[15] ——, "An improvement of the Griesmer bound for some classes of distances," *Probl. Inform. Transm.*, vol. 23, pp. 38–46, 1987.
[16] J. H. Griesmer, "A bound for error-correcting codes," *IBM J. Res. Develop.*, vol. 4, pp. 532–542, 1960.
[17] P. W. Heijnen, "Er bestaat geen binaire $[33, 9, 13]$ code," Afstudeerverslag, Tech. Univ. Delft, Delft, The Netherlands, 1993.
[18] T. Helleseth, "A characterization of codes meeting the Griesmer bound," *Inform. Contr.*, vol. 50, pp. 128–159, 1981.
[19] ——, "New constructions of codes meeting the Griesmer bound," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 434–439, May 1983.
[20] T. Helleseth and H. van Tilborg, "A new class of codes meeting the Griesmer bound," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 548–555, Sept. 1981.
[21] T. Helleseth and Ø. Ytrehus, "How to find a $[33, 8, 14]$ code," *Reports in Informatics (University of Bergen)*, vol. 41, 1989.
[22] D. B. Jaffe. Binary linear codes: New results on nonexistence, preprint (ongoing work). [Online] http://www.math.unl.edu/~djaffe/codes/code.ps.gz or code.dvi.gz; see ...~djaffe/binary/codeform.html for an online database, which is more frequently updated.
[23] ——, "Optimal binary linear codes of length ≤ 30," *Discr. Math.*, to be published.
[24] ——, "A brief tour of split linear programming," in *Proc. AAECC 12 (Lecture Notes in Computer Science)*, T. Mora and H. Mattson, Eds. Springer-Verlag: New York, 1997, vol. 1255, pp. 164–173.
[25] D. B. Jaffe and J. Simonis, "New binary linear codes which are dual transforms of good codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2136–2137, Sept. 1999.
[26] B. K. Kostova and N. L. Manev, "A $[25, 8, 10]$ code does not exist," in *C. R. Acad. Bulg. Sci.*, 1990, vol. 43, pp. 41–44.
[27] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
[28] B. D. McKay, "Practical graph isomorphism," *Congr. Numer.*, vol. 30, pp. 45–87, 1981.
[29] ——, (1990) Nauty User's Guide (Version 1.5). [Online] http://cs.anu.edu.au/people/bdm/nauty19/nauty19p.tar.Z.
[30] P. Piret, "Good linear codes of lengths 27 and 28," *IEEE Trans. Inform. Theory*, vol. IT-26, p. 227, Mar. 1980.
[31] A. Said and R. Palazzo, "Using combinatorial optimization to design good unit-memory convolutional codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1100–1108, May 1993.
[32] J. Simonis, "MacWilliams identities and coordinate partitions," *Linear Alg. Appl.*, vol. 216, pp. 81–91, 1995.
[33] G. Solomon and J. J. Stiffler, "Algebraically punctured cyclic codes," *Inform. Contr.*, vol. 8, pp. 170–179, 1965.
[34] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, "Further results on Goppa codes and their applications to constructing efficient binary codes," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 518–526, Sept. 1976.
[35] H. van Tilborg, "On quasicyclic codes with rate $1/m$," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 628–630, Sept. 1978.
[36] ——, "A proof of the nonexistence of a binary $(55, 7, 26)$ code," Techn. Hogeschool Eindhoven, Eindhoven, The Netherlands, Tech. Rep. 79-WSK-09, 1979.
[37] ——, "The smallest length of binary 7-dimensional linear codes with prescribed minimum distance," *Discr. Math.*, vol. 33, pp. 197–207, 1981.
[38] S. Topalova, "Construction and investigation of combinatorial designs with given automorphisms," PhD dissertation, Inst. Math. and Informatics, Bulgarian Acad. Sci., Bulgaria, 1998.
[39] Ø. Ytrehus and T. Helleseth, "There is no binary $[25, 8, 10]$ code," *IEEE Trans. Inform. Theory*, vol. 36, pp. 695–696, May 1990.
[40] Reference [10] supplemented by on-line updates: information regarding $[n, k, d]$ codes with fixed n, k. [Online] Available: http://www.win.tue.nl/~aeb/voorlincod.html

Adding a Parity-Check Bit

Juriaan Simonis, *Member, IEEE*

***Abstract*—The correspondence gives a new condition for a q-ary linear code of length n and minimum distance d to be extendable to a code of the same dimension, length $n + 1$, and minimum distance $> d$.**

***Index Terms*—Code extension, linear codes, parity-check bit.**

I. Introduction

A binary linear $[n, k, d]$-code $\mathcal{C}$ of odd minimum distance d can be extended to an $[n + 1, k, d + 1]$-code by adding a parity-check bit. This means that codewords of odd weight get an extra coordinate 1 and those with even weight an extra coordinate 0. Since the codewords of even weight in $\mathcal{C}$ constitute a one-codimensional subcode, adding a parity-check bit can be viewed as an application of Construction X. The codimension 1 case of this construction reads as follows. (All codes in this correspondence are supposed to be linear.)

Proposition 1 [6, pp. 581–583]: If an $[n, k, d]_q$-code $\mathcal{C}$ has a one-codimensional subcode $\mathcal{C}_0$ with minimum distance $> d$, then $\mathcal{C}$ can be extended to an $[n + 1, k, d + 1]_q$-code.

Proof: Choose an arbitrary vector $\boldsymbol{x} \in \mathcal{C} \backslash \mathcal{C}_0$. Then the extended code can be taken as the span in $\mathbb{F}_q^{n+1}$ of $(\boldsymbol{x}, 1)$ and the vectors $(\boldsymbol{c}, 0)$, $\boldsymbol{c} \in \mathcal{C}_0$. □

The obvious generalization of parity check extension to codes over a field of size $q > 2$ usually does not yield codes of larger minimum distance. But in 1995, Hill and Lizak proved the following theorem.

Theorem 2 [4], [5]: Let $\mathcal{C}$ be an $[n, k, d]$-code over $\mathbb{F}_q$ with $\gcd(d, q) = 1$ and with all weights congruent to 0 or d (modulo q). Then $\mathcal{C}$ can be extended to an $[n + 1, k, d + 1]$-code, all of whose weights are congruent to 0 or $d + 1$ (modulo q).

The essential step in the proof of this result is the establishment of the fact that the words of weight congruent to 0 modulo q in the codes under consideration form a 1-codimensional subcode. Then Proposition 1 immediately finishes the proof.

The next proposition shows that also something can be said if more than two weights modulo q occur. But then information on the weight distribution of the code must be available. By definition, the *weight distribution* of a code $\mathcal{C}$ is the sequence $(A_i(\mathcal{C}))_{i=0 \cdots n}$, with

$$A_i(\mathcal{C}) := |\{\boldsymbol{c} \in \mathcal{C} \mid \mathrm{wt}(\boldsymbol{c}) = i\}|.$$

Proposition 3: Let $\mathcal{C}$ be an $[n, k, d]$-code over a finite field $\mathbb{F}_q$ of characteristic p, and let t be any integer that is not divisible by p. Then the set

$$\mathcal{C}^{(t)} := \{\boldsymbol{c} \in \mathcal{C} \mid \mathrm{wt}(\boldsymbol{c}) \not\equiv t \bmod p\}$$

is a one-codimensional subcode of $\mathcal{C}$ if and only if its size is right, i.e., if and only if

$$\sum_{i \not\equiv t \bmod p} A_i(\mathcal{C}) = q^{k-1}.$$

Manuscript received November 6, 1999.

The author is with the Faculty of Information Technology and Systems, Delft University of Technology, 2600 GA, Delft, the Netherlands (e-mail: J.Simonis@twi.tudelft.nl).

Communicate by A. M. Barg, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(00)04642-3.

Proof: Let $q := p^r$. Consider the polynomial function

$$\varphi: \mathbb{F}_q^n \to \mathbb{F}_q, \qquad (x_1, x_2, \cdots, x_n) \longmapsto \sum_{i=1}^{n} (x_i)^{q-1}.$$

Actually, φ maps $\mathbb{F}_q^n$ onto the prime field $\mathbb{F}_p$. We can view $\mathbb{F}_q^n$ as an $\mathbb{F}_p$-vector space of dimension rn. The $\mathbb{F}_q$-degree of φ is $q-1$, but what about its $\mathbb{F}_p$-degree? The functions

$$x \longmapsto x^{p^i}, \qquad i = 0, 1, \cdots, r-1$$

are $\mathbb{F}_p$-*linear*. So, decomposing the monomial x^{q-1} as

$$x^{q-1} = x^{p-1}(x^p)^{p-1}(x^{p^2})^{p-1} \cdots (x^{p^{r-1}})^{p-1}$$

we see that the $\mathbb{F}_p$ degree of φ is equal to $r(p-1)$. The function

$$\psi: \mathcal{C} \to \mathbb{F}_p, \qquad \psi(\boldsymbol{c}) = \varphi(\boldsymbol{c}) - t,$$

on the rk-dimensional $\mathbb{F}_p$-vector space $\mathcal{C}$ will have degree at most $r(p-1)$. So ψ defines a word in the generalized Reed–Muller code $\mathcal{R}_p(r(p-1), rk)$. The weight of this word is the size of the support of ψ

$$\mathrm{wt}\,(\psi) = \sum_{i \not\equiv t \bmod p} A_i(\mathcal{C}).$$

It is well known (cf. [2] or [3]) that the minimum weight of $\mathcal{R}_p(r(p-1), rk)$ is equal to $p^{rk-r} = q^{k-1}$, and that the supports of the minimum-weight codewords are the $\mathbb{F}_p$-affine $(rk-r)$-flats in $\mathbb{F}_p^{rk}$. So, if

$$\sum_{i \not\equiv t \bmod p} A_i(\mathcal{C}) = q^{k-1}$$

then

$$\mathcal{C}^{(t)} := \{\boldsymbol{c} \in \mathcal{C} \,|\, \mathrm{wt}\,(\boldsymbol{c}) \not\equiv t \bmod p\}$$

is an $\mathbb{F}_p$-affine $(rk-r)$-flat in the rk-dimensional $\mathbb{F}_p$-vector space $\mathcal{C}$. Since we assumed that $t \not\equiv 0 \bmod p$, the set $\mathcal{C}^{(t)}$ contains the zero vector and hence is an $(rk-r)$-dimensional $\mathbb{F}_p$-*linear* subspace of $\mathcal{C}$. Finally, $\mathcal{C}^{(t)}$ is invariant under scalar multiplication with nonzero elements from $\mathbb{F}_q$. So $\mathcal{C}^{(t)}$ actually is a $(k-1)$-dimensional $\mathbb{F}_q$-linear subspace of $\mathcal{C}$. □

We now can invoke once more Construction X to obtain the following generalization of Hill and Lizak's result.

Theorem 4: Let $\mathcal{C}$ be an $[n, k, d]$-code over a finite field $\mathbb{F}_q$ of characteristic p. If $d \not\equiv 0 \mod p$ and

$$\sum_{i \not\equiv d \bmod p} A_i(\mathcal{C}) = q^{k-1}$$

then $\mathcal{C}$ can be extended to an $[n+1, k, d+1]$-code.

Remark 5: The weight distribution of the (generalized) Reed–Muller codes is known to possess gaps. See, for instance, [3] for a survey. This means that if $\sum_{i \not\equiv d \bmod p} A_i(\mathcal{C})$ is below a certain bound, then it has to be equal to q^{k-1}. We give two examples.

1) If $q := 3$ and $d \not\equiv 0 \bmod 3$, then
$$\sum_{i \not\equiv d \bmod 3} A_i(\mathcal{C}) < 5 \cdot 3^{k-2}$$
implies that
$$\sum_{i \not\equiv d \bmod 3} A_i(\mathcal{C}) = 3^{k-1}.$$
2) If $q := 4$, then
$$\sum_{i\ even} A_i(\mathcal{C}) < 7 \cdot 4^{k-2}$$
implies that
$$\sum_{i\ even} A_i(\mathcal{C}) = 4^{k-1}.$$

Theorem 4 can be combined with the MacWilliams identities and other constraints on the weight distribution to prove the nonexistence of codes with certain parameters. Here is one example.

Example 6: Let $\mathcal{C}$ be a putative $[85, 6, 61]_4$-code. We apply the usual linear program with respect to the MacWilliams equations and information on the dual distance and nonexistence of residual codes from the table in [1]. As a result, we find that

$$\sum_{i\ odd} A_i(\mathcal{C}) \le 1764 < 7 \cdot 4^{6-2}.$$

Hence the preceding remark and Theorem 4 imply that $\mathcal{C}$ can be extended to a $[86, 6, 62]_4$-code. The table in [1] tells us that such a code does not exist. Consequently, $\mathcal{C}$ does not exist.

REFERENCES

[1] A. E. Brouwer, "Bounds on the size of linear codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998.

[2] P. Delsarte, J.-M. Goethals, and F. J. MacWilliams, "On generalized Reed-Muller codes and their relatives," *Inform. Contr.*, vol. 16, pp. 403–442, 1970.

[3] S. Guritman, F. Hoogweg, and J. Simonis, "The degree of functions and weights in linear codes," *Discr. Appl. Math.*, to be published.

[4] R. Hill and P. Lizak, "Extensions of linear codes," in *Proc. Int. Symp. Information Theory*, Whistler, BC, Canada, 1995, p. 345.

[5] R. Hill, "An extension theorem for linear codes," in *Des. Codes Cryptogr.*, 1999, vol. 17, pp. 151–157.

[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 2nd ed. Amsterdam, New York, Oxford: North-Holland, 1983.

Cocyclic Hadamard Codes

Kathy J. Horadam and Parampalli Udaya, *Member, IEEE*

***Abstract*—We demonstrate that many well-known binary, quaternary, and q-ary codes are cocyclic Hadamard codes; that is, derived from a cocyclic generalized Hadamard matrix or its equivalents. Nonlinear cocyclic Hadamard codes meet the generalized Plotkin bound. Using presemifield multiplication cocycles, we construct new equivalence classes of cocyclic Hadamard codes which meet the Plotkin bound.**

***Index Terms*—Cocycle, generalized Hadamard matrix, Hadamard codes, presemifield, relative difference set.**

I. INTRODUCTION

In [12], the first author introduced a very general description of cocyclic codes in order to demonstrate the previously unrecognized (and well-hidden) presence of cocycles in several code construction techniques. Cocycles are mappings $\psi : G \times G \to C$, where G and C are finite groups with C Abelian, which satisfy a particular quasi-associative equation (1). They arise naturally in the topology of surfaces, in

Manuscript received January 5, 1999; revised February 15, 2000. This work was supported by the Australian Research Council under Large Grant A49701206. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory, MIT, Cambridge, MA, August 1998.

The authors are with the Department of Mathematics, the Royal Melbourne Institute of Technology, Melbourne, Vic. 3001, Australia.

Communicated by I. F. Blake, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(00)04281-4.