Abstract

Enumeration of Codes of Fixed Cardinality up to Isomorphism

Petr Lisoněk

Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada

We say that sequence (a_n) is *quasi-polynomial* in n if there are polynomials $P_0, ..., P_{s-1}$ such that $a_n = P_i(n)$ where $i \equiv n \pmod{s}$. A q-ary non-linear code with block size n and r codewords is a subset of A^n of cardinality r, where A is an alphabet of q symbols. Two codes are isomorphic if one can be obtained from the other by permuting the n coordinates and then in each coordinate independently permuting the alphabet symbols by some permutation from S_A. This isomorphism relation is induced by the group action of the wreath product $S_A \wr S_n$ on A^n.

Let $c_{q,r,n}$ denote the number of isomorphism classes of q-ary codes with block size n and r codewords. We prove that, when the values of q and r are fixed, the sequence $(c_{q,r,n})$ is quasi-polynomial in n. The main idea of the proof is to express, for any fixed q and r, the value $c_{q,r,n}$ as the lattice point count in the union of a finite set of polytopes parameterized by n.

We also discuss strategies for computing closed forms for the generating functions $f_{q,r}(z) = \sum_{n \geq 0} c_{q,r,n} z^n$. Besides counting lattice points in polytopes we also use G-partitions, which are orbits of number compositions with k parts under a subgroup $G \leq S_k$.