Classifying the complete arcs in small projective planes

K. Coolsaet, H. Sticker

Combinatorial Algorithms and Algorithmic Graph Theory
Ghent University

August 2012

Overview

- Arcs in finite Desargeusian projective planes
- Canonical augmentation
- Large arcs only (unfinished business)

Arcs in finite Desarguesian projective planes

Definitions

A projective plane **P** consists of points and lines, such that

- Two points are joined by exactly 1 line
- Two lines intersect in exactly 1 point

Example: the (Euclidian) plane with added line at infinity.

Definitions

A projective plane **P** consists of points and lines, such that

- Two points are joined by exactly 1 line
- Two lines intersect in exactly 1 point

Example: the (Euclidian) plane with added line at infinity.

An arc $\mathcal{K}$ in **P** is a set of points such that

- No three points of $\mathcal{K}$ lie on the same line

Example: conic (ellipse, hyperbola, parabola)

An arc $\mathcal{K}$ is complete if there exists no arc strictly containing $\mathcal{K}$.

Definitions

A projective plane **P** consists of points and lines, such that

- Two points are joined by exactly 1 line
- Two lines intersect in exactly 1 point

Example: the (Euclidian) plane with added line at infinity.

An arc $\mathcal{K}$ in **P** is a set of points such that

- No three points of $\mathcal{K}$ lie on the same line

Example: conic (ellipse, hyperbola, parabola)

An arc $\mathcal{K}$ is complete if there exists no arc strictly containing $\mathcal{K}$.

Goal: Find 'all' complete arcs in small projective planes.

Finite projective planes

If plane **P** is finite, then there are

- $q^2 + q + 1$ points and $q^2 + q + 1$ lines
- $q + 1$ points on each line, $q + 1$ lines through each point

q is the order of the projective plane.

caagt

Finite projective planes

If plane **P** is finite, then there are

- $q^2 + q + 1$ points and $q^2 + q + 1$ lines
- $q + 1$ points on each line, $q + 1$ lines through each point

q is the order of the projective plane.

All known examples have $q = p^h$ with p a prime number.
(Standard example: Desarguesian projective plane.)

Finite projective planes

If plane **P** is finite, then there are

- $q^2 + q + 1$ points and $q^2 + q + 1$ lines
- $q + 1$ points on each line, $q + 1$ lines through each point

q is the order of the projective plane.

All known examples have $q = p^h$ with p a prime number.
(Standard example: Desarguesian projective plane.)

Maximum size of an arc $\mathcal{K}$

- $q + 2$ when q is *even*,
- $q + 1$ when q is *odd*.

caagt

Desarguesian projective plane

Let **F** be a field.

- Points: $(x : y : z)$, $x, y, z \in \mathbf{F}$ (not all zero)
- Lines: $(A : B : C)^T$, $A, B, C \in \mathbf{F}$ (not all zero)

Desarguesian projective plane

Let **F** be a field.

- Points: $(x : y : z)$, $x, y, z \in \mathbf{F}$ (not all zero)
- Lines: $(A : B : C)^T$, $A, B, C \in \mathbf{F}$ (not all zero)
- Point on line iff

$$Ax + By + Cz = 0.$$

Desarguesian projective plane

Let **F** be a field.

- Points: $(x : y : z)$, $x, y, z \in \mathbf{F}$ (not all zero)
- Lines: $(A : B : C)^T$, $A, B, C \in \mathbf{F}$ (not all zero)
- Point on line iff

$$Ax + By + Cz = 0.$$

- Conic: points satisfying $y^2 = xz$, i.e.,

$$(1 : t : t^2) \qquad \text{with } t \in \mathbf{F},$$
$$(0 : 0 : 1) \qquad (t = \infty.)$$

Desarguesian projective plane

Let **F** be a field.

- Points: $(x : y : z)$, $x, y, z \in \mathbf{F}$ (not all zero)
- Lines: $(A : B : C)^T$, $A, B, C \in \mathbf{F}$ (not all zero)
- Point on line iff

$$Ax + By + Cz = 0.$$

- Conic: points satisfying $y^2 = xz$, i.e.,

$$(1 : t : t^2) \qquad \text{with } t \in \mathbf{F},$$
$$(0 : 0 : 1) \qquad (t = \infty.)$$

Today: field is finite with q elements
(= order of Desarguesian plane)

caagt

Finite fields

Field is uniquely determined by its number of elements q.

Finite fields

Field is uniquely determined by its number of elements q.

When q is prime: arithmetic modulo q.

Example $q = 13$:

$$\begin{aligned} 3 + 7 &= -3 \\ 3 - 7 &= -4 \\ 3 \cdot 7 &= -5 \\ 3 / 7 &= \end{aligned}$$

Finite fields

Field is uniquely determined by its number of elements q.

When q is prime: arithmetic modulo q.

Example $q = 13$:

$$\begin{aligned} 3 + 7 &= -3 \\ 3 - 7 &= -4 \\ 3 \cdot 7 &= -5 \\ 3 / 7 &= 6 \end{aligned}$$

Finite fields

Field is uniquely determined by its number of elements q.

When q is prime: arithmetic modulo q.

Example $q = 13$:

$$\begin{aligned} 3 + 7 &= -3 \\ 3 - 7 &= -4 \\ 3 \cdot 7 &= -5 \\ 3 / 7 &= 6 \end{aligned}$$

When q is not prime: *algebraic extension* of prime field.

Example $q = 9 = 3^2$

- Elements are $0, \pm 1, \pm i, \pm 1 \pm i$
- Arithmetic modulo 3, $i^2 = -1$

caagt

Symmetries

Let $M \in \mathbf{F}^{3\times 3}$, M nonsingular. The map

$$\begin{aligned} (x:y:z) &\mapsto (x:y:z)M, \\ (A:B:C)^T &\mapsto M^{-1}(A:B:C)^T \end{aligned}$$

is a projectivity. There are $\approx q^8$ projectivities.

(Examples: rotations, mirror symmetries, translations, ...)

A projectivity is an *automorphism* of **P** (incidence is preserved).

caagt

Symmetries

Let $M \in \mathbf{F}^{3\times 3}$, M nonsingular. The map

$$\begin{aligned}(x:y:z) &\mapsto (x:y:z)M,\\ (A:B:C)^T &\mapsto M^{-1}(A:B:C)^T\end{aligned}$$

is a projectivity. There are $\approx q^8$ projectivities.

(Examples: rotations, mirror symmetries, translations, ...)

A projectivity is an *automorphism* of **P** (incidence is preserved).

Goal: Find all complete arcs in Desarguesian projective planes up to projective equivalence.

caagt

Generation up to equivalence

Earlier results

- For $q \leq 9$. By hand (and mathematical theory).
- For $11 \leq q \leq 19$. By computer using *ad hoc* methods.

Generation up to equivalence

Earlier results

- For $q \leq 9$. By hand (and mathematical theory).
- For $11 \leq q \leq 19$. By computer using *ad hoc* methods.

Our algorithm: **canonical augmentation** [McKay 1986]

- For $q \leq 29$.

Generation up to equivalence

Earlier results

- For $q \leq 9$. By hand (and mathematical theory).
- For $11 \leq q \leq 19$. By computer using *ad hoc* methods.

Our algorithm: **canonical augmentation** [McKay 1986]

- For $q \leq 29$.

Alternative: **orderly generation** [Read, Faradzev 1978]

caagt

Generation up to equivalence

Earlier results

- For $q \leq 9$. By hand (and mathematical theory).
- For $11 \leq q \leq 19$. By computer using *ad hoc* methods.

Our algorithm: **canonical augmentation** [McKay 1986]

- For $q \leq 29$.

Alternative: **orderly generation** [Read, Faradzev 1978]

What next:

- For $q > 29$ there are too many results.

  (For $q = 29$ there are $> 12 \cdot 10^9$ non-equivalent complete arcs. Computations took ≈ 5 years.)

caagt

Canonical augmentation

Canonical augmentation — simplified

(Works for all subsets of **P** — not just arcs)

Canonical augmentation — simplified

(Works for all subsets of **P** — not just arcs)

Depends on the selection of an appropriate choice function F on **P** which chooses a point in every non-empty set S:

$$F : S \mapsto F(S) \in S.$$

- What is the 'best' choice function depends on the problem
- **Important**: $F(S)$ should be easily computed for most S

Canonical augmentation — simplified

(Works for all subsets of **P** — not just arcs)

Depends on the selection of an appropriate choice function F on **P** which chooses a point in every non-empty set S:

$$F : S \mapsto F(S) \in S.$$

- What is the 'best' choice function depends on the problem
- **Important**: $F(S)$ should be easily computed for most S

From F we derive a canonical dismantling:

$$S \to S' \to S'' \to \cdots \to \emptyset,$$

with $S' = S - \{F(S)\}, S'' = S' - \{F(S')\}, \ldots$

Canonical augmentation — simplified (cntd.)

Canonical augmentation reverses the dismantling process

$$\emptyset \to \cdots \to S'' \to S' \to S$$

- Start with the empty set,
- At each stage *augment* T to $T \cup \{t\}$ with $t \notin T$,
- Only do this when $T \cup \{t\}$ dismantles to T.

This guarantees that every set is generated only once !

Canonical augmentation — simplified (cntd.)

Canonical augmentation reverses the dismantling process

$$\emptyset \to \cdots \to S'' \to S' \to S$$

- Start with the empty set,
- At each stage *augment* T to $T \cup \{t\}$ with $t \notin T$,
- Only do this when $T \cup \{t\}$ dismantles to T.

This guarantees that every set is generated only once !

Generic example for F:

- Number the points of **P** in some way
- F chooses the element of S with largest sequence number

Canonical augmentation — simplified (cntd.)

Canonical augmentation reverses the dismantling process

$$\emptyset \to \cdots \to S'' \to S' \to S$$

- Start with the empty set,
- At each stage *augment* T to $T \cup \{t\}$ with $t \notin T$,
- Only do this when $T \cup \{t\}$ dismantles to T.

This guarantees that every set is generated only once !

Generic example for F:

- Number the points of **P** in some way
- F chooses the element of S with largest sequence number

This is too simple...

Canonical augmentation — up to equivalence

We need all sets only up to equivalence.

F must be group invariant:

$$F(S^\phi) = F(S)^\phi, \quad \text{for all projectivities } \phi$$

- Generic example does no longer work
- Harder to find F that can be efficiently computed

Canonical augmentation — up to equivalence

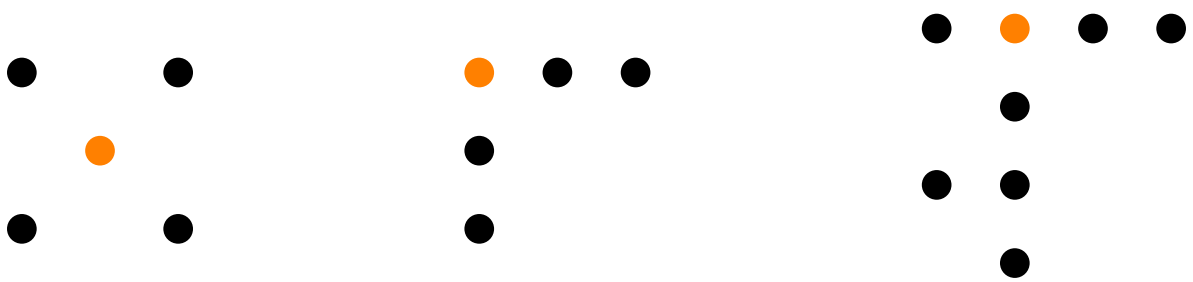
We need all sets only up to equivalence.

F must be group invariant:

$$F(S^\phi) = F(S)^\phi, \quad \text{for all projectivities } \phi$$

- Generic example does no longer work
- Harder to find F that can be efficiently computed

Typical example: F selects the point of largest 'degree'



Orbits — not points

A group invariant choice function does not always exist.

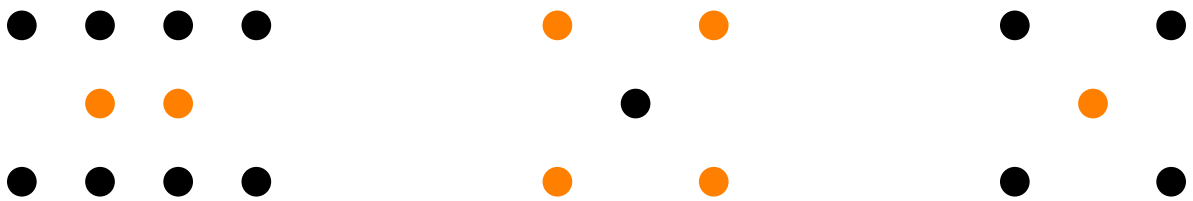
Orbits — not points

A group invariant choice function does not always exist.

Solution: F chooses an orbit of the symmetry group of S

$$F : S \mapsto F(S) \in G_S \backslash\backslash S$$

$F(S)$ is a subset of S

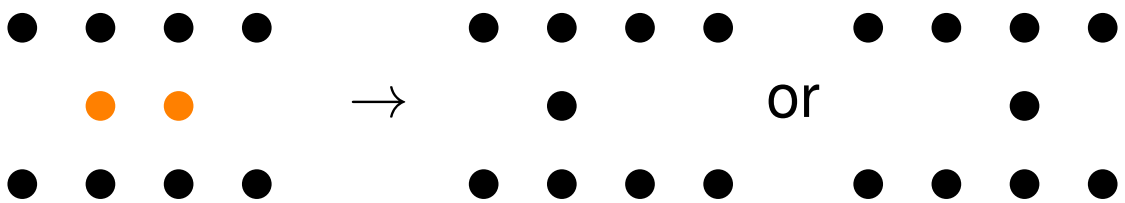


caagt

Canonical dismantling

The ‘parent’ is no longer unique

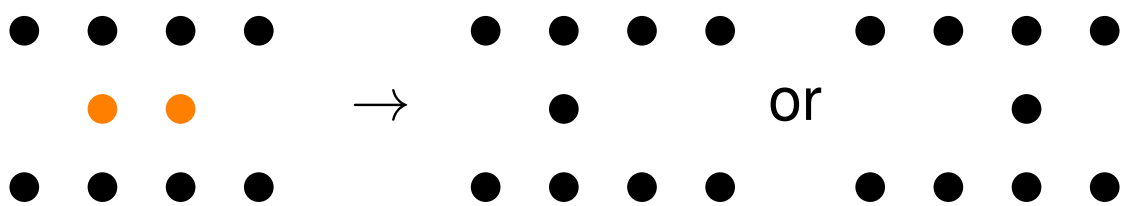
$$S' = S - \{s\}, \quad \text{with } s \in F(S).$$



Canonical dismantling

The ‘parent’ is no longer unique

$$S' = S - \{s\}, \quad \text{with } s \in F(S).$$



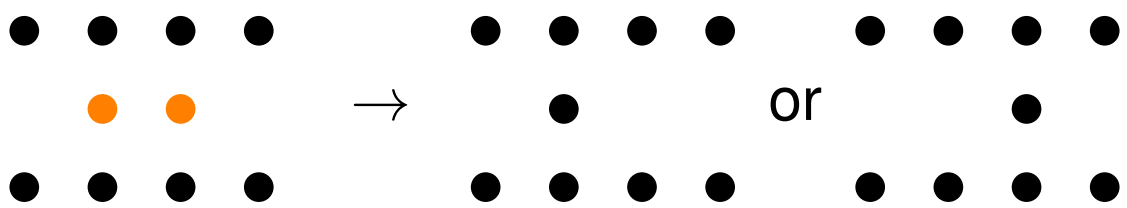
- Parents of S are projectively equivalent
- Parents of projective equivalent sets are projectively equivalent

caagt

Canonical dismantling

The ‘parent’ is no longer unique

$$S' = S - \{s\}, \quad \text{with } s \in F(S).$$



- Parents of S are projectively equivalent
- Parents of projective equivalent sets are projectively equivalent

Provides a canonical dismantling of *orbits* of sets.

caagt

Canonical augmentation

Canonical augmentation reverses the dismantling process:

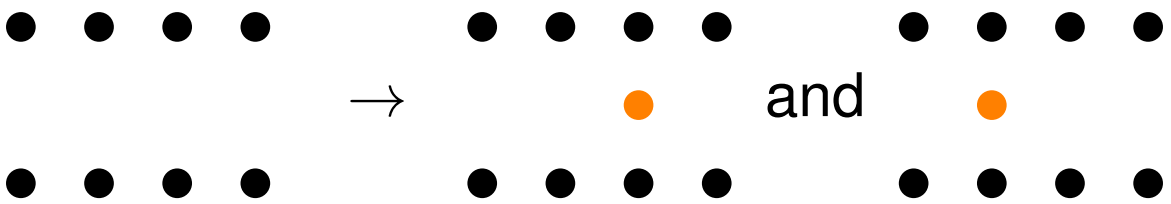
$$T \to T \cup \{t\}, \text{for all } t \notin T \text{ and } t \in F(T \cup \{t\})$$

Canonical augmentation

Canonical augmentation reverses the dismantling process:

$$T \to T \cup \{t\}, \text{for all } t \notin T \text{ and } t \in F(T \cup \{t\})$$

May lead to equivalent results!



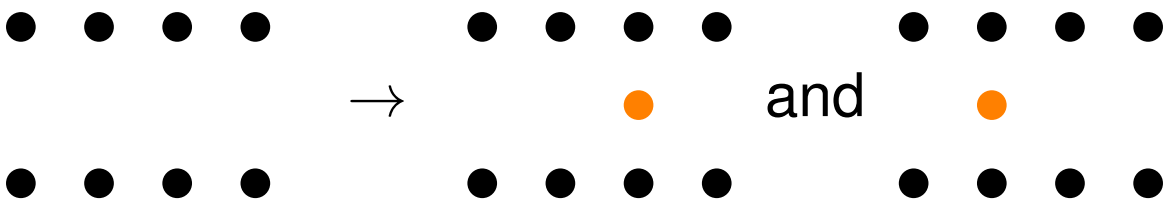
caagt

Canonical augmentation

Canonical augmentation reverses the dismantling process:

$$T \to T \cup \{t\}, \text{for all } t \notin T \text{ and } t \in F(T \cup \{t\})$$

May lead to equivalent results!



Solutions

- Add only one t for each orbit of $G_T \backslash\backslash T$
- Check for equivalence (only) one level deep

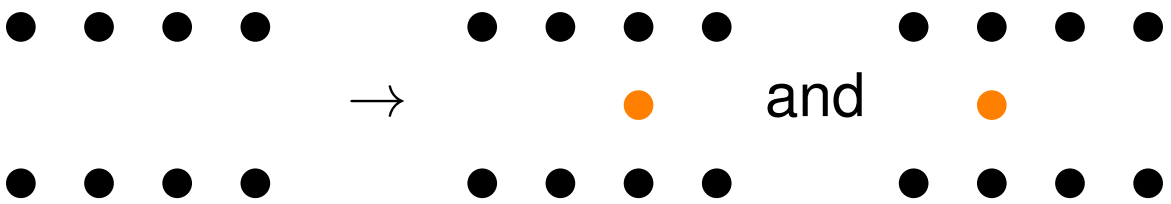
caagt

Canonical augmentation

Canonical augmentation reverses the dismantling process:

$$T \to T \cup \{t\}, \text{for all } t \notin T \text{ and } t \in F(T \cup \{t\})$$

May lead to equivalent results!



Solutions

- Add only one t for each orbit of $G_T \backslash\backslash T$
- Check for equivalence (only) one level deep

Requires computing with groups!

How to avoid computing with groups

Every group invariant partitions the set S in unions of group orbits.

If $F(S)$ is a singleton, then $F(S)$ is an orbit

How to avoid computing with groups

Every group invariant partitions the set S in unions of group orbits.

If $F(S)$ is a singleton, then $F(S)$ is an orbit

Strategy:

- Make F prefer singletons
- If no singletons exist for a specific S, try alternative choice function(s) for that S
- If all else fails: use slow *fallback* choice function.

Choice function for arcs

Choice function for arcs

Lines intersect $\mathcal{K}$ in 0, 1 or 2 points (*external* line, *tangent* of *bisecant*).

Degree $d(p)$ of a point p: number of bisecants through p

Choice function for arcs

Lines intersect $\mathcal{K}$ in 0, 1 or 2 points (*external* line, *tangent* of *bisecant*).

Degree $d(p)$ of a point p: number of bisecants through p

Note: degree cannot be used directly for defining F

Choice function for arcs

Lines intersect $\mathcal{K}$ in 0, 1 or 2 points (*external* line, *tangent* of *bisecant*).

Degree $d(p)$ of a point p: number of bisecants through p

Note: degree cannot be used directly for defining F

Line invariant and point invariant:

$$I(L) = \sum_{p \in L} d(p)^*, \quad I(p) = \sum_{L \ni p} I(L)^*,$$

where $\cdot^*$ is a simple *hash function*.

$I(p)$ **is a suitable invariant for defining** F

Final algorithm

Generate all arcs of size $k+1$ from all arcs of size k, *up to equivalence*:

- For each $\mathcal{K}'$ of size k,
- For all points $s \notin \mathcal{K}'$,
- Check that $\mathcal{K} = \mathcal{K}' \cup \{s\}$ is still an arc,
- Check that $\mathcal{K}$ dismantles to $\mathcal{K}'$,
- If so, add $\mathcal{K}$ to the result ($\pm$)

(Completeness is checked afterwards.)

caagt

Final algorithm

Generate all arcs of size $k+1$ from all arcs of size k, *up to equivalence*:

- For each $\mathcal{K}'$ of size k,
- For all points $s \notin \mathcal{K}'$,
- Check that $\mathcal{K} = \mathcal{K}' \cup \{s\}$ is still an arc,
- Check that $\mathcal{K}$ dismantles to $\mathcal{K}'$,
- If so, add $\mathcal{K}$ to the result ($\pm$)

(Completeness is checked afterwards.)

Do all of this depth first

caagt

Results - Complete arcs of size n

	$q=5$	$q=7$	$q=8$	$q=9$	$q=11$	$q=13$	$q=16$	$q=17$
$n=6$	1	2	1	1				
$n=7$				1	1			
$n=8$		1		1	9	2		
$n=9$					3	29	2	
$n=10$			1	1	1	21	501	560
$n=11$							30	2644
$n=12$					1	1	9	553
$n=13$							1	8
$n=14$						1		1
$n=15$								
$n=16$								
$n=17$								
$n=18$							2	1

Results - Complete arcs of size n

	$q = 19$	$q = 23$	$q = 25$	$q = 27$	$q = 29$
$n = 10$	29	1			
$n = 11$	9541				
$n = 12$	30135	112449	606	7	
$n = 13$	2232	4341514	4072545	221429	708
$n = 14$	70	1828196	29151431	106320273	171139332
$n = 15$		58361	5709597	198631499	7402140892
$n = 16$		564	124577	20335114	4776509549
$n = 17$		5	434	276112	271929757
$n = 18$			41	950	2457679
$n = 19$				5	4190
$n = 20$	1				57
$n = 21$			1		2
$n = 22$				1	
$n = 23$					
$n = 24$		1			1
$n = 25$					
$n = 26$			1		
$n = 27$					
$n = 28$				1	
$n = 29$					
$n = 30$					1
CPU time	$\leq$ 1 hour	1 day	10 days	33 days	5 years

Large arcs only (unfinished business)

Large arcs

(Henceforth q is odd.)

Theorem [Segre 1954] All arcs of size $q + 1$ are conics

Theorem [Segre 1961, Büke 1974, Thas 1987]
All arcs of size q extend to conics

Large arcs

(Henceforth q is odd.)

Theorem [Segre 1954] All arcs of size $q+1$ are conics

Theorem [Segre 1961, Büke 1974, Thas 1987]
All arcs of size q extend to conics

What about size $q-1$?

- For $q = 7, 9, 11, 13$, examples exist that do not lie on a conic.
- **Theorems [1990s]** For $q > 83$ all lie on a conic
- Unknown cases:
  $q = 37, 41, 43, 47, \underline{49}, 53, 59, 61, 67, 71, 73, 79, \underline{81}, 83$

caagt

Large arcs

(Henceforth q is odd.)

Theorem [Segre 1954] All arcs of size $q+1$ are conics

Theorem [Segre 1961, Büke 1974, Thas 1987]
All arcs of size q extend to conics

What about size $q-1$?

- For $q = 7, 9, 11, 13$, examples exist that do not lie on a conic.
- **Theorems [1990s]** For $q > 83$ all lie on a conic
- Unknown cases:
  $q = 37, 41, 43, 47, \underline{49}, 53, 59, 61, 67, 71, 73, 79, \underline{81}, 83$

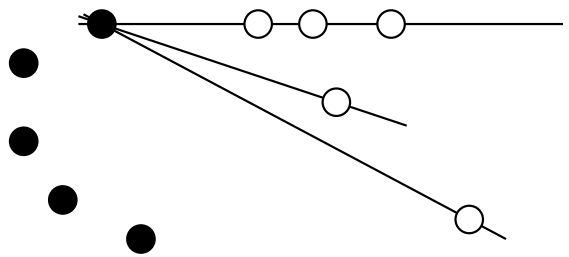
Can we settle this by computer?

caagt

Adapting the earlier algorithm

When extending $\mathcal{K}'$ to $\mathcal{K}$, make sure that

- There are enough free points left ($d(p) = 0$)
- There are enough free tangents left



These adaptations make $q = 31$ just feasible, but not $q \geq 37$.

caagt

The Lemma of Tangents

Let $\mathcal{K}$ denote an arc of size $q+2-t$. (Our case: $t=3$.)
Then every point of $\mathcal{K}$ lies on t tangents.

Theorem (Lemma of tangents) [Segre 1950s]
Assume $\mathcal{K}$ contains

$$e_1 : (1:0:0), \quad e_2 : (0:1:0), \quad e_3 : (0:0:1).$$

Assume the tangents through e_1, e_2, e_3 have equations

$$y = A_i z, \quad z = B_i x, \quad x = C_i y.$$

Then

$$\prod_{i=1}^{t} A_i B_i C_i = -1.$$

The Lemma of Tangents — cntd.

Lemma of Tangents for any three points of $\mathcal{K}$:

- Linear equation in $3t$ variables
- Coefficients depend on coordinates of three chosen points

The Lemma of Tangents — cntd.

Lemma of Tangents for any three points of $\mathcal{K}$:

- Linear equation in $3t$ variables
- Coefficients depend on coordinates of three chosen points

Four triples in fixed quadruple of points

- Yield four equations
- However: not linearly independent
- Still $4t - 3$ degrees of freedom

caagt

The Lemma of Tangents — cntd.

Lemma of Tangents for any three points of $\mathcal{K}$:

- Linear equation in $3t$ variables
- Coefficients depend on coordinates of three chosen points

Four triples in fixed quadruple of points

- Yield four equations
- However: not linearly independent
- Still $4t - 3$ degrees of freedom

Let $t = 3$, $|\mathcal{K}| = n$. Then there remain (at least)

$$\frac{1}{2}n(9 - n) - 1$$

degrees of freedom.

Generation strategy 1

For $n = 10$ we expect -6 degrees of freedom.

Generation strategy 1

For $n = 10$ we expect -6 degrees of freedom.

Algorithm 1:

- For every arc S of size 9 (up to equivalence)
- Run through all free points s
- Solve the equations for the 10 points of $S \cup \{s\}$
- Keep only those s for which there exists a solution
- Hopefully there are at least $q - 10$ of those.

caagt

Generation strategy 1

For $n = 10$ we expect -6 degrees of freedom.

Algorithm 1:

- For every arc S of size 9 (up to equivalence)
- Run through all free points s
- Solve the equations for the 10 points of $S \cup \{s\}$
- Keep only those s for which there exists a solution
- Hopefully there are at least $q - 10$ of those.

Not feasible: Even generating all S already takes too much time for $q = 83$.

caagt

Generation strategy 2

For $n = 9$ we expect -1 degrees of freedom.

Algorithm 2:

- For every arc S of size 8 (up to equivalence)
- Run through all free points s
- Solve the equations for the 9 points of $S \cup \{s\}$
- Partition the s according to the solutions
- Hopefully there is a part of size at least $q - 9$

Generation strategy 2

For $n = 9$ we expect -1 degrees of freedom.

Algorithm 2:

- For every arc S of size 8 (up to equivalence)
- Run through all free points s
- Solve the equations for the 9 points of $S \cup \{s\}$
- Partition the s according to the solutions
- Hopefully there is a part of size at least $q - 9$

Is this feasible for $q = 83$?

- Nr. of arcs of size 8: $\approx 8 \cdot 10^{10}$
- Nr. of free points per arc: $\approx q^2$
- Nr. of systems of equations to solve: $\approx 5 \cdot 10^{14}$

caagt

Generation strategy 2

For $n = 9$ we expect -1 degrees of freedom.

Algorithm 2:

- For every arc S of size 8 (up to equivalence)
- Run through all free points s
- Solve the equations for the 9 points of $S \cup \{s\}$
- Partition the s according to the solutions
- Hopefully there is a part of size at least $q - 9$

Is this feasible for $q = 83$?

- Nr. of arcs of size 8: $\approx 8 \cdot 10^{10}$
- Nr. of free points per arc: $\approx q^2$
- Nr. of systems of equations to solve: $\approx 5 \cdot 10^{14}$

Still not feasible: 250–500 years of computer time

caagt

External points with 6 tangents

Some properties:

- The number of tangents through an external point is always even.
- There is at least one external point with ≥ 4 tangents

External points with 6 tangents

Some properties:

- The number of tangents through an external point is always even.
- There is at least one external point with ≥ 4 tangents

Case 1: Arc has no points with ≥ 6 tangents.

The resulting arc must have additional regularity properties which should make it more easy to generate such arcs.

External points with 6 tangents

Some properties:

- The number of tangents through an external point is always even.
- There is at least one external point with ≥ 4 tangents

Case 1: Arc has no points with ≥ 6 tangents.

The resulting arc must have additional regularity properties which should make it more easy to generate such arcs.

Case 2: Arc contains at least one point with ≥ 6 tangents.

(Leads to next algorithm)

Generation strategy 3

For $n = 7$ we expect 6 degrees of freedom.

Algorithm 3

- For every arc S of size 6 (up to equivalence)
- Run through all free points p
- and through all (remaining) free points s
- Solve the equations for the 7 points of $S \cup \{s\}$
- Substitute the 6 known variables
- Partition the s according to the solutions

caagt

Generation strategy 3

For $n = 7$ we expect 6 degrees of freedom.

Algorithm 3

- For every arc S of size 6 (up to equivalence)
- Run through all free points p
- and through all (remaining) free points s
- Solve the equations for the 7 points of $S \cup \{s\}$
- Substitute the 6 known variables
- Partition the s according to the solutions

Is this feasible for $q = 83$?

- Nr. of arcs of size 6: 56361

caagt

Generation strategy 3

For $n = 7$ we expect 6 degrees of freedom.

Algorithm 3

- For every arc S of size 6 (up to equivalence)
- Run through all free points p
- and through all (remaining) free points s
- Solve the equations for the 7 points of $S \cup \{s\}$
- Substitute the 6 known variables
- Partition the s according to the solutions

Is this feasible for $q = 83$?

- Nr. of arcs of size 6: 56361
- **Feasible**: took 450 days of computer time
- **Results**: as expected (also for smaller q)

caagt

Case 1: Unfinished business

"The resulting arc must have additional regularity properties which should make it more easy to generate such arcs."

Easier said than done.

caagt

Do not yet abandon all hope

Why does Algorithm 2 take so much time ?

Do not yet abandon all hope

Why does Algorithm 2 take so much time ?

- Every arc of size $q-1$ has $\binom{q-1}{8}$ subsets S of size 8. ($\binom{82}{8} = 3.6 \cdot 10^{10}$).
- Every arc will be generated approximately that many times.

Do not yet abandon all hope

Why does Algorithm 2 take so much time ?

- Every arc of size $q-1$ has $\binom{q-1}{8}$ subsets S of size 8. ($\binom{82}{8} = 3.6 \cdot 10^{10}$).
- Every arc will be generated approximately that many times.

Possible solution:

Select a smaller collection of starting arcs of size 8 that still guarantees that all arcs of size $q-1$ will be generated (up to equivalence).

caagt

Veronesian arcs

Every 5 points of an arc lie on a unique conic.

Definition An arc $\mathcal{K}$ is called Veronesian if no 6 points of $\mathcal{K}$ lie on the same conic.

Conjecture If $\mathcal{K}$ is a Veronesian arc, then

$$|\mathcal{K}| \leq \frac{1}{3}(\sqrt{q}+1)^2$$

(For $q = 83$: $|\mathcal{K}| \leq 34$.)

- Mathematical proof? (With higher upper bound?)
- Provable by computer? (Even for $q = 83$?)

Generating non-Veronesian arcs

Corollary If $\mathcal{K}$ is large enough it must contain at least one subset of 6 points that lie on a conic.

Adapt Algorithm 2:

- Use only non-Veronesian arcs of size 8 as starting configurations

(Not yet clear what would be the gain in speed.)

Further thoughts:

- $(q-1)-6$ is still large enough to be non-Veronesian.
- $\mathcal{K}$ contains **two** conical subarcs of size 6.
- Is it feasible to generate all such arcs of 12 points ?

All suggestions are welcome!