INFORMATION AND CONTROL 27, 336–348 (1975)

Perfect Nonbinary *AN* Codes with Distance Three

MUNEHIRO GOTO

Faculty of Engineering, Gifu University, Kakamigahara, Japan

AND

TERUO FUKUMURA

Faculty of Engineering, Nagoya University, Nagoya, Japan

It has been proved that the perfect binary and ternary single error correcting *AN* codes exist.

In this paper, perfect radix-r single error correcting codes of type I and II are defined as generalized versions of perfect binary codes, and a general theory is developed for the existence of perfect single error correcting *AN* codes by using number theoretic concepts.

This leads us to the followings:

(1) There do not exist perfect radix $4k^2$ codes of type I and perfect radix k^2 codes of type II.

(2) In the cases of radix 4, 5, 8 and 9, no perfect code of either type exists.

(3) There exist perfect codes with radices 6 and 7.

1. INTRODUCTION

AN codes are useful for computation as well as data transmission. Therefore *AN* codes have been the subject of continuing investigation over the past years. However few papers treat perfect *AN* codes. We know only two works by Peterson (1961) and Gritsenko (1969). Peterson has proved that a prime p such that 2 or -2 is a primitive root modulo p generates a perfect binary single error correcting *AN* code. Gritsenko has shown that there exist perfect ternary single error correcting *AN* codes characterized in the manner similar to that of the binary case by Peterson.

In this paper we treat modular arithmetic *AN* codes (Massey and Garcia, 1972). First it is shown that no composite number generate perfect single

error correcting codes. Next perfect radix r codes of type I and II are defined as generalized versions of Peterson's. Number theoretic concepts are used to develop a general theory for the existence of perfect radix r codes. This theory leads us to the following conclusion:

(1) There do not exist perfect radix $4k^2$ codes of type I and perfect radix k^2 codes of type II.

(2) In the cases of radix 4, 5, 8 and 9, no perfect codes exist.

(3) There exist perfect codes with radices 6 and 7.

2. Preliminaries and Earlier Works on Perfect AN Codes

An AN code generated by an integer A is the set of integers AN for $0 \leqslant N < B$, where the code length is the number of digits required to represent the integer AB in the radix r system.

In this paper we use modular distance and modular weight as metric (Massey and Garcia, 1972). As well known, modular distance is a true metric if

$$AB = r^n \pm 1, \tag{1}$$

where n is the code length in the radix r system. In what follows we will impose this restriction on AB. In this metric, a radix r code is capable of single modular error correction for all numbers in the range of $0 \leqslant N < B$ if and only if the residues of $\pm a_i r^j$ modulo A, for $0 < a_i < r$ and for all j in $0 \leqslant j < n$, are all distinct and nonzero.

It follows that the total number of single error patterns to be corrected in the radix r code of length n is $2n(r-1)$. When no error occurs, the residue of a code word modulo A is zero. Therefore, for the code generated by A to be a single error correcting code, A must satisfy at least the following inequality.

$$A \geqslant 2n(r-1) + 1.$$

If the generator A satisfies

$$A = 2n(r-1) + 1, \tag{2}$$

A is said to generate a perfect single error correcting code. Clearly the perfect code uses all residues modulo A to correct errors.

Next we show that no composite number A can generate perfect single error correcting codes.

LEMMA 1. *Let A be a composite number, p be one of its factors where $1 < p < A$ and J be a multiple of p. Then if $J \equiv Qr^j \bmod A$, Q is a multiple of p, i.e., $Q = pq$.*

Proof. Because r and A are relatively prime, for any integer J, there exist integers Q and $j > 0$ such that

$$J \equiv Qr^j \mod A.$$

If J is a multiple of p, the factor p must be included in Q, as r and A are relatively prime. Q.E.D.

Suppose that the factor p is greater than r. Then it follows from Lemma 1 that no multiple J of p can be congruence to error pattern $a_i r^j$ modulo A, because $| a_i |$ is always less than r. Thus if a composite number A generate a perfect code, equivalently if there exists a one to one onto correspondence between the set of residues modulo A and the set of single error patterns, every factor p must be less than r. This means that A is less than r^2, and hence has weight of at most two. But, in the AN code, A itself is one of the code words and so the minimum distance of this code cannot be more than or equal to three, which is not enough to correct single errors. As a consequence we have the following theorem.

THEOREM 2. *No composite number generates a perfect single error correcting AN code.*

In the sequel the perfect codes generated by a prime p are investigated. In the binary and ternary cases, we know the existence of such perfect codes.

DEFINITION 3. Let $e(r, p)$ be the minimum positive integer satisfying

$$r^{e(r,p)} \equiv 1 \mod p. \tag{3}$$

THEOREM 4 (Peterson 1961). *An odd prime p such that $e(2, p) = p - 1$ generates a type I perfect binary code. Moreover an odd prime p such that $e(2, p) = (p - 1)/2$ and odd generates a type II perfect binary code.*

THEOREM 5 (Gritsenko 1969). *Let p be a prime of form $24k + 13$. If $e(3, p)$ is $(p - 1)/2$, p generates a type I perfect ternary code. If $e(3, p)$ is $(p - 1)/4$, p generates a type II perfect ternary code.*

The type I and II perfect codes stated in the above theorems will be defined later.

This paper investigates the existence and nonexistence of the perfect single error correcting codes with radices greater than three. To do this, we require some preliminaries.

DEFINITION 6. Let $G(p)$ be a set of $1, 2, \ldots, p-1$ and $\langle r, p\rangle$ be a subset of $G(P)$ consisting of integers k_i such that

$$k_i \equiv r^i \mod p. \tag{4}$$

As well known, for a prime p, $G(p)$ is a cyclic group under the operation of multiplication modulo p, and $\langle r, p\rangle$ is one of its subgroups. Thus $G(p)$ can be expanded into cosets of $\langle r, p\rangle$ in the following manner:

$$G(p)/\langle r, p\rangle = a_1\langle r, p\rangle + a_2\langle r, p\rangle + \cdots + a_q\langle r, p\rangle, \tag{5}$$

where the number q of cosets satisfies

$$q = (p-1)/e(r, p) \tag{6}$$

and a_i's are coset leaders.

It should be noted that the elements of each coset $a_i\langle r, p\rangle$ are of the same form as the single error patterns $a_i r^j$.

LEMMA 7. (i) *When $e(r, p)$ is even, both a and $-a$ are included in the same coset of $G(p)/\langle r, p\rangle$.*

(ii) *When $e(r, p)$ is odd, a and $-a$ are included in the distinct cosets of $G(p)/\langle r, p\rangle$.*

Proof. Let $e(r, p)$ be even. Then we get from congruence (3)

$$r^{e(r,p)} - 1 = (r^{e(r,p)/2} - 1)(r^{e(r,p)/2} + 1) \equiv 0 \mod p.$$

Since p does not divide $r^{e(r,p)/2} - 1$, p must divide $r^{e(r,p)/2} + 1$. Hence we have

$$r^{e(r,p)/2} \equiv -1 \mod p. \tag{7}$$

Next let $e(r, p)$ be odd. As $e(r, p)/2$ is not an integer, congruence (7) does not hold. Suppose $r^e \equiv -1 \bmod p$ for some e in the range $0 < e < e(r, p)$. From this congruence, we get $r^{2e} \equiv 1 \bmod p$ for some $2e$ in the range $0 < e < 2e(r, p)$. Definition 3 tells us that d satisfying $r^d \equiv 1 \bmod p$ must be a multiple of $e(r, p)$. Thus $2e$ in the range $0 < 2e < 2e(r, p)$ must be

equal to $e(r, p)$. This contradicts the assumption. Therefore, if $e(r, p)$ is odd, for any e

$$r^e \not\equiv -1 \mod p. \tag{8}$$

Elements a and $-a$ are included in a particular coset, if and only if for some j

$$-a \equiv ar^j \mod p.$$

This leads us to

$$r^j \equiv -1 \mod p,$$

because a and p are relatively prime. As previously known, this holds for even $e(r, p)$ but does not for odd $e(r, p)$. Q.E.D.

As a result, the coset expansion (5) may be rewritten as follows:
For even $e(r, p)$,

$$G(p)/\langle r, p\rangle = a_1\langle r, p\rangle + a_2\langle r, p\rangle + \cdots + a_q\langle r, p\rangle, \tag{9}$$

where both a and $-a$ belong to the same coset. For odd $e(r, p)$,

$$\begin{aligned} G(p)/\langle r, p\rangle = {} & a_1\langle r, p\rangle + a_2\langle r, p\rangle + \cdots + a_{q/2}\langle r, p\rangle \\ & + (-a_1)\langle a, p\rangle + (-a_2)\langle r, p\rangle + \cdots + (-a_{q/2})\langle r, p\rangle. \end{aligned} \tag{10}$$

Finally we describe some properties of quadratic residue modulo p.
Let a and p be relatively prime. Then a is a quadratic residue (QR) modulo p if the congruence

$$x^2 \equiv a \mod p \tag{11}$$

is solvable. If this congruence has no solution, a is said to be a quadratic nonresidue (QNR) modulo p.

For an odd prime p, Legendre introduced a symbol defined in the following manner:

DEFINITION 8.

$$\left(\frac{a}{p}\right) = 1, \qquad \text{when } a \text{ is a QR modulo } p.$$

$$\left(\frac{a}{p}\right) = -1, \qquad \text{when } a \text{ is a QNR modulo } p.$$

With regard to the quadratic residue, we have some useful results described in what follows. For the proofs see Nagell (1951).

LEMMA 9. *If a and p are relatively prime,*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p. \tag{12}$$

LEMMA 10. *If p is an odd prime, there are just as many quadratic residues as nonresidue modulo p in the set $G(p)$, i.e., therefore $(p-1)/2$ of each kind.*

Table I shows the forms of the prime p of which an integer a is a quadratic residue or a quadratic nonresidue modulo p.

TABLE I

The Forms of the Prime p of which a is a QR or a QNR Modulo p

a	QR	QNR
-1	$4k+1$	$4k-1$
2	$8k+1$	$8k+3$
-2	$8k+1, +3$	$8k-1, -3$
3	$12k+1$	$12k+5$
-3	$6k+1$	$6k+5$
5	$10k+1$	$10k+3$
-5	$20k+1, -3, -7, +9$	$20k-1, +3, +7, -9$
7	$28k+1, +3, +9$	$28k+5, +11, +13$

3. Nonexistence of Perfect Radix 4, 5, 8 and 9 Codes

At the beginning, we consider the conditions under which an odd prime p generates a perfect single error correcting code. By using the conditions derived, we show the nonexistence of some perfect codes.

First, it is clear from (2) that the code length n of perfect code must satisfy

$$n = (p-1)/2(r-1). \tag{13}$$

In addition to this, the residues of all possible single errors $\pm a_i r^j$ modulo p

must be distinct and exhaust all element of $G(p)$. These conditions can be satisfied only in the following two cases.

(I) $e(r, p)$ is $(p-1)/(r-1)$ and even, and the subsequent expansion

$$G(p)/\langle r, p\rangle = 1\langle r, p\rangle + 2\langle r, p\rangle + \cdots + (r-1)\langle r, p\rangle \tag{14}$$

holds.

(II) $e(r, p)$ is $(p-1)/(r-1)$ and odd, and the subsequent expansion

$$\begin{aligned} G(p)/\langle r, p\rangle = {} & 1\langle r, p\rangle + 2\langle r, p\rangle + \cdots + (r-1)\langle r, p\rangle \\ & + (-1)\langle r, p\rangle + (-2)\langle r, p\rangle + \cdots + (1-r)\langle r, p\rangle \end{aligned} \tag{15}$$

holds.

Except the cases (I) and (II), it may occur that p divides $r^n \pm a$ for some a less than r but not equal to one, and that p generates a perfect single error correcting code. But this means

$$pB = r^n \pm a, \tag{16}$$

and so no such case occurs in the modular AN codes satisfying (1).

For convenience, in the following investigation we call the perfect codes satisfying the conditions in (I) and (II) type I and II, respectively.

Type I. We have from congruence (3) and (12)

$$\left(\frac{r}{p}\right) \equiv r^{(p-1)/2} = (r^{e(r,p)/2})^{r-1} \equiv (-1)^{r-1} \bmod p. \tag{17}$$

Hence if r is odd, r is a QR modulo p. This implies that the elements of $\langle r, p\rangle$ are all QR's modulo p. Then in order for $G(p)$ expanded in the manner of Eq. (14) to satisfy Lemma 10, half of the coset leaders 2, 3,..., and r must be QR's and the remaining must be QNR's modulo p. Because r is a QNR modulo p in the cases where r is even, such a condition is not obtained.

Type II. We see in this type that r must be a QR modulo p and so $\langle r, p\rangle$ is the set of QR's, because, referring to (3), we have

$$\left(\frac{r}{p}\right) \equiv r^{(p-1)/2} = (r^{e(r,p)})^{r-1} \equiv 1 \bmod p. \tag{18}$$

Next, from the condition that the code length n ($e(r, p)$) is odd and (13), we have

$$p = 2(2k'' + 1)(r-1) + 1.$$

Suppose that r is odd. Then this may be written as $p = 4k + 1$. With regard to this p, we have $(a/p)(-a/p) = 1$, which means that both $a \cdot \langle r, p \rangle$ and $(-a) \cdot \langle r, p \rangle$ are the sets of QR's or QNR's modulo p. Therefore in order for $G(p)$ expanded in the form of (15) to satisfy Lemma 10, half of the coset leaders 2, 3,..., r must be QR's and the remaining must be QNR's modulo p. This condition is the same as that of type I. These discussions lead us to Table II.

TABLE II

Necessary Conditions for Perfect Codes

	Type I	Type II
p	$2k'(r-1)+1$	$2(2k''+1)(r-1)+1$
$e(r, p)$	$(p-1)/(r-1)$; even	$(p-1)/2(r-1)$; odd
n	$e(r, p)/2$	$e(r, p)$
(r/p)	$(-1)^{r-1}$	1
for odd r	Half of 2, 3,..., r are QR's and the remaining are QNR's modulo p.	

THEOREM 11. *If r is $(2k)^2$, there exists no perfect radix r code.*

Proof. As $(2k)^2$ is always a QR modulo p, $((2k)^2/p) = 1$. On the other hand $(-1)^{(2k)^2-1}$ is always -1. They contradict (17). Q.E.D.

THEOREM 12. *If r is k^2, there exists no type II perfect radix r code.*

Proof. From the definition of $e(r, p)$ we have

$$r^{e(r,p)} - 1 = (k^{e(r,p)} - 1)(k^{e(r,p)} + 1) \equiv 0 \mod p.$$

Hence either

$$k^{e(r,p)} \equiv 1 \mod p \tag{19}$$

or

$$k^{e(r,p)} \equiv -1 \mod p \tag{20}$$

holds.

Clearly k or $-k$ must be a coset leader in the expansion (15), because k

is less than r. This requires at least that the set $\langle r, p\rangle$ should not contain k or $-k$, i.e.,

$$r^j \not\equiv \pm k \mod p, \qquad 0 < j < e(r, p).$$

Referring to $r = k^2$, the above congruence means that

$$k^{2j-1} \not\equiv \pm 1 \mod p,$$

for any $2j - 1$ in the range $0 < 2j - 1 < 2e(r, p) - 1$. This, however, contradicts either (19) or (20), because $e(r, p)$ is odd in the type II. Hence the coset expansion (15) is impossible. Q.E.D.

By using the results obtained above, we investigate the cases of radix 4 and 5.

THEOREM 13. *There exists no perfect radix* 4 *code.*

Proof. This is obvious from Theorem 11 with $k = 1$ and Theorem 12 with $k = 2$, because $4 = 2^2$. Q.E.D.

Next we consider the case where r is five. It follows then from Table II that r must be $8k' + 1$ in the type I and $16k'' + 1$ in the type II. In both cases 2 is a QR modulo p. As the radix 5 is odd, 5 also must be a QR modulo p in both types. Trivially 4 is a QR modulo any p. These results contradict the necessary condition in the bottom row in Table II. Thus we get the subsequent theorem.

THEOREM 14. *There exists no perfect radix* 5 *code.*

The following lemma (Redei, 1967) dealing with finite cyclic groups is useful in the investigation of perfect radix 8 and 9 codes.

LEMMA 15. *Let H be a finite cyclic group with order h. Then H has one and only one subgroup whose order is a divisor of h. Such groups exhaust all subgroups of H.*

Let p be a prime and r be k^t. Then $G(p)$, $\langle k, p\rangle$ and $\langle k^t, p\rangle$ are all finite cyclic groups and their orders are $p - 1$, $e(k, p)$ and $e(k^t, p)$, respectively.

LEMMA 16. *Let d be the greatest common divisor of t and $e(k, p)$. Then*

$$e(k^t, p) = e(k, p)/d. \tag{21}$$

The proof is omitted here (Nagell, 1951). It should be noted that, if $d = 1$, then

$$\langle k^t, p\rangle = \langle k, p\rangle.$$

In order for the perfect code with radix k^t to exist, it is necessary that k as well as one are chosen as coset leaders of expansion $G(p)/\langle k^t, p\rangle$, because k and one are less than the radix k^t. But it is impossible when $\langle k, p\rangle = \langle k^t, p\rangle$, i.e., $d = 1$.

Next consider the case where $d \neq 1$. In the type I codes, we have from (14)

$$(p - 1)/e(k^t, p) = k^t - 1. \tag{22}$$

Similarly we have for type II

$$(p - 1)/e(k^t, p) = 2(k^t - 1). \tag{23}$$

Further as $\langle k, p\rangle$ is a subgroup of $G(p)$, $e(k, p)$ must divide $p - 1$. Thus for type I,

$$(p - 1)/e(k, p) = (p - 1)/de(k^t, p) = (k^t - 1)/d.$$

This implies that d must divide $k^t - 1$. Likewise in the type II, d must divide $2(k^t - t)$.

THEOREM 16. *Let d be the greatest common divisor of t and $e(k, p)$. If d equals one, no perfect radix k^t codes exist. Next let d be not one. Then, if d does not divide $k^t - 1$, no type I perfect codes with radix k^t exist. If d does not divide $2(k^t - 1)$, no type II perfect codes with radix k^t exist.*

COROLLARY 17. *There exists no perfect radix 8 code.*

Proof. As $8 = 2^3$, let k be 2 and t be 3. If d is not one, d must be 3. But 3 does not divide $2^3 - 1$ as well as $2(2^3 - 1)$. Q.E.D.

Finally we consider the perfect radix 9 codes. First of all, it is clear from Theorem 12 that there exist no type II perfect radix 9 code, because $9 = 3^2$. For type I, we obtain from Table II

$$p = 16k + 1. \tag{24}$$

Further, half of 2, 3,..., 8 and 9 must be QR's and the remaining must be QNR's modulo p. But 4 and 9 are trivially QR's, and 2 is a QR modulo p represented by (24). Thus 8 is also a QR. Hence the remaining 3, 5, 6 and 7 must be QNR's.

As $9 = 3^2$, let $k = 3$ and $t = 2$. Referring to Theorem 16, d, the greatest common divisor t and $e(k, p)$, must be 2 in order for the perfect codes with radix 3^2 to exist. From (21) and (24),

$$e(3, p) = (p - 1)/4 = 4k. \tag{25}$$

On the other hand, $G(p)$ is represented by $\langle g, p\rangle$, where g is a primitive root modulo p. The order of $G(p)$ is $p - 1$, which is divided by 4 [cf. (24)]. Thus

$$e(g^4, p) = (p - 1)/4 = 4k. \tag{26}$$

From (25), (26), and Lemma 15,

$$\langle g^4, p\rangle = \langle 3, p\rangle.$$

Clearly g^4 is always a QR and so $\langle g^4, p\rangle$ is the set of QR's. This contradicts the requirement that 3 must be a QNR. Hence we obtain the following theorem.

THEOREM 18. *There exists no perfect radix 9 code.*

4. Search for Perfect Radix 6, 7, and 10 Codes

Because 6 and 10 are even, the nonexistence of perfect radix 6 and 10 codes is not decided by using the conditions listed in Table II. The table gives us no information except that p must be of the form

$$10k + 1 \quad \text{or} \quad 18k + 1$$

if p generates a perfect radix 6 or 10 code.

For radix 7 codes, we have a little more information. From the first row in Table II, p must satisfy

$$p = 12k + 1. \tag{27}$$

Because the radix 7 is odd, 7 must be a QR modulo p. Obviously 3 is a QR modulo p satisfying (26). Trivially 4 is a QR. Therefore it follows from the last row in Table II that 2, 5, and 6 must be QNR's modulo p.

Referring to Table I, a prime p satisfying these conditions is one of the forms

$$\begin{array}{lll} 840k + 37, & 840 + 235, & 840k + 277, \\ 840k + 373, & 840k + 613, & 840k + 757. \end{array}$$

But these restriction on p are not enough to decide the existence or nonexistence of perfect radix 7 codes as well as in the cases of radix 6 and 10 codes.

In this paper, we search which prime p makes the expansion (14) or (15) with $r = 6, 7, 10$ possible. This required a long computation time. As a result, we found some perfect radix 6 and 7 codes (cf. Table III), but no perfect radix 10 code for p less than 10^6.

TABLE III

Examples of Perfect Codes with Radices 6 and 7

$\gamma = 6$			$\gamma = 7$		
prime	n	type	prime	n	type
7741	774	I	19237	1603	II
10831	1083	I	30013	2501	II
18191	1819	II	56053	4671	I
20611	2061	II	67453	5621	I

5. Conclusions

This paper treats a general theory with respect to perfect single error correcting AN codes. Almost all the results given here are negative for the existence of perfect codes. But this does not mean htat there exist no perfect codes except for binary and ternary cases. The extensive computation shows the existence of perfect radix 6 and 7 codes.

We do not obtain theoretical results to assure the nonexistence of perfect decimal codes, even though the computer search shows that there exist no such codes for primes p less than 10^6. This is an open problem of interest from a practical point of view.

Acknowledgments

We would like to acknowledge the continuing guidance and encouragement of Professor N. Honda of Tohoku University and Professor K. Ikegaya of Nagoya University.

We used the computer FACOM 230/60 at Nagoya University to obtain Table III.

Received: August 27, 1973; received: January 25, 1974

REFERENCES

GRITSENKO, V. M. (1969), Nonbinary arithmetic correcting codes, *Problems of Information Transmissions*, **5**, 21–27.

MASSEY, J. L., AND GARCIA, O. N. (1972), Error-correcting codes in computer arithmetic, *in* "Advances in Information Systems Science" (J. T. Tou, Ed.), Vol. 4, pp. 235–326, Plenum Press, New York.

NAGELL, T. (1951), "Introduction to Number Theory," John Wiley and Sons Inc., New York.

PETERSON, W. W. (1961), "Error-Correcting Codes," The MIT Press, Cambridge, MA.

REDEI, L. (1967), "Algebra," Vol. 1, Pergamon Press.