Bounds on sets with few distances modulo a prime in metric spaces of strength t
Blokhuis, A.; Singhi, N.M.

Published: 01/01/1981

Citation for published version (APA):
Bounds on sets with few distances
modulo a prime in metric spaces of strength $t$

by

A. Blokhuis - N.M. Singhi
Bound on sets with few distances
modulo a prime in metric spaces of strength t

by

A. Blokhuis - N.M. Singhi

0. Abstract

In this paper we prove an extension and slight generalization of a theorem of FRANKL and WILSON. [3]

Theorem: Let \((X,d)\) be a metric space of strength \(t\), and \(B \subseteq X\).

For a prime \(p\) and integer \(s\) let

(i) \(d^2(a,b) \in \mathbb{N}\) for all \(a,b \in B\)

(ii) \(d^2(a,b) \not\equiv 0 \pmod{p}\) for all \(a,b \in B\)

(iii) \# \{d^2(a,b) \pmod{p} \mid b \in B\} \leq s \leq \frac{1}{t}t\) for all \(a \in B\).

Then \(\text{card } B \leq \sum_{i=0}^{s} \dim \text{Harm}(s)\).

1. Preliminaries

All statements, propositions and definitions in this section are quoted from [1] (chapter 9).

Let \((X,d)\) be a metric space of finite diameter \(\sqrt{\delta}\). Call \(c_{xy} = d^2(x,y)\), whence \(0 \leq c_{xy} \leq \delta\). Let \(\omega\) denote a finite measure on \(X\), with

\[
\omega(X) = \int_X d\omega = w < \infty
\]

then \(\omega\) induces a measure \(\hat{\omega}\) on \(X \times X\). Let \(S\) be the set \(\{c_{xy} \mid x,y \in X\} \).
Then \( \hat{\omega} \) induces a finite measure \( \mu \) on \( S \). For \( A \in S \)

\[
\mu(A) = \frac{1}{\omega} \hat{\omega}\{x, y \mid c_{xy} \in A\}.
\]

The set of polynomials \( 1; x; x^2; \ldots \) can be orthonormalized w.r.t. the inner-product

\[
<f, g> = \int_S f(\alpha)g(\alpha)d\mu(\alpha)
\]

to give a set of polynomials \( \{q_i\}_{i=0}^{\infty} \) such that

\[
\int_S q_i(\alpha)q_j(\alpha)d\mu(\alpha) = \delta_{ij}
\]

where \( q_i \) is a polynomial in one variable of degree \( i \).

**Definition:** A metric space \((X,d,\omega)\) has **strength** \( t \) if

\[
\int_X c_{ax}^i c_{bx}^j d\omega(x) = f_{ij}(c_{ab}) \quad \forall i, j : i + j \leq t
\]

where \( f_{ij} \) denotes a polynomial of degree \( \leq \min(i, j) \).

**Comment:** A metric space of strength \( t \) for all \( t \) is called a Delsarte space.

Delsarte spaces of finite degree (i.e. where \( S \) is a finite set) are essentially the Q-polynomial schemes. Other examples are the compact symmetric spaces of rank 1, the real sphere, a real, complex or quaternion projective space, or the Cayley projective plane. A \( t \)-design, or spherical \( t \)-design, considered as a metric space by itself, is a metric space of strength \( t \) (cf. [1], page 66).

**Proposition:**

\[
\int_X q_i(c_{ax})q_j(c_{bx})d\omega(x) = q_1(0)q_i(c_{ab})\delta_{ij} \quad \text{if} \quad i + j \leq t.
\]
Definition: Harm(i) is the space of functions on X generated by the set
\[ \{ x \rightarrow q_i(c_{ax}) \mid a \in X \} . \]

Remark: By the proposition above we have Harm(0) \ldots \subseteq Harm(\lceil t/2 \rceil) with respect to the nondegenerate innerproduct:
\[ <f, g> = \int_X f(x)g(x)d\omega(x) . \]

Proposition: For \( i \leq \lceil \frac{t}{2} \rceil \) : \( \dim \text{Harm}(i) = q_i(x)^2 \omega \).

Remark: The actual values of \( \dim \text{Harm}(i) \) for the projective spaces can be found in HOGGAR [4].

Notation: \( H(s) := \text{Harm}(0) \oplus \ldots \oplus \text{Harm}(s) \).

2. Some lemma's

Lemma 1: Let \( s \leq \lceil \frac{t}{2} \rceil \). For all \( x \in X \) \( \exists \xi \in H(s) \) s.t. \( \forall f \in H(s) : <\xi, f> = f(x) \).

Proof: \( H(s) \) is finite dimensional, hence isomorphic to its dual. Furthermore the innerproduct is nondegenerate.

Lemma 2: Let \( M \) be a nonempty finite set of real numbers. Let \( \mathbb{Z}M \) be the set of all \( \mathbb{Z} \)-linear combinations of elements from \( M \). Then \( \mathbb{Z}M \subseteq p\mathbb{Z}M \) for some prime \( p \) implies \( M = \{0\} \).
Proof: This is a consequence of Krull's theorem [5], page 10. We'll give a proof for the sake of completeness.

QM is a finite dimensional vector space over Q. Write the elements of M as vectors over some fixed basis of this vectorspace. For \( m \in QM \) let \( p(m) := \) the minimal exponent of \( p \) in all coordinates of \( m \) (where \( p(0) := +\infty \)).

Now obviously \( p(m + n) \geq \min\{p(m), p(n)\} \). Therefore:

\[
\min_{m \in \mathbb{Z}M} p(m) = \min_{m \in M} p(m) = 1 + \min_{m \in pM} p(m)
\]

hence \( M = \{0\} \).

3. Proof of the theorem

We will show that \( \hat{B} \) (where \( \hat{\cdot} \) is as in Lemma 1) is an independent subset of \( H(s) \).

Now suppose this is not the case. We then have a dependency relation

\[
\sum_{b \in B} m_b \hat{b} = 0.
\]

For \( a \in B \) define \( F_a(u) = \prod_{i=1}^{s} (a_i - u) \) and \( f_a(x) = F_a(c_a x) \) here \( \{a_1, \ldots, a_s\} = \{c_{ab} \pmod{p} \mid b \in B\} \). Since \( F_a \) is a polynomial of degree \( s \) we have \( f_a \in H(s) \). This yields

\[
\sum_{b \in B} m_b \langle \hat{b}, f_a \rangle = 0.
\]

Now:
\( \langle b, f_a \rangle \equiv 0 \pmod{p} \) if \( b \neq a \),
\( \langle \hat{a}, f_a \rangle = \prod a_i \not\equiv 0 \pmod{p} \).

So we get \( m_a \in p\mathbb{Z}M \), where \( M = \{m_b \mid b \in \hat{B}\} \).
Since a was arbitrary we get $\mathbb{Z}M \in p\mathbb{Z}M$ but from Lemma 2 this implies

$$m_b = 0 \ \forall b \in B.$$ 

This finishes the proof of the theorem.

4. Final remarks

The theorem (and its proof, with some minor adjustments) is still valid if we replace $\mathbb{N}$ and $\mathbb{Z}$ by a unique factorization domain $D \subset \mathbb{R}$; and $Q$ in the proof of Lemma 2 by $Q \cap D$.

5. References:


