# EC500

Design of Secure and Reliable Hardware

Lecture 9

Mark Karpovsky

# 1 Arithmetical Codes

## 1.1 Detection and Correction of errors in arithmetical channels (adders, multipliers, etc)

Let $S = \{0,1,\cdots,2^n - 1\}$ and $C$ be a subset of $S$. We will call $C$ an arithmetical code.

For any $a, b \in S$, we denote the **arithmetical distance** between $a$ and $b$ as $d_A(a,b)$, where $d_A(a,b)$ is a minimal number of $\pm 2^i$ terms in representation of $|a-b|$, for $i < n$. Norm of $a$, $|a| = d_A(0,a)$. For the rest of this lecture note, we will denote $d_A(a,b)$ as just $d(a,b)$ for simplicity. As an example, for $n = 4$, we have $d(2,9) = 2$ since $9 - 2 = 7 = 2^3 - 2^0$, or $|7| = 2$. The arithemetical distance $d(C)$ of a code $C$ is the minimal distance between any two different codewords of the code.

If $y$ is distorted into $\tilde{y} = y + e$, then the multiplicity of the error $e$ is $|e|$. A code $C$ is capable of detecting $l$ errors iff $d(C) \geq l + 1$, and correcting $l$ errors iff $d(C) \geq 2l + 1$.

## 1.2 AN-Codes

$C = \{0, A, 2A, \cdots, (K-1)A\}$ where $(K-1)A \leq 2^n - 1$. For any $v \in C$, the residue of $v$ modulo $A$, $\mathrm{res_A}\, v$, is equal to $0$. ($\mathrm{res_A}\, v = 0$ is comparable to $Hv = 0$ for linear codes where $H$ is the check matrix for the code).

**Error detection:** verify that the output $\tilde{v}$ of the arithmetical device (AD) belongs to $C$. (verify that $\mathrm{res_A}\, \tilde{v} = 0$).

**Error correction:** for an output $\tilde{v}$, find the nearest (in terms of arithmetical distance) codeword $v$.

### 1.2.1 Single Error Detecting Arithmetical codes with distance 2

$A = 3$ since $\mathrm{res}_3 \pm 2^i$ is <u>not</u> equal to $0$. The number of codewords is less than or equal to $\frac{(2^n-1)}{3} + 1$.

### 1.2.2 Single Error Correcting (SEC) Arithmetical codes with distance 3

Any single error $e$ is in the form $\pm 2^i$ for $i = 0, 1, \cdots, n-1$. To correct single errors by AN-code, we need that the **syndromes $\mathbf{res_A} e$ should all be different and not equal to $\mathbf{0}$**.

**Example**

$n = 11$, $A = 23$

$\mathrm{res}_{11}\, 2^0 = 1$, $\mathrm{res}_{11} - 2^0 = 22$, $\mathrm{res}_{11}\, 2^1 = 2$, $\mathrm{res}_{11} - 2^1 = 21$, $\mathrm{res}_{11}\, 2^2 = 4$, $\mathrm{res}_{11} - 2^2 = 19$, $\mathrm{res}_{11}\, 2^3 = 8$, $\mathrm{res}_{11} - 2^3 = 15$, $\mathrm{res}_{11}\, 2^4 = 16$, $\mathrm{res}_{11} - 2^4 = 7$, $\cdots$, $\mathrm{res}_{11}\, 2^{10} = 12$, $\mathrm{res}_{11} - 2^{10} = 11 \pmod{23}$.

All numbers $\pm 2^i$ for $i = 0, 1, 2, 3, 4, \cdots, 11$ are different modulo 23 and we have a $23N$ single error correcting code $C = \{0,23,46,\cdots,2047\}$.

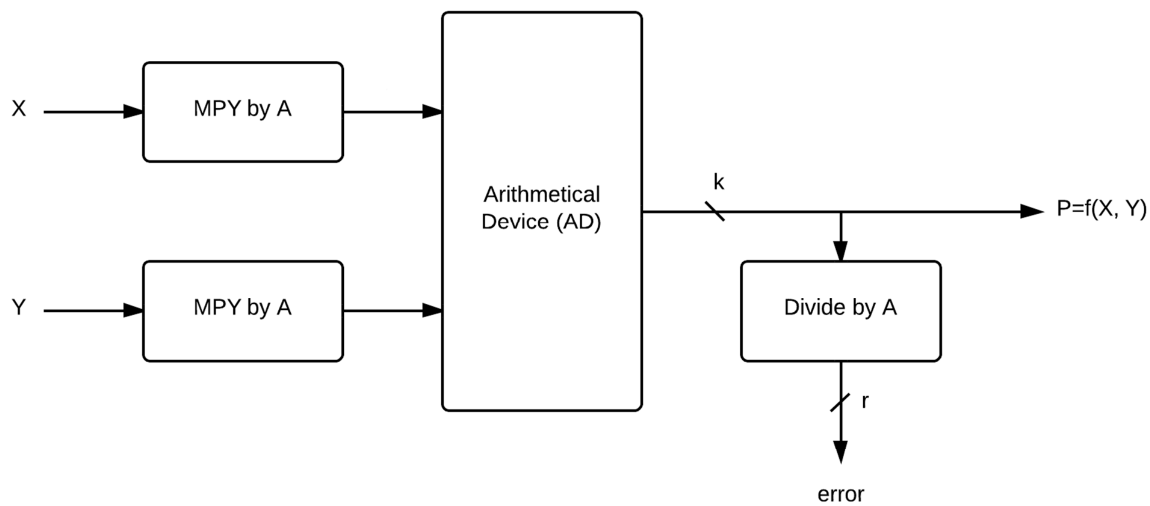
### 1.3 Hamming Bound

Let $V_A(n,l)$ be the volume of an **arithmetical ball with radius $l$**. (number of errors with multiplicity $l$ for $S = \{0,1,\cdots,2^n - 1\}$). Since for error correction by AN code, any 2 errors $e_1$ and $e_2$ should have different syndromes ($\mathrm{res_A} e_1 \neq \mathrm{res_A} e_2$), we have $\boldsymbol{A \geq V_A(n,l)}$. Compare to $2^{n-k} = 2^r \geq V_H(n,l)$ where $V_H(n,l)$ is the volume of the Hamming ball of radius $l$ for linear codes.

We say the code is **perfect** iff $\boldsymbol{A = V_A(n,l)}$. For single errors ($l = 1$, $d = 3$), $V_A(n,1) = 2n + 1$. SEC code is **perfect** iff $A = 2n + 1$. The $23N$ code shown in the previous example is perfect.

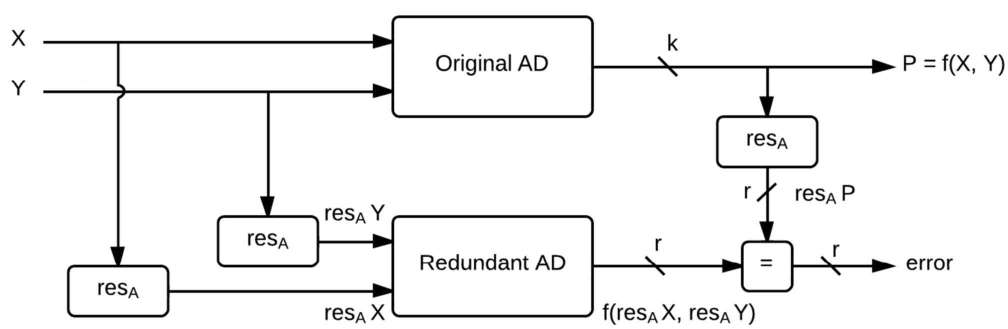
**Theorem.** AN codes are prefect SEC codes iff 2 is primitive modulo $A$.

### 1.4 Hardware Implementations of Nonsystematic Arithmetical Codes




### 1.5 Hardware Implementations of Systematic Arithmetical Codes

Codewords in the form $(P, \mathrm{res_A} P)$ ($P$ is $k$ bits, $\mathrm{res_A} P$ is $r = \log_2 A$ bits)



## 1.6 Low Cost AN Codes

Division is **not required** to compute $\mathrm{res_A}\, X$.

Denote $q = A + 1$, represent $X$ with radix $q$. $X = \sum_{i=0}^{m} X_i q^i$ where $X_i$ belongs to $\{0,1,\cdots,q-1\}$. Then, $\mathrm{res_A}\, X = \mathrm{res_A}\, X_0 + \mathrm{res_A}\, X_1 + \cdots + \mathrm{res_A}\, X_m = X_0 + X_1 + \cdots + X_m$ since $\mathrm{res_A}\, X_i = X_i$.

Or, denote $q = A - 1$, represent $X$ with radix $q$. $X = \sum_{i=0}^{m} X_i q^i$ where $v_i$ belongs to $\{0,1,\cdots,q-1\}$. Then, $\mathrm{res_A}\, X = \mathrm{res_A}\, X_0 - \mathrm{res_A}\, X_1 + \mathrm{res_A}\, X_2 - \mathrm{res_A}\, X_3 + \cdots + \mathrm{res_A}\, X_m = X_0 - X_1 + X_2 - X_3 \cdots + X_m$, where $\mathrm{res_A}\, X_i = X_i$ if $X_i < q - 1$ and $\mathrm{res_A}\, X_i = 0$ if $X_i = q - 1$.

For $q = 2^s$, $A = 2^s + 1$ or $A = 2^s - 1$. If $A = 2^s + 1$, then $\mathrm{res_A}\,(2^s) = 1$ and if $A = 2^s - 1$, then $\mathrm{res_A}\,(2^s) = -1$.

**Example 1**
$A = 31$, $s = 5$, $q = 32$, $n = 15$

Let $X = \sum_{i=0}^{14} x_i 2^i = \sum_{i=0}^{4} x_i 2^i + 2^5 \sum_{i=5}^{9} x_{i+5} 2^i + 2^{10} \sum_{i=10}^{14} x_{i+10} 2^i = X_0 + 2^5 X_1 + 2^{10} X_2$, where $X_0, X_1, X_2$ belong to $\{0,1,\cdots,31\}$. Then, $\mathrm{res_{31}}\, X = \mathrm{res_{31}}\, X_0 + \mathrm{res_{31}}\, X_1 + \mathrm{res_{31}}\, X_2 \pmod{31}$. $\mathrm{res_{31}}\, X_i = X_i$ if $X_i < 32$, and $\mathrm{res_{31}}\, X_i = 0$ if $X_i = 31$.

**Example 2**
$A = 33$, $s = 5$, $q = 32$, $n = 15$

Let $X = \sum_{i=0}^{14} x_i 2^i = \sum_{i=0}^{4} x_i 2^i + 2^5 \sum_{i=5}^{9} x_i 2^i + 2^{10} \sum_{i=10}^{14} x_i 2^i = X_0 + 2^5 X_1 + 2^{10} X_2$, where $X_0, X_1, X_2$ belong to $\{0,1,\cdots,31\}$. Then, $\mathrm{res_{33}}\, X = \mathrm{res_{33}}\, X_0 - \mathrm{res_{33}}\, X_1 + \mathrm{res_{33}}\, X_2 = X_0 - X_1 + X_2 \pmod{33}$.

## 2 Cyclic Hamming Codes

Let $n = 2^r - 1$ and consider $GF(2^r)$. Let $\alpha$ be primitive in $GF(2^r)$. $\alpha^i \neq \alpha^j$, $i \neq j$, $i, j = 0,1,\cdots,2^r - 2$. Take $H = [1 \quad \alpha \quad \alpha^2 \quad \cdots \quad \alpha^{2^r-2}]$, + since $\alpha^i \neq \alpha^j$, $H$ is a check matrix for a $(2^r - 1, 2^r - r - 1, 3)$ Hamming code.

For $r = 3$, $v \in V$ iff $v_0 + \alpha v_1 + \alpha^2 v_2 + \cdots + \alpha^6 v_6 = 0$. Let $v(x) = v_0 + v_1 x + v_2 x^2 + \cdots + v_6 x^6$ polynomial representation of $v$, $\boxed{\text{then } v \in V \text{ iff } v(\alpha) = 0,\ \alpha \text{ is a root of } v(x).}$ For $v = (v_0, v_1, \cdots, v_6)$, denote $y = \mathrm{Rot}\, v = (v_6, v_0, \cdots, v_5)$. Then in the polynomial form, $y(x) = v_6 + v_0 x + v_1 x^2 + \cdots + v_5 x^6 = v(x) \cdot x$ since $x^7 = x^0 = 1$.

There are no simple procedures to decide whether a polynomial $p(x)$ is primitive over $Z$ (irreducibility is a necessary condition for primitivity). For $GF(2^r)$, there are good tables of primitive polynomials.

**Example**

$Z = Z_2 = \{0,1\}$, $n = 3$

| Binary | Polynomial | Exponenetial |
|---|---|---|
| 0 0 0 | $0$ | - |
| 0 0 1 | $x^2$ | $\alpha^2$ |
| 0 1 0 | $x$ | $\alpha^1$ |
| 0 1 1 | $x + x^2$ | $\alpha^4$ |
| 1 0 0 | $1$ | $\alpha^0$ |
| 1 0 1 | $1 + x^2$ | $\alpha^6$ |
| 1 1 0 | $1 + x$ | $\alpha^3$ |
| 1 1 1 | $1 + x + x^2$ | $\alpha^5$ |
| $1 \quad \alpha \quad \alpha^2$ | | |

$p(x) = x^3 + x + 1 \rightarrow x^3 = x + 1$

$\alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$, $\alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1$

$\alpha^7 = \alpha^{2^n - 1} = \alpha^3 + \alpha = 1$, $|GF(2^r)| = 8$

$(101)(110) = \alpha^6 \cdot \alpha^3 = \alpha^9 = \alpha^2 = 001$

${}^{111}/_{110} = \alpha^2 = 001$, ${}^{110}/_{101} = \alpha^{-3} = \alpha^4 = 011$

Thus, $\boxed{\text{if } y = \mathrm{Rot}\, v, \text{ then } y(x) = xv(x)}$. If $v(\alpha) = 0 \leftrightarrow v \in V$, $y(x) = xv(x) \leftrightarrow y(\alpha) = 0 \leftrightarrow \mathrm{Rot}\, v \in V$. Our code is closed for circular shifts → cyclic code.

## 3 Binary Hamming Codes (cont'd)

$n = 2^r - 1$. Consider $GF(2^r)$ generated by $p(x)$ where $\deg P(x) = r$. Let $\alpha$ be the root of $p(x)$, $p(\alpha) = 0$. Take $H = [1 \quad \alpha \quad \alpha^2 \quad \alpha^3 \quad \cdots \quad \alpha^{n-1}]\,\}r$, $v \in C$ (Hamming code) iff $Hv = 0$, $v(\alpha) = 0$. If $v \in C \leftrightarrow v(\alpha) = 0$. Consider $Q(x) = v(x)\omega(x)$ for any $\omega(x)$, then $Q(\alpha) = v(\alpha)\omega(\alpha) = 0 \rightarrow Q \in C$. If $v$ is a codeword, all multiples of $v$ are codewords. Since $p(\alpha) = 0$, code $C$ consists of all multiples of $p(x)$.

For example, for $n = 3$, one can take $p(x) = x^3 + x + 1$ (primitive). Then $p(x) \in C \rightarrow (1101000) \in C$ and code consists of all multiples of $p(x) = x^3 + x + 1$.

**Example**
$(x^3 + x + 1)(x^2 + 1) = x^5 + x^3 + x^2 + x^3 + x + 1 = x^5 + x^2 + x + 1 \rightarrow 1110010 \in C$

***Remark***: Shortened Hamming codes with $n < 2^r - 1$ are not cyclic.

### 3.1 Generating Matrices for Binary Hamming Codes

Let $p(x)$ be used to construct $GF(2^r)$ $\deg p(x) = r$. $p(x)$ is primitive and $p(\alpha) = 0$, $p \in C$. Then $xp(x) \in C$ since $xp(x) = \operatorname{Rot} p(x)$. $x^2p(x) \in C$, $x^3p(x) \in C$ and the generating matrix $G$ can be taken as $G = \begin{bmatrix} p(x) \\ xp(x) \\ x^2p(x) \\ \vdots \\ x^{k-1}p(x) \end{bmatrix}$, where $k = n - r = 2^r - 1 - r$.

**Example**
$n = 2^3 - 1 = 7$, $r = 3$, $k = 4$
$p(x) = x^3 + x + 1 \rightarrow p = (1101000) \in C$
$xp(x) = x^4 + x^2 + x$ or in binary 0110100
$x^2p(x) = x^5 + x^3 + x^2$ or 0011010
$x^3p(x) = x^6 + x^4 + x^3$ or 0001101

$$\text{And } G = \left.\overbrace{\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}}^{n=7}\right\} k = 4 \text{ (not in standard form)}$$

**Example**
$r = 3$, $x^3 + x + 1 \rightarrow \alpha^3 + \alpha + 1 = 0$

$$H = \begin{array}{c} \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \\ \qquad\qquad\qquad \nwarrow \alpha^5 \end{array} \begin{array}{c} \alpha^2 \\ \alpha \\ 1 \\ \phantom{x} \end{array} = [1 \quad \alpha \quad \alpha^2 \quad \alpha^3 \quad \alpha^4 \quad \alpha^5 \quad \alpha^6]$$

(7,4,3) Hamming code $V$. Let $v = (v_0, v_1, \cdots, v_6) \in V$, then $Hv = 0$.