Des. Codes Cryptogr. (2008) 49:265–271
DOI 10.1007/s10623-008-9193-7

A family of ternary quasi-perfect BCH codes

Danyo Danev · Stefan Dodunekov

Received: 31 May 2007 / Revised: 14 December 2007 / Accepted: 19 December 2007 /
Published online: 21 March 2008

Abstract In this paper we present a family of ternary quasi-perfect BCH codes. These codes are of minimum distance 5 and covering radius 3. The first member of this family is the ternary quadratic-residue code of length 13.

Keywords Quasi-perfect codes · Packing radius · Covering radius · Algebraic decoding

AMS Classifications 94B15 · 94B35 · 11T71

1 Introduction

We start with several definitions which are traditional in the field of coding theory. The Galois field of q elements, where q is a prime power, is denoted by $GF(q)$. The Hamming space of all n-tuples of elements from $GF(q)$ will be denoted by $H(n, q)$. The elements of $H(n, q)$ will be referred to as words or vectors. The Hamming space can be considered as a metric space together with the metric function $d(\mathbf{x}, \mathbf{y})$, which is equal to the number of positions where $\mathbf{x}$ and $\mathbf{y}$ differ, known as Hamming distance. By sphere and ball of radius r around a vector $\mathbf{x}$ we understand the set of all vectors at Hamming distance exactly and at most r from $\mathbf{x}$, respectively. An arbitrary subset C of $H(n, q)$ is called q-ary error-correcting code, or simply a code. The parameter n is known as the length of the code. Clearly, $H(n, q)$ is a vector space over the field $GF(q)$ with addition and multiplication by scalar performed component-wise as in $GF(q)$. Any linear subspace of $H(n, q)$ is referred to as a linear code.

D. Danev (✉)
Department of Electrical Engineering, Linköping University, 581 83 Linkoping, Sweden
e-mail: danyo@isy.liu.se

S. Dodunekov
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
8 G. Bontchev Street, 1113 Sofia, Bulgaria
e-mail: stedo@moi.math.bas.bg

The minimum distance for a code C is defined by

$$d(C) \stackrel{\triangle}{=} \min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C,\ \mathbf{x} \neq \mathbf{y}\}.$$

We use the notation $(n, M, d)_q$ for a general code of length n, cardinality M and minimum distance $d(C) = d$. If the code is linear and its dimension as a subspace is k we denote it by $[n, k, d]_q$.

The minimum distance is an important parameter which defines the error-correcting properties of the code when it is used for communication over i.a. additive-white-Gaussian-noise (AWGN) communication channels. It is easy to see that up to

$$t(C) = \left\lfloor \frac{d(C) - 1}{2} \right\rfloor$$

errors can be successfully corrected and this quantity is known as the packing radius of the code C. This represents the largest possible integer number such that the spheres of this radius around the codewords are disjoint. In a similar manner the covering radius of a code C is defined as the least possible integer number such that the balls of this radius around the codewords cover the whole space $H(n, q)$. Formally we write

$$\rho(C) \stackrel{\triangle}{=} \max_{\mathbf{x} \in H(n,q)} \min_{\mathbf{c} \in C} d(\mathbf{x}, \mathbf{c}).$$

Obviously, the covering radius is at least as big as the packing radius. Codes that achieve this equality, i.e. $t(C) = \rho(C)$, are called perfect. The parameters for which perfect codes over Galois fields exist have been completely classified [11–13]. The possible cases for the parameters $(n, M, d)_q$ are

- $(n, q^n, 1)_q$—the whole space $H(n, q)$, where n is a positive integer and q is a prime power;
- $(2l - 1, 2, 2l - 1)_2$—the binary repetition codes, where l is a positive integer;
- $((q^s - 1)/(q - 1), q^{(q^s-1)/(q-1)-s-1}, 3)_q$—the Hamming codes, where s is a positive integer and q is a prime power;
- $(23, 4096, 7)_2$—the binary Golay code;
- $(11, 729, 5)_3$—the ternary Golay code.

The next interesting case is when the covering radius exceeds the packing radius by one, i.e. $\rho(C) = t(C) + 1$. Codes that satisfy this condition are known as quasi-perfect. Classification of the putative sets of parameters for quasi-perfect codes seems to be much more complicated than that for the perfect case. In a recently published paper by Etzion and Mounits [6] a survey of the known results for the binary case is given. It appears that there is a great variety of quasi-perfect codes of minimum distances up to 5. However, only two non-trivial examples of binary quasi-perfect codes of minimum distance greater than 5 are known and they are connected to the binary Golay code.

Considerably less is known for q-ary quasi-perfect codes with $q > 2$. One infinite family of ternary codes is known due to Gashkov and Sidel'nikov [7]. The family members are $[(3^s+1)/2, (3^s+1)/2-2s, 5]_3$-codes with covering radius 3. Similarly, two families of quaternary codes with the parameters $[(4^s-1)/3, (4^s-1)/3-2s, 5]_4$ and $[(2^{2s+1}+1)/3, (2^{2s+1}+1)/3 - 2s - 1, 5]_4$ have been presented by Gevorkjan et al. [8] and Dumer and Zinoviev [5], respectively. The parameter s above is an integer number greater than 1. The quasi-perfectness, i.e. the fact that the covering radius is 3, of these codes have been shown by one of the authors in [3,4]. In this paper we show that there exist $[(3^s-1)/2, (3^s-1)/2-2s, 5]_3$ quasi-perfect codes for all odd $s \geq 3$. The first member of the family is the $[13, 7, 5]_3$ quadratic-residue code [1].

In Sect. 2 we define the codes and determine their minimum distance while in Sect. 3 we prove that their covering radius is equal to 3. Finally in Sect. 4 we suggest possible decoding algorithms for the presented codes.

2 Definition of the codes

Recall that a code is called cyclic if every cyclic shift of a codeword is also a codeword. Linear cyclic codes can be identified by ideals in the polynomial ring $GF(q)[x]/(x^n - 1)$. Thus every q-ary linear cyclic code is defined by its generator polynomial $g(x) \in GF(q)[x]$ which is a divisor of $x^n - 1$.

Let us define α as a primitive $\sqrt[n]{1}$, where $n = (3^s - 1)/2$, in an extension field of $GF(3)$. The element α can be found in the field $GF(3^s)$. If β is a primitive element of $GF(3^s)$, then $\alpha = \beta^2$. The minimal polynomials of α and α^{-1} with respect to $GF(3)$ are

$$g_1(x) = (x - \alpha)(x - \alpha^3) \dots (x - \alpha^{3^{s-1}})$$

and

$$g_{-1}(x) = (x - \alpha^{-1})(x - \alpha^{-3}) \dots (x - \alpha^{-3^{s-1}}),$$

respectively. For every positive integer s let us define the code C_s to be the cyclic ternary code of length $n = (3^s - 1)/2$ with generator polynomial $g(x) = g_1(x)g_{-1}(x)$. Obviously the dimension of C_s is

$$k = n - 2s = \frac{3^s - 1}{2} - 2s.$$

To determine the minimum distance we use the BCH bound for the minimum distance of a cyclic code.

Proposition 1 *The cyclic codes C_s defined above have minimum distance $d(C_s) \geq 5$, when s is odd and $d(C_s) = 2$, when s is even.*

Proof We start with the case when s is odd. In this case we have $\gcd(2, n) = 1$. If we set $\gamma = \alpha^2$ we observe that the set

$$\left\{\gamma^{(n-3)/2}, \gamma^{(n-1)/2}, \gamma^{(n+1)/2}, \gamma^{(n+3)/2}\right\} = \left\{\alpha^{-3}, \alpha^{-1}, \alpha, \alpha^3\right\}$$

is a subset of roots of the generator polynomial of C_s. Thus by the BCH bound (see for example [10] Cor. 9, p. 202) the minimum distance is at least 5.

When s is even we have codes of even length and can easily check that the vector corresponding to the polynomial $c(x) = 1 + x^{n/2}$ is a codeword in C_s of weight 2, thus $d(C_s) \leq 2$. Clearly the minimum distance can not be strictly less than 2. □

We shall see at the end of the next section that for odd $s \geq 3$ the minimum distance $d(C_s)$ is actually exactly 5.

3 The covering radius

Here we show that the covering radius of the defined codes is always 3 whenever the parameter s is odd. We assume that s is odd throughout this section. Let $\mathbf{r} = (r_0, r_1, \dots, r_{n-1})$ be an arbitrary vector in $H(n, 3)$. Let us identify $\mathbf{r}$ with the polynomial

$$r(x) = \sum_{i=0}^{n-1} r_i x^i \in GF(3)[x].$$

We have to show that for arbitrary polynomial $r(x)$ of degree at most $n - 1$, there always exist polynomials $c(x)$ and $e(x)$, corresponding to vectors $\mathbf{c}$ and $\mathbf{e}$ from $H(n, 3)$, such that $r(x) = c(x) + e(x),\ c(x) \in C$ and $wt_H(e(x)) \leq 3$. Define, as usual, the syndromes

$$S_i(r) = r(\alpha^i) \in GF(3^s),$$

for $i \in \{\pm 1\}$. Since $c(x)$ is a codeword and $\alpha^{\pm 1}$ are roots of the generator polynomial $g(x)$, we can define

$$S_i = S_i(r) = r(\alpha^i) = e(\alpha^i) = S_i(e) \in GF(3^s),$$

for $i \in \{\pm 1\}$. Every vector $\mathbf{r} \in H((3^s - 1)/2, 3)$ corresponds to a pair of syndromes $(S_1, S_{-1}) \in (GF(3^s))^2$. Thus we have to show that for an arbitrary pair of elements (a, b) from $GF(3^s)$ there exists a polynomial $e(x)$ with at most 3 non-zero coefficients from $GF(3^s)$, such that

$$(S_1, S_{-1}) = (S_1(e), S_{-1}(e)) = (a, b). \tag{1}$$

Due to the special choice of the code-length we can identify the vectors of Hamming weight one in $H((3^s-1)/2, 3)$ with the non-zero elements of $GF(3^s)$. The following Lemma clarifies this identification.

Lemma 1 *For every non-zero element β^i of $GF(3^s)$ there exists an unique monomial $m(x) \in GF(3)[x]$ of degree at most $(3^s - 3)/2$, such that $m(\alpha) = \beta^i$, where $\alpha = \beta^2$.*

Proof It is sufficient to show the existence since both the number of monomials in $GF(3)[x]$ of degree at most $(3^s - 3)/2$ and the non-zero elements in $GF(3^s)$ is equal to $3^s - 1$. If i is even, i.e. $i = 2k$ for some $k \in \{0, 1, \ldots, (3^s - 3)/2\}$, then for $m(x) = x^k$ we have $m(\alpha) = \alpha^k = \beta^{2k} = \beta^i$ and $\deg m(x) \leq (3^s - 3)/2$. If i is odd, i.e. $i = 2k + 1$ for some $k \in \{0, 1, \ldots, (3^s-3)/2\}$, then the monomial $m(x) = -x^{k+(3^s+1)/4}$, for $0 \leq k \leq (3^s-7)/4$ and $m(x) = -x^{k-(3^s-3)/4}$, for $(3^s - 3)/4 \leq k \leq (3^s - 3)/2$ satisfies the conditions since $\beta^{(3^s-1)/2} = -1$ and $3^s \equiv 3 \pmod 4$ when s is odd. □

Every monomial $m(x)$ in $GF(3)[x]$ has the property that $m(x)m(x^{-1}) = 1$. If we represent the polynomial $e(x) \in GF(3)[x]$ of Hamming weight l, as a sum of monomials in the following way

$$e(x) = \sum_{i=1}^{l} e_i x^{p_i} = \sum_{i=1}^{l} e_i(x),$$

then we have

$$e(x^{-1}) = \sum_{i=1}^{l} (e_i(x))^{-1}.$$

In the light of Lemma 1 and the last observation, the search for a polynomial $e(x)$ that satisfies Eq. 1 is equivalent to solving the system of equations

$$\left| \begin{array}{lllll} z_1 & + z_2 & + \cdots + z_l & = a \\ z_1^{-1} & + z_2^{-1} & + \cdots + z_l^{-1} & = b \end{array} \right. \tag{2}$$

over the field $GF(3^s)$. According to Proposition 1 the system (2) has at most one solution (up to permutation) for $l = 1$ and $l = 2$. In the case $l = 1$ we have a solution if and only if $ab = 1$.

Let us arbitrarily fix the pair $(a, b) \in (GF(3^s))^2$, such that $(a, b) \neq (0, 0)$ and $ab \neq 1$. We shall provide a solution to the system (2) in the case $l = 3$. Define the functions $\mu(x) = a^2b^2x^2 + ax^4 + b$ and $\nu(x) = a^2b^2x^2 - ax^4 - b$ on the field $GF(3^s)$. For arbitrary $y \in (GF(3^s))^*$ we can easily check that

$$\mu(y - y^{-1}ab^2) + \nu(y + y^{-1}ab^2) = 0. \tag{3}$$

The element $-1 \in GF(3^s)$ is not a perfect square when s is odd since $\beta^{(3^s-1)/2} = -1$ and $(3^s - 1)/2$ is odd. Thus by Eq. 3 either $\mu(y - y^{-1}ab^2)$ or $\nu(y + y^{-1}ab^2)$ is a perfect square. Any of the equations $y - y^{-1}ab^2 = x$ and $y + y^{-1}ab^2 = x$ has at most two different solutions in y. Thus either $\mu(x)$ or $\nu(x)$ is a perfect square for at least $(3^s + 1)/4$ different x's.

In the case when $\mu(x)$ is a perfect square the following triple

$$(z_1, z_2, z_3) = \left(\frac{1 - ax^2}{b - x^2}, \frac{x(1 - ab) + \sqrt{\mu(x)}}{x(b - x^2)}, \frac{x(1 - ab) - \sqrt{\mu(x)}}{x(b - x^2)}\right),$$

is a solution to (2) with $l = 3$, whenever $x^2 \notin \{0, a^{-1}, b\}$. In the case when $\nu(x)$ is a perfect square the triple

$$(z_1, z_2, z_3) = \left(\frac{1 + ax^2}{b + x^2}, \frac{x(1 - ab) + \sqrt{\nu(x)}}{x(b + x^2)}, \frac{x(1 - ab) - \sqrt{\nu(x)}}{x(b + x^2)}\right),$$

is a solution to (2) with $l = 3$, whenever $x^2 \notin \{0, -a^{-1}, -b\}$. In both cases the number of "unsuitable" choices of x is at most 5. This means that there always exists x such that one of the suggested triples above provides a solution to the system (2) since $(3^s + 1)/4 > 5$ for $s \geq 3$.

It is well known that vectors with the same syndrome belong to the same coset defined by a code. Due to the fact that $d(C_s) \geq 5$, for fixed a and b such that $ab \neq 1$, it is not possible to have two different solutions of the system (2) with $l = 2$. We have shown that in the coset corresponding to the syndrome (a, b) for which $ab \neq 1$, there are at least $(3^s + 1)/4 - 5$ vectors of Hamming weight at most 3. Since $3[(3^s + 1)/4 - 5] - 1 > n = (3^s - 1)/2$ for all $s \geq 4$, we have two vectors of weight at most 3 in the coset which have a non-zero element in the same position. This means that we have a codeword in C_s of weight at most 5. The existence of a codeword of Hamming weight 5 in the case $s = 3$ can be checked directly [1].

The results above can be summarized in the following statement.

Theorem 1 *The ternary cyclic codes C_s defined in Sect. 2 have covering radius $\rho(C_s) = 3$ when $s \geq 3$ is odd. Moreover, the minimum distance of the codes is $d(C_s) = 5$.*

Direct consequence of this theorem is the following.

Corollary 1 *The codes C_s, defined in Sect. 2, are quasi-perfect for all positive odd integers $s \geq 3$.*

In [10] after showing that the double-error-correcting binary primitive BCH codes are quasi-perfect [9], the authors conjectured as a research problem (9.4) on pp. 280, that there are no other BCH codes which are quasi-perfect. Clearly, Corollary 1 provides an infinite family of counter-examples to that conjecture.

4 Decoding of the codes

It was mentioned in Sect. 2 that the codes C_s can be considered as BCH codes and thus any standard BCH decoder for double error correction can be applied in the case of odd s (see for example [2] Ch. 7).

A special syndrome-decoding algorithm can be designed based on the observations in Sect. 3. Short description of this algorithm follows.

Step 1. Calculate S_1 and S_{-1} as in (1).
Step 2. If $S_1 = S_{-1} = 0$, no errors. Otherwise go to Step 3.
Step 3. If $S_1 S_{-1} = 1$, one error. Calculate the error monomial $e(x)$ as in the proof of Lemma 1 for $a = S_1$. Otherwise go to Step 4.
Step 4. If $S_1 S_{-1}(S_1 S_{-1} - 1)$ is a non-zero perfect square in $GF(3^s)$, two errors. Determine the roots of the quadratic equation $S_{-1} y^2 - S_1 S_{-1} y + S_1 = 0$ and the error monomials $e_1(x)$ and $e_2(x)$ as in the proof of Lemma 1 for these roots. The error polynomial is $e(x) = e_1(x) + e_2(x)$.
Otherwise three errors.

Advantage of the suggested algorithm is that the error vector is obtained by simple calculations of the syndromes and possibly solution of a quadratic equation.

5 Conclusions

A family of ternary BCH codes previously unknown to be quasi-perfect has been presented. This is only the fourth infinite sequence of parameters for which non-binary quasi-perfect codes are known to exist. Unfortunately the construction works only for odd values of the parameter s. For the even case a new approach is needed. A challenging open question is the existence of quasi-perfect $[(3^s - 1)/2, (3^s - 1)/2 - 2s, 5]_3$ codes for even values of s. Some steps towards a solution of this problem has already been taken and hopefully we will be able to present a result in a near future.

Acknowledgments The authors would like to thank the anonymous reviewers for their valuable comments and suggestions. This work has been partially supported by the Swedish Research Council under grant 621-2002-4425 and the Bulgarian NSF under contract MM 1405.

References

1. Baicheva Ts., Dodunekov S.M., Kötter R.: On the performance of the ternary [13,7,5] quadratic-residue code. IEEE Trans. Inform. Theory **48**(2), 562–564 (2002).
2. Blahut R.E.: The Theory and Practice of Error Control Codes. Addison-Wesley, Reading, MA, USA (1993).
3. Dodunekov S.M.: The optimal double-error correcting codes of Zetterberg and Dumer-Zinov′ev are quasiperfect. C. R. Acad. Bulgare Sci. **38**(9), 1121–1123 (1985).
4. Dodunekov S.M.: Some quasiperfect double error correcting codes. Prob. Control Inform. Theory/Problemy Upravlen. Teor. Inform. **15**(5), 367–375 (1986).
5. Dumer I.I., Zinoviev V.A.: Some new maximal codes over GF(4). Problemy Peredachi Informatsii **14**(3), 24–34 (1978).
6. Etzion T., Mounits B.: Quasi-perfect codes with small distance. IEEE Trans. Inform. Theory **51**(11), 3928–3946 (2005).

7. Gashkov I.B., Sidel′nikov V.M.: Linear ternary quasiperfect codes that correct double errors. Problemy Peredachi Informatsii **22**(4), 43–48 (1986).
8. Gevorkjan D.N., Avetisjan A.M., Tigranjan G.A.: K voprosu o postroenii kodov s ispravleniem dvuh oshibok v metrike hemminga nad poljami galua. Vichislitel'naja tehnika **3**, 19–21 (1975).
9. Gorenstein D.C., Peterson W.W., Zeirler N.: Two-error correcting Bose-Chaudhuri codes are quasi-perfect. Info. Control **3**, 291–294 (1960).
10. MacWilliams F.J., Sloane N.J.A.: The Theory of Error Correcting Codes. Amsterdam, North-Holland, sixth printing (1988).
11. Tietäväinen A.: On the nonexistence of perfect codes over finite fields. SIAM J. Appl. Math. **24**, 88–96 (1973).
12. Tietäväinen A.: A short proof for the nonexistence of unknown perfect codes over GF(q), $q > 2$. Ann. Acad. Sci. Fenn. Ser. A I **580**, 6 (1974).
13. Zinoviev V.A., Leontiev V.K.: On non-existence of perfect codes over Galois fields. Prob. Control Inform. Theory/Problemy Upravlenija i Teorii Informacii **2**(2), 123–132 (1973).