Adding a Parity-Check Bit

Juriya 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 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 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]-code 𝐶 has a one-codimensional subcode 𝐶′ with minimum distance > 𝑑, then 𝐶 can be extended to an [𝑛 + 1, 𝑘, 𝑑 + 1]-code.

Proof: Choose an arbitrary vector ζ ∈ 𝐶′⊥. Then the extended code can be taken as the span in 𝐹𝑞+1 of (1, ζ) and the vectors (0, 𝜖), 𝜖 ∈ 𝐶′.

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 𝐶 be an [𝑛, 𝑘, 𝑑]-code over 𝐹𝑞 with gcd(𝑑, 𝑞) = 1 and with all weights congruent to 0 or 𝑑 (modulo 𝑞). Then 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 𝐶 is the sequence (𝐴𝑖(𝐶))𝑖≥0, with

\[ A_i(𝐶) := | \{ e ∈ C | \text{wt}(e) = i \} |. \]

Proposition 3: Let 𝐶 be an [𝑛, 𝑘, 𝑑]-code over a finite field 𝐹𝑞 of characteristic 𝑝, and let 𝑙 be any integer that is not divisible by 𝑝. Then the set

\[ C^{(l)} := \{ e ∈ C | \text{wt}(e) \neq l \mod p \} \]

is a one-codimensional subcode of 𝐶 if and only if its size is right, i.e., if, and only if

\[ \sum \limits_{i \not\equiv l \mod p} A_i(𝐶) = q^{n-1}. \]
Proof. Let \( q := p^r \). Consider the polynomial function
\[
\varphi : F_q^n \to F_q, \quad (x_1, x_2, \ldots, x_n) \mapsto \sum_{i=0}^{n} (x_i)^{q^i-1}.
\]
Actually, \( \varphi \) maps \( F_q^n \) onto the prime field \( F_p \). We can view \( F_q^n \) as an \( F_p \)-vector space of dimension \( n \). The \( F_q \)-degree of \( \varphi \) is \( q - 1 \), but what about its \( F_p \)-degree? The functions
\[
x \mapsto x^i, \quad i = 0, 1, \ldots, r - 1
\]
are \( F_p \)-linear. So, decomposing the monomial \( x^t \) as
\[
x^t = x^{q^i} (x^{q^{i+1}})^{q^i} \cdots (x^{p^{t-1}})^{q^i},
\]
we see that the \( F_q \)-degree of \( \varphi \) is equal to \( r(p - 1) \). The function
\[
\psi : C \to F_p, \quad \psi(\mathbf{e}) = \varphi(\mathbf{e}) - t,
\]
on the \( rk \)-dimensional \( F_q \)-vector space \( C \) will have degree at most \( r(p - 1) \). So \( \psi \) defines a word in the generalized Reed–Muller code \( R_\mu(r(p - 1), r k) \). The weight of this word is the size of the support of \( \psi \)
\[
\text{wt}(\psi) = \sum_{i \notin \mathbb{M} \mod p} A_i(C).
\]
It is well known (cf. [2] or [3]) that the minimum weight of \( R_\mu(r(p - 1), r k) \) is equal to \( p^{k-h} - 1 \), and that the supports of the minimum-weight codewords are the \( F_p \)-affine \((r k - r)\)-flats in \( F_p^k \). So, if
\[
\sum_{i \notin \mathbb{M} \mod p} A_i(C) = q^{k-1},
\]
then
\[
C^{(t)} := \{ \mathbf{e} \in C \mid \text{wt}(\mathbf{e}) \neq t \mod p \}
\]
is an \( F_p \)-affine \((r k - r)\)-flat in the \( rk \)-dimensional \( F_p \)-vector space \( C \). Since we assumed that \( t \neq 0 \mod p \), the set \( C^{(t)} \) contains the zero vector and hence is an \((r k - r)\)-dimensional \( F_p \)-linear subspace of \( C \). Finally, \( C^{(t)} \) is invariant under scalar multiplication with nonzero elements from \( F_q \). So \( C^{(t)} \) actually is a \((k - 1)\)-dimensional \( F_p \)-linear subspace of \( C \).

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

Theorem 4: Let \( C \) be an \( [n, k, d] \)-code over a finite field \( F_q \) of characteristic \( p \). If \( d \neq 0 \mod 3 \) and
\[
\sum_{i \notin \mathbb{M} \mod p} A_i(C) = q^{k-1},
\]
then \( C \) 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 \( \sum_{i \notin \mathbb{M} \mod p} A_i(C) \) is below a certain bound, then it has to be equal to \( q^{k-1} \). We give two examples.

1) If \( q := 3 \) and \( d \neq 0 \mod 3 \), then
\[
\sum_{i \notin \mathbb{M} \mod 3} A_i(C) < 5 \cdot 3^{k-2}
\]
implies that
\[
\sum_{i \notin \mathbb{M} \mod 3} A_i(C) = 3^{k-1}.
\]
2) If \( q := 4 \), then
\[
\sum_{i \notin \mathbb{M} \mod d} A_i(C) < 7 \cdot 4^{k-2}
\]
implies that
\[
\sum_{i \notin \mathbb{M} \mod d} A_i(C) = 4^{k-1}.
\]

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 \( C \) be a putative \([85, 6, 61]\)-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
\[
\sum_{i \neq \mathbb{M} \mod d} A_i(C) \leq 1764 < 7 \cdot 4^{6-2}.
\]

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

REFERENCES


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