Journal of Combinatorial Theory, Series A **94**, 196–202 (2001)
doi:10.1006/jcta.2000.3143, available online at http://www.idealibrary.com on IDEAL®

NOTE

New Codes from Old; A New Geometric Construction[1]

Aiden A. Bruen

Department of Mathematics, University of Western Ontario, London, Ontario N68 3K7, Canada
E-mail: bruen@uwo.ca

and

David L. Wehlau

Department of Mathematics and Computer Science, Royal Military College, Kingston, Ontario K7K 7B4, Canada
E-mail: wehlau@mast.queensu.ca

Communicated by the Managing Editors

Received July 14, 1999

We describe a new technique for obtaining new codes from old ones using geometric methods. Several applications are described. © 2001 Academic Press

1. INTRODUCTION

We want to provide some background from coding theory and geometry. Let C be a binary linear code of length N, dimension k, and minimum distance at least 4. Let G be a generator matrix for C of size $k \times N$. Then $C^{\perp}$ has length N and dimension $N-k$. Put $N-k=n+1$. A basis for $C^{\perp}$ gives a matrix M of size $(n+1) \times N$. Since C has minimum distance at least 4 it follows that the columns of M form a set S of N points in $\Sigma = \mathbb{PG}(n, 2)$ with no 3 collinear. Such a set S with no three of its points collinear is called a cap.

Let us say that C is extendable if C can be embedded as a subspace of codimension 1 in a binary linear code D of dimension $k+1$, length $N+1$ and minimum distance at least 4. Otherwise C is said to be inextendable or

[1] Research partially supported by NSERC and ARP.

0097-3165/01 $35.00

non-lengthening. One can show that C is non-lengthening (inextendable) if and only if the covering radius of C is 2.

The geometric result is that C is non-lengthening if and only if S is not properly contained in a larger cap in the same space $\Sigma = \mathbb{PG}(n, 2)$, i.e., if and only if the cap S is complete.

Again, start with C. As above we get a set S in $\Sigma = \mathbb{PG}(n, 2)$ from $C^{\perp}$. Using the ideas above, if C is extendable then S is properly contained in a cap S_1 of Σ with $|S_1| = |S| + 1$. Since the size of the largest cap in Σ is $2^n = 2^{N-k-1}$ we see that after a finite number of steps, the process of lengthening must stop. In this way every binary linear code C of minimum distance at least 4 is embedded in a non-lengthening binary linear code D of minimum distance at least 4. This brings out the crucial role of such non-lengthening codes or equivalently of complete caps in $\Sigma = \mathbb{PG}(n, 2)$.

A much-studied construction, the Plotkin doubling construction preserves completeness. This process has the effect of doubling the length of C and increasing its dimension (by a factor greater than 2). In this note we provide a new construction (black/white lifting) for getting new codes from old. Like the Plotkin construction black/white lifting increases the dimension by a factor greater than 2 but the length increases by a factor less than 2. Several new results are shown using this black/white construction.

2. A NEW CONSTRUCTION

We begin with some basic definitions.

A *cap* is a set of points in $\Sigma = \mathbb{PG}(n, 2)$ having no three of its points collinear. We say that a cap is *complete* or *maximal* if it is not a proper subset of any other cap in Σ.

Given a subset A of $\Sigma = \mathbb{PG}(n, 2)$, a *vertex* for A is a point v such that $v + A = A$. A subset A of Σ is said to be periodic if it has at least one vertex.

Given a complete cap S in $\Sigma = \mathbb{PG}(n, 2)$ one may easily construct from S a complete cap $\phi(S)$ in $\tilde{\Sigma} = \mathbb{PG}(n+1, 2)$ by the *Plotkin* or *doubling* construction as follows. We choose a point $v \in \tilde{\Sigma} \backslash \Sigma$ and define

$$\phi(S) = S \sqcup \{v + s \mid s \in S\}.$$

Clearly $|\phi(S)| = 2\,|S|$ and $\phi(S)$ is periodic with v as a vertex.

In [DT], Davydov and Tombak showed that if S is a complete cap in $\Sigma = \mathbb{PG}(n, 2)$ with $|S| \geqslant 2^{n-1} + 2$ then $S = \phi(S_1)$ where $S_1 = S \cap \Sigma_1$ is a complete cap in some hyperplane $\Sigma_1 \cong \mathbb{PG}(n-1, 2)$ of Σ. Thus if S is a complete cap in $\Sigma = \mathbb{PG}(n, 2)$ with $|S| = 2^t r \geqslant 2^{n-1} + 2$ where r is odd then $S = \phi^t(S')$ where S' is a complete cap in some subspace $\Sigma' \cong \mathbb{PG}(n-t, 2)$

of Σ. Furthermore $|S'| = t = 2^{n-t-1} + 1$ and $|S| = 2^{n-1} + 2^t$. We call a cap S of $\Sigma = \mathbb{PG}(n, 2)$ *large* if $|S| \geqslant 2^{n-1} + 1$, and *small* if $|S| \leqslant 2^{n-1}$.

DEFINITION 2.1. Let S be a cap in $\Sigma = \mathbb{PG}(n, 2)$. Given a point x of Σ not lying in S we partition the set S into two subsets as follows. The *Black points* of S with respect to x are the points

$$\mathscr{B}(x, S) := \{s \in S \mid x + s \in S\}.$$

The *White points* of S with respect to x are the points

$$\mathscr{W}(x, S) := \{s \in S \mid x + s \notin S\}.$$

In geometric language $\mathscr{B}(x, S)$ and $\mathscr{W}(x, S)$ are the secant and tangent cones of x respectively.

Next we define our construction of new caps from old ones. Let S be a complete cap in $\Sigma = \mathbb{P}G(n, 2)$ with w any point of $\Sigma \backslash S$. Embed Σ in a projective space $\tilde{\Sigma}$ of one dimension more. Fix $v \in \tilde{\Sigma} \backslash \Sigma$. We will construct a new cap $\psi_w(S)$ in $\tilde{\Sigma} = \mathbb{P}G(n+1, 2)$. We define

$$\psi_w(S) := S \sqcup \{x + v \mid x \in \mathscr{W}(w, S)\} \sqcup \{v + w\}.$$

We call $\psi_w(S)$ the *black/white lift of S* and we call v the apex. Note that $\psi_w(S) \cap \Sigma = S$.

THEOREM 2.2. *Let S be a cap in $\Sigma = \mathbb{PG}(n, 2)$, w a point of $\Sigma \backslash S$ and $\tilde{\Sigma} = \mathbb{P}G(n+1, 2)$ the projective space generated by an apex v together with the space Σ. Then $\psi_w(S)$ is a cap in $\tilde{\Sigma}$ with $|\psi_w(S)| = |S| + |\mathscr{W}(w, S)| + 1 = 2\,|S| - |\mathscr{B}(w, S)| + 1$.*

Proof. Write $w' = w + v$. Since $\psi_w(S) \backslash \{w'\}$ is contained in the Plotkin double of S we see that any line in $\psi_w(S)$ would have to pass through w'. Assume, by way of contradiction, that $\psi_w(S)$ does contain a line $\{w', u', z\}$ where without loss of generality $u' \notin \Sigma$ and $z \in S$. Since $w \notin S$, this line cannot contain v. Thus we may project the line from v into Σ to obtain a line $\{w, u = u' + v, z\}$. Since $u' \in \psi_w(S) \backslash w'$, we have $u \in S$. Therefore, $u, z \in \mathscr{B}(w, S)$. But then, by the definition of $\psi_w(S)$, this means that $u' \notin \psi_w(S)$. This contradiction shows that $\psi_w(S)$ is a cap. The formulae for $|\psi_w(S)|$ are clear. ∎

For further developments we need some more definitions.

DEFINITION 2.3. Let S be a cap in $\Sigma = \mathbb{PG}(n, 2)$. A point, w, of $\Sigma \backslash S$ is *dependable* or a *dependable point for S* if there does not exist any other point $x \in \Sigma \backslash S$ with $\mathscr{W}(w, S) \subseteq \mathscr{W}(x, S)$, i.e., if every point $x \in \Sigma \backslash S$ different from w satisfies $\mathscr{B}(w, S) \not\supseteq \mathscr{B}(x, S)$.

In particular, if a point $w \in \Sigma \backslash S$ lies on exactly one secant line to S, then w is dependable. We emphasize this important special case as follows.

Definition 2.4. Let S be a cap in $\Sigma = \mathbb{PG}(n, 2)$. A point, x, of Σ is a *faithful point* or a *faithful point for* S if x lies on a unique secant to S, i.e., if $|\mathscr{B}(x, S)| = 2$.

Proposition 2.5. *Let S be a complete cap in $\Sigma = \mathbb{PG}(n, 2)$ obtained by a sequence of Plotkin doublings beginning with a cap S' in $\mathbb{PG}(n-t, 2)$, i.e., $S = \phi^t(S')$. Let x be a point of Σ which is not in S and is not a vertex of S. Then the number of secants to S through x is divisible by 2^t.*

Proof. The proof is by induction on t. The result is trivial for $t = 0$. Suppose we have proved the result for $t-1$ and let S be a cap with $S = \phi^t(S')$ in $\Sigma = \mathbb{PG}(n, 2)$ where $S_1 := \phi^{t-1}(S') \subset \Sigma_1 \cong \mathbb{PG}(n-1, 2)$ and v is a vertex of S which is not contained in Σ_1. This means that we may consider S as having been obtained from S_1 by Plotkin doubling using the vertex v. Note that we may also view S as having been obtained by doubling from v the cap $v + S_1$ contained in the hyperplane $v + \Sigma_1$. Let x be any point of $\Sigma \backslash S$ with x not a vertex of S. Replacing Σ_1 by $v + \Sigma_1$ if necessary we may assume that $x \in \Sigma_1$. If x is a vertex of S_1, then $x + S_1 = S_1$ and therefore $x + S = x + (S_1 \sqcup (v + S_1)) = (x + S_1) \cup (v + x + S_1) = S_1 \cup (v + S_1) = S$, contradicting our assumption that x is not a vertex of S.

Therefore x cannot be a vertex of S_1 and thus by the induction hypothesis, the number of secants to S_1 through x is $r(2^t)$ for some integer r.

Consider one of these secants to S_1, $\{x, y, z\}$ where $y, z \in S_1 \subset S$. The points $y' := y + v$ and $z' = z + v$ lie in S. Then x lies on the two secants to S, $\{x, y, z\}$ and $\{x, y', z'\}$. Thus each secant of S_1 through x gives rise to two secants to S through x.

Conversely if u', w', x is some secant line to S not entirely contained in Σ_1 then we see that $u' + v, w' + v, x$ is a secant line to S_1 which is contained in Σ_1. Thus every secant line to S through x arises in the above manner from a secant line to S_1 through x. ∎

Corollary 2.6. *If $S = \phi(S_1)$ is a complete periodic cap in $\Sigma = \mathbb{PG}(n, 2)$ with $n \geqslant 2$ then there are no faithful points for S.*

Proof. The corollary follows easily from the preceding theorem and the fact that for $n \geqslant 2$ every complete cap has at least 4 points. ∎

For emphasis we mention a special case of the above corollary. Let S be a large complete cap in $\mathbb{PG}(n, 2)$. Then by the result of [DT] described above, $S = \phi^t(S')$ for some $t \geqslant 0$ and some cap S' in $\mathbb{PG}(n-t, 2)$ with $|S'| = 2^{n-t-1} + 1$. Therefore if $S \subset \mathbb{PG}(n, 2)$ is a large complete cap having a faithful point then $|S| = 2^{n-1} + 1$.

The following partial converse to the preceeding is proved in [BW, Theorem 13.8].

Proposition 2.7. *If S is a complete cap in $\Sigma = \mathbb{PG}(n, 2)$ with $|S| = 2^{n-1} + 1$ then there exists a faithful point w for S.*

We next consider how the black/white lift behaves when applied to complete caps.

Theorem 2.8. *Let S be a complete cap in $\Sigma = \mathbb{PG}(n, 2)$ where $n \geqslant 2$ with w a dependable point for S. Then the set $\psi_w(S)$ is a complete cap in $\tilde{\Sigma} = \mathbb{PG}(n+1, 2)$.*

Proof. We show that $\psi_w(S)$ is complete. Let x' be a point of $\tilde{\Sigma}$ not contained in $\psi_w(S)$. If $x' \in \Sigma$ then x' lies on a secant to S so we may suppose that $x' \notin \Sigma$. The point v lies on the secant line $\{v, y, y+v\}$ for every $y \in \mathscr{W}(w, S)$. Since w is dependable we must have $\mathscr{W}(w, S) \neq \varnothing$ and thus $x' \neq v$.

Consider the point $x = v + x' \in \Sigma$. If $x \in S$ then $x \in \mathscr{B}(w, S)$ since $x' \notin \psi_w(S)$. But then x' lies on the secant line to $\psi_w(S)$ given by $\{w', w+x, x'\}$. Thus we may suppose that $x \notin S$. Now since w is dependable for S there exists $y \in \mathscr{W}(w, S) \backslash \mathscr{W}(x, S)$. Since $y \in \mathscr{W}(w, S)$, we have $y' = y + v \in \psi_w(S)$. Since $y \notin \mathscr{W}(x, S)$, we have $y, x + y \in S$. Therefore x' lies on the secant line $\{(y+x), y', x'\}$ to $\psi_w(S)$. ∎

Now we are able to give an interesting application of our new construction. It is clear that if A and B are two distinct complete caps then $|A \cap B| \leqslant |A| - 1$. Here we show that this bound is actually attained, even when A and B contain a large number of points. To see this take any maximal cap S having a faithful point w and consider the two complete caps $\phi(S)$ and $\psi_w(S)$. We have that $|\phi(S) \cap \psi_w(S)| = |\psi_w(S)| - 1 = |\phi(S)| - 2$.

3. PROPERTIES OF THE BLACK/WHITE LIFT

In Proposition 2.7 we pointed out the existence of faithful points for certain important caps (the so-called critical caps—see [BW, DT]). Our construction provides many examples of complete caps having many faithful points.

PROPOSITION 3.1. *Let $S \subset \Sigma = \mathbb{PG}(n, 2)$ be a complete cap with w a dependable point for S. Let $x \in \mathcal{B}(w, S)$ and write $x' = v + x$ and $w' = v + w$. Then $\mathcal{B}(x', \psi_w(S)) = \{w', w + x\}$. In other words, each point of $v + \mathcal{B}(w, S)$ is a faithful point of $\psi_w(S)$.*

Proof. Since $x \in \mathcal{B}(w, S)$, $x' \notin \psi_w(S)$. Since $\psi_w(S)$ is a complete cap there exist two points $y, x' + y \in \mathcal{B}(x', \psi_w(S))$ with $y \in \Sigma$. Now $\{x, x + y, y\}$ is a line in Σ with $x, y \in S$. Thus, $x + y \notin S$ even though $(x + y) + v = x' + y \in \psi_w(S)$. Therefore, $x + y = w$ and $x' + y = w'$ and thus $y = w' + x' = w + x$. In other words, every secant to $\psi_w(S)$ through x' contains $w + x$, showing that there is only one secant, i.e., that x' is a faithful point for $\psi_w(S)$. ∎

PROPOSITION 3.2. *Let $S \subset \Sigma = \mathbb{P}G(n, 2)$ be a cap and take $x \in \Sigma \setminus S$. Then*

(1) $\mathcal{W}(x, \psi_w(S)) \cap \Sigma = \mathcal{W}(x, S)$,

(2) $\mathcal{B}(x, \psi_w(S)) \cap \Sigma = \mathcal{B}(x, S)$ *and*

(3) $\mathcal{B}(w, \psi_w(S)) = \mathcal{B}(w, S)$.

Proof. (1) and (2) are left to the reader. For (3), assume by way of contradiction that we have $y', z' = y' + w \in \mathcal{B}(w, \psi_w(S)) \setminus \Sigma$. Then both $y = y' + v$ and $z = z' + v$ must lie in $\mathcal{W}(w, S)$. But this cannot be because $y + z = w$. ∎

THEOREM 3.3. *Let $S \subset \mathbb{PG}(n, 2)$ be a cap with a dependable point w. Form the black/white lift of S, $\psi_w(S) \subset \mathbb{PG}(n + 1, 2)$ using the apex v. Then w is a dependable point for $\psi_w(S)$.*

Proof. We proceed by contradiction. Thus we assume that there exists a point $x' \notin \psi_w(S)$ such that $\mathcal{W}(w, \psi_w(S)) \subseteq \mathcal{W}(x', \psi_w(S))$. If $x' \in \Sigma$ then applying Proposition 3.2(1) we have $\mathcal{W}(w, S) \subseteq \mathcal{W}(x', S)$ violating the dependability of w for S. Thus we must have $x' \notin \Sigma$.

Now we show that $x' \neq v$ as follows. Since w is dependable, there exists $y \in \mathcal{W}(w, S)$. Then y and $y' = y + v$ both lie in $\psi_w(S)$ and thus $y \notin \mathcal{W}(v, \psi_w(S))$. Therefore x' cannot be v since $y \in \mathcal{W}(w, \psi_w(S)) \setminus \mathcal{W}(v, \psi_w(S))$.

Suppose that $x := x' + v \in S$. Since $w' := w + v \in \mathcal{W}(w, \psi_w(S)) \subseteq \mathcal{W}(x', \psi_w(S))$, $w' + x' \notin \psi_w(S)$. Thus $w + x \notin S$ which means that $x \in \mathcal{W}(w, S)$. Therefore $x' \in \psi_w(S)$ by the definition of $\psi_w(S)$. This contradiction shows that $x \notin S$.

Finally we consider the case $x \notin S$. Since w is dependable for S, there exists a point $y \in \mathcal{W}(w, S) \setminus \mathcal{W}(x, S)$. Thus $y \in S$ and $y + x \in S$ but $y + w \notin S$. Therefore $y' = y + v \in \psi_w(S)$ and $y' + w = (y + v) + w \notin \psi_w(S)$. This means that $y' \in \mathcal{W}(w, \psi_w(S)) \subseteq \mathcal{W}(x', \psi_w(S))$. Therefore $y + x = y' + x' \notin \psi_w(S)$. But we have already shown that $y + x \in S$. This contradiction completes the proof. ∎

4. SMALL COMPLETE CAPS

The structure of all large complete caps is now known (see [BW, DT]). However, this is not so for small complete caps. Indeed not even the cardinalities which occur are known. Here we sketch an example which illustrates how black/white lifting can be exploited to construct small complete caps. In [FHW, p. 294] a cap $C_3 \subset \mathbb{PG}(5, 2)$ of cardinality 12 is exhibited. As is easily verified, C_3 can be extended to only one complete cap, $\mathscr{H} \subset \mathbb{PG}(5, 2)$ and this cap has cardinality 13. The cap, $\mathscr{H}$, contains many faithful points. Let w denote one of these. We define new small complete caps via $\mathscr{H}_5 := \mathscr{H}$ and $\mathscr{H}_{i+1} := \psi_w(\mathscr{H}_i) = \psi_w^{i-4}(\mathscr{H})$ for $i \geqslant 5$. Thus $\mathscr{H}_n \subset \mathbb{PG}(n, 2)$ with $|\mathscr{H}_n| = 3(2^{n-3}) + 1$ and $|\mathbb{PG}(n, 2)| = 2^{n+1} - 1$ for $n \geqslant 5$. By Theorem 2.8 these new caps $\mathscr{H}_n$ are all complete.

Note that in the above construction we could have instead chosen a different faithful or dependable point for each lift.

Furthermore there exist dependable points w_0 for $\mathscr{H}$ with $|\mathscr{B}(w, \mathscr{H})| = 6$. In light of Theorem 3.3, using such a point w_0 in the role of w in the above construction we obtain complete caps $\psi_{w_0}^n(\mathscr{H}) \subset \mathbb{PG}(n, 2)$ with $|\psi_{w_0}^n(\mathscr{H})| = 2^{n-2} + 5$.

REFERENCES

[BW] A. A. Bruen and D. L. Wehlau, Long binary linear codes and large caps in projective space, *Des. Codes Cryptogr.* **17** (1999), 37–60.

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

[FHW] J. Fugère, L. Haddad, and D. Wehlau, 5-Chromatic Steiner triple systems, *J. Combin. Des.* **2**, No. 5 (1994), 287–299.

Printed in Belgium