MATHEMATICS OF COMPUTATION, VOLUME 25, NUMBER 115, JULY, 1971

On a Diophantine Equation Related to Perfect Codes

By Ronald Alter

Abstract. A necessary condition for the existence of perfect double Hamming-error-correcting codes on q symbols, for q a prime power, is that the Diophantine equation

$$\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 = q^k$$

have a nontrivial solution in positive integers. In this paper this equation is considered for all q, and by applying Newton's method for approximating the roots of a polynomial, it is established that it has no nontrivial solutions for all n, odd k, and q of the form $q = 2s^2$.

1. Introduction. Let V_n be the n-dimensional vector space of all n-tuples whose entries are taken from the ring of integers mod q (q a prime power). By the distance between two points of V_n, we mean the number of places in which the points disagree. A perfect double Hamming-error-correcting code on q symbols is a subspace S of V_n, subject to the following conditions:

The distance between any two points of S is at least 5.

Every point V_n is within distance 2 of some (hence a unique) point of S.

Clearly, $\#(V_n) = q^n$, and, since S is a subspace, $\#(S) = q^{n-k}$ for some $k \leqq n$. With regards to coding theory, n represents the number of transmission symbols and k is the number of check symbols.

It is known that a necessary condition for the existence of perfect double Hamming-error-correcting codes on q symbols is that V_n form disjoint spheres of radius two about the points of its subspace S. (For this sphere-packing development and more details and information about perfect Hamming-error-correcting codes, the reader is referred to Berlekamp [1].)

If S_q represents the number of points in each such sphere, then $\#(S)\cdot S_q = \#(V_n)$. But

$$S_q = \sum_{i=0}^{2} \binom{n}{i}(q-1)^i,$$

thus

$$\sum_{i=0}^{2} \binom{n}{i}(q-1)^i = q^k. \tag{1}$$

Writing (1) as a quadratic equation in n yields

$$(q-1)^2n^2 - (q^2 - 4q + 3)n + 2(1 - q^k) = 0. \tag{2}$$

Clearly, (2) always has the trivial solutions in positive integers $k = n = 1$ and

Received July 20, 1970.

AMS 1970 *subject classifications.* Primary 94A10; Secondary 10B05, 05B40.

Key words and phrases. Perfect double Hamming-error-correcting codes, Newton approximation method, exponential Diophantine equation, Thue-Siégel-Roth Theorem.

$k = n = 2$. By fixing q, (2) becomes a Diophantine equation in n and k. This equation has been completely solved by various authors, including the present one, for all k and n when $q < 10$. (For a discussion of this, the reader is referred to Alter [2].) J. H. van Lint [3] used (1) simultaneously with another Diophantine equation which is also a necessary condition for the existence of perfect Hamming-error-correcting codes and proved

THEOREM 1. *For $n > 2$ and $q > 3$ (q a prime power), there are no perfect double Hamming-error-correcting codes on q symbols.*

Because of the above theorem, (1) is no longer an equation of great importance to coding theorists. However, if one could show that, for the Hamming metric, when q is not a prime power, the total number of code words is still a power of q, (1) would then be an important equation in the study of perfect codes over a nonprime power alphabet. Nevertheless, independent of coding theory, (1) is an interesting Diophantine equation, for, among other things, very little is known about exponential Diophantine equations.

In [2], using a variation of the Thue-Siégel-Roth Theorem, it is proven that (2) has only finitely many integer solutions. In the present paper, using Newton's method for solving equations by constructing an approximating sequence to the roots, the following theorem is established.

THEOREM 2. *The Diophantine equation* (2) *has no nontrivial solutions in positive integers for k odd and q of the form $q = 2s^2$.*

2. Newton's Method. Returning to (2) and letting $n = x/(q - 1)$, it follows that

$$x^2 + (3 - q)x + 2(1 - q^k) = 0. \tag{3}$$

(If r is a root of (3), then $r/(q - 1)$ is a root of (2) and thus must be an integer.) To apply Newton's method, let

$$f(x) = x^2 + (3 - q)x + 2(1 - q^k). \tag{4}$$

Then

$$f'(x) = 2x + (3 - q) \quad \text{and} \quad f''(x) = 2. \tag{5}$$

Clearly, $f(x)$ is a monotone increasing function of x for all $x \geqq (q - 3)/2$, since $f'(x) \geqq 0$ for all such x. Also, since $f''(x)$ does not change sign, there are no points of inflection in the interval $[(q - 3)/2, \infty)$.

Make the initial guess

$$x_0 = \sqrt{2}\, q^{k/2} + \frac{q - 3}{2}. \tag{6}$$

Then it follows that the sequence

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}, \qquad n = 0, 1, 2, \cdots, \tag{7}$$

converges to the positive root r of $f(x)$.

The following computations, which are necessary for the application of this

method, are easily verified.

$$f(x_0) = -\frac{q^2 - 6q + 1}{4}. \qquad f'(x_0) = 2\sqrt{2}\, q^{k/2}.$$

$$x_1 = x_0 - \frac{f(x_0)}{f'(x_0)} = \sqrt{2}\, q^{k/2} + \frac{q-3}{2} + \frac{q^2 - 6q + 1}{8\sqrt{2}\, q^{k/2}}. \tag{8}$$

$$f(x_1) = \frac{(q^2 - 6q + 1)^2}{128q^k}. \qquad f'(x_1) = 2\sqrt{2}\, q^{k/2} + \frac{q^2 - 6q + 1}{4\sqrt{2}\, q^{k/2}}.$$

$$x_2 = \sqrt{2}\, q^{k/2} + \frac{q-3}{2} + \frac{q^2 - 6q + 1}{8\sqrt{2}\, q^{k/2}} - \frac{(q^2 - 6q + 1)^2}{16\sqrt{2}\, q^{k/2}(16q^k + q^2 - 6q + 1)}.$$

It is easy to see from the last two terms in the expansion of x_2, that the convergence to the positive root r of (3) is quite rapid. In fact, it follows that

$$f(x_0) < 0 = f(r) < f(x_2) < f(x_1) \quad \text{and thus} \quad x_0 < r < x_2 < x_1. \tag{9}$$

3. Proof of the Theorem. There are two parts to this proof, (i) $k > 3$ and (ii) $k = 3$.

(i) Letting $k = 2t - 1$ and $q = 2s^2$, it follows that

$$x_0 = 2^t s^k + s^2 - 2 + \tfrac{1}{2} = m + .5 \quad \text{for some integer } m.$$

$$x_1 = m + .5 + \epsilon, \quad \text{where, for } k > 3, \quad 0 < \epsilon = \frac{q^2 - 6q + 1}{8\sqrt{2}\, q^{k/2}} < \frac{1}{8\sqrt{2}} < .09.$$

Hence it follows, for $k > 3$ odd, that

$$m + .5 < r < m + .59. \tag{10}$$

Thus, r is not an integer and this completes the first part of the proof.

(ii) Here $k = 3$ and (4) becomes

$$f(x) = x^2 + (3 - q)x + 2(1 - q^3). \tag{11}$$

Once again Newton's method is used, however this time a closer initial guess is made. Letting

$$x_0 = \sqrt{2}\, q^{3/2} + \frac{q-3}{2} + \frac{q-7}{8(2q)^{1/2}}, \tag{12}$$

the following can be established.

$$f(x_0) = -\frac{31q^2 + 46q - 49}{128q}. \qquad f'(x_0) = 2\sqrt{2}\, q^{3/2} + \frac{q-7}{4(2q)^{1/2}}.$$

$$x_1 = \sqrt{2}\, q^{3/2} + \frac{q-3}{2} + \frac{q-7}{8(2q)^{1/2}} + \frac{31q^2 + 46q - 49}{16(2q)^{1/2}(16q^2 + q - 7)}. \tag{13}$$

$$f(x_1) = \left(\frac{31q^2 + 46q - 49}{16(2q)^{1/2}(16q^2 + q - 7)}\right)^2.$$

From (13) it follows that

$$f(x_0) < 0 = f(r) < f(x_1) \quad \text{and thus} \quad x_0 < r < x_1. \tag{14}$$

Since $q = 2s^2$, it follows that

$$x_0 = 4s^3 + s^2 - 2 + \left[\frac{s}{8}\right] + \frac{a}{8} + \frac{1}{2} - \frac{7}{16s} = M + \frac{a}{8} + \frac{1}{2} - \frac{7}{16s},$$

and $x_1 < M + a/8 + 1/2 - 6/16s$ holds for some integer M and where $[y]$ = greatest integer $\leqq y$ and $a \in A$ where $A = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Now letting a run through the members of A and using

$$M + \frac{a}{8} + \frac{1}{2} - \frac{7}{16s} < r < M + \frac{a}{8} + \frac{1}{2} - \frac{6}{16s}, \tag{15}$$

it follows for $s \geqq 3$ (for $s < 3$, the problem has already been solved) that r lies properly between two consecutive integers and thus cannot be an integer. This completes the proof of Theorem 2.

4. Remark. On examining Theorem 2 for k even and q of the form $q = 2s^2$, one can easily establish that $n \equiv 1$ or $2 \pmod 4$; however, it is not clear how to proceed from here.

University of Kentucky
Lexington, Kentucky 40506

1. E. R. BERLEKAMP, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968, pp. 302–309. MR 38 #6873.
2. R. ALTER, *Perfect Double Hamming-Error-Correcting Codes on Q-Symbols*, Proc. Third Annual Princeton Conf. on Information Sciences and Systems, 1969, pp. 547–550.
3. J. H. VAN LINT, "On the nonexistence of perfect 2- and 3-Hamming-error-correcting codes over GF (q)," *Information and Control*, v. 16, 1970, pp. 396–401.