Arithmetical Codes.

Detection and Correction of errors In Arithmetical Channels (Adders, Multipliers, etc)

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

For any a,b from S we denote the **arithmetical distance** between a and b as d(a,b), where d(a,b) is a minimal number of terms $+2^i$ or -2^i in representation of $|a-b|$, where $i<n$. Norm $|a|$ of a is d(0,a)

For example , for n=4 we have d(2,9)=2, since $9-2=+2^3-2^0$. ($|7|=2$)

The (arithmetical) **distance d(C) of a code C** is a minimal distance between any two different elements of the code.

If y is distorted into $y'=y+e$, then the multiplicity of error e is $|e|$.

Code C detects t errors iff d(C)≥t+1 . C corrects t errors iff d(C)≥2t+1.

AN-Codes

C={0, A, 2A,…,(K-1)A} where $(K-1)A\leq 2^n-1$. For any v from C we have residue of v modulo A $res_A v$ is equal to 0. ($res_A v=0$, compare to Hv=0 where H is a check matrix of a linear code)

Error detection: verify that the output v' of the Arithmetical Device (AD) belongs to C (verify that $res_A v'=0$)

Error correction: For an output v' find nearest (in terms of arithmetical distance) codeword v

Single Error Detecting Arithmetical codes with distance 2:

A=3 Since $res_3\, 2^i$ is NOT equal to 0 . Modulo 3 check.

Number of codewords $K\leq(2^n-1)/3$

Single Error Correcting (SEC) Arithmetical Codes with distance 3.

Any single error e is in the form $+2^i$ or -2^i (i=0,1,…,n-1)

To correct single errors by AN-code we need that syndromes **res_A e should be all different and not equal to 0.**

Example 1. n=5, A=11. Then $res_{11}\, 2^0=1$, $res_{11}\,(-2^0)=10$, $res_{11}\, 2^1=2$, $res_{11}\,(-2^1)=9$, $res_{11}\, 2^2=4$, $res_{11}(-2^2)=7$, $res_{11}\, 2^3=8$, $res_{11}\,(-2^3)=3$, $res_{11}\, 2^4=5$, $res_{11}\,(-2^4)=6$ (mod11)

All numbers $+2^i$ and -2^i (i=0,1,2,3,4) are different modulo 11 and we have 11N single error correcting code C={0,11,22}.

Hamming Bound

Let $V_A(n,t)$ number of errors with multiplicity t for S={0,1,…,2^n-1} (Volume of an **arithmetical ball with radius t**)

Since for error correction by AN code any 2 errors e and e' should have different syndromes ($res_A e \neq res_A e'$) we have

$$A \geq V_A(n,t)$$

(Compare to $2^{n-k}=2^r \geq V_H(n,t)$ where $V_H(n,t)$ is volume of the Hamming ball of radius t for algebraic codes)

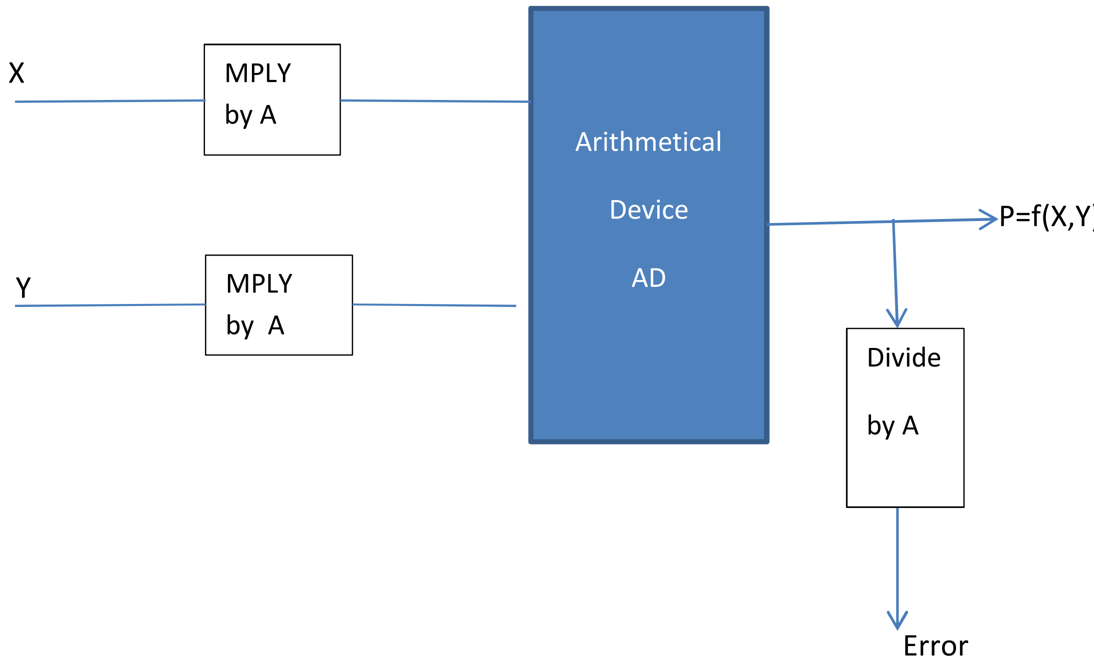
Code is **perfect** iff **$A=V_A(n,t)$**

For single errors (t=1, d=3) $V_A(n,1)=2n+1$

SEC code is **perfect** iff A=2n+1. The 11N code from the Example is perfect.

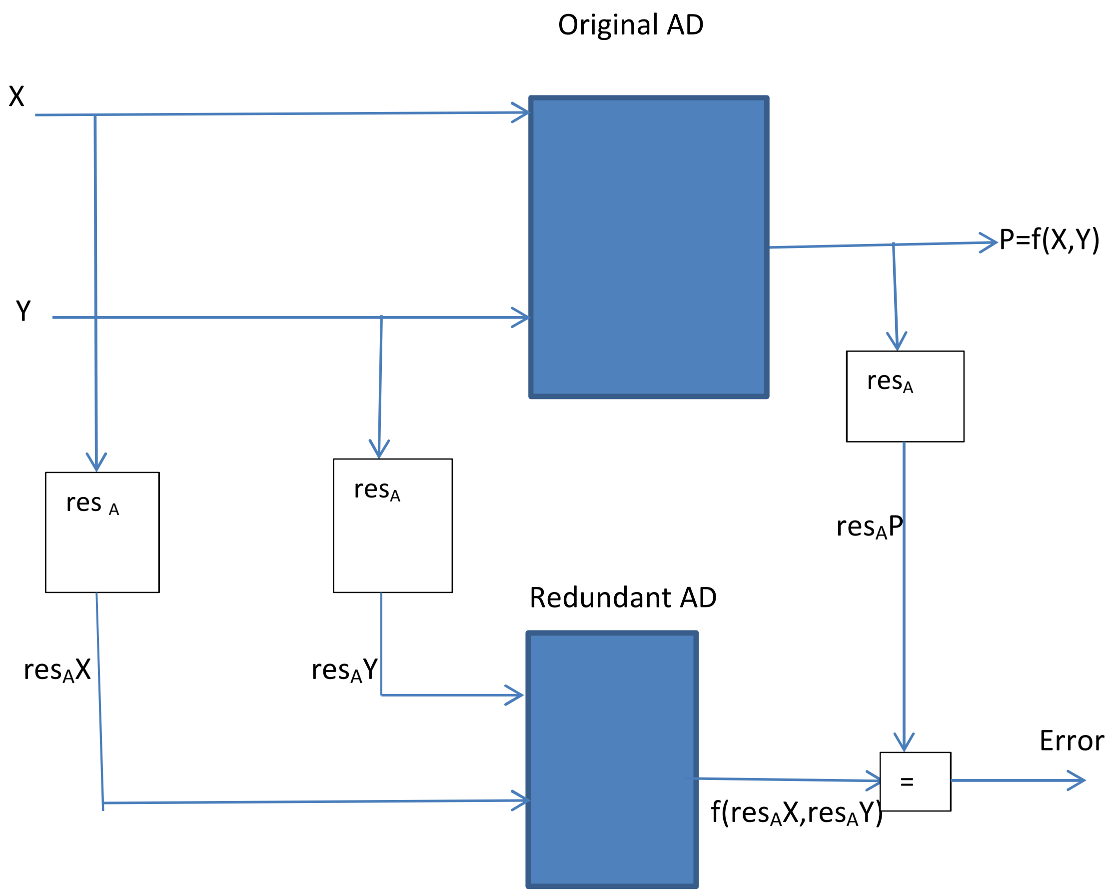
Theorem. AN code is perfect SEC code iff 2 is primitive modulo A.

Hardware Implementations of Nonsystematic Arithmetical Codes



Hardware Implementations of Systematic Arithmetical Codes

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



Low cost AN codes

division is not required to compute $res_A X$

Denote: $q=A-1$. Represent X with radix q

$$X=\sum_{i=0}^{m} X_i q^i \text{ where } X_i \text{ belongs to } \{0,1,\ldots,q-1\}.$$

Then $res_A X= res_A X_0+ res_A X_1+\ldots+ res_A X_m=X_0+X_1+\ldots X_m$ since $res_A X_i=X_i$

Or

$q=A+1$. Represent X with radix q

$$X=\sum_{i=0}^{m} X_i q^i \text{ where } X_i \text{ belongs to } \{0,1,\ldots,q-1\}.$$

Then $res_A X= res_A X_0- res_A X_1+ res_A X_2- res_A X_3+\ldots+ res_A X_m=X_0+X_1+\ldots X_m$ where $res_A X_i=X_i$ if $X_i<q-1$, $res_A X_i=0$ if $X_i=q-1$

For $q=2^s$

$A= 2^s+1$ or $A=2^s-1$.

If $A= 2^s+1$ then $res_A (2^s)=-1$ and If $A= 2^s-1$ then $res_A (2^s)=1$

Example1 . A=31, s=5 , n=15

$$\text{Let } X=\sum_{i=0}^{14} x_i 2^i=\sum_{i=0}^{4} x_i 2^i + 2^5 \sum_{i=5}^{9} x_{i+5}\, 2^i + 2^{10} \sum_{i=10}^{14} x_{i+10}\, 2^i=$$

$$=X_0+2^5X_1+2^{10}X_2 \text{ where } X_0, X_1, X_2 \text{ belong to } \{0,1,\ldots,31\}$$

Then

$res_{31}X= res_{31}X_0+ res_{31}X_1+ res_{31}X_2$ (mod31). $res_{31}X_i=X_i$ if $X_i<31$, and $res_{31}X_i=0$ if $X_i=31$

Example 2. A=33, s=5, n=15

Let X=$\sum_{i=0}^{14} x_i 2^i$=$\sum_{i=0}^{4} x_i 2^i + 2^5 \sum_{i=5}^{9} x_{i+5}\, 2^i + \ 2^{10} \sum_{i=10}^{14} x_{i+10}\, 2^i$=

=$X_0+2^5X_1+2^{10}X_2$ where X_0, X_1,X_2 belong to {0,1,…,31}

Then

$res_{33}X= res_{33}X_0 - res_{33}X_1+ res_{33}X_2 = X_0+X_1+X_2 \pmod{33}$