LOOKING FOR OVOIDS OF THE HERMITIAN SURFACE: A COMPUTATIONAL APPROACH

LUCA GIUZZI

ABSTRACT. In this note we introduce a computational approach to the construction of ovoids of the Hermitian surface and present some related experimental results.

CONTENTS

INTRODUCTION

Let q be a prime power and denote by $\mathcal{U}$ the non–degenerate Hermitian surface of $\mathrm{PG}(3,q^2)$. A *generator* of $\mathcal{U}$ is a maximal linear subspace contained in $\mathcal{U}$ — in the case of Hermitian surfaces, a generator is a line. A *Hermitian cap* $\mathcal{C}$ is a subset of $\mathcal{U}$ which is met by any generator in at most one point. A Hermitian cap is a *Hermitian ovoid* if and only if it is met by any generator of in exactly one point.

A Hermitian cap $\mathcal{C}$ is usually not a cap of the space $\mathrm{PG}(3,q^2)$. In this paper, 'caps' and 'ovoids' will always be assumed to mean Hermitian caps and Hermitian ovoids.

An example of ovoid is provided by the intersection of the Hermitian surface $\mathcal{U}$ with any non–tangent plane; however, several different constructions are known which lead to projectively inequivalent Hermitian ovoids, see for instance [1], [6], [5].

A Hermitian cap which is maximal with respect to inclusion is said to be *complete*. Hermitian ovoids are clearly complete; yet, there exist also complete caps which are not ovoids.

As a matter of fact, see [3], it is known that if $\widetilde{\mathcal{C}}$ is a complete cap, then

$$q^2+1 \leq |\widetilde{\mathcal{C}}| \leq q^3+1,$$

and both bounds are sharp: in particular, $\widetilde{\mathcal{C}}$ is an ovoid if and only if $|\widetilde{\mathcal{C}}| = q^3+1$.

Any maximal curve $\mathcal{D}$ embedded in $\mathcal{U}$ and different from the Hermitian curve, see [4], provides an example of a cap of size approximately $\frac{1}{4}(q^3-q^2)$. For q even, these caps are always complete; when q is odd, this is not the case: in fact, the set of the points of $\mathcal{D}$ is usually contained in an ovoid.

2000 *Mathematics Subject Classification.* Primary: 51E15 ; Secondary: 68W05, 14H50, 11E39.

Key words and phrases. Hermitian surface, caps, ovoids, algorithms.

The original motivation for this work has been to construct some tools in order to help with the investigation of the relationship between these partial caps and their completions. However, it is currently an open problem to determine the spectrum of cardinalities of complete caps of the Hermitian surface. Numerical evidence suggests that, at least for q prime, there should exist complete caps of cardinality t for almost all values $q^2+1 \leq t \leq q^3-q+1$. It appears also that complete caps are not evenly distributed within this range.

In Section 1, we introduce a strategy to look for complete caps of the Hermitian surface; in Section 2, some improvements on the basic algorithm are suggested; in Section 3, we provide the results of our computations for the cases $q=5$ and $q=7$; these result lead us to conjecture that the size of the second largest complete cap is q^3-q+1.

1. Basic completion strategy

A *generator* of the surface $\mathcal{U}$ is a line of $\mathrm{PG}(3,q^2)$ completely included in $\mathcal{U}$. For any $x \in \mathcal{U}$, denote by Gx the set of all generators of $\mathcal{U}$ passing through x. If we write by $T_x\mathcal{U}$ the tangent plane at x to $\mathcal{U}$, then the set Gx may be determined as

$$Gx = T_x\mathcal{U} \cap \mathcal{U}.$$

A point $p \in \mathcal{U}$ is *covered* by a set $\mathcal{M} \subseteq \mathcal{U}$ whenever

$$PP \cap \mathcal{M} \neq \emptyset.$$

The set of points being covered by $\mathcal{M}$ is written as $G\mathcal{M}$. It is straightforward to show that

$$G\mathcal{M} = \bigcup_{x\in\mathcal{M}} Gx.$$

Proposition 1. *Let $\mathcal{C}$ be a cap of $\mathcal{U}$; take $x \in \mathcal{U} \setminus \mathcal{C}$. Then, the set $\widetilde{\mathcal{C}} = \mathcal{C} \cup \{x\}$ is a cap of $\mathcal{U}$ if and only if $x \notin G\mathcal{C}$.*

Proof. If $x \in G\mathcal{C}$, then there exists a generator L of $\mathcal{U}$ such that $x \in L$ and $L \cap \mathcal{C} \neq \emptyset$. Since $x \notin \mathcal{C}$, it follows that

$$|L \cap \widetilde{\mathcal{C}}| = 2;$$

hence, in this case, $\widetilde{\mathcal{C}}$ is not a cap.

Assume now x not to be covered by $\mathcal{C}$ and let L be any generator of $\mathcal{U}$. If $x \in L$, then $L \cap \mathcal{C} = \emptyset$; hence, $|L \cap \widetilde{\mathcal{C}}| = 1$. On the other hand, if $x \notin L$, then

$$L \cap \widetilde{\mathcal{C}} = L \cap \mathcal{C},$$

which yields $|L \cap \tilde{\mathcal{C}}| \leq 1$. It follows that any generator L of $\mathcal{U}$ meets $\widetilde{\mathcal{C}}$ in at most one point — that is, $\widetilde{\mathcal{C}}$ is a cap. □

For any given cap $\mathcal{C}$, Algorithm 1.1 provides a complete cap $\widetilde{\mathcal{C}}$ with $\mathcal{C} \subseteq \widetilde{\mathcal{C}}$.

This algorithm is guaranteed to complete in *at most* $q^3+1-|\mathcal{C}|$ iterations.

An efficient way to implement step `(6)` is to compute $\mathcal{M}'$ as the set of points of $\mathcal{M}$ which are not conjugate to x according to the unitary polarity induced by $\mathcal{U}$.

2. Large and small completions

For any partial cap $\mathcal{C}$, Algorithm 1.1 determines a complete cap $\widetilde{\mathcal{C}}$ with $\mathcal{C} \subseteq \widetilde{\mathcal{C}}$. However, a small cap $\mathcal{C}$ usually admits several different completions, as it can be seen from the tables of Section 3.1. In fact, even completions with the same cardinality needs not be projectively equivalent, as it can be seen in the case of ovoids.

Algorithm 1.1 Basic completion algorithm

```
Input:  a cap $\mathcal{C}$;
Output: a complete cap $\widetilde{\mathcal{C}}$.
Complete($\mathcal{C}$):=
  (1) Compute the set $\mathcal{M}$ of points of $\mathcal{U}$
      not covered by $\mathcal{C}$;
  (2) If $\mathcal{M} = \emptyset$, return $\mathcal{C}$ and exit;
  (3) Pick a random element $x \in \mathcal{M}$;
  (4) $\mathcal{C} \leftarrow (\mathcal{C} \cup \{x\})$;
  (5) If $|\mathcal{C}| = q^3 + 1$, return $\mathcal{C}$ and exit;
  (6) Compute the set $\mathcal{M}' = (\mathcal{M} \setminus Gx)$;
  (7) $\mathcal{M} \leftarrow \mathcal{M}'$;
  (8) Go back to step (2).
```

Definition 1. A completion $\widetilde{\mathcal{C}}$ of $\mathcal{C}$ is *minimum* if, for any complete cap $\mathcal{D}$ such that $\mathcal{C} \subseteq \mathcal{D}$,

$$|\widetilde{\mathcal{C}}| \leq |\mathcal{D}|;$$

a completion $\widetilde{\mathcal{C}}$ is *maximum* if

$$|\widetilde{\mathcal{C}}| \geq |\mathcal{D}|,$$

for any complete cap $\mathcal{D}$ with $\mathcal{C} \subseteq \mathcal{D}$. We call a completion $\widetilde{\mathcal{C}}$ *optimal* if $\widetilde{\mathcal{C}}$ it is either maximum or minimum.

If there is a completion $\widetilde{\mathcal{C}}$ of $\mathcal{C}$ such that

$$|\widetilde{\mathcal{C}}| \leq |\mathcal{C}| + 1,$$

then, clearly, $\widetilde{\mathcal{C}}$ is a *minimum* completion of $\mathcal{C}$. Likewise, if there is an ovoid $\mathcal{O}$ containing $\mathcal{C}$, then again $\mathcal{O}$ is a *maximum* completion of $\mathcal{C}$.

To determine the size of the optimal completions of a given partial cap is, in general, non–trivial.

In this section, we introduce some refinements to Algorithm 1.1 in order to bias the construction toward obtaining 'large' or 'small' caps containing a prescribed set $\mathcal{C}$.

Definition 2. Let $\mathcal{C}$ be a non–empty cap; for any $x \in \mathcal{U}$, the *relevance* of x with respect to $\mathcal{C}$ is

$$r(x, \mathcal{C}) := |Gx \cup G\mathcal{C}| - |G\mathcal{C}|.$$

Clearly, if $x \in \mathcal{C}$, then $r(x, \mathcal{C}) = 0$. Hence, when $x \in \mathcal{C}$, we shall usually speak of the number

$$r(x, \mathcal{C} \setminus \{x\})$$

as the *relevance of x in $\mathcal{C}$*.

A dual notion to relevance is that of *coverage*.

Definition 3. For any $y \in \mathcal{U}$, the *coverage* of y by $\mathcal{C}$ is the number $c(y, \mathcal{C})$ of points in $x \in \mathcal{C}$ such that $y \in T_x\mathcal{U}$.

The most efficient way to determine $c(x, \mathcal{C})$ is as the cardinality of the set of points of $\mathcal{C}$ which are conjugate to x. From

$$|Gx \cup G\mathcal{C}| = |Gx| + |G\mathcal{C}| - |Gx \cap G\mathcal{C}|,$$

it follows that

$$r(x, \mathcal{C}) + c(x, \mathcal{C}) = |Gx| = q^3 + q^2 + 1.$$

Hence, $r(x, \mathcal{C})$ might be computed directly from $c(x, \mathcal{C})$.

Definition 4. The *weight* of the point $x \in \mathcal{C}$ in $\mathcal{C}$ is the number

$$w(x,\mathcal{C}) := \sum_{y\in Gx} \frac{1}{c(y,\mathcal{C})}$$

The assumption $x \in \mathcal{C}$ guarantees that $c(y,\mathcal{C}) \neq 0$.
For any $x \in \mathcal{C}$, define

$$\mathcal{C}_x := \mathcal{C} \setminus \{x\}.$$

Then, for any $y \in \mathcal{U}$, the relevance of y with respect to $\mathcal{C}_x$ may be written as

$$r(y,\mathcal{C}_x) = r(y,\mathcal{C}) + |(Gx \cap Gy) \setminus \mathcal{C}_x|.$$

Proposition 2. *Let $x \in \mathcal{C}$ and assume $y \notin G\mathcal{C}$. Then,*

$$|G\mathcal{C}_x| = |G\mathcal{C}| - r(x,\mathcal{C}_x),$$

and

$$|G(\mathcal{C} \cup \{y\})| = |G\mathcal{C}| + r(y,\mathcal{C}).$$

Furthermore, $\mathcal{C}$ is complete if and only if $|G\mathcal{C}| = (q^3+1)(q^2+1)$.

The weight of a point $x \in \mathcal{C}$ and its coverage by $\mathcal{C}_x$ are clearly related.

Proposition 3. *For any $x \in \mathcal{C}$,*

$$w(x,\mathcal{C}) = r(x,\mathcal{C}_x) + \sum_{y\in Gx\cap G\mathcal{C}_x} \frac{1}{c(y,\mathcal{C}_x)+1}.$$

Proof. If $y \in Gx$, then

$$c(y,\mathcal{C}) = c(y,\mathcal{C}_x) + 1.$$

For $y \in Gx \setminus G\mathcal{C}_x$, the coverage of y by $\mathcal{C}_x$ is $c(y,\mathcal{C}_x) = 0$; hence, $c(y,\mathcal{C}) = 1$. It follows that

$$\begin{aligned}\sum_{y\in Gx\setminus G\mathcal{C}_x} \frac{1}{c(y,\mathcal{C})} &= \sum_{y\in Gx\setminus G\mathcal{C}_x} 1 = |Gx \setminus G\mathcal{C}_x| = \\ &= |Gx \cup G\mathcal{C}_x| - |G\mathcal{C}_x| = r(x,\mathcal{C}_x).\end{aligned}$$

This implies

$$\begin{aligned} w(x,\mathcal{C}) &= \sum_{y\in Gx\setminus G\mathcal{C}_x} \frac{1}{c(y,\mathcal{C})} + \sum_{y\in Gx\cap G\mathcal{C}_x} \frac{1}{c(y,\mathcal{C})} = \\ &= r(x,\mathcal{C}_x) + \sum_{y\in Gx\cap G\mathcal{C}_x} \frac{1}{c(y,\mathcal{C}_x)+1}, \end{aligned}$$

and the result follows. □

A straightforward argument now proves that

$$r(x,\mathcal{C}) \geq 2w(x,\mathcal{C}) - (q^3+q^2+1).$$

Proposition 4. *For any complete cap $\mathcal{C}$,*

$$\sum_{x\in\mathcal{C}} w(x,\mathcal{C}) = (q^3+1)(q^2+1).$$

Proof. Since $\mathcal{C}$ is complete, the union of all Gx, as x varies in $\mathcal{C}$, is $\mathcal{U}$. Hence, $|G\mathcal{C}|$ might be written as

$$|G\mathcal{C}| = \sum_{x\in\mathcal{C}} \sum_{y\in Gx} \frac{1}{c(y,\mathcal{C})} = \sum_{y\in\mathcal{U}} \frac{c(y,\mathcal{C})}{c(y,\mathcal{C})} = \sum_{y\in\mathcal{U}} 1 = |\mathcal{U}|.$$

The proposition follows. □

Proposition 5. *Let $\mathcal{C}$ be a complete cap of cardinality q^2+1. Then, there exists $x\in\mathcal{C}$ such that*

$$w(x,\mathcal{C}) \geq q^3+1;$$

likewise, if $\mathcal{C}$ is an ovoid, then there is $x\in\mathcal{C}$ such that

$$w(x,\mathcal{C}) \leq q^2+1.$$

Proposition 5 can be proved as an immediate corollary of Proposition 4. It suggests that if a cap is large, then its points might be expected to have small weight and that, conversely, the weight of points of a large cap is usually fairly large.

Proposition 6. *Let $\mathcal{C}$ be a non–empty cap; then, for any $x\in\mathcal{U}$ not covered by $\mathcal{C}$,*

$$1 \leq r(x,\mathcal{C}) \leq q(q^2+q-1).$$

Furthermore, if there is $x\in\mathcal{U}$ such that $r(x,\mathcal{C})=1$, then $|\mathcal{C}|\geq q^2$.

Proof. Clearly, for $\mathcal{C}\subseteq\mathcal{C}'$,

$$r(x,\mathcal{C}) \geq r(x,\mathcal{C}').$$

Hence, in order to prove the upper bound on $r(x,\mathcal{C})$, it is enough to consider the case when $|\mathcal{C}|=1$. Assume x,y be two distinct points of $\mathcal{U}$ and suppose that x is not covered by y. Then, $x\notin T_y\mathcal{U}$ and neither x nor y are on the line

$$T_{xy}\mathcal{U} = T_x\mathcal{U}\cap T_y\mathcal{U}.$$

Furthermore, $T_{xy}\mathcal{U}$ meets $\mathcal{U}$ in $q+1$ points and

$$Gx\cap Gy = Gx\cap T_{xy}\mathcal{U}.$$

Hence,

$$|Gx\cap Gy| = q+1.$$

It follows that

$$r(x,\{y\}) = q(q^2+q-1).$$

The lower bound on $r(x,\mathcal{C})$ is immediate.

Suppose now $r(x,\mathcal{C})=1$, and consider a component L of $\mathcal{U}$ which is in Gx. All points of L but x are covered by some point of $y\in\mathcal{C}$. Hence,

$$\forall t\in L\setminus\{x\}, \exists y\in\mathcal{C} : t\in T_y\mathcal{U}\cap T_x\mathcal{U}.$$

Furthermore, if two points t,t' of L were covered by the same $y\in\mathcal{U}$, then $tt'=L\subseteq T_y\mathcal{U}$ and x would also by covered by y — a contradiction, since $r(x,\mathcal{C})=1$. This implies that $\mathcal{C}$ contains at least q^2 points. □

Proposition 7. *The second largest value for $r(x,\mathcal{C})$ is q^3+q^2-2q.*

Proof. As before, it might be assumed without loss of generality that $\mathcal{C}=\{y,z\}$. Let $x\in\mathcal{U}\setminus G\mathcal{C}$. Then, either

$$T_{xy}\mathcal{U} = T_{xz}\mathcal{U} = T_{xz}\mathcal{U} = L,$$

or

$$T_{xy}\mathcal{U}\cap T_{yz}\mathcal{U}\cap T_{xz}\mathcal{U} = \{p\}.$$

In the former case,

$$r(x,\mathcal{C}) = |T_x\mathcal{U} \cap \mathcal{U}| - |L \cap \mathcal{U}| = q(q^2+q-1).$$

In the latter, the lines T_{xy}, T_{yz} and T_{xz} are not tangent to the surface $\mathcal{U}$. Hence, each of them meets $\mathcal{U}$ in $q+1$ points. There are two possibilities:

(1) if $p \notin \mathcal{U}$, then

$$r(x,\mathcal{C}) = q^2(q+1)+1-2(q+1) = q^3+q^2-2q-1;$$

(2) if $p \in \mathcal{U}$, then

$$r(x,\mathcal{C}) = q^2(q+1)+1-2q-1 = q^3+q^2-2q.$$

The result follows □

We adopted two different approaches to the construction of optimal completions of a partial cap $\mathcal{C}$:

(1) a forward–looking algorithm, in which points to be added are chosen carefully at each iteration;
(2) a backtracking technique, in which a small completion of the original cap, obtained, say, using Algorithm 1.1, is enlarged by replacing suitable points.

2.1. **The forward–looking approach.** The main advantage of this approach is that it is possible to estimate *a priori* the complexity and the execution time of the algorithm; however, unless all possible completions are examined or an ovoid is found, we are usually unable to guarantee that the completion that has been constructed is actually optimal.

For any cap $\mathcal{C}$, define two functions

$$\begin{aligned} r^+(\mathcal{C}) :=& \ \max\nolimits_{x \notin G\mathcal{C}} r(x,\mathcal{C}); \\ r^-(\mathcal{C}) :=& \ \min\nolimits_{x \notin G\mathcal{C}} r(x,\mathcal{C}). \end{aligned}$$

Clearly, $r^-(\mathcal{C}) = 0$ if and only if $r^+(\mathcal{C}) = 0$ and the cap $\mathcal{C}$ is complete. One remarkable case arises when $r^+(\mathcal{C}) = 1$.

Proposition 8. *Let $\mathcal{C}$ be a cap and suppose $r^+(\mathcal{C}) = 1$. Then, there exists exactly one complete cap $\widetilde{\mathcal{C}}$ such that $\mathcal{C} \subseteq \widetilde{\mathcal{C}}$ and*

$$\widetilde{\mathcal{C}} = \mathcal{C} \cup (\mathcal{U} \setminus G\mathcal{C}).$$

Proof. Let $\mathcal{M} = \mathcal{U} \setminus G\mathcal{C}$. Clearly, if $\mathcal{C} \cup \mathcal{M}$ is a cap, then it is complete, since all the points of $\mathcal{U}$ are being covered by it. The proof that $\mathcal{C} \cup \mathcal{M}$ is a cap is by induction on $n = |\mathcal{M}|$.

For $n = 1$, the proposition is trivial.

Assume now $n > 1$, and let x be a point of $\mathcal{M}$. Since $r^+(\mathcal{C}) = 1$, then $r(x,\mathcal{C}) = 1$. Define $\mathcal{C}^x = \mathcal{C} \cup \{x\}$. Clearly $\mathcal{C}^x$ is a cap; furthermore,

$$G(\mathcal{C}^x) = G\mathcal{C} \cup \{x\},$$

that is

$$\mathcal{M}^x := (\mathcal{U} \setminus \mathcal{C}^x) = \mathcal{M} \setminus \{x\}.$$

Hence, $|\mathcal{M}^x| = n-1$ and for any $y \in \mathcal{M}^x$,

$$r(y,\mathcal{C}^x) = 1.$$

The result now follows from the inductive assumption. □

Proposition 9. *The function r^+ is monotonic non–increasing, in the sense that*

$$\mathcal{C}' \subseteq \mathcal{C} \Rightarrow r^+(\mathcal{C}') \geq r^+(\mathcal{C}).$$

Proof. It is possible to assume without loss of generality $\mathcal{C}' = \mathcal{C}_x$. Take $y \in \mathcal{U}$ to be a point of $\mathcal{U} \setminus G\mathcal{C}$ such that $r(y, \mathcal{C}) = r^+(\mathcal{C})$. Then,

$$r^+(\mathcal{C}_x) \geq r(y, \mathcal{C}_x) = r(y, \mathcal{C}) + |(Gx \cap Gy) \setminus \mathcal{C}_x| \geq r^+(\mathcal{C}).$$

The result follows. □

The simplest selection technique which can be used in order to construct large complete caps is *to choose at each iteration a point in $\mathcal{U}$ of minimal relevance*, that is $x \in \mathcal{U}$ such that

$$r(x, \mathcal{C}) = r^-(\mathcal{C}).$$

Clearly, this is the choice for a point to be added to $\mathcal{C}$ which is 'locally best', in the sense that it always minimises the number of new covered points. However, the function $r^-(\mathcal{C})$ needs not be monotonic and this approach might leave points of weight regrettably large to be added in the final stages of the construction — the cap thus obtained, hence, may not be *maximum*. In order to get further insights on this issue, the algorithm has been tested providing as initial input a small subset of the points of a known ovoid. The results of this approach are discussed in Section 3.2.

It has been seen that, if the initial datum is small and random, then the result is a complete cap of size which usually approximates $q^3 - q^2$. This confirms that, while the biased algorithm provides caps much larger than the ones of Algorithm 1.1, none the less the choice of the point x to be added to $\mathcal{C}$ at each iteration should not depend only on the value of $r^-(\mathcal{C})$.

Proposition 10. *Let $\mathcal{O}$ be an ovoid. Then, for any $x \in \mathcal{O}$,*

$$r(x, \mathcal{O}_x) = 1.$$

Proof. Any point $p \in \mathcal{U}$ belongs to exactly $q+1$ generators. An ovoid $\mathcal{O}$ is a set of q^3+1 points which blocks all $(q^3+1)(q+1)$ lines of the Hermitian surface $\mathcal{U}$; hence, for each $[\in \mathcal{U}$, all generators through p are blocked.

Assume now that $r(x, \mathcal{O}_x) > 1$. Then, there is a point $y \in \mathcal{U} \setminus \mathcal{O}$ such that $y \in Gx$ and $y \notin Gz$ for any $z \in \mathcal{O}_x$. Clearly, the only line through y which is blocked by x is xy. It follows that there are at least q points of $\mathcal{O}_x$ which cover y — a contradiction. It follows that $r(x, \mathcal{O}_x) = 1$. □

Proposition 11. *Let $\mathcal{O}$ be an ovoid. Then, for any $\Omega \subseteq \mathcal{O}$ such that $|\Omega| < q+1$,*

$$r^+(\mathcal{O} \setminus \Omega) = 1.$$

Proof. Any point $y \in \mathcal{U} \setminus \mathcal{O}$ is covered by $q+1$ points of $\mathcal{O}$. Hence, all the points of $\mathcal{U} \setminus \mathcal{O}$ are covered by the cap $\mathcal{O} \setminus \Omega$. Since Ω is a cap, it follows that the relevance of each $x \in \Omega$ is 1, which provides the result. □

An immediate consequence of Proposition 11 is that if a set $\mathcal{C}$ of $q^3 - q + 1$ points is contained in an ovoid $\mathcal{O}$, then $\mathcal{O}$ is the only complete cap containing $\mathcal{C}$.

Corollary 12. *Let $\mathcal{O}$ and $\mathcal{O}'$ be two distinct ovoids. Then,*

$$|\mathcal{O} \setminus \mathcal{O}'| \geq q+1.$$

There are complete ovoids which differ in exactly $q+1$ points; for instance, this is the case for ovoids obtained from each other by derivation, see [5].

Proposition 13. *Let $\mathcal{O}$ be an ovoid. Then, there is $\Omega \subseteq \mathcal{O}$ such that $|\Omega| \geq \frac{1}{2}(q^2+q)$ and the only complete cap containing $\mathcal{O}' := \mathcal{O} \setminus \Omega$ is $\mathcal{O}$.*

Proof. The set Ω will be constructed step by step. Let P_0 be any point of $\mathcal{U} \setminus \mathcal{O}$; then, P_0 is covered by $q+1$ points of $\mathcal{O}$. Take now as Ω_0 any set of q points of $\mathcal{O}$ covering P_0 and let

$$\Lambda_1 := \mathcal{O} \setminus \Omega_0.$$

From Proposition 11, the only complete cap containing Λ_1 is $\mathcal{O}$.

For each $q > i > 0$, fix a point P_i in $\mathcal{U} \setminus \mathcal{O}$ such that P_i is covered by at least $q + 1 - i$ points of

$$\Lambda_i := \Lambda_{i-1} \setminus \Omega_{i-1}.$$

Observe that any point of $\mathcal{U} \setminus \mathcal{O}$ different from the P_j's with $j < i$ satisfies this condition. Then, let Ω_i be a set of $q - i$ points of Λ_i covering P_i — it follows that Ω_i is, by construction, disjoint from any of the Ω_j for $j < i$. This procedure may be iterated q times. Define now

$$\Omega := \bigcup_{i=0}^{q-1} \Omega_i.$$

Since, for $i \neq j$,

$$\Omega_i \cap \Omega_j = \emptyset,$$

the cardinality of Ω is $\frac{1}{2}q(q + 1)$. Furthermore, each point of $\mathcal{U} \setminus \mathcal{O}$ is covered by $\mathcal{O}'$. It follows that any completion of $\mathcal{O}'$ is contained in $\mathcal{O}' \cup \Omega$. The result is now a consequence of the fact that $\mathcal{O}' \cup \Omega$ is a complete cap. □

Propositions 10, 11 and 13 suggest that a a partial cap $\mathcal{C}$ of size approximately $q^3 - q^2$ could be enough to determine an ovoid. However, in order for such a set $\mathcal{C}$ to be contained in an ovoid, it is necessary that many of the points of $\mathcal{U} \setminus G\mathcal{C}$ have small relevance.

This inspired the following strategy to look for large caps when provided only with a small initial datum: rather than choosing every time a point with the smallest relevance, it is possible to pick an x which yields a large number of points of minimal relevance for $\mathcal{C}^x$.

This approach may be implemented as follows. Given a cap $\mathcal{C}$ and a point x, define $\rho^-(x, \mathcal{C})$ as the number of points t in $\mathcal{C}_x$ such that $r(t, \mathcal{C}_x) = r^-(\mathcal{C}_x)$. Then,

$$\rho^-(x, \mathcal{C}) := |\{t \in \mathcal{U} : r(t, \mathcal{C}_x) = r^-(\mathcal{C}_x)\}|.$$

In Algorithm 2.1, a point x which maximises $\rho^-(\mathcal{C})$ is determined. The symbol $\oplus$ is used to denote the concatenation of two ordered lists.

Algorithm 2.1 Point selection: forward search

```
Input:  a cap $\mathcal{C}$;
Output: a point $x \notin G\mathcal{C}$.
Fw_Complete:=
  (1) if $r^-(\mathcal{C}) = 1$, then return any $x \in G\mathcal{C}$
      and exit;
  (2) $M \leftarrow [\ ]$;
  (3) For $t \notin G\mathcal{C}$,
      (a) $\mathcal{C}_0 \leftarrow \mathcal{C} \cup \{t\}$;
      (b) $L \leftarrow \{x \in \mathcal{U} : r(x, \mathcal{C}_0) = r^-(\mathcal{C}_0)\}$;
      (c) $M \leftarrow M \oplus [L]$;
  (4) $k \leftarrow \min\{|L| : L \in M\}$;
  (5) select $x \in G\mathcal{C}$ such that $\rho^-(x, \mathcal{C}) = k$.
```

2.2. **The backtracking approach.**

Proposition 14. *Let $\mathcal{C}$ be a complete cap of cardinality n and assume that there is $p \in \mathcal{C}$ such that for some $x \in Gp \setminus G\mathcal{C}_p$,*

$$r(p, \mathcal{C}_p) > r(x, \mathcal{C}_p).$$

Then, the cap $\mathcal{C}_p$ is contained in a complete cap of cardinality at least $n + 1$.

Proof. From Proposition 2,

$$|G(\mathcal{C}_p \cup \{x\})| = |G\mathcal{C}| - r(p, \mathcal{C}_p) + r(x, \mathcal{C}_p).$$

Since $r(x, \mathcal{C}_p) < r(p, \mathcal{C}_p)$, it follows that

$$|G(\mathcal{C}_p \cup \{x\})| < (q^3 + 1)(q^2 + 1).$$

Hence, $\mathcal{C}_p \cup \{x\}$ is a cap of cardinality n which is not complete and contains $\mathcal{C}$. The result follows. □

Another way to construct large caps is, as Proposition 14 suggests, by a backtracking procedure. The main idea underlying this technique is to start with a small complete cap $\mathcal{C}$ and try to replace points with large relevance with others whose relevance is smaller.

In general, it might not be possible to find a good replacement if only one point is removed; this is the case, for example, when the starting cap is already fairly large.

For instance, according to Proposition 11, if a cap $\mathcal{C}$ has size is at least $q^3 - q + 1$ and it is contained in an ovoid $\mathcal{O}$, then all the points which are not covered by $\mathcal{C}$ have relevance 1. Clearly, in order to succeed, the algorithm needs to remove as many points from the cap as to be able to fine some point which is not covered anymore and that has relevance larger than 1.

However, as the following propositions show, it has to be expected that very few points of a minimal complete cap have small relevance. Furthermore, if any point of a complete cap $\mathcal{C}$ has large relevance, then it is always possible to construct another complete cap $\mathcal{C}'$ in such a way as to have $|\mathcal{C} \setminus \mathcal{C}'| = 1$ and $|\mathcal{C}'| > |\mathcal{C}| + 1$.

Proposition 15. *Let $\mathcal{C}$ be a complete cap and assume that there is $p \in \mathcal{C}$ such that $r(p, \mathcal{C}_p) > q^2 + 1$. Then, for any $x \in \Gamma_p := Gp \setminus (G\mathcal{C}_p \cup \{p\})$,*

$$r(x, \mathcal{C}_p) < r(p, \mathcal{C}_p).$$

Proof. Since $r(p, \mathcal{C}_p) > q^2 + 1$, not all the points of Γ_p lie on a line. On the other hand, for any $x \in \Gamma_p$,

$$Gp \cap Gx = px$$

Let now $\mathcal{C}' = \mathcal{C}_p \cup \{x\}$. From the first remark above, there is $y \in Gp \setminus Gx$ such that

$$y \notin G(\mathcal{C}') = G\mathcal{C}_p \cup px.$$

Since $\mathcal{C}$ is complete,

$$Gx \setminus G\mathcal{C}_p = Gp \cap Gx = px.$$

From this, the result follows and

$$r(x, \mathcal{C}'_x) = r(x, \mathcal{C}_p) \leq q^2 + 1.$$

□

Proposition 16. *Let $\mathcal{C}$ be a complete cap of cardinality $q^2 + 1$. Then, there is $p \in \mathcal{C}$ such that $r(p, \mathcal{C}_p) > q^2 + 1$.*

Proof. Suppose that $r^+(\mathcal{C}) < q^2 + 1$. Then,

$$(q^3 + 1)(q^2 + 1) = |\mathcal{U}| \leq (q^2 + 1)r^+(\mathcal{C}) \leq (q^2 + 1)^2,$$

a contradiction. □

A simple backtracking approach is presented in Algorithm 2.2. Proposition 16 guarantees that, given any cap $\mathcal{C}$, a point is determined after at most $|\mathcal{C}| - q^2 - 1$ recursive calls.

Algorithm 2.2 Backtracking: large caps

```
Input:  a cap $\mathcal{C}$, a cap $\mathcal{C}'$ with $\mathcal{C} \subseteq \mathcal{C}'$;
Output: a cap $\mathcal{C}''$ with $\mathcal{C} \subseteq \mathcal{C}''$.

Large_Cap($\mathcal{C}$,$\mathcal{C}'$):=
  (1) if $\mathcal{C}' = \mathcal{C}''$, then exit;
  (2) compute $M = \max_{t \in \mathcal{C}' \setminus \mathcal{C}} r(t, \mathcal{C}')$;
  (3) select $x \in \mathcal{C}' \setminus \mathcal{C}$ such that $r(p, \mathcal{C}') = M$;
  (4) $\mathcal{C}'' \leftarrow \mathcal{C}' \setminus \{p\}$;
  (5) if $\exists x \notin G\mathcal{C}''$ such that $r(x, \mathcal{C}'' \cup \{x\}) <$
      $M$, then
        (a) $\mathcal{C}'' \leftarrow \mathcal{C}'' \cup \{x\}$;
        (b) return $\mathcal{C}''$;
      else
        (a) $\mathcal{C}'' \leftarrow$ Large_Cap($\mathcal{C}, \mathcal{C}''$);
  (6) let $x \notin G\mathcal{C}''$ such that
        $w(x, \mathcal{C}'' \cup \{x\}) = \min_{y \notin G\mathcal{C}''} w(y, \mathcal{C}'' \cup \{y\});$
  (7) $\mathcal{C}'' \leftarrow \mathcal{C}'' \cup \{x\}$.
```

3. Results of Algorithm 1.1

Algorithm 1.1, as presented in this paper, has been implemented with the computer algebra package GAP [2] and some tests have been performed for small values of q, namely $q = 5$ and $q = 7$. The methodology followed has usually been to iterate each test at least 1000 times and then consider an average of the results. The numbers in all the tables of this section represent the *chance* of obtaining a cap of given size using the algorithm, when a set of prescribed cardinality is provided as input.

3.1. **Random search.** Algorithm 1.1, with the selection of points done at random, may be used in order to investigate the *spectrum* of complete caps of the Hermitian surface. The results of a test performed with the empty set as initial datum are presented in Table 1 for $q = 5$ and in Table 2 for $q = 7$.

$\lvert\widetilde{\mathcal{C}}\rvert$	%
78	0.1
79	1.0
80	1.9
81	5.9
82	9.3
83	16.3
84	19.7
85	16.5
86	12.6
87	9.5
88	4.7
89	1.6
90	0.8
91	0.1

TABLE 1. Distribution of caps: results of Algorithm 1.1 with $q = 5$ and $\mathcal{C} = \emptyset$

The same algorithm, for $q = 5$, when the input $\mathcal{C}$ has been a set of 50 random points contained in an ovoid, has produced at least one large complete cap, but no ovoid, as it can be seen in Table 3. The

$\lvert\widetilde{\mathcal{C}}\rvert$	%
195	0.3
196	0.6
197	1.4
198	2.0
199	4.0
200	5.8
201	8.7
202	10.3
203	10.3
204	11.1
205	12.8
206	9.0
207	8.1
208	7.7
209	4.6
210	1.9
211	0.1
212	1.0
213	0.3

TABLE 2. Distribution of caps: results of Algorithm 1.1 with $q = 7$ and $\mathcal{C} = \emptyset$

$\lvert\widetilde{\mathcal{C}}\rvert$	%
81	0.1
82	0.2
83	0.7
84	1.0
85	2.4
86	4.8
87	7.9
88	12.7
89	10.3
90	12.4
91	10.9
92	10.3
93	6.5
94	5.9
95	4.3
96	2.8
97	3.0
98	1.4
99	1.0
100	0.4
101	0.4
102	0.2
103	0.2
104	0.1
106	0.1
112	0.1

TABLE 3. Distribution of caps: results of Algorithm 1.1 with $q = 5$ and $|\mathcal{C}| = 50$

$\lvert\widetilde{\mathcal{C}}\rvert$	%
198	0.2
199	0.5
200	0.1
201	1.9
202	2.8
203	4.0
204	5.0
205	8.6
206	9.2
207	11.2
208	13.1
209	11.1
210	9.3
211	7.3
212	7.0
213	3.6
214	2.5
215	1.0
216	0.8
217	0.5
218	0.2
219	0.1

TABLE 4. Distribution of caps: results of Algorithm 1.1 with $q = 7$ and $|\mathcal{C}| = 98$

results for $q = 7$ with an input set $\mathcal{C}$ of size 98 have been similar, see Table 4. Clearly, as it had to be expected, ovoids represent only a tiny fraction of possible complete caps and it is very difficult for them to occur if the initial cap has size much smaller than $q^3 - q^2$. However, as the size of the input set grows, the chances for a ‘random’ completion of the cap to be an ovoid increase as well: this can be seen in Table 5, where the results of an experiment realised with $|\mathcal{C}| = 69$ and $q = 5$ are presented.

$\lvert\widetilde{\mathcal{C}}\rvert$	%
100	0.1
101	0.6
102	0.5
103	0.9
104	1.0
105	1.1
106	1.8
107	1.1
108	3.5
109	3.3
110	4.8
111	4.8
112	6.7
113	6.0
114	3.0
115	2.7
116	14.4
117	9.0
118	1.9
119	8.0
121	22.4
126	9.7

TABLE 5. Distribution of caps: results of Algorithm 1.1 with $q = 5$ and $|\mathcal{C}| = 69$

$\lvert\widetilde{\mathcal{C}}\rvert$	%
291	0.1
293	0.1
296	0.1
299	0.1
300	0.2
301	0.3
302	0.1
303	0.2
304	0.3
305	0.3
306	0.4
307	0.7
308	1.0
309	0.5
310	0.9
311	1.2
312	1.4
313	1.7
314	2.0
315	0.9
316	1.0
317	2.3
318	4.4
319	3.7
320	1.6
321	0.8
322	0.3
323	5.6
324	8.5
325	5.3
326	2.2
327	1.2
328	0.3
329	0.1
330	15.3
331	6.4
332	0.9
333	0.2
335	0.2
337	19.4
344	7.6

TABLE 6. Distribution of caps: results of Algorithm 1.1 with $q = 7$ and $|\mathcal{C}| = 190$

Observe that no caps with size $121 < |\mathcal{C}| < 126$ have been found. The same computations for $q = 7$ and $|\mathcal{C}| = 190$ provide the results of Table 6. The same tests, when performed for $q = 7$ and $|\mathcal{C}| = 237$ and for $q = 9$ and $|\mathcal{C}| = 450$ have produced the results of Tables 7 and 8 — as it can be seen, in this cases most of the complete caps constructed have been ovoids.

$\lvert\widetilde{\mathcal{C}}\rvert$	%
331	2.0
337	17.0
344	81.0

TABLE 7. Distribution of caps: results of 100 runs of Algorithm 1.1 with $q = 7$ and $|\mathcal{C}| = 237$

$\lvert\widetilde{\mathcal{C}}\rvert$	%
705	1.0
712	3.0
713	4.0
720	1.0
721	24.0
730	67.0

TABLE 8. Distribution of caps: results of 100 runs of Algorithm 1.1 with $q = 9$ and $|\mathcal{C}| = 450$

However, no complete cap $\mathcal{C}$ with cardinality

$$q^3 - q + 1 < |\mathcal{C}| < q^3 + 1$$

has been found. This suggests the following conjecture.

Conjecture 17. *The size of the second largest complete cap of the Hermitian surface is* $q^3 - q + 1$.

3.2. **Biased search.** In this subsection we consider complete caps obtained by using a variant of Algorithm 1.1, in which the point to be added to the partial cap $\mathcal{C}$ at each iteration is required to have minimal relevance. The initial input, as before, is a partial cap $\mathcal{C}$ provided by a random subset of given size of an ovoid. This version of the algorithm has shown an interesting behaviour: when the initial *datum* is large enough, say $|\mathcal{C}| > 34$ for $q = 5$, the the result turns out to be usually, but not always, an ovoid — this proves that this procedure is a definite improvement over the purely random search, where, in order to have a reasonable chance of finding ovoids, at least 60 points had to be prescribed.

In order to be able to compare these results with those of the previous subsection, we have run the algorithm with 100 different random subsets of size 69 as input: the algorithm has, in all these cases, constructed an ovoid. As a matter of fact, an ovoid has been found even with an input *datum* as small as a set of only 10 points. However, we have also verified that there exist caps of size at least 34 for which this program produces completions of size 98.

The results for $q = 7$ and $|\mathcal{C}| \geq 90$ have been similar.

A future development of this work will be deeper investigation of these issues and their relationship with the structure of the original ovoid $\mathcal{O}$ as described by its group of automorphisms.

REFERENCES

[1] **A.E. Brouwer and H. Wilbrink**, *Ovoids and fans in the generalized quadrangles* $Q(4,2)$, Geom. Dedicata **36** (1990), 121–124.

[2] **The GAP Group**, *GAP – Groups, Algorithms, and Programming, Version 4.3* (2001), `http://www.gap-system.org.`

[3] **G. Korchmáros**, *Caps of the Hermitian variety arising from maximal curves*, preprint.

[4] **G. Korchmáros** and **F. Torres**, *Maximal curves embedded in a Hermitian variety*, Compositio Math. **128** (2001), 95–113.

[5] **S.E. Payne** and **J.A. Thas**, *Spreads and ovoids in finite generalized quadrangles*, Geom. Dedicata **52** (1994), no. 3, 227–253.

[6] **J.A. Thas**, *Old and new results on spreads and ovoids of finite classical polar spaces*, in A. Barlotti et al (eds), Combinatorics'90 Ann. Discrete Math. **52** (1992), 529–544.

LUCA GIUZZI, DIPARTIMENTO DI MATEMATICA, FACOLTÀ DI INGEGNERIA, UNIVERSITÀ DEGLI STUDI DI BRESCIA, VIA VALOTTI 9, 25133 BRESCIA (ITALY)

E-mail address: `giuzzi@dmf.unicatt.it`

URL: `http://www.dmf.unicatt.it/˜giuzzi`