# Non-primitive Hamming Codes

**Valery Lipnitski**
The Military Academy of the Republic of Belarus, Independence Avenue 220., Minsk, Belarus, 220057, valipnitski@yandex.ru

***Abstract:*** *The basic parameters of the non-primitive Hamming codes are investigated. It is shown that many of them have a minimum distance exceeding the constructive. Thus dimension and speed of these codes can have quite comprehensible values. The method for correction of the multiple non-primitive Hamming codes is developed. The simplicity and efficiency of this method realization make sure that a class of linear codes can found its actual application in new telecommunication systems.*

***Keywords:*** Linear code, Hamming code, BCH-code, minimal length, telecommunication system, parity-check matrix, Galois field, corrective opportunities.

## 1. THE CORRELATION OF PRIMITIVE AND NON-PRIMITIVE HAMMING CODES

The Hamming codes play more historical than practical role in noise-resistance coding. Indeed, there are the first codes [1] which have appeared almost simultaneously with the revolutionary Shannon K. ideas in the information theory [2]. The Hamming codes were an evident illustration to the Shannon K. theoretical principles on the error correction capabilities of any complexity in the information transfer in channels with noise, if the information previously skillfully adds redundant. Disappointingly feeble ability to adjust just single error in each transmittable word-message awoke creative thought of researchers to develop new codes. And more than 10-years incubation period was replaced in the 60s of XX century by explosion of the new ideas, new codes and new methods in the theory and practice of noise-resistant coding [3]. And the perfect Hamming code has graced pages of the first monographs and textbooks in the new direction of the applied mathematics.

In the «Bible of encoders» terms [3] the hamming code belongs to the primitive codes of Bose-Choudhori-Hokvingema (BCH codes) class, as a kind of minimal complex representative of this codes family. The specific Hamming code $C_x$ over a Galois Field, as a rule, characteristic 2, i.e. over $GF(2^m)$, m>1, has length $n=2^m-1$, and sets the parity-check matrix $H_x^n=(1\,\alpha\ldots\alpha^{n-1})$ where a – a primitive element of the field $GF(2^m)$, the root of some irreducible primitive polynomial $p(x)$ of the level $m$ over $Z/2Z$. Each element $\alpha^i$ of the matrix $H_x^n$ is actually a binary column of the coordinates $\alpha^i$ in basis $\alpha^{m-1},\alpha^{m-2},\ldots,\alpha,1, 0\le i\le 2^m-2$.

The code $C_x^n$ with given parity-check matrix certainly has minimum distance 3, and can actually correct only vectors of errors that weight is equal 1.

By definition [3] the arbitrary BCH-code $C_t$ is set by parity-check matrix

$$H_{C_t}=(\beta^i,\beta^{3i},\ldots,\beta^{(2t-1)i})^T,\ 0\le i\le n-1,$$

where $\beta=\alpha^\mu$, $\mu=1$ or $\mu$ is the divisor of the number $2^m-1$. Thus, the presence of the binary BCH-codes of any virtually odd length is tolerance. If $\mu>1$, the BCH-code is no longer primitive. Accordingly it is also possible to consider the non-primitive, and the Hamming codes of length $\nu=(2^m-1)/\mu$ with parity-check matrix of $H_x^\nu=(1,\beta,\ldots,\beta^{\nu-1})$ for $\beta=\alpha^\mu$.

The only general fact, known about the non-primitive Hamming codes, said that their minimum distance potentially can be more than 3. And what happened? The setting resource of these codes is too insignificant, the task of on-syndromic chasing for each regular vector-error not looks too optimistically. However, there is a reason for optimism.

## 2. THE EXISTENCE OF THE NON-PRIMITIVE HAMMING CODES

According to Euler's theorem for each odd $n>1$ $2^{\varphi(n)}\equiv 1(\mathrm{mod}\,n)$. Thus $\varphi(n)\le n-1$ and $\varphi(n)=n-1$ only in the case of simple values $n$. Perhaps there is an integer $\mu$ that is smaller than $\varphi(n)$ and such that $2^\mu\equiv 1(\mathrm{mod}\,n)$. The minimum value $m$ of these $\mu$ is called the exponent of two modulo $n$. Method by contradiction shows that $m$ is the factor $\varphi(n)$.

Comparison of $2^\mu\equiv 1(\mathrm{mod}\,n)$ means that $2^m-1$ divided on $n$. According to [3], the field $GF(2^m)$ in that case is the field of the BCH-code $C_t$ definition provided that $tm<n$. This field sets the matrix $H_{C_t}$.

By construction, if $t=1$ the inequality of $m<n$ is fulfilled automatically. It follows from this

**Theorem 1.** For each natural integer $n>1$ there is the (non-primitive) Hamming code of the length $n$.

Proof. As we have noted for the given $n$ the index of twain $m\le\varphi(n)\le n-1<n$ and value $2^m-1$ are divided into $n$ or $2^m-1=n$.

Let $2^m-1=n\cdot s$ for some integer $s>1$. Then the matrix $H_x^\nu=(1,\beta,\ldots,\beta^{n-1})$, for the primitive element $\alpha$ of the field $GF(2^m)$ and $\beta=\alpha^s$ has size $m\times n,\ m<n$. It can be considered as the check matrix of the some binary linear code. In terms of [3] this is the BCH-code $C_t$ with $t=1$, i.e the (non-primitive) Hamming code that length is equal $n$

## 3. THE MINIMUM DISTANCE OF THE NON-PRIMITIVE HAMMING CODES.

**Theorem 2.** The minimum distance $d$ of the non-primitive Hamming code of the length $n$ is in the range $3\le d\le\min(p,m)$, where $p$ is the smallest prime divisor

of the length $n$.

**Proof.** Let the code $C_x^n$ is defined over the field $GF(2^m)$. If $2^m - 1 = n$, than the code $C_x^n$ is primitive. According to the universal theorem [3] the minimum distance of the linear code is equal $d$ if and only if, when any $d-1$ columns are linearly independent in the parity-check matrix $H$, but there are $d$ linearly dependent columns. Any two columns are different in the matrix of primitive Hamming code, but there are always three linearly dependent columns.

The non-primitive Hamming code can be obtained from the primitive by decimation or ejection of sufficiently large number of columns of the primitive code matrix. Not surprisingly, the minimal distance can increase at the same time.

Let $p$ is a divisor of the odd number $n$. Then $p \geq 3,\ n = p \cdot \sigma$. Vector $\bar{c}$ with nonzero coordinates at the positions numbered $1, \sigma+1, \ldots, (p-1)^{\sigma+1}$ is a code word. This means that $H \cdot \bar{c}^T = \bar{0}$.

Indeed $H\bar{c}^T = 1 + \beta^\sigma + \beta^{2\sigma} + \ldots + \beta^{(p-1)\sigma} = \frac{(1+\beta^\sigma+\beta^{2\sigma}+\ldots+\beta^{(p-1)\sigma})(1+\beta^\sigma)}{(1+\beta^\sigma)} = \frac{1+\beta^{p\sigma}}{1+\beta^\sigma} = 0$ as $\beta^{p\sigma} = \alpha^{sp\sigma} = \alpha^{sn} = \alpha^{2^m-1} = 1$.

We found $p$ columns of matrix $H_x^n$ that binary sum, i.e. linear combination is equal 0. This means $d \leq p$.

**Corollary.** If the length of the Hamming code divided into 3 than $d = 3$.

Corollary means that third part of the non-primitive Hamming codes has modest traditional decoding capabilities, i.e. corrects only one error. There are the codes of length $n = 3 + 6k,\ k \geq 1$.

According to the theorem 2 the greatest minimal distance and the greatest correction possibilities should be expected the non-primitive Hamming code of prime length $n = p$. Here you can specify a class of the codes with maximum possible minimum distance $d = n = p$. There are codes with $m = \varphi(n) = \varphi(p) = p - 1$. Their parity check matrix has size $(p-1) \times p$. These codes have dimension $k = 1$ and contain only two code words $\bar{c}_1 = \bar{0}$ and $\bar{c}_2 = (11\ldots1)$. If the distance is peak they cannot transfer any information. Interest in them is no more than theoretical. There are 10 such codes of the length 11, 13, 19, 29, 37, 53, 59, 61, 67, 83 in the range of length from 9 to 99.

Nevertheless the codes of $d > 3$ and $k > 1$ and even with information transfer speed $\nu = \frac{k}{m} > \frac{1}{2}$ exist. The perfect Golay code, that has $n = 23,\ m = 11,\ k = 12,\ d = 7$ and $\nu = \frac{11}{23} > \frac{1}{2}$ and correct errors of the weight 1-3, belong to the non-primitive Hamming code class. Search of such codes involves significant computing. Even the simple check of theorem 2 (look above) requires the calculation of $m$, the construction of the Galois field $GF(2^m)$, forming the parity check matrix $H_x^n$, and finally solving a combinatorial problem with the columns of the matrix.

In this way we found a lot of codes with $d > 3n$, and even with $d > 7$. For example, the Hamming codes of length $n = 47,\ n = 71$ have a minimum distance 11, can correct all of the random errors of the weight from 1 to 5 inclusive, and the rate of both is greater than 0.5.

This is

$$C_{71}^1 + C_{71}^2 + C_{71}^3 + C_{71}^4 + C_{71}^5 = 71 \cdot 197905$$

error vectors for the code $C_x^{71}$ that is 197905 times more the number of single errors, correction of which is guaranteed a priori.

## 4. THE NON-PRIMITIVE HAMMING CODES DECODING METHOD OF ORBITS.

Through the efforts of the Belarus coding school there was developed the theory of syndrome norms [4, 5]. Applying the automorphisms of codes, it introduces the new parameter - the syndrome norm. The syndrome norm $\overline{N}(S(\bar{e}))$ of the error vector $\bar{e}$, that is calculated from the coordinates of the syndrome $S(\bar{e})$, determines the orbit $J$, $\bar{e}$ belongs to $J$. Each orbit is well-structured. We find an error much simpler there than in the whole array of corrected errors. The theory of syndrome norms is effective for the BCH-codes $C_t$ where $t > 1$. It is not applicable for the Hamming codes because the matrix $H_x^n$ is weak structured. However, the weaker analogue of this theory for the Hamming codes can be constructed.

Obviously, the Hamming code $C_x^n$ with parity-check matrix $H_x^n = (1, \beta, \ldots, \beta^{n-1})$ is cyclic. This means that the operator $\sigma(\bar{e}) = \sigma(e_1, \ldots, e_n) = (e_n, e_1, \ldots, e_{n-1})$ belongs to the group of code automorphisms $C_x^n$, generates a cyclic subgroup $\Gamma = \{\sigma, \sigma^2, \ldots, \sigma^n = e\}$ in this group. This group divides all error vectors into the orbits. Typically, the orbits contain $n$ error vectors and have next structure: $<\bar{e}> = \{\bar{e}, \sigma(\bar{e}), \ldots, \sigma^{n-1}(\bar{e})\}$. The syndrome of each error vector $\bar{e}$ is $S(\bar{e}) = H_x^n(\bar{e})^T$ - the element of Galois field $GF(2^m)$.

**Theorem 3**. $S(\sigma(\bar{e})) = \beta S(\bar{e})$.

Theorem 3 implies the orbit method of error correction by the Hamming codes. It should be remembered that the minimum distance $d = 2t+1$ or $d = 2t+2$ guarantees the paired difference of all error syndromes of weight $1, 2, \ldots, t$. We will divide error set $K$ that is corrected by the code into orbits. In each orbit $J$ we fix generatrix $\overline{e_J}$ and its syndrome $S(\overline{e_J}) = \alpha^{Z_J}$. In storage there is a list of all orbits of set ΓK, their generatrix $\overline{e_J}$ and syndromes $S(\overline{e_J})$.

Let the telecommunications System (TCS) functions

on the basis of the Hamming code $C_x^n$ . Let the next message $\bar{x}$ is received, its syndrome is $S(\bar{x}) \neq \bar{0}$. Therefore $\bar{x} = \bar{e} + \overline{e_J}$ . We select orbits $J$ from the list ГК for finding error vector $\bar{e}$ in message $\bar{x}$ and calculate $\nu = \deg S(\bar{x}) - \deg S(\overline{e_J}) / S$ , where $s$ is taken from $\beta = \alpha^S$ . There is the one orbit $J^* \in$ ГК, for which $\nu$ is integer. When we find it it will be the end of the algorithm, we will find the error vector $\bar{e} = \sigma^{\nu}(\overline{e_J})$

**5. CONCLUSION.**

The practice of noise-resistant coding shows that it is required multiple errors correction in the real communication channels on codes of the real length. The primitive Hamming codes, that are capable to correct single errors, had played its historical role, it became beautiful object of all textbooks. However, the non-primitive Hamming codes in many cases have a fairly large minimum distance, the effective error correction method has been developed for them that named the orbit method. The relative simplicity of decoding algorithms allows the use of the non-primitive Hamming codes in the modern real-TCS.

**6. REFERENCES**


[1] Hamming, R.W. Coding and Information Theory / R.W. Hamming // Prentice Hall. – 1986 – 2 Sub edition. – 272 p.

[2] Shannon, C.E. A mathematical theory of communication. Pt. I, II /C.E. Shannon // Bell. Syst. Tech. – 1948. – Vol. 27. – P.379-423; P.623-656.

[3] MacWilliams, F. J. The Theory of Error-Correcting Codes/ F. J. MacWilliams, N. J. A. Sloane.// North-Holland Mathematical Library. – 1977(11th reprint, 2003). –Vol. 16. – 762 p.

[4] Lipnitski, V.A. Norms decoding error controlled code and the algebraic equations / V.A. Lipnitski, V.K. Konopelko. – Minsk: BGU, 2007 (in Russian)

[5] Konopelko, V.K. The theory of syndrome norms and permutation decoding of error controlled code / V.K. Konopelko, V.A. Lipnitski // Editorial URSS. –2004. – 2 edition. – 176 p. (in Russian)