JOURNAL OF COMBINATORIAL THEORY, Series A 43, 331–333 (1986)

Note

Cyclic Projective Planes and Binary, Extended Cyclic Self-Dual Codes

VERA PLESS*

Mathematics Department, University of Illinois at Chicago, Chicago, Illinois 60680

Communicated by the Managing Editors

Received August 27, 1985

If P is a cyclic projective plane of order n, we give number theoretic conditions on n^2+n+1 so that the binary code of P is contained in a binary cyclic code C whose extension is self-dual. When this containment occurs C does not contain any ovals of P. As a corollary to these conditions we obtain that the extended binary code of a cyclic projective plane of order 2^s is contained in a binary, extended cyclic self-dual code if and only if s is odd.

We assume a familiarity with concepts in the areas of error-correcting codes and projective planes which can be found in [2, 6, 7]. As is customary the binary code of a projective plane P is the binary code generated by an incidence matrix A of P. If P is a cyclic plane we can, and do, choose A so that C is a cyclic code. In [2] various relations are given between self-orthogonal codes and designs. We continue this study with results about cyclic projective planes and their binary codes.

The next theorem is in [3, 8]. We prove it here since it is interesting that it has a coding proof.

THEOREM 1. *The only cyclic projective plane P of order $n \equiv 2 \pmod 4$ is the projective plane of order* 2.

Proof. The binary, cyclic code C of P has length n^2+n+1 and $\bar{C}$, the extended code of C, is self-dual [2, Theorem 11.7]. Hence the all one vector, h, is in C, C has dimension $(n+1)/2$ and the generating idempotent e of C must have odd weight. Let $\bar{e}$ denote the image of e under the coordinate permutation $i \to -i \pmod{n^2+n+1}$. Then $C^\perp$ has idempotent $1+\bar{e}$ [4] and dimension $(n-1)/2$. Hence $C = C^\perp \perp \langle h \rangle$ so that

* This work was supported in part by the National Science Foundation Grant MCS-8201311.

0097-3165/86 $3.00

$e = (1+\bar{e}) + h + h(1+\bar{e}) = 1 + \bar{e} + h$. As $h = 1 + e + \bar{e}$, the weight of e is $(n^2+n)/2$.

Now C has minimum weight $n+1$ and the lines of P are the only vectors of weight $n+1$ in C [2, Theorem 11.8]. Any binary, cyclic code is invariant under the coordinate permutation $i \to 2i \pmod{n^2+n+1}$ [6, Theorem 6.2] so this permutation clearly sends the lines in P onto themselves. As it has a fixed point, P has an invariant line e of weight $n+1$. Considered as a polynomial e is an idempotent, and as e and its cyclic shifts generate C, e is the generating idempotent of C. Hence $n+1 = (n^2+n)/2$ so that $n=2$.

THEOREM 2. *Let C be the cyclic code of a cyclic projective plane P of order n and let $\bar{C}$ be its extended code. Let $N = n^2+n+1$. Then $\bar{C}$ is contained in a binary, extended cyclic, self-dual code if and only if either $n=2$ or $n \equiv 0 \pmod 4$ and N is a product of primes p where each p is either $\equiv -1 \pmod 8$ or $\equiv 1 \pmod 8$ where the order of $2 \pmod p$ is odd.*

Proof. If n is odd, it is well-known that C has dimension n^2+n which is too large for $\bar{C}$ to be self-dual. Hence n is even and by Theorem 1 if $n \equiv 2 \pmod 4$, $n=2$. If a cyclic projective plane P of even order $n \equiv 0 \pmod 4$ exists, then $\bar{C}$ is self-orthogonal and extended cyclic. Hence $\bar{C}$ will be contained in an extended cyclic, self-dual code, if such exists, of length $N+1$. By [5, Theorem 6], they do exist whenever the conditions in this theorem on N hold.

The following corollary answers questions raised in [4].

COROLLARY. *The binary extended code $\bar{C}$ of a cyclic projective plane P of order 2^s is contained in a binary, extended cyclic, self-dual code if and only if s is odd.*

Proof. If s is even, $N = 2^s + 2^s + 1 \equiv 0 \pmod 3$. By the Theorem, 3 cannot divide N so s must be odd. As $(2^{3s}-1) = (2^s-1)N$, $2^{3s} \equiv 1 \pmod N$. Hence, if s is odd, the order of $2 \pmod N$ is odd. Thus the order of 2 mod each factor of N is odd and Theorem 2 applies.

Note that the binary extended code $\bar{C}$ of a cyclic projective plane P of order 2^s is contained in a binary extended quadratic residue code only when $s=1$ [1].

THEOREM 3. *Let C be a binary, cyclic code which contains the code of a cyclic projective plane of order n. Suppose also that the extended code $\bar{C}$ of C is self-dual. Then C does not contain any ovals of the plane unless $n=2$.*

Proof. As $\bar{C}$ is self-dual and extended cyclic, it is a duadic code [5, Theorem 5]. Hence all even weights in C are $\equiv 0 \pmod 4$ [by Theorem 2 in [5], parts 1 and 4]. As either $n \equiv 0 \pmod 4$ or $n=2$ by Theorem 2, an oval, which has weight $n+2$, cannot be in C unless $n=2$.

Acknowledgments

I wish to acknowledge several very helpful conversations with Dr. John M. Masley, who proved most of the corollary to Theorem 2. I thank Professor Jack van Lint for pointing out references [3] and [8].

References

1. R. Calderbank and D. B. Wales, Multiplying vectors in binary quadratic residue codes, *SIAM J. Algebraic Discrete Methods* **3** (1982), 43–55.
2. P. J. Cameron and J. H. van Lint, "Graph Theory, Coding Theory, and Block Designs," London Math. Soc. Lecture Note Series, No. 19, Cambridge Univ. Press, London, 1975.
3. D. Jungnickel and K. Vedder, On the geometry of planar difference sets, *European J. Combin.* 5 (1984), 143–148.
4. J. S. Leon, J. M. Masley, and V. Pless, Duadic codes, *IEEE Trans. Inform. Theory* **IT-30**, 709–714.
5. V. Pless, J. M. Masley, and J. S. Leon, On weights in duadic codes, *J. Combin. Theory Ser. A*, in press.
6. V. Pless, Introduction to the Theory of Error-Correcting Codes," Wiley–Interscience Series in Discrete Math., Wiley–Interscience, New York, 1982.
7. J. H. van Lint, "Introduction to Coding Theory," Springer-Verlag, New York, 1982.
8. H. A. Wilbrink, A note on planar difference sets, *J. Combin. Theory Ser. A* **38** (1985), 94–95.