

Covering all points except one

A. Blokhuis & A. E. Brouwer

Dept. of Mathematics, Technological University Eindhoven,
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
aartb@win.tue.nl, aeb@cwi.nl

and

T. Szőnyi*

Institute of Mathematics, Eötvös Loránd University,
H-1117 Budapest, Pázmány P. s. 1/C
and

Computer and Automation Research Institute
Hungarian Academy of Sciences
H-111 Budapest, Lágymányosi ú. 11
szonyi@cs.elte.hu

2008-11-27

Abstract

In many point-line geometries more lines are needed to cover all points except one, than to cover all points. Bounds can be given by looking at the dimension of the space of functions induced by polynomials of bounded degree.

AMS Classification: 51A*, 51E*.

1 Lagrange interpolation

Suppose A is a finite set, and F a field, and for each $a \in A$ we have a function $f_a : A \rightarrow F$ that vanishes on $A \setminus \{a\}$ but is nonzero in a . Then the vector space of functions on A , which has dimension $|A|$, has basis $\{f_a \mid a \in A\}$.

This very simple observation gives easy proofs for various inequalities.

Proposition 1.1 (Jamison [9], BS [6]) *Let $AG(2, q)$ and $PG(2, q)$ denote the desarguesian affine and projective plane of order q .*

- (i) *If S is a set of points in $AG(2, q)$ that meets every line, then $|S| \geq 2q - 1$.*
- (ii) *If S is a set of lines in $PG(2, q)$ that covers all points except one (which is not covered), then $|S| \geq 2q - 1$.*
- (iii) *If S is a set of lines in $AG(2, q)$ that covers all points except one (which is not covered), then $|S| \geq 2q - 2$.*

*The third author gratefully acknowledges the financial support of NWO, including the support of the DIAMANT and Spinoza projects. He thanks the Department of Mathematics of the Technological University Eindhoven for the warm hospitality. He was partly supported by OTKA Grants T 49662 and NK 67867.

Proof: Clearly (i) and (ii) are equivalent via the point-line duality in $PG(2, q)$. And (ii) and (iii) are equivalent: $PG(2, q)$ and $AG(2, q)$ differ by 1 line, and all lines in $PG(2, q)$ are equivalent. It remains to show (iii).

The vector space of functions on $AG(2, q)$ (with values in \mathbb{F}_q) has dimension q^2 and a basis consisting of the polynomials $X^i Y^j$ for $0 \leq i, j \leq q-1$. If $f_0 := \prod_{i=1}^m (a_i X + b_i Y + 1)$ vanishes everywhere except in $(0, 0)$, then $f_0(X-a, Y-b)$ vanishes everywhere except in the point (a, b) , so that the vector space of functions on $AG(2, q)$ is spanned by these $f_0(X-a, Y-b)$. But then there is a term $X^{q-1} Y^{q-1}$ in the expansion of the product for f_0 , and $m \geq 2(q-1)$. \square

We can do this again, and show with precisely the same proof

Proposition 1.2 (Jamison [9], BS [6]) *Let $AG(n, q)$ and $PG(n, q)$ denote the desarguesian affine and projective space of order q and dimension n . Let $n > 0$.*

(i) *If S is a set of points in $AG(n, q)$ that meets every hyperplane, then $|S| \geq n(q-1) + 1$.*

(ii) *If S is a set of hyperplanes in $PG(n, q)$ that covers all points except one (which is not covered), then $|S| \geq n(q-1) + 1$.*

(iii) *If S is a set of hyperplanes in $AG(n, q)$ that covers all points except one (which is not covered), then $|S| \geq n(q-1)$. \square*

Of course we did not really use the fact that the cover consists of hyperplanes, only the degrees mattered. We used a hyperplane to go from $PG(n, q)$ to $AG(n, q)$, but that can be avoided. First some preparation.

A homogeneous polynomial $f = f(X_1, \dots, X_{n+1})$ of degree d has values on $PG(n, q)$ that are defined up to a d -th power. In particular, it has well-defined values on $PG(n, q)$ when its degree is a multiple of $q-1$. Also inhomogeneous polynomials of which all terms have a degree divisible by $q-1$ are well-defined on $PG(n, q)$.

Proposition 1.3 *Each function f on $PG(n, q)$ can be written in a unique way as linear combination of monomials $X_1^{d_1} \dots X_{n+1}^{d_{n+1}}$ where $0 \leq d_i \leq q-1$ for all i , and $\sum d_i = j(q-1)$ where j is an integer, $0 \leq j \leq n$. The same is true with the condition $1 \leq j \leq n+1$.*

Proof: Since $X^q - X$ and $\prod(1 - X_i^{q-1})$ vanish identically, each function can be written in the indicated way. But the number of monomials as indicated equals the number $q^n + \dots + q + 1$ of points of $PG(n, q)$. \square

Proposition 1.4

(i) *If $f = f(X_1, \dots, X_n)$ is a polynomial that vanishes in all points of $AG(n, q)$ except one, then f has degree at least $n(q-1)$.*

(ii) *If $f = f(X_1, \dots, X_{n+1})$ is a polynomial without constant term and with all terms of degree divisible by $q-1$, and f vanishes in all points of $PG(n, q)$ except one, then f has degree at least $(n+1)(q-1)$.*

Proof: (i) This was proved already. (ii) Using linear transformations we find polynomials f_a that vanish everywhere except in the point a , so that these f_a span the space of functions on $PG(n, q)$. The degrees that occur among the

terms of the f_a are not larger than the degree of f , and by Proposition 1.3 degree $(n+1)(q-1)$ occurs. \square

Alon–Füredi [1] give a generalization of Proposition 1.2(iii) to rectangular boxes. Bounds on the degree of polynomials not vanishing in a nonempty subset of a grid can be found in Ball–Serra [3] in a more general situation.

1.1 Partial covers of $PG(2, q)$

In the above we looked at the case where a unique point is not covered. For the case of more holes (non-covered points), one has

Proposition 1.5 *A partial cover of $PG(2, q)$ with $h > 0$ holes, not all on one line, has size at least $2q - 1 - h/2$.*

Proof: We can add at most $h/2$ additional lines and get a cover with precisely 1 hole. By the foregoing, it uses at least $2q - 1$ lines. \square

This is stronger than recent results in [7], and is best possible since $q - 1$ lines on a fixed point together with m lines on a different point on one of the earlier lines leave $h = 2(q - m)$ holes, and equality holds.

1.2 Covering the complement of a conic

Let q be odd. A cover of the complement of a conic in $PG(2, q)$ with elliptic lines is a partial cover with $h = q + 1$ holes, not all on a line. Hence

Proposition 1.6 *A cover of the complement of a conic in $PG(2, q)$, q odd, by elliptic lines, contains at least $3(q - 1)/2$ lines.* \square

This is best possible for $q = 3, 5, 7, 11$. In each of these four cases there is up to isomorphism a unique cover of the complement of a conic by elliptic lines. There is no other example of size $3(q - 1)/2$ for odd q , $q < 25$. (These results were obtained by a computer search for solutions of a differential equation for certain lacunary polynomials very much along the lines of Section 4 in [5].)

2 Variations

Another approach to the same material is via power sums.

Proposition 2.1 *Let $n > 0$. If $f = f(X_1, \dots, X_{n+1})$ is a homogeneous polynomial that vanishes in all points of $PG(n, q)$ except one, then f has degree at least $n(q - 1) + 1$.*

Proof: Let $F = \mathbb{F}_q$. If $0 \leq i < q - 1$ then $\sum_{x \in F} x^i = 0$.

Let $X^d = X_1^{d_1} \dots X_{n+1}^{d_{n+1}}$. If $\sum d_i < (n+1)(q-1)$, then $\sum_{x \in F^{n+1}} x^d = 0$ since for at least one of the d_i we have $0 \leq d_i < q - 1$.

Suppose f has degree at most $n(q-1)$. We may multiply f by some monomial and assume that f has degree precisely $n(q-1)$. This is less than $(n+1)(q-1)$ so f sums to 0 over all of F^{n+1} . The degree of f is a multiple of $q-1$, so f is well defined on $PG(n, q)$, and the sum over a 1-space (projective point) is

$q - 1$ times the value in any representative. But f is nonzero in precisely one projective point. Contradiction. \square

Note that this gives a new proof of Proposition 1.2 and 1.4(i).

Slightly more general is the following version, following the old Brouwer-Schrijver argument.

Proposition 2.2 *If $f = f(X_1, \dots, X_{n+1})$ is a nonzero polynomial that vanishes everywhere except on some nonempty subset of $\mathbb{F}_q^* a$, where a is a nonzero vector, then f has degree at least $n(q - 1) + 1$.*

Proof: We may take $a = (0, \dots, 0, 1)$ and take f reduced mod $X_i^q - X_i$ for all i , so that no exponents larger than $q - 1$ occur. If $x_1 \neq 0$ then $f(x_1, X_2, \dots, X_{n+1})$ vanishes identically and hence is the zero polynomial. It follows that f has a factor $X_1^{q-1} - 1$. The same holds for X_2, \dots, X_n , so $f = (X_1^{q-1} - 1) \dots (X_n^{q-1} - 1)g$ for some polynomial g . Since $f(0) = 0$ the polynomial g is not constant. \square

3 Almost covering curves or surfaces

Let an *almost cover* of a set be a cover of all points of the set except one (which is not covered).

Let C be a subset of $PG(n, q)$ given by the equation $f(X) = f(X_1, \dots, X_{n+1}) = 0$, where f is a polynomial with values in the subfield \mathbb{F}_r of \mathbb{F}_q (say, $q = r^m$). Suppose that C is almost covered by a collection of $d > 0$ hyperplanes. Let L be the product of the equations of these hyperplanes. Then $L \cdot (1 - f^{r-1})$ vanishes everywhere except in a single point and by Proposition 2.2 has degree at least $n(q - 1) + 1$.

For a quadric (f of degree 2, $q = r$), degenerate or not, we find $d + 2(q - 1) \geq n(q - 1) + 1$, so that $d \geq (n - 2)(q - 1) + 1$.

Proposition 3.1 *Let $n > 2$ and let Q be a quadric in $PG(n, q)$ that is not the union of two hyperplanes. Then Q has an almost cover of size $(n - 2)(q - 1) + 1$ but no smaller almost cover.*

Proof: We already proved the upper bound. It remains to construct an almost cover of that size. If $n > 3$ then use induction: pick q hyperplanes on a fixed $PG(n - 2, q)$ that can be chosen later, to cover all points except those in the last hyperplane $PG(n - 1, q)$ (and in that $PG(n - 1, q)$ this $PG(n - 2, q)$ is already covered). For $n = 3$ if there is a plane π that meets Q in a single point P (that is, if Q is not a hyperbolic quadric) then pick a line L in π not on P , and take for S the set of q planes other than π on L . Finally if Q is a hyperbolic quadric, let π be a plane meeting Q in a conic C . Let P be a point of C , and take for S the set of q tangent planes in the points of C other than P . \square

For a hermitean variety, given by $\sum_{i=1}^k X_i^{r+1} = 0$ ($3 \leq k \leq n + 1$), where $q = r^2$, we find that $d + q - 1 \geq n(q - 1) + 1$, so that $d \geq (n - 1)(q - 1) + 1$.

Proposition 3.2 *Let H be a hermitean variety in $PG(n, q)$ that is not the union of hyperplanes, where $q = r^2$. Then H has an almost cover of size $(n - 1)(q - 1) + 1$ but no smaller almost cover.*

Proof: The proof of the previous proposition can be copied starting from an almost cover of size q of a hermitean curve in $PG(2, q)$. Such an almost cover can be obtained by taking the $r^2 - r$ non-tangent lines through a point p not on the curve and covering all but one points of p^\perp by r lines. \square

In particular, an almost cover of a classical unital(=hermitean curve) in $PG(2, q)$ (where $q = r^2$) has at least q lines. This property might characterize classical unitals.

Among the 4466 designs $S(2, 4, 28)$ with nontrivial automorphism group ([10]) all except the classical unital have the property that for each choice of a point, the complement of the point is the union of 7 or 8 lines (while for the classical unital always 9 lines are needed).

Thas [12] shows for a unital U (a design with parameters $S(2, r + 1, r^3 + 1)$) embedded in $PG(2, r^2)$ that if the tangents of U at collinear points are concurrent, then U is classical. Dually it follows for an embedded unital that if the points of tangency of concurrent tangents are collinear, then U is classical. Now if U is a unital embedded in $PG(2, r^2)$ and $a \notin U$, then there are $r + 1$ tangents and $r^2 - r$ secants through a to U . If the points of tangency are not collinear, then for some p we can cover $U \setminus \{p\}$ with $r^2 - 1$ lines, violating the above property. This shows that this property characterizes the classical unital among the embedded unitals.

The same argument shows that in the classical unital a partial spread of deficiency 1 can be extended to a full spread.

For more general (affine) curves we can prove something slightly weaker:

Proposition 3.3 *Let C be a subset of size $N(> 1)$ of an affine curve \mathcal{C} of degree d in $AG(2, q)$, given by an equation of the form*

$$f(X, Y) = X^d - g(X, Y) = 0,$$

without linear component, where g has no term X^d . Then there is a point $P \in C$ such that in order to cover $C \setminus \{P\}$ one needs at least $t = (N/d) + (d - 3)/2$ lines.

The condition on g simply means that the infinite point $(1 : 0 : 0)$ does not belong to the projective closure of \mathcal{C} so this is no restriction.

Note that this improves the trivial lower bound $(N - 1)/d$ for $d > 2$.

Proof: Let

$$h(X, Y) = \prod_{i=1}^t (a_i X + b_i Y + c_i),$$

be a cover of $C \setminus \{P\}$. Then h is contained after reducing X^d to $g(X, Y)$ in the subspace of dimension $(t + 1)d - d(d - 1)/2$ of $\mathbf{F}[X, Y]$ spanned by the monomials $X^k Y^l$, $k + l \leq t$, $k < d$. If this can be done for each point $P \in C$, then $(t + 1)d - d(d - 1)/2 \geq N$. \square

Note that for some points a cheaper cover may exist. For example, one can find a 9-point curve \mathcal{C} of degree 4 in $AG(2, 4)$ that is the union of two conics that meet in P , where $C \setminus \{P\}$ can be covered by two lines.

4 Almost covering projective space by subspaces

Jamison [9] showed that one needs $q^{n-m} - 1 + m(q - 1)$ copies of $AG(m, q)$ to cover all points except one of $AG(n, q)$. How many $PG(m - 1, q)$'s are needed to cover all points but one in $PG(n - 1, q)$?

Proposition 4.1 *Let $m \leq n/2$. Then the complement of a $PG(n - m - 1, q)$ in a projective space $PG(n - 1, q)$ has a partition into copies of $PG(m - 1, q)$.*

Proof: Let $t = n - m$. The projective space $PG(2t - 1, q)$ can be partitioned into $PG(t - 1, q)$'s, and any two of these $PG(t - 1, q)$'s span $PG(2t - 1, q)$. Fix one of the $PG(t - 1, q)$'s, say Z , and let Y be a $PG(n - 1, q)$ containing Z . Then Y meets each of the other $PG(t - 1, q)$'s in a $PG(m - 1, q)$. \square

Using the fact that $PG(m - 1, q)$ minus a point has a cover with q copies of $PG(m - 2, q)$ and $q - 1$ copies of $PG(i - 1, q)$ for each i , $1 \leq i \leq m - 2$, we find

Proposition 4.2 *In the projective space $PG(mt + r - 1, q)$, where $0 \leq r \leq m - 1$, one can cover all points except one with*

$$\frac{q^{mt+r} - q^r}{q^m - 1} + (m - 1)(q - 1)$$

copies of $PG(m - 1, q)$.

Proof: Cover the complement of a $PG(m + r - 1, q)$ in $PG(mt + r - 1, q)$ by $PG(m - 1, q)$'s. Next, if $r > 0$, fill up $PG(m + r - 1, q)$ by $q^r + 1$ copies of $PG(m - 1, q)$ on a common $PG(m - r - 1, q)$. Finally, replace one of the $PG(m - 1, q)$'s. If $r = 0$ we had a partition, and need $(m - 1)(q - 1) + 1$ hyperplanes. If $r > 0$ then already a $PG(m - r - 1, q)$ was covered, and we need one hyperplane less. \square

We will show that this is best possible, essentially using Jamison's proof. Identify the vector space underlying $PG(mt + r - 1, q)$ with $\text{GF}(q^{mt+r})$. Then 'projective' functions can be represented by polynomials where all terms have degrees divisible by $q - 1$. The space of these functions is spanned by the monomials $X^{(q-1)k}$, $0 \leq k < (q^{mt+r} - 1)/(q - 1)$. A subspace $PG(m - 1, q)$ has an equation in the subspace

$$\langle 1, X^{q-1}, X^{q^2-1}, \dots, X^{q^m-1} \rangle$$

(cf. [2, 9]).

Now consider a covering of all points but one by a collection \mathcal{A} of $(m - 1)$ -spaces. This gives us the function

$$\prod_{a \in \mathcal{A}} (a_0 + a_1 X^{q-1} + \dots + a_m X^{q^m-1})$$

with the property that all monomials $X^{(q-1)k}$ with $(q - 1)k < q^{mt+r} - 1$ occur in the expansion of this product. Assume $|\mathcal{A}| = \frac{q^{mt+r} - q^r}{q^m - 1} + (m - 1)(q - 1) - 1$. We will show that the exponent $q^{mt+r} - q^r - (m - 1)(q - 1)$ does not occur in the expansion of this product. Indeed, suppose

$$\sum_{i=0}^m \alpha_i (q^i - 1) = q^{mt+r} - q^r - (m - 1)(q - 1)$$

where $\sum \alpha_i = |\mathcal{A}|$. If we add $|\mathcal{A}|$ to both sides we find

$$\sum_{i=0}^m \alpha_i q^i = q^m \frac{q^{mt+r} - q^r}{q^m - 1} - 1$$

which is $-1 \pmod{q^m}$ so that $\sum_{i=0}^{m-1} \alpha_i \geq m(q-1)$. Given $|\mathcal{A}|$, the sum $\sum_{i=0}^m \alpha_i q^i$ is maximal when α_m is maximal. Hence

$$\sum_{i=0}^m \alpha_i q^i \leq \left(\frac{q^{mt+r} - q^r}{q^m - 1} - q \right) q^m + q^m - 1,$$

contradiction. We showed

Proposition 4.3 *In the projective space $PG(mt+r-1, q)$, where $0 \leq r \leq m-1$, one cannot cover all points except one with fewer than*

$$\frac{q^{mt+r} - q^r}{q^m - 1} + (m-1)(q-1)$$

copies of $PG(m-1, q)$. □

Note that one can cover all points of $PG(mt+r-1, q)$ with $\frac{q^{mt+r} - q^r}{q^m - 1} + 1$ copies of $PG(m-1, q)$, and this is best possible (for $1 \leq r \leq m$), see [4, 8].

5 Fractional versus integral covers

In [11] Lovász shows that a hypergraph (that is a set system) with fractional covering number τ^* and point degrees bounded by d there exists an integral cover of size $\tau \leq (1 + \log d)\tau^*$. Here a cover of a set system is a set of points intersecting each member of the set system. Almost covering $PG(n, q)$ by hyperplanes has $d = q^{n-1}$ and $\tau^* = q$ and $\tau = n(q-1) + 1$, so we essentially have this ratio up to a factor $\log q$. Something similar holds for the hermitean surface in $PG(n, q)$.

References

- [1] N. Alon & Z. Füredi, *Covering the Cube by Affine Hyperplanes* Europ. J. Comb. **14** (1993) 79–83.
- [2] S. Ball, *Polynomials in Finite Geometries*, in: *Surveys in Combinatorics*, 1999, Edited by J.D. Lamb & D.A. Preece 17–36.
- [3] S. Ball & O. Serra, *Punctured combinatorial Nullstellensätze*, *Combinatorica*, to appear.
- [4] A. Beutelspacher, *On t -covers in finite projective spaces*, *J. Geometry* **12** (1979) 10–16.
- [5] A. Blokhuis & A.E. Brouwer & H.A. Wilbrink, *Blocking sets in $PG(2, p)$ for small p , and partial spreads in $PG(3, 7)$* , in: special issue dedicated to Adriano Barlotti, *Adv. Geom.* (2003), suppl., S245–S253.

- [6] A. E. Brouwer & A. Schrijver, *The blocking number of an affine space*, J. Combin. Th. (A) **24** (1978) 251–253.
- [7] S. Dodunekov, L. Storme & G. Van de Voorde, *Partial covers of $PG(n, q)$* , preprint, Aug. 2008.
- [8] J. Eisfeld, *On smallest covers of finite projective spaces*, Arch. Math. **68** (1997) 77–80.
- [9] R. E. Jamison, *Covering finite fields with cosets of subspaces*, J. Combin. Th. (A) **22** (1977) 253–266.
- [10] V. Krčadinac, *Steiner 2-designs $S(2,4,28)$ with nontrivial automorphisms*, Glasnik Matematički **37 (57)** (2002) 259–268.
- [11] L. Lovász, *On the ratio of optimal integral and fractional covers*, Discrete Math. **13** (1975) 383–390.
- [12] J. A. Thas, *A Combinatorial Characterization of Hermitian Curves*, J. Alg. Combin. **1** (1992) 97–102.