shall prove

THEOREM 1. *There is an absolute constant c so that for $v > v_0$*

$$f(v) < v + v^{1/2+c},$$

where c can be any value $> \frac{11}{40}$.

Remark. If we make plausible assumptions about the distribution of primes we can prove $f(v) < v + v^{1/2}(\log v)^{\alpha}$ for some fixed α. Further we conjecture that

$$\limsup_{v} \frac{f(v)-v}{\sqrt{v}} = \infty.$$

Theorem 1 shows that all values in the upper portion of the range $b \in [v, \binom{v}{2}-4]$ are possible. For b close to v our results are quite different. To get interesting results it will be convenient to assume v is of the form p^2+p+1 (here p is not necessarily a prime or prime power).

We shall prove

THEOREM 2. *Let $v = p^2+p+1$. Then for $p^2+p+1 < b < p^2+2p+1$ there is no 2-design with v points and b lines.*

Remarks. This result fails for v not of this form: projective planes from which points have been deleted provide many examples where $b - v < \sqrt{v}$.

Theorem 2 is best possible in that it is easy to construct a 2-design with $b = p^2+2p+1$ lines. To see this it suffices to consider the lines $A_1, \dots, A_v$ of a projective plane of order p and replace $A_1 = \{x_1, \dots, x_{p+1}\}$ by $A_1^1 = \{x_2, x_3, \dots, x_{p+1}\}$, $A_1^i = \{x_1, x_i\}$, $2 \leqslant i \leqslant p+1$.

In general we may take any projective plane and obtain a new 2-design by "breaking up" any line, i.e., by replacing it with the lines of some 2-design on the same set of points. In the above example A_1 has been broken up into a *near pencil* on $p+1$ points.

We further prove

THEOREM 3. *If $v=p^2+p+1$ and $b=p^2+2p+1$, then the design is obtained from a projective plane of order p by "breaking up" one of its lines into a near pencil or projective plane.*

Theorem 3 is in some sense sharp; nevertheless we prove a stronger result.

THEOREM 4. *Let $v=p^2+p+1$ and $\mathbf{A}=\{A_1,..., A_b\}$ a 2-design which is neither a projective plane nor a near pencil nor is obtained from a projective plane by "breaking up" one of its lines. Then $b>p^2+(2+c)\,p$ where c can be taken as* 0.147899.

A special case of interest is for $v=p^2+p+1$, where $p=q^2+q$. By Theorem 2 applied to the $p+1=q^2+q+1$ points on a line of a projective plane of order p, the breaking up of that line results in a 2-design on $v=p^2+p+1$ points with either

$$b=(p^2+p+1)+p \qquad \text{or} \qquad b\geqslant(p^2+p+1)+p+q.$$

This latter inequality must, by Theorem 4, also be valid (when $b>v$) for 2-designs on $v=p^2+p+1$ points which cannot be obtained by breaking up a line of a projective plane (when $v>v_0$). In other words the interval $[v+p+1, v+p+q-1]$ is disjoint from M_v.

Remarks. In the theory of designs or extremal set theory there are two essentially different methods, the combinatorial and the linear-algebraic one. There are just a few theorems where both methods work. This is the case with Theorems 2 and 3. We give two proofs. Theorems 2 and 3 are actually consequences of Totten's classification [7, 8] of all 2-designs satisfying $(b-v)^2\leqslant v$, but the proof in [7, 8] is substantially longer than those we give here. One of the present authors (J.C.F.) has used the algebraic approach to give a shorter proof of Totten's complete result [4]. Our combinatorial proof of Theorems 2 and 3 gives with some additional reasoning the proof of Theorem 4.

Proof of Theorem 1. First of all we restrict ourselves to the case when $v=p^2+p+1$, where p is a power of a prime. It is well known that in this case there is a projective plane; $\mathbf{A}=\{A_1,..., A_v\}$ with $|A_i|=p+1$, $1\leqslant i\leqslant v$

and $|A_i \cap A_j| = 1$ for $i \neq j$. On the other hand, if there is such a projective plane, then v must be of the form $t^2 + t + 1$.

To prove Theorem 1, first we prove

THEOREM 1*. *Let* $v = p_k^2 + p_k + 1$, p_k *be* kth *prime power (in natural order). Then*

$$f(p_k^2 + p_k + 1) < p_k^2 + 2p_k + p_k^{1/2 + c}, \tag{1}$$

where c *can be any value* $> \frac{11}{40}$.

Proof. Let $A_1, ..., A_v$ be the lines of a finite geometry with v points. Observe that it is necessary to construct a 2-design only for $b < p_{k+1}^2 + p_{k+1} + 1$. For if $b \geqslant p_{k+1}^2 + p_{k+1} + 1$ it is easy to see that we can use for our consideration the finite geometries of size $p_r^2 + p_r + 1$, where p_r is the least prime for which $p_r^2 + p_r + 1 \geqslant b$.

Using a well-known theorem of Heath-Brown and Iwaniec [5] we have

$$p_{k+1} - p_k < p_k^{(11/20) + \varepsilon}. \tag{2}$$

Hence

$$p_{k+1}^2 + p_{k+1} + 1 < p_k^2 + p_k^{(31/20) + \varepsilon}.$$

Thus it suffices to consider the b's satisfying

$$p_k^2 + 2p_k + p_k^{(31/40) + \varepsilon} < b < p_k^2 + p_k^{(31/20) + \varepsilon}.$$

From the result of Erdös [2], it immediately follows that the values of b satisfying

$$p_k^2 + cp_k^{3/2} < b$$

can be taken care of by the block designs formed by breaking up the elements of L_i's into pairwise balanced designs. Thus it suffices to deal with the b satisfying

$$p_k^2 + 2p_k + p_k^{(31/40) + \varepsilon} < b < p_k^2 + cp_k^{3/2}. \tag{3}$$

Let $L_1 = \{x_1, ..., x_{p_k + 1}\}$. Let q be the smallest prime power satisfying

$$p_k + 1 < q^2 + q + 1 < p_k + p_k^{(31/40) + \varepsilon/2}. \tag{4}$$

Consider now a projective plane with the lines $B_1, ..., B_{q^2 + q + 1}$. Omit $y = q^2 + q - p_k < p_k^{(31/40) + \varepsilon}$ of the points of this projective plane (without destroying any of the lines). Let the remaining points be identified by $\{x_1, ..., x_{p_k + 1}\}$. Thus we obtain a 2-design on our set $\{x_1, ..., x_{p_k + 1}\}$ and therefore on our set S of $p_k^2 + p_k + 1$ elements. Now the number of lines of this design is $p_k^2 + p_k + q^2 + q + 1$; $p_k^2 + p_k$ of the lines have size $p_k + 1$, the other $q_r^2 + q_r + 1$ sets have size $q_r + 1$ or less. ("Less" because we had to omit x elements which are at our disposal.)

Let $B_1^*, \ldots, B_{q^2+q+1}^*$ be the blocks which remain after the omission of the x elements and let $t_i = |B_i^*|$. By breaking up the lines B_i^* we get b_i new lines for every b_i satisfying $ct_i^{3/2} \leqslant b_i < \binom{t_i}{2} - 3$. Choosing the values of t_i $(1 \leqslant i \leqslant q^2 + q + 1)$ properly we can get every value in the interval $(p_k^{31/40}, p_k^{(31/20)+\varepsilon})$ in the form $\sum_{v=1}^{l} b_{i_v}$ with appropriate

$$b_{i_v} \in \left[ct_{i_v}^{3/2}, \binom{t_{i_v}}{2} - 4 \right].$$

This completes the proof of Theorem 1*.

The proof of Theorem 1 now can be completed by the same method.

We now proceed to the proofs of Theorems 2–4. Henceforth we assume that we have a 2-design with $v = p^2 + p + 1$ and $b \leqslant p^2 + (2 + c)\,p$ for some $c < \frac{1}{2}$. We use the following notation: $A_1, A_2, \ldots, A_b$ are the blocks (lines); $x_1, x_2, \ldots, x_v$ are the points; $|A_i| = l_i =$ length of A_i; $r_j = |\{i: x_j \in A_i, 1 \leqslant i \leqslant v\}| =$ degree of x_j.

LEMMA 1. *No line of length $> p+1$ exists unless the design is a near pencil.*

Proof. From [6] we have $b \geqslant 1 + (l^2(v-l)/(v-1))$ if a line of length l exists. Let l be the maximum length of a block A. Suppose $l \geqslant p+2$.

Case 1. $l \leqslant \frac{2}{3}v$. Note that $l^2(v-l)$ is increasing for $0 \leqslant l \leqslant \frac{2}{3}v$. Thus

$$b \geqslant \frac{(p+2)^2(p^2+p+1-(p+2))}{p^2+p+1-1} = p^2 + 3p + 1 - 4/p,$$

a contradiction for $p \geqslant 2$.

Case 2. $l > \frac{2}{3}v$. If there are two points off A then the line through them and A both meet at least $(l-1)\,2$ other lines. Thus $b \geqslant (l-1)\,2 + 2 > \frac{4}{3}v = \frac{4}{3}p^2 + \frac{4}{3}p + \frac{4}{3}$, a contradiction for $p \geqslant 1$. Hence no more than one point lies off of A. So the design is either degenerate (only one line) or a near pencil.

In view of Lemma 1 we may assume that the maximum length of a block is $p+1$. Given this and $v = p^2 + p + 1$ we have the useful fact that a point has degree $p+1$ if and only if it lies only on lines of length $p+1$.

We will refer to blocks of length $p+1$ as *long* and $< p+1$ as *short*. Clearly if all blocks are long the design is a projective plane. Thus we assume that some short blocks exist.

LEMMA 2. *If $v=p^2+p+1$, $b \leqslant p^2+2p+1$, and there exists a block A all of whose points have degree $p+1$, then $b=v$.*

Proof. All blocks on a point of degree $p+1$ have size $p+1$. Thus A and the $(p+1)\,p$ blocks which meet A provide a set of p^2+p+1 blocks of size $p+1$. These cover $(p^2+p+1)\binom{p+1}{2}=\binom{v}{2}$ pairs, so there can be no other blocks.

LEMMA 3. *$r_i \geqslant p+1$ for all i.*

Proof. Since $v=p^2+p+1$, a point of degree p or less would lie on some line of length $p+2$ or more.

LEMMA 4. *Some point of degree $p+1$ exists.*

Proof. Suppose that $r_i \geqslant p+2$ for all i. Note first that a block, A_1, of length $p+1$ exists since otherwise

$$bp \geqslant \sum_{i=1}^{b} l_i = \sum_{i=1}^{v} r_i \geqslant (p+2)\,v = (p+2)(p^2+p+1)$$

implying $b \geqslant p^2+3p+2$, a contradiction.

Since $\min r_i \geqslant p+2$, the number of lines intersecting A_1 of length $p+1$ is at least $(p+1)(p+1)$. But any point not contained in A_1, is contained in a line not intersecting A_1. So we get at least $p^2/(p+1)=p-1+(1/(p+1))$ lines which do not intersect A_1. By this, $b \geqslant (p^2+2p+1)+p$.

LEMMA 5. *Every two lines of length $p+1$ meet.*

Proof. Let $|A_1|=|A_2|=p+1$, $A_1 \cap A_2=\varnothing$. Then together A_1 and A_2 both meet $(p+1)^2=p^2+2p+1$ blocks. Now any point contained in A_1 or A_2 is of degree $\geqslant p+2$. Therefore for $x \in A_1$ there is a line $B(x)$ containing x and $|B(x)|<p+1$; any point contained in $B(x)$ has degree $\geqslant p+2$. Hence we have at least $|B(x)|-1$ lines intersecting $B(x)$ but not intersecting A_1.

If $|B(x)|>p/2$ for some $x \in A_1$ then $b \geqslant p^2+\frac{5}{2}p$. If $|B(x)| \leqslant p/2$ for every $x \in A_1$, then x is of degree $\geqslant p+3$ if $x \in A_1$. In this case we have, by counting the lines meeting A_1, $b \geqslant (p+1)(p+2)>p^2+3p$.

Algebraic Proof of Theorem 2. To prove Theorem 2, let N be the $v \times b$ incidence matrix of the design and U its row space. It is well known that $N^{\mathrm{T}}(NN^{\mathrm{T}})^{-1}N$ is the matrix of the orthogonal projection from $\mathbb{R}^b$ (with the standard inner product) onto U, provided that N has rank v, or equivalently, $(NN^{\mathrm{T}})^{-1}$ exists.

In our case, $NN^{\mathrm{T}}=\Delta+J$, where $\Delta=\operatorname{diag}(r_x-1\colon x \in S)$ and r_x denotes the degree of the point x; and it is easily checked that $(\Delta + J)^{-1} = \Delta^{-1} + \sigma\Delta^{-1}J\Delta^{-1}$, where $\sigma = 1/(1+\alpha_S)$ and $\alpha_S = \sum_{x\in S}(1/(r_x - 1))$. The $b\times b$ matrix

$$Q = I - N^{\mathrm{T}}(NN^{\mathrm{T}})^{-1}N = I - N^{\mathrm{T}}\Delta^{-1}N + \sigma N^{\mathrm{T}}\Delta^{-1}J\Delta^{-1}N$$

is evidently the matrix of the orthogonal projection from $\mathbb{R}^b$ onto $U^{\perp}$, a subspace of dimension $b - v$. In particular, Q has rank $b - v$.

For a subset T of the set S of points, let

$$\alpha_T = \sum_{x\in T}\frac{1}{r_x - 1}.$$

The rows and columns of Q are indexed by the blocks $A, B, \ldots,$ of the design, and with the above notation,

$$Q = I - ((\alpha_{A\cap B})) + \sigma((\alpha_A\alpha_B)).$$

Let $\mathbb{F}$ be the set of r_{x_0} blocks on a fixed point x_0 and consider the r_{x_0} by r_{x_0} principal submatrix Q_0 of Q whose rows and columns are indexed by the members of $\mathbb{F}$. For distinct $A, B \in \mathbb{F}$, $\alpha_{A\cap B} = (1/(r_{x_0} - 1))$. Writing β_A for $1 - \alpha_A + (1/(r_{x_0} - 1))$, we have

$$Q_0 = \operatorname{diag}(\beta_A\colon A\in\mathbb{F}) - \frac{1}{r_{x_0} - 1}J + \sigma((\alpha_A\alpha_B))_{A,B\in\mathbb{F}}.$$

So far, this holds for any design.

With our hypothesis, Lemmas 1 and 3 show that all blocks have size $\leqslant p+1$ and all points have degree $\geqslant p+1$. Then

$$\beta_A = 1 - \sum_{\substack{x\in A\\ x\neq x_0}}\frac{1}{r_x - 1} \geqslant 1 - \sum_{\substack{x\in A\\ x\neq x_0}}\frac{1}{p} \geqslant 0$$

and $\beta_A = 0$ if and only if $|A| = p+1$ and all points of $A - \{x_0\}$ have degree $p+1$. Suppose, for contradiction, that $\beta_A > 0$ for all $A\in\mathbb{F}$. Then $\operatorname{diag}(\beta_A) + \sigma((\alpha_A\alpha_B))$, being the sum of a positive definite and positive semidefinite matrix, is positive definite and hence has rank r_{x_0}. Subtracting the rank 1 matrix $(1/(r_{x_0} - 1))\,J$ can reduce the rank by at most one, so

$$r_{x_0} - 1 \leqslant \operatorname{rank} Q_0 \leqslant \operatorname{rank} Q = b - v \leqslant p - 1,$$

which gives a contradiction $r_{x_0} \leqslant p$ to Lemma 3.

To summarize, there exists a block A on x_0 such that all points of $A - \{x_0\}$ have degree $p+1$. We now take x_0 to be any point of degree $p+1$ and Lemma 2 completes the proof.

Algebraic Proof of Theorem 3. Let $Y = \{x \in S: r_x = p+1\}$, $Z = \{x \in S: r_x > p+1\}$. By Lemma 2, there are no blocks $A \subseteq Y$. But let us call A *good* when A is long and all but one of its points is in Y. Because of Lemma 2 we may assume that each block on a point $y_0 \in Y$ contains at least one point of Z, so $|Z| \geqslant p+1$.

The argument involving Q_0 in the previous theorem shows in this case, that each point of Z is contained in at least one good block. Any two long blocks intersect. Let $\mathbf{G}$ be a set of blocks consisting of one good block containing z for each $z \in Z$ and consider the principal submatrix Q_1 of Q whose rows and columns are indexed by the members of $\mathbf{G}$. For distinct $A, B \in \mathbf{G}$, $\alpha_{A \cap B} = 1/p$ (since A, B intersect in a point of Y). Also, for $A \in \mathbf{G}$ containing $z \in Z$, $\alpha_A = (1/(r_z - 1)) + (p/p) < (1/p) + 1$. Then

$$Q_1 = \operatorname{diag}\left(1 + \frac{1}{p} - \alpha_A\right) - \frac{1}{p} J + \sigma((\alpha_A \cdot \alpha_B))_{A,B \in \mathbf{G}},$$

being the sum of a positive definite, a positive semidefinite, and a rank 1 matrix, is seen to have rank $\geqslant |\mathbf{G}| - 1 = |Z| - 1$. So

$$|Z| - 1 \leqslant \operatorname{rank} Q_1 \leqslant \operatorname{rank} Q = b - v = p.$$

We have now proved that $|Z| = p+1$.

Recall that all blocks containing a point of Y are long. Consider two good blocks A, A' containing $z, z' \in Z$. There are p^2 blocks other than A containing points of $A - \{z\}$, all of which are long. There are p blocks (including A) on z containing a point of $A' - \{z'\}$ and these too must be long. Thus there are at least $p^2 + p$ long blocks. These cover $(p^2+p)\binom{p+1}{2}$ pairs, leaving only $\binom{p+1}{2}$ pairs uncovered. The remaining $p+1$ blocks are short and cover these $\binom{p+1}{2}$ pairs. But all short blocks are contained in Z, and $|Z| = p+1$. Evidently, the short blocks form a (possibly degenerate) projective plane on Z.

Finally, the long blocks together with Z form a projective plane of order p on x, which proves Theorem 3.

Now we present combinatorial proofs of Theorems 2–4. Note that it suffices to prove Theorem 4 only since (using the de Bruijn–Erdös Theorem) the breaking up of a line in a projective plane immediately results in $b \geqslant p^2 + 2p + 1$. Equality holds only if the line is broken into a projective plane or near pencil.

We show first that the number of lines of length $p+1$ is at least p^2+1 and then show that this implies that exactly one line was broken up.

Let $q =$ (number of lines length $p+1$) and let the longest line not of length $p+1$ be $\hat{A}$, of length αp, $0 < \alpha \leqslant 1$. Thus every line has length $p+1$

or $\leqslant \alpha p$. By counting triples (x_i, x_j, A_k) with $x_i \in A_k$, $x_j \in A_k$, $x_i \neq x_j$; we have

$$(b-q)\,\alpha p(\alpha p-1)+qp(p+1) \geqslant v(v-1).$$

Using $v = p^2+p+1$ and $b \leqslant p^2+(2+c)\,p$ we have

$$q \geqslant p^2 + p\left(\frac{1-2\alpha^2-c\alpha^2}{1-\alpha^2}\right)+\frac{(1+\alpha c)\,p+1}{p(1-\alpha^2)+1+\alpha}.$$

So $q \geqslant p^2+1$ for $\alpha \leqslant \sqrt{1/(2+c)}$. We now take care of larger α.

Let x be a point of degree $p+1$. Then $x \notin \hat{A}$. Since $\hat{A}$ is short there exists a line of length $p+1$ through x missing $\hat{A}$. Denote this line by A and the lines through x meeting $\hat{A}$ by $A_1, A_2,\ldots, A_{\alpha n}$.

Consider now A_1 and A. Together both meet $(p+1-1)(p+1-1)+\text{degree}(x) = p^2+p+1$ lines.

Through each point $y \in \hat{A}\backslash A_1$ there is at least one line meeting A and missing A_1 (i.e., at least one of the $p+1$ lines from y to A must miss A_1, since $\hat{A}$ through y meets A_1 and misses A). Thus there are at least $\alpha p-1$ lines meeting A and missing A_1. Similarly if A^* is a line meeting A and missing A_1 there are at least $|A^*|-1$ lines meeting A_1 and missing A.

Adding these up, we have

$$b \geqslant (p^2+p+1)+(\alpha p-1)+(|A^*|-1).$$

Hence $|A^*| \leqslant (1+c-\alpha)\,p+1$.

Thus any line meeting A but missing A_1 has length $\leqslant (1+c-\alpha)\,p+1$. This same argument holds for any A_i, $1 \leqslant i \leqslant \alpha p$. Now suppose A' is any block meeting A. If A' misses some A_i, $1 \leqslant i \leqslant \alpha p$ then $|A'| \leqslant (1+c-\alpha)\,p+1$ by above. If A' meets every $A_1, A_2,\ldots, A_{\alpha p}$ in addition to A then $|A'| \geqslant \alpha p+1$. So $|A'| = p+1$ by maximality of $\hat{A}$.

We have shown that every block meeting A has length $p+1$ or $\leqslant (1+c-\alpha)\,p+1$. Let u be any point on A and

$$N_u = \text{No. of lines of length } p+1 \text{ through } u \text{ other than } A.$$

Then

$$\begin{pmatrix}\text{No. of lines through } u \text{ of}\\ \text{length } \leqslant (1+c-\alpha)\,p+1\end{pmatrix} \geqslant \frac{p^2-pN_u}{(1+c-\alpha)\,p+1-1}=\frac{p-N_u}{(1+c-\alpha)}.$$

So

$$\text{degree}(u)-1 \geqslant N_u+\frac{p-N_u}{(1+c-\alpha)}.$$

Summing over $u \in A$ then gives

$$b-1 \geqslant \sum_{u \in A} (\text{degree}(u)-1) \geqslant (q-1)\left(1-\frac{1}{1+c-\alpha}\right)+\frac{p(p+1)}{1+c-\alpha},$$

since $q-1=\sum_{u \in A} N_u$. Solving for q gives

$$q \geqslant p^2+p\left(\frac{1-(2+c)(1+c-\alpha)}{\alpha-c}\right)+\frac{1}{\alpha-c}.$$

Thus $q \geqslant p^2+1$ for $1+c-\alpha \leqslant 1/(2+c)$, i.e., $\alpha \geqslant (c^2+3c+1)/(c+2)$. Previously $q \geqslant p^2+1$ for $\alpha \leqslant \sqrt{1/(2+c)}$. We choose c so that these ranges overlap, i.e.,

$$\frac{c^2+3c+1}{c+2} \leqslant \sqrt{1/(2+c)}.$$

Equivalently $0 \geqslant c^4+6c^3+11c^2+5c-1$. To within six decimal places we can take $c=0.147899$.

We now complete the proof by showing that $q \geqslant p^2+1$ implies one line was broken up. Let $A_1, ..., A_{p^2+t}$ be the lines of length $p+1$, $t \geqslant 1$. Here we use the following theorem of Vanstone [9]: Let $|S|=p^2+p+1$, $\mathbf{B}=\{B_1, ..., B_m\}$, $m \geqslant p^2$ be a family of subsets of S, $|B_i|=p+1$ for $i=1, 2, ..., m$. If $|B_i \cap B_j|=1$, $1 \leqslant i<j \leqslant m$ then $\mathbf{B}$ is embeddable into a finite projective plane of order p.

We apply this theorem to the system $\{A_1, ..., A_{p^2+t}\}$. Let $B_1, ..., B_{p^2+p+1}$ be the finite projective plane into which we embed our system, and B_i, $1 \leqslant i \leqslant p-t+1$ the lines not belonging to our system. Then the pair covered by the lines B_i, $i \leqslant p-t+1$ must be covered by our lines A_j, $j>p^2+t$.

Observe that to every line B_i, $i \leqslant p-t+1$ there is an x_i, $x_i \in B_i$ and $x_i \notin B_j$, $j \leqslant p-t+1$, $j \neq 1$. This is obvious because $p-t<p+1$ and $|B_i \cap B_j|=1$ for $i \neq j$. Now for every A_j, $j>p^2+t$ which contains x_i we have $A_j \subset B_i$ since for $y \notin B_i(x_i, y)$ is covered by a line A_v, $v<p^2+t$. Since all the pairs (x_i, y), $y \in B_i$ must be covered by such a line A_j, and $|A_j|<p+1$, we have at least two lines which are contained in B_i. The short lines meeting some B_i induce a sub 2-design on the $p+1$ points of B_i. So by the de Bruijn–Erdös theorem the number of short lines which meet a B_i is at least $p+1$. Fixing B_1 we have at least $p+1$ short lines meeting B_1. The remaining $p-t$ lines B_i each contain at least two short lines. Thus

$$b \geqslant p^2+t+(p+1)+2(p-t) \geqslant p^2+2p+1$$

and equality holds iff $p=t$, i.e., exactly one line of a projective plane of order p was broken up.

If $t=1$, we have $b \geqslant p^2+3p-1$. Now we suppose $2 \leqslant p+1-t \leqslant p-1$. In this case every B_i, $1 \leqslant i \leqslant p+1-t$ contains at least $t+1$ points not contained in any other B_j, $i \neq j$, $1 \leqslant j \leqslant p+1-t$. Thus the short lines containing these points lie entirely within the given B_i.

Let $B_i = C_i \cup D_i$, $1 \leqslant i \leqslant p+1-t$ where

$$C_i = \left\{ x_j : x_j \in B_i, x_j \notin \bigcup_{\substack{v \neq i \\ 1 \leqslant v \leqslant p+1-t}} B_v \right\}$$

$$D_i = B_i \setminus C_i.$$

Case a. For an i, $1 \leqslant i \leqslant p+1-t$, the pairs of C_i are covered by one short line A_{μ_i}. Then for any $x_j \in C_i$ we need at least one line to cover each of the pairs (x_j, y), $y \in B_i \setminus A_{\mu_i}$ $(\neq \varnothing)$. For different x_j's we have different lines. This gives at least $|C_i| \geqslant t+1$ different short lines within B_i.

Case b. The pairs of C_i are covered by more than one line. In this case the de Bruijn–Erdös theorem gives at least $|C_i| \geqslant t+1$ different short lines within B_i.

The lines we considered are different for different i's. This gives, that the number of short lines is at least $(p+1-t)(t+1)$. Hence $b \geqslant p^2+t+(p+1-t)(t+1) \geqslant p^2+3p-1$ for $2 \leqslant t \leqslant p-1$. This completes the proof.

Before closing with several open problems we remark that a forthcoming paper by Erdös, Mullin, Sós, and Stinson [3] contains related results.

PROBLEM 1. Theorem 4 is not best possible. We conjecture that Theorem 4 holds with

$$b \geqslant p^2+3p+0(1).$$

Remark. Let $|S|=v$, $\mathbf{A}=\{A_1,\dots,A_b\}$ a 2-design. Assume $1 \leqslant |A_i| \leqslant v-2$. We can prove that the number of A_i's not containing x for every $x \in S$ is greater than $v-\sqrt{v}$. We have equality for finite geometries. This might be connected with the following conjecture of Dowling–Wilson.

PROBLEM 2. Let $x \in S$, and $x \notin A_i$. Assume that there are t lines through x not meeting A_i. Then $b \geqslant v+t$.

This is equivalent to the assertion that the number of lines not containing x is never less than the number of points not on A_i.

PROBLEM 3. Assume again $\mathbf{A}=\{A_1,\dots,A_b\}$ is a 2-design, $1 \leqslant |A_i| \leqslant v-2$ and that the 2-design is not a finite geometry, further that b is minimal satisfying this condition. Furthermore assume there is no finite geometry of order v and $v_1 > v$ is the least integer $> v$ for which there is a finite geometry. Is it true, that we obtain our 2-design by omitting elements from the finite geometry of size v_1 (perhaps we can completely omit some lines if $v_1 - v > \sqrt{v}$)?

PROBLEM 4. Let b be the minimal number of blocks of a design on v elements satisfying $|A_i| \leqslant v - 2$. Is it true that

$$\overline{\lim_{v \to \infty}} \frac{b - v}{\sqrt{v}} = \infty?$$

PROBLEM 5. Let $\{A_i\}$ be a design on $v = p^2 + p + 1$ elements for which $|A_1| = |A_2| = p + 1$, $A_1 \cap A_2 = \varnothing$. We proved in Lemma 6 that $b \geqslant p^2 + \frac{5}{2}p$. Determine the smallest possible value of b or give a better estimation.

REFERENCES

1. N. G. DE BRUIJN AND P. ERDÖS, On a combinatorial problem, *Nederl. Akad. Wetensch. Proc. Sect. Sci.* **51** (1948), 1277–1279.
2. P. ERDÖS, On a problem of Grünbaum, *Canad. Math. Bull.* **15** (1972), 23–25.
3. P. ERDÖS, R. C. MULLIN, V. T. SÓS, AND D. STINSON, Finite linear spaces and projective planes, to appear.
4. J. C. FOWLER, A short proof of Totten's classification of restricted linear spaces, to appear.
5. D. R. HEATH BROWN AND H. IWANIEC, On the difference between consecutive primes, *Invent. Math.* **55** (1979), 49–69.
6. R. G. STANTON AND J. G. KALBFLEISCH, The $\lambda - \mu$ problem, $\lambda = 1$, $\mu = 3$, *in* "Proc., Second Chapel Hill Conf. on Combinatorics," pp. 451–462, Chapel Hill, 1972.
7. J. TOTTEN, Basic properties of restricted linear spaces, *Discrete Math.* **13** (1975), 67–74.
8. J. TOTTEN, Classification of restricted linear spaces, *Canad. J. Math.* **28** (1976), 321–333.
9. S. VANSTONE, The extendability of $(r, 1)$-designs, *in* "Proc., Third Manitoba Conf. on Numerical Math.," pp. 409–418, 1973.