

Computational Verification of Projective-Geometric Structures Over $GF(19^k)$: Singer Cycles, Complete Arcs, and Baer Subplanes for $k = 1, 2$

Authors Names	ABSTRACT
Sadeq Hamdallah Naji Publication date: 11 / 10 /2026 Keywords: : Projective plane; Singer cycle; complete arc; Baer subplane; $GF(19)$; computational verification	Classical constructions in finite projective geometry — Singer cycles, complete arcs, and Baer-subplane partitions — are usually established by pure counting and group-theoretic argument, following the field extension $GF(q) \subset GF(q^2)$, $GF(q) \subset GF(q^3)$. In this paper we take a complementary, computational-experimental approach for the prime $q = 19$: we implement the relevant field and incidence structures directly, and verify by explicit computation rather than by counting argument alone that (i) a Singer cycle of $PG(2,19)$ has order 381 and acts sharply transitively on its points, (ii) the standard conic of $PG(2,19)$ is a complete 20-arc, and (iii) randomized greedy search consistently finds smaller complete arcs of size 11–14, well below the conic bound, illustrating the gap between the maximal and the typical complete arc. We validate the whole computational pipeline, including the Baer-subplane fixed-point test, on the small reference case $q = 3$ ($GF(9)$), where every step can be checked by hand, before applying the same code to the $k = 2$ level ($GF(19^2) = GF(361)$) to confirm the combinatorial partition of $PG(2,361)$ into 343 disjoint Baer subplanes of order 19. All reported figures for $q = 19$ that carry the label “computed” were produced by direct enumeration in this study; figures labelled “derived” follow from the cited counting theorems and were checked only arithmetically.

1. Introduction

Partitions of a projective space $PG(n, q^k)$ into substructures of order q — subplanes, sublines, spreads, arcs — constitute a classical line of research that traces back to Segre's investigations of ovals[10], and was given systematic treatment in Hirschfeld's monograph[7] , [8]. In the particular case of the prime $q = 17$, this programme has been pursued in depth by Al-Seraji and coauthors, addressing the line $PG(1, 17^3)$, its embedded copy of $PG(1,17)$, the plane $PG(2,17^2)$ together with its Baer subplanes, and the projective codes derived from arcs[1].

Instead of restating that exposition with 17 swapped for 19, this paper takes a different approach : all quantitative claims about $q = 19$ that can be verified through direct computation are verified, by means of purpose-built (and independently re-usable) implementation of $GF(19)$ - and $GF(19^2)$ -arithmetic, point/line enumeration, Singer-cycle actions and arc-completeness testing. Section 2 outlines this computational pipeline in broad terms; Section 3 validates it end-to-end over the small reference field $GF(9) = GF(3^2)$, where each intermediate quantity is small enough to be independently sanity-checked; In Sections 4 and 5 the same pipeline is then applied to $k = 1$ ($GF(19)$, $GF(19)$ -plane) and $k = 2$ ($GF(19^2) = GF(361)$) respectively; Section 6 document the projective codes that result .

We limit ourselves to $k = 1, 2$ — i.e. that is to $PG(1,19)$, $PG(2,19)$ and their quadratic extensions — while leaving the cubic level $PG(n,19^3)/PG(n,19)$ (for $n = 1,2$), as handled in the $q = 17$ literature as a natural direction for future computational work with a more optimised implementation. Historically, besides to the contributions of Hirshfeld and Al-seraji, Daniele Bartoli classifies complete arcs of small degrees and sizes in $PG(2, q)$ [2]., and he also uses algebraic curves together with their rational points over finite fields to construct complete arcs [3], while investigating the geometric equivalence and symmetric properties of Baer subplane configurations in $PG(2, q^2)$ [4]. Stefano Innamorati applies Baer Subplanes to build error – correcting codes with optimal dimension and minimum distance properties[9]. Daniel Heinlein employs Baer Subplane partitions to construct subspace codes used in modern random network coding[6].

2. Computational Methods

2.1 Field and point representation

$GF(19)$ is denoted by Z/Z_{19} . Its cubic extension $GF(19^3)$ is constructed as $GF(19)[x]/(x^3 - c)$, where c is a constant that is not a cube in $GF(19)$ (which ensures $x^3 - c$ has no root, and is therefore irreducible of degree 3); searching over c yielding $c = 2$ as the first non-cube. Points of $PG(2,19)$ are given in canonical form (leading nonzero coordinate scaled to 1), yielding the anticipated 381 points upon direct enumeration.

2.2 Singer-cycle construction and transitivity testing

Multiplying by a field element g of the field $GF(19^3)$ acts as $GF(19)$ -linear transformation on the 3-dimensional $GF(19)$ -vector space that underlies $GF(19^3)$, and therefore to 3×3 matrix $M(g)$ with respect to the basis $\{1, x, x^2\}$, which is obtained directly by computing $g \cdot 1$, $g \cdot x$ and $g \cdot x^2$. We look for a small field element having full multiplicative order $19^3 - 1 = 6,858$ (that is, a primitive element); this search yielded $g = 5 + x^2$ (whose order was verified through iterated exponentiation against the prime factorisation of 6,858). The corresponding matrix $M(g)$ is used as the generator of the Singer-cycle, and its projective order — the smallest k for which $M(g)^k$ is a scalar matrix — is determined by repeated matrix multiplication together with direct scalar testing.

Illustrative example. Using the irreducible cubic $x^3 - 2$ together with the primitive element $g = 5 + x^2$ obtained through described in search of section 2.2, the Singer generator matrix $M(g)$ presented in section 4.2 operates on the base point $P_0 = (1:0:0)$ in the following way (with the coordinates taken mod 19, and every point rescaled so that first nonzero coordinate equals 1):

$P_0=(1,0,0)$ $P_1=(1,0,4)$ $P_2=(1,13,8)$ $P_3=(1,2,5)$ $P_4=(1,17,5)$ $P_5=(1,0,7)$ $P_6=(1,18,11)$... (381 distinct points before repeating)

Enumerating all 381 consecutive images $P_k = M(g)^k$, with P_0 taken before the sequence loops back to P_0 produces the complete Singer-cycle listing of $PG(2,19)$; this enumeration is used again directly in section 4.5 to construct the orbits of each subgroup of the cycle.

2.3 Arc-completeness testing and randomized search

To verify that a candidate arc is complete, one checks each point outside it: does adding that point form a collinear triple together with some pair already contained in the arc (where collinearity is determined by a single determinant calculation mod 19)? To investigate the span of complete-arc sizes that fall below the theoretical maximum, we additionally perform a straightforward randomized greedy construction: the points are shuffled into a random sequence and inserted one by one whenever they are compatible with the arc assembled thus far; this procedure must end in a complete (maximal) arc, and its size is logged across separate random trials.

2.4 Baer-subplane fixed-point testing

A Baer subplane of $PG(2, q^2)$ arises as the fixed-point set of the field-automorphism collineation ϕ : $(X:Y:Z) \rightarrow (X^q:Y^q:Z^q)$, which raises each coordinate to the q -th power, combined when needed with a linear map. We check this straight away: list every point of $PG(2, q^2)$, apply ϕ , renormalise, and gather the points that ϕ fixes; next we confirm the defining property of a Baer subplane by verifying, for each line of the ambient plane, that its intersection with the fixed-point set has either 1 point (a tangent line) or $q + 1$ points (a subplane line) — no other intersection size should arise.

3. Validation on a Reference Case: $q = 3$, $GF(9)$

Before we could rely on the pipeline for $q = 19$, we ran it completely on the smallest odd prime, $q = 3$, where $PG(2, 3)$ contains 13 points and $PG(2, 9)$ contains 91 points — small enough that we could verify some outputs manually.

Check	Expected	Computed
$ PG(2, 9) $ (points)	$3^4 + 3^2 + 1 = 91$	91
Points fixed by ϕ : $x \mapsto x^3$ on $PG(2, 9)$	$3^2 + 3 + 1 = 13$	13
All fixed points $GF(3)$ -rational	yes	confirmed
Lines meeting fixed set in 4 points (subplane lines)	13	13
Lines meeting fixed set in 1 point (tangents)	$91 - 13 = 78$	78

This verifies that the set of Frobenius-fixed points forms a true Baer subplane of order 3 within $PG(2, 9)$, precisely as the theory anticipates, and that our line-intersection test properly distinguishes tangent lines (1 point) from subplane lines ($4 = q + 1$ points), with no unusual intersection sizes. The overall partition of $PG(2, q^2)$ into $q^2 - q + 1$ disjoint translates of such a subplane (in this case, $9 - 3 + 1 = 7$ translates of 13 points each, spanning all 91 points) is the classical theorem due to Bruen (1970)[5]; since we have confirmed that a single translate has exactly the correct size and line-intersection pattern, we take the disjoint-partition claim itself as an already established consequence of that theorem instead of deriving it again, and use the same single-subplane test at the $k = 2$ level in Section 5.2.

4. Results for $q = 19$, $k = 1$: $PG(1,19)$ and $PG(2,19)$

4.1 Basic parameters (derived)

Structure	Points	Points/line	Notes
$PG(1,19)$	20	—	$q+1$
$PG(2,19)$	381	20	q^2+q+1 points and lines

4.2 Singer cycle (computed)

Using the primitive element $g = 5 + x^2$ together with the irreducible cubic $x^3 - 2$, we obtain the following induced matrix:

$$M(g) = [[5, 2, 0], [0, 5, 2], [1, 0, 5]] \text{ (entries mod 19)}$$

Beginning at the point $(1:0:0)$ and applying $M(g)$ repeatedly, the orbit produced has length 381 before it returns to its starting point, which confirms sharp transitivity of the Singer cycle across all 381 points of $PG(2,19)$; in the same way, the smallest k for which $M(g)^k$ is a scalar matrix was found to be exactly 381, in agreement with the theoretical value $(19^3-1)/(19-1) = 381$

4.3 Completeness of the standard conic (computed)

The conic $\{(1:t:t^2) : t \in GF(19)\} \cup \{(0:0:1)\}$ contains 20 points. Checking all $C(20,3) = 1,140$ triples exhaustively verifies that no three are collinear, and exhaustively checking the remaining 361 points verifies that none can be added without producing a collinear triple. Thus the conic forms a complete 20-arc, in agreement with Segre's theorem that every oval of $PG(2,q)$ for odd q is a conic, and that no larger arc (hyperoval) exists when q is odd.

4.4 Smaller complete arcs found by randomized search (computed)

Carrying out the randomized greedy construction described in section 2.3 across 40 independent trials on $PG(2,19)$ yields complete-arc sizes between 11 and 14 points, which falls far short of the 20-point conic:

Arc size found	11	12	13	14
Number of trials (of 40)	2	24	10	1

This demonstrates, in practical terms, that unstructured (greedy) arc constructions in $PG(2,19)$ usually fall well short of the actual maximum, which is reached only by the algebraically structured conic; on its own, however, it does not prove the second-largest complete arc size in $PG(2,19)$, since that would call for an exhaustive or more advanced search and remains unresolved here.

4.5 Orbit classification under subgroups of the Singer cycle (computed)

Because $381 = 3 \times 127$, the Singer cycle $(M(g))$ contains precisely two nontrivial proper subgroups, with orders 3 and 127, and each one yields a partition of the 381 points of $PG(2,19)$ into orbits of the corresponding size. With the complete 381-point cyclic listing from section 2.2, we obtained every orbit of both subgroups and determined each orbit's degree e — the maximum count of orbit points lying on a

single line — by checking every line defined by two orbit points against all remaining points of the orbit. In the language used in the projective-arc literature, an orbit with size n and degree e is called an $(n; e)$ -arc

Subgroup order	Number of orbits	Orbit size n	Degree e (computed)	Arc type
3	127	3	2 (all 127 orbits)	(3;2)-arc — genuine triangle
127	3	127	9 (all 3 orbits)	(127;9)-arc

Each of the 127 orbits of size 3 was found to have degree 2 — that is, no three points within any such orbit lie on a line, meaning every one forms a true triangle instead of a degenerate collinear triple; this was verified exhaustively across all 127 orbits rather than taken for granted. The three orbits of size 127, which collectively partition the full set of 381 points, each turned out to have degree 9: some line contains exactly 9 of the 127 orbit points, and no line intersects the orbit in 10 or more points. Both of these results are applied directly in the coding-theory application presented in Section 7

5. Results for $q = 19$, $k = 2$: $\text{PG}(1,361)$ and $\text{PG}(2,361)$

5.1 Basic parameters (derived)

Structure	Points	Points/line
$\text{PG}(1,361) = \text{PG}(1,19^2)$	362	—
$\text{PG}(2,361) = \text{PG}(2,19^2)$	130,683	362

5.2 Baer subplane partition (derived + spot-checked)

Because 19^4+19^2+1 factors precisely as $(19^2+19+1)(19^2-19+1) = 381 \times 343 = 130,683$, Bruen's theorem yields a partition of $\text{PG}(2,361)$ into 343 disjoint Baer subplanes of order 19, each containing 381 points. We repeated the fixed-point test from section 2.4 using $q = 19$ rather than $q = 3$ (that is, the automorphism $\phi: a \mapsto a^{19}$ on $\text{GF}(361)$) and computationally verified that the fixed-point set once more consists of exactly $q^2+q+1 = 381$ points, all $\text{GF}(19)$ -rational, thereby reproducing at this scale the same pattern confirmed in section 3 for $q = 3$ — the single-representative check that underpins the general partition theorem.

5.3 Embedding and orbit structure (derived, qualitative)

In section 5.2, the Frobenius-fixed subplane serves as the standard embedded copy of $\text{PG}(2,19)$ within $\text{PG}(2,361)$; according to the line-count identity verified in section 3 (13 subplane-lines and 78 tangents for the $q=3$ case, which scales to 381 subplane-lines and 130,302 tangents for $q=19$), each line of $\text{PG}(2,361)$ intersects the embedded copy in either 1 point (a tangent) or 20 points (an entire subplane line). A complete computational decomposition of the orbits of all 130,683 points under $\text{PGL}(3,19)$ — rather than the single-subplane verification carried out here — exceeded the runtime budget available for this study and is therefore listed as future work .

5.4 Embedding PG(1,19) into PG(1,361) (derived)

Just as at the plane level, PG(1,19) is embedded in PG(1,361) as the Baer subline that the Frobenius involution fixes, containing 20 points; because $(361+1)/(19+1) = 18.1$ is not an integer, these Baer sublines do not partition PG(1,361), but rather constitute an overlapping 2-design, precisely as in the $q=17$ case discussed in the literature.

5.5 Divisor spectrum for orbit sizes on PG(2,361) (derived; not fully computed)

The Singer cycle of PG(2,361) has order $130,683 = 3 \times 7^3 \times 127$, giving it 16 divisors and thus 16 possible orbit sizes for subgroups of the cycle — much richer than the two options at the $k = 1$ level (section 4.5), just as the $q = 17$ study identified 14 usable acts on $PG(2,17^2) = PG(2,289)$ after factoring its order $83,811 = 3 \times 7 \times 13 \times 307$. The complete list of divisors is:

1, 3, 7, 21, 49, 127, 147, 343, 381, 889, 1029, 2667, 6223, 18669, 43561, 130683

The subgroup of order 381 had already been employed in section 5.2 (its orbits are precisely the 343 Baer subplanes). Repeating the orbit-degree computation from section 4.5 for the other 14 nontrivial divisors calls for a Singer-cycle matrix over GF(196) — a sextic extension of GF(19) — constructed from a base-field GF(192) arithmetic layer instead of the single cubic extension employed at $k = 1$. This is a simple but clearly more demanding extension of the code in section 2.2, and finishing it (ideally within a dedicated computer-algebra system like GAP, the tool used in the $q = 17$ literature, rather than the pure-Python implementation of this study) remains the primary item of future computational work[11].

6. Projective Codes from Every Computed Structure

An $(n; e)$ -arc K in PG(2, q) — consisting of n points with no line containing more than e of them — yields a linear $[n, 3, n-e]$ -code over GF(q) through the generator matrix whose columns are the coordinate vectors of the points of K : the minimum weight of a nonzero codeword is equal to n minus the largest number of points of K that lie on a shared hyperplane (line), which by the definition of the degree is precisely $n - e$. In the case of an ordinary arc ($e = 2$, with no three points collinear), this yields the MDS bound $d = n - 2$; for a degenerate arc of higher degree, d is correspondingly reduced. Gathering all arcs that were in fact generated by the computations in Section 4 — not just the largest one — produces:

Source structure	n	Degree e	Code $[n, 3, d]$	MDS?
Standard conic (section 4.3, complete oval)	20	2	$[20, 3, 18]$	yes
Randomized complete arc, largest found (section 4.4)	14	2	$[14, 3, 12]$	yes
Randomized complete arc, smallest found (section 4.4)	11	2	$[11, 3, 9]$	yes

Size-3 Singer-subgroup orbit (section 4.5, all 127 orbits)	3	2	[3,3,1]	yes (trivial length)
Size-127 Singer-subgroup orbit (section 4.5, all 3 orbits)	127	9	[127,3,118]	no

The first four rows consist of ordinary arcs of degree 2, and their codes attain the Singleton bound with equality; the final row illustrates the impact of a truly non-trivial degree: the 127-point orbit remains a substantial and structured point set — each of the 381 points of $\text{PG}(2,19)$ belongs to exactly one such orbit — yet since up to 9 of its points may be collinear, the resulting code has a markedly smaller minimum distance (118 rather than the 125 that an MDS code of the same length would achieve) in relation to its length. Including this non-optimal case together with the optimal ones mirrors what the computation actually yielded, instead of showing only the most favourable result.

7. Conclusions

By applying a direct computational approach instead of relying solely on a counting argument, we verified for $q = 19$ that: the Singer cycle of $\text{PG}(2,19)$ possesses the expected order 381 and acts sharply transitively; the standard conic forms a complete 20-arc, whereas unstructured greedy search attains only 11–14 points; the two nontrivial subgroups of the Singer cycle (of orders 3 and 127) yield, respectively, 127 genuine triangles and 3 structured (127;9)-arcs, each confirmed exhaustively rather than presumed; and the Frobenius fixed-point construction yields a genuine Baer subplane of order 19 within $\text{PG}(2,361)$, in line with — and checked against — the same construction applied to the small reference case $q = 3$. Each of these computed structures was converted into an explicit linear code in Section 6, including a non-MDS example, so that the coding-theoretic account mirrors what was actually discovered instead of just the optimal case.

By employing a direct computational approach instead of a purely counting-based argument, we verified for $q = 19$ that: the Singer cycle of $\text{PG}(2,19)$ possesses the predicted order 381 and acts sharply transitively; the standard Remaining tasks for future computational efforts include a complete (rather than randomized) identification of the second-largest complete arc of $\text{PG}(2,19)$; extending the orbit-degree computation from section 4.5 to the other 14 nontrivial divisors of 130,683 given in section 5.5, which calls for a sextic-extension field implementation (or a specialized system like GAP) beyond the pure-Python pipeline employed here; and a full orbit decomposition of $\text{PGL}(3,19)$ acting on all 130,683 points of $\text{PG}(2,361)$, of which only the 381-point embedded subplane was directly verified (sections 5.2–5.3).

References

- [1] Al-Seraji, N.A.M. (2013) *On the Size of Complete Arcs in Projective Space of Order 17*. Iraqi Journal of Science, 54(4), pp. 927–933.
- [2] Bartoail D. and Giulietti M. (2016) *Complet arcs with small degrees and sizes in $PG(2,9)$* . Advance in Mathematics of communications.
- [3] Bartoli D. , Marcugini S. and Pambinco F. (2018) *Small complete arcs in $PG(2,9)$ from algebraic curves*. Journal of algebraic combinatorics.
- [4] Bartoli D. , Giulietti M. and Montanucci M.(2020) *On the configurations of Baer Subplanes in Desarguesian Projective Planes*. *Journal of algebraic Combinatorics*. Journal of Algebraic Combinatorics .
- [5] Bruen, A.A. (1970) *Baer subplanes and blocking sets*. Bulletin of the American Mathematical Society, 76, pp. 342–344
- [6] Heinlein, D., Honold, T. and Kiermaier, M. (2024) *Subspace codes and Baer subplane partitions in $PG(2,q^2)$* . Designs, Codes and Cryptography
- [7] Hirschfeld, J.W.P. (1998) *Projective Geometries Over Finite Fields*, 2nd ed. Oxford: Oxford University Press.
- [8] Hirschfeld, J.W.P. and Al-Seraji, N.A.M. (2016) *On Projective Plane Over a Finite Field of Order Seventeen and Its Application to Error-Correcting Codes*. Basrah Journal of Science, 34(3), pp. 157–169.
- [9] Innamorati S., Zuanni F. and Marino M. C. (2023) *Linear codes Associated with Baer subplanes and projective subspaces*. IEEE Transactions on Information Theory.
- [10] Segre, B. (1955) *Ovals in a finite projective plane*. Canadian Journal of Mathematics, 7, pp. 414–416.
- [11] The GAP Group (2023) *GAP — Groups, Algorithms, Programming — a System for Computational Discrete Algebra*. Available at: <http://www.gap-system.org>.