15 Sums of squares on the hypercube

In this lecture we look at polynomial optimisation on the hypercube $S = \{-1,1\}^n$. One way to certify that a polynomial f is nonnegative on $\{-1,1\}^n$ is to try to express it in the following way:

$$f(x) = \sum_{i=1}^{l} q_i(x)^2 + \sum_{i=1}^{n} (x_i^2 - 1) h_i(x) \tag{1}$$

where q_i and h_i are arbitrary polynomials. It is clear that any f of the form (1) is nonnegative on $\{-1,1\}^n$. For example consider the function $f(x) = 1 + x_1$. Clearly f is nonnegative on $\{-1,1\}^n$ and one can verify that we have the following certificate of nonnegativity $1 + x_1 = \frac{1}{2}(1+x_1)^2 + (x_1^2 - 1) \cdot (-1/2)$.

Functions on the hypercube can be expressed in a specific basis, called the basis of *square-free monomials* (also known as *multilinear monomials*). A square-free monomial is a monomial of the form $x^S := \prod_{i \in S} x_i$ where $S \subseteq [n]$ (we use the notation $[n] := \{1, \ldots, n\}$).

Proposition 15.1. *Any function $f : \{-1,1\}^n \to \mathbb{R}$ can be expressed as*

$$f(x) = \sum_{S \subseteq [n]} f_S x^S \quad \forall x \in \{-1,1\}^n \tag{2}$$

for some coefficients $(f_S)_{S \subseteq [n]}$.

Proof. Let $a \in \{-1,1\}^n$ and let $\delta_a(x)$ be the function that takes value 1 at a and 0 elsewhere. Note that δ_a can be expressed as:

$$\frac{1}{2^n} \prod_{i=1}^{n} (1 + a_i x_i). \tag{3}$$

Expanding the product we see that δ_a is a linear combination of the square-free monomials. Finally since each function is a linear combination of the δ_as we get the desired result. ☐

Definition 15.1. We say that a function $f : \{-1,1\}^n \to \mathbb{R}$ is *k-sos on* $\{-1,1\}^n$ if it is a sum-of-squares of polynomials of degree at most k on $\{-1,1\}^n$, i.e., if there exists polynomials $q_1, \ldots, q_l$ of degree at most k such that $f(x) = \sum_{i=1}^{l} q_i(x)^2$ for all $x \in \{-1,1\}^n$.

Remark 1. *One can show (using e.g., the division algorithm for polynomials in more than one variable) that f is k-sos on $\{-1,1\}^n$ if and only if it can expressed as (1) where $\deg q_i \leq k$ for all $i = 1, \ldots, l$ and $\deg h_i \leq 2k - 2$ for all $i = 1, \ldots, n$ (assuming $\deg f \leq 2k$).*

Example 15.1.

- *The function $f(x) = 1 + x_1$ is 1-sos on $\{-1,1\}^n$ because $1 + x_1 = \frac{1}{2}(1+x_1)^2$ on $\{-1,1\}^n$.*

- *Any nonnegative function f on $\{-1,1\}^n$ is n-sos. Indeed we have $f = g^2$ on $\{-1,1\}^n$ where $g : \{-1,1\}^n \to \mathbb{R}$ is defined by $g(x) = \sqrt{f(x)}$. By Proposition 15.1 we know that g is a polynomial of degree at most n. Another way of seeing this same fact is to observe that the delta function δ_a defined in (3) satisfies $\delta_a = \delta_a^2$ and so we have:*

$$f = \sum_{a \in \{-1,1\}^n} f(a) \delta_a^2 \tag{4}$$

Since $f(a) \geq 0$ and each δ_a is a polynomial of degree at most n (cf. (3)), (4) shows that f is n-sos.

Degree cancellations: There is an important difference that one must keep in mind between (i) sum-of-squares certificates on the hypercube, and (ii) global sum-of-squares certificates. When writing a global sum of squares certificate for a polynomial f on $\mathbb{R}^n$, i.e., $f(x) = \sum_{i=1}^{l} q_i(x)^2$ for all $x \in \mathbb{R}^n$ then necessarily $\deg q_i \leq (\deg f)/2$. When working on $\{-1,1\}^n$ however, such degree bounds on the q_i's do not hold anymore as there can be *degree cancellations*. This is already evident in the two examples above (Example 15.1).

The next theorem shows that deciding whether a function $f : \{-1,1\}^n \to \mathbb{R}$ is k-sos is a semidefinite feasibility problem.

Theorem 15.1. *A function $f : \{-1,1\}^n \to \mathbb{R}$ is k-sos on $\{-1,1\}^n$ if and only if there exists a positive semidefinite matrix Q of size $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k}$ such that*

$$f_S = \sum_{\substack{U,V \subseteq [n] \\ |U|,|V| \leq k \\ U \triangle V = S}} Q_{U,V} \qquad \forall S \subseteq [n],\ |S| \leq 2k$$

where f_S is the coefficient of f in the expansion (2), and $U \triangle V$ is the symmetric difference of U and V, i.e., $U \triangle V = (U \setminus V) \cup (V \setminus U)$.

Proof. The proof is very similar to Theorem 13.2. Simply use the fact that $x^U x^V = x^{U \triangle V}$ on $\{-1,1\}^n$. $\square$