Introduction to Coding Theory
236309

Tutorial #12
Multiplication and Division Circuits for Encoding and Decoding

Technion – Israel Institute of Technology
Department of computer science, 2016
Prepared by Netanel Raviv
Agenda

• In this tutorial we will –
  – Define digital circuits.
  – Construct a circuit for traversing all elements of $GF(q^n)$.
  – Construct a *multiplication* circuit for non-systematic encoding of Reed-Solomon codes.
  – Construct a *division* circuit for systematic encoding of Reed-Solomon Codes.
Digital Circuits

• Ingredients:
  - Memory cells.
  - Multipliers.
  - Adders.

• Inputs from $GF(q)$.

\[
\begin{aligned}
\gamma + \beta \cdot \alpha \\
\end{aligned}
\]
Traversing All Elements of $GF(q^n)$

- Possible application – finding the roots of a polynomial.
- Let $p(x)$ be a primitive monic polynomial of degree $n$ over $GF(q)$.
- Let $\alpha$ be a root of $p(x)$. The powers of $\alpha$ generate the multiplicative group of $GF(q^n)$, constructed by $p(x)$.
- Denote $p(x) = \sum_{i=0}^{n} a_i \cdot x^i$, $(a_n = 1)$.
- $p(\alpha) = 0 \implies \alpha^n = \sum_{i=0}^{n-1} (-a_i) \alpha^i$.
- Any $\lambda \in GF(q^n)$ has a representation $\lambda = \sum_{i=0}^{n-1} \lambda_i \cdot \alpha^i$, $\lambda_i \in GF(q)$.
Traversing All Elements of $GF(q^n)$

- **Claim**: $\lambda \cdot \alpha = -\lambda_{n-1} \cdot a_0 + \sum_{i=1}^{n-1} (-\lambda_{n-1} \cdot a_i + \lambda_{i-1})\alpha^i$.

- **Proof**: Recall that $\alpha^n = \sum_{i=0}^{n-1} (-a_i)\alpha^i$, and

  \[
  \lambda = \sum_{i=0}^{n-1} \lambda_i \cdot \alpha^i \\
  \lambda\alpha = \sum_{i=0}^{n-1} \lambda_i \alpha^{i+1} \\
  \quad = \sum_{i=1}^{n} \lambda_{i-1} \alpha^i \\
  \quad = (\sum_{i=1}^{n-1} \lambda_{i-1} \alpha^i) + \lambda_{n-1} \alpha^n \\
  \quad = (\sum_{i=1}^{n-1} \lambda_{i-1} \alpha^i) + \lambda_{n-1} \sum_{i=0}^{n-1} (-a_i)\alpha^i \\
  \quad = -\lambda_{n-1} \cdot a_0 + \sum_{i=1}^{n-1} (-\lambda_{n-1} \cdot a_i + \lambda_{i-1})\alpha^i
  \]
Traversing All Elements of $GF(q^n)$

- $\lambda \cdot \alpha = -\lambda_{n-1} \cdot a_0 + \sum_{i=1}^{n-1} (-\lambda_{n-1} \cdot a_i + \lambda_{i-1})\alpha^i$.
- The circuit -

![Diagram of the circuit](image-url)
Traversing All Elements of $GF(q^n)$

\[ \lambda = a_0 \cdot \alpha^0 + a_1 \cdot \alpha^1 + a_2 \cdot \alpha^2 + \ldots + a_{n-1} \cdot \alpha^{n-1} \]
Traversing All Elements of $GF(q^n)$

• Initialization -

\[ \alpha^0 = \alpha^0 \]

\[ \alpha^1 = \alpha^0 \]

\[ \alpha^2 = \alpha^1 \]

\[ \alpha^{n-1} = \alpha^{n-1} \]
Traversing All Elements of $GF(q^n)$

- Step -

$$\alpha^1 = \alpha^0 \cdot \alpha^1 \cdot \alpha^2 \cdot \alpha^{n-1}$$
Traversing All Elements of $GF(q^n)$

- After $n$ steps –

\[ \alpha^{n-1} = \alpha^0 \cdot \alpha^1 \cdot \alpha^2 \cdot \ldots \cdot \alpha^{n-1} \]
Traversing All Elements of $GF(q^n)$

- Another step – $\alpha^n = \sum_{i=0}^{n-1} (-a_i) \alpha^i$

- Continue according to –

  \[ \lambda \cdot \alpha = -\lambda_{n-1} \cdot a_0 + \sum_{i=1}^{n-1} (-\lambda_{n-1} \cdot a_i + \lambda_{i-1}) \alpha^i \]
Reminder

• Let $C$ be an $[n, k]$ (conventional) Reed Solomon code over $GF(q)$.
• Every code word $c \in C$ can be considered as a polynomial $c(x)$ such that $\deg(c(x)) \leq n - 1$.
• The code $C$ has a generator monic polynomial $g(x)$ which satisfies $c \in C \iff c \in GF(q)^n \land g(x)|c(x)$
• $\deg(g(x)) = n - k$.
• In polynomial notation $-u(x) \in F^k[x], g(x) \in F^{n-k+1}[x], u(x) \cdot g(x) = c(x), c \in C$.
• In matrix notation $-$

$$
[u_0 \cdots u_{k-1}] \begin{bmatrix}
g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\
0 & g_0 & \cdots & \vdots & g_{n-k} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & g_0 & \cdots & g_{n-k}
\end{bmatrix} = [c_0 \cdots c_{n-1}]
$$
Non-Systematic Encoding of RS Codes

\[ c \in C \leftrightarrow \exists u(x), \deg(u(x)) \leq k - 1, u(x) \cdot g(x) = c(x) \]
Non-Systematic Encoding of RS Codes

\[ \ln T = 1, \]

\[ u_{k-1} \]

\[ g_{n-k} \]

\[ g_{n-k-1} \]

\[ g_{n-k-2} \]

\[ g_1 \]

\[ g_0 \]

\[ u_{k-1}g_{n-k} = c_{n-1} \]
Non-Systematic Encoding of RS Codes

\[ \ln T = 2, \]

\[ u_{k-2} \rightarrow u_{k-1} \rightarrow 0 \rightarrow 0 \]

\[ g_{n-k} \rightarrow g_{n-k-1} \rightarrow g_{n-k-2} \rightarrow g_1 \rightarrow g_0 \]

\[ u_{k-2}g_{n-k} + u_{k-1}g_{n-k-1} = c_{n-2} \]
Non-Systematic Encoding of RS Codes

\[ \ln T = n, \]

\[ u_k, \ldots, u_{n-1} = 0 \]

\[ u_0 g_0 = c_0 \]
Systematic Encoding of RS Codes

• Let $u(x) \in F^k[x]$.  
• Let $r(x)$ be the remainder in the division of $u(x) \cdot x^{n-k}$ by $g(x)$.  
• $u(x) \cdot x^{n-k} = g(x) \cdot q(x) + r(x), \deg(r(x)) < \deg(g(x)) = n - k$.  
• Define $c(x) \triangleq u(x) \cdot x^{n-k} - r(x) = g(x) \cdot q(x)$.  
• $g(x)|c(x)$, and thus $c \in C$.  
• Since $\deg(u(x)) \leq k - 1$ and $\deg(r(x)) < n - k$,  
  • $c = u_{k-1}, u_{k-2}, \ldots, u_0, -r_{n-k-1}, -r_{n-k-2}, \ldots, -r_0$.  
  • Hence, the encoding is systematic.  
• We construct a division circuit for this encoding.
Systematic Encoding of RS Codes

\[ c_0, c, \ldots, c_{n-1} \rightarrow u_0, u_1, \ldots, u_{k-1} \rightarrow \]

Diagram showing a systematic encoding circuit for RS codes.
Systematic Encoding of RS Codes

\[
\text{In } T = 1, \quad u_k = c_{n-1}
\]
Systematic Encoding of RS Codes

In $T = 2$,

\[
\begin{align*}
-g_0 & \cdot u_{k-1} \\
-g_1 & \cdot u_{k-1} \\
-g_2 & \cdot u_{k-1} \\
& \vdots \\
-g_{n-k-1} & \cdot u_{k-1} \\
\end{align*}
\]

\[u_{k-2} = c_{n-2}\]

\[u_{k-2} = g_0 u_{k-1} x - g_1 u_{k-1} x^2 - \cdots - g_{n-k-1} u_{k-1} x^{n-k-1} = u_{k-1} x^{n-k} \text{ MOD } g(x)\]
Systematic Encoding of RS Codes

• We can prove by induction that the content of the memory cells in the $\ell$-th clock tick is $x^{n-k} \sum_{i=1}^{\ell} u_{k-i} x^{\ell-i} \ MOD g(x)$.

• Hence, in the $k$-th clock tick it is
  
  $x^{n-k} \sum_{i=1}^{k} u_{k-i} x^{k-i} \ MOD g(x) = x^{n-k} u(x) \ MOD g(x) = r(x)$
Systematic Encoding of RS Codes

\[ \ln T = k + 1, \]

\[ B - r_{n-k-1} = c_{n-k-1} \]
Systematic Encoding of RS Codes

\[ \ln T = n, \]

\[ B - r_0 = c_0 \]