DESIGN OF AN ERROR CORRECTION SUBSYSTEM FOR USE WITH A DDS-2 RDAT TAPE SYSTEM

by

E. J. Weldon, Jr.
1152 Kealaolu Ave.
Honolulu, HI 96816

tel: 808-956-8597

January 10, 1995
corrections made
February 8, 1995

Appendix E

Finite-Field Isomorphisms

It is well known that there is only one finite field of a given order. One representation of GF(256) is as the residues of the binary irreducible polynomial $m_1(x) = x^8 + x^4 + x^3 + x^2 + 1$; this is the field representation used in this report.

There are advantages to representing this field in different ways. For example, computation of the inverse of an element is simpler when the field is represented as the residues of an irreducible quadratic over GF(16).

In this appendix we explain the relationship between two different representation of GF(256). The first of these, referred to as $GF(2^8)$, is the set of residues of $m_1(x)$ defined above. The second representation, $GF(16^2)$ is the set of residues of the polynomial

$$m_2(x) = x^2 + \beta^2 x + \beta$$

where β is a primitive element of $GF(2^4)$ defined by the irreducible binary polynomial $x^4 + x + 1$. The list of the elements of GF(16) is given in Reference 3. The first few elements of $GF(16^2)$ are listed in Table 1.

Now it is well known that an element in one representation is related to the corresponding element in the other by a linear transformation. Let A represent an element of $GF(2^8)$ defined by $m_1(x)$ and let B represent an element of $GF(16^2)$ defined by $m_2(x)$. Then we can write

$$B = MA$$

where

$$M = \begin{bmatrix} \beta^{13} & \beta^2 & \beta^{10} & \beta^6 & \beta^0 & \beta^2 & \beta^0 & 0 \\ \beta^3 & \beta^{11} & \beta^7 & \beta^1 & \beta^3 & \beta^1 & 0 & \beta^0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Example: let $A = \alpha^{14} =$ 0 0 0 1 0 0 1 1 (Appendix A). Then

$$B = MA = M \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} \beta^{13} \\ \beta^{4} \end{bmatrix}$$

Table 1 shows that $[\beta^{13}\ \beta^{4}] = \alpha^{14}$ in $GF(16^2)$.

Mapping from $GF(16^2)$ to $GF(2^8)$ can be done similarly. Clearly

$$A = M^{-1}B$$

Inverting M gives

$$M^{-1} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Example: In $GF(16^2)$ $\alpha^{14} = [\beta^{13}\ \beta^{4}] =$ [1 1 0 1 0 0 1 1]. Then

$$A = M^{-1} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \alpha^{14}$$

Each of the mappings M and M^{-1} employs roughly 14 2-input XOR gates or about 40 physical gates.

Appendix F

An Inverter for $GF(16^2)$

An element of GF(256) can be represented as the residue of a polynomial modulo an irreducible polynomial of degree 2 over $GF(2^4)$. For example, the polynomial

$$m_2(x) = (x + \alpha)(x + \alpha^{16}) = x^2 + \beta^2 x + \beta \qquad (1)$$

is irreducible over GF(16). Here $\beta = \alpha^{17}$ is an element of GF(16). This polynomial can be used to generate $GF(16^2)$.

Now since it is a residue of a quadratic, an element of this field is represented as a polynomial of degree 1 over GF(16). Let

$$\alpha^a = a_1 x + a_0 \qquad a_i \in (GF(16)) \qquad (2)$$

denote such an element. To compute the inverse of this element we must find an element

$$\alpha^b = b_1 x + b_0 \qquad (3)$$

such that $\alpha^a \cdot \alpha^b = 1$. Writing out this product gives

$$\alpha^a \cdot \alpha^b = a_1 b_1 x^2 + (a_1 b_0 + a_0 b_1)x + a_0 b_0 \qquad (4)$$

Now reducing this product polynomial modulo the defining quadratic $m_2(x)$ gives

$$\alpha^a \cdot \alpha^b = (a_1 b_0 + a_0 b_1 + a_1 b_1 \beta^2)x + (a_0 b_0 + a_1 b_1 \beta) \qquad (5)$$

Since $\alpha^a \cdot \alpha^b = 1$, it follows that

$$\begin{aligned} (a_1 b_0 + (a_0 + a_1 \beta^2) b_1 &= 0 \\ (a_0 b_0 + (a_1 \beta) b_1 &= 1 \end{aligned} \qquad (6)$$

Now these two linearly independent equations can be solved to give the coefficients of the desired inverse element, that is

$$b_0 = \frac{a_0 + a_1\beta^2}{a_1{}^2\beta + a_0{}^2 + a_0a_1\beta^2}$$

$$b_1 = \frac{a_1}{a_1{}^2\beta + a_0{}^2 + a_0a_1\beta^2} \qquad (7)$$

Thus the coefficients of the inverse element can be computed by performing a modest number of computations in GF(16). Figure 1 shows a diagram of a combinational logic circuit which performs these calculations. Figure 2 shows the fixed-element multipliers and squarer of Figure 1, while Figure 3 shows the general-purpose multiplier explained in Reference 3. All of these circuits operate in $GF(2^4)$ defined by $x^4 + x + 1$. The $GF(2^4)$ inverter used in Figure 1, which is a 4-input 4-output combinational logic circuit, can be implemented using conventional logic minimization techniques.

In Appendix E we explain the process of mapping one field representation onto another. Figure 4 shows the construction of an inverter for $GF(2^8)$ using an inverter for $GF(16^2)$ and two mapping circuits.

We estimate that the circuit of Figure 1 can be built using roughly 70 XOR's and 50 AND's for a total cost of roughly 260 gates. As explained in Appendix E, mapping to or from $GF(2^8)$ requires about 40 gates. Thus an inverter for $GF(2^8)$ will employ roughly 340 gates.