Joseph Battaglia

Magnetic Stripe Technology

http://www.sephail.net
sephail@sephail.net
+1 201-406-2929

How It Started

- NYC 2600 Meeting
  - MetroCards: 'card bending' – how does it work?
  - Is it possible for us to read MetroCards?
- Observation
  - Passing a magnetic stripe over the head of an open cassette player produces a sound

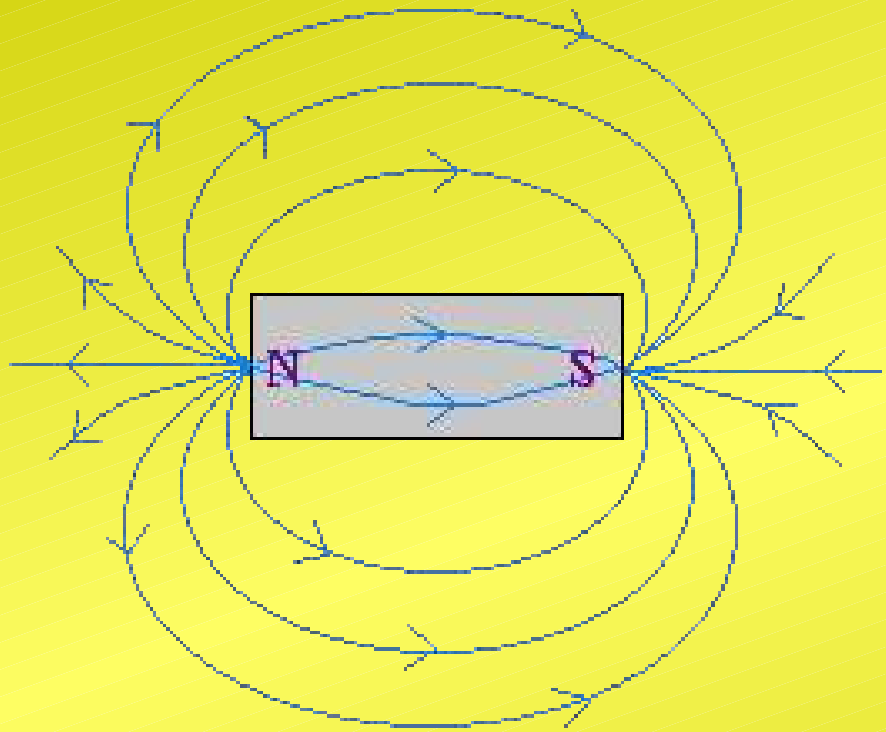
DEMO

- Idea
  - Interface to a sound card and write a software decoder

Magnetism Basics

- Magnetic poles
- Ferromagnetic materials (eg., iron)
- Coercivity (measured in Oersteds)
- Solenoids

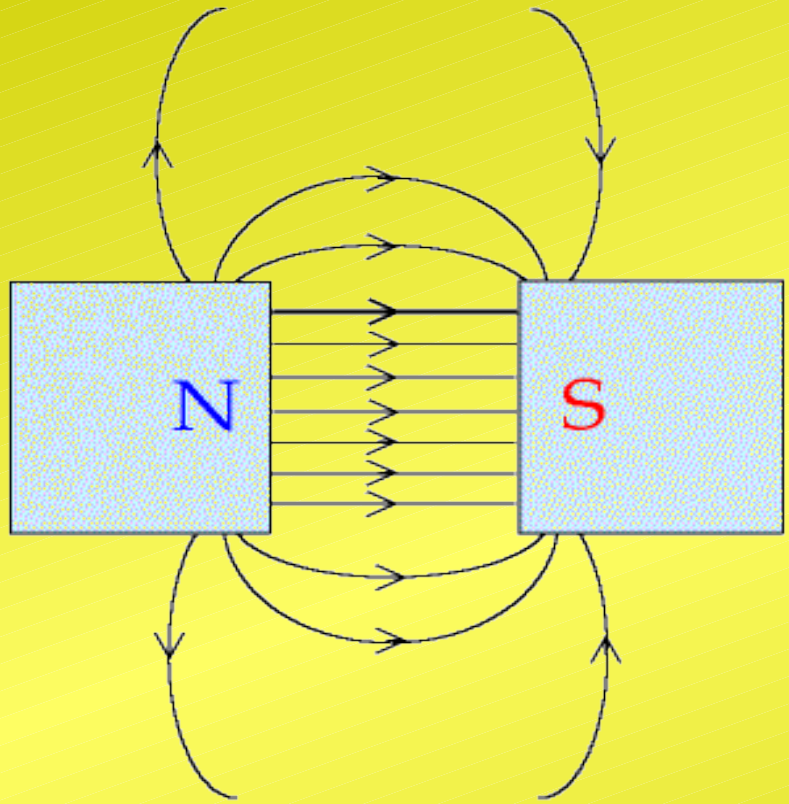
Magnetic Fields



- Magnetic field lines of a bar magnet run mostly horizontal (except at ends)
- An un-encoded magnetic stripe acts like a standard bar magnet

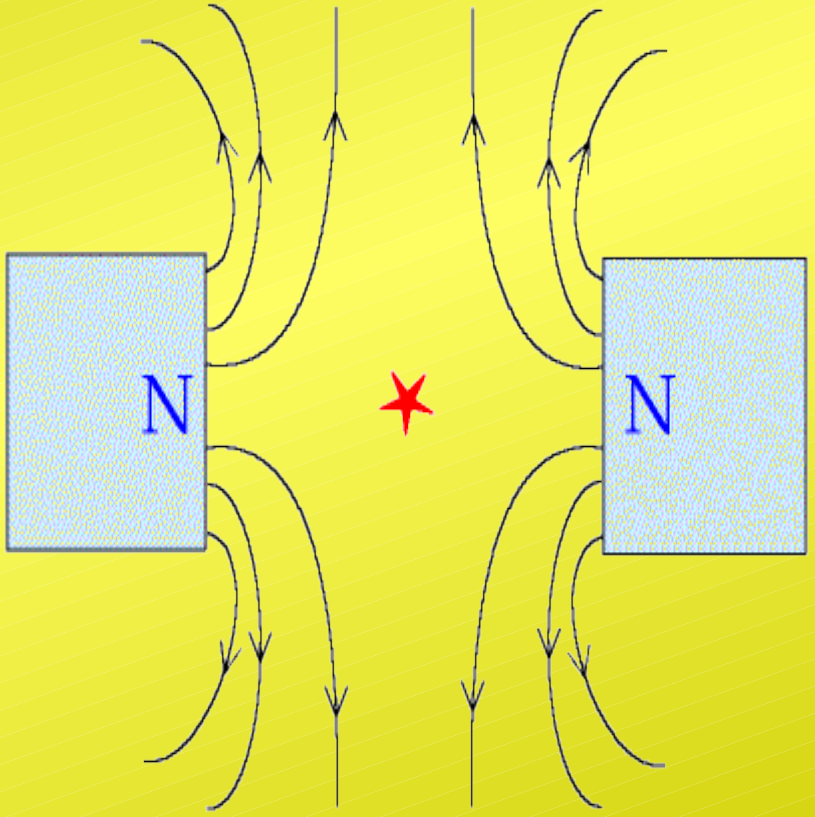
Flux Lines At Adjacent Poles

Attracting Poles



Horizontal Flux Lines

Poles which Repel



Vertical Flux Lines

How Magnetic Stripes Are Made

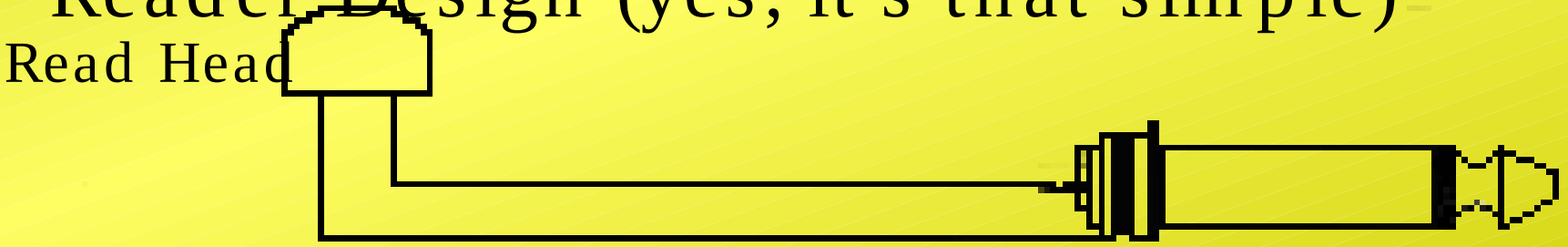
- Ferromagnetic particles are combined with a binder
- Particles are 'painted on' the stripe and held in alignment with an external magnetic field

How Magnetic Stripes Are Encoded

- A write head (solenoid) is used to 'flip' polarization of ferromagnetic materials
- Careful timing must be observed
  - Rollers can be used to move the card at a constant velocity or employ velocity correction for manual-swipe encoders

Waveform

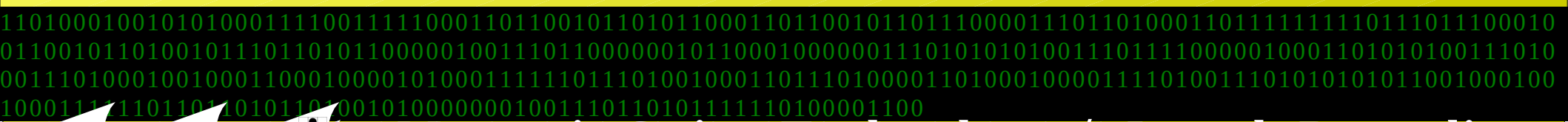
- Aiken Biphase
  - A form of Frequency Shift Keying (FSK)
  - Output frequencies (hand swipe) are well within audible frequency range (20 – 20,000Hz)
- Reader Design (yes, it's that simple)



DEMO

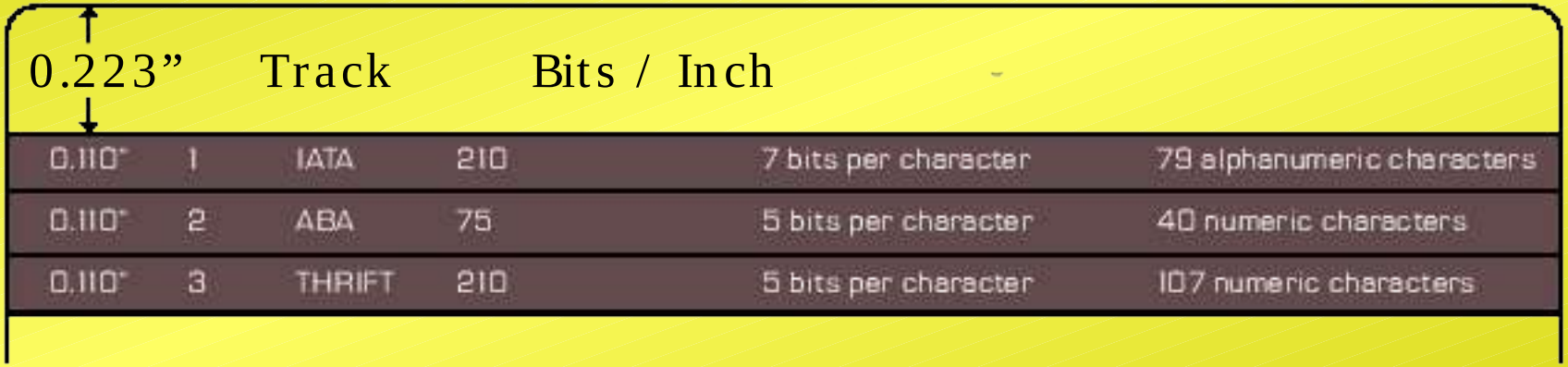
Benefits Of A Sound Card Interface

- Not dependent on the availability of a serial, parallel, PS/2, or game port
- All decoding is done in software – not limited to hardware capabilities
- Works with most laptops
- It's cheap!



Standard Encoding

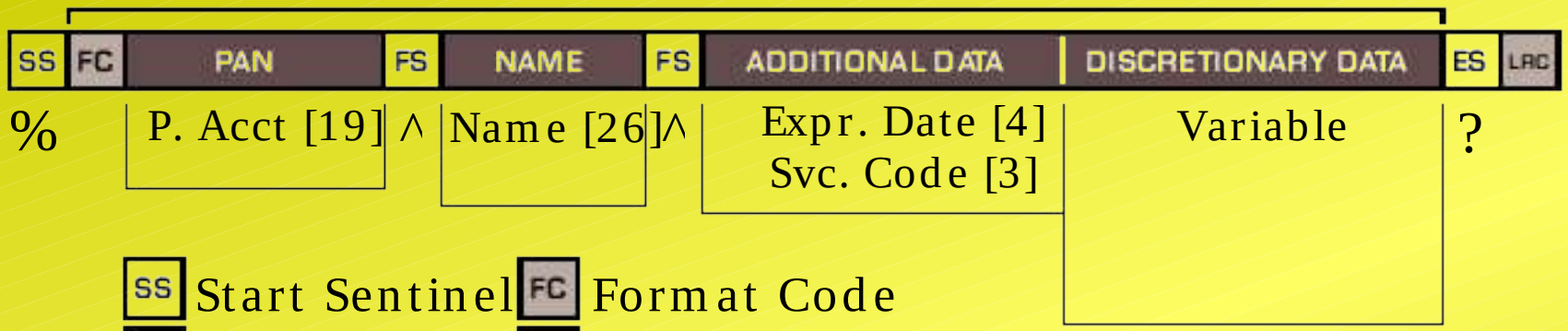
- ISO Specifications: 7811, 7813, and 4909



0.223”	Track	Bits / Inch		
0.110”	1	IATA	210	7 bits per character	79 alphanumeric characters
0.110”	2	ABA	75	5 bits per character	40 numeric characters
0.110”	3	THRIFT	210	5 bits per character	107 numeric characters

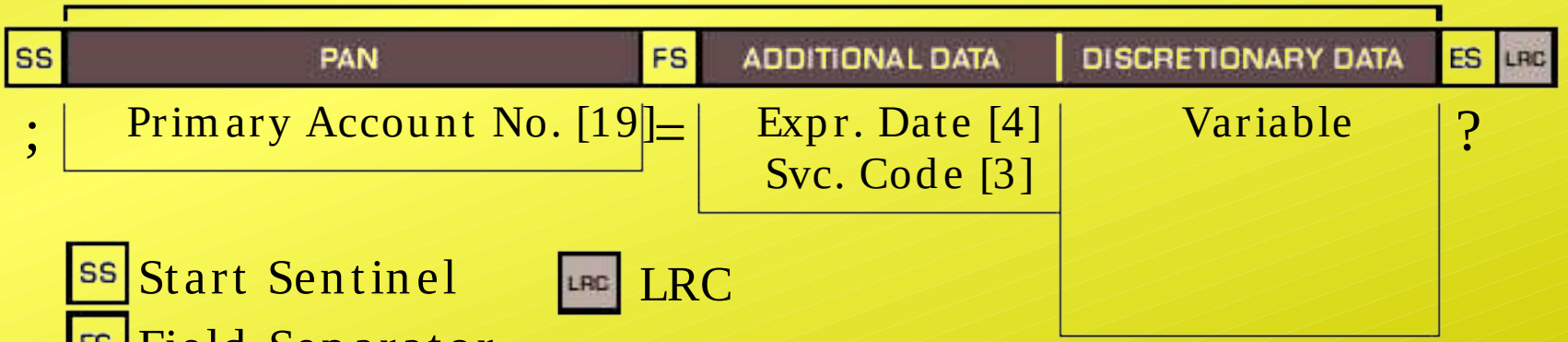
Typical Financial Card Data

Track 1



SS Start Sentinel
FC Format Code
FS Field Separator
LRC LRC
ES End Sentinel

Track 2

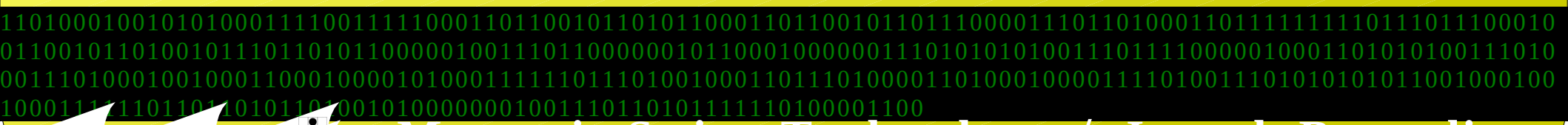


SS Start Sentinel
FS Field Separator
ES End Sentinel
LRC LRC

Reverse Engineering

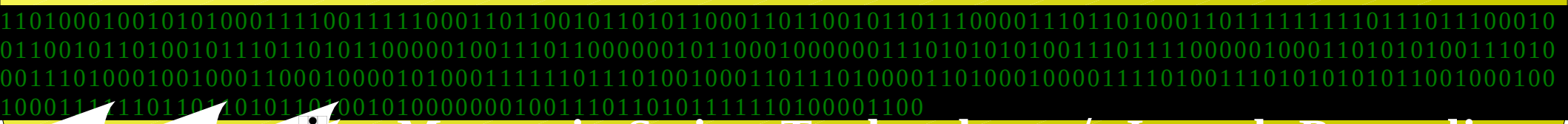
- MetroCards do not conform to any known standards
- How do you read cards without knowing how data is encoded onto them?

DEMO



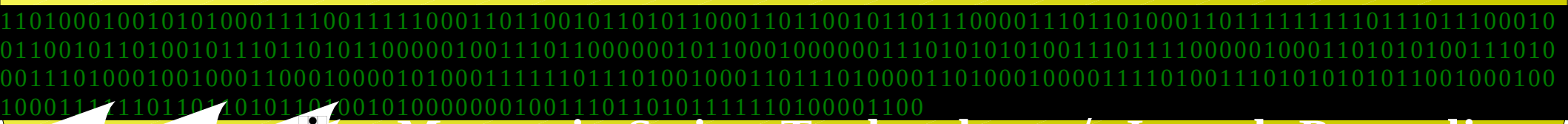
MetroCard Track 3

	Content	Offset	Length
1:	Start Sentinel	0	15
2:	Card Type	15	4
3:	Unknown	19	4
4:	Expiration Date	23	12
5:	Unknown	35	4
6:	Constant	39	8
7:	Unknown	47	8
8:	Serial Number	55	80
9:	Unused	135	16
A:	Unknown	151	16
B:	End Sentinel	167	93



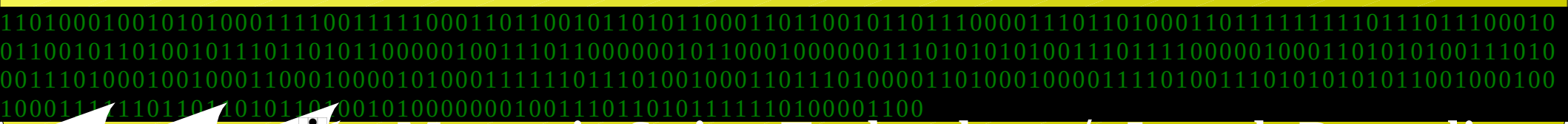
MetroCard Track 1-2

	Content	Offset	Length
1:	Start Sentinel	0	10
2:	Time	10	2
3:	Card Sub-Type	12	6
4:	Time	18	6
5:	Date	24	10
6:	Times Used	34	6
7:	Expiration Date	40	10
8:	Transfer Bit	50	1
9:	Last Used ID	51	15
A:	Card Value	66	16
B:	Purchase ID	82	16
C:	Unknown	98	20



Implications Of Software Readers

- Proprietary formats can be easily analyzed
- Poor “security through obscurity” models (e.g., the MetroCard) can be exploited
- Extremely cheap, small readers can be made



Articles / Software

- 2600 Magazine (Spring 2005)
  - New York City's MTA Exposed!
  - Magnetic Stripe Reading
- Article text and software
  - http://www.sephail.net/articles/magstripe
  - http://www.sephail.net/articles/metrocard