Non Binary Codes and “Mathematica” Calculations: Reed-Solomon Codes Over GF (2n)

Conference Paper · May 2005

DOI: 10.1007/11428862_90 · Source: DBLP

Igor Gashkov
Karlstads Universitet

Non Binary Codes and “Mathematica” Calculations: Reed-Solomon Codes Over GF (2^n)*

Igor Gashkov

Karlstad University, Department of Engineering Sciences, Physics and Mathematics 65188
Karlstad Sweden
Igor.Gachkov@kau.se

Abstract. The effect of changing the basis for representation of Reed-Solomon codes in the binary form may change the weight distribution and even the minimum weight of codes. Using “Mathematica” and package “Coding Theory” we give some examples of effective changing of basis which gives the binary code with greatest minimum distance [1] (Ch.10. §5. p 300) and codes which have the same distance independently of basis changing.

1 Reed-Solomon Code

A Reed-Solomon (RS) code over the Galois Field GF(q) is a special BCH - code having the length of the code words equal to the number of nonzero elements in the ground field. The RS - codes are cyclic and have as generator polynomial

$$g(x) = (x - a^{b})(x - a^{b+1})...(x - a^{d-1}) \tag{1}$$

where a is a primitive element of the field GF(q) and d is the code distance.
The elements of GF(q) can be represented as m-vector of elements from GF(p). Choosing p = 2 we get the binary codes by substituting for each symbol in GF(2^m) the corresponding binary m - vector. We will use the package” Coding Theory” [2], [5].

```
In[1]:=<<CodingTheory.m;BIP=BinaryIrrPolynomials[3,x]
```

Out[1] = $\{1+x^2+x^3, 1+x+x^3\}$

```
In[2]:=r=BIP[[2]];ShowBinaryGaloisField[r, x, a, a]
```

GF(8) is received by extending the field Z_2 by the irreducible polynomial $r(x) = 1 + x + x^3$ and observe that a is a primitive element in this extension field.

Out[2] =

Log	Vector	Polynomial		Min. polynomial
0	(1, 0, 0)	1	1	$1+x$
1	(0, 1, 0)	a	a	$1+x+x^3$
…		…		…
6	(1, 0, 1)	a^6	$1+a^2$	$1+x^2+x^3$

* The research was support by The Royal Swedish academy of Sciences

V.S. Sunderam et al. (Eds.): ICCS 2005, LNCS 3516, pp. 663 – 666, 2005.

2 The Effect of Changing the Basis

Example 1. We construct the generator polynomial for the RS-code of length 7 over the field GF(8) with code distance 4.

```
In[4] := b = 1; d = 4;
Rt = Table[GF[[2+Mod[b+i,Length[GF]-1],3]],{i,0,d-2}];
g = Product[x - Rt[[i]], {i, 1, Length[Rt]}];g =
Collect[PolynomialMod[PolynomialMod[Expand[g],r/.x ->
a], 2], x];g//.CD
```

Out[4]=

$$(x-a)(x-a^2)(x-a^3) \quad x^3+(a^2+1)x^2+ax+a^2+1$$

$$x^2a^6+a^6+xa+x^3$$

We have got the RS - code with the generator polynomial g with parameters [Length=7, Dimension=4, Distance=4] over the field GF(8). First of all we control that binary subspace (over GF(2)) give the code with parameters [7,1,7] with generator polynomial f(x) (Out[5]).

```
In[5] := CmRt = Complement[a^Union[Flatten[
Table[CyclotomicCoset[Exponent[Rt, a][[i]], 2, n], {i,
1, Length[Rt]}]]], Rt];
g1=g*Product[x - CmRt[[i]], {i, 1, Length[CmRt]}]
f = Collect[PolynomialMod[PolynomialMod[
Expand[g1],r/.x -> a], 2], x]
```

Out[5]=

$$x^6+x^5+x^4+x^3+x^2+x+1$$

With 4 information bits our RS – code (over GF(8)) has 4096 code words, and we can construct all these code words and we calculate all code vectors over GF(8)

$$\{\{0,0,0,a^2,a+a^2,a^2,1+a\},\{0,0,0,1,a^2,1,a\},\ldots\langle 4091\rangle\ldots,$$
$$\{1+a+a^2,a+a^2,1,1,1,1+a+a^2,a^2\},\{1+a+a^2,a+a^2,1,a^2,1+a,1+a^2\}\}$$

and overwrite as

$$\{\{0,0,0,a^2,a^4,a^2,a^3\},\{0,0,0,1,a^2,1,a\},\{0,0,0,a^4,a^6,a^4,a^5\},\ldots\langle 4089\rangle\ldots,$$
$$\{a^5,a^4,1,0,a^6,a^4,a^4\},\{a^5,a^4,1,1,1,a^5,a^2\},\{a^5,a^4,1,a^2,a^3,a,a^6\}\}$$

All code vectors with minimum weight can we calculate using Mathematica

$$\{\{0,0,0,a^2,a^4,a^2,a^3\},\{0,0,0,1,a^2,1,a\},\{0,0,0,a^4,a^6,a^4,a^5\},\ldots\langle 239\rangle\ldots,$$
$$\{a^5,a^3,a^4,0,0,0,a^3\},\{a^5,a^4,0,0,a,0,a^6\},\{a^5,a^4,a^3,0,0,1,0\}\}$$

Its means that we have all code vectors with weight 4 and first coordinate is 1.

$$\begin{pmatrix}
1 & a^2 & 1 & a & 0 & 0 & 0 \\
1 & 0 & a^5 & a^4 & a^3 & 0 & 0 \\
1 & 0 & a^3 & 0 & a^5 & a^3 & 0 \\
1 & 0 & a^3 & a^3 & 0 & 0 & a^4 \\
1 & 0 & a^4 & 0 & 1 & 0 & a^2 \\
1 & 0 & a & 0 & 0 & a^6 & a^3 \\
1 & 0 & a^2 & 1 & 0 & a^4 & 0 \\
1 & 0 & 0 & a^5 & a^2 & a^6 & 0 \\
1 & 0 & 0 & a^4 & 0 & a^2 & a \\
1 & 0 & 0 & a & a^4 & 0 & 1 \\
1 & 0 & 0 & 0 & a^6 & a & a^6 \\
1 & a^6 & 0 & 0 & a^3 & 0 & a \\
1 & a^6 & a^5 & 0 & 0 & a^2 & 0 \\
1 & a & 0 & 0 & 0 & 1 & a^2 \\
1 & 1 & 0 & 0 & a & a^4 & 0 \\
1 & a^5 & 0 & a^2 & 0 & a^5 & 0 \\
1 & a^5 & a^6 & 0 & 0 & 0 & a^5 \\
1 & a^4 & a & 0 & a^2 & 0 & 0 \\
1 & a^4 & 0 & a^5 & 0 & 0 & a^3 \\
1 & a^3 & 0 & a^6 & a^6 & 0 & 0
\end{pmatrix}$$

We can see that a change of the basis (the representation of the elements of the field GF(8) as binary vector) may change the minimum weight of the code. If we take the standard basis: $1 \to (0,0,1); a \to (0,1,0); a^2 \to (1,0,0)$ we get the binary code with parameters [3*7 = 21, 3*4 = 12, 4] with the same code distance , we have vector (1, a, 0, 0, 0, 1, a^2) , but if we change basis as :

$$1 \to (0,0,1); a \to (0,1,0); a^2 \to (1,1,1) \tag{2}$$

we obtained a code with parameters [21, 12, 5] and weight polynomial

$$w(x) = x^{21} + 21x^{16} + 168x^{15} + \ldots + 168x^6 + 21x^5 + 1$$

We finally consider the dual to the found code. As usual we find the weight polynomial of the dual code by using the Mc Williams Identity:

```
In[6] :=McWilliamsIdentity[W+1,21,x]
```

Out[6]= $1+210x^{8}+280x^{12}+21x^{16}$

We see that the dual code has the parameters [21, 9, 8] (Golay code).

3 Conclusion

With the introduction of computers and computer algebra and some application program as “Mathematica “and special packages [3] [4] gives possibility to solve some problems which solving without computers is very difficult. Using above construction we can find some Reed-Solomon codes which have the same distance independently of basis changing.

Example 2. We construct the generator polynomial for the RS-code of length 7 over the field GF (8) with code distance 3.
The same procedure as (**Example 1**) gives the generator polynomial of RS code

$$\left(x-a^{4}\right)\left(x-a^{5}\right)$$

which have the same code distance as independently of basis changing.

```
In[7] :=  CyclotomicCoset[5, 2,Length[GF]- 1]
CyclotomicCoset[2, 2, Length[GF] - 1]
```

Out[7]=

{5, 3, 6} {2, 4, 1}

References

1. MacWilliams, F. J., and Sloane, N. J. A. (1977) The Theory of Error - Correcting Codes. North - Holland, Amsterdam.
2. I Gachkov (2003) *Error Correcting codes with Mathematica,* Lecture note in Computer science LNCS 2657 737-746
3. I Gachkov (2004) *Computation of weight enumerators of binary linear codes using the package “ Coding Theory “* 6th International Mathematica Symposium Banff Canada eProceedings 16 p.
4. I. Gashkov (2004) *Constant Weight Codes with Package CodingTheory.m in Mathematica* . Lecture note in Computer science LNCS 3039 370-375
5. I. Gashkov (2004) *Package CodingTheory.m in Mathematica.* Download the package Mathematica web page http://library.wolfram.com/infocenter/MathSource/5085/