NASA TECHNICAL MEMORANDUM NASA TM-75204

POSSIBILITIES FOR IMPROVING THE EFFICIENCY OF LINEAR ERROR-CORRECTING CODES

R. R. Varshamov

(NASA-TM-75204) POSSIBILITIES FOR IMPROVING THE EFFICIENCY OF LINEAR ERROR-CORRECTING CODES (National Aeronautics and Space Administration) 9 p CSCL 09B N78-17746
Unclas
00/63 05470

Translation of "O vozmozhnostyakh uvelicheniya moshchnosti lineynykh korrektiruyshchikh kodov", Doklady Akademii Nauk SSR, vol. 223, No.1, 1975, pp. 60-63.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
WASHINGTON, D.C. 20546 NOVEMBER 1977

POSSIBILITIES FOR IMPROVING THE EFFICIENCY OF LINEAR ERROR-CORRECTING CODES

R. R. Varshamov
Computing Center of the Academy of Sciences of the Armenian SSR
and Yerivan State University

The elaboration of design methods for the construction of noiseproof coding systems with a maximal data transmission rate (or equivalently with maximum efficiency of code subsets) when the main parameters of the system are specified is one of the main tasks of algebraic coding theory. Here n is the length of a code block, t is the number of detected errors, and q is the base of the code. This note presents some results which are relevant to possibilities for constructing, within Hamming distance, noiseproof systems of signals in which the efficiency of code subsets exceeds many times the efficiency of all similar known linear codes described in the literature. /60*

The following theorem states our basic concept.

Theorem 1. Regardless of the magnitude of the number θ and method used to construct error-correcting codes correcting t symmetric errors, values of the parameters n and q can always be found (on the basis of this method) for which the following is true:

a) new classes of codes can be constructed in which the efficiency of code subsets is more than θ times greater than the efficiency of the corresponding codes that were constructed using the original method.

b) the error-correcting capacity of the old codes is preserved.

We will assume that a method for constructing coding systems correcting a fixed number t of errors is given if a completely defined method which allows the construction of such systems is specified for any arbitrary n and q.

---

* Numbers in margin indicate pagination in the foreign text

The physical interpretation of Theorem 1 will be discussed using Hamming and Bose-Choudhuri-Hocquenghem codes as examples.

1. Hamming Codes. It is well known [1] that Hamming codes represent the class of linear codes correcting single symmetric errors. Although these codes are optimal in the class of linear codes, they belong to a class of codes for which a construction method has been developed. Therefore, according to the statement of theorem 1, new classes of codes allowing an improvement in the efficiency of Hamming codes (even without limit) can be constructed.

Henceforth we will denote by $g(n,q)$ the efficiency of the optimal Hamming code of length n with base q. We will also use the notation $\varepsilon_q(n) = q^{[\log_q n]}$ where $[x]$ is the greatest integer not greater than x, and $\{x\} = x - [x]$.

The case $q = 3$[1]

Theorem 2. For any integers n, satisfying the inequalities

$$\log_3 {}^3/_2 < \{\log_3 n\} < 2\log_3 (3\sqrt{5}),$$

signal systems with base 3 correcting single symmetric errors exist in which the efficiency of code subsets $b(n,3)$ is strictly greater than the efficiency of the corresponding Hamming codes and satisfies the inequality

$$b(n, 3) > 3^{1-\{\log_3 5n\}} g(n, 3).$$

/61

This result can be stated in somewhat stronger form, namely as the following theorem,

Theorem 3. Values of the parameter n can always be found for which coding systems with base 3 correcting single errors can be constructed in which the efficiency of code subsets $b(n,3)$ satisfies the inequality

$$b(n, 3) > 3^{1-\{\log_3 (5n+\delta(n))\}} g(n, 3),$$

where $\delta(n) = 1$ or 2.

Thus, for example, the following theorem holds:

---

[1] Our method is inefficient in the case $q = 2$

Theorem 4. Let $m = p_1 \ldots p_\sigma$, p_s, $s = 1, \ldots, \sigma$, be primes of the form $8k + 5$ and g_s be a primitive root modulo p_s,

$$Q_s = p_1 \ldots p_s \ (Q_0 = 1), \quad m_s = Q_s^{-1} m, \quad M_s = \frac{m - m_s}{4},$$

$$p_s' = \frac{p_s - 1}{4}, \quad \{\log_3 m\} > \log_3 2.$$

Then for any integers α and n ($\varepsilon_3(m) < 2n < m/2$), the set of all possible solutions of the congruence

$$\sum_{s=1}^{\sigma} \sum_{v=0}^{m_s - 1} \sum_{u=1}^{p_s'} Q_{s-1}(g_s^{iu} + p_s v) x_{M_s + p_s' v + u} \equiv \alpha \pmod{m},$$

were x_u, u n[2], taking on arbitrarily the values 0, 1 and 2, is a code of length n with base 3, correcting single symmetric errors. Among these codes the efficiency of the optimal code is

$$b(n, 3) > 3^{1 - \{\log_3 m\}} g(n, 3), \quad \delta(n) = 1.$$

The following theorem is also valid.

Theorem 5. Let $m = p_1 \ldots p_\sigma$, where p_s are primes of the form $8k + 3$, $m > {}_3(2m)$ and $q = 3$.

Then for arbitrary integers α, β and n ($\varepsilon_3(2n) < 2n < m$), the set of all possible solutions of the system of congruences

$$\sum_{s=1}^{\sigma} \sum_{v=0}^{m_s - 1} \sum_{u=1}^{2p_s'} Q_{s-1}(g_s^{2u} + p_s v) x_{2M_s + 2p_s' v + u} \equiv \alpha \pmod{m},$$

$$\sum_{u=1}^{n} x_u \equiv \beta \pmod{2}.$$

where $x_u = 0, 1$ and 2 ($u \leq n$) and $x_u = 0$ ($u > n$), is a code of length n correcting single symmetric errors. Among these codes, the efficiency of the optimal code is

$$b(n, 3) > 3^{1 - \{\log_3 2m\}} g(n, 3), \quad \delta(n) = 2.$$

We will now consider the general case of arbitrary $q = p^\nu$[3]

---

2 $x_u = 0$ for all $u > n$

3 p is an odd prime

Theorem 6 ($\nu > 1$). For any integer values n, satisfying the inequalities

$$\log_q (q-1)^{-1} q \leqslant \{\log_q n\} \leqslant 1/\nu,$$

signal systems with base q correcting single symmetric errors exist in which the efficiency of code subsets b(n,q) satisfies the relation

$$b(n, q) = p^{\nu-1} g(n, q)$$

/62

Theorem 7 ($\nu = 1$). For any integer values n satisfying the inequalities

$$\log_p (p-1)^{-1} p \leqslant \{\log_p n\} \leqslant \log_p p/\omega(n), \quad 2 \leqslant \omega(n) < 4,$$

signal systems with base p exist in which the efficiency of code subsets b(n,p) satisfies the inequality

$$b(n, p) > p^{1-\{\log_p n\omega(n)\}} g(n, p)$$

This result can be stated in somewhat stronger form.

Theorem 8. Values of n exist such that codes with base p correcting single symmetric errors can be constructed in which the efficiency of code subsets satisfies the inequality

$$b(n, p) > p^{1-\{\log_p 2n\}} g(n, p).$$

2. Bose-Chandhuri-Hocquenghem (B. C. H.) codes. B. C. H. codes are a generalization of Hamming codes to the multi-error correcting case, and like Hamming codes, they belong to a class of codes for which a construction method exists. Therefore, according to our concept, new more efficient codes correcting multiple errors can be constructed on the basis of these codes.

Let us denote by $G_t(n,q)$ the efficiency of optimal B. C. H. codes of length n with base q correcting t symmetric errors.

The case q = 2, t = 2.

Theorem 9. For any integers n ($\{\log_2 n\} < \log_2(2/\sqrt{3})$) and $q = 2$, codes correcting binary symmetric errors can be constructed whose efficiency $B_2(n,2)$ is strictly greater than the efficiency of the corresponding B. C. H. codes and satisfies the inequality

$$B_2(n,2) > 4^{1-\{\log_2 n\sqrt{3}\}} G_2(n,2). \qquad (1)$$

Thus, for example, the following theorem holds.

Theorem 10. Let p be a prime of the form $6k-1$ satisfying the inequality $\{\log_2 p\} < \log_2(2/\sqrt{3})$.

Then for any integers α, β, γ_u and n ($\varepsilon_2(p) \leq n \leq p$), the set of all possible solutions of the system of congruences

$$\sum_{u=1}^{n} u x_u \equiv \alpha \pmod{p},$$

$$\sum_{u=1}^{n} u^2 x_u \equiv \beta \pmod{p},$$

$$\sum_{u=1}^{n} x_u \equiv \gamma \pmod{3},$$

where $x_u = 0$ or 1, is a code of length n with base 2 correcting two symmetric errors. Among these codes, the efficiency of the optimal codes is strictly greater than the efficiency of analogous B. C. H. codes, and it satisfies inequality 1.

The case $q = 3$, $t = 2$.

Theorem 11. Let n be any integer satisfying the inequality $\{\log_3 n\} < \log_3 3/2$ and g be a primitive element of the Galois field GF $(\varepsilon_3(3n))$.

Then the set of all possible solutions of the equations /63

$$\sum_{u=1}^{n} g^{-u} x_u = a, \quad \sum_{u=1}^{n} g^{u} x_u = b,$$

where $x_u \notin GF(3)$ and a, b $\notin GF(\varepsilon_3(3n))$, is a code of length n with base 3, correcting two symmetric errors, whose efficiency $B_2(n,3)$ is

$$B_2(n,3)=(\sqrt{3})^{1-(-1)^{[\log_3 n]}}G_2(n,3).$$

The case $q = 4$, $t = 2$.

Theorem 12. Suppose an arbitrary natural number $n > 5$ and a primitive element g of the Galois field $GF(\varepsilon_4(12n))$, are given.

Then the set of all possible solutions of the equations

$$\sum_{u=1}^{n} g^{-u}x_u=a, \quad \sum_{u=1}^{n} g^{u}x_u=b,$$

where $x_u \notin GF(4)$ and $a,b \in GF(\varepsilon_4(12n))$ is a code of length n with base 4 correcting two symmetric errors, whose efficiency strictly exceeds the efficiency of the analogous B. C. H. code and satisfies the relation

$$B_2(n,4)=4^{h(n)}G_2(n,4),$$

where $h(n) = [\log_4 n] - (-1)^{[4\varepsilon_4(n)/3n]}$.

However, on the basis of only the Bose-Chaudhuri-Hocquenghem results, one can also prove the following theorem.

Case of arbitrary p.

Theorem 13. For any arbitrary values $t \geq 2$, $p \geq 2t$ and n ($\{\log_p n\} < \log_p(p/\nu(n))$, $1 \leq \nu(n) < 2$), codes of length n with base p, correcting t symmetric errors can be constructed, whose efficiency $B_t(n,p)$ is strictly greater than the efficiency of the corresponding B. C. H. codes correcting the same number of errors, and whose efficiency satisfies the inequality

$$B_t(n,p)>(p^{1-\{\log_p \nu(n)n\}})^{2t-1}G_t(n,p).$$

Note that when n approaches infinity, the quantity $\nu(n)$ takes on the value 1 infinitely many times. Hence the following theorem holds.

Theorem 14. For fixed t and $p \geq 2t$, the inequality

$$B_t(n,p)>(p^{1-\{\log_p n\}})^{2t-1}G_t(n,p)$$

is satisfied infinitely many times as n approaches infinity.

REFERENCES

Peterson, W. Kody, ispravlyayushchiye oshibki (Error-correcting codes). Mir Press, Moscow, 1964.

STANDARD TITLE PAGE

1. Report No. NASA TM-75204	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle POSSIBILITIES FOR IMPROVING THE EFFICIENCY OF LINEAR ERROR-CORRECTING CODES		5. Report Date November 1977
		6. Performing Organization Code
7. Author(s) R. R. Varshamov		8. Performing Organization Report No.
		10. Work Unit No.
9. Performing Organization Name and Address Leo Kanner Associates Redwood City, California 94063		11. Contract or Grant No. NASw-2790
		13. Type of Report and Period Covered Translation
12. Sponsoring Agency Name and Address National Aeronautics and Space Administration, Washington, D.C. 20546		14. Sponsoring Agency Code

15. Supplementary Notes

Translation of "O vozmozhnostyakh uvelicheniya moshchnosti lineynykh korrektiruyushchikh kodov," Doklady Akademii Nauk SSR, vol. 223, No. 1, 1975, pp. 60-63.

16. Abstract

Results are presented in the form of 14 theorems specifying sufficient conditions under which it is possible to construct new more efficient single- and multi-error correcting codes from existing ones when the method used to construct existing codes is known.

17. Key Words (Selected by Author(s))	18. Distribution Statement This copyrighted Soviet work is reproduced and sold by NTIS under license from VAAP, the Soviet copyright agency. No further copying is permitted without permission from VAAP.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	9	