Orthogonal Latin squares in low dimensions

Máté Matolcsi

Budapest University of Technology
Budapest, Hungary

(joint work with M. Weiner)

Overview

- The Delsarte LP-bound in general
- An improvement in special cases
- Application: orthogonal Latin squares

Delsarte LP-bound (the set-up)

A general problem

$\mathcal{G}$ (finite) Abelian group, $0 \in S = -S \subset \mathcal{G}$ symmetric set.

$\Delta(S) = \max\{|A| : (A - A) \cap S = \{0\}\} =?$

(Independence number of the Cayley graph corresponding to $S \subset \mathcal{G}$.)

Examples:

- Sphere-packing: what is the maximal density of a packing of unit spheres in $\mathbb{R}^n$? $G = \mathbb{R}^n$, $S = B(0, 2)$. Exact bound by Maryna Viazovska in dimensions 8, 24.
- Sets avoiding the unit distance: what is the maximal density of a measurable set A in $\mathbb{R}^2$ such that $|a - a'| \neq 1$ for all $a, a' \in A$? $G = \mathbb{R}^2$, $S =$ unit circle $\cup\{0\}$. Best bound so far: *dens* $A \leq 0.2587$ by Filho, Keleti, M., Ruzsa.)
- Orthogonal Latin squares ($G =?$, $S =?$)

Delsarte LP-bound (Fourier formulation)

Observation: $f(x) = |A \cap (A - x)|$ =(number of solutions to $x = a - a'$)

is a positive definite function on G. Also, f is zero on S and $\hat{f}(\mathbf{1}) = \sum f(x) = |A|^2, f(0) = |A|$.

Delsarte LP-bound

$\Delta(S) \leq$

$\sup\{\frac{\hat{f}(\mathbf{1})}{f(0)} : \ f(x) \geq 0 \ \forall x \in \mathcal{G}, f(x) = 0 \ \forall x \in S \setminus \{0\}, \hat{f}(\gamma) \geq 0 \ \forall \gamma \in \hat{\mathcal{G}}\} =$

$\inf\{\frac{h(0)}{\hat{h}(\mathbf{1})} : \ h(x) \leq 0 \ \forall x \in S^c, \hat{h}(\gamma) \geq 0 \ \forall \gamma \in \hat{\mathcal{G}}\}$

Last equality by linear duality. Best possible functions f or h can be found by linear programming (LP). Function h is called a *witness function.*

Delsarte LP-bound – an improvement

A general problem

$\mathcal{G}$ (finite) Abelian group, $0 \in S = -S \subset \mathcal{G}$ symmetric set.

$\Delta(S) = \max\{|A| : (A - A) \cap S = \{0\}\} = ?$

What if some elements $a_1, \dots a_k \in A$ are already given. Can we improve the Delsarte LP-bound in this case?

Theorem (M., Weiner, 2015)

Assume h is a witness function in Delsarte's LP-bound, giving $\Delta(S) \leq \frac{h(0)}{\hat{h}(\mathbf{1})} = m \in \mathbb{Z}$. Assume $a_1, \dots a_k \in A$ are already given, $a_i - a_j \in S^c$. Let D be the set of "candidate" elements d in G such that $d - a_i \in S^c$ for all a_i. Assume there is a function $K : G \to \mathbb{R}$ such that

$\hat{K}(\mathbf{1}) = 0$, and $\hat{K}(\gamma) = 0$ whenever $\hat{h}(\gamma) = 0$

$\sum_{j=1}^{k} K(a_j) = 1$

$K(x) \geq \frac{-1}{m-k}$ for all $x \in D$

Then $|A| \leq m - 1$. (K is called a *second witness function.)*

Latin squares

A Latin square L is an $n \times n$ squares filled out with numbers $0, 1, \ldots, n-1$ such that each row and each column contains each symbol exactly once.

Two Latin squares L_1, L_2 are called orthogonal if the ordered pairs $(L_1(i,j), L_2(i,j))$ exhaust all possible n^2 arrangements as i and j range from 1 to n.

Problem

What is the maximal number $L(n)$ of mutually orthogonal Latin squares (MOLs) in dimension n?

Well-known results

$L(n) \leq n-1$ for all n
$L(n) = n-1$ if n is a prime power.

The existence of a complete set of $n-1$ orthogonal Latin squares is equivalent to the existence of a finite projective plane of order n.

Delsarte-bound for Latin squares I.

So, how does the problem of Latin squares fit into the Delsarte scheme?

Let $G = \mathbb{Z}_n^n$. We associate vectors in G to a complete set of orthogonal Latin squares $L_1, \ldots, L_{n-1}$.

Associated vectors

Let $v_j^k \in G$ be the vector corresponding to the positions of symbol k in L_j: the mth coordinate of v_j^k is the index of the column in which the symbol k appears in the mth row of L_j.

We append this system with the constant vectors $(k, k, \ldots, k)$ for $k = 0, \ldots, n-1$. In this way we obtain n^2 vectors in G.

Delsarte-bound for Latin squares II.

These n^2 vectors have the following properties:

if u, v come from the same Latin square then $u - v$ has no 0 coordinate.
if u, v come from different Latin squares then $u - v$ has exactly one 0 coordinate.

So, in the Delsarte formulation: $G = \mathbb{Z}_n^n$, $S = \{$vectors with more than one 0 coordinates$\}$. For finding a witness function h it is better to think of G as the cyclic group of nth roots of unity.

Witness function

Let $h(z_1, \ldots, z_n) = \left(\sum_{j=1}^{n} \sum_{k=0}^{n-1} z_j^k\right)\left(-n + \sum_{j=1}^{n} \sum_{k=0}^{n-1} z_j^k\right)$.
Then $h(\mathbf{1}) = n^2(n^2 - n)$ and $\hat{h}(0) = n^2 - n$, so the Delsarte bound gives $|A| \leq n^2$, which is sharp if n is a prime power.

The improved bound and implications

How can we go about proving non-existence of complete sets of MOLs in dimension 6 or 10? Or uniqueness of complete sets (up to isomorphisms) in dimension 7 and 8?

Brute force method: if vectors $v_1, \ldots, v_k \in G$ are already selected then we can list the set of further candidate vectors $u \in G$ such that $u - v_j$ has at most one 0 coordinate. If at any point we find no such vectors u, we can stop and conclude that the system $v_1, \ldots, v_k$ cannot be extended any further. This is very slow.

Use the improved Delsarte bound

Instead we use the improved Delsarte bound: if vectors $v_1, \ldots, v_k \in G$ are already selected and we find a suitable second witness function K, then we can conclude that the system $v_1, \ldots, v_k \in G$ cannot be extended to a *complete system of n^2 vectors.*

The function K, if it exists, can be found by linear programming. This is much faster than the brute force method.

Results

The efficiency of the method depends on how many vectors $v_1, \ldots, v_k$ we typically need for a second witness function K to exist. As long as the dimension is small, it is very efficient. Results are summarized below:

Corollaries (M., Weiner, 2017)

For $n = 6$ there exist no complete set of MOLs.
For $n = 7, 8$ complete sets of MOLs exist and are unique.

These results were known anyway... For $n = 9, 10$ the method still looks feasible with enough computing power. However, $n = 12$ seems far out of range.

Thank you for your attention