Designs, Codes and Cryptography, 17, 37–60 (1999)
© 1999 Kluwer Academic Publishers, Boston. Manufactured in The Netherlands.

Long Binary Linear Codes and Large Caps in Projective Space

AIDEN A. BRUEN bruen@uwo.ca
Department of Mathematics, University of Western Ontario, London, Ont., Canada N6A 3K7

DAVID L. WEHLAU wehlau@mast.queensu.ca
Department of Mathematics and Computer Science, Royal Military College, Kingston, Ontario, Canada K7K 7B4 and Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada K7L 3N6

Dedicated to the memory of E. F. Assmus

Received February 20, 1998; Revised October 20, 1998; Accepted October 29, 1998

Abstract. We obtain, in principle, a complete classification of all long inextendable binary linear codes. Several related constructions and results are presented.

Keywords: caps, codes, periodic, projective space

1. Introduction

Recall that a cap in $\Sigma = \mathbb{PG}(n, 2)$ is a set S of points with no three collinear. The connection between such caps and binary linear codes (of minimum distance 4) has been well-studied (see for example [6, 7, 13, 3, 8]). For further background we refer also to [1, 2]. In particular the following can be shown: A cap S is maximal if and only if the corresponding code C is non-lengthening, i.e., has covering radius 2.

This result explains the fundamental importance of maximal caps S in $\Sigma = \mathbb{PG}(n, 2)$. Let S be such a maximal cap. One can argue as follows. Each line of Σ must intersect the complement of S, S^C. Thus when $|S|$ gets very big one can show, since S^C is small and intersects all lines that S^C contains a hyperplane L. Thus S, being maximal, must be all of affine space, i.e., $S = \mathbb{AG}(n, 2)$ and $|S| = 2^n$. One wants to determine the "cut-off point" beyond which $|S| = 2^n$.

In their remarkable paper [6] the authors make a profound contribution to the theory. In particular they are able to show using a celebrated result on abelian groups due to M. Kneser (see [10, 11] and [9]) the following: if $|S| \geq 2^{n-1} + 2$ then S is obtained by successively doubling a cap in lower dimensions. It follows from this that, if $|S| > 2^{n-1}$ then $|S| = 2^{n-1} + 2^t$. It also follows that, to determine the structure of S one needs only determine the structure of critical caps, i.e., caps of cardinality $2^{n-1}+1$, which are maximal in $\Sigma = \mathbb{PG}(n, 2)$.

This is in fact the main unsolved problem in [6]. In the present paper we solve this problem, at least formally (see Theorem 13.6), and explore several different but related issues as follows.

Section 2 contains basic definitions. In Theorem 3.16 using work in [6] we show that if $|S| \geq 2^{n-1}+1$ then there exists a subspace $H_\infty \cong \mathbb{PG}(n-2,2)$ in $\Sigma = \mathbb{PG}(n,2)$ disjoint from S. Section 4 gives the construction for critical maximal caps having a tangent hyperplane. We mention here that in [6] the authors show that in $\mathbb{PG}(n,2)$, with $n \leq 5$, all critical maximal caps have tangent hyperplanes. The construction of critical caps with a tangent hyperplane is easy: the difficulty is in finding a criterion for maximality. This criterion leads to a very general result (Theorem 5.1) concerning binary codes linear or not. Some combinatorial applications are treated in Section 6.

In Section 7 we introduce the useful notion of a quasi-maximal critical cap in $\Sigma = \mathbb{PG}(n,2)$. These may or may not be maximal and are characterized in Theorem 7.4.

A very general class of examples of critical caps in $\mathbb{PG}(n,2)$, called *fractal caps*, is constructed in Section 9. Using this (see Corollary 10.2) we can show that for $n \geq 6$ there exist critical maximal caps having no tangent hyperplanes.

Various structure theorems are given in Section 11. For example, it is shown that every critical quasi-maximal cap which is not maximal has a tangent hyperplane. In Theorem 12.1 we show that a critical maximal cap is either P_1-decomposable (Section 11) or has a tangent hyperplane. Finally in Section 13 we obtain the complicated structure of all P_1-decomposable critical maximal caps. It transpires that they are all obtained by starting from a fractal cap J and applying a sequence of at most $n-2$ W-moves in $\mathbb{PG}(n,2)$ to J.

2. Large Maximal Caps

DEFINITION 2.1 A set of points in $\mathbb{PG}(n,2)$ is a *cap* if it contains no line of $\mathbb{PG}(n,2)$. A cap is *maximal* if it is not a proper subset of any other cap in $\mathbb{PG}(n,2)$. We will call a cap, S, in $\mathbb{PG}(n,2)$ *large* if $|S| \geq 2^{n-1}+1$ and *critical* (or critical in $\mathbb{PG}(n,2)$) if $|S| = 2^{n-1}+1$.

There is a one-to-one correspondence between caps in $\mathbb{PG}(n,2)$ and binary codes (see for example [6, 7, 13, 3, 8, 1, 2]). Briefly, let C be a binary linear code of length N, dimension k and minimum distance 4. Let $C^\perp$ be the dual code. A basis for C yields a $k \times N$ matrix and a basis for $C^\perp$ yields a matrix M of size $(N-k) \times N$. Set $n := N-k-1$. Then the columns of M yield a cap S consisting of N points in $\mathbb{PG}(n,2)$. Moreover, C is a code with covering radius 2 if and only if S is a maximal cap. The process can be reversed to obtain a code from a cap. Thus our results may be simultaneously interpreted in terms of codes or caps.

We want to apply results of KEMPERMAN from the paper which is concerned with small sumsets in discrete abelian groups. Let $V(n+1,2)$ denote an $n+1$ dimensional vector space over the field of order 2. We denote the origin of this vector space by $\mathbf{0}$. By definition, elements of $\mathbb{PG}(n,2)$ correspond to lines in $V(n+1,2)$ through $\mathbf{0}$. Such a line consists of two elements: $\{v, \mathbf{0}\}$. We will identify this line with its non-zero element v. This identifies $\mathbb{PG}(n,2)$ with the set of non-zero vectors in the abelian group $V(n+1,2)$. This identification establishes a correspondence between subgroups F of $V(n+1,2)$ and projective subspaces $\mathbb{PG}(F) = F \setminus \{\mathbf{0}\}$ of $\mathbb{PG}(n,2)$.

DEFINITION 2.2 Let X be a non-empty subset of $\Sigma = \mathbb{PG}(n,2)$. A *vertex* for X is a point v of Σ such that $v + X = X$. If X has a vertex we say that X is *periodic*.

LEMMA 2.3 *If X is periodic then $|X|$ is even.*

Proof. Let v be a vertex for X. If v were an element of X then $\mathbf{0} = v + v \in X$ contradicting the fact that $\mathbf{0}$ is not a point of Σ. Thus $v \notin X$. Moreover, by definition, if we join v to a point of X then third point of the resulting line is also in X. ∎

Often we will decompose $\Sigma = \mathbb{PG}(n, 2)$ by fixing a subspace $H_\infty \cong \mathbb{PG}(n-2, 2)$ of Σ and considering the pencil of three hyperplanes L_A, L_B and L_C of Σ which contain H_∞. In this situation we will call a line of Σ a *cross-line* (with respect to H_∞) if it contains no points of H_∞.

3. Large Caps

THEOREM 3.1 *Let $S \subset \Sigma = \mathbb{PG}(n, 2)$ be a large cap which is disjoint from some hyperplane L of Σ. Then the only maximal cap of Σ which contains S is $\Sigma \setminus L$.*

Proof. All points of $\Sigma \setminus L$ extend S. On the other hand, let x be a point of L. We show that there is a secant to S through x. There are 2^{n-1} lines of Σ passing through x which are not contained entirely in L. Since $|S| > 2^{n-1}$ at least one of these lines must be a secant line to S. ∎

COROLLARY 3.2 *Let $S \subset \Sigma$ be a large cap.*

(1) If S is disjoint from a hyperplane L of Σ, then S meets every hyperplane of Σ different from L.

(2) If S is maximal and $|S| < 2^n$ then S intersects every hyperplane of Σ.

Proof. Use the fact that if M is a hyperplane of Σ with $S \cap M = \emptyset$ then S is a subset of the maximal cap $\Sigma \setminus M$. ∎

Let S be a cap in $\Sigma = \mathbb{PG}(n, 2)$ which is disjoint from some projective subspace $H_\infty \cong \mathbb{PG}(n-2, 2)$ of Σ.

DEFINITION 3.3 We say that S is *quasi-maximal* (with respect to H_∞) if every point of Σ which is not a point of H_∞ either lies in S or lies on a secant to S. Thus if S is quasi-maximal but not maximal it can only be extended by points of H_∞.

An easy example where S is quasi-maximal but not maximal can be constructed in $\mathbb{PG}(2, 2)$ as follows. Choose any point H_∞. There are three lines L_A, L_B and L_C on H_∞. Choose points a, b, c all different from H_∞ on L_A, L_B, L_C respectively with a, b, c not collinear. Then $S = \{a, b, c\}$ is quasi-maximal but not maximal since H_∞ is the unique point extending S.

DEFINITION 3.4 Let S be a cap in $\Sigma = \mathbb{PG}(n, 2)$ and let $H_\infty \cong \mathbb{PG}(n-2, 2)$ be a subspace disjoint from S. Let L be any one of the three hyperplanes containing H_∞. Assume that every point of $L \setminus H_\infty$ lies on a secant to S. Then we say that S is *L-maximal*.

Clearly S is quasi-maximal with respect to H_∞ if and only if S is L-maximal for each of the three hyperplanes L of Σ containing H_∞.

LEMMA 3.5 *Let $S \subset \Sigma$ be a large cap which is quasi-maximal with respect to a subspace $H_\infty \cong \mathbb{PG}(n-2,2)$. Suppose that for one of the three hyperplanes, L, of Σ containing H_∞ we have $|L \cap S| \geq |S|/2$. Then S is maximal.*

Proof. If $|L \cap S| \geq |S|/2$ then $|L \cap S| \geq 2^{n-2}+1$. Consider $x \in H_\infty$. Since there are 2^{n-2} lines in L passing through x and not contained in H_∞ we see that one of these lines must be a secant of S passing through x. ∎

Given a cap $S \subset \Sigma = \mathbb{PG}(n,2)$ the *doubling* or *Plotkin* construction yields a periodic cap $\widetilde{S} \subset \widetilde{\Sigma} \cong \mathbb{PG}(n+1,2)$ with $|\widetilde{S}| = 2|S|$ as follows. Choose a point $v \in \widetilde{\Sigma} \setminus \Sigma$ to play the role of a vertex. For each point $x \in S$ put $x' = x + v$. Then $\widetilde{S}$ is the cap defined by $\widetilde{S} = \{x' \mid x \in S\} \sqcup S$. It is easy to verify that S is maximal (respectively L-maximal) if and only if $\widetilde{S}$ is also maximal (respectively $\widetilde{L}$-maximal).

LEMMA 3.6 *Let $S \subset \Sigma = \mathbb{PG}(n,2)$ be a periodic set with vertex v. Let L be a hyperplane of Σ not containing v. Then S is the double of $S \cap L$.*

Proof. Consider a point $y \in \Sigma$ and define $y' = v + y$. Since $v \notin L$ exactly one of the two points y, y' lies in L. Furthermore since v is a vertex of S, $y \in S$ if and only if $y' \in S$. ∎

NOTATION 3.7 Let $S \subset \Sigma$ be a large cap. Let $H_\infty \cong \mathbb{PG}(n-2,2)$ be disjoint from S. Denote the three hyperplanes of Σ which contain S by L_A, L_B and L_C. Write $H_A := L_A \setminus H_\infty, H_B := L_B \setminus H_\infty, H_C := L_C \setminus H_\infty, A := S \cap L_A = S \cap H_A, B := S \cap L_B = S \cap H_B$ and $C := S \cap L_C = S \cap H_C$.

THEOREM 3.8 $|A+B| \leq |A| + |B| - 1$. *Furthermore we have equality if and only if S is critical and L_C-maximal.*

Proof. Since S is a cap, $A + B \subset H_C \setminus C$. Therefore

$$\begin{aligned} |A+B| &\leq 2^{n-1} - |C| \\ &= 2^{n-1} - (|S| - |A| - |B|) \\ &\leq 2^{n-1} - (2^{n-1}+1) + |A| + |B| \\ &= |A| + |B| - 1 \end{aligned}$$

with equality if and only if S is critical and $H_C = (A+B) \sqcup C$. ∎

LEMMA 3.9 *Let $S \subset \Sigma$ be a cap which is quasi-maximal with respect to H_∞. Suppose that for one of the three hyperplanes, L, of Σ containing H_∞ the set $S \cap L$ is periodic. Then S is periodic. Furthermore, if v is a vertex for $S \cap L$ then v is also a vertex for S.*

Proof. For ease of notation we assume that $L = L_B$, i.e., $v + B = B$. Thus $v \in H_\infty$. Assume, by way of contradiction, that v is not a vertex for S. Then there exists a point x of

S such that $x' := x + v \notin S$. Clearly $x \notin L_B$ and thus $x' \notin L_B$. Without loss of generality $x \in A$. Since S is maximal, x' lies on a secant of S: say $x' = y + z$ where $y \in B$ and $z \in C$. Therefore $y' := v + y \in B$. But $y' = v + y = v + x' + z = x + z$ and thus the line $\{y', x, z\}$ is fully contained in S, a contradiction. ■

COROLLARY 3.10 *Let S be a critical quasi-maximal cap. Then none of $A + B$, A, B or C is periodic.*

Proof. Since $|S|$ is odd, S cannot be periodic by Lemma 2.3. Thus by Lemma 3.9, none of A, B or C is periodic. Since S is a quasi-maximal cap $C = H_C \setminus (A + B)$. If $(A + B)$ has a vertex v then v is the third point of a line joining two points of $A + B$ and thus $v \in H_\infty$. Then $v + H_C = H_C$ and therefore $v + C = C$ contradicting Lemma 3.9. ■

In [6] the following theorem (there phrased for codes) is proved.

THEOREM 3.11 *Let $S \subset \Sigma = \mathbb{PG}(n, 2)$ be a cap with $|S| \geq 2^{n-1} + 2$. Then there exists a subspace $H_\infty \cong \mathbb{PG}(n - 2, 2)$ of Σ such that $S \cap H_\infty = \emptyset$.*

The following is from [10, 11]:

THEOREM 3.12 *Let X and Y be finite non-empty subsets of an abelian group satisfying $|X + Y| \leq |X| + |Y| - 2$. Then $X + Y$ is periodic.*

In [6] the following two results are also proved.

THEOREM 3.13 *Let $S \subset \Sigma \cong \mathbb{PG}(n, 2)$ be a cap which is quasi-maximal with respect to H_∞. Suppose $|S| \geq 2^{n-1} + 2$. Then S is periodic.*

Proof. By Theorem 3.8 we have $|A + B| \leq |A| + |B| - 2$. Therefore by Theorem 3.12, $A + B$ is periodic. Since S is L_C-maximal, $C = H_C \setminus (A + B)$ and thus C is periodic. Hence by Lemma 3.9, S is periodic. ■

COROLLARY 3.14 *Let $S \subset \Sigma$ be a large maximal cap. Then $|S| = 2^{n-1} + 2^j$ for some $j = 0, 1, \ldots n - 3$ or $n - 1$.*

Proof. This Corollary is easily proved by induction using the previous Theorem. That there are no maximal caps in Σ of cardinality $2^{n-1} + 2^{n-2}$ follows from the fact that there are no maximal caps of cardinality 3 in $\mathbb{PG}(2, 2)$. ■

REMARK 3.15 Since critical maximal caps exist in $\mathbb{PG}(m, 2)$ for all $m \geq 3$ (see Theorem 4.1) the doubling construction provides maximal caps in $\mathbb{PG}(n, 2)$ of cardinality $2^{n-1} + 2^j$ for every $j = 0, 1, \ldots n - 3$. The complement of a hyperplane in Σ provides a maximal cap in $\mathbb{PG}(n, 2)$ of cardinality $2^{n-1} + 2^{n-1} = 2^n$. This last cap may also be thought of as the result of repeated doubling the cap in $\mathbb{PG}(1, 2)$ consisting of 2 points.

Theorem 3.13 shows that the structure of all large (quasi-)maximal caps is determined by the structure of all critical (quasi-)maximal caps.

We will need the following improvement of Theorem 3.11.

THEOREM 3.16 *Let $S \subset \Sigma = \mathbb{PG}(n,2)$ be a large cap. Then there exists a subspace $H_\infty \cong \mathbb{PG}(n-2,2)$ of Σ such that $S \cap H_\infty = \emptyset$.*

Proof. By Theorem 3.11 we may suppose that $|S| = 2^{n-1}+1$. Embed Σ in $\widetilde{\Sigma} \cong \mathbb{PG}(n+1,2)$ and let $v \in \widetilde{\Sigma} \setminus \Sigma$. Construct a cap $\widetilde{S} \subset \widetilde{\Sigma}$ by the doubling construction using v as vertex. Then $|\widetilde{S}| = 2|S| = 2^n + 2$. Therefore by Theorem 3.11, there exists a projective subspace $\widetilde{H_\infty} \cong \mathbb{PG}(n-1,2)$ of $\widetilde{\Sigma}$ with $\widetilde{H_\infty} \cap \widetilde{S} = \emptyset$. Now $\widetilde{H_\infty} \cap \Sigma$ is a subspace isomorphic to either $\mathbb{PG}(n-1,2)$ or $\mathbb{PG}(n-2,2)$ which is disjoint from S which completes the proof. ∎

4. Critical Maximal Caps With Tangent Hyperplanes

Here we describe a simple construction of some critical maximal caps. We begin with $\Sigma = \mathbb{PG}(n,2)$ and a fixed subspace $H_\infty \cong \mathbb{PG}(n-2,2)$. As in 3.7 there are three hyperplanes L_A, L_B and L_C of Σ which contain H_∞. Write $H_A := L_A \setminus H_\infty$, $H_B := L_B \setminus H_\infty$ and $H_C := L_C \setminus H_\infty$.

We construct a maximal cap S in $\mathbb{PG}(n,2)$ of size $2^{n-1}+1$ which is disjoint from H_∞. Choose a point $s_0 \in H_C$. Next choose $B := \{s_1, \ldots, s_b\} \subset H_B$ where $1 \le b \le 2^{n-1}-1$. Put $t_i := s_0 + s_i$, the third point of the (cross-)line joining s_0 and s_i for $1 \le i \le b$. Finally we let $A := \{s_{b+1}, \ldots, s_{2^{n-1}}\} = H_A \setminus \{t_1, \ldots, t_b\}$ and define $S = \{s_0, \ldots, s_{2^{n-1}}\}$.

THEOREM 4.1 *The cap S so-constructed is a critical cap. Furthermore*

(1) every point not in L_C lies on a secant to S through s_0;

(2) if $b \neq 2^{n-2}$ then in addition every point of H_∞ lies on a secant to S;

(3) if b is odd then S is a maximal cap.

Proof. It is clear that S is a cap of size $2^{n-1}+1$. To see (1) let $x \in H_A$ with $x \notin S$. Then $x = t_i$ for some i and thus x lies on the secant to S joining s_0 to s_i. Similarly, all points of H_B not in S lie on a secant to S through s_0.

For (2), suppose that $b \neq 2^{n-2}$. Using the symmetry between the roles of A and B we may assume that $|H_A \cap S| =: a \ge b = |H_B \cap S|$. Since $b \neq 2^{n-2}$ this implies that there are at least $2^{n-1}+1$ points of S in H_A. There are $2^{n-1}-1$ lines in L_A passing through a point x of H_∞. Of these, $2^{n-2}-1$ are in H_∞ and each of the remaining 2^{n-2} lines contains 2 points of H_A. Thus at least one of these 2^{n-2} lines of L_A not contained in H_∞ and passing through x is a secant to S.

Finally we prove (3). Suppose that S is not maximal. By (1) and (2) this implies that there exists $x \in H_C$ with $x \neq s_0$ such that $x \notin A + B$. Put $A' = H_A \setminus A$ and $v = x + s_0 \in H_\infty$. Then $x + B = A'$ and $s_0 + B = A'$. Therefore $v + B = x + s_0 + B = x + A' = B$. Therefore B is periodic with (non-zero) vertex v. Hence applying Lemma 2.3, we see that if S is not maximal then b must be even. ∎

REMARK 4.2 Note that the above proof actually shows that if the set B (or A) is not periodic and $b \neq 2^{n-2}$ (or $a \neq 2^{n-2}$) then the cap S is maximal.

REMARK 4.3 In the above theorem, if b does equal 2^{n-2} then the cap S need not be maximal. See Theorem 7.4.

DEFINITION 4.4 A hyperplane L such that $|S \cap L| = 1$ is called a *tangent hyperplane* for S.

Observe that L_C is a tangent hyperplane to the cap S constructed in the above manner.

5. Applications and Extensions to Arbitrary Codes

Let U denote an arbitrary binary code, linear or otherwise, of length t. In other words, U is a collection of binary t-tuples. Denote by U' the set of all t-tuples not in U. Our main result is as follows.

THEOREM 5.1 *Assume that $|U|$ is odd. Then every t-tuple apart from the all zero t-tuple is expressible as the binary sum of an element in U and an element in U'. In particular, $|U + U'| = 2^t - 1$.*

Proof. The result is clear if $t = 1$. Assume $t \geq 2$. Changing notation, let $t = n - 1$ and put $\Sigma = \mathbb{PG}(n, 2)$. Each point of Σ has homogeneous coordinates $(x_0 : x_1 : \ldots : x_n)$. Let H_∞ denote the $n - 2$ dimensional subspace with equations $x_0 = x_1 = 0$. The three hyperplanes containing H_∞ are L_A, L_B and L_C with equations $x_0 + x_1 = 0$, $x_0 = 0$ and $x_1 = 0$ respectively. Let s_0 in L_C have coordinates $(1 : 0 : \ldots : 0)$. Denote by A the set of all points in L_A with coordinates $(1 : 1 : u_1 : \ldots : u_t)$ with $(u_1, \ldots, u_t) \in U$. Denote by B the set of points in L_B with coordinates $(0 : 1 : b_1 : \ldots : b_t)$ where $(b_1, \ldots, b_t) \in U'$. Then $S = \{s_0\} \sqcup A \sqcup B$ is a cap of cardinality $2^{n-1} + 1$. By Theorem 4.1 (3) S is maximal. Now let $(w_1, \ldots, w_t)$ be any non-zero t-tuple and form the point $z = (1, 1, w_1, \ldots, w_t)$ in $L_C \setminus H_\infty$. Since $z \neq s_0$ and S is a maximal cap it follows that z is expressible as the sum of 2 points in S. Thus $z = (1 : 0 : w_1 : \ldots : w_t) = (1 : 1 : u_1 : \ldots : u_t) + (0 : 1 : b_1 : \ldots : b_t)$. This gives $(w_1, \ldots, w_t) = (u_1, \ldots, u_t) + (b_1, \ldots, b_t)$ proving the result. ∎

6. Some Combinatorial Applications

Let X be a set of cardinality $n+1$. Then any subset of X is indicated by a binary $(n+1)$-tuple in the usual way. For example if $X = \{1, 2, 3, 4, 5\}$ and $Y = \{2, 4\}$ then Y is represented by $(0, 1, 0, 1, 0)$. Then many of the results of this paper can be applied to the combinatorial situation. For example Corollary 3.14 can be rephrased as follows.

THEOREM 6.1 *Let $\mathcal{F}$ be a family of non-empty subsets of X which is maximal with respect to the property that no subset in $\mathcal{F}$ is equal to the symmetric difference of two other subsets of $\mathcal{F}$. Assume that $|\mathcal{F}| > 2^{n-1}$. Then $|\mathcal{F}| = 2^{n-1} + 2^i$ where $i = 0, 1, \ldots, n-3$ or $n-1$.*

Similarly, Theorem 5.1 can be rephrased as follows.

THEOREM 6.2 *Let U be a family of subsets of $X = \{1, 2, \ldots, t\}$. Assume that the cardinality of U is odd. Denote by U' the family consisting of those subsets of X not in U. Then every non-empty subset of X is expressible as the symmetric difference of some set in U with some set in U'.*

7. Non-maximal Quasi-maximal Caps

We want to return to Theorem 4.1 (see also Remark 4.3) by showing that when $b = |B| = 2^{n-2}$ then the cap S may be maximal or not.

NOTATION 7.1 Let U and W denote sets of binary t-tuples. Then $U \oplus W = \{a_1 + a_2 \mid a_1 \in U, a_2 \in W \text{ and } a_1 \neq a_2\}$.

Let U_r denote the set of all the binary t-tuples which contain exactly r ones and $t - r$ zeroes. The following Lemma is easily proved.

LEMMA 7.2 *Let $r \geq s$. $U_r \oplus U_s = U_{r-s} \sqcup U_{r-s+2} \sqcup U_{r-s+4} \sqcup \ldots \sqcup U_f$ where $f = r + s$ if $r + s \leq t$ and $f = 2t - r - s$ if $r + s \geq t$.*

Using Lemma 7.2 it is easy to construct sets W (of the form $W = U_{r_1} \sqcup \ldots \sqcup U_{r_m}$) such that $W \oplus W$ is the set of all non-zero t-tuples and $|W| \leq 2^{t-1}$ for any $t \geq 4$. Choose such a set W. Arbitrarily add more t-tuples to obtain a set U with $|U| = 2^{t-1}$. Let U' denote the set of all t-tuples not contained in U. Define $A = \{(1 : 1 : a_1 : \ldots : a_t) \mid (a_1, \ldots, a_t) \in U\}$, $B = \{(0 : 1 : b_1 : \ldots : b_t) \mid (b_1, \ldots, b_t) \in U'\}$, $C = \{s_0 = (1 : 0 : 0 : \ldots : 0)\}$ and $S = (A \sqcup B \sqcup C) \subset \Sigma = \mathbb{PG}(t + 1, 2) = \mathbb{PG}(n, 2)$.

LEMMA 7.3 *The cap S of $\Sigma = \mathbb{PG}(n, 2)$ constructed above is a critical maximal cap with $|A| = |B| = 2^{n-2}$.*

Proof. By construction S is critical with $|A| = |B| = 2^{n-2}$. Note that this construction is a special case of that used in Section 4. By Theorem 4.1 (1) every point not in the hyperplane L_C defined by the equation $x_1 = 0$ lies on a secant to S. By construction, $A + B = H_C \setminus \{s_0\}$ and thus S is quasi-maximal. To see that there is no point of H_∞ which could extend use the fact that $A \oplus A = H_\infty$ by the definition of W. Thus S is maximal. ∎

Next we can use this same cap S to construct a quasi-maximal cap which is not maximal in $\widetilde{\Sigma} = \mathbb{PG}(t + 2, 2)$. In fact any critical maximal cap in $\mathbb{PG}(n, 2)$ with $|A| = |B| = 2^{n-2}$ will suffice. Apply the doubling construction, with respect to the vertex $v = (1 : 0 : \ldots : 0 : 1) \in \widetilde{\Sigma} \setminus \Sigma$ to the cap S to construct a new maximal cap $\widetilde{S} \subset \widetilde{\Sigma}$ with $|\widetilde{S}| = 2|S| = 2^{t+1} + 2$. Define $\widetilde{S}^\circ := \widetilde{S} \setminus \{z\}$ where $z = v + s_0 = (1 : 0 : \ldots : 0 : 0)\}$ so that $\widetilde{S}^\circ$ is a critical cap in $\widetilde{\Sigma}$. Let $\widetilde{L_A}$ denote the hyperplane of $\widetilde{\Sigma}$ obtained by doubling L_A with respect to v. Similarly define $\widetilde{L_B}$, $\widetilde{A} = \widetilde{S} \cap \widetilde{L_A}$, $\widetilde{H_\infty} = \{0 : 0 : a_1 : \ldots : a_{t+1})\}$, etc. Using this notation we have:

THEOREM 7.4 *(1) $\widetilde{S}^\circ$ is a quasi-maximal cap which is not maximal.*

(2) Every quasi-maximal cap which is not maximal is obtained in this way.

Proof. Clearly $\widetilde{S}^\circ$ is non-maximal since it may be extended by z. Furthermore, as in the proof of Theorem 4.1 (1) every point of $\widetilde{\Sigma}$ not lying in $\widetilde{L_C}$ lies on a secant to $\widetilde{S}^\circ$ passing through s_0. Assume by way of contradiction that there exists a point z' of H_C not on any secant to $\widetilde{S}^\circ$. Now z' does lie on a secant to $\widetilde{S}$ since $\widetilde{S}$ is a maximal cap. Thus this secant to

$\widetilde{S}$ must pass through z and another point of $\widetilde{S} \cap \widetilde{L_C}$. But $\widetilde{S} \cap \widetilde{L_C} = \{s_0\}$ which implies that $z' = s_0 + z = v$. But this is absurd since the vertex v lies on 2^t secants to $\widetilde{S}^\circ$. Therefore $\widetilde{S}^\circ$ is quasi-maximal but not maximal.

For the proof of (2) see Proposition 11.17. ■

8. Swiss Caps

Let L be a hyperplane of $\Sigma = \mathbb{PG}(n, 2)$ and let S be a critical cap in Σ disjoint from L. It then follows, as in the proof of Theorem 3.1 that each point of L lies on at least one secant of S. Note also that by Corollary 3.2 (1) that L is the only hyperplane of Σ disjoint from S.

DEFINITION 8.1 The critical cap S is said to be a *Swiss* cap if there exists a point z of L lying on exactly one secant line Λ to S. We sometimes say that S is a Swiss cap with respect to (L, Λ, z).

Let S in $\Sigma = \mathbb{PG}(n, 2)$ be a Swiss cap with respect to some (L, Λ, z). There are $2^{n-1} - 1$ points of S not in Λ and lying in $\Sigma \setminus L$. Consider the $2^{n-1} - 1$ lines of Σ passing through z which are not contained in L and which are different from Λ. Since Λ is the only secant of S through z, each of these lines must contain exactly one point of S. Thus for $w \notin \Lambda$ we have $w \notin S$ if and only if $w + z \in S$.

The above paragraph shows how to construct Swiss caps. Having fixed L, Λ and z, for each of the $2^{n-1} - 1$ lines $\{z, w, z + w\} \neq \Lambda$ which are not contained in L we include in S exactly one of w or $z + w$. The remaining two points of S are just $\Lambda \setminus \{z\}$.

Now we show that the assumption of a the existence of a special point z for S is essential (except in small dimensions).

THEOREM 8.2 *Let S be a critical cap in $\Sigma = \mathbb{PG}(n, 2)$ disjoint from a hyperplane L of Σ. Then there may or may not be a point of L lying on exactly one secant of S.*

Proof. Let us sketch a proof. Working in $\mathbb{PG}(4, 2)$ we make use of the cap $T = \{(1 : 0 : 0 : 0 : 0), (1 : 1 : 0 : 0 : 0), (1 : 0 : 1 : 0 : 0), (1 : 0 : 0 : 1 : 0), (1 : 0 : 0 : 0 : 1), (1 : 1 : 1 : 1 : 1)\}$. Here we are using homogeneous coordinates x_0, x_1, x_2, x_3, x_4. Let L be the hyperplane defined by $x_0 = 0$. Then it is easy to check that each point of L lies on exactly one secant to T. Doubling we obtain, $\widetilde{L}$ and $\widetilde{T}$ in $\mathbb{PG}(5, 2)$. Here $\widetilde{T}$ is a cap of size 12 and $\widetilde{L}$ is a hyperplane. Moreover each point of $\widetilde{L}$ lies on exactly 2 secants of $\widetilde{T}$. Adjoin, any 5 points not in $\widetilde{L}$ to $\widetilde{T}$. This gives a cap S with $|S| = 17$, disjoint from the hyperplane $\widetilde{L}$. Moreover every point of $\widetilde{L}$ lies on at least 2 secants to S. Thus S is not a Swiss cap even though S is critical and disjoint from a hyperplane. Similar arguments, using for example Lemma 7.2, will apply in $\mathbb{PG}(n, 2)$ for $n \geq 6$. ■

9. Fractal Caps

In this section we describe a method to construct certain critical maximal caps in $\Sigma \cong \mathbb{PG}(n, 2)$ where $n \geq 4$. We call these caps *fractal caps*. We begin with some notation which will be maintained throughout the remainder of the paper.

NOTATION 9.1 Given a large cap in $\Sigma = \mathbb{PG}(n,2)$ there exists a projective subspace $H_\infty \cong \mathbb{PG}(n-2,2)$ which contains no points of S by Theorem 3.16. There are three hyperplanes of Σ which contain H_∞. As before we denote them by L_A, L_B and L_C. We also write $H_A = L_A \setminus H_\infty$, $H_B = L_B \setminus H_\infty$ and $H_C = L_C \setminus H_\infty$.

We want to apply results from the paper [9] which is concerned with abelian groups. We regard $\Sigma = \mathbb{PG}(n,2)$ as obtained from the vector space $V(n+1,2)$ which is in particular an abelian group G of cardinality 2^{n+1}. The points of Σ are in one-to-one correspondence with the non-zero elements of G as described in Section 2.

Let F be a subgroup of $V(n+1,2)$ with $|F| = 2^{k+1}$ where $1 \le k \le n-3$. F gives rise to a projective subspace of Σ, $F_\infty \cong \mathbb{PG}(k,2)$. Let $F+a$ be a coset of F. If $F_\infty \subset H_\infty$ and $a \notin H_\infty$ then $F+a$ is a set of points lying outside H_∞. Moreover, $(F+a) \cup F_\infty$ is a projective subspace of Σ of projective dimension $k+1$. By abuse of notation we will often use the same symbol to denote both this projective subspace and the coset $F+a$.

If $F_\infty \subset H_\infty$ we often make us of the quotient geometry $\overline{\Sigma}$ of Σ with respect to F_∞. Thus $\overline{\Sigma} \cong \mathbb{PG}(u,2)$ (where $u = n-k-1$) is just the projective space associated to the quotient group $V(n+1,2)/F$. The quotient map $\sigma_F = \sigma : V(n+1,2) \to V(n+1,2)/F$ induces a map also called σ_F (or more simply σ) from $\Sigma \to \overline{\Sigma}$. We will also denote this map using overbars; thus $\overline{H_\infty}$ denotes $\sigma_F(H_\infty)$.

Now we proceed to explain the construction of fractal caps. The ingredients are $F_\infty \cong \mathbb{PG}(k,2) \subset H_\infty$ as above, a Swiss cap $\widehat{S}$ in the quotient geometry $\overline{\Sigma}$ and a critical cap T in $\Lambda = \mathbb{PG}(k+2,2)$.

We suppose our Swiss cap $\widehat{S}$ in $\overline{\Sigma}$ is a Swiss cap with respect to $(\overline{L_C}, \overline{\Lambda}, \overline{Z})$ where $\overline{Z} \notin \overline{H_\infty}$. Write $\overline{\Lambda} = \{\overline{X}, \overline{Y}, \overline{Z}\}$. Observe that by definition $\overline{Z}$ is *not* a point of $\widehat{S}$ but $\overline{X}$ and $\overline{Y}$ are in $\widehat{S}$. Let $\overline{v_1}, \ldots, \overline{v_{2^{u-1}-1}}$ be the other points of $\widehat{S}$. Now without loss of generality $\overline{X} \in \overline{L_A}$, $\overline{Y} \in \overline{L_B}$ and $\overline{Z} \in \overline{L_C}$. Lift $\overline{X}$ (respectively $\overline{Y}$, $\overline{Z}$, $\overline{v_i}$) to a $k+1$ dimensional projective space X (respectively Y, Z, v_i) of Σ containing F_∞. Also denote $X \cup Y \cup Z$ by Λ. Thus $\Lambda \cong \mathbb{PG}(k+2,2)$. Define $\pi_i = (v_i \setminus F_\infty) \cong \mathbb{AG}(k+1,2)$. In Λ we have our critical maximal cap T. Thus $|T| = 2^{k+1}+1$. We define

$$S = T \bigsqcup \left(\bigsqcup_{i=1}^{2^{u-1}-1} \pi_i \right).$$

In what follows, we note that the only points of S lying in the hyperplane L_C are the points of T that lie in Z. To further elucidate our notation, notice that the image under σ of the cap S in $\overline{\Sigma}$ is not $\widehat{S}$. Rather the set $\overline{S} = \widehat{S} \sqcup \overline{Z}$ is not a cap but consists of the cap $\widehat{S}$ together with one additional point.

DEFINITION 9.2 The three cosets X, Y and Z of F are called the *improper (F-)cosets*.

THEOREM 9.3 *S is a cap of size $2^{n-1}+1$.*

Proof. $|S| = |T| + (2^{u-1}-1)|\pi_i| = 2^{k+1}+1+(2^{u-1}-1)2^{k+1} = 2^{k+u}+1 = 2^{n-1}+1$, since $u = n-k-1$.

To see that S is a cap we assume, by way of contradiction, that S contains a line m. Since $S \cap H_\infty = \emptyset$, the line m must contain exactly one point w_1 of A, one point w_2 of B and

one point w_3 of C. As we observed above the point w_3 must lie in T. If m is contained in Λ then $m \subset S \cap \Lambda = T$ contradicting the fact that T is a cap. Thus $m \cap \Lambda = \{w_3\}$. Therefore there exist i and j such that $w_1 \in \pi_i$ and $w_2 \in \pi_j$. Thus $\overline{v_i} + \overline{v_j}$ is a point of $\overline{L_C}$ which in fact is different from $\overline{Z}$ since $\widehat{S}$ is a Swiss cap with respect to $(\overline{L_C}, \overline{\Lambda}, \overline{Z})$. Hence $w_3 = w_1 + w_2 \in L_C \setminus \Lambda$ and this contradiction proves the theorem. ∎

DEFINITION 9.4 The cap S of Theorem 9.3 is called a *fractal cap*.

THEOREM 9.5 *S is a maximal (quasi-maximal) cap in Σ if and only if T is a maximal (quasi-maximal) cap in Λ.*

Proof. It is easy to see, by considering points of Λ that if S is maximal then T must be maximal.

Suppose now that T is maximal. Let w be some point of Σ with $w \notin S$. We must show that w lies on some secant to S. This is clear if $w \in \Lambda$ by the maximality of the cap T. Henceforth we assume that $w \notin \Lambda$.

Since T is a critical maximal cap in $\Lambda \cong \mathbb{PG}(k+2, 2)$, it meets every hyperplane of Λ by Corollary 3.2 (2). In particular, $T \cap X \neq \emptyset$, $T \cap Y \neq \emptyset$ and $T \cap Z \neq \emptyset$. We use this below.

Suppose first, that $w \in L_C \setminus H_\infty$. Let $\overline{w}$ denote the point in $\overline{\Sigma}$ which is the image of the subspace W of Σ generated by w and F_∞. Since $w \notin \Lambda$, $\overline{w} \notin \overline{\Lambda}$ and thus $\overline{w} \neq \overline{Z}$. Furthermore, $w \notin S$ implies that $\overline{w} \notin \widehat{S}$. Since $\widehat{S}$ is a Swiss cap, there is a secant line $\overline{\ell}$ to $\widehat{S}$ different from Λ passing through $\overline{w}$. At least one of the two other points of $\overline{\ell}$ is not a point of $\overline{\Lambda}$ and is therefore equal to some $\overline{v_i}$. Lifting $\overline{\ell}$ we obtain a pencil of subspaces containing F_∞ namely W, v_i and a third subspace U. Either $U = X$ or $U = Y$ or else $U = v_j$ for some j. In either event $U \cap S \neq \emptyset$. Recall that all points of $\pi_i = v_i \setminus F_\infty$ are contained in S. We conclude that w lies on a secant line to S.

Next, suppose that $w \in (L_A \cup L_B) \setminus H_\infty$. Without loss of generality we may assume that $w \in L_A \setminus H_\infty$. Let $\overline{w}$ denote the point in $\overline{\Sigma}$ which is the image of the subspace of Σ, W, generated by w and F_∞. Since $w \notin \Lambda$, $\overline{w} \notin \overline{\Lambda}$ and thus $\overline{w} \neq \overline{Y}$. Furthermore, $w \notin S$ implies that $\overline{w} \notin \widehat{S}$ and thus there is a cross-line different from Λ, say $\{\overline{w}, \overline{Z}, \overline{v_i}\}$, passing through $\overline{w}$ and $\overline{Z}$. Lifting this secant line to Σ we obtain a pencil of subspaces $\{W, Z, v_i\}$ on F_∞ with $w \in W$. As in the previous case we find the desired secant line to S through w.

We have now shown that S is quasi-maximal. To show the maximality of S we consider the case where $w \in H_\infty$. Without loss of generality $|\widehat{S} \cap \overline{L_A}| \geq |\widehat{S} \cap \overline{L_B}|$ and thus $\widehat{S} \cap \overline{L_A}$ is a set of size at least $2^{u-2} + 1$; one of these points is $\overline{X}$. Therefore $|S \cap L_A| \geq (2^{k+1})(2^{u-2}) + 1 = 2^{n-2} + 1$ since $|S \cap X| \geq 1$. By an easy counting argument as in the proof of Lemma 3.5 we see that S is maximal.

Similar arguments apply for the quasi-maximal case. ∎

REMARK 9.6 The construction of fractal caps is somewhat subtle. In the construction it is essential that $k \leq n - 3$. For, let S be *any* large cap in $\Sigma = \mathbb{PG}(n, 2)$ with S not equal to $\mathbb{AG}(n, 2)$ and let H_∞ be an $n - 2$ dimensional projective subspace disjoint from S. Then by taking the quotient with respect to H_∞ we obtain a projective line and a Swiss

cap. Summing up, if we do not require that $k \leq n-3$ then *every* large cap different from $\mathbb{AG}(n,2)$ can be regarded as a fractal cap.

REMARK 9.7 In the construction of the fractal cap S it is not necessary that the cap T be critical. Indeed if T is any maximal cap in Λ then S is a maximal cap in Σ with $|S| = 2^{n-1} + |T| - 2^{k+1}$. In particular, S is a large cap in Σ if and only if T is a large cap in Λ. Hence we may also use the fractal construction to construct new non-large caps from old ones.

10. Critical Maximal Caps Having No Tangent Hyperplane

It is easy to see how to construct a maximal fractal cap which has a tangent hyperplane. In this section we show how to construct a maximal fractal cap which has no tangent hyperplanes. We maintain the notation of the previous section. Further we assume, without loss of generality that $|\widehat{S} \cap \overline{L_A}| \geq |\widehat{S} \cap \overline{L_B}|$. Thus $|\widehat{S} \cap \overline{L_A}| \geq 2^{u-2}+1$. In order to guarantee that S has no tangent hyperplanes it suffices to ensure that the choices of $\widehat{S}$ and T satisfy each of the following three conditions:

THEOREM 10.1 *Let S be constructed by the method of the previous section. Further suppose that*

(1) $|T \cap Z| > 1$,

(2) either $|T \cap X| > 1$ *or* $|\widehat{S} \cap \overline{L_A}| \neq 2^{u-2}+1$,

(3) either $|T \cap Y| > 1$ *or* $|\widehat{S} \cap \overline{L_B}| > 1$.

Then for every hyperplane M of Σ we have $|M \cap S| > 1$.

Proof. Let M be a hyperplane of Σ. If $M = L_C$ then condition (1) guarantees that $|L_C \cap S| > 1$. For $M = L_B$ we have that $|L_B \cap S| = 2^{k+1}(|\widehat{S} \cap \overline{L_B}| - 1) + |T \cap Y|$. Now $\widehat{S} \cap \overline{L_B}$ contains $\overline{Y}$ and thus $|\widehat{S} \cap \overline{L_B}| \geq 1$. Then condition (3) implies $|L_B \cap S| > 1$. If $M = L_A$ we have $|M \cap S| > 1$ since $|\widehat{S} \cap \overline{L_A}| \geq |\widehat{S} \cap \overline{L_B}|$.

Thus we may suppose that M does not contain H_∞. Since $\widehat{S}$ is a critical cap in $\overline{\Sigma} = \mathbb{PG}(u,2)$ we have that $|\widehat{S} \cap \overline{L_A}| + |\widehat{S} \cap \overline{L_B}| = 2^{u-1}+1$. By assumption $|\widehat{S} \cap \overline{L_A}| \geq |\widehat{S} \cap \overline{L_B}|$. Therefore $|\widehat{S} \cap \overline{L_A}| > 2^{u-2}$. Using (2) it follows that $|S \cap L_A| = 2^{k+1}(|\widehat{S} \cap \overline{L_A}| - 1) + |T \cap X| > 2^{k+1}(2^{u-2}) + 1 = 2^{n-2}+1$. There are three hyperplanes of L_A which contain $M \cap H_\infty$: $L_A \cap M$, H_∞ and a third, say J. Any points of S lying in J are outside of $J \cap H_\infty$ and this implies that J can contain at most 2^{n-2} points of S. Since there are no points of S in H_∞ and $|S \cap L_a| > 2^{n-2}+1$, we see that $M \cap L_A$ must contain more than 1 point of S. ∎

COROLLARY 10.2 *Let $\Sigma = \mathbb{PG}(n,2)$.*

(1) If $n \leq 5$ then all critical maximal caps in Σ have a tangent hyperplane.

(2) If $n \geq 6$ then there exist critical maximal caps in Σ having no tangent hyperplane.

Proof. Part (1) is shown in [6]. Part (2) will follow from Theorem 10.1. ∎

11. Uniqueness

We introduce some definitions from [9].

Let X and Y be *non-empty* finite subsets of an abelian group, G.

DEFINITION 11.1 If $g \in G$ then $\nu_g(X, Y)$ denotes the number of representations of g as $g = x + y$ where $x \in X$ and $y \in Y$. For an arbitrary subset C of G, $H(C)$ will denote the subgroup $H(C) := \{g \in G \mid C + g = C\}$.

DEFINITION 11.2 We say that C is *periodic* if $H(C) \neq \{\mathbf{0}\}$.

DEFINITION 11.3 $P_1(X, Y)$ denotes the (possibly empty) collection of pairs (F, D) such that

(1) F is a finite subgroup of G with $|F| \geq 2$;

(2) D is a proper non-empty subset of $X + Y$ contained in some F-coset; moreover, $(X + Y) \setminus D$ is a union of one or more F-cosets;

(3) if $X + Y$ is periodic then $D = F + d$ is an F-coset where $\nu_d(X, Y) = 1$;

(4) $\sigma(D)$ has exactly one representation $\sigma(D) = \overline{x} + \overline{y}$ where $\overline{x} \in \sigma(X)$ and $\overline{y} \in \sigma(Y)$ where $\sigma : G \to G/F$ is the quotient map.

REMARK 11.4 In terms of previous notation, condition (4) says that $\nu_{\sigma(D)}(\sigma(X), \sigma(Y)) = 1$.

Let S be a critical cap in $\Sigma = \mathbb{PG}(n, 2)$. Let H_∞ be some $n - 2$ dimensional subspace of Σ disjoint from S, —the existence of which is guaranteed by Theorem 3.16. As in 3.7 there arises sets A, B and C with $A = S \cap L_A$, $B = S \cap L_B$ and $C = S \cap L_C$.

In order to apply results from the paper [9] we remind the reader that, as explained in Section 2, the points of $\Sigma = \mathbb{PG}(n, 2)$ are the non-zero elements of the elementary abelian group $G = V(n + 1, 2)$ of cardinality 2^{n+1}.

DEFINITION 11.5 Suppose there exist H_∞, A, B and C such that S is L_C-maximal and $P_1(A, B)$ is non-empty then we say that S is P_1-*decomposable* (with respect to H_∞). If there exists a set D and a subgroup F with $(F, D) \in P_1(A, B)$ we will say that F is a P_1-*decomposing subgroup* for S.

REMARK 11.6 The above definition implies the existence of three F-cosets: $U = \sigma^{-1}(\overline{x})$, $V = \sigma^{-1}(\overline{y})$ and $W = \sigma^{-1}(\sigma(D))$. We will refer to U, V and W as the *improper* F-cosets.

For emphasis we now state the following lemma which is used repeatedly in the sequel.

LEMMA 11.7 *Assume $\mathbb{PG}(F) \subset H_\infty$ with $|F| = 2^f$. Suppose that S is a critical L_C-maximal cap which has F as a P_1-decomposing subgroup. Then $|S \cap U| + |S \cap V| + |S \cap W| = 2^f + 1$.*

Proof. This follows from [9, Lemma 4.4]: see the discussion immediately following Lemma 11.12. ∎

We remark that a fractal cap is P_1-decomposable with the subgroup consisting of $F = F_\infty \cup \{\mathbf{0}\}$ as a decomposing subgroup since $A + B$ cannot be periodic by Corollary 3.10.

In [9], a subset X of G is said to be in *arithmetic progression* if X is of the form $X = \{x_0 + jz \mid j = 0, 1, \ldots, |X| - 1\}$. The element z is called *difference* of X. In the case where $G = V(n+1, 2)$, every element z of G satisfies $2z = \mathbf{0}$. Thus, if X is in arithmetic progression we have $|X| \leq 2$. In [9] the author considers pairs (X, Y) satisfying the following condition: X and Y are in arithmetic progression with a common difference d where d is of order at least $|X| + |Y| - 1$ (see condition (II) [9, pg. 78]). In our case this implies that $|X| + |Y| - 1 \leq 2$ which implies that either $|X| = 1$ or $|Y| = 1$. This reduces then to condition (I) in [9, pg. 78].

The definition of an *elementary pair* is given in [9, pg. 78] where it is shown that if (X, Y) is an elementary pair then $|X + Y| = |X| + |Y| - 1$. Specializing the definition to the case where $G = V(n+1, 2)$ and using the above remarks we obtain the following definition.

DEFINITION 11.8 Let X and Y be non-empty subsets of $G = V(n+1, 2)$. Then (X, Y) is an *elementary pair* if at least one of the following three conditions holds:

(i) Either $|X| = 1$ or $|Y| = 1$.

(ii) For some non-trivial subgroup F of G, each of X, Y is contained in an F-coset while $|X| + |Y| = |F| + 1$ (hence $X + Y$ is itself an F-coset). Moreover, precisely *one* element g of G satisfies $\nu_g(X, Y) = 1$.

(iii) X is not periodic. Further for some non-trivial subgroup F of G, X is contained in an F-coset while Y is of the form $Y = g_0 + ((a + F) \setminus A)$ for some $a \in X$. (Here $X + Y$ is obtained from an F-coset by deleting a single element from that coset.) Moreover *no* element g of G satisfies $\nu_g(X, Y) = 1$.

REMARK 11.9 Let us clarify these latter two conditions. Write $F = \{f_1, \ldots, f_\ell\}$ and $X = \{a + f_1, \ldots, a + f_s\}$ where $2 \leq s \leq \ell - 2$. Define t by $s - t = |(a + X) \cap (b + Y)|$. Since $|X| + |Y| = |X + Y| + 1$ we may then write $Y = \{b + f_{t+1}, \ldots, b + f_{\ell+t-s}\}$ where $g_0 = a + b$ and $s \geq t$.

The second sentence in condition (iii) implies the following: If $t \leq s-1$ then $g_0 + a + f_s \in Y$ and thus $a + f_s \in (A + F)$ A contradicting the fact that $a + f_s \in A$. Thus we conclude that we must have $Y = \{b + f_{s+1}, \ldots, b + f_\ell\}$.

Next consider condition (ii). Since $X \subseteq a + F$ and $Y \subseteq b + F$, we have $X + Y = (x + y) + F$. Relabelling if necessary we may take $x + y = g$ as the (unique) element satisfying $\nu_g(X, Y) = 1$. Then $x + y = (x + f_s) + (y + f_s)$ is the unique decomposition of $x + y$. But if $t \leq s-2$ then we also have the decomposition $x + y = (x + f_{s-1}) + (y + f_{s-1})$. This contradiction shows that $s - t = 1$ and thus $Y = \{b + f_s, \ldots, b + f_\ell\}$.

The following is Lemma 5.2 of [9] specialized to our situation.

THEOREM 11.10 *Let X and Y be non-empty subsets of $V(n+1, 2)$. Suppose that $|X + Y| = |X| + |Y| - 1$ and that if $X + Y$ is periodic then there exists at least one g such that $\nu_g(X, Y) = 1$. Then either (X, Y) is an elementary pair or $P_1(X, Y)$ is non-empty.*

As before, we identify points of Σ with non-zero vectors in $V(n+1, 2)$. In particular, the subgroup F of G corresponds to a projective subspace of Σ denoted by $\mathbb{PG}(F) \cong \mathbb{PG}(k, 2)$.

Let us recall the notation and definitions of Section 3. In $\Sigma = \mathbb{PG}(n, 2)$, let S be a critical cap which is disjoint from H_∞. Let L_A, L_B and L_C be the three hyperplanes of Σ which contain H_∞. Also put $H_A = L_A \setminus H_\infty$, $H_B = L_B \setminus H_\infty$ and $H_C = L_C \setminus H_\infty$. Now take $A = S \cap L_A = S \cap H_A$, $B = S \cap L_B = S \cap H_B$ and $C = S \cap L_C = S \cap H_C$.

Suppose S is a critical L_C-maximal cap which is P_1-decomposable with respect to H_∞. Then there exists a subgroup $F \neq \{\mathbf{0}\}$ such that $A + B = D' \sqcup D$ where $D' = (F + d_1) \sqcup \ldots \sqcup (F + d_r)$, $r \geq 1$, $D \subset (F + d_0)$ and $\sigma(D)$ has exactly one representation $\sigma(D) = \overline{a_0} + \overline{b_0}$ where $\overline{a_0} \in \sigma(A)$ and $\overline{b_0} \in \sigma(B)$ where $\sigma\colon G \to G/F$ is the quotient map. In other words, $A + B$ is a union of r complete F-cosets together with a subset D of an F-coset and a_0, b_0 and d_0 represent the three improper cosets.

Using this notation, suppose F is any is a subgroup of $V(n+1, 2)$ with $|F| = 2^{k+1}$ with $0 \leq k \leq n-3$. Assume further that $\mathbb{PG}(F) \subset H_\infty$. Let $\overline{\Sigma}$ denote the quotient geometry of Σ with respect to $\mathbb{PG}(F)$. Thus $\overline{\Sigma} \cong \mathbb{PG}(u, 2)$ where $u = n - k - 1$.

DEFINITION 11.11 $\widehat{S}$ is the cap in $\overline{\Sigma}$ defined as follows.

$$\widehat{S} = (\sigma(A) \sqcup \sigma(B) \sqcup \sigma(C)) \setminus \sigma(a_0 + b_0)$$

Applying Theorem 3.8 we have that $|A + B| = |A| + |B| - 1$. Moreover, either by [9, Lemma 4.4] or by an elementary argument we have that $|\overline{A}| + |\overline{B}| = |\overline{A} + \overline{B}| + 1$.

Let us further suppose that S is quasi-maximal and consider an F-coset, $F + a$ which is contained in H_A and which is different from the improper coset $F + a_0$. Suppose that $F + a$ is not fully contained in S. Then there exists a point $f_1 + a \in (F + a) \setminus S$. Since S is quasi-maximal there exist two points $f_2 + b \in H_B \cap S$ and $f_3 + c \in H_C \cap S$ such that $f_1 + a = (f_2 + b) + (f_3 + c)$. By the uniqueness of the decomposition of $\sigma(d_0)$ we must have $\sigma(d_0) \neq \sigma(c)$. Therefore $F + c$ is fully contained in S. Since $(f_2 + b) + (F + c) = F + a$ we see that $F + a$ is disjoint from S. Thus we see that every F-coset in H_A, other than the improper coset is either disjoint from S or fully contained in S. Similarly for the F-cosets in H_B. Since $|A| + |B| = |A + B| + 1$, we may write

(1) $A = A_0 \sqcup (F + a_1) \sqcup \ldots \sqcup (F + a_t)$ with $A_0 \subseteq (F + a_0)$;

(2) $B = B_0 \sqcup (F + b_1) \sqcup \ldots \sqcup (F + b_s)$ with $B_0 \subseteq (F + b_0)$;

(3) $A + B = (A_0 + B_0) \sqcup (F + d_1) \sqcup \ldots \sqcup (F + d_{s+t})$ with $(A_0 + B_0) \subseteq (F + a_0 + b_0)$. Here $F + a_0$, $F + b_0$ and $F + a_0 + b_0$ are the three improper cosets.

LEMMA 11.12 *With the above notation let S be a critical L_C-maximal cap. Suppose that F is a P_1-decomposing subgroup for S (with respect to H_∞). Then*

(1) $|\overline{A} + \overline{B}| = |\overline{A}| + |\overline{B}| - 1$;

(2) $\mathbb{PG}(F) \subseteq H_\infty$;

(3) Define k by $\mathbb{PG}(F) \cong \mathbb{PG}(k, 2)$. Then $k \leq n - 3$;

(4) $\widehat{S}$ *is a critical cap which is* $\overline{L_C}$*-maximal;*

(5) There is at least one element $\overline{g}$ *of* $\overline{L_C}$ *which is uniquely expressible as the sum of a point in* $\overline{A}$ *and a point in* $\overline{B}$.

Proof. The statement (1) was already given above.

Consider $\mathbf{0} \neq f \in F$. We have $d_1 = \mathbf{0} + d_1 \in F + d_1 \subseteq A + B \subset H_C$ and $f + d_1 \in F + d_1 \subset H_C$. Therefore $f = (f + d_1) + d_1 \in H_\infty$. This proves (2).

To prove (3) we have from (2) that $k \leq n-2$. From Definition 11.3 we have that $(A+B)$ contains D together with at least one full F-coset not equal to the coset containing D. Thus $k \leq n-3$.

The proof of (4) follows from Theorem 3.8 together with the fact pointed out above that $|\overline{A}| + |\overline{B}| = |\overline{A} + \overline{B}| + 1$

The statement (5) follows from the fact that $\sigma(D)$ has exactly one representation $\sigma(D) = \overline{a} + \overline{b}$ where $\overline{a} \in \sigma(A)$ and $\overline{b} \in \sigma(B)$. ∎

Let A_F be the F-coset $F + a_0$ containing A_0, let B_F be the F-coset $F + b_0$ containing B_0 and let C_F be the F-coset $F + a_0 + b_0$ containing $A_0 + B_0$. These are the three improper cosets. Let C_0 denote $S \cap C_F$. Since S is L_C-maximal, $H_C = C_0 \sqcup (A_0 + B_0)$. Let Λ denote the subspace of Σ generated by the three improper cosets. Thus $\Lambda \cong \mathbb{PG}(k+2, 2)$. We have a decomposition $\Lambda = X \cup Y \cup Z$ with $X \cong Y \cong Z \cong \mathbb{PG}(k+1, 2)$ and $A_0 \subset X$, $B_0 \subset Y$ and $C_0 \subset Z$.

By part (2) of the above Lemma we may subdivide H_C into F-cosets: $H_C = (F + d_0) \sqcup (F + d_1) \sqcup \ldots \sqcup (F + d_{s+t}) \sqcup (F + d_{s+t+1}) \sqcup \ldots \sqcup (F + d_r)$ where $F + d_0 = C_F$ and $r = 2^{n-k-2} - 1$. Then $C = C_0 \sqcup (F + d_{s+t+1}) \sqcup \ldots \sqcup (F + d_r)$. Therefore $2^{n-1} + 1 = |S| = |A| + |B| + |C| = |A_0| + s(2^{k+1}) + |B_0| + t(2^{k+1}) + |C_0| + (2^{n-k-2} - 1 - (s+t))2^{k+1}$. From this we obtain that $|A_0| + |B_0| + |C_0| = 2^{k+1} + 1$. Finally since, $A_0 + B_0 = C_F \setminus C_0$ it follows using Theorem 3.8 that $T := A_0 \sqcup B_0 \sqcup C_0$ is a critical cap in $\Lambda \cong \mathbb{PG}(t+2, 2)$ which is Z-maximal.

LEMMA 11.13 *Let* $w \in \Lambda$. *Then every secant line of* S *passing through* w *is in fact a secant of* T.

Proof. Take $w \in \Lambda \setminus S$ and suppose that $y, z \in S$ with $y + z = w$. Assume by way of contradiction, that $y \notin \Lambda$. Then $z \notin \Lambda$ also. By the uniqueness of the decomposition $\overline{C_F} = \overline{A_F} + \overline{B_F}$ this implies that $\overline{w} \neq \overline{C_F}$, i.e., that $w \notin L_C$. Without loss of generality suppose that $y \in B$ and $z \in C$ and thus $w \in A_F$. Choose $w' \in (A_F \cap S) = A_0$. Since $y \notin B_F$ and $z \notin C_F$ we have that the complete cosets $F + y$ and $F + z$ are contained in S. But then $w' + y \in F + z$ and the line $\{w', y, w' + y\}$ is contained in S. This contradiction proves the lemma. ∎

LEMMA 11.14 *Let* S *be a critical cap which is quasi-maximal with respect to* H_∞. *If* S *is* P_1*-decomposable with respect to* H_∞ *then one of the three hyperplanes* L *of* Σ *containing* H_∞ *satisfies* $|S \cap L| \geq 2^{n-2} + 1$.

Proof. The proof is by induction on n. If $n = 3$ then it is easily seen that the ovoid is the only quasi-maximal cap and that the ovoid satisfies the conclusions of the lemma.

Suppose now that $n \geq 4$. Let $(F, C'') \in P_1(A, B)$ and define k by $\mathbb{PG}(F) \cong \mathbb{PG}(k, 2)$. Let Ω denote the quotient geometry of Σ by $\mathbb{PG}(F)$. Construct $\widehat{S}$ in Ω as above. Then $\widehat{S}$ is critical and quasi-maximal.

We now consider two cases:

Case 1. $\widehat{S}$ is P_1 decomposable with respect to $\overline{H_\infty}$.
By induction there exists a hyperplane $\overline{L}$ of $\overline{\Sigma}$ containing $\overline{H_\infty}$ and such that $|\overline{L} \cap \widehat{S}| \geq 2^{n-k-3} + 1$. Then $|H \cap S| \geq 1 + (2^{n-k-3})(2^{k+1}) = 1 + 2^{n-2}$.

Case 2. $\widehat{S}$ is not P_1-decomposable with respect to $\overline{H_\infty}$.
By Theorem 11.10, $(\overline{A}, \overline{B})$ is an elementary pair. Since S is P_1-decomposable, we see by Lemma 11.12 (5) that case (iii) of Definition 11.8 does not apply.

Assume we are in case (ii). Then there exists a group F' such that $\overline{A} + \overline{B}$ is a coset of F'. Defining k' by $|F'| = 2^{k'}$ we have that $k + k' \leq n - 3$ since, by Lemma 11.12 (3) $k \leq n - 3$. First suppose that $k + k' \leq n - 4$. Since $\widehat{S}$ is quasi-maximal, $|\overline{L_C} \cap \widehat{S}| = 2^{n-k-2} - 2^{k'}$. Thus $|S \cap L_C| \geq 1 + 2^{k+1}(2^{n-k-2} - 2^{k'}) = 2^{n-1} - 2^{k+k'+1} + 1 \geq 2^{n-1} - 2^{n-2} + 1 = 2^{n-2} + 1$. Now, if $k + k' = n - 3$ then $\overline{A} + \overline{B} = \overline{L_C} \setminus \overline{H_\infty}$. Then, without loss of generality $|\overline{A}| \geq |\overline{B}|$ and hence $|\overline{A}| \geq 2^{n-k-3} + 1$. Therefore $|S \cap L_A| \geq 2^{k+1}(2^{n-k-3} + 1) = 2^{n-2} + 2^{k+1}$.

Finally assume we are in case (i) of Definition 11.8 with $|\overline{A}| = 1$ say. Then $|\widehat{S} \cap (\overline{L_B} \sqcup \overline{L_C})| = 2^{n-k-2}$. Assuming first that $|\widehat{S} \cap \overline{L_B}| \leq \frac{1}{2}(2^{n-k-2})$ we obtain that $|\widehat{S} \cap \overline{L_C}| \geq 2^{n-k-3}$ and therefore $|C| = |S \cap L_C| \geq 2^{k+1}(2^{n-k-3}) + 1 = 2^{n-2} + 1$. Suppose on the other hand that $|\widehat{S} \cap \overline{L_B}| \geq 2^{n-k-3} + 1$. Then $S \cap L_B \geq 2^{k+1}(2^{n-k-3} + 1 - 1) + 1 = 2^{n-2} + 1$. ∎

We have seen that any maximal fractal cap gives a critical maximal cap and so the structure of critical maximal caps appears quite flexible. In view of this our next result is somewhat surprising in that it pins down the structure, and even more so in the case when S is critical and quasi-maximal but not maximal (see Corollary 11.16).

THEOREM 11.15 *In $\Sigma = \mathbb{PG}(n, 2)$ let S be a critical cap which is quasi-maximal with respect to H_∞. Then either one of the three hyperplanes of Σ containing H_∞ is tangent to S or else one of these three hyperplanes intersects S in at least $2^{n-2} + 1$ points.*

Proof. By Lemma 3.10, $A + B$ is not periodic. Applying Theorem 11.10 we obtain that either (A, B) is elementary or S is P_1-decomposable. In the latter case, the result follows from Lemma 11.14.

Let us suppose then that (A, B) is elementary. If $|A| = 1$ or $|B| = 1$ then S has a tangent hyperplane of the required type.

Since S is quasi-maximal with respect to H_∞, $A + B = H_C \setminus C$. We examine cases (ii) and (iii) of Definition 11.8. First suppose $|F| = 2^{n-1}$. Then for case (ii) $|A| + |B| = 2^{n-1} + 1$ and this is an odd number. So we may choose notation so that $|S \cap L_A| \geq 2^{n-2} + 1$. (This case can also be disposed of as follows: $|F| = 2^{n-1}$ implies that $S \cap L_C = \emptyset$ which cannot happen because of the definition of S.) We consider case (iii) with $|F| = 2^{n-1}$. Then $A + B$ is obtained from a complete F-coset by removing a vector and thus $|A + B| = 2^{n-1} - 1$. But $H_C = (A + B) \sqcup C$. Therefore $|C| = 1$ and L_C is a tangent hyperplane.

Suppose now that $|F| \leq 2^{n-2}$. For case (iii) using again this $H_C = (A+B) \sqcup C$ we obtain that $|C| = |L_C \cap S| \geq 2^{n-1} - (2^{n-2}-1) = 2^{n-2}+1$. For case (ii), since $|A|+|B| = |F|+1$ both A and B cannot be complete F-cosets. So we assume that A is a proper subset of some F-coset, $F+a$. We have that $A+B$ is an F-coset, say $F+d$. Now $|F| \geq 2$. Choose two points d, $f+d \in A+B$ with $f \neq \mathbf{0}$; both of these points lie in H_C. Adding we see that $f \in H_\infty$. Therefore $\mathbb{PG}(F) \subset H_\infty$. Since S is quasi-maximal, we have as before that $H_C = (A+B) \sqcup C$. Thus since $\mathbb{PG}(F) \subset H_\infty$, C is a union of complete F-cosets. Therefore no point of $(F+a) \setminus A$ can lie on a secant of S. This contradicts the quasi-maximality of S. ■

COROLLARY 11.16 *Let S be a critical non-maximal cap which is quasi-maximal with respect to H_∞. Then there is a tangent hyperplane L to S which contains H_∞. Furthermore the other two hyperplanes which contain H_∞ each contain 2^{n-2} points of S.*

Proof. This follows immediately from the above theorem together with Lemma 3.5. ■

We are now able to describe all critical quasi-maximal caps which are not maximal.

PROPOSITION 11.17 *In $\Sigma = \mathbb{PG}(n,2)$ let S be a non-maximal critical cap which is quasi-maximal with respect to H_∞. Then there exists a unique point $e \in H_\infty$ which lies on no secant to S and S is obtained from the construction described in Section 7. Thus $S \sqcup \{e\}$ is the unique maximal cap containing S.*

Proof. Since, as is easily checked, there are no non-maximal, quasi-maximal caps in $\mathbb{PG}(2,2)$ we assume that $n \geq 3$. Let E be the set of points of Σ lying on no secants to S. We first show that E is itself a cap in H_∞. By the above Corollary, we may assume that $|A| = |B| = 2^{n-2}$ and $C = \{c\}$. Take $e_1, e_2 \in E$ and choose any point $a \in A$ and define $a_1 = e_1 + a$ and $a_2 = e_2 + a$. Then $a_1, a_2 \in H_A \setminus A$. Therefore $b_1 = a_1 + c$ and $b_2 = a_2 + c$ are both points of B. Therefore $e_1 + e_2 = b_1 + b_2$ lies on a secant to S and is not a point of E. Thus E is a cap. Therefore $\widetilde{S} := S \sqcup E$ is the unique maximal cap containing S. Since $|\widetilde{S}| > |S|$, $\widetilde{S}$ is a periodic cap. Let V be the set of vertices for $\widetilde{S}$. Since $|A| = |B| = 2^{n-2} > 1$, we see that $V \subseteq H_C$. But then for each $v \in V$ we have $E = v + C = \{v + c\}$ and thus $|E| = 1$. ■

12. A Structure Theorem

Let S be a critical quasi-maximal cap. We use the notation of previous sections. We have seen above that the set $A+B$ is not periodic. From Theorem 11.10 it follows that either (A, B) is an elementary pair or else S is P_1-decomposable. We have described the construction of fractal caps in Section 9: as explained earlier fractal caps are P_1-decomposable. However, as pointed out in Section 10 such caps may or may not possess tangent hyperplanes. Our first structure result is as follows.

THEOREM 12.1 *Let S be a critical quasi-maximal cap in $\Sigma = \mathbb{PG}(n,2)$. Take $H_\infty \cong \mathbb{PG}(n-2,2)$ a subspace of Σ disjoint from S. Assume that S is not P_1-decomposable with*

respect to H_∞. Then one of the three hyperplanes containing H_∞ is a tangent hyperplane for S.

Proof. From Section 3 we know that A and B are non-empty. By Theorem 3.10, $A + B$ is not periodic. From Theorems 3.8 and 11.10, we have that (A, B) is an elementary pair. Referring to Definition 11.8 we see that in case (i) either L_A or L_B is a tangent hyperplane to S containing H_∞. Case (ii) implies that $A + B$ is periodic contradicting Theorem 3.10.

Assume case (iii) occurs. Thus there exist a subgroup F of $V(n+1, 2)$ such that $A + B$ is obtained from an F-coset by deleting a single element from that coset. Define $m(C)$ by $|F| = 2^{m(C)}$. Thus $|C| = 2^{n-1} - 2^{m(C)} + 1$. If $m(C) = n - 1$ then $|C| = 1$ and L_C is a tangent hyperplane.

Therefore we may assume that $m(C) \leq n - 2$. Interchanging the roles of A and C we may assume that again case (iii) occurs and that the corresponding integer $m(A)$ satisfies $m(A) \leq n - 2$. Interchanging B and C we may similarly assume that $m(B) \leq n - 2$. But then $|S| = |A|+|B|+|C| = 3(2^{n-1}+1)-(2^{m(A)}+2^{m(B)}+2^{m(C)}) \geq 3(2^{n-1}+1)-3(2^{n-2}) = 3(2^{n-2}+1) > 2^{n-1}+1 = |S|$. This contradiction completes the proof. ∎

13. Another Structure Theorem

Let S be a critical cap with $H_\infty \cap S = \emptyset$ and $H_\infty \cong \mathbb{PG}(n-2, 2)$. Let L be any one of the three hyperplanes of Σ containing H_∞: for ease of notation let us assume that $L = L_C$. We proceed to define a so-called W-move using L. Let F be a subgroup of $V(n+1, 2)$ with $|F| = 2^{k+1}$. Let X, Y and $Z = X + Y$ be F-cosets with $X \cap A \neq \emptyset$, $Y \cap B \neq \emptyset$ and $Z \cap C \neq \emptyset$ such that $|X \cap A| + |Y \cap B| + |Z \cap C| = 2^{k+1} + 1$. Let a_0 be a single point in $X \cap A$ and put $X_1 := \{a_0\}$, $Y_1 = Y$ and $Z_1 = \emptyset$. Define the set S^* as follows. $S^* = (S \setminus (X \sqcup Y \sqcup Z)) \sqcup (X_1 \sqcup Y_1 \sqcup Z_1)$. Observe that $|S^*| = |S| = 2^{n-1} + 1$.

DEFINITION 13.1 We say that S is obtained from S^* by applying a *$W(F)$-move* (or more simply a *W-move*) to S^*. We denote this by writing $S \overset{F}{\rightarrow} S^*$.

To illustrate the usage of W-moves we state the following result.

THEOREM 13.2 *Every fractal cap is obtained by applying a single W-move to some critical cap.*

Proof. Let us use the notation of Section 3 pertaining to the fractal cap S. Put $X_1 = X \cap S$, $Y_1 = Y \cap S$ and $Z_1 = Z \cap S$. Let s_0 be a point of X_1 and put $X_2 := \{s_0\}$. Let $Y_2 := Y \setminus H_\infty$ and $Z_2 := \emptyset$. Put $S_1 := (S \setminus (X_1 \sqcup Y_1 \sqcup Z_1)) \cup (X_2 \sqcup Y_2 \sqcup Z_2)$. Note that S_1 is a critical cap. Moreover S is obtained from S_1 by a single W-move. ∎

Our goal now is to show that every critical quasi-maximal cap which is P_1-decomposable can be obtained by performing a certain sequence of W-moves starting with a fractal cap.

First however, we examine the situation described below.

NOTATION 13.3 Assume that S is a critical, L_C-maximal cap in $\Sigma = \mathbb{PG}(n, 2)$. Let S be P_1 decomposable and let F be a maximal P_1-decomposing subgroup for S. Let

$\sigma_F\colon \Sigma \to \Sigma/F = \overline{\Sigma}$ be the quotient map. Then (see 11.11 and the discussion preceding it) construct the cap $S_F := \widehat{S}$ in $\overline{\Sigma}$. Here $S_F = (\sigma_F(A) \sqcup \sigma_F(B) \sqcup \sigma_F(C)) \setminus \sigma_F(D)$. Let $A_F = F + a_0$, $B_F = F + b_0$ and $C_F = \sigma^{-1}(\sigma(D)) = F + d_0$ be the three improper cosets for S. Then $C_F = A_F + B_F$ is the unique expression of C_F as a sum of two F-cosets which meet S non-trivially.

Now suppose that S_F is also P_1-decomposable with respect to $\overline{H_\infty}$. This decomposition then yields a subgroup, say K, of the group $V(n+1,2)$ with $F \subset K$. Let $\widehat{S_{\overline{K}}}$ be the cap in $\overline{\Sigma}/K$ constructed from the P_1-decomposable cap S_F. Let $A_{\overline{K}}$, $B_{\overline{K}}$ and $C_{\overline{K}}$ be the three improper $\overline{K}$-cosets of S_F. Then $C_{\overline{K}} = A_{\overline{K}} + B_{\overline{K}}$ is the unique expression of $C_{\overline{K}}$ as a sum of $\overline{K}$-cosets meeting S_F. Let $A_K = \sigma_F^{-1}(A_{\overline{K}})$, $B_K = \sigma_F^{-1}(B_{\overline{K}})$ and $C_K = \sigma_F^{-1}(C_{\overline{K}})$.

LEMMA 13.4 *Using the above notation we have that $C_F \not\subset C_K$. Furthermore either ($A_F \subset A_K$ and $B_F \not\subset B_K$) or ($A_F \not\subset A_K$ and $B_F \subset B_K$).*

Proof. If $C_F \subset C_K$ then $A_F \subset A_K$ and $B_F \subset B_K$ by the uniqueness of the expressions for C_F and $C_{\overline{K}}$. This then implies that S is P_1 decomposable with respect to K contradicting the maximality of F. Thus we conclude that $C_F \not\subset C_K$.

We claim that this implies that each F-coset in $K + d_0$ different from $F + d_0$ contains no points of S. To see this assume by way of contradiction that there is a point $c \in (K + d_0) \setminus (F + d_0)$ which lies in S. Then $\sigma_F(c) \in S_F$ and $\sigma_F(c)$ does not lie in the improper coset $C_{\overline{K}}$. Hence the entire $\overline{K}$-coset, $\overline{K} + \sigma_F(c)$ is contained in S_F. But this contradicts the fact that $\sigma_F(d_0) \notin S_F$.

Next we note that if $A_F \subset A_K$ and $B_F \subset B_K$ then using the expressions for C_F and $C_{\bar{K}}$ we obtain $C_F \subset C_K$. Therefore we may assume without loss of generality that $B_F \not\subset B_K$. We observe now that every F-coset in $K + b_0$ different from $F + b_0$ is entirely contained in S.

Consider an F-coset, $F + a_1$, different from A_F which is contained in $K + a_0$. Then $(F + a_1) + (F + d_0)$ is an F-coset different from $B_F = F + a_0 + d_0$ and contained in $K + a_1 + d_0 = K + a_0 + d_0 = K + b_0$. Therefore $(F + a_1) + (F + d_0) \subset S$. Thus if there were a point of S lying in $F + a_1$ and one in $F + d_0$ then S would contain a line. Thus since there are points of S in $F + d_0$ it follows that $(F + a_1) \cap S = \emptyset$. We have thus shown that every F-coset different from A_F and contained in $K + a_0$ is disjoint from S, i.e., $(K + a_0) \cap S = (F + a_0) \cap S$. If $A_F \not\subset A_K$ then every F-coset in $K + a_0$ different from $F + a_0$ would be entirely contained in S but we have just shown that every such F-coset is disjoint from S. We conclude that $A_F \subset A_K$. ∎

Without loss of generality assume that $A_F \subset A_K$ and $B_F \not\subset B_K$.

From our original cap S we construct a cap S_1 as follows. Put $X_1 = A_F \cap S$, $Y_1 = B_F \cap S$ and $Z_1 = C_F \cap S$. Pick any point s_0 in X_1 and let $X_2 = \{s_0\}$. Put $Y_2 = B_F$ and $Z_2 = \emptyset$. Define $S_1 = (S \setminus (X_1 \sqcup Y_1 \sqcup Z_1)) \sqcup (X_2 \sqcup Y_2 \sqcup Z_2)$. By Lemma 11.13 we see that S_1 is a cap, in fact a critical cap.

We now have the following result.

THEOREM 13.5 *K is a P_1-decomposing subgroup for S_1 and S is obtained from S_1 by applying a single $W(F)$-move to S_1. Moreover S_1 is L_C-maximal.*

Proof. By construction S_1 has K as a P_1-decomposing subgroup. Furthermore, it follows directly from the definition of a $W(F)$ move that S is obtained from S_1 by applying a single $W(F)$-move. That S_1 is L_C-maximal follows from Theorem 3.8. ∎

We now come to the main structure theorem for caps which are P_1-decomposable.

THEOREM 13.6 *Let S be a critical L_C-maximal cap which is P_1-decomposable with repect to H_∞. Then there exists a sequence $S = S^0, S^1, S^2, \ldots S^t$ of critical caps and a sequence of subgroups of $V(n+1,2)$ $\{0\} \subsetneq F = F_1 \subsetneq F_2 \subsetneq \ldots \subsetneq F_{t+1}$ with $t \leq n-2$ satisfying the following properties*

(1) $S^{i-1} \xrightarrow{F_i} S^i$,

(2) *F_{i+1} is a P_1-decomposing subgroup for S^i, and*

(3) *S^t is fractal*

Proof. Let F be a maximal P_1-decomposing subgroup for S. We examine the cap $\widehat{S} = S_F$. By a straightforward argument as in Lemma 11.12 we have that $|\overline{A} + \overline{B}| = |\overline{A}| + |\overline{B}| - 1$.

Case 1. S_F is not P_1-decomposable (with respect to $\overline{H_\infty}$).
Since S is P_1-decomposable, the improper coset in L_C is uniquely expressible as a sum of a coset in L_A plus a coset in L_B both containing points of S namely as the sum of the two other improper cosets. From the above discussion of P_1-decomposability we see that in the quotient space the improper coset in L_C gives rise to an element g such that $\nu_g(\overline{A}, \overline{B}) = 1$. Therefore the hypotheses of Theorem 11.10 are satisfied and thus the pair $(\overline{A}, \overline{B})$ is elementary as per Definition 11.8. We have seen that case (iii) does not apply.

Suppose that we are in case (ii) so that there is a subgroup K with $|K| = 2^k$. Moreover K contains F and is such that $\overline{A}$ lies in a $\overline{K}$-coset, say $\overline{U}$, $\overline{B}$ lies in a $\overline{K}$-coset, say $\overline{V}$ and that $\overline{A} + \overline{B}$ is itself a $\overline{K}$-coset, $\overline{W} = \overline{U} + \overline{V}$. As in the proof of Theorem 11.12 (2) we may assume that $\mathbb{PG}(K) \subset H_\infty$. Initially suppose $\mathbb{PG}(K) = H_\infty$. Then $\overline{A} + \overline{B} = \overline{H_C}$ and $\widehat{S}$ is a Swiss cap. Using the improper cosets of F we see that S is a fractal cap. Next suppose that $\mathbb{PG}(K)$ is properly contained in H_∞. Since $\mathbb{PG}(K) \subset H_\infty$, we can decompose H_C as a disjoint union of K-cosets: $H_C = W_1 \sqcup W_2 \sqcup \ldots \sqcup W_r$ where $W = W_1$ and $r = 2^{n-k-1}$. Since S is L_C-maximal it follows that $W_2, W_3, \ldots W_r$ are each contained in the cap S. Then $S_K := (A/K) \sqcup (B/K) \sqcup (C/K)$ is cap in $(\Sigma/\mathbb{PG}(K)) \cong \mathbb{PG}(n-k, 2)$ of cardinality $r + 1 = 2^{n-k-1} + 1$. Furthermore since $|B/K| = 1$ (or using the property of the improper cosets of F), we obtain that there is unique secant of S_K containing the point A/K. Moreover by direct calculation we obtain $|S \cap U| + |S \cap V| + |S \cap W| = 2^k + 1$. Therefore S_K is a Swiss cap in $\Sigma/\mathbb{PG}(K)$. Therefore S is fractal.

Finally suppose that case (i) applies with $|\overline{A}| = 1$. Since S is P_1-decomposable with repect to H_∞, $\overline{A}$ must correspond to an improper coset. It follows with a proof similar to the above that S is a fractal cap.

Case 2. S_F is P_1-decomposable (with respect to $\overline{H_\infty}$).
By Lemma 11.12 (5), Lemma 13.4 and Theorem 13.5 there exists a critical cap S_1 satisfying the following properties:

(1) $S \overset{F_1}{\to} S_1$;

(2) there exists a subgroup K of $V(n+1, 2)$ with $F \subsetneq K$ such that K is a P_1-decomposing subgroup for S_1;

(3) there are at least two distinct K-cosets in L_C each having the property that it is uniquely expressible as the sum of a K-coset in L_A which intersects S_1 plus a K-coset in L_B which intersects S_1;

(4) S_1 is L_C-maximal;

(5) $\mathbb{PG}(K) \subset H_\infty$.

Next let $K^* \supseteq K$ be a maximal P_1-decomposing subgroup for S_1. Put $S^0 = S$, $S^1 = S_1$, $F_1 = F$ and $F_2 = K^*$.

We examine the cap $E = (S_1)_{F_2}$. This is a cap in the quotient geometry of Σ by $\mathbb{PG}(F_2)$ where as in the proof of Lemma 11.12 (2) $\mathbb{PG}(F_2) \subset H_\infty$. As usual let $\sigma = \sigma_{F_2}$ denote the quotient map $\sigma\colon V(n+1, 2) \to V(n+1, 2)/(K^*)$. By Lemma 11.12, E is a critical cap. Then $\overline{A} = \sigma(L_A \cap S) = \sigma(L_A \cap S_1)$ and $\overline{B} = \sigma(L_B \cap S) = \sigma(L_B \cap S_1)$. Therefore by Lemma 11.12 (1) we have $|\overline{A} + \overline{B}| = |\overline{A}| + |\overline{B}| - 1$. By the statement (3) above we are in a position to apply Theorem 11.10. Again we consider two cases.

Case A. E is not P_1-decomposable.
From Theorem 11.10 the pair (A, B) is elementary. It follows from (3) above that we are not in case (ii) nor case (iii) of Definition 11.8. We conclude that we are in case (i). Arguing as in Case 1 above we conclude that S_1 is a fractal cap.

Case B. E is P_1-decomposable.

Then as before, we choose a maximal P_1-decomposing subgroup for E. We proceed as above. Now the chain of P_1-decomposing subgroups $F_1 \subsetneq F_2 \subsetneq \dots$ is strictly increasing. Therefore eventually we obtain a subgroup F_t and a cap S^t such that the cap $(S^t)_{F_t}$ is not P_1-decomposable. As above S^t is a fractal cap and furthermore $S_{i-1} \overset{F_i}{\to} S_i$ for all $1 \le i \le t$ Now $|F_i| \ge 2^i$. Thus $\dim \mathbb{PG}(F_t) \ge t - 1$ and thus by Lemma 11.12 (2) we have that $t - 1 \le n - 3$ giving $t \le n - 2$. This completes the proof. ∎

Note next that quasi-maximality implies L_C-maximality. Thus, combining Theorem 13.6 with Theorem 12.1 we have the following structure theorem.

THEOREM 13.7 *Let S be a critical quasi-maximal cap in $\Sigma = \mathbb{PG}(n, 2)$. Then*

(1) there exists a subspace $H_\infty \cong \mathbb{PG}(n-2, 2)$ of Σ which is disjoint from S;

(2) if S is not P_1-decomposable then there exists a hyperplane containing H_∞ which is tangent to S;

(3) if S is P_1-decomposable then S is obtained from a fractal cap by a sequence of at most $n-2$ W-moves as detailed in Theorem 13.6.

We conclude by showing that for a critical quasi-maximal cap there is always at least one point of space which lies on a unique secant line.

THEOREM 13.8 *Let $\Sigma = \mathbb{PG}(n,2)$ and suppose that $S \subset \Sigma$ is a critical quasi-maximal cap with respect to H_∞. Then there exists a point of $\Sigma \setminus H_\infty$ lying on exactly one secant line to S.*

Proof. We proceed by induction on n. The result is vacuously true for $n = 2$. The result is also easily verified for $n = 3$ since there every point of $\Sigma \setminus S$ lies on exactly one secant line.

Taking $n \geq 4$ we see that by Theorem 11.10, either (A, B) is an elementary pair or S is P_1-decomposable.

Suppose that (A, B) is elementary. Then (A, B) satisfies one of the three conditions of Definition 11.8.

First suppose $|A| = 1$ and write $A = \{a_0\}$. Then if $b \in B$ clearly $w = a_0 + b$ lies on a unique secant to S. A similar argument handles the possibility that $|B| = 1$.

Secondly we suppose that (A, B) is elementary and satifies condition (ii) of Definition 11.8. Then $A + B$ is periodic in contradiction to Theorem 3.10.

Thirdly we suppose (A, B) satifies condition (iii) of Definition 11.8. Then there exists a subgroup F of $\mathbb{AG}(n+1,2)$ such that $A+B$ is obtained by deleting a single element from an F-coset. Define $m(C)$ by $|F| = 2^{m(C)}$. Thus $|C| = 2^{n-1} - 2^{m(C)} + 1$. If $m(C) = n-1$ then $|C| = 1$ and L_C is a tangent hyperplane and we proceed as in case (i) above.

Therefore we may assume that $m(C) \leq n-2$. Interchanging the roles of A and C we may assume that again case (iii) occurs and that the corresponding integer $m(A)$ satisfies $m(A) \leq n-2$. Interchanging B and C we may similarly assume that $m(B) \leq n-2$. But then $|S| = |A|+|B|+|C| = 3(2^{n-1}+1)-(2^{m(A)}+2^{m(B)}+2^{m(C)}) \geq 3(2^{n-1}+1)-3(2^{n-2}) = 3(2^{n-2}+1) > 2^{n-1}+1 = |S|$. This contradiction shows that if (A, B) is an elementary pair then there is a point of $\Sigma \setminus H_\infty$ lying on only one secant to S.

Thus we suppose that S is P_1-decomposable. Then we have the subcap S_0 which is a critical quasi-maximal cap in Λ. By induction, there is a point w of $\Lambda \setminus (\Lambda \cap H_\infty)$ lying on a unique secant line to S_0. Applying Lemma 11.13 we see that this line is the only secant line to S passing through w. ∎

Acknowledgments

We thank Professors Clark, Haddad, Helleseth, and Rogers for valuable comments. Research partially supported by NSERC and ARP.

References

1. A. A. Bruen and D. L. Wehlau, Maximal caps, line free sets and quasi-perfect codes, submitted.
2. Aiden A. Bruen, L. Haddad and D. L. Wehlau, Binary codes and caps, *J.C.D.*, Vol. 6, No. 4 (1998) pp. 275–284.
3. R. C. Bose and J. N. Srivastava, On a bound useful in the theory of factorial designs and error correcting codes, *Ann. Math. Stat.*, Vol. 35, No. 1 (1964) pp. 408–414.
4. W. Edwin Clark, Blocking sets in finite projective spaces and uneven binary codes, *Discrete Math.*, Vol. 94 (1991) pp. 65–68.
5. W. E. Clark, L. A. Dunning and D. G. Rogers, Binary set functions and parity check matrices, *Discrete Math.*, Vol. 80 (1990) pp. 249–265.
6. A. A. Davydov and L. M. Tombak, Quasiperfect linear binary codes with distance 4 and complete caps in projective geometry, *Problems of Information Transmission*, Vol. 25, No. 4 (1990) pp. 265–275.
7. T. Helleseth, On the covering radius codes, *Discr. Appl. Math.*, Vol. 11, No. 2 (1985) pp. 151–173.
8. R. Hill, Caps and codes, *Discrete Math*, Vol. 22, No. 2 (1978) pp. 111–137.
9. J. H. B. Kemperman, On small sumsets in an abelian group, *Acta. Math. Stockholm*, Vol. 103, Nos. 1–2 (1960) pp. 62–88.
10. M. Kneser, Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen, *Math. Z.*, Vol. 61 (1955) pp. 429–434.
11. M. Kneser, Summenmengen in Iokalkompakten abelschen Gruppen, *Math. Z.*, Vol. 66 (1956) pp. 88–110.
12. B. Segre, Introduction to Galois geometries, *Atti. Accad. Naz. Lincei Memorie*, Vol. 8 (1967) pp. 133–236.
13. G. Tallini, On caps of kind s in a Galois r-dimensional space, *Acta Arithmet.*, Vol. 7, No. 1 (1961) pp. 19–28.
14. W. T. Tutte, Colouring problems, *Math. Intelligencer*, Vol. 0 (1977) pp. 72–75.