On lifting completely regular codes

Joaquim Borges, Josep Rifà

Department of Information and
Communications Engineering
Universitat Autònoma de Barcelona,
Spain

and

Victor Zinoviev
Institute for Problems of Information
Transmission,
Moscow, Russia

Summary. **It has been proved recently that lifting any code implies completely regularity if and only if the initial code is a Hamming code. In this paper we go further, proving that lifting any completely regular code (which is not a Hamming code) implies uniformly packed condition, if the initial completely regular code has covering radius $\rho = 2$ and its dual code is antipodal.**

We use the standard notation $[n,k,d]_q$ for a linear code of length n, dimension k and minimum distance d over the finite field $\mathbb{F}_q$. For two codes A and B of the same length let

$$A+B=\{\mathbf{a}+\mathbf{b}:\ \mathbf{a}\in A,\ \mathbf{b}\in B\}.$$

We consider *nontrivial* linear $[n,k,d]_q$ codes, i.e.

$$2\leq k\leq n-2 \ \text{ and } \ d\geq 3.$$

For a vector $\mathbf{v}\in\mathbb{F}_q^n$ let $\mathrm{wt}(\mathbf{v})$ denote its Hamming weight. For a code C and a vector $\mathbf{v}$, define the *distance between* $\mathbf{x}$ *and* C:

$$d(\mathbf{v},C) \ = \ \min\{d(\mathbf{v},\mathbf{c}):\ \mathbf{c}\in C\}.$$

The *covering radius* of a code C is

$$\rho=\max_{\mathbf{v}\in\mathbb{F}_q^n}\{d(\mathbf{v},C)\}.$$

For a code C with covering radius ρ define

$$C(i) \ = \ \{\mathbf{x}\in\mathbb{F}_q^n:\ d(\mathbf{x},C)=i\}, \ \ i=1,2,...,\rho.$$

Definition 1 *A code C is completely regular, if for all $l\geq 0$ every vector $x\in C(l)$ has the same number c_l of neighbors in $C(l-1)$ and the same number b_l of neighbors in $C(l+1)$.*

Definition 2 *Let C be a q-ary code of length n and let ρ be its covering radius. We say that C is* uniformly packed in the wide sense, *i.e. in the sense of $[BZZ]$, if there exist rational numbers $\beta_0, \ldots, \beta_\rho$ such that for any $\mathbf{v} \in \mathbb{F}_q^n$*

$$\sum_{k=0}^{\rho} \beta_k \, A_k(\mathbf{v}) \;=\; 1, \qquad (1)$$

where $A_k(\mathbf{v})$ is the number of codewords at distance k from $\mathbf{v}$. The case

$$\rho = e + 1 \quad \textit{and} \quad \beta_{\rho-1} = \beta_\rho$$

corresponds to uniformly packed codes in the narrow sense $[SZZ]$ *and the case $\rho = e + 1$ corresponds to* uniformly packed *codes $[GT]$ (here $e = \lfloor (d-1)/2 \rfloor$.*

Let C be a q-ary linear nontrivial code of length n over the field $\mathbb{F}_q$ with minimum distance $d \geq 3$. Let H be a parity check matrix of C and consider the code denoted by $\mathcal{C}^{(r)}$ of length n over the field $\mathbb{F}_{q^r}$ with the same parity check matrix H. Say that *the code $\mathcal{C}^{(r)}$ is the lifted code obtained from C.* In the recent paper [RZ] we studied lifted codes from Hamming codes.

Theorem 1 *Let C be an $[n, k, d]_q$ code and $\mathcal{C}^{(r)}$ be its lifted code over $\mathbb{F}_{q^r}$. Then $\mathcal{C}^{(r)}$ is a completely regular code with covering radius*

$$\rho \;=\; \min\{m, r\},$$

if and only if C is a Hamming code.

Here we describe all completely regular codes (which are not Hamming codes), whose lifted codes give uniformly packed, in the wide sense, codes. These codes coincide with the class of completely regular codes, which has been considered in our recent paper [BRZ], namely codes with covering radius $\rho = 2$, whose dual is antipodal.

Lemma 1 *Let C be a code with covering radius ρ and external distance s. Then:*

(i) $\rho \leq s$ *[Delsarte].*

(ii) $\rho = s$ *if and only if C is uniformly packed in the wide sense [BZ], [GT] (for $\rho = e+1$).*

Denote by U_m the matrix of size $m \times q^m$ whose columns are all the q^m vectors of length $m \geq 1$, and by D_m denote the matrix of size $(m+1) \times q^m$ obtained from U_m by adding an extra $(m+1)$th row with all elements equal to 1; (the matrix U_m generates a *difference matrix*). Let $\mathcal{D}^{(m)}$ denote the *difference matrix code*, whose parity check matrix is the matrix D_m. Denote by $\mathcal{H}^{(m)}$ a perfect (Hamming) $[n_m, k, 3]_q$ code of length $n_m = (q^m - 1)/(q-1)$ with parity check matrix H_m and by $\mathcal{H}^{(m,r)}$ the code obtained by lifting $\mathcal{H}^{(m)}$ over $\mathbb{F}_{q^r}$, i.e. the code over $\mathbb{F}_{q^r}$ with parity check matrix H_m.

For a given $[n, k, d]_q$ code C with parity check matrix H define its *complementary* $[n_m - n, m, \bar{d}]$ code $\bar{C}$, whose parity check matrix $\bar{H}$ is obtained from the matrix H_m by removing all columns of

H, and columns which are mutually dependent on columns of H.

Lemma 2 [*Delsarte*] *A linear projective* $[n, k, d]_q$ *code* C *with covering radius* $\rho = 2$ *does exist simultaneously with its complementary projective code* $\bar{C}$ *with covering radius* $\bar{\rho} \leq 2$*. Furthermore,* $\bar{\rho} = 1$*, if and only if* C *is a difference matrix code* $\mathcal{D}^{(m)}$ *and* $\bar{C}$ *is a Hamming code* $\mathcal{H}^{(m)}$*.*

Let $\mathbf{h}_i$ denote the i-th row of H_m, the parity check matrix of Hamming code of length

$$n_m = (q^m - 1)/(q - 1).$$

Lemma 3 *Let r, m be integers, such that $1 \le r \le m$. Let*

$$\mathbf{g} = \sum_{i=1}^{m} \xi_i \mathbf{h}_i, \quad \textit{where} \ \ \xi_i \in \mathbb{F}_{q^r}.$$

If among $\xi_i, \ \ i = 1, \ldots, m$ there are f linearly independent over $\mathbb{F}_q$ elements from $\mathbb{F}_{q^r}$, then

$$wt(\mathbf{g}) \ = \ q^{m-1} + q^{m-2} + \ldots + q^{m-1-f}.$$

It is clear that the minimum distance of the lifted code $C^{(r)}$ is the same that in the initial code C over $\mathbb{F}_q$. We can specify a little more in the following two lemmas.

Lemma 4 *Let* $\mathbf{c}$ *be a codeword of* $\mathcal{C}^{(r)}$ *of minimum weight. Then* $\mathbf{c} = \beta\,\mathbf{c}'$ *where* $\beta \in \mathbb{F}_{q^r}$ *and* $\mathbf{c}'$ *is a codeword of minimum weight in* C*.*

Lemma 5 *Let* α *be a primitive element of* $\mathbb{F}_{q^r}$*. Then*

$$\mathcal{C}^{(r)} \;=\; C + \alpha C + \alpha^2 C + \ldots + \alpha^{r-1} C.$$

The following property will be useful:

(P.1) *For every nonzero codeword $\mathbf{v} \in C$, every symbol which occurs in a coordinate position of $\mathbf{v}$, occurs in this codeword the same number of times as any other symbol which also occurs in $\mathbf{v}$, in particular, exactly $n - wt(\mathbf{v})$ times, if $wt(\mathbf{v}) \neq n$, where $wt(\mathbf{v})$ is the weight of $\mathbf{v}$.*

Recall that a linear code C of length n is *antipodal*, if there is codeword $\mathbf{v}$ of weight $\mathrm{wt}(\mathbf{v}) = n$. In [BRZ] we have considered completely regular codes with $\rho = 2$ and dual antipodal. One of the main statements was the following theorem.

Theorem 2 *A nontrivial $[n, k, d]_q$ code C with parity check matrix H is completely regular with $\rho = 2$ and dual antipodal code $C^{\perp}$ if and only if the matrix H is, up to equivalence, as follows:*

$$H = \begin{bmatrix} 1 & \cdots & 1 \\ & M & \end{bmatrix}, \qquad (2)$$

where M generates an equidistant code E which fulfills the property (P.1)

In the next lemma we will show that for the dual of a Hamming code, Property $(P.1)$ coincides with the condition, when the Hamming code can be extended up to minimum distance $d = 4$.

Lemma 6 *Let E be a code of length*

$$n = \frac{q^m - 1}{q - 1} + 1$$

given by lengthening of the dual Hamming q-ary code, adding a zero coordinate. Then E has Property $(P.1)$ if and only if we are exactly in one of the two following cases:

(i) *$q = 2$ and $m \geq 2$.*

(ii) *$q = 2^g \geq 4$ and $m = 2$.*

Let $\mathcal{E}^{(m,r)}$ denote the lifted code over $\mathbb{F}_{q^r}$ obtained from an equidistant code E, such that its generator matrix M consists on mutually linear independent over $\mathbb{F}_q$ columns.

Lemma 7 *The code $\mathcal{E}^{(m,r)}$ satisfies Property $(P.1$ if and only if the initial equidistant code E satisfies Property $(P.1)$.*

Denote by $\mathcal{C}^{(m,r)}$ the lifted code over $\mathbb{F}_{q^r}$ obtained from C which has a parity check matrix H of size $m \times n$ over $\mathbb{F}_q$. The next statement is the main result of this paper.

Theorem 3 *Let C be a completely regular, but not perfect, code with covering radius $\rho = 2$ and dual antipodal. Let H be a $m \times n$ parity check matrix for the code C over $\mathbb{F}_q$. Then the code $\mathcal{C}^{(m,r)}$, obtained by lifting C over $\mathbb{F}_{q^r}$, is uniformly packed in the wide sense, but not completely regular, with covering radius*

$$\rho = 1 + \min\{m, r\}.$$

Corollary 1 *There exist the following classes of uniformly packed, in the wide sense, linear codes over $\mathbb{F}_{q^r}$ with $\rho = 1 + \min\{m, r\}$, which are not completely regular, obtained by lifting completely regular codes with $\rho = 2$ and dual antipodal:*
(i) Lifted binary extended Hamming
$[n = 2^m, n - m - 1, 4]_{2^r}$ *codes;*
(ii) Lifted extended Hamming $[q + 2, q - 1, 4]_{q^r}$ *codes, where* $q = 2^g$*;*
(iii) Lifted Difference matrix
$[n = q^m, n - m - 1, 3]_{q^r}$ *codes;*
(iv) $[n, n - 3, 3]_{q^r}$ *codes with* $n = 1 + t(q + 1)$, *where* $t + 1 \geq 4$ *is a divisor of* q *and* $q = 2^g$*;*
(v) Lifted Latin squares $[n, n-2, 3]_{q^r}$ *codes, where* $3 \leq n \leq q$ *and* $q \geq 3$ *is any prime power.*

References

[BZZ] L.A. Bassalygo, G.V. Zaitsev and V.A. Zinoviev, “Uniformly packed codes,” *Problems Inform. Transmiss.,* v. 10, no. 1, pp. 9-14, 1974.

[BZ] L.A. Bassalygo and V.A. Zinoviev, “A note on uniformly packed codes”, *Problems Inform. Transmiss.*, v. 13, no. 3, 22-25, 1977.

[BRZ] J. Borges, J. Rifa and V.A. Zinoviev, ”On completely regular codes with covering radius 2 and dual antipodal”, *Advances in Mathematics of Communication*, 2010, to appear.

[D] P. Delsarte, *Two-weight linear codes and strongly regular graphs*, MBLE Research Laboratory, Report R160, 1971.

[GT] J.M. Goethals and H.C.A. Van Tilborg, “Uniformly packed codes,” *Philips Res.*, v. 30, pp. 9-36, 1975.

[RZ] J. Rifà and V.A. Zinoviev, ”On lifting perfect codes", *IEEE Trans. on Inform. Theory*, (2010), submitted.

[SZZ] N.V. Semakov, V.A. Zinoviev and G.V. Zaitsev, "Uniformly packed codes," *Problems Inform. Transmiss.*, v. 7, no. 1, pp. 38-50, 1971.