

Definition 0.1. Fix an algebraic structure \mathbb{R} and a set of polynomials $\mathcal{F} = \{F_i\}$. Let d be a non-negative integer. A d -design for \mathbb{R} is a mapping D from \mathbb{R} -polynomials of degree $\leq d$ to \mathbb{R} such that:

1. $D(1) = 1$
2. D is linear, which means $D(X + Y) = D(X) + D(Y)$.
3. $D(Q \cdot F_i) = 0$ for any polynomial Q and $F_i \in \mathcal{F}$ such that $\deg(Q) + \deg(F_i) \leq d$.
4. $D(x_i^2 Q) = D(x_i Q)$, where x is a variable in $R[x_1, x_2, \dots, x_n]$ and $\deg(Q) < d - 1$.

Notice that the mapping D is actually determined by the values it assigns to monomials of degree less than d , since it is a linear mapping and any polynomial can be decomposed into some monomials. Furthermore, due to property 4, it suffices to consider only multilinear monomials when determining the value of D . Alternatively, we can assume that \mathcal{F} includes $x_i(x_i - 1)$ for all i , in which case property 3 implies property 4.

Naturally, for multilinear monomials, we can view them as conjunctions of the atomic statements represented by the propositional variables in the monomial. Furthermore, we found there is a connection between d -designs and Nullstellensatz refutation of degree d . Next, two theorems describe this connection.

Theorem 0.1. If \mathcal{F} exists a d -design, then there cannot be a Nullstellensatz refutation of degree $\leq d$ to refute \mathcal{F} .

Proof. If there exists a Nullstellensatz refutation of degree $\leq d$, then

$$1 = \sum_i P_i \cdot F_i + \sum_j Q_j \cdot (x_j^2 - x_j)$$

. Using the d -design for \mathcal{F} ,

$$D(1) = 1 \neq 0 = \sum_i D(P_i \cdot F_i) + \sum_j D(Q_j x_j^2) - D(Q_j x_j)$$

□

A converse of the above theorem, to some extent, also holds:

Theorem 0.2. Suppose the algebraic structure \mathbb{R} is a field. If \mathcal{F} does not have a Nullstellensatz refutation of degree d , then there is a d -design for \mathcal{F} .

Proof. Suppose there are n variables used in our proposition. Let δ be the number of monomials of degree $\leq d$. Then we can calculate $\delta = \sum_{i=0}^d \binom{n+i-1}{i}$. Recall that $\binom{n+i-1}{i} = \binom{n+i-1}{n-1}$. It means δ is not infinite. Then for any polynomial H of degree $\leq d$, it can be viewed as a vector \mathbf{v}_H where each element a_Q is the coefficient of a monomial Q . Therefore, \mathbf{v}_H has dimension δ .

Let \mathcal{G} be a set of polynomials in the form $Q \cdot F$, where Q is a monomial and $F \in \mathcal{F}$, and $\deg(Q \cdot F) \leq d$. For simplicity, we consider \mathcal{F} to include all polynomials of the form $x_i(x_i - 1)$. Each $g_i \in \mathcal{G}$ can be viewed as a vector \mathbf{v}_{g_i} , analogous to what was done for H .

Define a vector \mathbf{v}_1 with only one nonzero element on the constant term. A Nullstellensatz refutation of degree at most d exists if and only if there is an R -linear combination of the vectors $\{\mathbf{v}_{g_i}\}$. Let \mathbf{M} be the $\delta \times |\mathcal{G}|$ matrix with columns \mathbf{v}_{g_i} , where $\delta = \sum_{i=0}^d \binom{n+i-1}{i}$. This is equivalent to finding a solution \mathbf{w} to the linear equation $\mathbf{M}\mathbf{w} = \mathbf{v}_1$.

It's equivalent to checking whether the rank of coefficient matrix \mathbf{M} equals the rank of the augmented matrix $[\mathbf{M}, \mathbf{v}_1]$. Since there is only one nonzero element in \mathbf{v}_1 , that element cannot be a linear combination of zeros. It's therefore equivalent to checking whether the last row of \mathbf{M} is a linear combination of other rows in \mathbf{M} .

Thus, there is a Nullstellensatz refutation of degree $\leq d$ if and only if the last row of \mathbf{M} is linearly independent of the rest of the row vectors. If the last row is a linear combination, we can indeed find a possible d -design. Denote

each row as \mathbf{u}_Q where Q corresponds to that row. Suppose the combination is

$$\sum_{\deg(Q) \leq d} \alpha_Q \mathbf{u}_Q = 0. \quad (1)$$

Then we can actually use α_Q as $D(Q)$ for all monomials Q , and $D(1) = 1$.

The rest is to check if D is valid. Since it's sufficient that all properties hold for monomials, we only need to consider the case for monomials. For any monomial Q and $F \in \mathcal{F}$, $Q \cdot F$ must be in \mathcal{G} . Because this is a column in matrix \mathbf{M} , equation (1) holds for the column $Q \cdot F$. Then $D(Q \cdot F) = D(\sum_{\deg(Q) \leq d} \alpha_Q u_Q^{Q \cdot F}) = 0$. It's not difficult to check that D is linear. \square