Binary Codes and Caps

Aiden A. Bruen,[1] Lucien Haddad,[2] David L. Wehlau[3]

[1] *Dept. of Mathematics, University of Western Ontario, London, Ontario, Canada N6A 3K7*

[2] *Dept. of Mathematics and Computer Science, Royal Military College of Canada, Kingston, Ontario, Canada K7K 5L0*

[3] *Dept. of Mathematics and Computer Science, Royal Military College of Canada, Kingston, Ontario Canada K7K 5L0 and Dept. of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada K7L 3N6*

Received September 12, 1996; accepted February 20, 1997

Abstract: The connection between maximal caps (sometimes called complete caps) and certain binary codes called quasi-perfect codes is described. We provide a geometric approach to the foundational work of Davydov and Tombak who have obtained the exact possible sizes of large maximal caps. A new self-contained proof of the existence and the structure of the largest maximal nonaffine cap in $\mathbb{P}G(n, 2)$ is given. Combinatorial and geometric consequences are briefly sketched. Some of these, such as the connection with families of symmetric-difference free subsets of a finite set will be developed elsewhere. © 1998 John Wiley & Sons, Inc. J Combin Designs 6: 275–284, 1998

Keywords: *caps; codes; 2–blocks; projective space.*

1. CODES

Let C be a binary linear code of length N, and minimum distance $d = 4$ with r check symbols. Put $r = n + 1$. So C has cardinality $|C| = 2^{N-r}$ and C has linear (vector-space) dimension equal to $N - r$.

Correspondence to: Dr. D. L. Wehlau, Department of Mathematics and Computer Science, Royal Military College of Canada, Kingston, ON K7K 5LO; e-mail: wehlau@mast.queensu.ca

Dedicated to the memory of Giuseppe Tallini (1930–1995).

Contract grant sponsor: NSERC

* e-mail: bruen@uwo.ca

† e-mail: haddad@rmc.ca

CCC 1063 8539/98/040275-10

Let $C^{\perp}$ denote the dual code. Then $C^{\perp}$ has length N and dimension $r = n + 1$. Choosing a basis we can think of $C^{\perp}$ as a matrix (the check matrix) of size $r \times N$. Then each of the N columns can be regarded as a point in $\Sigma = \mathbb{P}G(n, 2)$, the projective space of dimension n over $GF(2)$.

Warning: Here, and in the sequel, dimension normally means projective dimension.

Since $d = 4$, the columns of $C^{\perp}$ are all nonzero, no two are equal, and no column of $C^{\perp}$ equals a sum of two other columns of $C^{\perp}$. Therefore C gives rise to a *cap* S in Σ of size N, i.e., a set of N points in Σ with no 3 collinear. Conversely, given such a cap we can recover C.

The connections between codes and caps have been well studied (see for example [1], [4–6], [11]). In particular the following can be shown.

Theorem 1.1. *The cap S is maximal if and only if the code C has covering radius* 2*.*

If the code C of minimum distance 4 has covering radius 2 it is called *quasi-perfect* (see [4]). The fundamental nature of such codes C using Theorem 1.1, is that C is ''nonlengthening'' in the sense that no nonzero column can be added to the check matrix without reducing the code distance. Using this one can show that any binary linear code with $d = 4$ is either a quasi-perfect code or a shortening of some quasi-perfect code with $d = 4$. Because of the existence of a large body of geometric techniques for studying caps we concentrate on caps.

2. MAXIMAL CAPS IN $\Sigma = \mathbb{P}G(n, 2)$

Suppose S is any cap in Σ. One can argue as follows. By definition, no 3 points of S are collinear. It follows that each line of Σ intersects $\bar{S}$, the complement of S. As S gets bigger, $\bar{S}$ gets smaller while still intersecting every line. Then when S gets large one can show, since $\bar{S}$ is small and meets all lines, that $\bar{S}$ will contain an hyperplane L. We want to find the cut-off point for $|S|$.

We generalize the usual definition of ''affine'' as follows.

Definition 2.1. *In $\Sigma = \mathbb{P}G(n, 2)$ a set S is affine if S lies in the complement of some hyperplane L of Σ.*

Remark. A single point always forms an affine set. However, for single points we will work with a specified hyperplane L, i.e., a point is said to be *affine* if it does not lie on the specified hyperplane L, in accordance with standard usage.

Note that if S is affine and a maximal cap then S must consist of the affine space $\Sigma \setminus L$. The following result is not difficult (see [6]).

Theorem 2.2. *Let S be a maximal cap in $\Sigma = \mathbb{P}G(n, 2)$. Then $|S| \leq 2^n$. Moreover, $|S| = 2^n$ if and only if S is the complement of an hyperplane in Σ, i.e., if and only if $S = \mathbb{A}G(n, 2)$, the affine n dimensional space over $GF(2)$.*

The following sheds some light on the cut-off point mentioned above (see [10] p. 108).

Theorem 2.3. *If S is a maximal cap in $\Sigma = \mathbb{P}G(n, 2)$ which is not affine then $|S| \leq \frac{2^{n+1}-1}{3}$.*

The following is easily shown.

Theorem 2.4. *The bound of Theorem* 2.3 *is best possible in the case* $n = 3$. *Moreover if* $n = 3$ *and* $|S| = 5$ *then* S *is the set of points in an ovoid* $\mathcal{O}$ *of* $\mathbb{P}G(3, 2)$. *Of the* 15 *planes in* $\mathbb{P}G(3, 2)$, 10 *meet* $\mathcal{O}$ *in* 3 *points and* 5 *are tangent to* $\mathcal{O}$.

In a remarkable article [4] published in 1990, A. A. Davydov and L. M. Tombak make a profound contribution to the theory. Related results have been obtained in [2] and [3]. To explain some of these results we need some further background and definitions as follows.

In $\Sigma_n = \mathbb{P}G(n, 2)$ let S be any cap and let v be a point not in S. We say that v is a *vertex* for S if whenever we join v to a point p of S the third point q on the line vp is also in S.

Examples can be constructed as follows. Let S_n be any cap in Σ_n. Embed Σ_n in Σ_{n+1} and let v be any point in $\Sigma_{n+1} \setminus \Sigma_n$. We now construct a cap, S_{n+1}, in Σ_{n+1} by adjoining to S_n the set of all points q where q is the third point of the line vp where p is any point of S_n. We have that $|S_{n+1}| = 2|S_n|$ and that S_{n+1} is maximal in Σ_{n+1} if and only if S_n is maximal in Σ_n. Note that v now is a vertex for the cap S_{n+1}. This construction of S_{n+1} from S_n is called the *doubling construction* or *Plotkin construction*.

In fact every vertex arises in this way. For, if v is a vertex of S and H is any hyperplane not on v then S is obtained by doubling $S \cap H$ from v.

In $\Sigma = \mathbb{P}G(n, 2)$ let T be any set of points. The set T is called a k*-block* (see [12]) if every $(n - k)$ dimensional subspace of Σ contains at least one point of T.

Let $k = 2$ and suppose that T is a 2-block. Let Z be any subset of T, let W be an $(n - 2)$ dimensional subspace of Σ containing all the points of Z and therefore all the points of T which are linearly dependent on Z. If W contains no further points of T we call it a *generalized tangent* of T at Z. The 2-block T is called a *tangential 2-block* if every nonempty proper subset Z of T has a generalized tangent of T at Z. Note that if Z is a single point then a generalized tangent just means a tangent $(n - 2)$ dimensional space at this point in the usual sense of the term. The importance of tangential 2-blocks is that, as pointed out by W. T. Tutte ([12]) all other 2-blocks can be regarded as certain ''derivatives'' of them.

So far only three tangential 2-blocks have been found. These are the Fano plane, the Desargues block consisting of the 10 points of a Desargues configuration in 3 dimensions and the 5 dimensional Petersen block which represents the Petersen graph in a dual manner with cut-sets representing circuits in the definition of linear dependence. It is conjectured that these are the only tangential 2-blocks. It is a remarkable fact that a proof of this conjecture would imply the celebrated 4-color theorem for planar graphs.

Some of the main results of [4] can be summarized as follows.

Theorem 2.5. *No cap* S *in* $\Sigma = \mathbb{P}G(n, 2)$ *with* $|S| > 2^{n-1} + 1$ *can be a* 2*-block.*

Theorem 2.6. *If* S *is a maximal cap in* Σ *with* $|S| > 2^{n-1} + 1$ *and* $n \geq 3$, *then* S *is obtained by the doubling construction. It follows that if* S *is a maximal cap and* $|S| > 2^{n-1} + 1$ *then either* S *is affine or else* $|S| = 2^{n-1} + 2^i$, *for some* $i \geq 1$. *It can be shown that* $i \leq n - 3$. *Moreover, if* $|S| = 2^{n-1} + 2^{n-3}$ *or* $|S| = 2^{n-1} + 2^{n-4}$ *then the structure of* S *is known and* S *is unique up to collineations of* Σ.

We now proceed to give a sketch of the proof by Davydov and Tombak of Theorem 2.6, but casting it in a geometric framework consistent with our methods.

Using Theorem 2.5 let H_∞ denote an $(n-2)$ dimensional subspace that contains no point of S. Let L_1, L_2, and L_3 denote the three hyperplanes on H_∞ in Σ. We denote by A, B, and C the set of points of S lying in L_1, L_2, and L_3, respectively. For p in A and q in B the line joining p to q meets L_3 in a point which cannot lie in S since S is a cap, and also cannot lie in H_∞. We denote by $A+B$ the set of all such points. Since S is a cap, any line in L_3 contains at most two points of S. Then from the maximality of S it follows that each point of L_3 not in H_∞ and not in $A+B$ must be a point of S. Therefore $|S| = |A| + |B| + (2^{n-1} - |A+B|)$. Let $|S| = 2^{n-1} + \alpha$, with $\alpha \geq 1$. It follows that

$$|A+B| = |A| + |B| - \alpha, \quad \text{with } \alpha \geq 1.$$

Now suppose that $\alpha \geq 2$. Let G denote the elementary abelian group of order 2^{n+1} obtained from the vector space $V(n+1,2)$ underlying Σ. Then, since A, B are subsets of G satisfying the above relation, it follows from an old result of Kneser in additive number theory (see Kneser [8], [9], and Kemperman [7, p. 69]) that $A+B$ is *periodic*, i.e., there exists $g_0 \neq 0$ in G with $g_0 + (A+B) = A+B$. Then g_0 corresponds to a point v in L_3 such that if we join v to any point w in $A+B$ then the third point of this line also lies in $A+B$. Since all points of $A+B$ are affine points of L_3 (i.e., are on $L_3 \setminus H_\infty$) and since a line of L_3 contains just 2 affine points we get that v is in H_∞. It follows that v is a vertex for $S \cap L_3$. One can then show that in fact v is a vertex for the entire cap S. In other words S is obtained by the doubling construction.

To finish the sketch of the proof of Theorem 2.6 let us now suppose that $|S| = 2^{n-1} + 2^{n-3}$. Then S is obtained by successively doubling, beginning with a cap of size 5 in $\mathbb{P}G(3,2)$, which must be the set of points on the ovoid described earlier. Therefore the structure of S can be described and S is unique. Using the fact that the structure of a cap in $\mathbb{P}G(4,2)$ of size 9 is unique, we can in a similar fashion obtain the structure of S when $|S| = 2^{n-1} + 2^{n-4}$.

From Theorem 2.6 we obtain the following corollary (see [2–4]).

Corollary 2.7. *Let $n \geq 3$. In $\mathbb{P}G(n,2)$ let S be a maximal cap with S not affine. Then $|S| \leq 2^{n-1} + 2^{n-3}$. If $|S| = 2^{n-1} + 2^{n-3}$ then the structure of S is known and is unique.*

(Actually, only the inequality part of this result is shown in [2].)

3. A GEOMETRIC RESULT

The proof of Corollary 2.7 that is given in [4] is very algebraic and uses the sophisticated result on additive number theory by Kneser mentioned earlier as well as the crucial Theorem 2.5 which seems very difficult to establish. The maximal cap S of size $2^{n-1}+2^{n-3}$ (which is unique up to collineations of $\Sigma = \mathbb{P}G(n,2)$) is described by means of an intricate generator matrix constructed inductively.

Here we give a transparent geometric construction of S. Moreover, our construction also provides examples of maximal caps S with $|S| = 2^{n-1} + 2^i$ for $0 \leq i \leq n-3$. Following that we then present a new elementary and self-contained proof of Corollary 2.7. In fact we prove the slightly stronger Corollary 3.6. Our proof does not use the results on additive number theory nor does it use Theorem 2.5.

For the construction in $\Sigma = \mathbb{P}G(n,2)$, let H_∞ denote a subspace of dimension $n-2$. Let L_1, L_2, and L_3 denote the three hyperplanes of Σ on H_∞. Choose a subspace Ω_1 of dimension $n-3$ contained in L_1 and not contained in H_∞. Let $\Omega_1 \cap H_\infty = \Psi$. Let Ω_2 denote a subspace of L_2 containing also Ψ and of dimension $n-3$. Denote the affine points of Ω_1, Ω_2 by A and B respectively, i.e., A, B denote all points of Ω_1, Ω_2 not in H_∞. So $|A| = |B| = 2^{n-3}$. Put $S = A \cup B \cup C$ where C denotes the set of all points in L_3 not in H_∞ and not in $A + B$, where $A + B$ denotes the points of the form $p + q$ with $p \in A$ and $q \in B$. Then S is a maximal cap with $|S| = 2^{n-1} + 2^{n-3}$. Moreover, this construction can be generalized. If Ω_1 and Ω_2 have dimension i then S is a maximal cap of size $2^{n-1} + 2^i$ for $0 \leq i \leq n-3$. If $i = n-2$ the cap fails to be maximal. The unique maximal cap containing it is $\mathbb{A}G(n, 2)$. If $i = n-1$ we get the maximal cap $\mathbb{A}G(n, 2)$.

Next we proceed to give a new proof of Corollary 2.7. Denote by X_n the maximal cap of size $2^{n-1} + 2^{n-3}$ in $\mathbb{P}G(n, 2)$ described above. Let S be any nonaffine cap of size $2^{n-1} + 2^{n-3}$ contained in $\mathbb{P}G(n, 2)$. We will show that S is isomorphic to X_n.

Notation: If Y is any set, SY denotes the set $S \cap Y$.

Proof of Corollary 2.7 We proceed by induction. The case $n = 3$ is easily checked by direct computation. Thus we suppose that $\Sigma = \mathbb{P}G(n, 2), n \geq 4$ and that $|S| = 2^{n-1} + 2^{n-3}$.

Lemma 3.1. *Let K be an hyperplane of Σ with $|SK| > |S|/2$. Then SK is an affine cap in K, i.e., there is an hyperplane of K containing no points of SK.*

Proof. Embed SK in a maximal cap T of $K = \mathbb{P}G(n-1, 2)$. Then $|T| \geq |SK| > |S|/2 = 2^{n-2} + 2^{n-4}$. Then by induction we have that T and hence also SK is an affine cap in K. □

By a counting argument involving incidences of hyperplanes with pairs of points of S we may establish the existence of an hyperplane containing more than half of the points of S. (The counting argument works for any set T in $\mathbb{P}G(n, 2)$ with $|T| \leq 2^n - 1$, not just for caps.) Let H be an hyperplane such that $|SH|$ is maximum amongst all hyperplanes. Then SH is a cap in $\mathbb{P}G(n-1, 2)$ with $|SH| = 2^{n-2} + 2^{n-4} + \epsilon$ where $\epsilon \geq 1$. Since $|SH| > |S|/2$ we conclude from Lemma 3.1 that SH is an affine cap, i.e., that there is an hyperplane H_∞ of H with $SH_\infty = \emptyset$. Denote the other two hyperplanes containing H_∞ by A and B.

Lemma 3.2. *Any hyperplane K with $K \neq A, B, H$ contains at most $2^{n-3} + 2^{n-5} + \frac{3}{2}\epsilon$ points of SH.*

Proof. Define $\alpha := |K \cap SH|$. The number of points in $S \setminus H$ is $2^{n-2} + 2^{n-4} - \epsilon$. Therefore one of the two hyperplanes on $K \cap H$ other than H (one of which is K), say M, contains at least half these points. So we get $\alpha + 2^{n-3} + 2^{n-5} - \epsilon/2 \leq |SM| \leq |SH| = 2^{n-2} + 2^{n-4} + \epsilon$. This gives $\alpha \leq 2^{n-3} + 2^{n-5} + 3\epsilon/2$. □

Lemma 3.3. *Any hyperplane K with $K \neq A, B, H$ contains at least $2^{n-3} + 2^{n-5} - \frac{1}{2}\epsilon$ points of SH.*

Proof. Define $\beta := |K \cap SH|$. Working in H let the pencil determined by $K \cap H_\infty$ consist of $H_\infty, K \cap H$ and M say. Note that SM consists of exactly those points of SH not lying in $K \cap H$. So $|SM| = |S|/2 + \epsilon - \beta$. Now extend M to an hyperplane of Σ not equal to H and apply Lemma 3.2. □

Lemma 3.4. *Let K be any hyperplane with $|SK| = |S|/2 + \theta$ where $\theta \geq 1$. Let K_∞ be one of the hyperplanes of K missing S guaranteed by Lemma* 3.1 *and let C and D be the other two hyperplanes of Σ on K_∞. Then $\theta \leq 2^{n-4}, |SC| \geq 2^{n-3}$, and $|SD| \geq 2^{n-3}$. In particular, $\epsilon \leq 2^{n-4}, |SA| \geq 2^{n-3}$, and $|SB| \geq 2^{n-3}$.*

Proof. Let $c := |SC|$ and $d := |SD|$. Then $c + d = |S| - |SK| = |S|/2 - \theta$. Since S is assumed to be nonaffine, no hyperplane misses S and thus $SC \neq \emptyset$. By joining a point of C to the points of D we get, since S is a cap, that $|SK| \leq 2^{n-1} - d$. Similarly, $|SK| \leq 2^{n-1} - c$. Thus $2|SK| \leq 2^n - (c + d)$, i.e., $|S| + 2\theta + c + d \leq 2^n$. Therefore, $3|S|/2 + \theta \leq 2^n$. Since $|S| = 2^{n-1} + 2^{n-3}$, this gives $\theta \leq 2^{n-4}$.

Now without loss of generality, $c \leq d$. Joining a point of SC to each point of SK yields $2^{n-2} + 2^{n-4} + \theta$ affine (with respect to K_∞) points of D, none of which are in SD, since S is a cap. Therefore $d + 2^{n-2} + 2^{n-4} + \theta \leq 2^{n-1}$. Thus $d \leq 2^{n-2} - 2^{n-4} - \theta$. From the above, $c + d + \theta = |S|/2 = 2^{n-2} + 2^{n-4}$. Assume, by way of contradiction, that $c < 2^{n-3}$. Then $d + \theta > 2^{n-2} + 2^{n-4} - 2^{n-3}$, i.e., $d > 2^{n-2} - 2^{n-4} - \theta$. But from the above, $d \leq 2^{n-2} - 2^{n-4} - \theta$ and this contradiction proves $c \geq 2^{n-3}$. Since $d \geq c$, we also have $d \geq 2^{n-3}$. □

Lemma 3.5. *Let Y be a nonempty affine subset of $\mathbb{P}G(n, 2)$ where $n \geq 2$. Suppose $|Y| \neq 2^{n-1}$ and $|Y| \neq 2^n$. Then there exist at least three hyperplanes of $\mathbb{P}G(n, 2)$ which contain more than $|Y|/2$ points of Y.*

Proof. By induction on n. The case $n = 2$ is easily verified. Fix $n \geq 3$. Since Y is affine there exists a hyperplane K which misses Y. Let K_∞ be any hyperplane of K. Denote by M and N the other two hyperplanes of $\mathbb{P}G(n, 2)$ which contain K_∞. Let $m = |M \cap Y|, n = |N \cap Y|$ where without loss of generality $m \geq n$. Then $m + n = |Y|$. □

We consider two cases.

Case I. For every choice of K_∞ we have $m > |Y|/2$. In this case, since there are at least three distinct choices for K_∞ and since $K_\infty = M \cap K$ we get at least three distinct hyperplanes M_1, M_2, and M_3 each containing more than $|Y|/2$ points of Y.

Case II. There exists M with $m = |Y|/2$. Then $M \cap Y$ is an affine subset of M and $|M \cap Y| \neq 2^{n-2}, 2^{n-1}$. Therefore by induction there exist at least three hyperplanes Ω_1, Ω_2, and Ω_3 of M which contain more than half of the $|Y|/2$ points of $M \cap Y$. Let R_i, N_i, and M be the three hyperplanes of $\mathbb{P}G(n, 2)$ which contain Ω_i for $i = 1, 2, 3$. Without loss of generality $|R_i \cap Y| \geq |N_i \cap Y|$. Then the three hyperplanes R_i each contain more than half of the points of Y. Finally since $R_i \cap M = \Omega_i$ we see that the hyperplanes R_1, R_2, and R_3 are distinct. □

Remark. One can prove a stronger version of Lemma 3.5 where the restrictions on $|Y|$ are replaced by the restrictions $Y \ncong \mathbb{A}G(n-1, 2)$ and $Y \ncong \mathbb{A}G(n, 2)$.

Now we proceed with the proof of Corollary 2.7. Let J be one of the hyperplanes of H guaranteed by Lemma 3.5 which contains more than half of the points of SH. Then $|J \cap SH| > 2^{n-3} + 2^{n-5} + \epsilon/2$. There are two hyperplanes U and V, different from H which contain J. Since all the points of S not in H lie in $U \cup V$ at least one of these hyperplanes, say U, satisfies $|SU| > |S|/2$.

Notation. Write $|SU| = |S|/2 + \theta$ where $\theta \geq 1$.

By Lemma 3.1, SU is an affine cap in U. Thus there is an hyperplane U_∞ of U which misses S. Let C and D be the two hyperplanes of Σ other than U which contain U_∞. Now since $U \neq H$ the two sets $\{A, B\}$ and $\{C, D\}$ are different. Hence we may suppose that $C \neq A$ and $C \neq B$. Also $C \neq H$ since $SU \cap C = \emptyset$, whereas $SU \cap H = SJ \neq \emptyset$. Therefore $C \in \{A, B, H\}$.

We have $|SC| + |SD| + |SU| = |S|$. Therefore, $|SC| = |S|/2 - \theta - |SD| \leq |S|/2 - \theta - 2^{n-3}$ by Lemma 3.4, i.e., $|SC| \leq 2^{n-3} + 2^{n-4} - \theta$. Of the points in the set SC at least $2^{n-3} + 2^{n-5} - \epsilon/2$ lie on H by Lemma 3.3. Therefore, $SC \cap A \leq (2^{n-3} + 2^{n-4} - \theta) - (2^{n-3} + 2^{n-5} - \epsilon/2) = 2^{n-5} - \theta + \epsilon/2$. By Lemma 3.4, $|SA| \geq 2^{n-3}$ and hence $|SA \setminus SC| \geq 2^{n-3} - (2^{n-5} - \theta + \epsilon/2) = 2^{n-3} - 2^{n-5} + \theta - \epsilon/2$. Similarly $|SB \setminus SC| \geq 2^{n-3} - 2^{n-5} + \theta - \epsilon/2$.

Using Lemma 3.4 this last number is at least 1 and thus there exists at least one point in SB and not in SC. Let us denote it by p_0. Similarly, there exists q_0 in $SA \setminus SC$. Working in A, let Ω_A denote the third member of the pencil of hyperplanes determined by H_∞ and $C \cap A$. Form the hyperplane Ω of Σ containing Ω_A and p_0. Put $\Omega_B := \Omega \cap B$.

Recall that a point is an *affine* point of A (respectively, B, H) if it is a point of A (respectively, B, H) not on H_∞. Note that all points of SA, SB, and SH are affine. Also the points of SA are partitioned by $A \cap C$ and Ω_A. Similarly, the points of SB are partitioned by $B \cap C$ and Ω_B because $C \cap B, H_\infty$ and Ω_B form a pencil in B (due to the fact that $C \cap A$ and $C \cap B$ both contain $C \cap H_\infty$).

Now let $p_1 = p_0$ and p_2 be two points of SB with $p_1 = p_0$ in Ω_B and let q_1 and q_2 be two points of $SA \setminus SC$. Then q_1 and q_2 are points of Ω_A. The points $r_i := p_i + q_i$ are affine points of H. Suppose $r_1 = r_2$. Now $p_1, q_1 \in \Omega$ implies $p_1 + q_1 \in \Omega$. Since q_2 is also in Ω, this implies that the line joining $p_2 + q_2 = p_1 + q_1$ to q_2 is in Ω, i.e., $p_2 \in \Omega$. In summary, if $p_2 \notin \Omega_B$ then $p_1 + q_1 \neq p_2 + q_2$.

Assume, by way of contradiction, that there exists $p_2 \in SB \setminus \Omega$. Forming all the points $p_1 + q$ and $p_2 + q$ for $q \in SA \setminus SC$ gives us a set of affine points of H which are not in S, since S is a cap, and this set is of size $2|SA \setminus SC| = 2|S\Omega_A|$. From the above, $2|S\Omega_A| \geq 2^{n-2} - 2^{n-4} + 2\theta - \epsilon$. However, the total number of affine points of H not in S is $2^{n-1} - |SH| = 2^{n-1} - (2^{n-2} + 2^{n-4} + \epsilon) = 2^{n-2} - 2^{n-4} - \epsilon$. Thus $2^{n-2} - 2^{n-4} + 2\theta - \epsilon \leq 2^{n-2} - 2^{n-4} - \epsilon$. This contradicts $\theta \geq 1$. We conclude that there is no point in $SB \setminus \Omega$ so that $SB \setminus SC = SB$.

Let $q_1 = q_0$ be a point of $SA \setminus SC$. From the definition, it follows that the hyperplane containing Ω_B and q_1 is Ω. Assume, by way of contradiction, that there exists $q_2 \in SA \cap C$. In particular, $q_2 \notin \Omega$. Hence if p_1, p_2 are in Ω_B then, repeating a previous argument, $p_1 + q_1 \neq p_2 + q_2$. Therefore, as above, forming all points $q_1 + p$ and $q_2 + p$ where p is in $SB \setminus SC = SB$ gives a set of affine points in H not in S. By Lemma 3.4, $|SB| \geq 2^{n-3}$ so this set of affine points in H not in S has cardinality at least $2(2^{n-3}) = 2^{n-2}$. Again, as above this gives $2^{n-2} \leq 2^{n-2} - 2^{n-4} - \epsilon$, a contradiction. We conclude that there are no points q_2 in $SA \cap C$. Thus $C \cap SA = \emptyset$. Using the same argument but interchanging the roles of A and B we obtain $C \cap SB = \emptyset$.

Next, assume, by way of contradiction, that $D \neq A$ and $D \neq B$. Then $D \neq H$ since $SU \cap D = \emptyset$ whereas $SU \cap H = SJ \neq \emptyset$. Interchanging the roles of C and D then gives that $D \cap SA = \emptyset$ and $D \cap SB = \emptyset$. Now SA, SB, and SJ are disjoint subsets of SU. From Lemma 3.4, $SA \geq 2^{n-3}$ and $SB \geq 2^{n-3}$. By definition, $|SJ| > (2^{n-2} + 2^{n-4} + \epsilon)/2$. Therefore $|SU| > 2^{n-3} + 2^{n-3} + (2^{n-2} + 2^{n-4} + \epsilon)/2 > 2^{n-2} + 2^{n-3} + 2^{n-5}$. But $|SH| = 2^{n-2} + 2^{n-4} + \epsilon \leq 2^{n-2} + 2^{n-3}$ by Lemma 3.4. Thus $|SU| > |SH|$, contradicting the maximality of SH. Therefore either $D = A$ or $D = B$.

From Lemma 3.5 there exist at least three choices for the hyperplane J of H. Let J_1, J_2, and J_3 be 3 distinct hyperplanes of H with each containing more than $|SH|/2$ points of S. Recall that from J we constructed U, C, and D. Thus from J_i we obtain U_i, C_i, and D_i where $C_i \cap SA = C_i \cap SB = \emptyset$, forcing D_i to be either A or B for $i = 1, 2, 3$. Without loss of generality $D_1 = D_2 = B$. Since $A \cap B = H_\infty$ we have $SA \cap D_1 = SA \cap D_2 = \emptyset$. In particular, $SA \cap C_1 = \emptyset$. Then $SA \cap C_1 = SA \cap D_1 = \emptyset$. Since C_1, D_1 and U_1 form a pencil of hyperplanes in Σ we obtain $SA \subset U_1$. Similarly $SA \subset U_2$. Furthermore, since the three J_i are distinct, and $J_i = U_i \cap H$ for $i = 1, 2, 3$ we have that the three U_i are distinct. In particular, SA is contained in the 3 distinct hyperplanes A, U_1, and U_2.

Finally we assume, by way of contradiction, that A, U_1, and U_2 are a pencil of hyperplanes on $A \cap U_1 = A \cap U_2 = U_1 \cap U_2$. Then $H = (U_1 \cap H) \cup (U_2 \cap H) \cup (A \cap H)$. Intersecting with S gives $SH = (U_1 \cap SH) \cup (U_2 \cap SH) \cup (A \cap SH) = SJ_1 \cup SJ_2$ since $A \cap SH = \emptyset$. Now $J_1 \subset U_1$ and $J_2 \subset U_2$ implies $J_1 \cap J_2 \subset U_1 \cap U_2 = A \cap U_1$. Intersecting with $S \cap H$ gives $S \cap H \cap J_1 \cap J_2 \subset S \cap H \cap A \cap U_1 = \emptyset$. Since the set on the left side contains SJ_1 and SJ_2 we conclude that SJ_1 and SJ_2 are disjoint subsets of SH. But this contradicts the fact that $|SJ_1|$ and $|SJ_2|$ both exceed $|SH|/2$. This contradiction shows that the three hyperplanes, A, U_1, and U_2, containing SA are linearly independent.

Therefore $|SA|$ is at most 2^{n-3} since SA is an affine subset of A. But by Lemma 3.4 SA has at least 2^{n-3} points. Therefore $SA = (A \cap U_1 \cap U_2) \setminus H_\infty \cong \mathbb{A}G(n-3, 2)$.

We have that SA lies in the $(n-3)$ dimensional subspace $\Lambda_A := A \cap U_1 \cap U_2$. Choose a point q_0 in SB. Form the $(n-2)$ dimensional space Λ generated by q_0 and Λ_A and denote by Λ_B its intersection with B. Then Λ_B is also of dimension $n-3$ since no point of SA lies in B, and $q_0 \notin SA$. Suppose, by way of contradiction, that q is a point of SB which is not in Λ_B. Joining the points q_0 and q to the points of SA yields $2(2^{n-3})$ affine points of H not in S. Thus $|SH| \leq 2^{n-1} - 2(2^{n-3}) = 2^{n-2}$. But $|SH| = 2^{n-2} + 2^{n-4} + \epsilon$ where $\epsilon \geq 1$ and we have a contradiction. Therefore all points of SB lie in $\Lambda_B \setminus H_\infty$. By Lemma 3.4, $|SB| \geq 2^{n-3}$. Therefore $SB = \Lambda_B \setminus H_\infty \cong \mathbb{A}G(n-3, 2)$. In particular, $|SB| = 2^{n-3}$.

Since $|S| = 2^{n-1} + 2^{n-3}$, it follows that $|SH| = 2^{n-1} - 2^{n-3}$. Moreover, since S is a cap we have that the points of SH are all the affine points of H that do not lie in the subspace Λ. Thus S is obtained by the construction for X_n described at the beginning of this section. $\square$

It is interesting to note that this proof establishes Corollary 2.7 without invoking the hypothesis of maximality there. Thus we have in fact proved the following result.

Corollary 3.6. *Let $n \geq 3$. In $\mathbb{P}G(n, 2)$ let S be a cap with S not affine. Then $|S| \leq 2^{n-1} + 2^{n-3}$. If $|S| = 2^{n-1} + 2^{n-3}$ then the structure of S is known and is unique.*

4. SOME PROPERTIES OF X_n

Our proof of Corollary 2.7 given above has the advantage of pointing the way to obtaining several interesting combinatorial and geometric properties of X_n. We state a few of these here.

Proposition 4.1. *All but 15 of the hyperplanes of $\mathbb{P}G(n, 2)$ where $n \geq 3$ meet X_n in exactly $|X_n|/2$ points. Each of these hyperplane intersections forms a copy of X_{n-1}. Of the remaining 15 hyperplanes , 5 of them $A_1, \ldots, A_5$ meet X_n in exactly 2^{n-3} points and the other 10 hyperplanes $H_1, \ldots, H_{10}$ meet X_n in exactly $2^{n-1} - 2^{n-3}$ points. The*

15 *hyperplanes form a structure isomorphic to the hyperplanes of* $\mathbb{P}G(3,2)$ *in which* $A_1,\ldots,A_5$ *are the tangent planes to an ovoid* $\mathcal{O}$ *and* $H_1,\ldots,H_{10}$ *are the secant planes of* $\mathcal{O}$.

Thus for every hyperplane K of Σ the cardinality of $X_n \cap K$ is one of the three numbers $\{2^{n-1}-2^{n-3}, 2^{n-2}+2^{n-4}, 2^{n-3}\}$ if $n \geq 3$. For X_3, only the sizes 3 and 1 occur. Hence X_3 is a *2-character* set and for $n \geq 4$, X_n is a *3-character* set.

Using our explicit construction of X_n (or invoking the general result of Theorem 2.6 implying that X_n is obtained by applying the doubling construction) one can see that the five hyperplanes $A_1 \cdots A_5$ partition X_n into 5 disjoint sets: $X_n = (X_n \cap A_1) \sqcup \cdots \sqcup (X_n \cap A_5)$. Symmetrically each point of X_n lies in exactly 6 of the hyperplanes $H_1,\ldots,H_{10}$.

Proposition 4.2. *The automorphism group of* X_n *consists of the group of matrices of the form*

$$\left(\begin{array}{c|c} A & 0 \\ \hline C & B \end{array}\right)$$

where $A \in \mathrm{Aut}(X_3) \cong S_5$ (*the symmetric group on* 5 *letters*), *with* A *a* 4×4 *matrix*, $B \in \mathrm{Aut}(\mathbb{P}G(n-4,2))$, *and* C *any matrix of size* $(n-3) \times 4$.

We give a very rough sketch of the proof as follows. We examine the set of secants to X_n. Using our explicit geometric construction of X_n (or invoking the general doubling result stated in Theorem 2.6) one sees that Σ is the disjoint union of three sets: $\Sigma = X_n \sqcup V \sqcup Z$ where every point of V lies on exactly $|X_n|/2$ secants and every point of Z lies on exactly $|X_n|/5 = 2^{n-3}$ secants. Each point of V is (see our previous definition) a vertex for X_n. Moreover, V is the set of points in a copy of $\mathbb{P}G(n-4,2)$. The submatrix B acts on V. The submatrix A acts on the copy of $\mathbb{P}G(3,2)$ containing the copy of X_3 from which X_n is constructed by the doubling construction. It is easy to verify that $\mathrm{Aut}(X_3) \cong S_5$. In this way one can show that $\mathrm{Aut}(X_n)$ is as described in Proposition 4.2. □

Note added in Proof. We have now determined the complete structure of all maximal caps in $\mathbb{P}G(n,2)$ whose size is at least $2^{n-1}+1$.

ACKNOWLEDGMENTS

We are grateful to two anonymous referees for their very careful and helpful reports. This research is partially supported by NSERC grants.

REFERENCES

[1] R. C. Bose and J. N. Srivastava, *On a bound useful in the theory of factorial designs and error correcting codes*, Ann. Math. Stat. **35,** No. 1, (1964), 408–414.

[2] W. Edwin Clark, *Blocking sets in finite projective spaces and uneven binary codes*, Discrete Math. **94** (1991), 65–68.

[3] W. E. Clark, L. A. Dunning, and D. G. Rogers, *Binary Set Functions and Parity Check Matrices*, Discrete Math. **80** (1990), 249–265.

[4] A. A. Davydov and L. M. Tombak, *Quasiperfect linear binary codes with distance 4 and complete caps in projective geometry*, Problems of Information Transmission **25** No. 4 (1990), 265–275.

[5] T. Helleseth, *On the covering radius codes*, Discr. Appl. Math. **11,** No. 2 (1985), 151–173.

[6] R. Hill, *Caps and Codes*, Discrete Math. **22** No. 2, (1978), 111–137.

[7] J. H. B. Kemperman, *On small sumsets in an Abelian group*, Acta. Math. Stockholm **103,** Nos. 1–2 (1960), 62–88.

[8] M. Kneser, *Ein Satz über abelschen Gruppen mit Anwendungen auf die Geometrie der Zahlen*, Math. Z. **61** (1955), 429–434.

[9] ——— , *Summenmengen in lokalkompakten abelschen Gruppen*, Math. Z. **66** (1956), 88–110.

[10] B. Segre, *Introduction to Galois geometries*, Atti. Accad. Naz. Lincei Memorie **8** (1967), 133–236.

[11] G. Tallini, *On Caps of Kind s in a Galois r-dimensional space*, Acta Arithmet. **7,** No. 1, (1961), 19–28.

[12] W. T. Tutte, *Colouring problems*, Math. Intelligencer **0** (1977), 72–75.