Secure Data Transmission: The Mathematics Behind Identification Numbers and Check Digit Schemes

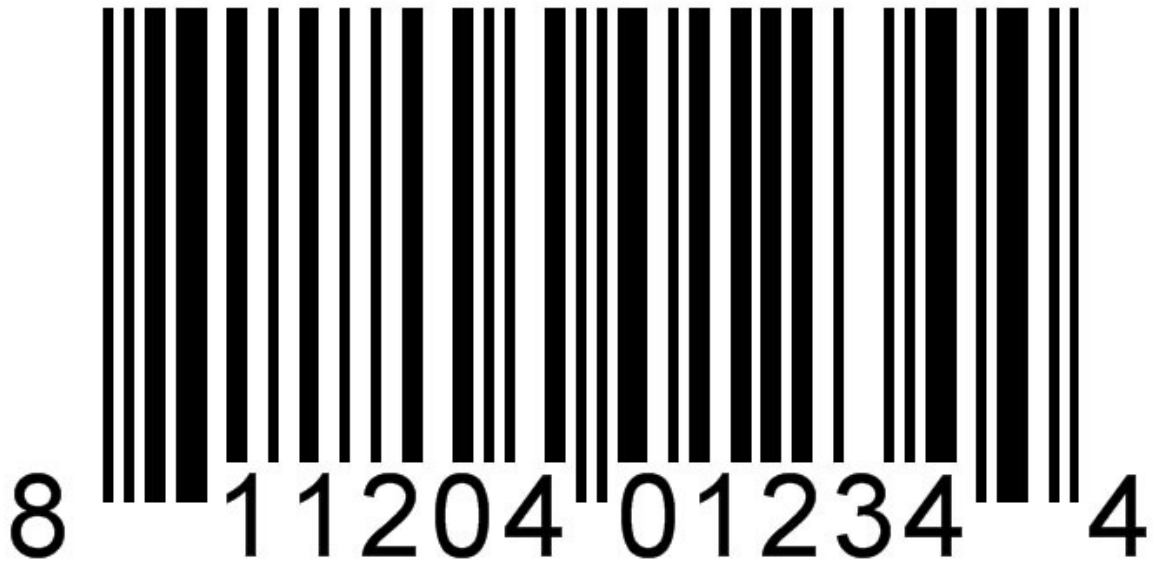
Joseph Kirtland

Marist College

Meeting of the Poughkeepsie Chapter of the ACM
Marist College
April 18, 2016

US Postal Money Order

Universal Product Code - UPC



Vehicle Identification Number & State of Washington Driver's License Number

1 G 1 Y Z 2 3 J 9 P 5 8 0 0 0 0 1

ISBN/EAN/ISBN-13

Credit Card Numbers

German Bank Note

Transmission Errors

$$\underline{728166153146}$$

$$728166753146$$

$$721866153146$$

$$721866113546$$

$$728199153146$$

Common Error Patterns

Error Type	**Form**	**Relative Frequency**
single digit error	$a \to b$	79.1%
transposition of adjacent digits	$ab \to ba$	10.2%
jump transposition	$abc \to cba$	0.8%
twin error	$aa \to bb$	0.5%
phonetic error*	$a0 \leftrightarrow 1a$	0.5%
jump twin error	$aca \to bcb$	0.3%

*For $a = 2, 3, 4, 5, 6, 7, 8, 9$.

Modulo Arithmetic

Let x and n be integers with $n > 0$. The remainder r obtained when x is divided by n is denoted by **x (mod n)** where $0 \leq r \leq n - 1$.

Let n be a positive integer. Given two integers x and y, then **x is congruent to y modulo n**, denoted **x $\equiv$ y (mod n)**, if x and y have the same remainder when divided by n.

US Postal Money Order

General Form: $a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11}$

- Document Number: $a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10}$
- Check Digit: a_{11}

$$a_{11} = (a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10}) \pmod 9$$

Valid Number: 67021200988

$$\begin{aligned}(6 + 7 + 0 + 2 + 1 + 2 + 0 + 0 + 9 + 8) \pmod 9 &= 35 \pmod 9 \\ &= 8\end{aligned}$$

Detection Rate

$$dr = \frac{\text{number of ways an error is detected}}{\text{number of ways to make an error}}$$

Single Digit Errors ($a \to b$): 10 choices for a and 9 choices for b resulting in 90 possible ways.

Transposition of Adjacent Digit Errors ($ab \to ba$): 10 choices for a and 9 choices for b resulting in 90 possible ways.

Detection Rate - USPMO

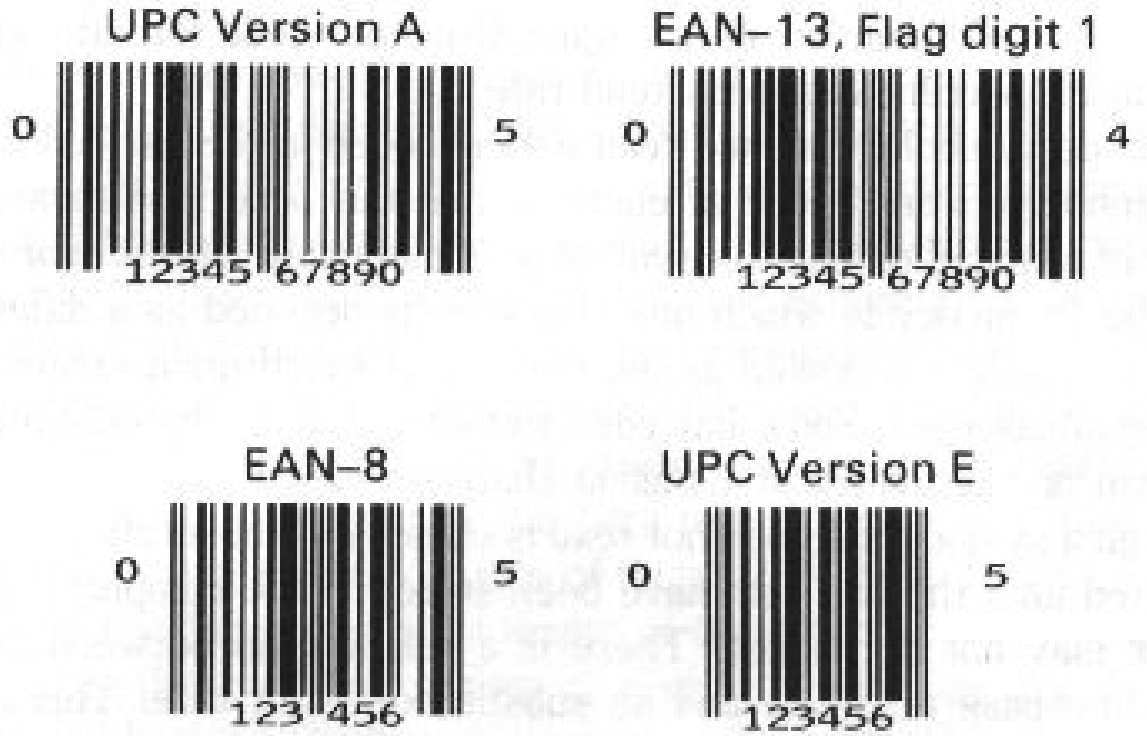
Single Digit Errors:

$$dr = \frac{88}{90} = 98\%$$

Transposition of Adjacent Digit Errors:

$$dr = \frac{0}{90} = 0\%$$

UPC and EAN


UPC Version A
0
5
12345 67890
EAN–13, Flag digit 1
0
4
12345 67890
EAN–8
0
5
123 456
UPC Version E
0
5
123456

UPC Version A

General Form: $a_1 - a_2a_3a_4a_5a_6 - a_7a_8a_9a_{10}a_{11} - a_{12}$

- a_1 - number system character
- $a_2a_3a_4a_5a_6$ - company number
- $a_7a_8a_9a_{10}a_{11}$ - product number
- a_{12} - check digit

$$3a_1 + a_2 + 3a_3 + a_4 + 3a_5 + a_6 + 3a_7 + a_8 + 3a_9 + a_{10} + 3a_{11} + a_{12} \equiv 0 \pmod{10}$$

No. System Char: 0 - General Groceries; 2 - Meat, Produce, Weight Items; 3 - Drugs and Health Products; 4 - In-Store Items; 5 - Coupons; 6,7 - Other Items;

UPC Version A

ID Number: 5-02003-91562 UPC: 5-02003-91562-C

$$3{\cdot}5 + 0 + 3{\cdot}2 + 0 + 3{\cdot}0 + 3 + 3{\cdot}9 + 1 + 3{\cdot}5 + 6 + 3{\cdot}2 + C = 0 \pmod{10}$$
$$15 + 0 + 6 + 0 + 0 + 3 + 27 + 1 + 15 + 6 + 6 + C = 0 \pmod{10}$$
$$79 + C = 0 \pmod{10}$$

Thus $C = 1$ and the UPC is 5-02003-91562-1.

UPC Version A - Single Digit Errors

The UPC Check Digit Scheme catches all single digit errors.

$$\ldots a \ldots \rightarrow \ldots b \ldots$$

$$c + 3a = 0 \pmod{10} \qquad \& \qquad c + 3b = 0 \pmod{10}$$

$$\begin{aligned}
(c + 3a) - (c + 3b) &= 0 \pmod{10} \\
3a - 3b &= 0 \pmod{10} \\
3(a - b) &= 0 \pmod{10} \\
a - b &= 0 \pmod{10} \\
a &= b
\end{aligned}$$

UPC Version A - Transposition of Adjacent Digit Errors

The UPC Check Digit Scheme does not catch all transposition of adjacent digit errors.

$$\ldots ab \ldots \rightarrow \ldots ba \ldots$$

$$c + 3a + b = 0 \pmod{10} \qquad \& \qquad c + 3b + a = 0 \pmod{10}$$

$$\begin{aligned} (c + 3a + b) - (c + 3b + a) &= 0 \pmod{10} \\ 2a - 2b &= 0 \pmod{10} \\ 2(a - b) &= 0 \pmod{10} \end{aligned}$$

Undetected when $|a - b| = 5$.

UPC Version A - Detection Rates

Single Digit Errors:

$$dr = \frac{90}{90} = 100\%$$

Transposition of Adjacent Digit Errors:

$$dr = \frac{80}{90} = 89\%$$

Weighted Sums - Mod 10

$$\sum_{i=1}^{n} w_i a_i = 0 \pmod{10}$$

$$w_1 a_1 + w_2 a_2 + \cdots + w_n a_n = 0 \pmod{10}$$

w_i - weights

a_i - digits in the identification number

catch all single digits errors	w_i relatively prime to 10
catch all transposition of adjacent digit errors	$w_{i+1} - w_i$ relatively prime to 10

Weighted Sums in General

$$\sum_{i=1}^{n} w_i a_i = 0 \pmod{M}$$

$$w_1 a_1 + w_2 a_2 + \cdots + w_n a_n = 0 \pmod{M}$$

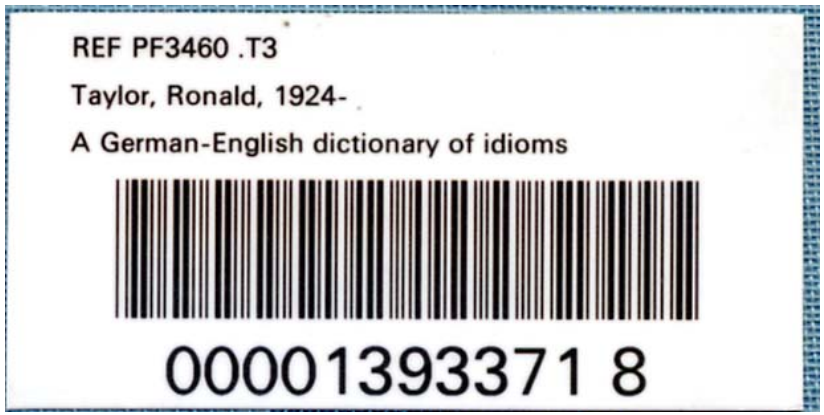
w_i - weights

a_i - digits in the identification number

catch all single digits errors	w_i relatively prime to M
catch all transposition of adjacent digit errors	$w_{i+1} - w_i$ relatively prime to M

IBM Scheme


BRITISH AIRWAYS
4417 1234 5678 9112
CARDMEMBER SINCE 1999
GOOD THRU 00/00
D. WALDEN
EXECUTIVE CLUB # 12345678
VISA
SIGNATURE


REF PF3460 .T3
Taylor, Ronald, 1924-
A German-English dictionary of idioms
00001393371 8

IBM Scheme

$$\sigma(a) = \begin{cases} 2a & \text{if } 0 \leq a \leq 4 \\ 2a - 9 & \text{if } 5 \leq a \leq 9 \end{cases} \qquad = 2a + \left\lfloor \frac{2a}{10} \right\rfloor \pmod{10}$$

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & 9 \end{pmatrix}$$

General Form : $a_1 a_2 \cdots a_{n-1} a_n$

n-even:

$$\sigma(a_1) + a_2 + \sigma(a_3) + a_4 + \cdots + \sigma(a_{n-1}) + a_n = 0 \pmod{10}$$

n-odd:

$$a_1 + \sigma(a_2) + a_3 + \sigma(a_4) + \cdots + \sigma(a_{n-1}) + a_n = 0 \pmod{10}$$

IBM Scheme

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & 9 \end{pmatrix}$$

Specific Number: 1324136 9

$$\begin{aligned} \sigma(1) + 3 + \sigma(2) + 4 + \sigma(1) + 3 + \sigma(6) + 9 \pmod{10} & \\ = 2 + 3 + 4 + 4 + 2 + 3 + 3 + 9 \pmod{10} & \\ = 30 \pmod{10} & \\ = 0 & \end{aligned}$$

IBM Scheme - Single Digit Errors

The IBM Scheme catches all single digit errors.

$$\ldots a \ldots \rightarrow \ldots b \ldots$$

$$c + \sigma(a) = 0 \pmod{10} \qquad \& \qquad c + \sigma(b) = 0 \pmod{10}$$

$$\begin{aligned}
(c + \sigma(a)) - (c + \sigma(b)) &= 0 \pmod{10} \\
\sigma(a) - \sigma(b) &= 0 \pmod{10} \\
\sigma(a) &= \sigma(b) \pmod{10} \\
\sigma(a) &= \sigma(b) \\
a &= b
\end{aligned}$$

IBM Scheme - Transposition of Adjacent Digit Errors

The IBM Scheme does not catch all transposition of adjacent digit errors.

$$\ldots ab \ldots \rightarrow \ldots ba \ldots$$

$$c+\sigma(a)+b = 0 \pmod{10} \qquad \& \qquad c+\sigma(b)+a = 0 \pmod{10}$$

$$\begin{aligned} (c+\sigma(a)+b)-(c+\sigma(b)+a) &= 0 \pmod{10} \\ \sigma(a)-a-\sigma(b)+b &= 0 \pmod{10} \\ \sigma(a)-a &= \sigma(b)-b \pmod{10} \end{aligned}$$

Undetected when $a = 0, b = 9$ or $a = 9, b = 0$.

IBM Scheme - Transposition of Adjacent Digit Errors

$0 \leq a \leq 4$	$5 \leq b \leq 9$
$\sigma(a) - a \pmod{10}$	$\sigma(b) - b \pmod{10}$
$2a - a \pmod{10}$	$2b - 9 - b \pmod{10}$
$a \pmod{10}$	$b - 9 \pmod{10}$
	$b + 1 \pmod{10}$
0	9

IBM Scheme - Transposition of Adjacent Digit Errors

$$\sigma(0) - 0 = 0 - 0 = 0$$
$$\sigma(1) - 1 = 2 - 1 = 1$$
$$\sigma(2) - 2 = 4 - 2 = 2$$
$$\sigma(3) - 3 = 6 - 3 = 3$$
$$\sigma(4) - 4 = 8 - 4 = 4$$
$$\sigma(5) - 5 = 1 - 5 = 6$$
$$\sigma(6) - 6 = 3 - 6 = 7$$
$$\sigma(7) - 7 = 5 - 7 = 8$$
$$\sigma(8) - 8 = 7 - 8 = 9$$
$$\sigma(9) - 9 = 9 - 9 = 0$$

IBM Detection Rates

Single Digit Errors:

$$dr = \frac{90}{90} = 100\%$$

Transposition of Adjacent Digit Errors:

$$dr = \frac{88}{90} = 98\%$$

A Theorem by Gumm, 1985

Suppose an error detecting scheme with an even modulus detects all single digit errors. Then for every i and j there is a transposition error involving positions i and j that cannot be detected.

$$a_1 \cdots a_i \cdots a_j \cdots a_n \to a_1 \cdots a_j \cdots a_i \cdots a_n$$

Proof:

- Let $2m$ be the even modulus.
- For $a_1 a_2 \cdots a_n$, the CDS is

$$\sigma_1(a_1) + \sigma_2(a_2) + \cdots \sigma_n(a_n) = 0 \pmod{2m}$$

- To catch all single digit errors, each σ_i must be a permutation of $\mathbb{Z}_{2m} = \{0, 1, 2, \ldots, 2m-1\}$.

A Theorem by Gumm, 1985

- To detect all transposition errors involving positions i and j ($\ldots a \ldots b \ldots \to \ldots b \ldots a \ldots$, $a \neq b$), we must have

$$\sigma_i(a) + \sigma_j(b) \neq \sigma_i(b) + \sigma_j(a)$$

or

$$\sigma_j(b) - \sigma_i(b) \neq \sigma_j(a) - \sigma_i(a)$$

- In this case, the map $\sigma(x) = \sigma_j(x) - \sigma_i(x)$ is a permutation of $\mathbb{Z}_{2m}$.

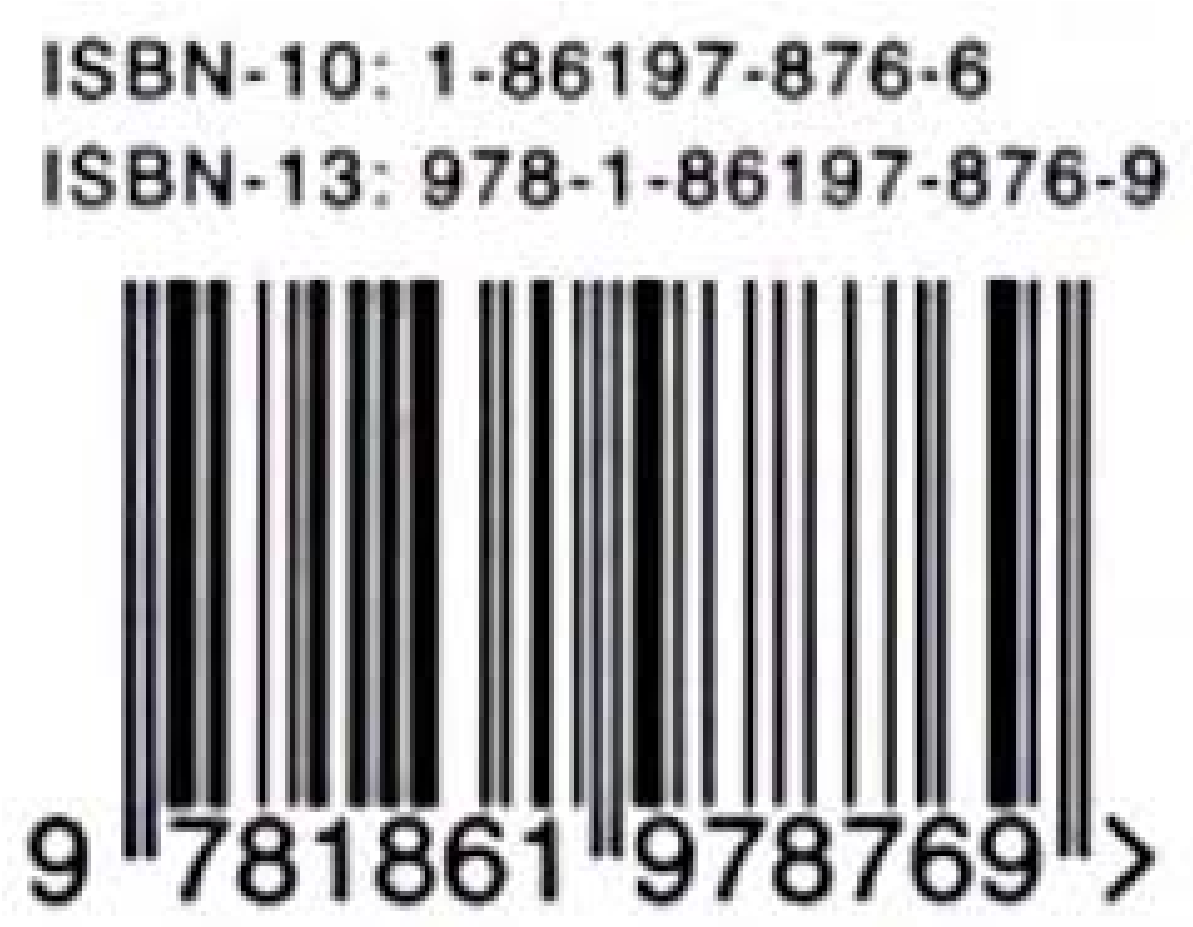
A Theorem by Gumm, 1985

- Summing the elements of $\mathbb{Z}_{2m}$ (mod $2m$) obtains

$$\begin{aligned} m &= m + 0 + (1 + 2m - 1) + (2 + 2m - 2) + \ + (m - 1 + m + 1) \\ &= \sum x \\ &= \sum \sigma(x) \\ &= \sum (\sigma_j(x) - \sigma_i(x)) \\ &= \sum \sigma_j(x) - \sum \sigma_i(x) \\ &= m - m \\ &= 0 \end{aligned}$$

This is a contradiction.

ISBN...ISBN-10...ISBN-13...EAN-13...EAN



ISBN-10

General Form: $a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10}$

- $a1\ldots$: group/country number (0,1=English, 3=German, 9978=Ecuador)
- $a_i \ldots a_j$: publisher number
- $a_{j+1} \ldots a_9$: serial number
- a_{10}: check digit

$$10 \cdot a_1 + 9 \cdot a_2 + 8 \cdot a_3 + 7 \cdot a_4 + 6 \cdot a_5 + 5 \cdot a_6 + 4 \cdot a_7 + 3 \cdot a_8 + 2 \cdot a_9 + 1 \cdot a_{10} \equiv 0 \pmod{11}$$

If $a_{10} = 10$, the letter X is used.

ISBN-10

ISBN-10: 1-86197-876-6

$$10{\cdot}1 + 9{\cdot}8 + 8{\cdot}6 + 7{\cdot}1 + 6{\cdot}9 + 5{\cdot}7 + 4{\cdot}8 + 3{\cdot}7 + 2{\cdot}6 + 1{\cdot}6 \equiv 0 \pmod{11}$$

$$10 + 72 + 48 + 7 + 54 + 35 + 32 + 21 + 12 + 6 \equiv 0 \pmod{11}$$

$$297 = 17{\cdot}11 \equiv 0 \pmod{11}$$

ISBN-10 Detection Rates

Single Digit Errors:

$$dr = \frac{90}{90} = 100\%$$

Transposition of Adjacent Digit Errors:

$$dr = \frac{90}{90} = 100\%$$

But why don't we like this scheme?

German Banks

German banks use a mod 11 weighted scheme that does catch all of the errors from the first table and any transposition error when $n \leq 10$.

$$2a_1 + 2^2a_2 + 2^3a_3 + \cdots + 2^na_n = 0 \pmod{11}$$

Transposition involving position i and j where $1 \leq i < j \leq n$.

$$\ldots a \ldots b \ldots \rightarrow \ldots b \ldots a \ldots$$

$$c+2^ia+2^jb = 0 \pmod{11} \qquad \& \qquad c+2^ib+2^ja = 0 \pmod{11}$$

$$2^i(2^{j-i} - 1)b = 2^i(2^{j-i} - 1)a \pmod{11}$$

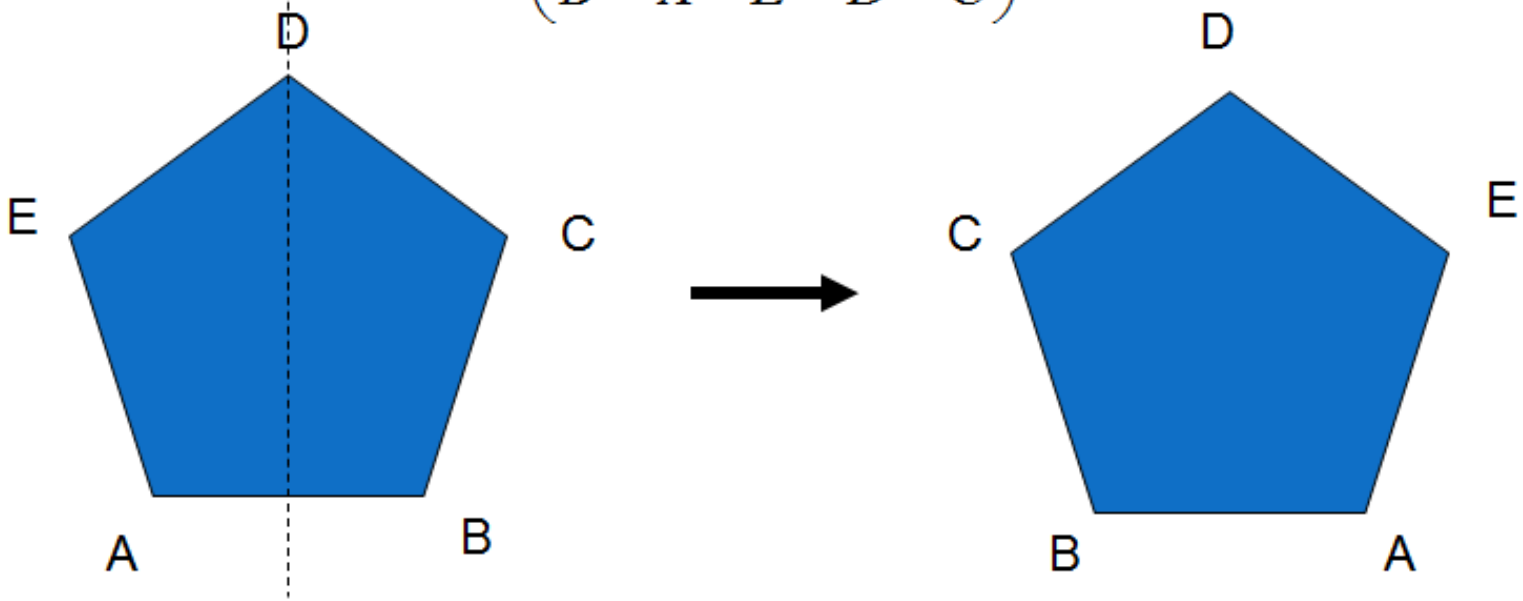
German Banks

$$2^1 - 1 = 1$$
$$2^2 - 1 = 3$$
$$2^3 - 1 = 7$$
$$2^4 - 1 = 15 = 3 \cdot 5$$
$$2^5 - 1 = 31$$
$$2^6 - 1 = 63 = 3^2 \cdot 7$$
$$2^7 - 1 = 127$$
$$2^8 - 1 = 255 = 3 \cdot 5 \cdot 17$$
$$2^9 - 1 = 511 = 7 \cdot 73$$
$$2^{10} - 1 = 1023 = 3 \cdot 11 \cdot 31$$

Symmetries of a Regular Pentagon

Reflection

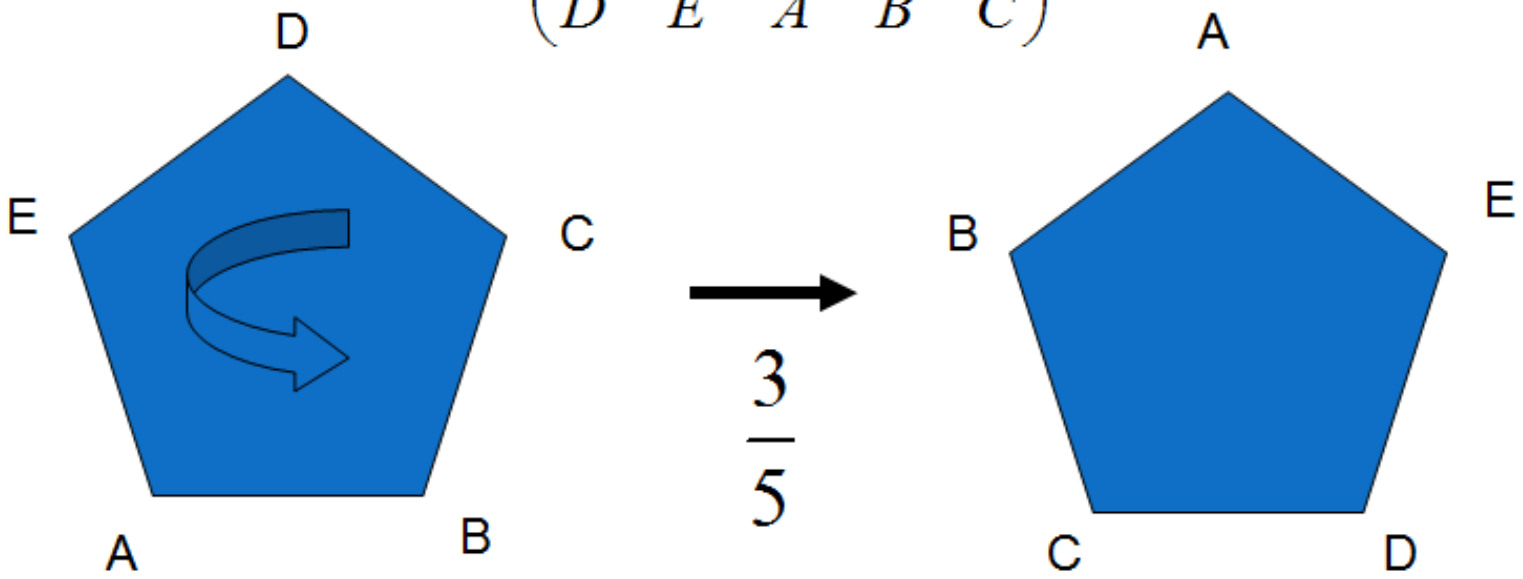
$$\begin{pmatrix} A & B & C & D & E \\ B & A & E & D & C \end{pmatrix}$$



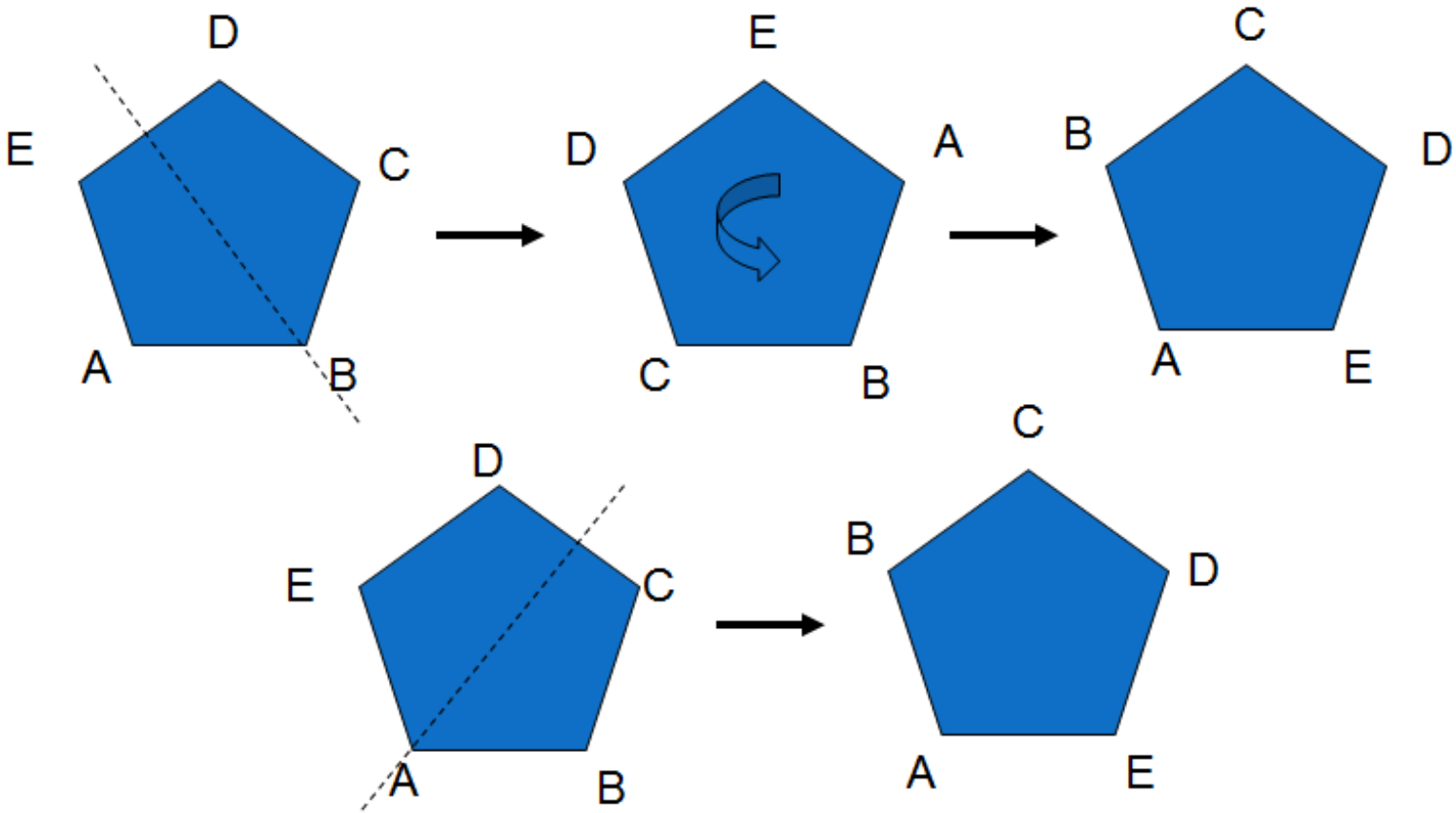
Symmetries of the Regular Pentagon

Rotations

$$\begin{pmatrix} A & B & C & D & E \\ D & E & A & B & C \end{pmatrix}$$



Symmetries of a Regular Pentagon



Symmetries of a Regular Pentagon

$$0 = \begin{pmatrix} A & B & C & D & E \\ A & B & C & D & E \end{pmatrix} \quad 1 = \begin{pmatrix} A & B & C & D & E \\ B & C & D & E & A \end{pmatrix}$$

$$2 = \begin{pmatrix} A & B & C & D & E \\ C & D & E & A & B \end{pmatrix} \quad 3 = \begin{pmatrix} A & B & C & D & E \\ D & E & A & B & C \end{pmatrix}$$

$$4 = \begin{pmatrix} A & B & C & D & E \\ E & A & B & C & D \end{pmatrix} \quad 5 = \begin{pmatrix} A & B & C & D & E \\ A & E & D & C & B \end{pmatrix}$$

$$6 = \begin{pmatrix} A & B & C & D & E \\ E & D & C & B & A \end{pmatrix} \quad 7 = \begin{pmatrix} A & B & C & D & E \\ D & C & B & A & E \end{pmatrix}$$

$$8 = \begin{pmatrix} A & B & C & D & E \\ C & B & A & E & D \end{pmatrix} \quad 9 = \begin{pmatrix} A & B & C & D & E \\ B & A & E & D & C \end{pmatrix}$$

The Multiplication Table for D_5

$8 * 3 = 5$ $\quad$ $3 * 8 = 6$ $\quad$ The operation is not commutative!

$*$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

The Verhoeff Scheme

- Number: $a_1 a_2 \cdots a_n$
- Permutation: $\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 4 & 3 & 2 & 1 & 6 & 7 & 8 & 9 & 5 \end{pmatrix}$ not unique

  Any permutation works as long as

$$\sigma(a) * b \neq \sigma(b) * a \qquad \text{for } a \neq b.$$

- $*$ is the group operation from D_5.

$$\sigma^{n-1}(a_1) * \sigma^{n-2}(a_2) * \sigma^{n-3}(a_3) * \cdots * \sigma(a_{n-1}) * a_n = 0$$

The Verhoeff Scheme

Note: Since σ is a permutation, for each $i \in \mathbb{N}$, σ^i is also a permutation.

$$\sigma^3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 4 & 3 & 2 & 1 & 6 & 7 & 8 & 9 & 5 \end{pmatrix} \circ$$

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 4 & 3 & 2 & 1 & 6 & 7 & 8 & 9 & 5 \end{pmatrix} \circ \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 4 & 3 & 2 & 1 & 6 & 7 & 8 & 9 & 5 \end{pmatrix}$$

$$\sigma^3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 4 & 3 & 2 & 1 & 8 & 9 & 5 & 6 & 7 \end{pmatrix}$$

The Verhoeff Scheme - Single Digit Errors

Catches all single digit errors.

$$\ldots a \ldots \rightarrow \ldots b \ldots$$

$$c_1 * \sigma^i(a) * c_2 = 0 \qquad \& \qquad c_1 * \sigma^i(b) * c_2 = 0$$

$$\begin{aligned} c_1 * \sigma^i(a) * c_2 &= c_1 * \sigma^i(b) * c_2 \\ \sigma^i(a) * c_2 &= \sigma^i(b) * c_2 \\ \sigma^i(a) &= \sigma^i(b) \\ a &= b \end{aligned}$$

The Verhoeff Scheme - Transposition of Adj. Digit Errors

Catches all transposition of adjacent digit errors.

$$\ldots ab \ldots \rightarrow \ldots ba \ldots$$

$$c_1 * \sigma^{i+1}(a) * \sigma^i(b) * c_2 = 0 \qquad \& \qquad c_1 * \sigma^{i+1}(b) * \sigma^i(a) * c_2 = 0$$

$$\begin{aligned} c_1 * \sigma^{i+1}(a) * \sigma^i(b) * c_2 &= c_1 * \sigma^{i+1}(b) * \sigma^i(a) * c_2 \\ \sigma^{i+1}(a) * \sigma^i(b) * c_2 &= \sigma^{i+1}(b) * \sigma^i(a) * c_2 \\ \sigma^{i+1}(a) * \sigma^i(b) &= \sigma^{i+1}(b) * \sigma^i(a) \\ \sigma(\sigma^i(a)) * \sigma^i(b) &= \sigma(\sigma^i(b)) * \sigma^i(a) \end{aligned}$$

The Verhoeff Scheme

$$\sigma(\sigma^i(a)) * \sigma^i(b) = \sigma(\sigma^i(b)) * \sigma^i(a)$$

Since $a \neq b$, it follows that $\sigma^i(a) \neq \sigma^i(b)$. Let $c = \sigma^i(a)$ and $d = \sigma^i(b)$. Then

$$\sigma(\sigma^i(a)) * \sigma^i(b) = \sigma(\sigma^i(b)) * \sigma^i(a)$$
$$\sigma(c) * d = \sigma(d) * c$$

This is a contradiction.

The German Bundesbank Scheme

The German Bundesbank Scheme

- Number: $a_1 a_2 \cdots a_{11}$
- Permutation: $\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \end{pmatrix}$
-

A	D	G	K	L	N	S	U	Y	Z
0	1	2	3	4	5	6	7	8	9

- $*$ is the group operation from D_5.

$$\sigma(a_1) * \sigma^2(a_2) * \sigma^3(a_3) * \cdots * \sigma^{10}(a_{10}) * a_{11} = 0$$

The German Bundesbank Scheme

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \end{pmatrix}$$

$\text{DL0998939U1} \rightarrow 14099893971$

$$\sigma(1) * \sigma^2(4) * \sigma^3(0) * \sigma^4(9) * \sigma^5(9) * \sigma^6(8) *$$
$$\sigma^7(9) * \sigma^8(3) * \sigma^9(9) * \sigma^{10}(7) * 1 = 0$$
$$5 * 7 * 8 * 0 * 1 * 1 * 8 * 3 * 4 * 1 * 1 = 0$$
$$0 = 0$$

German Bundesbank Scheme

This scheme has one major problem, what is it?

Euro

An Error Correcting Scheme

Number: $a_1 a_2 \cdots a_8 a_9 a_{10}$ with a_9, a_{10} check digits.

$$a_1 + a_2 + \ldots + a_8 + a_9 + a_{10} = 0 \pmod{11}$$

$$a_1 + 2a_2 + \ldots + 8a_8 + 9a_9 + 10a_{10} = 0 \pmod{11}$$

An Error Correcting Scheme

$62150334a_9a_{10}$

$$a_1 + a_2 + \ldots + a_8 + a_9 + a_{10} = 0 \pmod{11}$$
$$6 + 2 + 1 + 5 + 0 + 3 + 3 + 4 + a_9 + a_{10} = 0 \pmod{11}$$
$$24 + a_9 + a_{10} = 0 \pmod{11}$$
$$2 + a_9 + a_{10} = 0 \pmod{11}$$

$$a_1 + 2a_2 + \ldots + 8a_8 + 9a_9 + 10a_{10} = 0 \pmod{11}$$
$$6 + 2\cdot 2 + 3\cdot 1 + 4\cdot 5 + 5\cdot 0 + 6\cdot 3 + 7\cdot 3 + 8\cdot 4 + 9\cdot a_9 + 10\cdot a_{10} = 0 \pmod{11}$$
$$104 + 9\cdot a_9 + 10\cdot a_{10} = 0 \pmod{11}$$
$$5 + 9\cdot a_9 + 10\cdot a_{10} = 0 \pmod{11}$$

An Error Correcting Scheme

$$6215033472 \rightarrow 6218033472$$

$$\begin{aligned} a_1 + a_2 + \ldots + a_8 + a_9 + a_{10} &\pmod{11} \\ 6 + 2 + 1 + 8 + 0 + 3 + 3 + 4 + 7 + 2 &\pmod{11} \\ 36 &\pmod{11} = 3 \end{aligned}$$

$$\begin{aligned} a_1 + 2a_2 + \ldots + 8a_8 + 9a_9 + 10a_{10} &= 3i \pmod{11} \\ 6 + 2\cdot 2 + 3\cdot 1 + 4\cdot 8 + 5\cdot 0 + 6\cdot 3 + 7\cdot 3 + 8\cdot 4 + 9\cdot 7 + 10\cdot 2 &= 3i \pmod{11} \\ 199 &= 3i \pmod{11} \\ 1 &= 3i \pmod{11} \\ i &= 4 \end{aligned}$$

References

- Gallian, J. A., The Mathematics of Identification Numbers, *College Mathematics Journal* 22(3), 1991, 194-202.
- Gallian, J.A., Error Detection Methods, *ACM Computing Surveys* 28(3), 1996, 504-517.
- Consortium for Mathematics and Its Applications, *For All Practical Purposes: Mathematical Literacy in Today's World*, 9th ed., W. H. Freeman, 2013.
- Kirtland, J. *Identification Numbers and Check Digit Schemes*, The Mathematical Association of America - Classroom Resource Materials Series, 2001.