On Repeated-Root Cyclic Codes

Guy Castagnoli, James. L. Massey, *Fellow, IEEE*, Philipp A. Schoeller, and Niklaus von Seemann

***Abstract*—A parity-check matrix for a q-ary repeated-root cyclic code is derived using the Hasse derivative. Then the minimum distance of a q-ary repeated-root cyclic code C is expressed in terms of the minimum distance of a certain simple-root cyclic code $\bar{C}$ that is determined by C. With the help of this result, several binary repeated-root cyclic codes of lengths up to $n = 62$ are shown to contain the largest known number of codewords for their given length and minimum distance. It is further shown that to a q-ary repeated-root cyclic code C of length $n = p^{\delta}\bar{n}$, where p is the characteristic of GF(q) and $\gcd(p, \bar{n}) = 1$, there corresponds a simple-root cyclic code $\hat{C}$ of rate and relative minimum distance at least as large as the corresponding values of C, however, of length $\bar{n}$, i.e., shorter by a factor of p^{δ}. The relative minimum distance $d_{\min}/n$ of q-ary repeated-root cyclic codes C of rate $r \geq R$ is proven to tend to zero as the largest multiplicity of a root of the generator $g(x)$ increases to infinity. It is further shown that repeated-root cyclic codes cannot be asymptotically better than simple-root cyclic codes.**

***Index Terms*—Cyclic codes, generator polynomial, formal derivative, Hasse derivative.**

I. Introduction

THE theory of cyclic codes, i.e., of linear block codes whose set of codewords is closed under cyclic shifting, enjoys a prominent place in the theory of error-correcting codes. The great majority of known constructions for good linear block codes yield cyclic codes or codes closely related thereto, such as the Justesen codes [1]. As is well known, an (n, k) q-ary cyclic code, i.e., a cyclic code of blocklength n whose codewords form a k-dimensional subspace of the vector space of n-tuples over the finite field GF(q), is completely described by its generator polynomial $g(x)$, which is a q-ary monic polynomial of degree $n-k$ that divides $x^n - 1$, in the manner that the q-ary n-tuple $[a_{n-1}, a_{n-2}, \cdots, a_0]$ is a codeword if and only if $g(x)$ divides $a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$, [2, p. 207]. (We shall refer to such a polynomial $a(x)$ corresponding to a codeword $[a_{n-1}, a_{n-2}, \cdots, a_0]$ as a code polynomial.) The code rate is $r = k/n$. Conversely, any q-ary monic polynomial $g(x)$ of degree less than n that divides $x^n - 1$ is the generator polynomial of an (n, k) q-ary cyclic code with $n-k$ equal to the degree of $g(x)$. To avoid the trivial case where the minimum distance $d_{\min}$ of the cyclic code would be 2, when given a q-ary monic polynomial with $g(0) \neq 0$ (i.e., when given a possible generator polynomial of a q-ary cyclic code), the length n of the cyclic code generated by $g(x)$ is always understood to mean the smallest positive integer n such that $g(x)$ divides $x^n - 1$. Virtually all previous studies of cyclic codes assume at the outset that $\gcd(n, p) = 1$ where p is the characteristic of GF(q). This is equivalent to assuming that $g(x)$ has no repeated irreducible factors, as follows from the fact that $g(x)$ divides $x^n - 1$ but not its formal derivative nx^{n-1} unless and only unless the latter is 0, which is equivalent to the condition that p divides n or, equivalently, that $\gcd(n, p) = p > 1$. By a *repeated-root cyclic code*, we shall mean a cyclic code for which $g(x)$ has at least one irreducible factor of multiplicity at least 2. The conventional cyclic codes where $\gcd(n, p) = 1$ will, for contrast, be called *simple-root cyclic codes*. Our choice of terminology stems from the fact that, in the splitting field $E = \text{GF}(q^s)$ of $g(x)$, the root-set of $g(x)$ (i.e., the multiset of solutions of $g(x) = 0$) will contain only simple roots if the code is a simple-root cyclic code, but will have at least one root of multiplicity at least 2 if the code is a repeated-root cyclic code. Some exceptions in the literature where repeated-root cyclic codes have been considered are the papers by Massey, Costello, and Justesen [3] and by Berman [4], which treat the case where the root-set has only one distinct root (of multiplicity necessarily $n-k$), and the paper [5] by Castagnoli, which considers asymptotic properties of the minimum distance of the class of repeated-root cyclic codes whose blocklengths are products of powers of a fixed finite set of primes.

The purpose of this paper is to present a rather complete theory of repeated-root cyclic codes. In Section II, we show that the derivative introduced by Hasse [6] more than 50 years ago, rather than the formal derivative, is the natural tool for studying repeated-root cyclic codes. In particular, it is shown with the aid of the Hasse-derivative how one can construct a parity-check matrix for a repeated-root cyclic code from its root-set. Section III contains the main result of this paper, showing that the minimum distance of a repeated-root cyclic code is uniquely determined by the minimum distances of a corresponding set of simple-root cyclic codes. This result effectively reduces the theory of repeated-root cyclic codes to the theory of "conventional" simple-root cyclic codes. A list of some specific repeated-root cyclic codes, which were found with the aid of this result, is given. Section IV shows that to a repeated-root cyclic code C of length $n = p^{\delta}\bar{n}$, where p is the characteristic of GF(q) and $\gcd(p, \bar{n}) = 1$, there corresponds a simple-root cyclic code $\bar{C}$ with rate and relative minimum distance at least as large as the corresponding values of C; however, the length of $\bar{C}$ is only $\bar{n}$, i.e., shorter by a factor equal to p^{δ}. The relative minimum distance $d_{\min}/n$ of q-ary repeated-root cyclic

Manuscript received December 6, 1989. This work was presented in part at the IEEE International Symposium on Information Theory, Ann Arbor, MI, October 6–9, 1986.

G. Castagnoli was with the Institute for Signal and Information Processing, Swiss Federal Institute of Technology, Zürich, Switzerland. He is now with IBM Switzerland, Postfach, CH-8022, Zürich, Switzerland.

J. L. Massey is with the Institute for Signal and Information Processing, Swiss Federal Institute of Technology, CH-8092, Zürich, Switzerland.

P. A. Schoeller and N. von Seemann were with the Institute for Signal and Information Processing, Swiss Federal Institute of Technology, Zürich, Switzerland. They are now with the GSM Gesellschaft für Synergie Management, Goethestrasse 74, D-8000 München 2, Germany.

IEEE Log Number 9041642.

codes C of rate $r \geq R$ is proven to tend to zero when the largest multiplicity of a root of the generator $g(x)$ tends to infinity. This result is used to show that the existence of an asymptotically-good sequence of cyclic codes would imply the existence of an asymptotically-good sequence of simple-root cyclic codes. This effectively reduces the question of whether asymptotically-good cyclic codes exist to the question of whether asymptotically-good simple-root cyclic codes exist. Section V contains some summarizing remarks.

II. Hasse Derivatives Applied to Repeated-Root Cyclic Codes

Let $a(x) = \sum_i a_i x^i$ be a polynomial (or a formal power series) with coefficients in a field F. Then the jth formal derivative of $a(x)$ is the polynomial (or formal power series)

$$a^{(j)}(x) = \sum_i i(i-1)\cdots(i-j+1)\cdot a_i x^{i-j}$$

$$= j! \cdot \sum_i \binom{i}{j} a_i x^{i-j}. \tag{1}$$

The polynomial (or formal power series)

$$a^{[j]}(x) = \sum_i \binom{i}{j} \cdot a_i x^{i-j} \tag{2}$$

is called, in honor of its originator [6], the jth Hasse derivative of $a(x)$ (and is sometimes also called the jth hyper-derivative of $a(x)$). The fact that

$$a^{(m)}(x) = m! \cdot a^{[m]}(x) \tag{3}$$

explains why the Hasse derivative is much more useful than the formal derivative in fields with a prime characteristic p because then $m! = 0$ and hence also $a^{(m)}(x) = 0$ for all $m \geq p$. Note that it is always true that $a^{(1)}(x) = a^{[1]}(x)$.

Let $F[x]$ denote the set of polynomials in the indeterminate x with coefficients in a field F. A key property of Hasse derivatives is given in the following test, a proof of which may be found in [7, p. 305].

Repeated Factor Test: If $m(x)$ is irreducible in $F[x]$ with $m^{(1)}(x) \neq 0$ and if e is any positive integer, then $[m(x)]^e$ divides $a(x)$ if and only if $m(x)$ divides $a(x)$ and its first $e-1$ Hasse derivatives.

If F is either a finite field (as will always be the case hereafter) or a field of characteristic 0, then every $m(x)$ that is irreducible in $F[x]$ automatically has $m^{(1)}(x) \neq 0$. However, if F is an infinite field with prime characteristic p, it is possible that $m(x)$ is irreducible in $F[x]$ but that $m^{(1)}(x) = 0$. In this case, the condition $m^{(1)}(x) \neq 0$ in the test is essential.

With the aid of the Hasse derivative, it is a simple matter to construct a parity-check matrix for a repeated-root cyclic code when given the root-set of its generator polynomial $g(x)$. We remark that the attempt to carry out such a construction for q-ary codes with the use of the formal derivative, as given for instance in [2, p. 216], fails when some root of $g(x)$ has multiplicity p or greater, where p is the characteristic of GF(q).

Parity-Check Matrix Construction: Let $g(x)$ generate a q-ary (n, k) cyclic code C. Then the matrix $\bar{H}$ having as rows the n-tuples $\left[\binom{n-1}{j}\alpha^{n-1}, \binom{n-2}{j}\alpha^{n-2}, \cdots, \binom{1}{j}\alpha, \binom{0}{j}\right]$, where α is in the root-set of $g(x)$ with multiplicity e and $0 \leq j < e$, is a parity-check matrix for the q^s-ary (n, k) cyclic code $\bar{C}$ generated by $g(x)$ over the splitting field $E = \mathrm{GF}(q^s)$ of $g(x)$. A parity-check matrix H for C can be derived from $\bar{H}$ essentially by replacing the entries of $\bar{H}$ by their q-ary column vector representations.

Proof: The q^s-ary polynomial $a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$ is a code polynomial of $\bar{C}$ if and only if the fact that α is an element of multiplicity e in the root-set of $g(x)$ implies

$$a^{[j]}(\alpha) = 0, \qquad \text{for } j = 0, 1, \cdots, e-1. \tag{4}$$

The left side of (4) can be written in matrix form as

$$[a_{n-1}, a_{n-2}, \cdots, a_0] \cdot \left[\binom{n-1}{j}\alpha^{n-1}, \binom{n-2}{j}\alpha^{n-2}, \cdots, \binom{1}{j}\alpha, \binom{0}{j}\right]^T, \tag{5}$$

where the superscript T denotes transpose. Thus (4) is equivalent to the statement that the n-tuples

$$\left[\binom{n-1}{j}\alpha^{n-1}, \binom{n-2}{j}\alpha^{n-2}, \cdots, \binom{1}{j}\alpha, \binom{0}{j}\right] \qquad \text{for } j = 0, 1, \cdots, e-1$$

are orthogonal to every codeword of $\bar{C}$ or, equivalently, that these vectors are in the dual code of $\bar{C}$. Since $[a_{n-1}, a_{n-2}, \cdots, a_0]$ is a codeword of $\bar{C}$ if and only if (4) holds for every element α of the root-set of $g(x)$ and every j satisfying $0 < j \leq e-1$, $\bar{H}$ is indeed a parity-check matrix of $\bar{C}$. Deriving a parity-check matrix H for C from the parity-check matrix $\bar{H}$ of $\bar{C}$ is a standard technique, see [2, p. 214]. □

III. Minimum Distance of Repeated-Root Cyclic Codes

Let C be a q-ary repeated-root cyclic code of length $n = p^\delta \bar{n}$, where p is the characteristic of GF(q) and

$$\gcd(p, \bar{n}) = 1.$$

Consider the factorization

$$g(x) = \prod_{i=1}^{l} m_i(x)^{e_i} \tag{6}$$

of the generator polynomial $g(x)$ of C into distinct monic irreducible polynomials $m_i(x)$ of multiplicity e_i. The multiplicity δ of p in the blocklength n is then equal to the maximum of the terms $\lceil \log_p e_i \rceil$ for $i = 1, \cdots, l$. The minimum distance $d_{\min}$ of C will be investigated using the following class of simple-root cyclic codes $\bar{C}_t$ of length $\bar{n}$, where $0 \leq t \leq p^\delta - 1$. The generator of $\bar{C}_t$, $\bar{g}_t(x)$, is defined as the product of those irreducible factors $m_i(x)$ of $g(x)$ that occur with multiplicity $e_i > t$ in $g(x)$. If this product turns out to be $x^n - 1$, then the corresponding $\bar{C}_t$ contains only the all-zero codeword and we set $d_{\min}(\bar{C}_t) = \infty$. If all e_i satisfy $e_i \leq t$, then, by way of convention, $\bar{g}_t(x) = 1$ and $d_{\min}(\bar{C}_t) = 1$. We shall also need the fact [2], [3] that the Hamming weight (i.e., the number of nonzero coefficients) of the polynomial $(x-1)^t$ is given by

$$w_H\big((x-1)^t\big) = P_t, \tag{7}$$

where

$$P_t = \prod_i (t_i + 1), \tag{8}$$

and where the t_i's are the coefficients of the radix-p expansion of t.

Lemma 1: The minimum distance $d_{\min}(C)$ of the repeated-root cyclic code C defined above satisfies

$$d_{\min}(C) \le P_t \cdot d_{\min}(\bar{C}_t), \qquad \text{for all } t \in \{0,1,\cdots,p^\delta - 1\}. \tag{9}$$

Proof: In the sequel, we will write $a(x) \bmod b(x)$ to denote the remainder of $a(x)$ upon dividing by $b(x)$. Let $\bar{v}_t(x)$ be a nonzero code polynomial of $\bar{C}_t$, then the polynomial

$$\bar{c}_t(x) = (x^{\bar{n}} - 1)^t \bar{v}_t(x)^{p^\delta} \bmod x^n - 1 \tag{10}$$

is a nonzero code polynomial in C as we now show. Because $x^n - 1 = (x^{\bar{n}} - 1)^{p^\delta}$ and $t < p^\delta$, it follows from (10) that all those irreducible factors of $x^{\bar{n}} - 1$ that occur in $g(x)$ with a multiplicity not exceeding t are contained in $\bar{c}_t(x)$ with multiplicity at least t. Moreover, those irreducible factors of $x^{\bar{n}} - 1$ that occur in $g(x)$ with a multiplicity greater than t are also factors of $\bar{v}_t(x)$ and hence are contained in $\bar{c}_t(x)$ with a multiplicity of at least p^δ.[1] Therefore, $\bar{c}_t(x)$ is divisible by $g(x)$ and hence is a code polynomial of C. Moreover, not every root of $x^{\bar{n}} - 1$ can be a root of $\bar{v}_t(x)$ since this latter polynomial has degree less than $\bar{n}$. Thus, there must be a root of $x^{\bar{n}} - 1$ whose multiplicity in $(x^{\bar{n}} - 1)^t \bar{v}_t(x)^{p^\delta}$ is exactly t and hence this latter polynomial cannot be divisible by $x^n - 1 = (x^{\bar{n}} - 1)^{p^\delta}$. Thus, $\bar{c}_t(x)$ is indeed a nonzero code polynomial of C. It follows that $g(x)$ divides $\bar{c}_t(x)$. The Hamming weight of $\bar{c}_t(x)$ satisfies

$$\begin{aligned} w_H(\bar{c}_t(x)) &= w_H\left((x^{\bar{n}} - 1)^t \bar{v}_t(x)^{p^\delta} \bmod (x^n - 1)\right) \\ &\le w_H\left((x^{\bar{n}} - 1)^t \bar{v}_t(x)^{p^\delta}\right) \\ &\le w_H\left((x^{\bar{n}} - 1)^t\right) \cdot w_H\left(\bar{v}_t(x)^{p^\delta}\right) \\ &= w_H\left((x-1)^t\right) \cdot w_H(\bar{v}_t(x)) \\ &= P_t \cdot w_H(\bar{v}_t(x)), \end{aligned} \tag{11}$$

as follows from the fact that the operation modulo $x^n - 1$ cannot increase Hamming weight and from (7).[2] Now choosing $\bar{v}_t(x)$ so that $w_H(\bar{v}_t(x)) = d_{\min}(\bar{C}_t)$, we see that (9) follows from (11), which proves the lemma. □

If $t < t'$, then $\bar{g}_{t'}(x)$ divides $\bar{g}_t(x)$, i.e., $\bar{C}_t \subseteq \bar{C}_{t'}$ and hence $d_{\min}(\bar{C}_t) \ge d_{\min}(\bar{C}_{t'})$. If in addition $P_t \ge P_{t'}$, then the upper bound (9) with t cannot be better than that with t'. The only interesting values of t in (9), therefore, are those values $t < p^\delta$ for which

$$P_t < P_{t'}, \qquad \text{for all } t' \in \{t+1, t+2, \cdots, p^\delta - 1\}. \tag{12}$$

The set T of values of $t < p^\delta$ satisfying (12) consists of $t = 0$ yielding $P_0 = 1$ and the values

$$t = (p-1)p^{\delta-1} + \cdots + (p-1)p^{\delta-(j-1)} + rp^{\delta-j} \tag{13a}$$

yielding

$$P_t = p^{j-1} \cdot (r+1), \tag{13b}$$

where

$$j \in \{1,\cdots,\delta\} \qquad \text{and } r \in \{1,\cdots,p-1\}. \tag{13c}$$

We shall now prove that the minimum distance of the repeated-root cyclic code C is equal to the smallest of the expressions $P_t \cdot d_{\min}(\bar{C}_t)$ on the right of (9) by proving that there exists a minimum weight nonzero code polynomial in C of the form (10) for some $\bar{t} \in T$.

Lemma 2: Let C be a q-ary repeated-root cyclic code of blocklength $n = p^\delta \bar{n}$ with p the characteristic of GF(q), $\delta \ge 1$ and $\gcd(p, \bar{n}) = 1$. Let $c(x)$ be an arbitrary nonzero code polynomial in C and write $c(x)$ as

$$c(x) = (x^{\bar{n}} - 1)^t v(x), \tag{14}$$

where $x^{\bar{n}} - 1$ is not a divisor of $v(x)$. Then, if $\bar{t} = \min\{\bar{t} \in T | \bar{t} \ge t\}$, the polynomial

$$\bar{c}_{\bar{t}}(x) = \left((x^{\bar{n}} - 1)^{\bar{t}} \cdot \bar{v}(x)^{p^\delta}\right) \bmod (x^n - 1), \tag{15}$$

where

$$\bar{v}(x) = v(x) \bmod x^{\bar{n}} - 1, \tag{16}$$

is also a nonzero code polynomial of C and satisfies

$$w_H(\bar{c}_{\bar{t}}(x)) \le w_H(c(x)). \tag{17}$$

Proof: Because $g(x)$ divides $c(x)$, the polynomial $v(x)$ in (14) contains all factors $m_j(x)$ of $g(x)$ which occur in $g(x)$ with a multiplicity e_j greater than t and hence is divisible by $\bar{g}_t(x)$. Then, since by hypothesis $x^{\bar{n}} - 1$ does not divide $v(x)$, $\bar{v}(x)$ is a nonzero code polynomial of $\bar{C}_t$ and of $\bar{C}_{\bar{t}} \supseteq \bar{C}_t$. Therefore, by the same argument as used in the proof of Lemma 1, $\bar{c}_{\bar{t}}(x)$ is a nonzero code polynomial of C. We now prove (17). Writing $v(x)$ in the form

$$v(x) = \sum_{i=0}^{\bar{n}-1} x^i v_i(x^{\bar{n}}), \tag{18}$$

we note first that

$$\begin{aligned} w_H(c(x)) &= w_H\left((x^{\bar{n}} - 1)^t v(x)\right) \\ &= w_H\left((x^{\bar{n}} - 1)^t \cdot \sum_{i=0}^{\bar{n}-1} x^i v_i(x^{\bar{n}})\right) \\ &= w_H\left(\sum_{i=0}^{\bar{n}-1} x^i \cdot \left((x^{\bar{n}} - 1)^t v_i(x^n)\right)\right) \\ &= \sum_{i=0}^{\bar{n}-1} w_H\left((x^n - 1)^t v_i(x^{\bar{n}})\right) \\ &= \sum_{i=0}^{\bar{n}-1} w_H\left((x-1)^t v_i(x)\right). \end{aligned} \tag{19}$$

According to [3, Theorem 6.1], it follows that, for each $v_i(x) \ne 0$,

$$\begin{aligned} w_H\left((x-1)^t v_i(x)\right) &\ge \min_{p^\delta > \bar{t} \ge t} \left(w_H\left((x-1)^{\bar{t}}\right)\right) \\ &= \min_{p^\delta > \bar{t} \ge t} P_{\bar{t}} = P_{\bar{t}}, \end{aligned} \tag{20}$$

where we have used (7) and the fact that the multiplicity of $x^{\bar{n}} - 1$ in $v_i(x^{\bar{n}})$ is less than $p^\delta - t$. Therefore, if N_v is the number of nonzero $v_i(x)$'s in (18), then (19) and (20) yield

$$w_H(c(x)) \ge N_v \cdot P_{\bar{t}}. \tag{21}$$

[1] Because of the reduction modulo $x^n - 1$ in (10), the multiplicity is actually equal to p^δ.

[2] Since $t < p^\delta$, $\deg \bar{v}_t(x) < \bar{n}$, and since $\gcd(\bar{n}, p^\delta) = 1$, the second inequality in (11) is actually an equality.

With the same reasoning as in (11), we can upper bound the Hamming weight of $\bar{c}_{\bar{i}}(x)$ by

$$w_H(\bar{c}_{\bar{i}}(x)) \le w_H\big((x-1)^{\bar{i}}\big)\cdot w_H(\bar{v}(x)) = P_{\bar{i}}\cdot w_H(\bar{v}(x)). \tag{22}$$

Since $f(x^n) \bmod (x^n-1) = f(1)$ for any polynomial $f(x)$, we have

$$v_i(x^{\bar{n}}) \bmod (x^{\bar{n}}-1) = v_i(1). \tag{23}$$

Therefore, using (18), we have

$$\bar{v}(x) = v(x) \bmod (x^{\bar{n}}-1) = \left(\sum_{i=0}^{\bar{n}-1} x^i v_i(x^{\bar{n}})\right) \bmod (x^{\bar{n}}-1)$$

$$= \sum_{i=0}^{\bar{n}-1} x^i (v_i(x^{\bar{n}}) \bmod (x^{\bar{n}}-1)) = \sum_{i=0}^{\bar{n}-1} x^i v_i(1) \tag{24}$$

and thus

$$w_H(\bar{v}(x)) = N_{\bar{v}} \tag{25}$$

where $N_{\bar{v}}$ is the number of i's for which $v_i(1) \neq 0$. Inequality (22) can now be written as

$$w_H(\bar{c}_{\bar{i}}(x)) \le P_{\bar{i}}\cdot N_{\bar{v}}. \tag{26}$$

Now, $N_v \ge N_{\bar{v}}$, since $v_i(1) \neq 0 \Rightarrow v_i(x) \neq 0$. From (21) and (26), we thus obtain

$$w_H(c(x)) \ge N_v \cdot P_{\bar{i}} \ge N_{\bar{v}} \cdot P_{\bar{i}} \ge w_H(\bar{c}_{\bar{i}}(x)), \tag{27}$$

which implies (17). □

Theorem 1: Let C be a q-ary repeated-root cyclic code of blocklength $n = p^{\delta}\bar{n}$ with p the characteristic of GF(q), $\delta \ge 1$ and $\gcd(p, \bar{n}) = 1$. Then

$$d_{\min}(C) = P_{\bar{i}}\cdot d_{\min}(\bar{C}_{\bar{i}}) \tag{28}$$

for some $\bar{i} \in T$, where T is the set defined following (12).

Proof: If in Lemma 2 we choose $c(x)$ to be a minimum weight nonzero code polynomial of C, then $\bar{c}_{\bar{i}}$ of (15) will also have minimum Hamming weight. Inequality (27) then reads as

$$w_H(c(x)) = P_{\bar{i}}\cdot N_v = P_{\bar{i}}\cdot N_{\bar{v}} = w_H(\bar{c}_{\bar{i}}(x)). \tag{29}$$

With the aid of (29) and (25), we can express the minimum distance of C as

$$d_{\min}(C) = w_H(\bar{v}(x))\cdot P_{\bar{i}}. \tag{30}$$

Now, $\bar{v}(x)$ must be a minimum weight nonzero code polynomial of $\bar{C}_{\bar{i}}$, for else there would exist a nonzero code polynomial of C of the form (10) with $t = \bar{i}$ and Hamming weight bounded by (11), which would be less than the right side of (30). Thus, $w_H(\bar{v}(x)) = d_{\min}(\bar{C}_{\bar{i}})$ and inserting this in (30) gives (28).

With the aid of Theorem 1, several repeated-root binary cyclic codes were found that contain the maximum number of codewords among all known binary codes of the same length and minimum distance as was established by comparison of their parameters to those in [9, Appendix A]. These codes are listed in Table I. The codes with distance $d = 4$ in this table for $n = 6$, 14, 30, and 62 are instances of the infinite optimum family of repeated-root cyclic codes, found by van Lint [10], whose codewords are the even weight codewords in a shortened Hamming code.

TABLE I
SOME BINARY REPEATED-ROOT CYCLIC CODES WITH A MAXIMUM NUMBER OF CODEWORDS AMONG ALL BINARY BLOCKCODES WITH THE SAME LENGTH AND MINIMUM DISTANCE

n	$d_{\min}$	$n-k$	Roots
6	4	4	0(2), 1(1)
12	8	10	0(4), 1(3)
14	4	5	0(2), 1(1)
14	8	11	0(2), 1(2), 3(1)
18	12	16	0(2), 1(2), 3(1)
24	16	22	0(8), 1(7)
28	4	6	0(3), 1(1)
28	16	25	0(4), 1(4), 3(3)
30	4	6	0(2), 1(1)
30	16	26	0(2), 1(2), 3(2), 5(2), 7(1)
30	20	28	0(2), 1(2), 3(2), 5(1), 7(2)
36	24	34	0(4), 1(4), 3(3)
42	28	40	0(2), 1(2), 3(2), 5(2), 7(1), 9(2)
60	4	7	0(3), 1(1)
62	4	7	0(2), 1(1)

The codes are specified by the root of the generator polynomial $g(x)$ in the manner that 3(2) indicates that α^3 has multiplicity 2 in $g(x)$ where α is a fixed element of order $\bar{n}$ in the appropriate extension of GF(2) and $\bar{n}$ is the largest odd factor of n. Only one root in each conjugate class is specified.

IV. Asymptotic Badness of Repeated-Root Cyclic Codes

The following theorem will be the key to our demonstration of the "asymptotic badness' of repeated-root cyclic codes.

Theorem 2: Let C be a q-ary repeated-root cyclic code of blocklength $n = p^{\delta}\bar{n}$ with p the characteristic of GF(q), $\delta \ge 1$ and $\gcd(p, \bar{n}) = 1$. Then there exists a simple-root cyclic code $\hat{C}$ of length $\bar{n}$ with both rate and relative minimum distance at least as large as the corresponding values for C.

Proof: Let $g(x)$ be the generator polynomial of C and let $\hat{C}$ be the length $\bar{n}$ simple-root cyclic code generated by the product $\hat{g}(x)$ of those irreducible factors of $g(x)$ that occur in $g(x)$ with multiplicity p^{δ}. If $g(x)$ should possess no such factors, then we take $\hat{g}(x) = 1$. Since $p^{\delta}\cdot \deg \hat{g} \le \deg g$, the rate $\hat{r}$ of $\hat{C}$ is at least as large as the rate r of C. Observe that $\hat{C}$ is the code $\bar{C}_{p^{\delta}-1}$ in the notation of Section III. Lemma 1 now gives us the following upper bound on $d_{\min}(C)$ in terms of $d_{\min}(\hat{C})$:

$$d_{\min}(C) \le P_{p^{\delta}-1}\cdot d_{\min}(\hat{C}). \tag{31}$$

Since $P_{p^{\delta}-1} = p^{\delta}$, dividing both sides of inequality (31) by $n = p^{\delta}\bar{n}$ gives

$$\frac{d_{\min}(C)}{n} \le \frac{d_{\min}(\hat{C})}{\bar{n}}, \tag{32}$$

i.e., the relative minimum distance of the simple-root cyclic code $\hat{C}$ is no smaller than the relative minimum distance of the repeated-root cyclic code C, which proves the theorem. □

To avoid misinterpretation of Theorem 2, one should be careful to note that the blocklength of $\hat{C}$ is only $\bar{n}$ while the blocklength of C is $p^{\delta}\bar{n}$, i.e., larger by a factor of p^{δ}. Hence the conclusion that repeated-root cyclic codes are not better than simple-root cyclic codes cannot be drawn from Theo-

rem 2. However, in the limit as δ in $n = p^{\delta}n$ tends to infinity, we can use Lemma 1 to prove that repeated-root cyclic codes of rate $r \geq R$ are asymptotically bad.

Lemma 3: Let p be the characteristic of GF(q). Then, for any R ($0 < R < 1$), there exists a constant $\gamma(R)$ such that, for any q-ary repeated-root cyclic code C of rate $r > R > 0$ and blocklength $n = p^{\delta}\bar{n}$,

$$d_{\min} \leq p^{\gamma(R)}\bar{n}. \tag{33}$$

Proof: Let $g(x)$ be the generator of a q-ary repeated-root cyclic code C of rate $r > R$ and blocklength $n = p^{\delta}\bar{n}$. Then $\deg g < (1-R)n$; therefore at least one irreducible factor of $x^{\bar{n}} - 1$ must occur in $g(x)$ with multiplicity less than $(1-R)p^{\delta}$. Now, if $t \geq \lfloor (1-R)p^{\delta} \rfloor$, then $\bar{g}_t(x)$, the product of those irreducible factors of $g(x)$ that occur in $g(x)$ with multiplicity greater than t, is not $x^n - 1$ and thus generates a nonzero simple-root cyclic code $\bar{C}_t$ such that Lemma 1 applies and yields

$$d_{\min}(C) \leq P_t \cdot d_{\min}(\bar{C}_t) \leq P_t \cdot \bar{n}. \tag{34}$$

Inequality (33) now follows from (34) upon defining

$$\gamma(R) \stackrel{\text{def}}{=} \max_{\delta \geq 1} \left(\min_{p^{\delta} > t \geq \lfloor (1-R)p^{\delta} \rfloor} \log_p P_t \right). \tag{35}$$

The expression on the right of (35) can be seen to be finite as follows. If

$$1 - R = \sum_{i=1}^{\infty} s_i \cdot p^{-i} \tag{36}$$

is the expansion of $1 - R$ into powers of p, then

$$\lfloor (1-R)p^{\delta} \rfloor = \sum_{i=1}^{\delta} s_i \cdot p^{\delta - i}. \tag{37}$$

Therefore, as follows from the definition (8) of P_t, if $s_1 = s_2 = \cdots = s_{j0} = p - 1$ and $s_{j0+1} = u < p - 1$, where $j_0 < \delta$, then

$$\max_{\delta \geq 1} \left(\min_{p^{\delta} > t \geq \lfloor (1-R)p^{\delta} \rfloor} P_t \right) = \begin{cases} p^{j_0} \cdot (u+1) & \text{if } s_j = 0, \quad \text{all } j > j_0 + 1 \\ p^{j_0} \cdot (u+2), & \text{if there is an } s_j \neq 0 \text{ with } j > j_0 + 1. \end{cases} \tag{38}$$

□

From equality (33) of Lemma 3, we see directly that the relative minimum distance $d_{\min}(C)/n$ of q-ary repeated-root cyclic codes of rate $r > R$ is arbitrarily small when δ in $n = p^{\delta}n$ is sufficiently large, i.e., we have the following theorem.

Theorem 3: Any sequence of q-ary repeated-root cyclic codes C_i of rates $r_i \geq r > 0$ and blocklengths $n_i = p^{\delta_i}\bar{n}_i$ such that

$$\liminf_{i \to \infty} \delta_i = \infty, \tag{39}$$

satisfies

$$\lim_{i \to \infty} \frac{d_{\min}(C_i)}{n_i} = 0. \tag{40}$$

From Theorem 3 one can conclude directly only that repeated-root cyclic codes whose multiplicities grow without bound must be asymptotically bad. Combining this result with Theorem 2, however, shows that repeated-root cyclic codes cannot be asymptotically better than simple-root cyclic codes.

Theorem 4: If there exists a sequence of q-ary cyclic codes C_i of rates $r_i \geq r > 0$ and blocklengths n_i such that

$$\lim_{i \to \infty} n_i = \infty \tag{41}$$

and

$$\liminf_{i \to \infty} \frac{d_{\min}(C_i)}{n_i} = \Delta > 0, \tag{42}$$

then there also exists a sequence of q-ary simple-root cyclic codes $\hat{C}_i$ of rates $\hat{r}_i \geq r > 0$ and blocklengths $\hat{n}_i$ such that

$$\lim_{i \to \infty} \hat{n}_i = \infty \tag{43}$$

and

$$\liminf_{i \to \infty} \frac{d_{\min}(\hat{C}_i)}{\hat{n}_i} \geq \Delta > 0. \tag{44}$$

Proof: One simply needs to replace a repeated-root code C_i in the original sequence by its simple-root counterpart $\hat{C}_i$ as constructed in the proof of Theorem 2. Since the relative minimum distance is not thereby decreased, (44) must hold and it remains only to show that (43) holds. But the failure of (43) to hold would imply the existence of an $\hat{n}$ such that $n_i \leq p^{\delta_i}\hat{n}$ for infinitely many indices i. Thus, (41) would imply that the corresponding subsequence of the original sequence of cyclic codes fulfills the hypothesis of Theorem 3, and thus that (40) holds for this subsequence in contradiction to (42). Hence (43) must hold, which proves the theorem. □

V. Summary and Remarks

In this paper we have given a parity-check matrix for repeated-root cyclic codes based on the Hasse derivative. We pointed out that the use of the conventional formal derivative fails whenever the generator polynomial contains roots with multiplicities at least as large as the characteristic p of the ground field GF(q). We then derived an expression for the minimum distance $d_{\min}$ of q-ary repeated-root cyclic codes in terms of the minimum distance of related simple-root cyclic codes. This result was used to find several binary repeated-root cyclic codes that have a maximal number of codewords among all binary block codes of the same length and minimum distance. We also showed that if p is the characteristic of GF(q), then to a q-ary repeated-root cyclic code C of length $n = p^{\delta}\bar{n}$ with $\gcd(p, \bar{n}) = 1$ and rate r, relative minimum distance $d_{\min}/n = d$, there corresponds a simple-root cyclic code $\bar{C}$ of length $\bar{n}$ whose rate and relative minimum distance are at least as large as r and d, respectively. We also showed that, if p is the characteristic of GF(q), then any sequence of q-ary repeated-root cyclic codes of lengths $n_i = p^{\delta_i}\bar{n}_i$, rates $r_i \geq r > 0$ and in which the maximum multiplicity of a root of the generator polynomial $g_i(x)$ of C_i increases to infinity with i, has an asymptotically vanishing relative minimum distance. Finally, we showed that, if an asymptotically-good sequence of cyclic codes exists, then there also exists a sequence of simple-root cyclic codes whose "asymptotic goodness" is at least as good.

Van Lint [10] has recently given a more combinatorial approach to repeated-root cyclic codes that in many ways complements the algebraic approach of this paper. The reader is referred to his paper both for the additional insight

that it offers and also for many interesting constructions of such codes that it contains.

Acknowledgment

The authors are grateful to the referees for their careful reading of the original manuscript and their helpful suggestions.

References

[1] J. Justesen, "A class of constructive asymptotically good algebraic codes," *IEEE Trans. Inform. Theory*, vol. IT-18, no. 5, pp. 652–656, Sept. 1972.
[2] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, Second ed. Cambridge, MA: MIT Press, 1972.
[3] J. L. Massey, D. J. Costello, and J. Justesen, "Polynomial weights and code constructions," *IEEE Trans. Inform. Theory*, vol. IT-19, no. 1, pp. 101–110, Jan. 1973.
[4] S. D. Berman, "On the theory of group codes," *Cybern.*, vol. 3, no. 1, pp. 25–31, 1967.
[5] G. Castagnoli, "On the asymptotic badness of cyclic codes with blocklengths composed from a fixed set of prime factors," pp. 164–168, in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer Lecture Notes in Computer Science*, vol. 357, 1989.
[6] H. Hasse, "Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik," *J. Reine. Ang. Math.*, vol. 175, pp. 50–54, 1936.
[7] R. Lidl and H. Niederreiter, *Finite Fields*. Reading, MA: Addison-Wesley, 1983.
[8] Ph. Schoeller and N. von Seemann, *Binary Repeated-Root Cyclic Codes*, Diploma thesis, Inst. for Signal and Inform. Processing, Swiss Fed. Inst. of Technol., Zürich, Switzerland, 1983.
[9] F. J. MacWilliams and N. J. A Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.
[10] J. H. van Lint, "Repeated-root cyclic codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 2, pp. 343–345, Mar. 1991.