Journal of Combinatorial Theory, Series A **100**, 181–188 (2002)
doi:10.1006/jcta.2002.3286

NOTE

On the Cardinality of Intersection Sets in Inversive Planes

Marcus Greferath and Cornelia Rößing[1]

Department of Mathematics, San Diego State University, San Diego, California 92182
E-mail: roessing@math.sdsu.edu

Received January 22, 2001; published online July 19, 2002

Intersection sets and blocking sets play an important role in contemporary finite geometry. There are cryptographic applications depending on their construction and combinatorial properties. This paper contributes to this topic by answering the question: how many circles of an inversive plane will be blocked by a d-element set of points that has successively been constructed using a greedy type algorithm? We derive a lower bound for this number and thus obtain an upper bound for the cardinality of an intersection set of smallest size. Defining a coefficient called *greedy index*, we finally give an asymptotic analysis for the blocking capabilities of circles and subplanes of inversive planes. © 2002 Elsevier Science (USA)

Key Words: inversive plane; finite geometry; blocking set; intersection set.

INTRODUCTION

Finite inversive planes are also known as 3-designs with parameters $(q^2+1, q+1, 1)$. It has been proposed in 5–7 to use them in order to reduce storage requirements for cryptographic key distribution in secure networks. For this application the question of minimal cardinality of intersection sets is directly related to the security of the underlying network communication.

Intersection sets and blocking sets have extensively been studied in projective planes and other line geometries. Little is known however for circle geometries, i.e. 3-designs. In the present article, we present a bound for the cardinality of an intersection set of a (finite) inversive plane. In doing so, we consider a hypothetical algorithm that successively adds points to a given set of points in such a way, that a maximal number of circles will be intersected by the enriched set. As this algorithm does not revise its past choices, it works according to a greedy principle.

In this way, we define a function g that assigns every element in $d \in \{1, \ldots, q^2-1\}$ a lower bound for the number of circles of the inversive

[1] To whom correspondence should be addressed.

0097-3165/02 $35.00

plane, that can be blocked by a d-element subset of points. Having this function we define the *greedy index* of a given point set D as the ratio of the number of circles actually blocked by D to the number $g(|D|)$. This greedy index is designed to measure what could be called the blocking quality of a given set. In addition, the function g can directly be used to derive an upper bound for the cardinality of an intersection set of the given plane.

We conclude our investigation with an analysis of the blocking capability of two classes of point sets in inversive planes. On the one hand, we consider the set of points on a single circle, and show that the blocking capability of these sets is asymptotically inferior to that of the points of a (maximal) subplane.

1. FINITE INVERSIVE PLANES

An inversive plane is an incidence structure $M := (P, C)$ where P is a set of points and $C \subseteq 2^P$ is a set of circles satisfying the following axioms:

(i) Any three distinct points are contained in a unique circle.

(ii) If p, q are points and c is a circle containing p but not q, then there exists a unique circle containing q and intersecting c exactly in p.

(iii) There are four points which are not contained in a common circle.

Equivalently, an inversive plane can be characterized as an incidence structure $M := (P, C)$ where the internal structure

$$M_p := (P \backslash \{p\}, C_p) \quad \text{with} \quad C_p := \{c \backslash \{p\} \mid c \in C \quad \text{and} \quad p \in c\}$$

is an affine plane for every point p of M. Therefore, all circles of a finite inversive plane have the same number of points, say $q + 1$, and we call q the order of the plane. As we have already indicated in the Introduction the finite planes of order q are exactly the 3-designs with parameters $(q^2 + 1, q + 1, 1)$. They possess a total number of $q(q^2 + 1)$ circles.

The smallest example of an inversive plane is given by the trivial design $\binom{P}{3}$ where P is a five-element set (see Fig. 1), and inversive planes of order q can easily be constructed whenever q is a prime power.

If $M = (P, C)$ is a finite inversive plane and S a subset of its points, then we define the *blocking number* of S by

$$b(S) := |\{c \in C \mid c \cap S \neq \emptyset\}|,$$

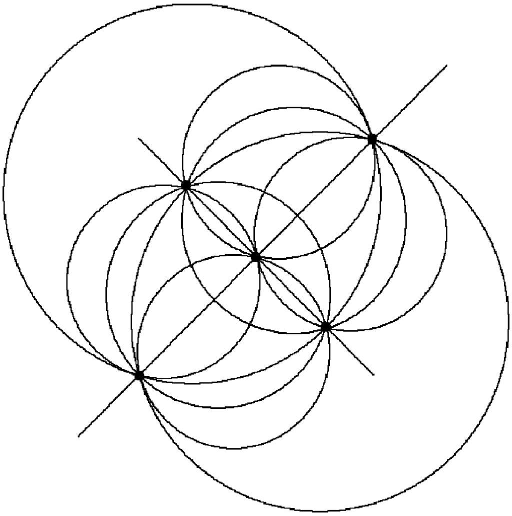

FIG. 1. Inversive plane of order 2.

where S is called an *intersection set* of M, if $b(S) = |C|$. A trivial example of an intersection set is P itself, and it is clear that examples of lower, possibly minimal cardinality are in focus.

2. TWO BOUNDS

In order to find a lower bound for the cardinality of an intersection set we look first for a lower bound for the maximal blocking number that can be achieved by a set of given cardinality.

The blocking numbers for one-, two- and three-element point sets of an inversive plane follow directly from the design properties and are given by $q(q+1)$, $2q^2+q-1$ and $3q^2-2$, respectively. Our first theorem gives a lower bound for the maximal blocking number of a d-element set of points of a finite inversive plane.

Theorem 2.1. *In an inversive plane $M = (P, C)$ of order q for every d with $0 \leqslant d \leqslant q^2+1$ there exists a d-element set D of points such that*

$$b(D) \geqslant q\,(q^2+1)\left(1 - \frac{\binom{q^2+1-d}{q+1}}{\binom{q^2+1}{q+1}}\right).$$

Proof. We will inductively construct the desired point set D for given d and first observe that our claim obviously holds for $d = 0$ and $D = \emptyset$. If D is a d-element set of points satisfying our claim, and if $d < q^2 + 1$ then there is a point p not contained in D that is contained in at most

$$\frac{b(D)\,(q+1) - dq(q+1)}{q^2 + 1 - d}$$

circles which are already blocked by D. This results from double counting the set of pairs

$$Q_D := \{(p, c) \in P \times C \mid c \cap D \neq \emptyset\}.$$

On the one hand, the cardinality of this set is obviously given by $(q+1)\,b(D)$. On the other hand, we have

$$|Q_D| = dq(q+1) + \sum\nolimits_{p \notin D} |\{c \in C \mid p \in c \text{ and } c \cap D \neq \emptyset\}|.$$

So, the number of pairs on the right-hand side of the last expression averaged over the points outside of D is given by

$$\frac{1}{q^2 + 1 - d} \sum\nolimits_{p \notin D} |\{c \in C \mid p \in c \text{ and } c \cap D \neq \emptyset\}| = \frac{b(D)(q+1) - dq(q+1)}{q^2 + 1 - d},$$

and hence there must exist a point p outside of D that is contained in at most this number of circles blocked by D. Adding this point to D we obtain

$$b(D \cup \{p\}) \geqslant b(D) + q(q+1) - \frac{b(D)(q+1) - dq(q+1)}{q^2 + 1 - d},$$

which by our assumption on D is seen to be lower bounded in the desired way, i.e.,

$$b(D \cup \{p\}) \geqslant q(q^2 + 1) \left(1 - \frac{\binom{q^2+1-(d+1)}{q+1}}{\binom{q^2+1}{q+1}} \right). \quad \blacksquare$$

Note that the bound in the foregoing theorem is met by one-, two- and three-element point sets. For a non-concircular set of four points this bound is slightly weaker than the blocking number that is actually achieved. The next statement shows consequences for the cardinality of an intersection set.

THEOREM 2.2. *In an inversive plane of order q there exists an intersection set of at most*

$$q^2+1-\sqrt[q+1]{\binom{q^2}{q}(q-1)!}$$

elements.

Proof. Defining $g(d):=q(q^2+1)\left(1-\frac{\binom{q^2+1-d}{q+1}}{\binom{q^2+1}{q+1}}\right)$ we have to find d such that $g(d)\geqslant q(q^2+1)$ or, equivalently, $g(d)>q(q^2+1)-1$. Expanding this expression and using the inequality

$$\binom{q^2+1-d}{q+1}\leqslant\frac{(q^2+1-d)^{q+1}}{(q+1)!}$$

we obtain the claim. ∎

REMARK 2.3. A power series expansion of the latter bound yields the asymptotic result that an inversive plane of order q contains an intersection set of at most

$$3q\ln(q)+\frac{1}{2}q+\frac{1}{24}-\frac{9}{2}\ln(q)-\frac{9}{2}\ln(q)^2+O\left(\frac{1}{q}\right)=3q\ln(q)+\frac{1}{2}q+O(1)$$

points.

3. GREEDY INDICES OF POINT SETS

Using Theorem 2.1, we define the following measure for the blocking capability of a given point set of an inversive plane.

DEFINITION 3.1. Let $M:=(P,C)$ be an inversive plane of order q. The *greedy index* of M is the function

$$r:2^P\to\mathbb{R},\ D\mapsto\frac{b(D)}{g(|D|)},\qquad \text{where } g(d)=q(q^2+1)\left(1-\frac{\binom{q^2+1-d}{q+1}}{\binom{q^2+1}{q+1}}\right).$$

The higher this index the "better" are the blocking capabilities of the given point set in comparison to the theoretic bound derived in Theorem 2.1. The construction of point sets of asymptotically high greedy index (meaning at least 1) is a non-trivial task. In the following, we consider two classes of point sets and determine the asymtotic behaviour of their greedy indices.

PROPOSITION 3.2. *In an inversive plane of order q the point set of a circle blocks $\frac{1}{2}q^2(q+3)$ circles. As q increases the corresponding greedy index monotonically decreases and approaches $\frac{1}{2}\frac{e}{e-1} \approx 0.79$ where e denotes the Eulerian number.*

Proof. A circle c of an inversive plane of order q contains $q+1$ points. Each of these points is incident with $q(q+1)$ circles, each pair of points is incident with q circles whereas each triple of distinct points is incident exactly with c. Therefore, we obtain

$$\begin{aligned} b(c) &= (q+1)\,(q\,(q+1)-1) - \binom{q+1}{2}q + 1 \\ &= \tfrac{1}{2}q^2(q+3), \end{aligned}$$

and the asymptotic behaviour of the corresponding greedy index is easily checked. Figure 2 gives an illustration of this behaviour. ∎

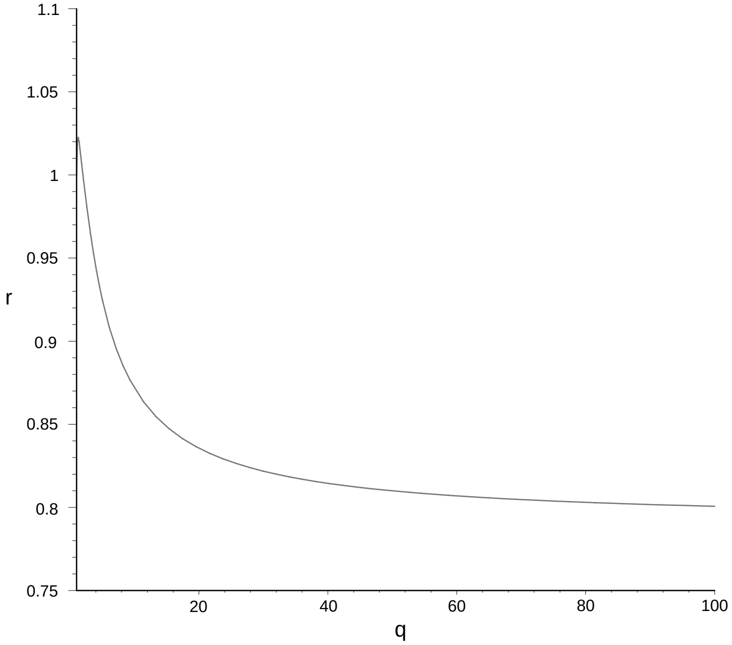

FIG. 2. Greedy index of a circle (asymptotic behaviour).

Definition 3.3. Let $M := (P, C)$ be an inversive plane. For $Q \subseteq P$ and

$$D := \{c \cap Q \mid c \in C \text{ and } |c \cap Q| \geqslant 3\},$$

the incidence structure $N := (Q, D)$ is called a subplane of M, if N is an inversive plane itself, and if any pair of tangent circles of N does not have a further intersection in M.

Proposition 3.4. *The blocking number of a subplane of order r in an inversive plane of order q is given by* $(r^2 + 1)(q^2 + q - \frac{1}{2}q^2 r + \frac{1}{2}r^3 - r^2)$.

Proof. Let $N := (Q, D)$ be a subplane of the inversive plane $M := (P, C)$. In order to derive the blocking number of Q we have to add the numbers of circles intersecting Q in 2 points, in 1 point and those which intersect Q in at least 3 points (i.e., which are circles of N). For an arbitrary point p of N the internal structure N_p is an affine subplane of M_p (cf. [4]).

The number of lines incident with exactly one point of N_p is the number of circles of M intersecting with N in p and one further point. Every point of the affine subplane N_p is incident with $q - r$ lines touching the subplane. Hence, we obtain $r^2(q - r)$ lines of M_p which touch N_p. In the inversive plane M this results in $\frac{1}{2}(r^2 + 1)r^2(q - r)$ circles intersecting N in p and one further point.

The lines of M_p which do not intersect with N_p correspond to the circles of M touching N in p. The number of lines of M_p intersecting N exactly in p is the number of lines of the affine plane M_p which are neither lines of N_p nor intersecting N_p. This number is given by $(q^2 + q) - (r^2 + r) - (r^2(q - r)) = q^2 + q - r^2 q + r^3 - r^2 - r$. From this we obtain the total number of circles of M which are tangent to N as $(r^2 + 1)(q^2 + q - r^2 q + r^3 - r^2 - r)$.

Adding the results of these cases to the number of circles of N we get

$$b(Q) = r(r^2 + 1) + (r^2 + 1)(q^2 + q - qr^2 + r^3 - r^2 - r) + \tfrac{1}{2}(r^2 + 1)r^2(q - r)$$

$$= (r^2 + 1)(q^2 + q - \tfrac{1}{2}qr^2 + \tfrac{1}{2}r^3 - r^2). \quad \blacksquare$$

Remark 3.5. Assuming N to be a subplane of maximum size in M, i.e. $q = r^3$ in the foregoing theorem, the greedy index approaches 1 for increasing q. Figure 3 gives an illustration of the asymptotic behaviour of this index.

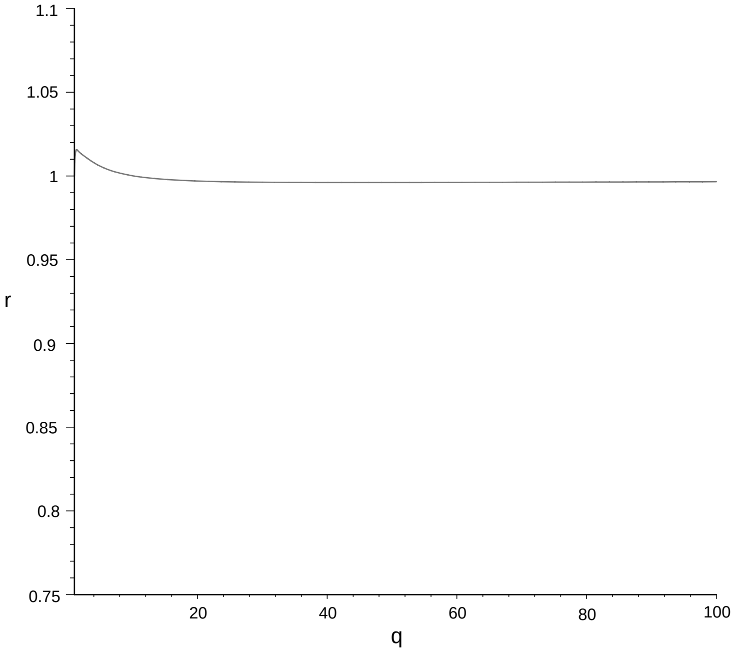

FIG. 3. Greedy index of a maximal subplane (asymptotic behaviour).

REFERENCES

1. A. Beutelspacher, "Einführung in die endliche Geometrie," BI Wissenschaftsverlag, Mannheim 1983.
2. A. Beutelspacher, Blocking sets and partial spreads in finite projective spaces, *Math. Z.* **145** (1975), 211–229.
3. A. A. Bruen and B. L. Rothschild, Lower bounds on blocking sets, *Pacific J. Math.* **118** (1985), 303–311.
4. P. Dembowski, Finite geometries, *in* "Ergebnisse der Mathematik und ihrer Grenzgebiete," Vol. 44, Springer, Berlin, 1968.
5. C. Mitchell and F. Piper, The cost of reducing key-storage requirements in secure networks, *Comput. Security* **6** (1987), 339–341.
6. C. Mitchell and F. Piper, Key storage in secure networks, *Discrete Appl. Math.* **21** (1988), 215–228.
7. C. Mitchell and F. Piper, "Combinatorial Techniques for Key Storage Reduction in Secure Networks," Hewlett-Packard Laboratories, Technical Memo, 1987.