Bachelor Project 1

Designing RS Decoder for DVB-T Receivers

Sajjad Akherati

June 13, 2021

DVB-T

- DVB_T is an acronym of the phrase Digital Video Broadcasting — Terrestrial means that we can transfer digital images using an VHF/UHF antenna.
- to establish such communication, it is necessary to have different components in transmitter and reciever.
- our goal in this project is to implement different parts of the receiver using VHDL hardware description language on FPGA boards.

- Due to the importance of dealing with noise and error in the transmitter, it is used two type of coding included sequential and convolutional and the effect of each one must be returned at the receiver.
- The usual method is to use two decoding blocks, Viterby and Reed-Solmon in the receiver. Implementing these two decoding methods using VHDL will be one of our main goals in this project.

Definition		Resolution W x H (PPI)	Aspect Ratio	Frame Rate
Ultra High Definition (4k UHD)	2160p	3840 x 2160	16:9	24 fps 30 fps 60 fps 120 fps
High Definition (HDTV)	1080p	1920 x 1080	16:9 1:1	24 fps 30 fps
	1080i			30 fps
	720p	1280 x 720		24 fps 30 fps 60 fps
Standard Definition (SDTV)	480p	704 x 480	16:9 4:3	24 fps 30 fps 60 fps
		640 x 480	4:3 1:1	
	480i	704 x 480	16:9 4:3	30 fps
		640 x 480	4:3 1:1	

Figure: Digital Television's

- assume HDTV 720p with resolution 1280*720 with apect ratio 1:1 and frame rate of 60 fps.
- so we transfer 2,985,984,000 byte of data in one second:

$$3840 \times 2160 \times 120 \times 3 = 2,985,984,000\ Byte \simeq 2.78\ GB$$

- assume we receive a bad noise like lightning in 0.2ms.
- so the total number of 11059 byte of data in a row becomes noisy.

$$0.2 \times 10^{-3} \times 2985984000 \cong 597197 \cong 580\ KB$$

- coding and interleaving are so important to delete noise and reicive the right data.

Introduction To Coding Theory

Introduction To Algebra

Set G under a binary operator * is a group if it has the following properties:

1. closing:
$$\forall a, b \in G : a * b \in G.$$
2. identity element:
$$\exists e \in G : \forall a \in G : a * e = e * a = a.$$
3. inverse element:
$$\forall a \in G : \exists a' \in G : a * a' = a' * a = e.$$
4. associativity:
$$\forall a, b, c \in G : a * (b * c) = (a * b) * c.$$

1. Identity element is unique.
   Assume that is not and assume that e, e' are identity:

$$e' = e' * e = e \ \text{※}$$

2. Inverse element of each element in the group is unique.
   Assume that there are tow inverse element a', a'' for element a:

$$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a'') \ \text{※}$$

1. A commutative group:

$$\forall a, b \in G : a * b = b * a.$$

2. A finite groupe: a group that has finite elements.
3. Order of the group: number of elements in a group; showed by $|G|$.

- Additive Group:

$$\forall m \in \mathbb{N} : \exists G = \{0, 1, 2, \ldots, m-1\} : \forall a, b \in G : a * b = R_m\{a + b\}.$$

1. closing:
$$\forall a, b \in G : a * b = R_m\{a + b\} \in G.$$
2. identity element:
$$e = 0 : \forall a \in G : a * 0 = R_m\{a + 0\} = a.$$
3. inverse element:
$$\forall a \in G : a' = m - a : a * a' = R_m\{a + (m - a)\} = 0.$$
4. It is associative, too.

- Multiplicative Group:

$$\forall p \in \mathbb{N} \ \& \ \text{p is a prime} : \exists G = \{0, 1, 2, \ldots, p-1\}$$
$$: \forall a, b \in G : a * b = R_p\{a \times b\}.$$

1. closing:
$$\forall a, b \in G : a * b = R_p\{a \times b\} \in G.$$
2. identity element:
$$e = 1 : \forall a \in G : a * 1 = R_p\{a \times 1\} = a.$$
3. inverse element:
if $a \in G$ the $(a, p) = 1$;
if $(a, p) = 1 \Rightarrow \exists s, r : sa + rp = 1$.
$$as = -rp + 1 \Rightarrow R_p(as) = 1.$$

$$\begin{cases} s < p \Rightarrow a' = s; \\ s > p \Rightarrow s = s_1 p + s_2, s_2 < p \Rightarrow as = as_1 p + as_2 \\ \Rightarrow R_p(as_2) = R_p(as) = 1 \Rightarrow a' = s_2. \end{cases}$$

- Subgroup: Assume that G is a group under the binary operator * and H is a un-empty subsequense of G; we call H a subgroup, if it has the following prpperties:
  1. H is closed under the operator *.

$$\forall a, b \in H : a * b \in H.$$

  2. for each element H, its inverse element be at H.

$$\forall a \in H : a' \in H.$$

  - conclusion: the identity element is in H.

$$\begin{cases} a \in H \\ a' \in H \end{cases} \Rightarrow a * a' = e \in H.$$

The set F with binary operators $+$ and $.$ is a field, if it has the following properties:

- F is a commutative group under $+$.
- $F/\{0\}$ is a commutative group under $.$ operator.
- $+$ is distributable on $.$:

$$\forall a, b, c \in F : a.(b + c) = a.b + a.c$$

Filed Properties:

1. $\forall a \in F \setminus \{0\} : a.0 = 0.a = 0$
2. $\forall a, b \in F \setminus \{0\} : a.b \neq 0$
3. $-(a.b) = (-a).b = a.(-b)$
4. if $a.b = a.c$ and $a \neq 0 \Rightarrow b = c$

- GF(p): for each prime number p, there is a finite field $GF(p)$ with binary operators $R_p(+), R_p(.)$ such that:

$$GF(p) = \{0, 1, 2. \ldots, p-1\}$$

- $-a := a - a = 0$
- $a^{-1} := a.(a^{-1}) = 1$
- example: $GF(5) = \{0, 1, 2, 3, 4\}$

$$-4 = 1 \qquad 4^{-1} = 4$$
$$2 - 4 = 2 + (-4) = 2 + 1 = 3 \qquad 2 \div 4 = 2.(4^{-1}) = 2.4 = 3$$

Field Characteristic: λ

- $1 \in GF(q)$
- $1+1 \in GF(q)$
- $1+1+\cdots+1 \in GF(q)$

$$\exists m, n : \sum_{i=1}^{m} 1 = \sum_{i=1}^{n} 1 \Rightarrow \sum_{i=1}^{m-n} 1 = 0$$

λ is minimom number such that $\sum_{i=1}^{\lambda} 1 = 0$.

- λ is a prime.
  assume that is not; so $\lambda = a.b$ and $a, b < \lambda$:

$$\sum_{i=1}^{\lambda} 1 = 0 \Rightarrow \sum_{i=1}^{a.b} 1 = 0 \Rightarrow \sum_{i=1}^{a} 1 . \sum_{i=1}^{b} 1 = 0 \Rightarrow \sum_{i=1}^{a} 1 = 0 \text{ or } \sum_{i=1}^{b} 1 = 0$$

Field Order:n

for any element a in a field F, It is the minimom number n such that $a^n = 1$.

- for all elements in field GF(q): $a^{q-1} = 1$:
  consider all nonzeros elements of GF(q) that they are $b_1, b_2, \ldots, b_{q-1}$;
  so $a.b_1, a.b_2, \ldots, a.b_{q-1}$ are the nonzeros elements of the field, too:

$$b_1.b_2.\ldots.b_{q-1} = (a.b_1).(a.b_2).\ldots.(a.b_{q-1})$$

$$= a^{q-1}.(b_1.b_2.\ldots.b_{q-1}) \Rightarrow a^{q-1} = 1.$$

- $q-1$ is divisable to order of each element in the field.

- $GF(2) = \{0, 1\}$

addition	multiplication
$1+0=0+1=1$	$1.0=0.1=0.0=0$
$1+1=0+0=0$	$1.1=1$

- example: $\begin{cases} X+Y=1 \\ X+Z=0 \\ X+Y+Z=1 \end{cases}$

$$X=\frac{\begin{vmatrix}1&1&0\\0&0&1\\1&1&1\end{vmatrix}}{\begin{vmatrix}1&1&0\\1&0&1\\1&1&1\end{vmatrix}}=\frac{0}{1}=0.1=0, Y=1, Z=0$$

- Polynomials with variable X and coefficients on GF(2):

$$f(x) = f_0 + f_1X + f_2X^2 + \cdots + f_nX^n, f_i \in GF(2)$$

- Addition and multiplication of polynomials in GF(2):

$$g(x) = g_0 + g_1X + g_2X^2 + \cdots + g_nX^n, g_i \in GF(2)$$

$$f(x) + g(x) = (f_0 + g_0) + (f_1 + g_1)X + (f_2 + g_2)X^2 + \cdots + (f_n + g_n)X^n$$

$$f(x).g(x) = c_0 + c_1X + c_2X^2 + \cdots + c_nX^n$$

$$c_0 = f_0.g_0$$
$$c_1 = f_1.g_0 + f_0.g_1$$
$$\vdots$$

- Dividing polynomials in $GF(2)$:

$$f(x) = q(x)g(x) + r(x)$$

- example: $f(x) = x^6 + x^5 + x^4$ and $g(x) = x^3 + x + 1$:

$$\underbrace{x^6 + x^5 + x^4}_{f(x)} = \underbrace{(x^3 + x^2)}_{q(x)} . \underbrace{(x^3 + x + 1)}_{g(x)} + \underbrace{x^2}_{r(x)}$$

- Any polynomial degree m in GF(2) divides $X^{2^m-1}+1$.
- The polynomial p(x) degree m is prime if:

$$\begin{cases} p(x)|x^n+1 \\ \min(n)=2^m-1 \end{cases} \Rightarrow \text{ p(x) is prime.}$$

- For any polynomial in GF(2), we have:

$$[f(x)]^{2i}=f(x^{2i})$$

- Building the finite field of $GF(2^m)$:
  - $F := \{0, \alpha, \alpha^2, \ldots, \alpha^n\} : n = 2^m - 1$
  - Multiplication and Addition:

$$\alpha^i.0 = 0.\alpha^i = 0$$

$$\alpha^i.1 = 1.\alpha^i = \alpha^i$$

$$\alpha^i.\alpha^j = \alpha^{i+j}$$

  - The fundumental polynomial of the field with degree m and root α: p(x)

$$x^{2^m-1} + 1 = q(x).p(x)$$

$$\Rightarrow \alpha^{2^m-1} + 1 = q(\alpha).\underbrace{p(\alpha)}_{0} = 0 \Rightarrow \alpha^{2^m-1} = 1$$

- Closed under multiplication:

$$\alpha^i.\alpha^j = \alpha^{i+j} \begin{cases} i+j \leq 2^m-1 \Rightarrow \alpha^{i+j} \\ i+j > 2^m-1 \end{cases} \begin{array}{l} \\ \Rightarrow i+j = 2^m-1+r \\ \Rightarrow \alpha^{i+j} = \alpha^{2^m-1}.\alpha^r = \alpha^r \end{array}$$

- $\alpha^{-i} = \alpha^{2^m-1-i}$
- $0 + \alpha^i = \alpha^i$
- $0.\alpha^i = 0$

- example: $p(x) = x^4 + x + 1$

$$p(\alpha) = \alpha^4 + \alpha + 1 = 0 \Rightarrow \alpha^4 = \alpha + 1$$

0	0	0000
α^0	α^0	0001
α^1	α^1	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha^1 + 1$	0011
α^5	$\alpha.\alpha^4 = \alpha^2 + \alpha$	0110
$\vdots$	$\vdots$	$\vdots$
α^{15}	$\alpha.\alpha^{14} = \ldots$	$\ldots$

Table: Field Element Tacle of $GF(2^4)$

- if $f(x)$ be a polynomial that its coeffiecients belong to $GF(2)$ and β be its root:

$$f(\beta) = 0 \Rightarrow f(\beta^{2^l}) = 0 \qquad l \geq 0$$

  we call β^{2^l}, β conjugates.
- All $2^m - 1$ nonzero elements of $GF(2^m)$ are roots of $x^{2^m-1} + 1$.
- $p(X)|X^{2^m-1} + 1 \Rightarrow p(X)|X^{2^m} + X$
- if β is a fundumental element in $GF(2^m)$, then it conjucates are the fundumental elements, too.

Refrences

- DVB-T Standard
- **Error Control Coding:** fundumental and applications, SHU LIN \ DANIEL J.COSTELLO,Jr.


Thank you