AAECC **13**, 53–56 (2002)

AAECC
Applicable Algebra in
Engineering, Communication
and Computing

Note on Niederreiter-Xing's Propagation Rule for Linear Codes

Ferruh Özbudak[1], **Henning Stichtenoth**[2]

[1] Middle East Technical University, Department of Mathematics, Ínönü Bulvari, 06531 Ankara, Turkey (e-mail: ozbudak@arf.math.metu.edu.tr)
[2] Universität Essen, FB 6 Mathematik, 45117 Essen, Germany
(e-mail: stichtenoth@uni-essen.de)

Received: June 23, 2000

Abstract. We present a simple construction of long linear codes from shorter ones. Our approach is related to the product code construction; it generalizes and simplifies substantially the recent "Propagation Rule" by Niederreiter and Xing. Many optimal codes can be produced by our method.

Keywords: Linear Codes, Optimal codes, Product codes.

Recently H. Niederreiter and C. P. Xing proposed a sophisticated construction of long linear codes from shorter ones [3]. For a given $[n, k, d]$ code over $\mathbb{F}_q$ and integers h, r, s satisfying $2 \leq h \leq q$, $1 \leq r < h$ and $0 \leq s \leq r$ they obtained a linear $[N, K, D]$ code over $\mathbb{F}_q$ with

$$N = h \cdot n,$$

$$K = k(s + 1) + r - s,$$

$$D \geq \min\{(h - s) \cdot d, (h - r) \cdot n\}.$$

The main ingredients of their construction are: representing an arbitrary linear code as a (generalized) algebraic geometric code, and ramification theory of algebraic function fields. They also present several examples to show that their construction is a powerful method for finding good long codes from shorter ones.

The aim of this note is to show that the Niederreiter-Xing construction is in fact a very special case of a quite elementary construction that uses only basic linear algebra. All codes considered here are linear codes over $\mathbb{F}_q$. The parameters of a code C are denoted by length (C), $\dim(C)$ and $d(C)$:= minimum distance of C. For our construction we need:

(1) a code C of length m and dimension k, and
(2) a collection of k $(= \dim(C))$ codes $W_1, \ldots, W_k$, all of them having the same length n.

Elements of C will be written as row vectors, and elements of W_j as column vectors. We fix a basis $(c^{(1)}, \ldots, c^{(k)})$ of C and denote by G the $k \times m$ matrix whose rows are $c^{(1)}, \ldots, c^{(k)}$. Thus G is a generator matrix of C. For $1 \le j \le k$ we set

$$C_j := \operatorname{span}\{c^{(1)}, \ldots, c^{(j)}\} \subseteq \mathbb{F}_q^m.$$

Then C_j is a code of length m and dimension j, and

$$C_1 \subseteq C_2 \subseteq \cdots \subseteq C_k = C.$$

Let M be the set of all $n \times k$ matrices whose j-th column is in W_j, for $1 \le j \le k$. Obviously M is a linear space of dimension

$$\dim(M) = \sum_{j=1}^{k} \dim(W_j).$$

Theorem. *Notations as above. Then the linear code*

$$W := \{A \cdot G \mid A \in M\}$$

has parameters as follows:

$$\begin{aligned} \text{length } (W) &= \text{length } (C) \cdot \text{length } (W_j) = m \cdot n, \\ \dim(W) &= \sum_{j=1}^{k} \dim(W_j), \\ d(W) &\ge \min\{d(W_j) \cdot d(C_j) \mid 1 \le j \le k\}. \end{aligned}$$

Proof. First we observe that an element $X = A \cdot G \in W$ is an $n \times m$ matrix and hence can be considered as a vector in $\mathbb{F}_q^{m \cdot n}$. It is then clear that W is a linear code of length $m \cdot n$ = length $(C) \cdot$ length (W_j) (note that all W_j have the same length n). For $A \in M$ we denote by $a^{(i)} \in \mathbb{F}_q^k$ the i-th row of A; then

$$A \cdot G = \begin{pmatrix} a^{(1)} \cdot G \\ \vdots \\ a^{(n)} \cdot G \end{pmatrix}$$

with $a^{(i)} \cdot G \in C$ for $1 \le i \le n$. Since the rows of G are linearly independent, it follows that $A \neq 0$ implies $A \cdot G \neq 0$, hence

$$\dim(W) = \dim(M) = \sum_{j=1}^{k} \dim(W_j).$$

Now let $X \in W$ be a nonzero codeword in W. We write $X = A \cdot G$ with a matrix $A \in M$ and denote by $w_1, \ldots, w_k$ the columns of A (where $w_j \in W_j$ for $1 \le j \le k$). Let $l := \max\{j | w_j \neq 0\}$. Then $a^{(i)} \cdot G \in C_l$ for all rows $a^{(1)}, \ldots, a^{(n)}$ of A. There are at least $d_l := d(W_l)$ nonzero components of w_l, and hence the matrix A has at least d_l nonzero rows. For these rows, the vector $a^{(i)} \cdot G \in C_l$ has weight $\ge d(C_l)$. It follows that

$$\text{weight }(X) = \sum_{i=1}^{n} \text{weight }(a^{(i)} \cdot G) \ge d_l \cdot d(C_l). \qquad \square$$

Remark 1. The definition of the code W (as well as the assertion on its minimum distance) depends not only on the codes $C, W_1, \ldots, W_k$ but also on the choice of the basis $(c^{(1)}, \ldots, c^{(k)})$ of C.

Remark 2. Choosing $W_1 = \cdots = W_k = B$ where B is a code of length n, our construction yields the product code $W = B \otimes C$, cf. [2, p. 568]. Thus our Theorem can be considered as a generalization of the well-known fact that $d(B \otimes C) = d(B) \cdot d(C)$. Our construction is also related to a code construction due to Zinoviev [2, p. 510].

Remark 3. The Niederreiter-Xing construction [3] can be seen to be a special case of our construction (in a non-obvious manner). With notation as in our Theorem, the code C is taken a generalized Reed-Solomon (GRS) code of length h and dimension $r + 1$ (with $2 \le h \le q$ and $1 \le r < h$) and the subcodes $C_j \subseteq C$ are chosen to be GRS codes of dimension j and minimum distance $d(C_j) = h+1-j$ (for $1 \le j \le r+1$). Let $W_1 = \cdots = W_{s+1}$ be a code with parameters $[n, k, d]$, and choose $W_{s+2} = \cdots = W_h$ to be the repetition code with parameters $[n, 1, n]$. The resulting code W has by the Theorem above the parameters

$$\begin{aligned}
\text{length }(W) &= h \cdot n, \\
\dim(W) &= \sum_{j=1}^{r+1} \dim(W_j) = (s+1) \cdot k + (r - s), \\
d(W) &\ge \min\{d(W_j) \cdot d(C_j) \mid 1 \le j \le r+1\} \\
&= \min\{d \cdot (h - s), n \cdot (h - r)\},
\end{aligned}$$

which is the main result of [3].

Remark 4. As pointed out in [3], the Niederreiter-Xing construction yields many good codes. In our construction one has much more freedom to choose the codes C and W_j properly, so we can produce many other good long codes. We illustrate this by the following examples.

Example 1. $q = 2$, C has parameters $[2, 2, 1]$ and C_1 has parameters $[2, 1, 2]$. Choose W_1, W_2 with parameters $[20, 19, 2]$, resp. $[20, 14, 4]$. Then W has parameters $[40, 33, 4]$. In fact, W is optimal: there is no binary $[40, 33, \delta]$ code with $\delta > 4$ (see [1]).

Example 2. $q = 5$, C has parameters $[3, 3, 1]$, $d(C_1) = 3$, $d(C_2) = 2$, $d(C_3) = 1$, and W_1, W_2, W_3 are codes with parameters $[12, 12, 1]$, resp. $[12, 11, 2]$, resp. $[12, 9, 3]$. The resulting code W has then parameters $[36, 32, 3]$. Also this code W is optimal.

Example 3. $q = 2$. It is not known whether there is a code B with parameters $[79, 38, 20]$. Assume it exists. Then we choose C with parameters $[2, 2, 1]$ and $C_1 \subseteq C$ with parameters $[2, 1, 2]$, and we choose W_1 with parameters $[79, 6, 39]$ and $W_2 = B$. Our construction would produce a binary code W with parameters $[158, 44, d \geq 39]$.

References

1. Brouwer, A. E.: Bounds on the Minimum Distance of Linear Codes, www.win.tue.nl/~aeb/voorlincod.html
2. Mac Williams, F. J., Sloane, N. J. A.: The Theory of Error-Correcting Codes, Amsterdam: North Holland Publ. Comp., 1997
3. Niederreiter, H., Xing, C. P.: A Propagation Rule for Linear Codes, AAECC (to appear)