Algorithmic Invariant Theory

Gregor Kemper

Invariant theory can be put in a very general context: If "$\sim$" is an equivalence relation on a set X, then an **invariant** is a function on X which is constant on every equivalence class. So invariants serve to parametrize equivalence classes. The goals of invariant theory are to find all invariants that meet some further restrictions (such as continuity or polynomiality), and to study to which extent these invariants separate equivalence classes. For example, the determinant of a square matrix is an invariant w.r.t. the equivalence relation given by similarity.

In the classical situation of invariant theory, the equivalence classes are given by the orbits of a group action. In fact, one considers the following setting: G is a linear algebraic group over an algebraically closed field K, and V is a finite-dimensional K-vector space with a linear G-action, given by a morphism $G \times V \to V$. In other words, we assume that the action can be described by polynomial functions. A natural extension is to substitute V by an affine K-variety X, which is then called a **G-variety**. The **invariant ring**

$$K[V]^G := \{f \in K[V] \mid f \circ \sigma = f \text{ for all } \sigma \in G\}$$

consists of all polynomials $f\colon V \to K$ which are constant on every G-orbit. Observe that the above example of the determinant of a square matrix falls into this situation, with $G = \mathrm{GL}_n(K)$ acting on $V = K^{n\times n}$ by conjugation. The following questions are central in invariant theory:

- *Hilbert's 14th Problem*: Is $K[V]^G$ finitely generated as a K-algebra?
- If so, find generators (algorithmically).
- Which G-orbits can be separated by invariants, i.e., for which $x, y \in V$ does there exist $f \in K[V]^G$ with $f(x) \neq f(y)$?

Invariant theory has gone a long way towards answering Hilbert's 14th Problem. In fact, it is known by results of Hilbert, Nagata, Haboush and Popov that $K[X]^G$ is finitely generated for all G-varieties X if and only if G is reductive. However, it happens quite often that for a given non-reductive group G and a given linear representation V, the invariant ring $K[V]^G$ is finitely generated in spite of this result. So the problem to classify all pairs (G, V) or (G, X) such that the invariant ring is finitely generated is still open. Note that the class of reductive groups include all finite groups and all classical groups.

The algorithmic side of the problem has been trailing behind the theoretical progress, but has by now almost completely caught up. In fact, we do have an algorithm for computing generators of $K[X]^G$ in the case that G is reductive and X is a G-variety. Major stepping stones towards this algorithm were provided by Derksen's algorithm, which solves the problem for linearly reductive groups, and by an algorithm for computing separating invariants, a topic that we will address shortly.

If G acts linearly on V, then the invariant ring $K[V]^G$ is a graded algebra. If it is finitely generated, there exists a number, written as $\beta\left(K[V]^G\right)$, which is the smallest d such that $K[V]^G$ can be generated by homogeneous invariants of degree $\leq d$. This number is interesting since any upper bound for $\beta\left(K[V]^G\right)$ leads to an algorithm for computing generators. If G is finite of order not a multiple of the characteristic $\mathrm{char}(K)$ of K, then the famous Noether bound (which in this generality was not proved until 2000) tells us that

$$\beta\left(K[V]^G\right) \leq |G|.$$

This bound becomes (catastrophically) wrong in the *modular case*, i.e., when $\mathrm{char}(K)$ divides $|G|$.

A fairly recent trend in invariant theory has been the study of *separating invariants*. By definition, a subset $S \subseteq K[V]^G$ is called **separating** if for all pairs of points $x, y \in V$ the existence of $f \in K[V]^G$ with $f(x) \neq f(y)$ implies the existence of $f \in S$ with $f(x) \neq f(y)$. In other words, S has the same capabilities of separating orbits as $K[V]^G$. Every generating subset of $K[V]^G$ is separating, so the concept of a separating subset is a *weakening* of the concept of a generating subset. But separating subsets have better properties than separating ones. For example,

- there always exists a finite separating subset (even if $K[V]^G$ is not finitely generated), and
- for G finite, there exists a separating set of homogeneous invariants of degree $\leq |G|$, even in the modular case. So Noether's bound always holds for separating invariants.

Separating invariants are also useful for algorithmic purposes: The author has found an algorithm for computing separating invariants in the case that G is reductive. Since we also have algorithms for extending a separating subset into a generating subset, we obtain the above-mentioned algorithm for computing $K[X]^G$ for G reductive.

The following problems are still open:

- Find an algorithm for computing a separating subset for G non-reductive.
- Find a test for finite generation of $K[V]^G$.
- Compute $K[V]^G$ as the ring of regular functions of a quasi-affine variety U:
  $$K[V]^G = K[U].$$
  (By a result of Nagata, such a U exists even if $K[V]^G$ is not finitely generated.)
- Implement the known algorithms (i.e., beyond Derksen's algorithm and the finite groups case).