MATHEMATICS OF COMPUTATION
VOLUME 49, NUMBER 180
OCTOBER 1987, PAGES 621–633

Perfect Multiple Error-Correcting Arithmetic Codes

By Daniel M. Gordon*

Abstract. An *arithmetic code* is a subgroup of $\mathbf{Z}_{r^n \pm 1}$, with the arithmetic distance $d(x, y) = \min_t x - y \equiv \sum_{i=1}^{t} c_i r^{n(i)} \pmod{r^n \pm 1}$, for $|c_i| < r$, $n(i) \geqslant 0$ for $1 \leqslant i \leqslant t$. A *perfect* e-error-correcting code is one from which all $x \in \mathbf{Z}_{r^n \pm 1}$ are within distance e of exactly one codeword. Necessary and sufficient (assuming the Generalized Riemann Hypothesis) conditions for the existence of infinitely many perfect single error-correcting codes for a given r are known. In this paper some conditions for the existence of perfect multiple error-correcting codes are given, as well as the results of a computer search for examples.

1. Introduction. The most general definition of a code is a set X (usually thought of as messages), a subset C (codewords) and a distance function (number of errors), with C chosen so that the codewords are far apart in the given metric. In the Hamming metric, X is the set of all strings of 0's and 1's of a given length, and the distance is the number of different digits. In this paper, we deal with a different type of code:

Definition. For $x \in \mathbf{Z}_m$, the ring of integers mod m, the *arithmetic weight* of x is the minimal number of nonzero entries in any representation $x \equiv \sum_{i=0}^{\infty} c_i r^i \pmod{m}$, with $|c_i| < r$ for all i.

Every x has many different representations. One example is the base r representation of x, although that is in general not minimal.

The reason for this definition is that, when doing computer arithmetic in $\mathbf{Z}_m$ with radix r, an error consists of changing a digit, i.e., adding or subtracting a multiple of r^i. The arithmetic weight gives a lower bound on the number of changed digits in a number.

Definition. For $x, y \in \mathbf{Z}_m$, the *arithmetic distance* $d(x, y)$ is the arithmetic weight of $x - y$.

For the purposes of arithmetic codes, m is always taken to be $r^n \pm 1$, for several reasons. In these cases the arithmetic distance is a sensible measure of the number of errors, which is not true in general. Also, arithmetic mod $r^n \pm 1$ is easy to do on a computer (see [4]). Since $r^n \equiv \pm 1 \pmod{m}$, we need only take n digits in a representation. For notational convenience, a representation $x \equiv \sum_{i=0}^{n-1} c_i r^i$ will be written as $(c_{n-1}, c_{n-2}, \ldots, c_1, c_0)$.

Definition. Let $m = r^n \pm 1 = AB$, for some $A, B \in \mathbf{Z}^+$. An *arithmetic code* is a subgroup $C = \{AN \mid 0 \leqslant N < B\}$ of $\mathbf{Z}_m$.

Received April 4, 1986; revised February 6, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 94B20.
*Computer time for this work was provided by the San Diego Supercomputer Center.

From this definition, B is the number of codewords in C, which is the ideal generated by A. To use this code, a number N is encoded as AN, and an addition would be done: $AN_1 + AN_2 = A(N_1 + N_2) + error$. Since $A(N_1 + N_2)$ is a codeword, the result can be decoded if few enough errors have been made, and the sum recovered.

If $m = r^n - 1$, the code is called *cyclic*, because any cyclic shift of a codeword is also a codeword: If $x = (c_{n-1}, \ldots, c_0)$ is in a code C, then

$$rx \equiv (c_{n-2}, \ldots, c_0, c_{n-1}) \pmod{r^n - 1}$$

is also in the code. If $m = r^n + 1$, the code is called *negacyclic*, for similar reasons:

$$rx \equiv (c_{n-2}, \ldots, c_0, -c_{n-1}) \pmod{r^n + 1}.$$

Definition. An *e-error-correcting code* (*e-code* for short) is a code for which every element of $\mathbf{Z}_m$ is distance $\leqslant e$ from at most one codeword. Equivalently, any two codewords are distance $\geqslant 2e + 1$ apart. A code is called *perfect* if every element is distance $\leqslant e$ from *exactly* one codeword.

Perfect codes are good in the sense that they have no wasted space (errors which cannot be decoded). Also, perfect codes tend to be nice mathematical structures. For Hamming codes the existence of perfect codes is more or less solved. For arithmetic codes, only the case of single error-correcting codes is well understood. Lenstra, in [5], finds necessary and sufficient conditions for an infinite number of perfect 1-error-correcting codes to exist for a given r and n, assuming the Generalized Riemann Hypothesis.

As an example, take $r = 3$, $n = 3$ and $m = r^n - 1 = 26$. Then $A = 13$ generates a perfect 1-error-correcting code with two codewords, 0 and 13. The sphere of radius 1 around zero has thirteen elements: $\{0, \pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\}$. The other thirteen elements of $\mathbf{Z}_{26}$ form a 1-sphere around 13, which has weight 3.

In this paper we examine the existence of perfect e-error-correcting arithmetic codes for $e > 1$. In Section 2 an explicit version of the sphere-packing condition is developed to give a powerful necessary condition on the existence of these codes. A table of all cases passing this condition for $A < 2^{41}$ is given. To eliminate most of the entries in this table, more necessary conditions are derived in Section 3, using some combinatorial arguments and some elementary number theory.

In Section 4 we give the only known family of perfect codes, one for each e. Each of these codes has only two codewords and is analogous to the repetition codes in the Hamming metric (where the two codewords are the vector of all zeros and the vector of all ones). Despite a fairly extensive computer search, no other perfect codes were found.

The last part of the paper is devoted to a heuristic argument that other perfect multiple error-correcting arithmetic codes, if any exist, are very rare, and would involve huge numbers. This argument uses some sieve theory and a reasonable, if unprovable, assumption.

2. The Sphere-Packing Condition. From now on we will only consider perfect codes. A starting point for any investigation of perfect codes is the sphere-packing condition: Since the space $\mathbf{Z}_m$ is partitioned into a union of e-spheres, the size of the sphere (denoted $|S_e(r, n)|$) must divide the size of the whole space.

$m = (\#\text{ of codewords}) \cdot |S_e(r, n)| = B \cdot |S_e(r, n)|$. But $m = AB$ by the definition of the code, so $A = |S_e(r, n)|$. For convenience we will refer to A as the size of any e-sphere, not writing out its dependence on e, r and n, and whether m is $r^n + 1$ or $r^n - 1$.

In the case of arithmetic codes, the size of the e-sphere is not obvious. Different error patterns give the same result; for instance, $3 = 2^1 + 2^0 = 2^2 - 2^0$. To calculate it, the following results from van Lint [6] are needed:

Definition. The pair (b, c) is *admissible* if any one of the following hold:

(2.1a) (i) $bc = 0$,

(2.1b) (ii) $bc > 0$ and $|b + c| < r$,

(2.1c) (iii) $bc < 0$ and $|b| > |c|$.

Definition. A representation $x = \sum_{i=0}^{\infty} c_i r^i$, with $c_i \in Z$, $|c_i| < r$ for all i and $c_i = 0$ for all large i is called an *NAF* (*nonadjacent form*), if for every $i \geqslant 0$ the pair (c_{i+1}, c_i) is admissible.

THEOREM 1. *Every integer x has exactly one NAF. If this is*

$$x = \sum_{i=0}^{\infty} c_i r^i,$$

then its arithmetic weight is

$$w(x) = |\{ i \mid i \geqslant 0,\ c_i \neq 0 \}|.$$

Proof. See [6]. van Lint gives an algorithm which turns any representation into an NAF of lesser or equal weight. Then he shows that the NAF is unique, completing the proof. □

The reason for the name "nonadjacent form" is that, for $r = 2$, an admissible pair (b, c) must satisfy $bc = 0$. Thus, in an NAF in radix 2, there are no adjacent nonzero digits.

Definition. A representation

$$x \equiv \sum_{i=0}^{n-1} c_i r^i \pmod{m}$$

is called a *CNAF* (*cyclic NAF*) if (c_{i+1}, c_i) is admissible for $i = 0, 1, \ldots, n-2$, and (c_0, c_{n-1}) is admissible if $m = r^n - 1$, or $(-c_0, c_{n-1})$ is admissible if $m = r^n + 1$.

THEOREM 2. *Every $x \in \mathbf{Z}_m$ has a unique CNAF, unless $(r + 1)x \equiv 0 \neq x \pmod{m}$. In the exceptional cases, x either has two CNAFS ($m = r^n - 1$) or none ($m = r^n + 1$).*

Proof. This theorem was given in [2] and [6] for the $m = r^n - 1$ case without proof. We will give the proof for $m = r^n + 1$, which is substantially the same as the other case.

Let $1 < x < r^n$ (the negative of a CNAF is a CNAF, and $x \equiv 1$ is obvious). The CNAF for x is also an NAF for some number congruent to $x \pmod{r^n + 1}$. The absolute value of a CNAF is less than r^n, since each of the c_i's are $< r$, and $\sum_{i=0}^{n-1}(r - 1)r^i = r^n - 1$. Thus the CNAF of x is the NAF for x itself or $x - (r^n + 1)$.

Let $y = r^n + 1 - x$. Then to determine whether x has a unique CNAF, we must determine whether the NAF's for x and y can both be CNAF's or both not be. For an NAF to be a CNAF it must have $c_i = 0$ for $i > n - 1$ and $(-c_0, c_{n-1})$ admissible. To help with this, we have the following lemma from van Lint [6]:

LEMMA 2.1. *If we denote the maximal value of i for which $c_i \neq 0$ in an NAF for x by $i(x)$ and define $i(0) := -1$ then*

$$i(x) \leqslant k \Leftrightarrow |x| < \frac{r^{k+2}}{r+1}.$$

From this follows:

LEMMA 2.2. *If c_{n-1} is the largest nonzero digit in the NAF of x, for $x > 0$, then*

$$c_{n-1} = \left[\frac{(r+1)x}{r^n}\right].$$

Now let the NAF of x be $\sum_{i=0}^{\infty} c_i r^i$, and the NAF of y be $\sum_{i=0}^{\infty} d_i r^i$. Suppose both of these are CNAF's. Then, since $i(x) < n$,

$$(r+1)x < r^{n+1}, \tag{2.2}$$

$$c_{n-1} = \left[\frac{(r+1)x}{r^n}\right] \geqslant 0, \tag{2.3}$$

$$c_0 \equiv x \pmod{r}. \tag{2.4}$$

Let $\bar{x}$ be the least positive residue of $x \bmod r$, i.e., $0 < \bar{x} \leqslant r$. Then, since $(-c_0, c_{n-1})$ is admissible, we get two possibilities from Eqs. (2.1):

$$c_0 > 0 \Rightarrow \bar{x} > c_{n-1}, \tag{2.5a}$$

$$c_0 \leqslant 0 \Rightarrow c_{n-1} + r - \bar{x} < r. \tag{2.5b}$$

But these implications are the same. Similarly, looking at the CNAF for y, we get $\bar{x} < r + 1 - d_{n-1}$. Putting these together, we have

$$c_{n-1} < \bar{x} < r + 1 - d_{n-1}. \tag{2.6}$$

Now since

$$d_{n-1} = \left[\frac{(r+1)y}{r^n}\right] = \left[r + 1 - \frac{(r+1)(x-1)}{r^n}\right], \tag{2.7}$$

Eq. (2.6) becomes

$$\left[\frac{(r+1)x}{r^n}\right] < \bar{x} < r + 1 - \left[r + 1 - \frac{(r+1)(x-1)}{r^n}\right] \tag{2.8}$$

and so

$$\frac{(r+1)(x-1)}{r^n} > \bar{x} > \frac{(r+1)x}{r^n}. \tag{2.9}$$

This is clearly impossible, so at most one of the NAF's can be a CNAF.

Next suppose that neither NAF is a CNAF. This can happen because c_n or d_n are not zero, or when $c_n = d_n = 0$, but $(-c_0, c_{n-1})$ and $(-d_0, d_{n-1})$ are both not admissible. Both cases are similar, so we will only do the latter case.

Since now we are assuming both pairs are nonadmissible, we get Eq. (2.8) turned around:

$$\left[\frac{(r+1)x}{r^n}\right] \geqslant \bar{x} \geqslant r + 1 - \left[r + 1 - \frac{(r+1)(x-1)}{r^n}\right], \tag{2.10}$$

and this gives Eq. (2.9) with the inequalities reversed. After multiplying through by r^n,

$$(r+1)x \geqslant \bar{x}r^n \geqslant (r+1)(x-1), \tag{2.11}$$

and we get

$$\bar{x}r^n \leqslant (r+1)x \leqslant \bar{x}r^n + r + 1. \tag{2.12}$$

Since $(r+1)x \equiv x \pmod{r}$, we get

$$(r+1)x = \bar{x}r^n + \bar{x} = \bar{x}(r^n+1). \tag{2.13}$$

All that is left to complete the proof is to show that the weights of the exceptional cases are as given. This is easily done by writing down the NAF's of these numbers and seeing that they have the proper weights:

$$\mathrm{NAF}\left(\frac{r^n+1}{r+1}\right) = (1,0,1-r,0,\ldots,0,1-r),$$

$$\mathrm{NAF}\left(r\frac{r^n+1}{r+1}\right) = (1,0,1-r,0,\ldots,1-r,0),$$

$$\mathrm{NAF}\left(k\frac{r^n+1}{r+1}\right) = (k,1-k,k+2-r,\ldots,1-k,k+2-r).$$

It is easy to verify that these are the NAF's of the given numbers, and that they have the right weights. □

COROLLARY 2.1. *The arithmetic weight of $x \in \mathbf{Z}_m$ is equal to the number of nonzero digits in its CNAF. In the exceptional cases mentioned in the last theorem, the weight of x is $[(n+1)/2]$ if $x \equiv \pm m/(r+1)$, and n otherwise.*

The exceptional cases are a nuisance, but for a fixed e they only matter for $[(n+1)/2] \leqslant e$. But any nonzero codeword in a perfect e-code must have weight $\geqslant 2e+1$, so clearly n must be at least $2e+1$. Thus, if we exclude trivial codes (where zero is the only codeword), $[(n+1)/2] \geqslant [(2e+2)/2] > e$, so the exceptional cases do not affect the search for perfect codes. From now on, we will assume that $n \geqslant 2e+1$.

Let $B_e(r,n)$ be the ball of radius e, for a given r and n, i.e., all x such that $d(0,x) = e$. From the above results we obtain the main enumeration theorem:

THEOREM 3.

$$|B_e(r,n)| = \sum_{k=1}^{e} 2^k (r-1)^k (r-2)^{e-k} \frac{n}{k} \binom{e-1}{k-1} \binom{n-e-1}{k-1}.$$

Proof. Consider any CNAF of weight e. It has e nonzero digits, broken up by zeros into some number of blocks. We will prove the theorem by counting the number of ways to break up the nonzero digits, and then count the number of blocks of each length.

A *k-composition* of n is a set of positive integers $\lambda_1, \lambda_2, \ldots, \lambda_k$ such that $\lambda_1 + \cdots + \lambda_k = n$. These are also known as *ordered partitions*. The total number of k-compositions of n is $\binom{n-1}{k-1}$.

Any weight e CNAF may be thought of as a k-composition of e, for some k. We need to figure out how many ways a given k-composition may be arranged among the n digits, and how many admissible strings of each block length exist.

LEMMA 2.3. *The number of ways to position the blocks of a k-composition* $\lambda_1, \ldots, \lambda_k$ *of e among n digits is* $\binom{n-e}{k} + \binom{n-e-1}{k-1}\lambda_k$.

Proof. The number of arrangements with the last position zero is $\binom{n-e}{k}$, since there are $n - e$ zeros in the word, and a single block may be placed to the left of any of these zeros.

If the last position is nonzero, then the kth block must be at the end, and the other $k - 1$ blocks may be placed to the left of any of the zeros *except* the first (because then the first and last blocks would cyclically coincide, and become one block). There are $\binom{n-e-1}{k-1}$ ways to position these blocks. Then the final block may be cyclically "wrapped around" by $0, 1, \ldots, \lambda_k - 1$ digits, giving $\binom{n-e-1}{k-1}\lambda_k$ possibilities in total. □

LEMMA 2.4. *The number of admissible blocks of length* λ_i *is* $2(r-1)(r-2)^{\lambda_i - 1}$.

Proof. Call an admissible block $(a_1, \ldots, a_{\lambda_i})$. a_1 is nonzero and between $-(r-1)$ and $r - 1$, a total of $2(r-1)$ possibilities.

Now look at a_j, for $j = 2, \ldots, \lambda_i$. If a_{j-1} is negative, $a_j \in \{-r - a_{j-1} + 1, \ldots, -1, 1, \ldots, -a_{j-1} - 1\}$, by Eqs. (2.1). If a_{j-1} is positive, then $a_j \in \{-a_{j-1} + 1, \ldots, -1, 1, \ldots, r - a_{j-1} - 1\}$. In either case, there are exactly $r - 2$ possible values for a_j, $j = 2, 3, \ldots, \lambda_i$. Thus the total number of admissible blocks is $2(r-1)(r-2)^{\lambda_i - 1}$. □

Proof of Theorem 3. Using Lemmas 2.3 and 2.4, we have

$$
\begin{aligned}
|B_e(r,n)| &= \sum_{k=1}^{e} \sum_{\substack{k\text{-comps of } e \\ \lambda=(\lambda_1,\ldots,\lambda_k)}} (\#\ \textit{of ways to position}\ \lambda) \\
&\quad \cdot \prod_{i=1}^{k} (\#\ \textit{of admissible blocks of length}\ \lambda_i) \qquad (2.14) \\
&= \sum_{k=1}^{e} \sum_{\lambda} \left[\binom{n-e}{k} + \binom{n-e-1}{k-1}\lambda_k \right] \\
&\qquad \cdot 2^k (r-1)^k (r-2)^{\lambda_1 - 1 + \lambda_2 - 1 + \cdots + \lambda_k - 1}.
\end{aligned}
$$

But $\lambda_1 - 1 + \cdots + \lambda_k - 1 = e - k$, since λ is a k-composition of e. Now the λ_k term is the only term depending on λ. Since $(\lambda_1, \ldots, \lambda_{k-1})$ is a $(k-1)$-composition of $e - \lambda_k$, we can rewrite Eq. (2.14) as

$$
\begin{aligned}
|B_e(r,n)| &= \sum_{k=1}^{e} 2^k (r-1)^k (r-2)^{e-k} \\
&\quad \cdot \left[\binom{n-e}{k}\binom{e-1}{k-1} + \binom{n-e-1}{k-1} \sum_{\lambda_k=1}^{e-k+1} \sum_{\substack{(k-1)\text{-comps} \\ \text{of } e-\lambda_k}} \lambda_k \right]. \qquad (2.15)
\end{aligned}
$$

Since no terms depend on the $(k-1)$-composition of $(e - \lambda_k)$, we can replace that sum by the total number of such compositions, $\binom{e-\lambda_k-1}{k-2}$, to get

$$
\begin{aligned}
|B_e(r,n)| &= \sum_{k=1}^{e} 2^k (r-1)^k (r-2)^{e-k} \\
&\quad \cdot \left[\binom{n-e}{k}\binom{e-1}{k-1} + \binom{n-e-1}{k-1} \sum_{\lambda_k=1}^{e-k+1} \binom{e-\lambda_k-1}{k-2}\lambda_k \right]. \qquad (2.16)
\end{aligned}
$$

It is nonobvious how to simplify this further. The following lemma was determined empirically:

LEMMA 2.5.

$$\sum_{\lambda_k=1}^{e-k+1} \binom{e-\lambda_k-1}{k-2}\lambda_k = \binom{e}{k}.$$

Proof. There probably is a good combinatorial reason for this, but it is not obvious, so a proof by induction will suffice. For $e \leqslant k$ the equation is trivially true, and calling the sum $S(e,k)$, it is easy to show that it obeys the recurrence $S(e,k) = S(e-1,k) + S(e-1,k-1)$, so it must be $\binom{e}{k}$. □

Using this lemma, Eq. (2.16) becomes

$$|B_e(r,n)| = \sum_{k=1}^{e} 2^k(r-1)^k(r-2)^{e-k} \cdot\left[\binom{n-e}{k}\binom{e-1}{k-1} + \binom{n-e-1}{k-1}\binom{e}{k}\right] \tag{2.17}$$

$$= \sum_{k=1}^{e} 2^k(r-1)^k(r-2)^{e-k}\frac{n}{k}\binom{e-1}{k-1}\binom{n-e-1}{k-1}. \quad \square \tag{2.18}$$

THEOREM 4.

$$|S_e(r,n)| = 1 + \sum_{l=1}^{e}\sum_{k=1}^{l} 2^k(r-1)^k(r-2)^{l-k}\frac{n}{k}\binom{l-1}{k-1}\binom{n-l-1}{k-1}.$$

Proof. The e-sphere is just a union of balls of radius $\leqslant e$, so sum the formula in the last theorem to get this one. □

COROLLARY 2.2. $|S_2(r,n)| = 2(r-1)^2n(n-2) + 1$.

COROLLARY 2.3. $|S_2(2,n)| = 2n^2 - 4n + 1$.

This theorem is a very strong necessary condition. For $e = 2$ there are only 13 cases where $|S_2(r,n)| = A|r^n \pm 1$, for $A < 2^{41}$:

TABLE 1

Cases satisfying the sphere-packing condition

r	n	A	Comment
2	12	241	$3 \mid n$ (Corollary 3.3)
2	33	2047	$3 \mid n$ (Corollary 3.3)
2	65	8191	$2^{13} \equiv 1 \pmod{A}$
2	90	15841	$2^{45} \equiv 1 \pmod{A}$
2	513	524287	$2^{19} \equiv 1 \pmod{A}$
2	16385	536870911	$2^{29} \equiv 1 \pmod{A}$
2	262145	137438953471	$2^{37} \equiv 1 \pmod{A}$
2	325098	211376118817	$n \equiv 2 \pmod 4$ (Corollary 3.5)
3	5	121	Perfect 2-code
3	47	16921	$3^{22} - 3^{17} + 2*3^1 - 3^0 \equiv 0 \pmod{A}$
8	112	1207361	$2^{112} = 2*8^{37} \equiv -1 \pmod{A}$
9	1008	129798145	$9^{168} \equiv 1 \pmod{A}$
27	2354	7485494017	$27^{214} \equiv -1 \pmod{A}$

Most of the comments give reasons for the nonexistence of a perfect code for the given r, n, and A, using either nonexistence results proved in the next section, or the fact that A must be a primitive divisor of $r^n \pm 1$ (if $2^k \equiv 1 \pmod{A}$ for $k < n$, then $2^k - 1$ is a codeword of weight 2, which cannot happen in an e-error-correcting code for $e \geqslant 1$).

The most difficult case is where $r = 3$ and $n = 47$. Computations revealed the weight 4 codeword shown in Table 1, so the code generated by A corrects only one error and therefore is not perfect, but no theorem is known which explains why this happens. Such a theorem might help in proving stronger general nonexistence results.

Most of the $r = 2$ cases are part of an infinite family: When $n = 2^m + 1$, then

$$|S_2(2, n)| = 2n^2 - 4n + 1 = 2^{2m+1} - 1, \tag{2.19}$$

and, if $2m + 1 | 2^m + 1$,

$$|S_2(2, n)| = 2^{2m+1} - 1 | 2^n - 1 = 2^{2^m+1} - 1, \tag{2.20}$$

and so the sphere-packing condition is satisfied. Whenever $2m + 1$ is prime, this will happen if $(2 | (2m + 1)) = -1$, which is true when $2m + 1 \equiv \pm 3 \pmod{8}$. None of these give perfect codes, since in these cases $2^{2m+1} \equiv 1 \pmod{A}$, and so 1 has two different weight 1 CNAF's (mod A).

For $e = 3$, a search for all $A < 2^{50}$ found *only* the case $r = 3$, $n = 7$, which is a perfect 3-code.

3. Nonexistence Results. Stronger necessary conditions are needed, and the ones for $e = 1$ are not true in general. The following results are true for all e:

THEOREM 5. *$p | A$ implies $p \equiv 1 \pmod{2n/\operatorname{lcm}(e, e-1, \ldots, 2)}$.*

Proof. $\mathbf{Z}_m/C \cong \mathbf{Z}_A$, by the definition of a code. But for a perfect code, every element can be written as a unique codeword plus an error vector, so $\mathbf{Z}_m/C \cong \{$*errors of weight* $\leqslant e\}$. Thus, for a perfect code to exist, there must be exactly A CNAF's of weight $\leqslant e$ (as stated after Corollary 2.1; since $n \geqslant 2e + 1$ there are no exceptional cases, and each error in the e-sphere corresponds to a unique CNAF by Theorem 2).

This set of CNAF's is acted on by multiplication by the group $\{\pm r^j\}$, $j = 0, 1, \ldots, n - 1$. Multiplying by r has the effect of shifting the digits of the CNAF cyclically, sending $(c_{n-1}, \ldots, c_0)$ to $(c_{n-2}, \ldots, c_0, \pm c_{n-1})$, the sign being changed for negacyclic codes. Thus this group action can be thought of as all cyclic shifts and negations of the set of CNAF's.

This group action splits the nonzero CNAF's into orbits. It is a basic combinatorial lemma that the size of the orbit containing an object equals the size of the group acting on the object divided by the number of group elements which fix that object. Since our group of cycle shifts and negations has order $2n$, each orbit will have size $2n/f$, for some f.

In particular, each orbit has order a multiple of $2n/f$, where f is the number of nonzero entries in the CNAF. For instance, for 2-error-correcting codes, the CNAF's consist of 0, and all weight one and two admissible representations. Each of the weight one orbits has size $2n$ (only the identity fixes both the position and sign of the nonzero entry). All of the weight 2 orbits also have $2n$ elements, unless n is even,

in which case the orbit represented by

$$c^{n/2} + c = (0, \ldots, 0, c, 0, \ldots, 0, c)$$

has only n elements. Each member of the orbit is fixed by multiplication by $r^{n/2}$, a cyclic shift of $n/2$ digits.

Similarly, orbits of size $2n/f$ may be created if $f \mid n$, by spacing a number c evenly f times through the n digits of a CNAF. This does not work for a negacyclic code, since the sign changes when a number is wrapped around. To get an orbit of size $2n/f$ for a negacyclic code, f must be odd, and the sign of c must be alternated. For example, the orbit represented by

$$c^{2n/3} - c^{n/3} + c = (0, \ldots, 0, c, 0, \ldots, 0, -c, 0, \ldots, 0, c)$$

has $2n/3$ elements. Each member of the orbit is fixed by multiplication by $-r^{n/3}$, a cyclic shift of $n/3$ digits and a negation, as well as the identity and multiplication by $r^{2n/3}$.

In general, the possible sizes of orbits in a cyclic code are multiples of $2n/f$, for any $f \leqslant e$. This is true because each orbit consists of CNAF's of weight $\leqslant e$, and as described above, all orbits of weight f have size a multiple of $2n/f$.

So if $A = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$, let $Q_i = A/p_i$. Then $\{Q_i, 2Q_i, \ldots, (p_i - 1)Q_i\}$ is closed under multiplication by $\pm r$, so it is a union of orbits, each of which having size $2n/f$ for some $f \leqslant e$. So for some integral k_f's:

$$\sum_{f=1}^{e} k_f \frac{2n}{f} \mid |Q_i, \ldots, (p_i - 1)Q_i|$$

and so

$$(2n/\operatorname{lcm}(e, \ldots, 2)) \mid (p_i - 1). \quad \square$$

If we restrict the theorem to negacyclic codes, then it may be strengthened by only taking the least common multiple of the odd numbers $\leqslant e$.

Let $\Omega(A)$ be the number of prime factors of A, counted with multiplicity. In other words,

$$\Omega(p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}) = \alpha_1 + \cdots + \alpha_r.$$

COROLLARY 3.1. *For a fixed e and r, $\Omega(A) \geqslant e$ for at most a finite number of perfect codes.*

For $e = 2$, this gives a weakened version of the results for $e = 1$:

COROLLARY 3.2. *For $e = 2$ and a fixed r, any A generating a perfect code is prime, with at most finitely many exceptions.*

Proof. By Theorem 5, for a perfect code we have

$$A = |S_e(r, n)| = \prod_{i=1}^{l} \left(k_i \frac{2n}{\operatorname{lcm}(e, \ldots, 2)} + 1 \right), \qquad k_i \in \mathbf{Z}^+.$$

The left-hand side is a polynomial of degree e, by Theorem 4, so if $l > e$, and n is sufficiently large, there will be no solutions to the equation. If $l = e$, there are only a finite number of $\{k_i\}$ and n which will give solutions, unless for some choice of k_i's the polynomials are identical. But this can never happen, because the coefficients in

the polynomial on the right-hand side are all clearly positive, while from the formula for $|S_e(r, n)|$ given in Theorem 4 it can easily be shown that the coefficient of n^{e-1} is always negative.

Aside from these finite number of solutions, the sphere-packing bound cannot be met unless $l < e$. □

For an example, look at $e = r = 2$, so $A = 2n^2 - 4n + 1$. For $r = 2$, the only possible composite A would be $(n + 1)(n + 1)$, since $(2n + 1)(n + 1)$ and $(n + 1)^3$ are greater than A for all $n \geqslant 5$. Setting $(n + 1)^2 = 2n^2 - 4n + 1$, we get $n = 6$, so $A = 49$. But 49 does not divide $2^6 \pm 1$, so no such code exists. Thus, in this case A must be prime.

THEOREM 6. *For $e = 2$, $r \leqslant 81$, A must be prime, except for the case where $r = 3$, $A = 121$.*

Proof. A computer search for solutions to $A = 2(r - 1)^2 n(n - 2) + 1 = (an + 1)(bn + 1)$, done exactly as the $r = 2$ case above, revealed only a few cases [see Table 1], with only one actual perfect code. Checking higher-degree equations is harder, but unnecessary if all n such that $2(r - 1)^2 n(n - 2) + 1 \geqslant (n + 1)^3$ have been checked. Another computer search checked the sphere-packing condition for $A < 2^{41}$, which includes $n < 13100$ for $r \leqslant 81$. For $n \geqslant 13100$ and $r \leqslant 81$, $2(r - 1)^2 n(n - 2) + 1 < (n + 1)^3$, so all possible cases have been covered. □

Once the composite cases have been dealt with, as above, the primality of A gives more conditions on possible perfect codes. For instance:

COROLLARY 3.3. *No perfect e-code exists with $e \geqslant 2, 3 \mid n$ and A prime.*

Proof. Depending on m, we use one of the factorizations:

$$r^{3n} - 1 = (r^n - 1)(r^{2n} + r^n + 1),$$

$$r^{3n} + 1 = (r^n + 1)(r^{2n} - r^n + 1).$$

In either case, $A \mid m$ implies one of the factors on the right-hand side is a multiple of A, since A is prime. But the arithmetic weight of those factors is clearly $\leqslant 3$, contradicting the fact that weight$(AN) \geqslant 2e + 1$ for all nonzero codewords AN of the code. □

COROLLARY 3.4. *No perfect e-code exists with $e \geqslant 2, 2 \mid n$, A prime and $m = r^n - 1$.*

Proof. As above, using $r^{2n} - 1 = (r^n - 1)(r^n + 1)$. □

COROLLARY 3.5. *No perfect e-code exists with $e \geqslant 2$, $n \equiv 2 \pmod 4$, A prime, $r = 2$ and $m = 2^n + 1$.*

Proof. Use the Aurifeuillian factorization

$$2^{4k+2} + 1 = (2^{2k+1} + 2^{k+1} + 1)(2^{2k+1} - 2^{k+1} + 1). \quad \square$$

These results are helpful for doing computer searches, but do not exclude the existence of perfect codes for any e or r. The only such theorem we have is a generalization of one by Lenstra:

THEOREM 7. *No perfect cyclic code exists with r a square.*

Proof. Suppose $s^2 = r$. We know that $2n \mid \phi(A)$, since $\{\pm r^j\}$ is a subgroup of $\mathbf{Z}_A^*$ of order $2n$. Define $\alpha = \phi(A)/2n$. Then:

$$s^{\phi(A)/\alpha} = s^{2n} = r^n \equiv 1 \pmod{A}.$$

So s is an αth power in $\mathbf{Z}_A^*$. This implies s is the identity element in $\mathbf{Z}_A^*/\{\pm r^j\}$, since the order of this group is α. But $1 < s < r$, and each of $1, 2, \ldots, (r-1)$ are the representatives of different cosets, so we get a contradiction, and r cannot be a square. □

4. Existence Results and Computer Searches. A search for perfect e-codes for $e = 2, 3$ and 4 was done on a Cray supercomputer. The only perfect codes that were found are trivial ones and the following family of perfect codes:

THEOREM 8. *For* $r = 3$, $n = 2e + 1$, $\{0, (3n-1)/2\}$ *form a perfect e-code in* $\mathbf{Z}_{3^n-1}$.

Proof. It suffices to show that the nonzero codeword has weight $2e + 1$, and that exactly half of the elements of $\mathbf{Z}_{3^n-1}$ have weight $\leqslant e$. The CNAF's of $(3^{2e+1} - 1)/2$ are $(1, \ldots, 1)$ and $(-1, \ldots, -1)$, proving the first point.

The second is demonstrated by a bijection between CNAF's of weight $\leqslant e$ and those of weight $> e$. To construct the bijection, let u_i denote any string of zero digits, and v_i denote any admissible string of nonzero digits. Then any CNAF may be decomposed uniquely as either $(u_1, v_1, \ldots, u_k, v_k)$, or $(v_1, u_1, \ldots, v_k, u_k)$, depending on whether the CNAF starts with a zero or not. If the last digit and the first digit are both either zero or nonzero, then u_1 or v_1 is considered to "wrap around".

The crucial thing to note is that for $r = 3$ there are only four possible admissible strings of a given length:

$$(1, 1, \ldots, 1), \quad (-1, -1, \ldots, -1), \quad (2, -1, \ldots, -1), \quad (-2, 1, \ldots, 1).$$

Also note that the first digit of a string determines the whole string. The bijection consists of interchanging the u_i's and v_i's: Each string of nonzero digits is changed to zeros, and the corresponding string of zeros is changed to a nonzero string with the same first digit as the old nonzero string had.

The only exceptions to this decomposition are a CNAF with only zero digits or only nonzero digits. But these are just $(0, \ldots, 0)$ and $(1, \ldots, 1)$ (or equivalently $(-1, \ldots, -1)$), the two codewords, so it is natural to have the mapping interchange these.

It is not hard to check that this mapping is in fact a bijection. Also, if a CNAF has weight w, then its image has weight $2e + 1 - w$, since the arithmetic weight is just the number of nonzero digits of a CNAF. Thus CNAF's of weight $\leqslant e$ are mapped to those of weight $> e$, and vice versa, so there are the same number of each, and the theorem is proven. □

These codes were known before, in a sense that they are a special case of the Mandelbaum-Barrows codes (see [6] for a definition of these codes). They suffer the usual problem of these codes: far too few codewords to be useful in practice.

Aside from the empirical evidence of the searches, a heuristic argument suggests that perfect codes are rare for $e \geqslant 2$:

Conjecture. For any fixed r and $e \geqslant 2$, the number of perfect e-codes with $n < x$ is $O(\log\log x)$.

Heuristic Argument. Assume $\Omega(A) < e$, since the number of perfect codes for which A has e or more prime factors has been shown to be finite. Then for a fixed r, $A = f(n)$, where f is the polynomial given in Theorem 4. Define

$$T(x) = \left| \left\{ n \leqslant x,\ f(n) = \Pi\left(k_i \frac{2n}{\operatorname{lcm}(e,\ldots,2)} + 1 \right) \right\} \right|, \tag{4.1}$$

where each factor in the product is prime. Then we have

LEMMA 4.1. $T(x) = O(x/\log x)$.

Proof. This lemma is a special case of Theorem 5.3 of [3], in the case where $A = f(n)$ is prime. The proof given there also works for any A; the only necessary condition is that the prime factors of $f(n)$ are bounded from below, and in this case each prime factor is $\gg n$.

Let $\operatorname{ord}_A(r)$ be the order of $r \bmod A$, i.e., the smallest exponent l for which $r^l \equiv 1 \pmod{A}$. For a given A, if a perfect code exists, $\operatorname{ord}_A(r) = n$ (for $m = r^n + 1$ this is $2n$, but the argument is otherwise unchanged). We need to estimate the probability that this happens.

For $e = 2$, for which A is prime, the analysis is easy: $\mathbf{Z}_A^*$ is a cyclic group of order $A - 1 = 2(r-1)^2(n-2)n$. Exactly $2(r-1)^2(n-2)$ elements in the group have order n, so the probability that r has order n is heuristically

$$\frac{1}{2(r-1)^2(n-2)} \ll \frac{1}{n}. \tag{4.2}$$

In general, the analysis is more difficult. For A composite, $\mathbf{Z}_A^*$ is no longer cyclic. The group is isomorphic to a direct product of cyclic groups, the largest of which has order $\lambda(A)$, where λ is Carmichael's universal exponent function (see [4] for details about $\lambda(n)$).

If

$$A = \prod_{i=1}^{l} \left(k_i \frac{2n}{\operatorname{lcm}(e,\ldots,2)} + 1 \right),$$

then

$$\lambda(A) \geqslant \operatorname{lcm}\left(\left\{ k_i \frac{2n}{\operatorname{lcm}(e,\ldots,2)}, i = 1,\ldots,l \right\} \right) = \frac{2n}{\operatorname{lcm}(e,\ldots,2)} \cdot \operatorname{lcm}(k_1,\ldots,k_l).$$

The fraction of elements which have order n depends on this number and the length of the other cycles which make up $\mathbf{Z}_A^*$. For the purposes of this argument we will assume that the common factors of the k_i's are not very important, so we can approximate the length of the cycle by

$$\frac{2n}{\operatorname{lcm}(e,\ldots,2)} \prod_{i=1}^{l} k_i,$$

and so the probability of an element having order n by

$$\frac{\operatorname{lcm}(e,\ldots,2)}{2\prod_{i=1}^{l} k_i} \ll \frac{1}{n}. \tag{4.3}$$

The inequality follows from the fact that, for n sufficiently large, the leading coefficient of

$$\prod_{i=1}^{l}\left(k_i\frac{2n}{\operatorname{lcm}(e,\ldots,2)}+1\right)$$

must be $\gg n^{e-l}$, since $A = f(n)$ is a polynomial in n of degree e, and $l \leqslant e-1$.

From Eq. (4.3) we get

$$\operatorname{Exp}\left(\left|\{n < x, \operatorname{ord}_A(r) = n\}\right|\right) \ll \sum_{\substack{n=2e+1 \\ \Omega(f(n))<e}}^{x} \frac{1}{n}$$

which, by the definition of $T(n)$, equals

$$\sum_{n=2e+1}^{x} T(n)\left[\frac{1}{n}-\frac{1}{n+1}\right] \ll \sum_{n=2e+1}^{x} \frac{n}{\log n}\frac{1}{n(n+1)}$$

$$\ll \sum_{n=2e+1}^{x} \frac{1}{n\log n},$$

where the last two relations follow from Lemma 4.1.

This sum is $O(\log\log x)$. The assumption made is not provable, but it does give the right order for $e = 1$, and it has been used before for empirically supported arguments, such as Artin's Conjecture (see [8]).

This argument *does not* support the conjecture that infinitely many perfect e-codes exist. There are cases which satisfy the sphere-packing condition and are not excluded by any of the nonexistence results of Section 3, but for which no perfect code exists. When $r = 3$ and $n = 47$, $A = 16921 \mid 3^{47} + 1$, and none of the nonexistence theorems apply, but some codewords have weight 4. Without more evidence it is impossible to conjecture either way, but the argument does indicate that any further examples will be extremely large.

Department of Mathematics
The University of Georgia
Athens, Georgia 30602

1. W. E. CLARK & J. J. LIANG, "On arithmetic weight for a general radix representation of integers," *IEEE Trans. Inform. Theory*, v. 19, 1973, pp. 823–826.

2. W. E. CLARK & J. J. LIANG, "On modular weight and cyclic nonadjacent forms for arithmetic codes," *IEEE Trans. Inform. Theory*, v. 20, 1974, pp. 767–770.

3. H. HALBERSTAM & H. E. RICHERT, *Sieve Methods*, Academic Press, New York, 1974.

4. D. E. KNUTH, *The Art of Computer Programming*, Vol. 2, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

5. H. W. LENSTRA, JR., *Perfect Arithmetic Codes*, Séminaire Delange-Pisot-Poitou (Théorie des Nombres, 1977/78).

6. J. H. VAN LINT, *Introduction to Coding Theory*, Springer-Verlag, New York, 1982.

7. H. RIESEL, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985.

8. D. SHANKS, *Solved and Unsolved Problems in Number Theory*, 3rd ed., Chelsea, New York, 1985.