A Justesen Construction of Binary Concatenated Codes that Asymptotically Meet the Zyablov Bound for Low Rate

B.-Z. Shen

***Abstract*—An explicit construction of a sequence of binary codes that asymptotically meet the Zyablov bound for rate lower than 0.30 is given by using Justesen's construction of concatenation. The outer codes are constructed from generalized Hermitian curves. These outer codes can be described without any algebraic geometry terminology, while the proofs of some properties deeply rely on algebraic geometry.**

***Index Terms*—Concatenated codes, algebraic–geometric codes, Zyablov bound, generalized Hermitian curves.**

I. Introduction

A sequence of binary linear codes $\{C_i\}_{i=1}^{\infty}$ such that the codelength $n_i \to \infty$ when $i \to \infty$ is called asymptotically good if both the rates k_i/n_i and the relative minimum distances d_i/n_i are bounded away from zero, where k_i and d_i are the dimension and minimum distance of the code C_i, respectively. If we fix the rate R, the following Gilbert–Varshamov (GV) bound gives a lower bound that d_i/n_i can achieve, $\liminf_{i\to\infty} d_i/n_i \geq H_2^{-1}(1-R)$. For $H_2^{-1}(y)$, we have $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ and $x = H_2^{-1}(y)$, if and only if $y = H_2(x)$ for $0 \leq x \leq 1/2$. Unfortunately, until now, no one has found an algebraic construction of a sequence of binary codes meeting this bound with polynomial time complexity.

In 1966, Forney [2] introduced the concept of concatenated codes in which the m information digits of an inner binary code are treated as single digits of an outer code over GF(2^m). Therefore, if one takes a sequence of linear codes $\{C(k)\}_{k=1}^{\infty}$, where $C(k)$ is a $[N, K, D]$ code over GF(2^k), as the outer codes and for every k one chooses a binary $[n, k, d]$ code as an inner code, one gets a sequence of binary concatenated codes. In 1971, Zyablov [18] proved that there exists a sequence of concatenated binary codes with the inner codelength $n \to \infty$ and the outer codelength $N \to \infty$, in which the outer code is maximal distance separable (MDS), and which satisfy

$$\liminf \frac{\text{distance}}{\text{length}} \geq \max_{0\leq r\leq 1}\left\{\left(1-\frac{R}{r}\right)H_2^{-1}(1-r)\right\},$$

if the overall rate is R. In this correspondence, we call this the *Zyablov bound.* But in the proof, he took the inner code to meet the GV bound. Therefore it was still in doubt whether it is at all possible to give an explicit algebraic construction of a sequence of asymptotically good binary codes. It was in 1972 that Justesen [4] succeeded in doing this by generalizing Forney's concept of concatenation to allow variation of the inner code. In this correspondence, we call such a construction a *Justesen construction.* By using this construction in [4], Justesen also proved that for overall rate not lower than 0.30, the Zyablov bound is constructive. Later, for low rate, several improvements have been made, see [1], [13], [17]. But none of them meets the Zyablov bound when the overall rate $R < 0.30$. Now the question is, is it possible to give an explicit construction for binary concatenated codes which meet the Zyablov bound when the rate is lower than 0.30? MacWilliams and Sloane put this question as a research problem (10.3) in their book [9, p.315].

Manuscript received December 18, 1991; revised April 6, 1992.
The author is with the Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands.
IEEE Log Number 9203004.

In 1982, a surprising result of Tsfasman, Vlăduţ, and Zink [16] was published. This result shows that there is a sequence of codes over GF(q), which are algebraic–geometric codes and which exceed the GV bound whenever q is a square and $q \geq 49$. Moreover, these codes are polynomially constructible. By using a sequence of codes over a fixed field GF(2^k) $(2^k \geq 49)$, which meet the Tsfasman, Vlăduţ, and Zink bound, as outer codes and a fixed $[n, k, d]$ binary inner code, Katsman, Tsfasman, and Vlăduţ [6] improved the Zyablov bound for binary concatenated codes in 1984. However, since the time complexity of finding the generator matrices of their outer codes is $O(N^{30})$, see [15, ch. 4.3], where N is the outer codelength, they hardly can be called constructive from any practical perspective. Therefore, it is still a problem to find binary codes asymptotically meeting or exceeding the Zyablov bound, of low complexity.

In this correspondence, by using a class of algebraic–geometric codes as outer codes which have somehow similar properties to MDS codes when the codelengths are sufficiently large, we give a Justesen construction of concatenated codes which asymptotically meet the Zyablov bound for rates lower than 0.30. In this way, we solve the open problem (10.3) of [9]. Our outer codes are the codes constructed from generalized Hermitian curves that we will define in the Appendix. The construction of the generalized Hermitian curves and their codes turn out to be very simple and can be written explicitly. In fact, those algebraic–geometric codes are simply defined by a defining set and a polynomial set.

II. The Construction of the Outer Codes

Recall that in a Justesen code, the outer code is taken to be a $[2^m-1, k, 2^m-1-k+1]$ Reed–Solomon code over GF(2^m) which is MDS. So it has the maximal minimum distance among all the $[2^m-1, k]$ codes over GF(2^m). The inner codes exhaust all 2^m-1 distinct binary codes in Wozencraft's ensemble of randomly shifted codes described by Massey [10, p. 21]. The reason that Justesen codes cannot meet the Zyablov bound for rate lower than 0.30 is that the construction requires a good ensemble of inner codes with at most 2^m-1 (the length of a Reed–Solomon code) codes and such an ensemble for rates less than $1/2$ cannot be constructively specified. Therefore, if we can construct outer codes over the same field but with the length N much longer than 2^m-1, such that they behave almost like MDS codes when the codelength becomes sufficiently large, then to specify an ensemble with N codes for rates lower than $1/2$ becomes possible. Fortunately, the algebraic geometry method again provides a possibility to construct such outer code. Over every field GF(2^{2n}), the outer code we will construct in this section is a $[2^{2n(l+1)}-1, K, D]$ code, where l is an integer greater than 1 and $D \geq \left(2^{2n(l+1)}-1\right)-K+1-g$. Therefore, if g is relatively small it behaves almost like a MDS code. In fact, g is the genus of the curve used and is approximately $1/2(l-1)2^{nl}$. Thus, $g/2^{2n(l+1)}$ tends to 0 for $n \to \infty$. In the rest of this section, we will give the details of this construction.

Definition 1: Let $q = 2^n$. Let $\boldsymbol{F}_{q^2}$ be a finite field with q^2 elements. Let l be an integer such that $l \geq 2$. Given an element $a \in \boldsymbol{F}_{q^2}$, define $A_l(a)$ to be a set of all $(x_1, \cdots, x_l) \in \overline{\boldsymbol{F}_2}^l$ such that the following equations hold:

$$x_1 = a; \qquad x_{i+1}^q + x_{i+1} = x_i^{q+1}, \qquad \text{for } i = 1, \cdots, l-1,$$

where $\overline{\boldsymbol{F}_2}$ denotes the algebraic closure of $\boldsymbol{F}_2$. We denote $A(l,q) = \cup_{a\in \boldsymbol{F}_{q^2}} A_l(a)$.

Proposition 1:

$$A(l,q) \subseteq \boldsymbol{F}_{q^2}^l,$$

and it has q^{l+1} elements.

Proof: We follow the proof of [3, Section 1, Lemma].

Let $a \in F_{q^2}$. Suppose b is a solution of $Y^q + Y = a^{q+1}$, that is $b^q + b = a^{q+1}$. Raising to the qth power and using the fact that $a^{q(q+1)} = a^{q+1}$, we have

$$b^{q^2} + b^q = a^{q(q+1)} = a^{q+1} = b^q + b.$$

From this, we conclude that $b \in F_{q^2}$. Therefore, every solution of $A_l(a)$ is in $F_{q^2}^l$. This proves the first claim of the proposition. The last claim of the proposition is a consequence of the first conclusion and the fact that a polynomial of degree q has a most q zeros. □

Definition 2: Let l, m be integers, and $l \geq 2$. Define $P(l,q,m)$ to be the subspace of $F_{q^2}[x_1, \cdots, x_l]$ generated by

$$\left\{ x_1^{k_1} \cdots x_l^{k_l} | (k_1, \cdots, k_l) \in N^l, \sum_{i=1}^{l} k_i q^{l-i}(q+1)^{i-1} \leq m \right\},$$

where N is the set of all nonnegative integers.

Definition 3: Let N be an integer such that $0 < N < q^{l+1}$. Let $A = \{a_1, \cdots, a_N\} \subseteq A(l,q)$. A linear code $C(A,l,q,m)$ is defined by

$$C(A,l,q,m) = \{(f(a_1), \cdots, f(a_N)) | f \in P(l,q,m)\}.$$

We call A and $P(l,q,m)$ a defining set and a polynomial set, respectively, of $C(A,l,q,m)$. In Section IV, we will use this code as an outer code to construct a concatenated code.

Theorem 1: If $m < N$, then $C(A,l,q,m)$ is a linear $[N,K,D]$ code over F_{q^2} with

$$K \geq m + 1 - g(l,q) \quad \text{and} \quad D \geq N - m$$

Therefore,

$$D \geq N - K + 1 - g(l,q),$$

where

$$g(l,q) = \frac{1}{2}\left\{ \sum_{i=1}^{l-1} q^{l+1-i}(q+1)^{i-1} - (q+1)^{l-1} + 1 \right\}.$$

Furthermore, $K = m + 1 - g(l,q)$ if $m > 2g(l,q) - 2$. Therefore, if we take $N = q^{l+1} - 1$, then $g(l,q)/N \to 0, q \to \infty$.

Proof: See the Appendix. □

III. The Ensemble of Inner Codes

Let r be a positive rational number less than $1/2$. Then we always can write $r = n_1/(n_1 + n_2)$, where n_1 and n_2 are positive integers, $n_2 \geq n_1$ and $(n_1, n_2) = 1$. The aim of this section is to construct an ensemble of binary codes with rate r, such that the number of the distinct codes in this ensemble is $2^{n_2} - 1$ and the intersection of every two distinct codes is $\{(0, \cdots, 0)\}$. In Section IV, we use this ensemble as our inner codes to construct a concatenated code.

Let n be a positive integer. Then every element in the finite field F_{2^n} can be written as an element in $F_2[x]/\langle f \rangle$, where $\langle f \rangle$ is the ideal in $F_2[x]$ generated by f, an irreducible polynomial of degree n in $F_2[x]$. Let n_1, n_2 be positive integers such that $n_2 \geq n_1$. We have

$$F_{2^{n_1}} = \{\alpha(x) + \langle f_1 \rangle | \alpha(x) \in F_2[x] \quad \text{and} \quad \deg(\alpha(x)) < n_1\}$$

and

$$F_{2^{n_2}} = \{\beta(x) + \langle f_2 \rangle | \beta(x) \in F_2[x] \quad \text{and} \quad \deg(\beta(x)) < n_2\},$$

where $f_i, i = 1, 2$ are irreducible polynomials of degree n_i in $F_2[x]$.

Definition 4: For every $\beta \in F_{2^{n_2}}^*$, define a map ϕ_β from $F_{2^{n_1}}$ to $F_{2^{n_2}}$ by

$$\phi_\beta(\alpha) = \gamma(x) + \langle f_2 \rangle \text{ with } \quad \deg(\gamma(x)) < n_2,$$

where $\gamma(x) \equiv \beta(x)\alpha(x) \pmod{f_2}$ for $\beta(x) + \langle f_2 \rangle = \beta$ with $\deg(\beta(x)) < n_2$ and $\alpha = \alpha(x) + \langle f_1 \rangle \in F_{2^{n_1}}$ with $\deg(\alpha(x)) < n_1$.

It is easy to see that ϕ_β is well defined and $\phi_\beta(\alpha_1 + \alpha_2) = \phi_\beta(\alpha_1) + \phi_\beta(\alpha_2)$ for $\alpha_1, \alpha_2 \in F_{2^{n_1}}$.

Furthermore, we define a map ν_n from $F_{2^n} = F_2[x]/\langle f \rangle$ to F_2^n by

$$\nu_n(\alpha) := (a_0, \cdots, a_{n-1}),$$

for every $\alpha = \sum_{i=0}^{n-1} a_i x^i + \langle f \rangle \in F_{2^n}$. It is easy to see that ν_n is injective and linear over F_2. Now we can define our ensemble of binary codes.

Definition 5: For every $\beta \in F_{2^{n_2}}^*$, the binary code C_β of length $n_3 = n_1 + n_2$ is defined by

$$C_\beta := \{(\nu_{n_2}(\alpha), \nu_{n_2}(\phi_\beta(\alpha))) | \alpha \in F_{2^{n_1}}\}.$$

For the convenience of explanation in Section IV, we can describe this code as a map φ_β from $F_{2^{n_1}}$ to $F_2^{n_3}$ defined by

$$\varphi_\beta(\alpha) := (\nu_{n_1}(\alpha), \nu_{n_2}(\phi_\beta(\alpha))), \qquad \text{for every } \alpha \in F_{2^{n_1}}.$$

Proposition 2: For every $\beta \in F_{2^{n_2}}^*, C_\beta$ is a binary $[n_1 + n_2, n_1]$ linear code. For every two distinct $\beta, \beta' \in F_{2^{n_2}}^*, C_\beta \cap C_{\beta'} = \{(0, \cdots, 0)\}$. Therefore, there are $2^{n_2} - 1$ distinct codes in the ensemble.

In other words, if $c_1, \cdots, c_T$ are nonzero elements in $F_{2^{n_1}}$ and $\beta_1, \cdots, \beta_T$ are distinct elements in $F_{2^{n_2}}^*$, then $\varphi_{\beta_1}(c_1), \cdots, \varphi_{\beta_T}(c_T)$ are also different.

Proof: This follows immediately from Definition 4 and Definition 5. □

IV. The Concatenated Codes

In this section, we construct the sequence of binary concatenated codes, and prove that these codes meet the Zyablov bound for rate lower than 0.30.

Definition 6: Let l be an integer such that $l \geq 2$ and $0 < t \leq 1$ such that $t = t_1/t_2$ for some positive integers t_1 and t_2. Let $n = t_2 k$ and $q = 2^n$, where k is a positive integer. Let $N = q^{l+t} - 1$. Then, from Section II, one gets a linear code $C(A,l,q,m)$ with defining set A ($A \subseteq A(l,q)$) containing N elements. Furthermore, let $n_1 = 2n, n_2 = (l+t)n$ and $n_3 = n_1 + n_2 = (2+l+t)n$. A binary concatenated code $C_c(l,t,k,m)$ of length $M := (2+l+t)nN$ is defined by

$$\{(\varphi_{\beta_1}(c_1), \cdots, \varphi_{\beta_N}(c_N)) | (c_1, \cdots, c_N) \in C(A,l,q,m)\},$$

where $\{\beta_1, \cdots, \beta_N\} = F_{q^{l+t}}^*$ and φ_{β_i} is the map from $F_{2^{n_1}}$ to $F_2^{n_3}$ defined by Definition 5. We call $C(A,l,q,m)$ the outer code of the code $C_c(l,t,k,m)$.

Proposition 3: Let l be an integer ≥ 2. Let $\{t_{1k}\}$ and $\{t_{2k}\}$ be two sequences of integers such that $t_k := t_{1k}/t_{2k} \to t(k \to \infty)$ for some $0 < t \leq 1$. Let $r_k := 2/(2+l+t_k)$ and $r := 2/(2+l+t)$. Finally, let R_k, d_k and M_k be the rate, minimum distance and length, respectively, of the code $C_c(l,t_k,k,m_k)$. *Suppose* $\liminf R_k = R$ $(k \to \infty)$, then

$$\liminf_{k \to \infty} d_k/M_k \geq (1 - R/r)H_2^{-1}(1-r).$$

Proof: Suppose the outer code $C(A_k, l, p_k, m_k)$ is an $[N_k, K_k, D_k]$ code. Then, $D_k \geq N_k - K_k + 1 - g(l, q_k)$ by Theorem 1, where $q_k = 2^{n_k}$ and

$$R_k = \frac{2n_k K_k}{(2+l+t_k)n_k N_k} = r_k \frac{K_k}{N_k},$$

where $n_k = t_{2k}k$. Hence, we have

$$D_k \geq N_k(1 - R_k/r_k - g(l,q_k)/N_k) = \left(q_k^{(l+t_k)} - 1\right) \cdot \{1 - R_k/r_k + o(1)\}, \qquad k \to \infty,$$

since.

$$N_k = q_k^{(l+t_k)} - 1, g(l, q_k) = \left\{\sum_{i=1}^{l-1} q_k^{l+1-i}(q_k+1)^{i-1} - (q_k+1)^{l-1} + 1\right\} \bigg/ 2,$$
$$q_k = 2^{n_k} \quad \text{and} \quad t_k n_k \to \infty.$$

Now let

$$L_k = (2+l+t_k)n_k,$$
$$\delta_k = (l+t_k)/(2+l+t_k) = 1 - r_k,$$
$$\text{and} \quad M_{L_k} = D_k.$$

Then,

$$2^{-L_k\delta_k} M_{L_k} \geq 2^{-(l+t_k)n_k}\left(2^{(l+t_k)n_k} - 1\right) \cdot \{1 - R_k/r_k + o(1)\} = 1 - R_k/r_k + o(1).$$

Now, by Proposition 2 and the following lemma, we have

$$d_k \geq (1 - R_k/r_k)(2+l+t_k)n_k 2^{(l+t_k)n_k} \cdot \left\{H_2^{-1}(1-r_k) + 0(1)\right\}, \qquad k \to \infty.$$

Therefore,

$$\liminf_{k\to\infty} d_k/M_k \geq (1 - R/r)H_2^{-1}(1-r). \qquad \square$$

Lemma 1: Let $\gamma, \delta \in (0,1)$. Let $(M_L)_{L\in N}$ be a sequence of natural numbers with the property $M_L \cdot 2^{-L\delta} = \gamma + o(1)(L \to \infty)$. Let W be the sum of the weights of M_L distinct words in F_2^L. Then,

$$W \geq \gamma L 2^{L\delta}\left\{H_2^{-1}(\delta) + o(1)\right\}, \qquad L \to \infty.$$

Proof: See [4]. $\square$

Theorem 2: For overall rate R satisfying $0 < R < 0.30$, the Zyablov bound can be achieved by a sequence of concatenated codes $\{C_c(l, t_k, k, m_k)\}_{k=1}^{\infty}$, where $t_k = t_{1k}/t_{2k} \leq 1$ and l, t_{1k}, t_{2k} and $m_k \in N^*$.

Proof: Let $r_0 \in [0,1]$ such that

$$(1 - R/r_0)H_2^{-1}(1-r_0) = \max_{0\leq r\leq 1}\left\{(1-R/r)H_2^{-1}(1-r)\right\}.$$

Then, we know that $r_0 < 1/2$ (see [9, p. 314]) and $r_0 > R$. It is easy to see that there exists an integer $l \geq 2$ and $0 < t \leq 1$ such that $2/(2+l+t) = r_0$. Let $\{t_k\}$ be a sequence of rational numbers such that $t_k \to t$ $(k \to \infty)$. Denote $r_k := 2/(2+l+t_k)$, then $\lim_{k\to\infty} r_k = r_0$. Then, we get a sequence of concatenated codes $C_c(l, t_k, k, m)$ for every $m > 0$. Now choose m_k such that the rate R_k of $C_c(l, t_k, k, m_k)$ satisfies:

$$\liminf_{k\to\infty} R_k = \liminf_{k\to\infty} \frac{2n_k K_k}{(2+l+t_k)n_k N_k} = R, \qquad k \to \infty,$$

where $n_k = t_{2k}k(t_{1k}/t_{2k} := t_k)$ and $K_k = m_k + 1 - g(l, q_k)$ and $N_k = 2^{(l+t_k)n_k} - 1$ are the dimension and minimum distance, respectively, of the outer code $C(A_k, l, q_k, m_k)$ (this can always be done by Theorem 1).

Now by Proposition 3, for the sequence of concatenated codes $C_c(l, t_k, k, m_k)$ with the minimum distance d_k and the length M_k, we have

$$\liminf_{k\to\infty} d_k/M_k \geq (1 - R/r_0)H_2^{-1}(1-r_0).$$

This proves the theorem. $\square$

Remark 1: By using the dual code $C(A, l, q, m)$ as the outer code, we also can get the same result as the above theorem. For the details of the dual code $C(A, 2, q, m)^{\perp}$ we refer to [12] and [14].

Appendix A
Proof of Theorem 1

Definition 7: Let $q = 2^n$. Let F_{q^2} be a finite field with q^2 elements. Let $PG(l, q^2)$ be a l dimensional projective space over F_{q^2}. Let $\mathcal{H}(l, q)$ be a closed subscheme over F_2 in $PG(l, q^2)$ defined by the homogeneous ideal

$$I(l,q) = \left(X_i^{q+1} + X_{i+1}X_0^q + X_{i+1}^q X_0, \qquad i = 1, \cdots, l-1\right)$$

in $F_2[X_0, \cdots, X_l]$.

Proposition 4: The scheme $\mathcal{H}(l,q)$ is a projective, absolutely irreducible, reduced curve over F_2. It has exactly one point P_∞ at the hyperplane H with equation $x_0 = 0$. The curve is nonsingular outside P_∞ and goes through q^{l+1} rational points of $PG(l, q^2)$ outside the hyperplane H. The genus of this curve is

$$g(l,q) = \frac{1}{2}\left\{\sum_{i=1}^{l-1} q^{l+1-i}(q+1)^{i-1} - (q+1)^{l-1} + 1\right\}.$$

Proof: The proof is the same as the proof of [11, Propositions 3 and 4]. $\square$

The function field of $\mathcal{H}(l,q)$ is $K(l, q^2) := F_q^2(x_1, \cdots, x_l)$ with defining equations

$$x_i^{q+1} = x_{i+1} + x_{i+1}^q, \qquad i = 1, \cdots, l-1.$$

It is the function field of a Hermitian curve over F_q^2 when $l = 2$, see [12] and [14]. Therefore, we call the curve $\mathcal{H}(l,q)$ a generalized Hermitian curve.

This generalized Hermitian curve is an example of so called Artin–Schreier extensions, see [7]. Its properties also follow from the research in that paper. This curve was mentioned in [5, Example 7] too, but there it was not proved that this curve is absolutely irreducible.

The $q^{l+1}+1$ rational points of the curve $\mathcal{H}(l,q)$ are the following: the common pole P_∞ of x_i for $i = 1, \cdots, l$, and for any $a_1 \in F_{q^2}$ and any a_i such that $a_i^q + a_i = q_{i-1}^{q+1}$ for $i = 2, \cdots, l$, the common zero $P = P_{a_1,\cdots,a_l}$ of $x_i - a_i$ for $i = 1, \cdots, l$.

For a divisor G of $K(l, q^2)$, the space $L(G)$ is defined by $L(G) = \{f \in K(l, q^2) | (f) \geq -G\}$. The following result can be obtained by the same method as in the proof of [11, Proposition 6].

Proposition 5: For each $m \geq 0$

$$L(mP_\infty) = P(l, q, m),$$

where $P(l, q, m)$ is defined in Definition 2.

Proposition 6: Let D be a divisor of $K(l, q^2)$ defined by $D = \sum_{i=1}^{N} P_i$, where $0 < N \leq q^{l+1} - 1$ and P_i are different and chosen from rational points of $\mathcal{H}(l,q)$ such that $P_i \notin \{P_\infty, P_{0,\cdots,0}\}$. Let m be any nonnegative integer. Then, the algebraic–geometric code $C_L(D, mP_\infty)$ is equal to $C(A, l, q, m)$.

Proof: This follows immediately from the definition of $C(A, l, q, m)$ in Section II and the definition of algebraic–geometric code $C_L(D, mP_\infty)$, see [8, p. 55] and [15, p. 266]. □

Proof of Theorem 1: Since $C(A, l, q, m) = C_L(D, mP_\infty)$ by Proposition 6, the theorem follows from the well-known result about dimension and minimum distance of an algebraic–geometric code. For this result, we refer to [8, p. 57, Remark 3.8] and [15, p. 267, Theorem 3.1.1]. □

Acknowledgment

The author would like to thank F. W. Sun, J. Koolen, and Dr. R. Pellikaan for their discussions and comments. The author also would like to thank the referees for their detailed and helpful comments.

References

[1] N. Alon, J. Bruck, J. Naor, M. Naor, and R. M. Roth, "Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs," *IEEE Trans. Inform. Theory*, vol. 38, pt. I, pp. 509–516, Mar. 1992.

[2] G. D. Froney, Jr., *Concatenated Codes.* Cambridge, MA: MIT, 1966.

[3] A. Garcia and P. Viana, "Weierstrass points on certain non-classical curves," *Arch. Math.*, vol. 46, pp. 315–322, 1986.

[4] J. Justesen, "A class of constructive asymptotically good algebraic codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 652–656, 1972.

[5] J. Justesen, K. J. Larsen, H. E. Jensen, A. Havemose, and T. Høholdt, "Construction and decoding of class of algebraic–geometric codes," *IEEE Trans. Inform. Theory*, vol. 35, pp. 811–821, July 1989.

[6] G. L. Katsman, M. A. Tsfasman, and S. G. Vlăduţ, "Modular curve and codes with a polynominal construction," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 353–355, 1984.

[7] G. Lachaud, "Artin-Schreier curves, exponential sums, and the Carlitz–Uchiyama bound for geometric codes," *J. Numerical Theory*, vol. 39, pp. 18–40, 1991.

[8] J. H. van Lint and G. van der Geer, *Introduction to Coding Theory and Algebraic Geometry, DMV Seminar*, vol. 12. Berlin: Birkhäuser Verlag, 1988.

[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam, The Netherlands: North Holland, 1977.

[10] J. L. Massey, *Threshold Decoding.* Cambridge, MA: MIT Press, 1963.

[11] R. Pellikaan, B.-Z. Shen, and G. J. M. van Wee, "Which linear codes are algebraic–geometric?" *IEEE Trans. Inform. Theory*, vol. 37, pt. 1, pp. 583–602, May 1991.

[12] H. Stichtenoth, "A note on Hermitian codes over $GF(Q^2)$," *IEEE Trans. Inform. Theory*, vol. 34, pt. 11, pp. 1345–1348, Sept. 1988.

[13] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, "Superimposed concatenated codes," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 735–736, 1980.

[14] H. J. Tiersma, "Remarks on codes from Hermitian curves," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 605–609, July 1987.

[15] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic–Geometric Codes.* Dordrecht: Kluwer, 1991.

[16] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, "Modular curves, Shimura curves and Goppa codes, better than Vershamov–Gilbert bound," *Math. Nachrichten*, vol. 109, pp. 21–28, 1982.

[17] E. J. Weldon, Jr., "Some results on the problem of constructing asymptotically good error-correcting codes," *IEEE Trans Inform. Theory*, vol. IT-21, pp. 412–417, 1975.

[18] V. V. Zyablov, "An estimate of the complexity of constructing binary linear cascade codes," *Probl. Inform. Trans.*, vol. 7, no. 1, pp. 3–10, 1971.

On the Optimum Bit Orders with Respect to the State Complexity of Trellis Diagrams for Binary Linear Codes

Tadao Kasami, *Fellow, IEEE,* Toyoo Takata, *Member, IEEE,* Toru Fujiwara, *Member, IEEE,* and Shu Lin, *Fellow, IEEE*

***Abstract*—It was shown earlier that for a punctured Reed–Muller (RM) code or a primitive BCH code, which contains a punctured RM code of the same minimum distance as a large subcode, the state complexity of the minimal trellis diagram is much greater than that for an equivalent code obtained by a proper permutation on the bit positions. To find a permutation on the bit positions for a given code that minimizes the state complexity of its minimal trellis diagram is an interesting and challenging problem. This permutation problem is related to the generalized Hamming weight hierarchy of a code, and is shown that for RM codes, the standard binary order of bit positions is optimum at every bit position with respect to the state complexity of a minimal trellis diagram by using a theorem due to Wei. The state complexity of trellis diagram for the extended and permuted (64, 24) BCH code is discussed.**

***Index Terms*—Minimal trellis diagram, optimum bit order, and generalized Hamming weight hierarchy.**

I. Definitions and Concepts

Consider a binary linear (N, K) code C. For two integers h_1 and h_2 such that $0 \leq h_1 < h_2 \leq N$, let K_{h_1, h_2} (or $K_{h_1, h_2}[C]$) be the dimension of the linear subcode of C consisting of all codewords whose components are all zero except for the $h_2 - h_1$ components from the $(h_1 + 1)$th bit position to the h_2th bit position. For convenience, $K_{h, h}$ is defined as zero. For a nonnegative integer h not greater than N, the binary logarithm K_h (or $K_h[C]$) of the number of states of the minimal trellis diagram just after the hth bit position is given by Forney [7] and Muder [8] as

$$K_h[C] = K - K_{0,h}[C] - K_{h,N}[C]. \tag{1.1}$$

For integers h_1 and h_2 such that $h_1 \leq h_2$, let $[h_1, h_2]$ denote the set $h_1, h_1 + 1, \cdots, h_2$. For a permutation π on $[1, N]$, let $\pi[C]$ be the equivalent code of C obtained by permuting the components of each codeword in C based on π.

For a binary N-tuple $\boldsymbol{v}$, the support of $\boldsymbol{v}$, denoted $s(\boldsymbol{v})$, is defined as the set of indexes of bit positions where the components of $\boldsymbol{v}$ are nonzero. For a block code C of length N, let $s[C]$ denote the support of C, which is defined by $\cup_{\boldsymbol{v} \in C} s(\boldsymbol{v})$. For a linear (N, K) code C and a positive integer u less than $K + 1$, the uth generalized Hamming weight [6] of C, denoted $d_u[C]$, is defined as the size of the smallest support of a u-dimensional subcode of C. Then the following monotonicity holds [6]:

$$1 \leq d_1[C] < d_2[C] < \cdots < d_K[C] \leq N. \tag{1.2}$$

Manuscript received September 16, 1991; revised February 11, 1992. This work was supported by NASA Grant NAG 5-931, NSF Grants NCR-8813480 and NCR-9115400, and the Ministry of Education, Japan, under Grant (c) 63550255.

T. Kasami, T. Takata, and T. Fujiwara are with the Department of Information and Computer Sciences, Faculty of Engineering Science Osaka University, Toyonaka, Osaka 560, Japan.

S. Lin is with the Department of Electrical Engineering, University of Hawaii at Manoa, Holmes Hall 483, 2540 Dole Street, Honolulu, HI 96822.

IEEE Log Number 9203013.