5-1990

Simplifications to "A New Approach to the Covering Radius..."

H. F. Mattson Jr

SU-CIS-90-11

Simplifications to "A New Approach to the Covering Radius..."

H. F. Mattson, Jr.

May 1990

School of Computer and Information Science
Syracuse University
Suite 4-116
Center for Science and Technology
Syracuse, New York 13244-4100

Simplifications to "A New Approach to the Covering Radius..."

H. F. Mattson, Jr.

School of Computer and Information Science
Center for Science and Technology 4-116
jen@SUVM.acs.syr.edu / jen@SUVM.bitnet
Syracuse University
Syracuse NY 13244

Simplifications to "A New Approach to the Covering Radius..."

by H. F. Mattson, Jr.

Abstract. We simplify the proofs of four results in [3], restating two of them for greater clarity.

The main purpose of this note is to give a brief transparent proof of Theorem 7 of [3], the main upper bound of that paper. The secondary purpose is to give a more direct statement and proof of the integer programming determination of covering radius of [3].

Theorem 7 of [3] follows from a simple result in [2], which we state with the notation (for the linear code A)

$$\begin{aligned} g(A) &:= \text{a generator matrix of } A, \\ t(A) &:= \text{the covering radius of } A. \end{aligned} \tag{1}$$

THEOREM 1 [2]. If A is a code with generator matrix

$$g(A) = \begin{array}{|c|c|} \hline g(A_1) & * \\ \hline 0 & g(A_0) \\ \hline \multicolumn{1}{c}{X} & \multicolumn{1}{c}{\bar{X}} \end{array}$$

then $t(A) \leq t(A_0) + t(A_1)$.

To describe the codes A_0 and A_1: Pick any subset X of coordinate-places of A. A_1 is the projection of A on X; we get A_0 from the subcode D of A which vanishes on X by projecting D on $\bar{X}$. (A_0 [A_1] is sometimes called a shortened [punctured] code of A.)

Before stating Theorem 2, let us agree that all codes B, C are binary, linear, and have no coordinates identically 0. (The last need not be true of C_0.) We also need the following notation:

(2.1)

$$S_k := [2^k - 1, k] \text{ simplex code.}$$

(2.2) B denotes an $[n,k]$ code having in $g(B)$ exactly $m_i \geq 0$ copies of column i of $g(S_k)$ for $i = 1, \ldots, 2^k - 1$. Thus $n = \sum m_i$.

(2.3) We often identify a vector in $\mathbf{Z}_2^n$ with its support. In this note the support is a subset of the set of columns of S_k, or a multisubset thereof. In that identification we may denote the weight of the vector x by $|x|$, the cardinality of the support of x. The columns of $g(B)$ form a multisubset of the set of columns of $g(S_k)$. The vector $(m_1, \ldots, m_{2^k-1})$ of multiplicities of the columns is called the *signature* of B.

(3) The normalized covering radius [**3**] of B is defined as

$$\rho(B) := \rho(m_1, \ldots, m_{2^k-1}) := t(B) - \sum_i \left\lfloor \frac{m_i}{2} \right\rfloor .$$

The *projective core* of B is the code C for which $g(C)$ consists of the columns of $g(B)$ without any repetitions. I.e., in the signature $(\ldots, \nu_i, \ldots)$ of C, $\nu_i = 1$ if $m_i > 0$ and $\nu_i = 0$ if $m_i = 0$.

For any column Q of $g(B)$ we define $\eta := \eta_Q$ to be the total number of vectors $\{P, Q, R\}$ of weight 3 in $C^\perp$ for which m_P and m_R are odd. The vectors are denoted as in (2.3).

Before going on, we comment on (3). Recall from [**1**, II D] the definition of a catenation A of the $[n_1, k_1]$ code A_1 and the $[n_2, k_2]$ code A_2, with $k_1 \leq k_2$. It has generator matrix

$$g(A) = \begin{array}{|c|c|} \hline g(A_1) & g(A_2) \\ \hline 0 & \\ \hline \end{array} \;,$$

and its covering radius satisfies $t(A) \geq t(A_1) + t(A_2)$ [**1**, II D]. We take A_2, say, to be the "even" part of the code B. That is, write $m_i = 2\mu_i + \epsilon_i$, where $\epsilon_i = 0$ or 1, and take A_1 and A_2 to have signatures $(\ldots, \epsilon_i, \ldots)$ and $(\ldots, 2\mu_i, \ldots)$, respectively. Then B is a catenation of A_1 and A_2, and $t(B) \geq t(A_1) + t(A_2)$. From [**2**, (11)] we get an immediate proof of Thm. 6 of [**3**]: $t(A_2) = \sum \mu_i$, since the "double" of any code of length ℓ has covering radius ℓ. Therefore, $t(B) \geq t(A_1) + \sum \mu_i$ and $\rho(B) \geq t(A_1)$. (This is Thm. 5 of [**3**].)

To state the result, choose any column Q of $g(B)$. After row-operations (which do not change B even though they permute the m_i's) column Q becomes simply $(10\cdots0)^{tr}$, and

(4)

$$g(B) = \begin{array}{l} \;\leftarrow \; m_Q \; \rightarrow \\ \begin{array}{|c|c|} \hline 11\cdots1 & * \\ \cline{2-2} 0 & g(B_0) \\ \hline \end{array} \end{array} \quad ,$$

where B_0 has signature $(m'_1, m'_2, \ldots, m'_{2^{k-1}-1})$.

THEOREM 2 ([**3**]). The normalized covering radius of B satisfies

$$\rho(B) \leq \eta_Q + \rho(m'_1, \ldots, m'_{2^{k-1}-1}).$$

Proof. Since B_1 in (4) is an $[m_Q, 1, m_Q]$ repetition code, $t(B_1) = \lfloor m_Q/2 \rfloor$. Thus, from Theorem 1,

(5)

$$t(B) \leq \lfloor m_Q/2 \rfloor + t(B_0).$$

To express (5) in terms of normalized covering radii, we subtract $\sum_i \lfloor m_i/2 \rfloor$ from both sides. We get

(6)

$$\rho(B) := t(B) - \sum_i \lfloor m_i/2 \rfloor \leq t(B_0) - \sum_{i \neq Q} \lfloor m_i/2 \rfloor.$$

Each pair of columns P and R of $g(B)$ which agree except on their top coordinate have sum Q. That is, for some vector N, $P = (0, N)^{tr}$ and $R = (1, N)^{tr}$. Thus $m_P + m_R = m'_N$, and $\{P, Q, R\}$ is (the support of) a vector of weight 3 in $C^{\perp}$. We note that

(7)

$$\left\lfloor \frac{m_P}{2} \right\rfloor + \left\lfloor \frac{m_R}{2} \right\rfloor = \left\lfloor \frac{m_P + m_R}{2} \right\rfloor$$

unless m_P and m_R are odd, in which case the right-hand side of (7) must be decreased by 1. Thus (6) becomes

$$\rho(B) \leq t(B_0) - \sum_j \left\lfloor \frac{m'_j}{2} \right\rfloor + \eta. \qquad \square$$

Remark. Theorem 1 allowed us to avoid the notion of "height" used in [**3**]. We have also restated the result by defining η not with finite geometry, as in [3], but in terms of the code. Except for this change of language the proof after (5) is similar to that of [3].

Finally, we simplify the integer programming determination [**3**, Thm. 1] of $\rho(B)$ by eliminating "height" from the statement and proof.

In terms of (2), it is simple to see [**1**] that x is a coset leader of a code A iff

(8)

$$\forall a \in A \;\; 2|x \cap a| \;\leq\; |a|.$$

Letting the $[n,k]$ code B have signature $(\cdots, m_i, \cdots)$, define [**3**,(5)] for any $x \in \mathbf{Z}_2^n$, $x := (x^{(1)}, \ldots, x^{(n)})$, where $x^{(i)}$ is the "sub" vector of the coordinates of x at the m_i places where column i appears in $g(B)$. Define

(9)

$$w_i(x) := wt(x^{(i)}).$$

It follows that $0 \leq w_i(x) \leq m_i$ for all i and x, and that $wt(x) = \sum_i w_i(x)$.

We also project B onto the projective core C by the rule

$$b = (\ldots, b^{(i)}, \ldots) \to (\ldots, c_i, \ldots) = c,$$

where $c_i = 1$ iff $b^{(i)} \neq 0$. It follows that $|b| = \sum_i c_i m_i$, where c_i is regarded as real 0 or 1.

Using (2.3) we calculate for any $b \in B$ and any $x \in \mathbf{Z}_2^n$

$$x \cap b = \bigcup_i x^{(i)} \cap b^{(i)} = \bigcup_{c_i=1} x^{(i)}.$$

Hence

$$|x \cap b| = \sum_i c_i w_i(x).$$

Thus we see from (8) that x is a coset leader for B iff for all $c = (\ldots, c_i, \ldots)$ in C,

$$\sum_i c_i w_i(x) \leq \frac{1}{2} \sum_i c_i m_i.$$

Since the covering radius of B is the weight of a coset leader of maximum weight we have proved (*cf.* [**3**, Thm. 1])

THEOREM 3. The covering radius of B is the solution to the following integer programming problem:

Maximize $W := w_1 + \cdots + w_{2^k-1}$ subject to the constraints

$w_i \in \mathbf{Z}, 0 \leq w_i \leq m_i$

and $\sum_i c_i w_i \leq \frac{1}{2} \sum_i c_i m_i$ for all $c = (c_i) \in C$.

COROLLARY. $\rho(B) = \max W - \sum \left\lfloor \frac{m_i}{2} \right\rfloor$.

References

[**1**] G. Cohen, M. Karpovsky, H. F. Mattson, Jr., and J. R. Schatz, "Covering radius—survey and recent results," *IEEE Trans. Inform. Theory* IT-31 (1985), 328–343.

[**2**] H. F. Mattson, Jr., "An improved upper bound on covering radius," pages 90–106 in *Algebraic Algorithms and Error-Correcting Codes*, ed. A. Poli, Lecture Notes in Computer Science #228, Springer-Verlag, Berlin, 1986. (Proceedings of Conference AAECC-2, Toulouse, October, 1984.)

[**3**] N. J. A. Sloane, "A new approach to the covering radius of codes," *J. Combin. Theory*, A42 (1986), 61–86.