Flag algebras and extremal combinatorics

Note: These are very rough scribe notes of what was covered by Pablo Parrilo. Please see the video for more complete coverage.

Look at the problem of certifying $p(x) \geq 0$ for symmetric polynomial $p$.

Example: Compute $\alpha(G)$ where $G$ is the Hamming weight graph with vertices corresponding to $\{0, 1\}^n$ and edges corresponding to pairs with Hamming distance at most $k$. In this case $\alpha(G)$ is the maximum size of an error correcting code of block length $n$ and distance $k$.

1. Definition. Let $\mathcal{G}$ be a group of linear transformations over $\mathbb{R}^n$. We say that a polynomial $p$ is $\mathcal{G}$ symmetric if $p(x) = p(\tau(x))$ for every $\tau \in \mathcal{G}$.

Digression to representation theory.

A representation is $\rho: \mathcal{G} \to GL(V)$ where $V$ is a subspace which is homomorphic.

Example: $S_2$: group of permutations on set of two elements. We can write $S_2 = \{e, g\}$, $g^2 = e$ and $e$ is the identity element.

Natural representation is $\rho: S_2 \to GL(\mathbb{R}^2)$ where $\rho(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\rho(g) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. That is $\rho(e)$ is the map $(x, y) \mapsto (x, y)$ while $\rho(g)$ is the map $(x, y) \mapsto (-y, x)$.

This representation has two invariant one dimensional subspaces $\{x = y\}$ and $\{x = -y\}$. Restricting it to these two subspaces gives the trivial representation and the alternating / sign representation where $\rho(g) = +1$ and $\rho(e) = -1$.

An invariant subspace of a representation $\rho: \mathcal{G} \to GL(V)$ is a subspace $W \subseteq V$ such that $\rho(GgW) = W$ for all $g \in \mathcal{G}$. We say that an invariant subspace is trivial if $W = V$ or $W = \{0\}$. An irreducible representation (irrep) is a representation without any non-trivial invariant subspace.

We say that two representations $\rho: \mathcal{G} \to GL(V)$ and $\rho': \mathcal{G} \to GL(V')$ are equivalent if there is an invertible linear transformation $T: V \to V'$ such that

$$\rho(g) = T^{-1}\rho'(g)T$$

for every $g \in \mathcal{G}$. 
Example 2: $S_3$ - group of permutations on set of three elements. We can write $S_3 = \{e, s, c, c^2, cs, sc\}$ where in cycle notation $s = (1, 2)$ and $c = (1, 2, 3)$. The relations that this satisfies is $c^3 = e$, $s^2 = e$ and $s = cs$. We can express the possible irreps in a Young tableus that satisfy the relation $n! = \sum d_i^2$.

Example 3: $C_n = \{0, \ldots, n-1\}$ with addition modulo $n$. We can represent this in $n$ ways with $\rho_k(j) = \omega^{kj}$ for $\omega = e^{2\pi i/n}$. (In Abelian group all irreps have dimension one.)

Convexity and symmetry

Suppose we want to minimize a univariate function $f : \mathbb{R} \to \mathbb{R}$ and suppose that it is symmetric in the sense that $f(x) = f(-x)$. A priori that gives us no information about it, but if we add the condition that $f$ is convex then we can deduce that it must have a global minimum at $x = 0$.

More generally, we say that $f : V \to \mathbb{R}$ is symmetric with respect to a group $G$ and a representation $\rho$ if $f(\rho(g)x) = f(x)$ for all $g \in G$.

2. Lemma. If $f$ is symmetric w.r.t. $G, \rho$ and convex then it always has a minimum $x$ that satisfies the property that $x = \rho(g)x$ for every $g \in G$.

Proof. Given $x$ which achieves the minimum of $f$, by symmetry and convexity, the same will hold for $x' = \frac{1}{|G|} \sum_{g \in G} \rho(g)x$, but it is not hard to verify (exercise!) that the latter will satisfy the above property. 

For a group $G$ and a representation $\rho : G \to V$, we define the fixed point subspace of $\rho$ to be $\{ x \in V : x = \rho(g)x \forall g \in G \}$. (Exercise: Verify that this is indeed a linear subspace.)

Example: Lovasz theta function

Consider the following convex relaxation for the independent set problem:

For an $n$ vertex graph $G$, recall that the independent set number is defined as $\alpha(G) = \max \sum x_i$ over $x \in \{0, 1\}^n$ such that $x_ix_j$ for all $i \sim j$ in $G$. We can relax this as $\vartheta(G) = \max Tr(JX)$ over all p.s.d.
matrices $X \succeq 0$ such that $\text{Tr}(X) = 1$, $X_{i,j} = 0$ for all $i \sim j$ and where $J$ is the all 1’s matrix.

For every $G$, the value $\vartheta(G)$ can be thought of as the maximum of a concave (in fact linear) function over a convex set and so also as minimizing a convex function. If the graph itself has symmetries then $\vartheta$ itself has symmetries and so its minimum is known to lie in some nice space. For example, if the graph is the cycle, then the minimum is achieved by a matrix $X$ which is circulant.

**Semidefinite programs and representations.**

In sos programs the representations inherit the symmetry in the instance in a “nice form” which is that if $X \in \mathbb{R}^{n \times n}$ is a matrix representing the degree 2d sos solution and $\rho : \mathcal{G} \to GL(\mathbb{R}^n)$ is a representation with respect to the original function is symmetric, then if we let $\rho' : \mathcal{G} \to GL(\mathbb{R}^{nd})$ be the representation obtained by tensoring $\rho$ then the value of $X$ as a solution to the sos program equals the value of $\rho'(g)^\top X \rho'(g)$ for all $g \in \mathcal{G}$. This allows to use Shor’s Lemma to reduce the study of solution to a potentially much smaller number of equivalence classes.

**Examples:**

- Minimizing univariate $p(x)$ that satisfies $p(x) = p(-x)$ and hence $p(x) = q(x^2)$.
- Minimizing $p(x)$ over $x \in \{0, 1\}^n$ such that $p$ is $S_n$-symmetric and hence $p(x) = q(\frac{1}{n} \sum x_i)$ for some $q$.
- In coding, we can bound the best possible rate of a code with given distance (which is the logarithm of the independence number of the Hamming graph) by the $\vartheta$ function, which corresponds to degree 2 sos, and analyze it using symmetry which allows to reduce this SDP to an LP. A more sophisticated bound was given by looking at the degree 4 sos.

**References**