Arcs in Galois geometries and their applications

Angelo Sonnino

A k-arc in a finite projective space $\mathrm{PG}(r, q)$, with $q = p^h$ and p a prime, is a set $\mathcal{K}$ consisting of k points no $r + 1$ of which are contained in a hyperplane. A k-arc is said to be complete in $\mathrm{PG}(r, q)$ if it is not contained in a $(k + 1)$-arc.

A strong motivation for the study of arcs comes from coding theory. In fact, it is well known that k-arcs and Maximum Distance Separable codes are equivalent objects, and many known "good" covering codes and saturating sets arise from complete arcs. Furthermore, k-arcs in finite projective spaces are used in cryptography in order to produce some multilevel secret sharing schemes.

For $q > 4$ and $r = 3$ the upper bound for the size of a k-arc is $q + 1$. The group of projectivities fixing a $(q + 1)$-arc $\mathcal{K}$ in $\mathrm{PG}(3, q)$ is isomorphic to the subgroup $\mathrm{PGL}(2, q)$ of $\mathrm{PGL}(4, q)$, and acts on $\mathcal{K}$ as $\mathrm{PGL}(2, q)$ in its natural 3-transitive permutation group representation. Hence, every $(q+1)$-arc in $\mathrm{PG}(3, q)$ is transitive. Here the term of a "transitive" arc of $\mathrm{PG}(3, q)$ is used to denote a k-arc $\mathcal{K}$ such that the projectivity group fixing $\mathcal{K}$ acts transitively on its points. This poses the problem of finding a suitable finite group acting faithfully as a projectivity group in $\mathrm{PG}(3, q)$. Actually, such groups can exist under certain conditions on q.

The projective space $\mathrm{PG}(3, q)$ has a projectivity group isomorphic to the classical group $\mathrm{PSL}(2, 7)$ if and only if $q \equiv 1 \pmod 7$. The question arises whether or not a $\mathrm{PSL}(2, 7)$-invariant k-arc exists in $\mathrm{PG}(3, q)$ for a fixed k and infinitely many values of q. In this talk we address the case of transitive k-arcs fixed by a projectivity group isomorphic to $\mathrm{PSL}(2, 7)$ in $\mathrm{PG}(3, q^2)$, with $k = 42$, $q \geq 29$ and $q \equiv 1 \pmod 7$. Interestingly, for $q = 29$ these 42-arcs turn out to be complete in $\mathrm{PG}(3, 29^2)$.

Motivated by applications to multilevel secret sharing schemes, we also investigate k-arcs contained in a $(q + 1)$ arc Γ of $\mathrm{PG}(3, 2^h)$ which have only a small number of focuses on a real axis of Γ.