4-1972

Generalized Finite-Geometry Codes

Carlos R.P. Hartmann
Syracuse University, chartman@syr.edu

Luther D. Rudolph
Syracuse University

72-2

GENERALIZED FINITE-GEOMETRY CODES

CARLOS R. P. HARTMANN
LUTHER D. RUDOLPH

APRIL, 1972

SYSTEMS AND INFORMATION SCIENCE
SYRACUSE UNIVERSITY

GENERALIZED FINITE-GEOMETRY CODES

Carlos R. P. Hartmann
Luther D. Rudolph

SYSTEMS AND INFORMATION SCIENCE
SYRACUSE UNIVERSITY
SYRACUSE, NEW YORK 13210
(315) 476-5541 Ext. 2368

ABSTRACT

A technique is presented for constructing cyclic codes that retain many of the combinatorial properties of finite-geometry codes, but are often superior to geometry codes. It is shown that L-step orthogonalization is applicable to certain subclasses of these codes.

ACKNOWLEDGEMENT

The authors wish to acknowledge the contributions to this work by graduate students Ralph Longobardi and James Ducey of Systems and Information Science, Syracuse University.

TABLE OF CONTENTS

SECTION 1

INTRODUCTION

The use of finite geometries in the construction of cyclic error-correcting codes first appeared in the unpublished work of Prange[1,2], who used the projective planes of orders 4 and 8 to construct and analyze the (21,11) and (73,45) codes respectively. The general classes of projective-geometry and Euclidean-geometry codes were introduced by Rudolph[3,4]. Independently, Weldon[5] introduced difference-set codes, a subclass of the projective-geometry codes. The theory of finite-geometry codes and some generalizations of finite-geometry codes have been further developed by a number of researchers[6-19]. Our purpose in this paper is to present a new generalization of finite Euclidean-geometry and projective-geometry codes.

In Section 2, we introduce the concept of a generalized Euclidean geometry and define a new class of associated codes. Majority-logic decoding for two subclasses of generalized Euclidean-geometry codes is considered. In Section 3, generalized projective geometries are introduced and the associated codes are similarly analyzed. The results are discussed in Section 4.

SECTION 2

GENERALIZED EUCLIDEAN-GEOMETRY CODES

2.1 Generalized Euclidean geometries

In order to construct a generalized Euclidean geometry, it is first necessary to generalize the concept of "flat". The points of the generalized Euclidean geometry GEG(m,p) over GF(p) will be taken to be the elements of GF(p^m). Thus the points of GEG(m,p) coincide with the points of EG(m,p). The generalized flats of GEG(m,p), which we call "plates", do not in general coincide with the flats of EG(m,p), however. In order to define a plate, it is first necessary to introduce a generalized definition of linear independence.

Let $S_1,\ldots,S_k$ be sets of elements from GF(p^m) and let α be a primitive element of GF(p^m). We will say that the points $\alpha^{e_1},\ldots,\alpha^{e_k}$ of GEG(m,p) are linearly independent over the sets $S_1,\ldots,S_k$ if and only if there is no set of k elements $a_1,\ldots,a_k$, not all zero with $a_i \in S_i$ for $i = 1,\ldots,k$, such that

$$a_1\alpha^{e_1} + \ldots + a_k\alpha^{e_k} = 0.$$

Let the positive integer n_j be a proper divisor of $p^m - 1$. Corresponding to each n_j is a proper multiplicative subgroup of the multiplicative group of $GF(p^m)$. Denote by S_j the set of elements of $GF(p^m)$

$$S_j = \{ 0, 1, \alpha^{\frac{p^m-1}{n_j}}, \alpha^{2\frac{p^m-1}{n_j}}, \ldots, \alpha^{(n_j-1)\frac{p^m-1}{n_j}} \}.$$

Define N_k to be the k-tuple $N_k = (n_1,\ldots,n_k)$, where the positive integers n_j are a set of k proper divisors of $p^m - 1$ with $n_i \leq n_j$ for $i > j$ and $n_j \equiv -1 \pmod p$ for $j = 1,\ldots,k$. We now define a (k,N_k)-plate in GEG(m,p) to be the set of points

$$\alpha^j = \alpha^{e_0} + \beta_1\alpha^{e_1} + \ldots + \beta_k\alpha^{e_k}, \ \beta_j \in S_j,$$

where $\alpha^{e_1},\ldots,\alpha^{e_k}$ are fixed points in GEG(m,p) that are linearly independent over $S_1,\ldots,S_k$ and β_j ranges over all possible values in S_j, $1 \leq j \leq k$. A $(0,N_0)$-plate is a point of GEG(m,p). As in the case of flats of ordinary Euclidean geometries[20], we may represent a plate by a polynomial over GF(p). The term "plate" will be used to denote both the point set and the associated polynomial.

In the special case when $n_j = p^s - 1$ for $j = 1,\ldots,k$, where s is a divisor of m, a (k,N_k)-plate is a k-flat in $EG(\frac{m}{s}, p^s)$. We remark here that if $n_j = p^{s_j} - 1$, where s_j

is a divisor of m for $j = 1,\ldots,k$, the (k,N_k)-plate is what Lin and Weldon[15] have called a "frame" in EG(m,p).

2.2 GEG codes

The $(r,N_{r+1})^{th}$-order generalized Euclidean-geometry (GEG) code of length $n = p^m - 1$ with symbols from GF(p) is defined to be the largest cyclic code whose dual code contains all the $(r+1,N_{r+1})$-plates in GEG(m,p) that do not pass through the origin.

In order to determine the dimension of a GEG code, it is necessary to specify the roots of its parity check polynomial h(x). In order to do this, we require two technical lemmas and a generalization of the concept of s-weight[20] which we call a "p-cover".

Lemma 1: Let $\beta \in GF(p^m)$ be a primitive N^{th} root of unity with $N \equiv -1 \pmod p$. Then

$$\sum_{i=0}^{N-1,\infty} \beta^{ih} = \begin{cases} N & \text{if } 0 \neq h = kN \\ 0 & \text{otherwise} \end{cases}$$

where β^{∞} denotes the zero element of $GF(p^m)$.

(Proof) First suppose $h \neq 0$. Then

$$\sum_{i=0}^{N-1,\infty} \beta^{ih} = \sum_{i=0}^{N-1} \beta^{ih} = \frac{\beta^{Nh} - 1}{\beta^{h} - 1}\,.$$

Since $\beta^{Nh} - 1 = 0$ for any h, $\sum_{i=0}^{N-1,\infty} \beta^{ih} = 0$ unless $\beta^h = 1$, in which case $h = kN$. But then

$$\sum_{i=0}^{N-1,\infty} \beta^{ih} = \sum_{i=0}^{N-1} \beta^{kNi} = N.$$

Now suppose $h = 0$. Then $\sum_{i=0}^{N-1,\infty} \beta^{ih} = N + 1$ since $(\beta^\infty)^0 = (0)^0 = 1$. But $N + 1 \equiv 0 \pmod p$, so that $\sum_{i=0}^{N-1,\infty} \beta^{ih} = 0$.

Q.E.D.

Lemma 2: Let $M = M_0 + M_1 p + M_2 p^2 + \ldots$ and $K = K_0 + K_1 p + K_2 p^2 + \ldots$, where $0 \leq M_i < p$ and $0 \leq K_i < p$. Then

$$\binom{M}{K} \not\equiv 0 \pmod p$$

if and only if $M_i \geq K_i$ for all i.

(Proof) See Peterson and Weldon, Chapter 10[20].

We now introduce the concept of a p-cover. A nonnegative integer t is said to be a p-cover of $N_k = (n_1, \ldots, n_k)$ if and only if there exists a set of integers $b_0, b_1, \ldots, b_k$ satisfying the following conditions:

(i) $t = b_0 + b_1 n_1 + \ldots + b_k n_k$ where $b_0 \geq 0$ and $b_i > 0$ for $i = 1, \ldots, k$.

(ii) $t_i \geq \sum_{j=1}^{k} k_{ij}$ for $i = 0, 1, \ldots, I$, where t_i and k_{ij} are the i^{th} p-ary digits in the radix-p expansions of t and $b_j n_j$ respectively, i.e.

$$t = t_0 + t_1 p + \ldots + t_I p^I, \; 0 \leq t_i < p$$

$$b_j n_j = k_{0j} + k_{1j} p + \ldots + k_{Ij} p^I, \; 0 \leq k_{ij} < p.$$

For example, let $p = 2$, $m = 6$ and $N_2 = (7,3)$. Then $t = 31 = 011111 = 011000 + 000111$ is a 2-cover of N_2 but $t = 27 = 011011$ is not. In the special case when $n_i = p^s - 1$ for $i = 1,\ldots,k$, t is a p-cover of N_k if and only if $W_s(t) \geq k$, where $W_s(t)$ denotes the s-weight of t.

Theorem 1: Let α be a primitive element of $GF(p^m)$. Then α^t, $0 \leq t < p^m-1$ is a root of $h(x)$, the parity check polynomial of the $(r,N_{r+1})^{th}$-order GEG code, provided that t is not a p-cover of $N_{r+1} = (n_1,\ldots,n_{r+1})$.

(Proof) Let $f(x)$ be the polynomial associated with an $(r+1,N_{r+1})$-plate in GEG(m,p). Then

$$f(\alpha^t) = \sum_{\beta_j \varepsilon S_j} (\alpha^{e_o} + \beta_1 \alpha^{e_1} + \ldots + \beta_{r+1}\alpha^{e_{r+1}})^t$$

$$= \sum_{\beta_j \varepsilon S_j} \sum_{\underline{h}} \frac{t}{h_0! n_1! \ldots h_{r+1}!} (\alpha^{e_0})^{h_0} (\beta_1 \alpha^{e_1})^{h_1} \ldots (\beta_{r+1}\alpha^{e_{r+1}})^{h_{r+1}}$$

where $\underline{h} = (h_o, h_1, \ldots, h_{r+1})$ and the sum is taken over all $\underline{h}$ such that

$$h_0 + h_1 + \ldots + h_{r+1} = t$$

where $h_i \geq 0$ for $i = 0,1,\ldots,r+1$. Reversing the order of summation and applying Lemma 1, we see that $f(\alpha^t) = 0$ unless $0 \neq h_j = b_j n_j$ for $j = 1,\ldots,r+1$. Hence

$$f(\alpha^t) = \prod_{j=1}^{r+1} n_j \sum_{\underline{h}} \frac{t!}{h_0!(b_1n_1)!\ldots(b_{r+1}n_{r+1})!} \alpha^{h_0 e_0} \alpha^{b_1 n_1 e_1} \ldots \alpha^{b_{r+1}n_{r+1}e_{r+1}}$$

where $\underline{h} = (h_0, b_1n_1, \ldots, b_{r+1}n_{r+1})$ and $h_0 + b_1n_1 + \ldots + b_{r+1}n_{r+1} = t$. The multinomial coefficient in the above expression can be written as

$$\binom{t}{b_1n_1}\binom{t-b_1n_1}{b_2n_2} \cdots \binom{t - \sum_{i=1}^{r} b_in_i}{b_{r+1}n_{r+1}}.$$

Let

$$t = t_0 + t_1p + \ldots + t_{m-1}p^{m-1},\ 0 \leq t_i < p$$

and $b_jn_j = k_{0j} + k_{1j}p + \ldots + t_{(m-1)j}p^{m-1},\ 0 \leq k_{ij} < p$

be the radix-p expansions of t and b_jn_j. Assume that t is not a p-cover of $N_{r+1} = (n_1,\ldots,n_{r+1})$. Then there exists at least one i, $0 \leq i < m$, such that $t_i < \sum_{j=1}^{r+1} k_{ij}$.

Let ϕ, $1 \leq \phi \leq r$, be such that $t_i \geq \sum_{j=1}^{\phi} k_{ij}$ for $i = 1,\ldots,m-1$ and $t_\theta < \sum_{j=1}^{\phi+1} k_{\theta j}$ for some θ, $0 \leq \theta < m$. Since $t_i \geq \sum_{j=1}^{\phi} k_{ij}$ for $i = 0,1,\ldots,m-1$, the i^{th} coefficient of the radix-p form of $t - \sum_{j=1}^{\phi} b_jn_j$ is equal to $t_i - \sum_{j=1}^{\phi} k_{ij}$. Then the $(\phi+1)^{th}$ factor of the multinomial coefficient is

$$\binom{t - \sum_{j=1}^{\phi} k_j n_j}{k_{\phi+1} n_{\phi+1}}.$$

Noting that $t - \sum_{j=1}^{\phi} k_{\theta j} < k_{\theta(\phi+1)}$ and applying Lemma 2, we see that

$$\binom{t - \sum_{j=1}^{\phi} k_j n_j}{k_{\phi+1} n_{\phi+1}} \equiv 0 \pmod p$$

in which case α^t is a root of $f(x)$. Q.E.D.

In the general case it is not necessarily true that the intersection of two plates is a plate. This means that in general we cannot determine d_{ML}, the minimum distance guaranteed by L-step orthogonalization. However, in some special cases d_{ML} can be determined as will be seen in the next section.

2.3 Examples of GEG codes

In this section we consider two classes of GEG codes to which L-step orthogonalization applies. The first class, which we call regular GEG codes, contains the classical EG codes and the two-fold EG codes of Lin and Weldon(15) as proper subclasses. The second class we consider is the class of $(0,N)^{th}$-order GEG codes. This class contains the $(0,s)^{th}$-order EG codes as a proper subclass.

2.3 Regular GEG codes

In the special case when $n_j = p^{s_j} - 1$ for $j = 1,\ldots,r+1$ and n_{j+1} divides n_j for $j = 1,\ldots,r$, an $(r+1,N_{r+1})$-plate in GEG(m,p) is called a regular plate. We define a regular $(r,N_{r+1})^{th}$-order GEG code of length $n = p^m - 1$ to be the largest cyclic code whose dual code contains all the regular $(r+1,N_{r+1})$-plates in GEG(m,p) that do not pass through the origin. We note that since s_{r+1} divides s_j, $GF(p^{s_j})$ is a vector space of dimension $\theta_j = s_j/s_{r+1}$ over $GF(p^{s_{r+1}})$ for $j = 1,\ldots,r$. Thus a regular $(r+1,N_{r+1})$-plate in GEG(m,p) is a $(\theta_1+\theta_2+\ldots+\theta_r+1)$-flat in $EG(m/s_{r+1},p^{s_{r+1}})$, which means that the regular $(r,N_{r+1})^{th}$-order GEG code is a supercode of the $(\sum_{i=1}^{r} \theta_i, s_{r+1})^{th}$-order EG code.

We now derive an expression for d_{ML}, the minimum distance guaranteed by L-step orthogonalization, for regular GEG codes. We have pointed out that a regular $(r+1,N_{r+1})$-plate is a $(\theta_1+\ldots+\theta_r+1)$-flat in $EG(m/s_{r+1},p^{s_{r+1}})$. Further, a regular (r,N_r)-plate is a $(\theta_1+\ldots+\theta_r)$-flat in $EG(m/s_{r+1},p^{s_{r+1}})$. Hence the number of regular $(r+1,N_{r+1})$-plates orthogonal on a given regular (r,N_r)-plate is equal to the number of $(\theta_1+\ldots+\theta_r+1)$-flats orthogonal on a $(\theta_1+\ldots+\theta_r)$-flat. This number is[20]

$$J_{r+1} = \frac{p^{m-(s_1+\ldots+s_r)} - 1}{p^{s_{r+1}} - 1} - 1.$$

Now since s_r divides s_j, $GF(p^{s_j})$ is a vector space of dimension $\phi_j = s_j/s_r$ over $GF(p^{s_r})$ for $j = 1,\ldots,r-1$. Thus a regular (r,N_r)-plate is a $(\phi_1+\ldots+\phi_{r-1}+1)$-flat in $EG(m/s_r, p^{s_r})$. It follows that there are

$$J_r = \frac{p^{m-(s_1+\ldots+s_{r-1})} - 1}{p^{s_r} - 1} - 1$$

regular (r,N_r)-plates orthogonal on a regular $(r-1,N_{r-1})$-plate. In general, there are

$$J_k = \frac{p^{m-(s_1+\ldots+s_{k-1})} - 1}{p^{s_k} - 1} - 1$$

regular (k,N_k)-plates orthogonal on a regular $(k-1,N_{k-1})$-plate for $k = 1,\ldots,r+1$.

To show that $d_{ML} = J_{r+1} + 1$, it is sufficient to verify that $J_k \geq J_{k+1}$ for $k = 1,\ldots,r$. Assume, to the contrary, that $J_k < J_{k+1}$ for some $1 \leq k \leq r$. Then

$$\frac{p^{m-(s_1+\ldots+s_{k-1})} - 1}{p^{s_k} - 1} < \frac{p^{m-(s_1+\ldots+s_k)} - 1}{p^{s_{k+1}} - 1}$$

or

$$(p^{s_{k+1}}-2)\, p^{m-(s_1+\ldots+s_{k-1})} + p^{m-(s_1+\ldots+s_k)} + p^{s_{k+1}}(p^{s_k-s_{k+1}}-1) < 0.$$

But $p \geq 2$, $s_{k+1} \geq 1$ and $s_k \geq s_{k+1}$. Hence the left-hand side cannot be negative, which is a contradiction. We have thus proved

<u>Theorem 2</u>: The regular $(r,N_{r+1})^{th}$-order GEG code of length $n = p^m - 1$ can be (r+1)-step majority decoded provided $t_{ML} = [(d_{ML} - 1)/2]$ or fewer errors occurred, where

$$d_{ML} = \frac{p^{m-(s_1+\ldots+s_r)} - 1}{p^{s_{r+1}} - 1}$$

and [x] denotes the integer part of x.

The regular $(r,N_{r+1})^{th}$-order GEG codes for which $n_j = 2^s - 1$ for $j = 1,\ldots,r+1$ are the classical $(r,s)^{th}$-order EG codes. When $n_{r+1} = 1$, $n_j = 2^s - 1$ for $j = 1,\ldots,r$ and $p = 2$, the regular $(r,N_{r+1})^{th}$-order GEG code is a two-fold EG code. We now give some examples of regular GEG codes.

<u>Example 1</u>: The regular $(1,N_2)^{th}$-order GEG code of length $n = 2^6 - 1$ with $N_2 = (3,1)$ is a binary (63,24) code with $t_{ML} = 7$. This code, which was also found by Lin and Weldon[15], is a BCH code and is orthogonalizable in two steps.

<u>Example 2</u>: The regular $(2,N_3)^{th}$-order GEG code of length $n = 2^{12} - 1$ with $N_3 = (15,1,1)$ is a binary (4095,2000) code with $t_{ML} = 63$. The corresponding $(5,1)^{th}$-order EG code (5^{th} order RM code) with $t_{ML} = 63$ is a binary (4095,1586) code. The GEG code is orthogonalizable in three steps, the EG code in two[21]. (The complexity of a conventional

3-step majority decoder is much greater than that of a conventional 2-step majority deocder for the same n and t_{ML}. However, if sequential code reduction[22] is used instead of conventional majority decoding, decoder complexity in both cases is greatly reduced and the difference in complexity between 2-step and 3-step decoding is small).

Example 3: The regular $(1,N_2)^{th}$-order GEG code of length $n = 2^{16} - 1$ with $N_2 = (15,3)$ is a binary (65535,15715) code with $t_{ML} = 682$. The corresponding $(2,2)^{th}$-order EG code with $t_{ML} = 682$ is a binary (65535,12273) code. Both codes can be orthogonalized in two steps.

A table of all binary regular GEG codes of length $n = 2^{14} - 1$ or less is given in the Appendix.

2.3.2 $(0,N_1)^{th}$-order GEG codes

The dual of the $(0,N_1)^{th}$-order GEG code contains all the $(1,N_1)$-plates in GEG(m,p) that do not pass through the origin, where $N_1 = (n_1)$. Consider two $(1,N_1)$-plates f and $\bar{f}$ consisting of the points

$$f: \quad \alpha^j = \alpha^{e_o} + \beta_1\alpha^{e_1}, \quad \beta_1 \in S_1$$

$$\bar{f}: \quad \alpha^j = \alpha^{e_0} + \beta_1\alpha^{\bar{e}_1}, \quad \beta_1 \in S_1.$$

If $\alpha^{e_0} + \alpha^{\bar{e}_1}$ does not belong to f, then f and $\bar{f}$ clearly intersect in α^{e_0}. We note that for each $\alpha^{e_1} \neq \beta_1\alpha^{e_0}$, $\beta_1 \varepsilon S_1$, we have a $(1,N_1)$-plate in GEG(p,m) that passes through α^{e_0} and does not pass through the origin. There are n_1 points in a $(1,N_1)$-plate passing through α^{e_0} that do not belong to any other $(1,N_1)$-plate that also passes through α^{e_0}. Since the total number of points in GEG(p,m), excluding α^{e_0}, contained in all $(1,N_1)$-plates passing through α^{e_0} but not the origin is $p^m - (n_1 + 1)$, the number of $(1,N_1)$-plates orthogonal on α^{e_o} is

$$J = \frac{p^m - (n_1 + 1)}{n_1} = \frac{p^m - 1}{n_1} - 1.$$

Thus we have proved

Theorem 3: The $(0,N_1)^{th}$-order GEG code of length $n = p^m - 1$ is one-step majority decodable provided that $t_{ML} = [(d_{ML} - 1)/2]$ or fewer errors occurred, where

$$d_{ML} = \frac{p^m - 1}{n_1}.$$

The $(0,N_1)^{th}$-order GEG codes for which $n_1 = p^s - 1$ are the classical $(0,s)^{th}$-order EG codes. We now give an example of a $(0,N_1)^{th}$-order GEG code.

Example 4: The $(0,N_1)^{th}$-order GEG code of length $n = 2^{11} - 1$ with $N_1 = (23)$ is a binary (2047,573) code with $t_{ML} = 44$.

SECTION 3

GNEERALIZED PROJECTIVE-GEOMETRY CODES

3.1 Generalized projective geometries

Let α be a primitive element of $GF(p^m)$ and n_0 a proper divisor of $p^m - 1$ such that $n_0 \equiv -1 (\mathrm{mod}\ p)$. The sets of $n_0{}^{th}$ roots of unity form a proper subgroup, G, of the multiplicative group of $GF(p^m)$. The points of the generalized projective geometry $GPG(m,n_0,p)$ over $GF(p)$ will be taken to be the cosets with respect to G in the multiplicative group of $GF(p^m)$. The coset $\{\alpha^{j_1},\ldots,\alpha^{j_{n_0}}\}$ will be denoted bv (α^j) where $j = \min(j_1,\ldots,j_{n_0})$. Note that under this index convention the cosets are $(\alpha^0),(\alpha^1),\ldots,(\alpha^{n-1})$, where $n = (p^m - 1)/n_0$.

Let $N_k = (n_1,\ldots,n_k)$ where the positive integers n_j are a set of k proper divisors of $p^m - 1$, with $n_i \leq n_j$ for $i > j$, $n_j = \theta_j n_0$, and $n_j \equiv -1 (\mathrm{mod}\ p)$ for $j = 1,\ldots,k$. Denote by S_j the set of elements

$$S_j = \{0,1,\alpha^{\frac{p^m-1}{n_j}},\alpha^{2\frac{p^m-1}{n_j}},\ldots,\alpha^{(n_j-1)\frac{p^m-1}{n_j}}\}$$

for $j = 0,1,\ldots,k$. We define a (k,N_k)-plate in $GPG(m,n_0,p)$ to be the set of points

$(\alpha^j) = (\beta_0\alpha^{e_0} + \ldots + \beta_k\alpha^{e_k})$, $\beta_i \in \mathbf{S}_i$ and β_i not all 0, where $\alpha^{e_0}, \ldots, \alpha^{e_k}$ are a fixed set of k+1 points of GEG(m,p) that are linearly independent over the sets $S_0, \ldots, S_k$, and β_j ranges over all possible values in S_j except that not all β_i are simultaneously zero. We adopt the convention that a $(0,N_0)$-plate in GPG(m,n_0,p) denotes a point in GPG(m,n_0,p). As in the case of flats in an ordinary finite projective geometry[20], we may represent a plate in GPG(m,n_0,p) by a polynomial of degree less than n.

In the special case where $n_j = p^s - 1$ for $j = 0,1,\ldots k$, a (k,N_k)-plate in GPG(m,n_0,p) is a k-flat in PG$((m-s)/s,p^s)$.

3.2 GPG codes

The $(r,N_r)^{th}$-order generalized projective-geometry (GPG) code of length $n = (p^m - 1)/n_0$ with symbols from GF(p) is defined to be the largest cyclic code whose dual code contains all the (r,N_r)-plates in GPG(m,n_0,p).

The roots of the parity check polynomial h(x) of a GPG code are specified by the following

Theorem 4: Let α be a primitive element of GF(p^m). Then α^{tn_0}, $1 \leq t < n$, is a root of h(x), the parity check polynomial of the $(r,N_r)^{th}$-order GPG code, provided that tn_0 is not a p-cover of $N_{r+1} = (n_1,\ldots,n_r,n_{r+1})$, where $N_r = (n_1,n_2,\ldots,n_r)$ and $n_{r+1} = n_0$.

(Proof) Let $f(x)$ be the polynomial associated with the (r,N_r)-plate

$$f: \quad (\alpha^j) = (\beta_0\alpha^{e_0} + \ldots + \beta_r\alpha^{e_r}), \ \beta_i \in S_i \text{ and } \beta_i \text{ not all } 0,$$

in $GPG(m,n_0,p)$ and let $\bar{f}(x)$ be the polynomial associated with the corresponding $(r+1,N_{r+1})$-plate

$$\bar{f}: \quad \alpha^j = \beta_0\alpha^{e_0} + \ldots + \beta_r\alpha^{e_r}, \ \beta_i \in S_i,$$

in $GEG(m,p)$. Now note that if $(\alpha^j) \in f$, then $\{\alpha^j, \alpha^{j+n}, \ldots, \alpha^{j+(n_0-1)n}\} \in \bar{f}$ since n_0 divides n_j for $j = 1,\ldots,r$. Thus

$$\bar{f}(x) = (f(x))(1 + x^n + \ldots + x^{(n_0-1)n}) + x^\infty$$

where x^∞ is the polynomial associated with the origin in $GEG(m,p)$. Now suppose that tn_0, $1 \leq t < n$, is not a p-cover of $N_{r+1} = (n_1,\ldots,n_r,n_{r+1})$ where $n_{r+1} = n_0$. Then by an argument analogous to that used in the proof of Theorem 1, $\bar{f}(\alpha^{tn_0}) = 0$. But then $f(\alpha^{tn_0}) = 0$ since $1 + \alpha^{tn_0 n} + \ldots + \alpha^{tn_0(n_0-1)n} = n_0 \equiv -1 \pmod{p}$ and $(\alpha^{tn_0})^\infty = 0$ for $1 \leq t < n$.

Q.E.D.

As was the case for generalized Euclidean geometries, the intersection of two plates in a generalized projective geometry is not necessarily a plate, so that we cannot in general calculate d_{ML} for GPG codes. There is a special case, however, for which d_{ML} can be determined.

3.3 Examples of GPG codes

In the section we will consider two classes of GPG codes. L-step orthogonalization is applicable to all codes in the first class, which we call the class of regular GPG codes, but not to all codes in the second class, which we call the class of uniform GPG codes. The classical PG codes are a proper subclass of both regular and uniform GPG codes.

3.3.1 Regular GPG codes

In the special case where $n_j = p^{s_j} - 1$ for $j = 0,1,...r$ and n_{j+1} divides n_j for $j = 1,...,r-1$, an (r,N_r)-plate in $GPG(m,n_0,p)$ is called a regular plate. We define a regular $(r,N_r)^{th}$-order GPG code of length $n = (p^m - 1)/n_0$ to be the largest cyclic code whose dual code contains all the regular (r,N_r)-plates in $GPG(m,n_0,p)$. We note that since s_0 divides s_j, $GF(p^{s_j})$ is a vector space of dimension $\theta_j = s_j/s_0$ for $j = 1,...,r$. Thus a regular (r,N_r)-plate in $GPG(m,n_0,p)$ is a $(\theta_1 +...+ \theta_r)$-flat in $PG((m-s_0)/s_0,p^{s_0})$, which means that a regular $(r,N_r)^{th}$-order GPG code is a supercode of the $(\sum_{i=1}^{r} \theta_i,s_0)^{th}$-order PG code.

We now derive an expression for d_{ML} for the regular GPG codes. Let

$$N^*_{r+1} = (n_1,\ldots,n_r,n_0)$$

$$N^*_r = (n_1,\ldots,n_{r-1},n_0)$$

$$\vdots$$

$$N^*_{r-j} = (n_1,\ldots,n_{r-j-1},n_0)$$

$$\vdots$$

$$N^*_1 = (n_0).$$

If $\bar{f}_1,\ldots,\bar{f}_u$ are regular $(r-j+1,N^*_{r-j+1})$-plates orthogonal on a regular $(r-j,N^*_{r-j})$-plate $\bar{f}$ in GEG(m,p), then the corresponding $(r-j,N_{r-j})$-plates $f_1,\ldots,f_u$ are orthogonal on the corresponding $(r-j-1,N_{r-j-1})$-plate f in GPG(m,n_0,p). So the number of $(r-j,N_{r-j})$-plates orthogonal on a $(r-j-1,N_{r-j-1})$-plate in GPG(m,n_0,p) can be determined by finding the number, J^*_{r-j+1}, of corresponding $(r-j+1, N^*_{r-j+1})$-plates orthogonal on the corresponding $(r-j,N^*_{r-j})$-plate in GEG(m,p). Since s_0 divides s_j for $j = 1,\ldots,r$, the $(r-j+1, N^*_{r-j+1})$-plates are subsets of the regular $(r-j+1,\bar{N}_{r-j+1})$-plates in GEG(m,p) where $\bar{N}_{r-j+1} = (n_1,\ldots,n_{r-j},n_{r-j})$, and the $(r-j,N^*_{r-j})$-plate is a subset of the regular $(r-j,N_{r-j})$-plate. Noting that the $(r-j+1,\bar{N}_{r-j+1})$-plates and the $(r-j,N_{r-j})$-plate pass through the origin in GEG(m,p), we see that the number, $\bar{J}_{r-j+1}$, of $(r-j+1,\bar{N}_{r-j+1})$-plates orthogonal on a $(r-j,N_{r-j})$-plate is, from Section 3.2,

$$\bar{J}_{r-j+1} = J_{r-j+1} + 1 = \frac{p^{m-(s_1+\ldots+s_{r-j})} - 1}{p^{s_{r-j}} - 1} .$$

$\bar{J}_{r-j+1}$ is thus a lower bound on J^*_{r-j+1} for $j = 0,1,\ldots,r-1$.

It is not true in general that $\bar{J}_{r-j+1} \leq \bar{J}_{r-j}$, so d_{ML} is determined not by $\bar{J}_{r+1}$, as in the case of regular GEG codes, but rather by the minimum of the $\bar{J}_{r-j+1}$. Thus we have proved

<u>Theorem 5</u>: The regular $(r,N_r)^{th}$-order GPG code of length $n = (p^m - 1)/n_0$ can be r-step majority decoded provided that $t_{ML} = [(d_{ML} - 1)/2]$ or fewer errors occurred, where $d_{ML} = \min_{0\leq j<r} \{\bar{J}_{r-j+1} + 1\}$.

The regular $(r,N_r)^{th}$-order codes for which $n_j = 2^s - 1$ for $j = 0,1,\ldots,r$ are the classical $(r,s)^{th}$-order PG codes. In this case $d_{ML} = \bar{J}_{r+1} + 1$. We now give two examples of regular GPG codes.

<u>Example 5</u>: The regular $(2,N_2)^{th}$-order GPG code of length $n = (2^{16} - 1)/3$ with $n_0 = 3$ and $N_2 = (15,3)$ is a binary (21845,8908) code with $t_{ML} = 136$. The corresponding PG code is the $(3,2)^{th}$-order (21845,8536) code with $t_{ML} = 170$. Both codes can be majority decoded in two steps[21].

<u>Example 6</u>: The regular $(3,N_3)^{th}$-order GPG code of length $n = (2^{20} - 1)/3$ with $n_0 = 3$ and $N_3 = (15,3,3)$ is a binary

(349525,145859) code with $t_{ML} = 682$. The corresponding PG code with $t_{ML} = 682$ is the $(4,2)^{th}$-order (349525,145055) code. The GPG code can be majority decoded in three steps, the PG code in two.

A table of all binary regular $(r,N_r)^{th}$-order GPG codes of length $n = 21845$ or less for which $d_{ML} = \bar{J}_{r+1} + 1$ and $n_0 = n_r \neq 1$ is given in the Appendix.

3.3.2 Uniform GPG codes

In the special case where $n_j = n_0$ for $j = 1,\ldots,r$, an (r,N_r)-plate in GPG(m,n_0,p) is called a uniform plate. We define a uniform $(r,N_r)^{th}$-order GPG code to be the largest cyclic code of length $n = (p^m - 1)/n_0$ whose dual code contains all the uniform (r,N_r)-plates in GPG(m,n_0,p). If $n_0 = p^s - 1$, the uniform $(r,N_r)^{th}$-order GPG code is the $(r,s)^{th}$-order PG code.

If n_0 is not of the form $p^s - 1$, two uniform plates do not necessarily intersect in a uniform plate. Thus we cannot in general give a closed form expression for the number of errors that can be corrected by L-step orthogonalization. In fact, it appears that this subclass of uniform GPG codes is better suited for majority decoding using nonorthogonal parity checks, as illustrated by the following example.

Example 7: The uniform $(1,N_1)^{th}$-order GPG code of length $n = (2^8 - 1)/5$ with $n_0 = n_1 = 5$ is a binary (51,16) code with minimum distance $d = 16$[23]. Using 49 nonorthogonal $(1,N_1)$-plates in GPG(8,5,2), it is possible to correct up to six errors[24] by one-step weighted-majority decoding[25]. The BCH bound for this code[26] is $d_{BCH} = 12$, so that five or fewer errors could be corrected using Berlekamp's iterative algorithm[23]. This code could be decoded up to seven errors either by one-step weighted-majority decoding with a sufficiently large number of nonorthogonal parity checks, or by an extended BCH decoding algorithm[27]. However, we conjecture that the increase in decoding complexity in either case would be substantial.

SECTION 4

DISCUSSION

We have presented a new technique for constructing cyclic codes that retain many of the combinatorial properties of finite-geometry codes, but which are in many cases superior to these codes. We have been able to show that L-step orthogonalization is applicable to some of these new codes. For others, weighted-majority decoding using nonorthogonal parity checks is more appropriate. Because of their rich subcode structure, generalized finite-geometry codes are particularly well suited for decoding by sequential code reduction. This makes generalized finite-geometrv codes attractive for use in practical error-control systems where very long codes are required.

REFERENCES

1. Prange, E., "Some Cyclic Error Correcting Codes with Simple Decoding Algorithms," AFCRC-TN-58-156, Air Force Cambridge Research Center, Cambridge, Mass. (1958).

2. Prange, E., "The Use of Coset Equivalence in the Analysis and Design of Group Codes," AFCRC-TR-59-164, Air Force Cambridge Research Center, Cambridge, Mass. (1959).

3. Rudolph, L. D., "Geometric Configurations and Majority Logic Decodable Codes," MEE Thesis, University of Oklahoma, Norman, Oklahoma (1964).

4. Rudolph, L. D., "A Class of Majority Logic Decodable Codes," IEEE Trans. on Info. Theory, IT-13, pp. 305-307 (1967).

5. Weldon, E. J., Jr., "Difference-Set Cyclic Codes," Bell System Tech. J., 45, pp. 1045-1055 (1966).

6. Chow, D. K., "A Geometric Approach to Coding Theory with Application to Information Retrieval," Coordinated Sci. Lab. Rept. R-368, University of Illinois, Urbana (1967).

7. Delsarte, P., J. M. Goethals, and F. J. MacWilliams, "On GRM and Related Codes," Information and Control, 16, pp. 403-442 (1970).

8. Goethals, J. M. and P. Delsarte, "On a Class of Majority-Logic Decodable Codes," IEEE Trans. on Info. Theory, IT-14, pp. 182-188 (1968).

9. Graham, F. L. and F. J. MacWilliams, "On the Number of Parity Checks in Difference Set Cyclic Codes," Bell System Tech. J., 45, pp. 1057-1070 (1966).

10. Hamada, N., "The Rank of the Incidence Matrix of Points of d-flats in Finite Geometries," J. Sci. Hiroshima University, 32, pp. 381-396 (1968).

11. Kasami, T., S. Lin and W. W. Peterson, "New Generalizations of the Reed-Muller Codes - Part I: Primitive Codes," IEEE Trans. on Info. Theory, IT-14, pp. 189-198 (1968).

12. Kasami, T., S. Lin and W. W. Peterson, "Polynomial Codes," IEEE Trans. on Info. Theory, IT-14, pp. 807-814 (1968).

13. Lin, S., "On a Class of Cyclic Codes," Chapter 7, Error-Correcting Codes, H. Mann, Ed., Wiley, New York (1968).

14. Lin, S., "On the Number of Information Symbols of Polynomial Codes," IEEE Trans. on Info. Theory, to appear.

15. Lin, S. and E. J. Weldon, Jr., "New Efficient Majority-Logic-Decodable Cyclic Codes," presented at the IEEE International Symposium on Info. Theory, Asilomar, California (1972).

16. MacWilliams, F. J. and H. B. Mann, "On the p-rank of the Design Matrix of a Difference Set," Information and Control, 12, pp. 474-488 (1968).

17. Smith, K. J. C., "On the p-rank of the Incidence Matrix of Points and Hyperplanes in a Finite Projective Geometry," J. Combinatorial Theory, 7, pp. 122-129 (1969).

18. Weldon, E. J., Jr., "Euclidean Geometry Cyclic Codes," Procedings of the Symposium of Combinatorial Mathematics at the University of North Carolina, Chapel Hill, N.C. (1967).

19. Weldon, E. J., Jr., "New Generalizations of the Reed-Muller Codes - Part II: Non-primitive Codes," IEEE Trans. on Info. Theory, IT-14, pp. 199-205 (1968).

20. Peterson, W. W. and E. J. Weldon, Jr., Error-Correcting Codes, 2nd Edition, M.I.T. Press, Cambridge, Mass. (1972).

21. Chen, C. L., "Note on Majority-Logic Decoding of Finite Geometry Codes," IEEE Trans. on Info. Theory, to appear.

22. Rudolph, L. D. and C. R. P. Hartmann, "Decoding by Sequential Code Reduction," presented at the IEEE International Symposium on Information Theory, Asilomar, California (1972).

23. Berlekamp, E. R., Algebraic Coding Theory, McGraw-Hill, New York (1968).

24. Ducey, J., private communication (April, 1972).

25. Rudolph, L. D. and W. E. Robbins, "One-Step Weighted-Majority Decoding," IEEE Trans. on Info. Theory, IT-18, pp. 446-448 (1972).

26. Chen, C. L., "Computer Results on the Minimum Distance of Some Binary Cyclic Codes," IEEE Trans. on Info. Theory, IT-16, pp. 359-360 (1970).

27. Hartmann, C. R. P., "Decoding Beyond the BCH bound," IEEE Trans. on Info. Theory, IT-18, pp. 441-444 (1972).

APPENDIX

Table I gives all binary regular $(r,N_{r+1})^{th}$-order GEG codes of length $n = 2^m - 1$ for $m = 3,\ldots,14$. The remarks in Table I are encoded as follows:

A : EG Code

B : Cyclic RM Code

C : BCH Code

D : Two-fold EG Code

E : Same k and t_{ML} as the corresponding EG Code

F : Greater k and same t_{ML} as the corresponding EG Code

Table II gives all binary regular $(r,N_r)^{th}$-order GPG codes of length $n = (2^m - 1)/n_0$ for which $n_r = n_0$ and $d_{ML} = J_{r+1} + 1$ for $m = 6,\ldots,16$, and all possible values of $n_0 = 2^{s_0} - 1 \neq 1$. The remarks in Table II are encoded as follows:

$\bar{A}$: PG Code

$\bar{B}$: Same k and t_{ML} as the corresponding PG code

TABLE I

m	r	N_{r+1}	(n,k,t_{ML})	Remarks
3	0	(1)	(7,1,3)	A,B
3	1	(1,1)	(7,4,1)	A,B
4	0	(1)	(15,1,7)	A,B
4	0	(3)	(15,7,2)	A
4	1	(1,1)	(15,5,3)	A,B
4	1	(3,1)	(15,11,1)	D,E
4	2	(1,1,1)	(15,11,1)	A,B
5	0	(1)	(31,1,15)	A,B
5	1	(1,1)	(31,6,7)	A,B
5	2	(1,1,1)	(31,16,3)	A,B
5	3	(1,1,1,1)	(31,26,1)	A,B
6	0	(1)	(63,1,31)	A,B
6	0	(3)	(63,13,10)	A
6	0	(7)	(63,36,4)	A
6	1	(1,1)	(63,7,15)	A,B
6	1	(3,1)	(63,24,7)	C,D,F
6	1	(7,1)	(63,45,3)	C,D,F
6	1	(3,3)	(63,48,2)	A
6	2	(1,1,1)	(63,22,7)	A,B
6	2	(3,1,1)	(63,42,3)	E
6	2	(3,3,1)	(63,57,1)	E
6	2	(7,1,1)	(63,57,1)	E
6	3	(1,1,1,1)	(63,42,3)	A,B
6	3	(3,1,1,1)	(63,57,1)	E
6	4	(1,1,1,1,1)	(63,57,1)	A,B

m	r	N_{r+1}	(n,k,t_{ML})	Remarks
7	0	(1)	(127,1,63)	A,B
7	1	(1,1)	(127,8,31)	A,B
7	2	(1,1,1)	(127,29,15)	A,B
7	3	(1,1,1,1)	(127,64,7)	A,B
7	4	(1,1,1,1,1)	(127,99,3)	A,B
7	5	(1,1,1,1,1,1)	(127,120,1)	A,B
8	0	(1)	(255,1,127)	A,B
8	0	(3)	(255,21,42)	A
8	0	(15)	(255,175,8)	A
8	1	(1,1)	(255,9,63)	A,B
8	1	(3,1)	(255,45,31)	D,F
8	1	(15,1)	(255,191,7)	D,F
8	1	(3,3)	(255,127,10)	A
8	1	(15,3)	(255,231,2)	E
8	2	(1,1,1)	(255,37,31)	A,B
8	2	(3,1,1)	(255,95,15)	F
8	2	(15,1,1)	(255,223,3)	F
8	2	(3,3,1)	(255,171,7)	D,F
8	2	(15,3,1)	(255,247,1)	E
8	2	(3,3,3)	(255,231,2)	A
8	3	(1,1,1,1)	(255,93,15)	A,B
8	3	(3,1,1,1)	(255,163,7)	E
8	3	(15,1,1,1)	(255,247,1)	E
8	3	(3,3,1,1)	(255,219,3)	E
8	3	(3,3,3,1)	(255,247,1)	D,E
8	4	(1,1,1,1,1)	(255,163,7)	A,B
8	4	(3,1,1,1,1)	(255,219,3)	E
8	4	(3,3,1,1,1)	(255,247,1)	E

m	r	N_{r+1}	(n,k,t_{ML})	Remarks
8	5	(1,1,1,1,1,1)	(255,219,3)	A,B
8	5	(3,1,1,1,1,1)	(255,247,1)	E
8	6	(1,1,1,1,1,1,1)	(255,247,1)	A,B
9	0	(1)	(511,1,255)	A,B
9	0	(7)	(511,139,36)	A
9	1	(1,1)	(511,10,127)	A,B
9	1	(7,1)	(511,184,31)	D,F
9	1	(7,7)	(511,448,4)	A
9	2	(1,1,1)	(511,46,63)	A,B
9	2	(7,1,1)	(511,274,15)	F
9	2	(7,7,1)	(511,475,3)	D,F
9	3	(1,1,1,1)	(511,130,31)	A,B
9	3	(7,1,1,1)	(511,385,7)	F
9	3	(7,7,1,1)	(511,502,1)	E
9	4	(1,1,1,1,1)	(511,256,15)	A,B
9	4	(7,1,1,1,1)	(511,466,3)	E
9	5	(1,1,1,1,1,1)	(511,382,7)	A,B
9	5	(7,1,1,1,1,1)	(511,502,1)	E
9	6	(1,1,1,1,1,1,1)	(511,466,3)	A,B
9	7	(1,1,1,1,1,1,1,1)	(511,502,1)	A,B
10	0	(1)	(1023,1,511)	A,B
10	0	(3)	(1023,31,170)	A
10	0	(31)	(1023,781,16)	A
10	1	(1,1)	(1023,11,255)	A,B
10	1	(3,1)	(1023,76,127)	D,F
10	1	(31,1)	(1023,813,15)	D,F
10	1	(3,3)	(1023,288,42)	A
10	2	(1,1,1)	(1023,56,127)	A,B
10	2	(3,1,1)	(1023,186,63)	F

m	r	N_{r+1}	(n,k,t_{ML})	Remarks
10	2	(31,1,1)	(1023,893,7)	F
10	2	(3,3,1)	(1023,438,31)	D,F
10	2	(3,3,3)	(1023,748,10)	A
10	3	(1,1,1,1)	(1023,176,63)	A,B
10	3	(3,1,1,1)	(1023,388,31)	F
10	3	(31,1,1,1)	(1023,973,3)	F
10	3	(3,3,1,1)	(1023,648,15)	F
10	3	(3,3,3,1)	(1023,868,7)	D,F
10	3	(3,3,3,3)	(1023,988,2)	A
10	4	(1,1,1,1,1)	(1023,386,31)	A,B
10	4	(3,1,1,1,1)	(1023,638,15)	E
10	4	(31,1,1,1,1)	(1023,1013,1)	E
10	4	(3,3,1,1,1)	(1023,848,7)	E
10	4	(3,3,3,1,1)	(1023,968,3)	E
10	4	(3,3,3,3,1)	(1023,1013,1)	D,E
10	5	(1,1,1,1,1,1)	(1023,638,15)	A,B
10	5	(3,1,1,1,1,1)	(1023,848,7)	E
10	5	(3,3,1,1,1,1)	(1023,968,3)	E
10	5	(3,3,3,1,1,1)	(1023,1013,1)	E
10	6	(1,1,1,1,1,1,1)	(1023,848,7)	A,B
10	6	(3,1,1,1,1,1,1)	(1023,968,3)	E
10	6	(3,3,1,1,1,1,1)	(1023,1013,1)	E
10	7	(1,1,1,1,1,1,1,1)	(1023,968,3)	A,B
10	7	(3,1,1,1,1,1,1,1)	(1023,1013,1)	E
10	8	(1,1,1,1,1,1,1,1,1)	(1023,1013,1)	A,B
11	0	(1)	(2047,1,1023)	A,B
11	1	(1,1)	(2047,12,511)	A,B
11	2	(1,1,1)	(2047,67,255)	A,B
11	3	(1,1,1,1)	(2047,232,127)	A,B

m	r	N_{r+1}	(n,k,t_{ML})	Remarks
11	4	(1,1,1,1,1)	(2047,562,63)	A,B
11	5	(1,1,1,1,1,1)	(2047,1024,31)	A,B
11	6	(1,1,1,1,1,1,1)	(2047,1486,15)	A,B
11	7	(1,1,1,1,1,1,1,1)	(2047,1816,7)	A,B
11	8	(1,1,1,1,1,1,1,1,1)	(2047,1981,3)	A,B
11	9	(1,1,1,1,1,1,1,1,1,1)	(2047,2036,1)	A,B
12	0	(1)	(4095,1,2047)	A,B
12	0	(3)	(4095,43,682)	A
12	0	(7)	(4095,406,292)	A
12	0	(15)	(4095,1377,136)	A
12	0	(63)	(4095,3367,32)	A
12	1	(1,1)	(4095,13,1023)	A,B
12	1	(3,1)	(4095,119,511)	D,F
12	1	(7,1)	(4095,590,255)	D,F
12	1	(15,1)	(4095,1568,127)	D,F
12	1	(63,1)	(4095,3431,31)	D,F
12	1	(3,3)	(4095,581,170)	A
12	1	(15,3)	(4095,2306,42)	F
12	1	(63,3)	(4095,3815,10)	F
12	1	(7,7)	(4095,2585,36)	A
12	1	(63,7)	(4095,3971,4)	E
12	1	(15,15)	(4095,3840,8)	A
12	2	(1,1,1)	(4095,79,511)	A,B
12	2	(3,1,1)	(4095,329,255)	F
12	2	(7,1,1)	(4095,980,127)	F
12	2	(15,1,1)	(4095,2000,63)	F
12	2	(63,1,1)	(4095,3623,15)	F
12	2	(3,3,1)	(4095,988,127)	D,F
12	2	(15,3,1)	(4095,2774,31)	F
12	2	(63,3,1)	(4095,3879,7)	F

m	r	N_{r+1}	(n,k,t_{ML})	Remarks
12	2	(7,7,1)	(4095,2921,31)	D,F
12	2	(63,7,1)	(4095,4035,3)	F
12	2	(3,3,3)	(4095,2122,42)	A
12	2	(15,3,3)	(4095,3572,10)	E
12	2	(63,3,3)	(4095,4047,2)	E
12	2	(15,15,3)	(4095,4047,2)	E
12	2	(7,7,7)	(4095,3971,4)	A
12	3	(1,1,1,1)	(4095,299,255)	A,B
12	3	(3,1,1,1)	(4095,806,127)	F
12	3	(7,1,1,1)	(4095,1652,63)	F
12	3	(15,1,1,1)	(4095,2666,31)	F
12	3	(63,1,1,1)	(4095,3863,7)	F
12	3	(3,3,1,1)	(4095,1660,63)	F
12	3	(15,3,1,1)	(4095,3356,15)	F
12	3	(63,3,1,1)	(4095,4023,3)	F
12	3	(7,7,1,1)	(4095,3401,15)	F
12	3	(63,7,1,1)	(4095,4083,1)	E
12	3	(15,15,1,1)	(4095,4029,3)	F
12	3	(3,3,3,1)	(4095,2702,31)	D,F
12	3	(15,3,3,1)	(4095,3837,7)	F
12	3	(63,3,3,1)	(4095,4083,1)	E
12	3	(7,7,7,1)	(4095,4035,3)	D,F
12	3	(3,3,3,3)	(4095,3572,10)	A
12	3	(15,3,3,3)	(4095,4047,2)	E
12	4	(1,1,1,1,1)	(4095,794,127)	A,B
12	4	(3,1,1,1,1)	(4095,1588,63)	F
12	4	(7,1,1,1,1)	(4095,2534,31)	F
12	4	(15,1,1,1,1)	(4095,3338,15)	F
12	4	(63,1,1,1,1)	(4095,4023,3)	F
12	4	(3,3,1,1,1)	(4095,2522,31)	F
12	4	(15,3,1,1,1)	(4095,3801,7)	F

m	r	N_{r+1}	(n,k,t_{ML})	Remarks
12	4	(63,3,1,1,1)	(4095,4083,1)	E
12	4	(7,7,1,1,1)	(4095,3809,7)	F
12	4	(15,15,1,1,1)	(4095,4083,1)	E
12	4	(3,3,3,1,1)	(4095,3332,15)	F
12	4	(15,3,3,1,1)	(4095,4017,3)	E
12	4	(7,7,7,1,1)	(4095,4083,1)	E
12	4	(3,3,3,3,3)	(4095,4047,2)	A
12	4	(3,3,3,3,1)	(4095,3837,7)	D,F
12	4	(15,3,3,3,1)	(4095,4083,1)	E
12	4	(3,3,3,3,3)	(4095,4047,2)	A
12	5	(1,1,1,1,1,1)	(4095,1586,63)	A,B
12	5	(3,1,1,1,1,1)	(4095,2510,31)	E
12	5	(7,1,1,1,1,1)	(4095,3305,15)	F
12	5	(15,1,1,1,1,1)	(4095,3801,7)	F
12	5	(63,1,1,1,1,1)	(4095,4083,1)	E
12	5	(3,3,1,1,1,1)	(4095,3302,15)	E
12	5	(15,3,1,1,1,1)	(4095,4017,3)	E
12	5	(7,7,1,1,1,1)	(4095,4017,3)	E
12	5	(3,3,3,1,1,1)	(4095,3797,7)	E
12	5	(15,3,3,1,1,1)	(4095,4083,1)	E
12	5	(3,3,3,3,1,1)	(4095,4017,3)	E
12	5	(3,3,3,3,3,1)	(4095,4083,1)	E
12	6	(1,1,1,1,1,1,1)	(4095,2510,31)	A,B
12	6	(3,1,1,1,1,1,1)	(4095,3302,15)	E
12	6	(7,1,1,1,1,1,1)	(4095,3797,7)	E
12	6	(15,1,1,1,1,1,1)	(4095,4017,3)	E
12	6	(3,3,1,1,1,1,1)	(4095,3797,7)	E
12	6	(15,3,1,1,1,1,1)	(4095,4083,1)	E

m	r	N_{r+1}	(n,k,t_{ML})	Remarks
12	6	(7,7,1,1,1,1,1)	(4095,4083,1)	E
12	6	(3,3,3,1,1,1,1)	(4095,4017,3)	E
12	6	(3,3,3,3,1,1,1)	(4095,4083,1)	E
12	7	(1,1,1,1,1,1,1,1)	(4095,3302,15)	A,B
12	7	(3,1,1,1,1,1,1,1)	(4095,3797,7)	E
12	7	(7,1,1,1,1,1,1,1)	(4095,4017,3)	E
12	7	(15,1,1,1,1,1,1,1)	(4095,4083,1)	E
12	7	(3,3,1,1,1,1,1,1)	(4095,4017,3)	E
12	7	(3,3,3,1,1,1,1,1)	(4095,4083,1)	E
12	8	(1,1,1,1,1,1,1,1,1)	(4095,3797,7)	A,B
12	8	(3,1,1,1,1,1,1,1,1)	(4095,4017,3)	E
12	8	(7,1,1,1,1,1,1,1,1)	(4095,4083,1)	E
12	8	(3,3,1,1,1,1,1,1,1)	(4095,4083,1)	E
12	9	(1,1,1,1,1,1,1,1,1,1)	(4095,4017,3)	A,B
12	9	(3,1,1,1,1,1,1,1,1,1)	(4095,4083,1)	E
12	10	(1,1,1,1,1,1,1,1,1,1,1)	(4095,4083,1)	A,B
13	0	(1)	(8191,1,4095)	A,B
13	1	(1,1)	(8191,14,2047)	A,B
13	2	(1,1,1)	(8191,92,1023)	A,B
13	3	(1,1,1,1)	(8191,378,511)	A,B
13	4	(1,1,1,1,1)	(8191,1093,255)	A,B
13	5	(1,1,1,1,1,1)	(8191,2380,127)	A,B
13	6	(1,1,1,1,1,1,1)	(8191,4096,63)	A,B
13	7	(1,1,1,1,1,1,1,1)	(8191,5812,31)	A,B
13	8	(1,1,1,1,1,1,1,1,1)	(8191,7099,15)	A,B
13	9	(1,1,1,1,1,1,1,1,1,1)	(8191,7814,7)	A,B
13	10	(1,1,1,1,1,1,1,1,1,1,1)	(8191,8100,3)	A,B
13	11	(1,1,1,1,1,1,1,1,1,1,1,1)	(8191,8178,1)	A,B
14	0	(1)	(16383,1,8191)	A,B

m	r	N_{r+1}	(n,k,t_{ML})	Remarks
14	0	(3)	(16383,57,2730)	A
14	0	(127)	(16383,14197,64)	A
14	1	(1,1)	(16383,15,4095)	A,B
14	1	(3,1)	(16383,176,2047)	D,F
14	1	(127,1)	(16383,14325,63)	D,F
14	1	(3,3)	(16383,1072,682)	A
14	2	(1,1,1)	(16383,106,2047)	A,B
14	2	(3,1,1)	(16383,540,1023)	F
14	2	(127,1,1)	(16383,14773,31)	F
14	2	(3,3,1)	(16383,2017,511)	D,F
14	2	(3,3,3)	(16383,5351,170)	A
14	3	(1,1,1,1)	(16383,470,1023)	A,B
14	3	(3,1,1,1)	(16383,1513,511)	F
14	3	(127,1,1,1)	(16383,15445,15)	F
14	3	(3,3,1,1)	(16383,3783,255)	F
14	3	(3,3,3,1)	(16383,7472,127)	D,F
14	3	(3,3,3,3)	(16383,11728,42)	A
14	4	(1,1,1,1,1)	(16383,1471,511)	A,B
14	4	(3,1,1,1,1)	(16383,3487,255)	F
14	4	(127,1,1,1,1)	(16383,16005,7)	F
14	4	(3,3,1,1,1)	(16383,6576,127)	F
14	4	(3,3,3,1,1)	(16383,10216,63)	F
14	4	(3,3,3,3,1)	(16383,13443,31)	D,F
14	4	(3,3,3,3,3)	(16383,15473,10)	A
14	5	(1,1,1,1,1,1)	(16383,3473,255)	A,B
14	5	(3,1,1,1,1,1)	(16383,6478,127)	F
14	5	(127,1,1,1,1,1)	(16383,16285,3)	F
14	5	(3,3,1,1,1,1)	(16383,9922,63)	F

m	r	N_{r+1}	(n,k,t_{ML})	Remarks
14	5	(3,3,3,1,1,1)	(16383,12953,31)	F
14	5	(3,3,3,3,1,1)	(16383,14983,15)	F
14	5	(3,3,3,3,3,1)	(16383,15984,7)	D,F
14	5	(3,3,3,3,3,3)	(16383,16320,2)	A
14	6	(1,1,1,1,1,1,1)	(16383,6476,127)	A,B
14	6	(3,1,1,1,1,1,1)	(16383,9908,63)	E
14	6	(127,1,1,1,1,1,1)	(16383,16369,1)	E
14	6	(3,3,1,1,1,1,1)	(16383,12911,31)	E
14	6	(3,3,3,1,1,1,1)	(16383,14913,15)	E
14	6	(3,3,3,3,1,1,1)	(16383,15914,7)	E
14	6	(3,3,3,3,3,1,1)	(16383,16278,3)	E
14	6	(3,3,3,3,3,3,1)	(16383,16369,1)	D,E
14	7	(1,1,1,1,1,1,1,1)	(16383,9908,63)	A,B
14	7	(3,1,1,1,1,1,1,1)	(16383,12911,31)	E
14	7	(3,3,1,1,1,1,1,1)	(16383,14913,15)	E
14	7	(3,3,3,1,1,1,1,1)	(16383,15914,7)	E
14	7	(3,3,3,3,1,1,1,1)	(16383,16278,3)	E
14	7	(3,3,3,3,3,1,1,1)	(16383,16369,1)	E
14	8	(1,1,1,1,1,1,1,1,1)	(16383,12911,31)	A,B
14	8	(3,1,1,1,1,1,1,1,1)	(16383,14913,15)	E
14	8	(3,3,1,1,1,1,1,1,1)	(16383,15914,7)	E
14	8	(3,3,3,1,1,1,1,1,1)	(16383,16278,3)	E
14	8	(3,3,3,3,1,1,1,1,1)	(16383,16369,1)	E
14	9	(1,1,1,1,1,1,1,1,1,1)	(16383,14913,15)	A,B
14	9	(3,1,1,1,1,1,1,1,1,1)	(16383,15914,7)	E
14	9	(3,3,1,1,1,1,1,1,1,1)	(16383,16278,3)	E
14	9	(3,3,3,1,1,1,1,1,1,1)	(16383,16369,1)	E
14	10	(1,1,1,1,1,1,1,1,1,1,1)	(16383,15914,7)	A,B
14	10	(3,1,1,1,1,1,1,1,1,1,1)	(16383,16278,3)	E

m	r	N_{r+1}	(n,k,t_{ML})	Remarks
14	10	(3,3,1,1,1,1,1,1,1,1,1)	(16383,16369,1)	E
14	11	(1,1,1,1,1,1,1,1,1,1,1,1)	(16383,16278,3)	A,B
14	11	(3,1,1,1,1,1,1,1,1,1,1,1)	(16383,16369,1)	E
14	12	(1,1,1,1,1,1,1,1,1,1,1,1,1)	(16383,16369,1)	A,B

TABLE II

m	n_0	r	N_r	(n,k,t_{ML})	Remarks
6	3	1	(3)	(21,11,2)	$\bar{A}$
8	3	1	(3)	(85,24,10)	$\bar{A}$
8	3	2	(3,3)	(85,68,2)	$\bar{A}$
9	7	1	(7)	(73,45,4)	$\bar{A}$
10	3	1	(3)	(341,45,42)	$\bar{A}$
10	3	2	(3,3)	(341,195,10)	$\bar{A}$
10	3	3	(3,3,3)	(341,315,2)	$\bar{A}$
12	3	1	(3)	(1365,76,170)	$\bar{A}$
12	7	1	(7)	(585,184,36)	$\bar{A}$
12	15	1	(15)	(273,191,8)	$\bar{A}$
12	3	2	(3,3)	(1365,483,42)	$\bar{A}$
12	7	2	(7,7)	(585,520,4)	$\bar{A}$
12	3	3	(3,3,3)	(1365,1063,10)	$\bar{A}$
12	3	3	(15,3,3)	(1365,1328,2)	$\bar{B}$
12	3	4	(3,3,3,3)	(1365,1328,2)	$\bar{A}$
14	3	1	(3)	(5461,119,682)	$\bar{A}$
14	3	2	(3,3)	(5461,1064,170)	$\bar{A}$
14	3	3	(3,3,3)	(5461,3185,42)	$\bar{A}$
14	3	4	(3,3,3,3)	(5461,4900,10)	$\bar{A}$
14	3	5	(3,3,3,3,3)	(5461,5411,2)	$\bar{A}$
15	7	1	(7)	(4681,590,292)	$\bar{A}$
15	31	1	(31)	(1057,813,16)	$\bar{A}$
15	7	2	(7,7)	(4681,3105,36)	$\bar{A}$
15	7	3	(7,7,7)	(4681,4555,4)	$\bar{A}$
16	3	1	(3)	(21845,176,2730)	$\bar{A}$
16	15	1	(15)	(4369,1568,136)	$\bar{A}$

m	n_0	r	N_r	(n,k,t_{ML})	Remarks
16	3	2	(3,3)	(21845,2136,682)	$\bar{A}$
16	15	2	(15,15)	(4369,4112,8)	$\bar{A}$
16	3	3	(3,3,3)	(21845,8536,170)	$\bar{A}$
16	3	3	(15,3,3)	(21845,16628,42)	$\bar{B}$
16	3	4	(3,3,3,3)	(21845,16628,42)	$\bar{A}$
16	3	4	(15,3,3,3)	(21845,20884,10)	$\bar{B}$
16	3	4	(15,15,3,3)	(21845,21780,2)	$\bar{B}$
16	3	5	(3,3,3,3,3)	(21845,20884,10)	$\bar{A}$
16	3	5	(15,3,3,3,3)	(21845,21780,2)	$\bar{B}$
16	3	6	(3,3,3,3,3,3)	(21845,21780,2)	$\bar{A}$