Matrix-Product Codes over $\mathbb{F}_q$

Tim Blackmore$^1$, Graham H. Norton$^2$

$^1$ Infineon Technologies, Stoke Gifford, BS34 8HP, UK
(e-mail: tim.blackmore@infineon.com)

$^2$ Department of Mathematics, University of Queensland, Brisbane 4072, Australia
(e-mail: ghn@maths.uq.edu.au)

Received: July 20, 1999; revised version: August 27, 2001

Abstract. Codes $C_1, \ldots, C_M$ of length $n$ over $\mathbb{F}_q$ and an $M \times N$ matrix $A$ over $\mathbb{F}_q$ define a matrix-product code $C = [C_1 \cdots C_M] \cdot A$ consisting of all matrix products $[c_1 \cdots c_M] \cdot A$. This generalizes the $(u|u+v)$-, $(u+v+w|2u+v|u)$-, $(a+x)b + x(a + b + x)$-, $(u + v|u - v)$- etc. constructions. We study matrix-product codes using Linear Algebra. This provides a basis for a unified analysis of $|C|$, $d(C)$, the minimum Hamming distance of $C$, and $C^\perp$. It also reveals an interesting connection with MDS codes. We determine $|C|$ when $A$ is non-singular. To underbound $d(C)$, we need $A$ to be ‘non-singular by columns (NSC)’. We investigate NSC matrices. We show that Generalized Reed-Muller codes are iterative NSC matrix-product codes, generalizing the construction of Reed-Muller codes, as are the ternary ‘Main Sequence codes’. We obtain a simpler proof of the minimum Hamming distance of such families of codes. If $A$ is square and NSC, $C^\perp$ can be described using $C_1^\perp, \ldots, C_M^\perp$ and a transformation of $A$. This yields $d(C^\perp)$. Finally we show that an NSC matrix-product code is a generalized concatenated code.

Keywords: Binary $(u|u+v)$-construction, Ternary $(u+v+w|2u+v|u)$-construction, Generalized Reed-Muller Codes, Generalized concatenated codes.

1 Introduction

If $C_1$ is an $(n, K_1, d_1)$ code and $C_2$ is an $(n, K_2, d_2)$ code, Plotkin’s well-known $(u|u + v)$-construction gives a $(2n, K_1 K_2, \min\{2d_1, d_2\})$ code. It is

---

*Research funded by the UK Engineering and Physical Sciences Research Council under grant GR/K27728.*
a standard iterative way of defining the Reed-Muller \((RM)\)-codes. The ternary \((u + v + w)|2u + v|u\)-construction produces good codes, giving a \((3n, K_1K_2K_3, \min\{3d_1, 2d_2, d_3\})\) code, where \(C_i\) is an \((n, K_i, d_i)\) code for \(i = 1, \ldots, 3\), [5]. This construction is iterated to produce a ‘Main Sequence (MS)’ subfamily of the ternary Reed-Muller codes in [5, Section IV.C], which we write as \(MS_3\). The matrices

\[
\begin{bmatrix}
1 & 1 \\
0 & 1 \\
\end{bmatrix}
\quad \text{and} \quad
\begin{bmatrix}
1 & 2 & 1 \\
1 & 1 & 0 \\
1 & 0 & 0 \\
\end{bmatrix}
\]

are associated with the \((u|u + v)\)- and \((u + v + w|2u + v|u)\)-constructions respectively. More generally, it was conjectured in [5, Section IV.D] that for any prime \(p\) a family (‘Main-Sequence’) \(MS_p\) codes over \(F_p\) having properties similar to those of the binary \(RM\)-codes would be obtained using a construction with associated upper-triangular \(p \times p\) \(F_p\)-matrix \(MS_p = \left[(\frac{-1}{p-1})\right] \mod p\). A \((u + v|u - v)\)-construction (see [11, Theorem 6]) has also been applied to construct new codes in [4] and generalizations of Turyn’s \((a+x|b+x|a+b+x)\)-construction appear in a study of quasi-cyclic codes in [6].

We define matrix-product codes which include the above as special cases. The matrix-product code \(C = \left[C_1 \cdots C_M\right]\) consists of all matrix products \([c_1 \cdots c_M]\). \(A\) where \(c_i \in C_i\) and \(A\) is an \(M \times N\) matrix over \(F_q\). Here \(M \leq N\) and \(C_i\) is an \((n, |C_i|, d_i)\) code over \(F_q\) for \(i = 1, \ldots, M\). We show that \(|C| = |C_1| \cdots |C_M|\) if \(A\) has a right inverse and \(d(C) \geq \min\{Nd_1, \ldots, (N - M + 1)d_M\}\), provided \(A\) is ‘non-singular by columns (NSC)’; see Definition 3.1 for precise details. We show that the generalized Reed-Muller \((GRM)\)-codes (which are not equivalent to the \(p\)-ary Reed-Muller codes of [7]) are iterative NSC matrix-product codes, thus generalizing the iterative construction of \(RM\)-codes and the iterative description of their generator and parity check matrices. Our approach based on Linear Algebra gives a new proof of the minimum distance of \((GRM)\)-codes (see Theorem 3.7), which is simpler than [1, Corollary 5.5.4]. We also show that \(MS_p\) is an NSC matrix, and in fact our proof of Theorem 3.7 is valid for any iterative ‘triangular’ NSC matrix-product code. Thus we also obtain the minimum distance of the ‘Main Sequence Codes’.

In Section 6 we show that for square matrices, the dual of an NSC matrix-product code is an explicit NSC matrix-product code. This yields \(d(C^\perp)\), see Theorem 6.6. In Section 7 we show that NSC matrix-product codes are generalized concatenated codes, as was already known for codes obtained by the \((u|u + v)\)- and \((u + v + w|2u + v|u)\)-constructions. Thus in particular \((GRM)\)-codes are generalized concatenated codes.

Viewing \((GRM)\)-codes as iterative NSC matrix-product codes may be useful in studying other aspects of these codes. For example, it follows that \((GRM)\)-codes are decomposable and hence can be decoded by multistage decoding in the terminology of [3]. Studying matrix-product codes using e.g. [8] may yield interesting codes over finite rings.