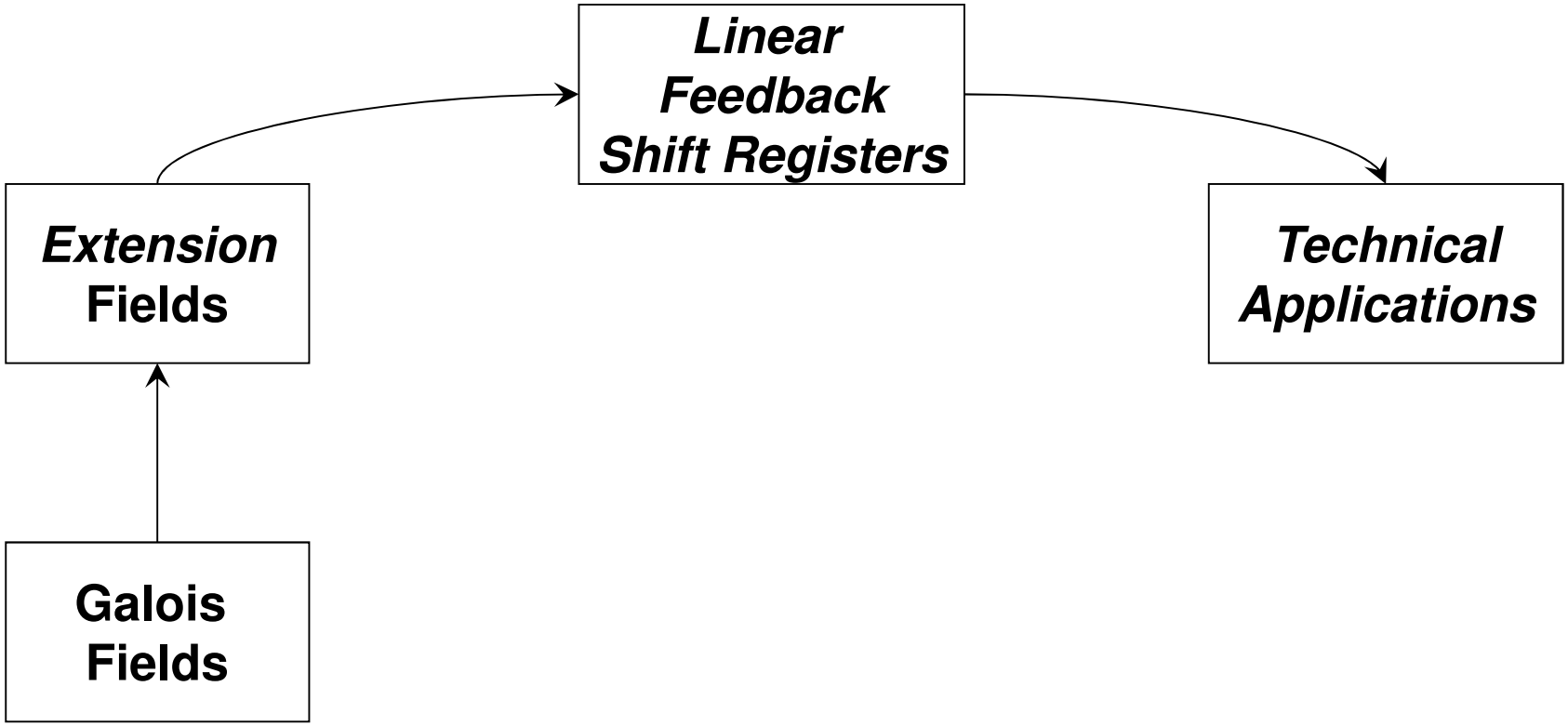
Galois Fields, Linear Feedback Shift Registers and their Applications

Prof. Dr.-Ing. Ulrich Jetzek
Kiel University of Applied Sciences, Germany
Institute for Communications Technology and Embedded Systems

17th International Symposium on
Ambient Intelligence and Embedded Systems
September 12th – 15th, 2018

Kiel University of Applied Sciences, Kiel, Germany

Bridge: Galois Fields → Technical Applications



Overview

- Galois fields over primes → Extension fields
- Linear Feedback Shift Register circuits derived from generator polynomials
- m-sequences and their properties
- GPS:
  - C/A (coarse-acquistion)-Code Generation
  - P(recision)-code
- GALILEO
  - Open Service Primary Code Generation
- Cryptography: Stream ciphers
  - A5/1 stream cipher used in GSM
- Cyclic Redundancy Check (CRC)

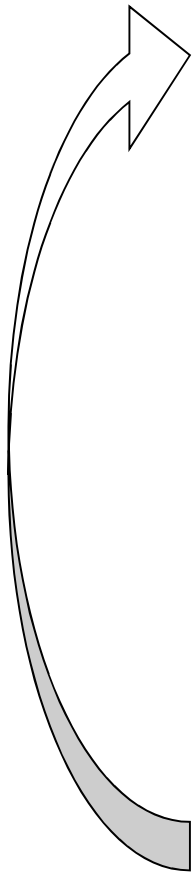
Galois Fields – Finite Fields over primes

- Galois Field
  - **Finite set of elements** $GF(p) = \{0,1,2, \dots, p-1\}$, where p is a prime together with
  - **Two operations ‚addition' and ‚multiplication'**, where each operation is performed $modulo\ p$.

- Main Properties of a Galois Field:
  - **Isolation:** Result of any addition or multiplication is an element of the given Galois Field.
  - **Inversion** – Any operation can be reverted:
    - **Additive Inverse:** For each field element there exists an additive inverse element, i.e. each addition can be reverted.
    - **Multiplicative Inverse:** For each field element except ‚0' there exists a mulitplicative inverse, i.e. each multiplication (except ‚0'-multiplication) can be reverted.

Example Galois Field $GF(11)$

- $GF(11) = \{0,1,2,3,4,5,6,7,8,9,10\}$
- **Generator:** field element, whose powers generates all field elements except ‚0‘.
- Example:
- Generator: $a = 2$



$$a^1 = 2$$
$$a^2 = a \cdot a = 4$$
$$a^3 = a^2 \cdot a = 8$$
$$a^4 = a^3 \cdot a = 16 \bmod 11 \equiv 5$$
$$a^5 = a^4 \cdot a = 5 \cdot 2 = 10$$
$$a^6 = a^5 \cdot a = 10 \cdot 2 = 20 \bmod 11 \equiv 9$$
$$a^7 = a^6 \cdot a = 9 \cdot 2 = 18 \bmod 11 \equiv 7$$
$$a^8 = a^7 \cdot a = 7 \cdot 2 = 14 \bmod 11 \equiv 3$$
$$a^9 = a^8 \cdot a = 3 \cdot 2 = 6$$
$$a^{10} = a^9 \cdot a = 6 \cdot 2 = 12 \bmod 11 \equiv 1$$
$$a^{11} = a^{10} \cdot a = 1 \cdot 2 = 2$$

Extension Fields $\boldsymbol{GF(2^m)}$

- Digital systems work bit-oriented (0;1) → $GF(2)$
- However: In most cases these systems work over groups of bits, often byte- or multi-byte-oriented.⇒
- $GF(2)$ will be extended towards a so-called Extension Field, $\boldsymbol{GF(2^m)}$.
- Each field element is (not an integer, but) a polynomial.

$$a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x^1 + a_0x^0$$
$$\text{with } a_i \in 0{,}1 \; for \; i = 0{,}1{,}2, \ldots, m-1$$

- Short notation:

$$(a_{m-1} \;\; a_{m-2} \;\; \ldots \;\; a_1 \;\; a_0) \; with \; a_i \in 0{,}1 \; for \; i = 0{,}1{,}2, \ldots, m-1$$

Extension Fields $GF(2^m)$

- Within prime fields: calculations modulo integer p
- Within Extension Fields: calculations modulo a specific polynomial, so-called generator polynomial $p(x)$
- For an Extension Field $GF(2^m)$ the generator polynomial always is a polynomial of degree m.

Ex.: Ext. Field $GF(2^4)$, generator: $p(x) = x^4 + x + 1$

$p(x) = x^4 + x + 1$ $\quad$ $by\ definition$: $\alpha^4 + \alpha + 1 := 0$

$$\alpha^4 \equiv \alpha + 1$$

$$\alpha^0 \equiv 0\cdot\alpha^3 + 0\cdot\alpha^2 + 0\cdot\alpha^1 + 0\cdot\alpha^0 \Leftrightarrow 0001$$

$$\alpha^1 \equiv 0\cdot\alpha^3 + 0\cdot\alpha^2 + 1\cdot\alpha^1 + 0\cdot\alpha^0 \Leftrightarrow 0010$$

$$\alpha^2 \equiv 0\cdot\alpha^3 + 1\cdot\alpha^2 + 0\cdot\alpha^1 + 0\cdot\alpha^0 \Leftrightarrow 0100$$

$$\alpha^3 \equiv 1\cdot\alpha^3 + 0\cdot\alpha^2 + 0\cdot\alpha^1 + 0\cdot\alpha^0 \Leftrightarrow 1000$$

$$\alpha^4 \equiv 0\cdot\alpha^3 + 0\cdot\alpha^2 + 1\cdot\alpha^1 + 1\cdot\alpha^0 \Leftrightarrow 10000 \equiv 0011$$

$$\alpha^5 \equiv 0\cdot\alpha^3 + 1\cdot\alpha^2 + 1\cdot\alpha^1 + 0\cdot\alpha^0 \Leftrightarrow 100000 \equiv 0110$$

$$\alpha^6 \equiv 1\cdot\alpha^3 + 1\cdot\alpha^2 + 0\cdot\alpha^1 + 0\cdot\alpha^0 \Leftrightarrow 1000000 \equiv 1100$$

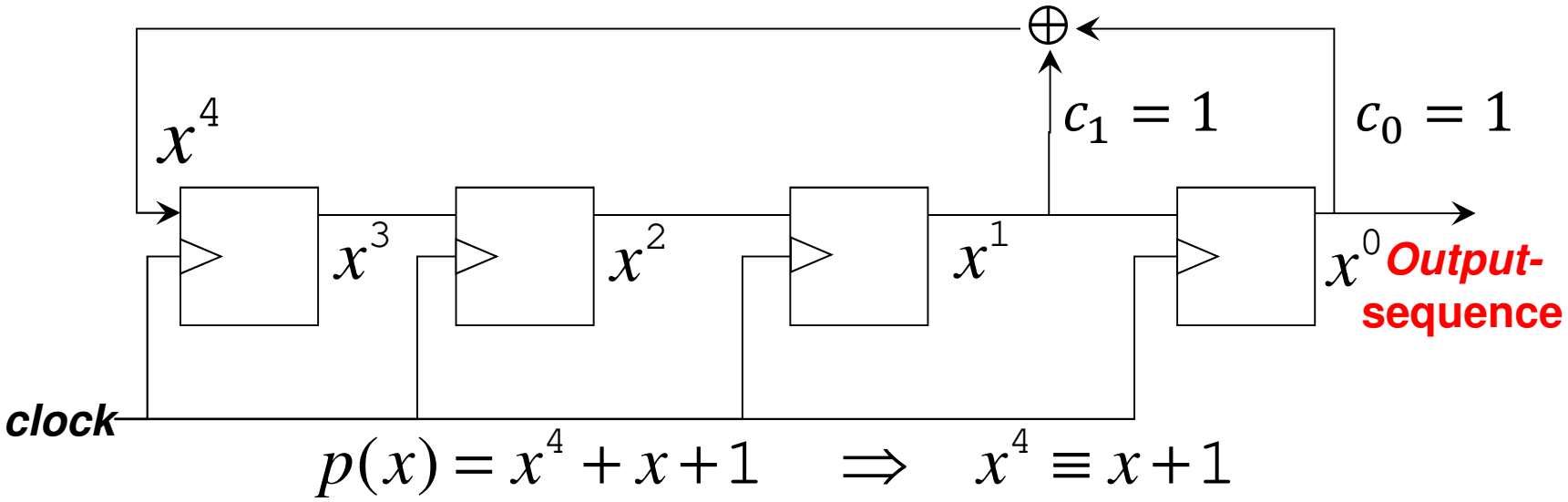
$$\vdots$$

$$\alpha^{14} \equiv 1\cdot\alpha^3 + 0\cdot\alpha^2 + 0\cdot\alpha^1 + 1\cdot\alpha^0 \Leftrightarrow 1\underbrace{0....0}_{14 zeros} \equiv 1001$$

$$\alpha^{15} \equiv 0\cdot\alpha^3 + 0\cdot\alpha^2 + 0\cdot\alpha^1 + 1\cdot\alpha^0 \Leftrightarrow 1\underbrace{0....0}_{15 zeros} \equiv 0001$$

Ex. LFSR for Ext. Fields $GF(2^4)$

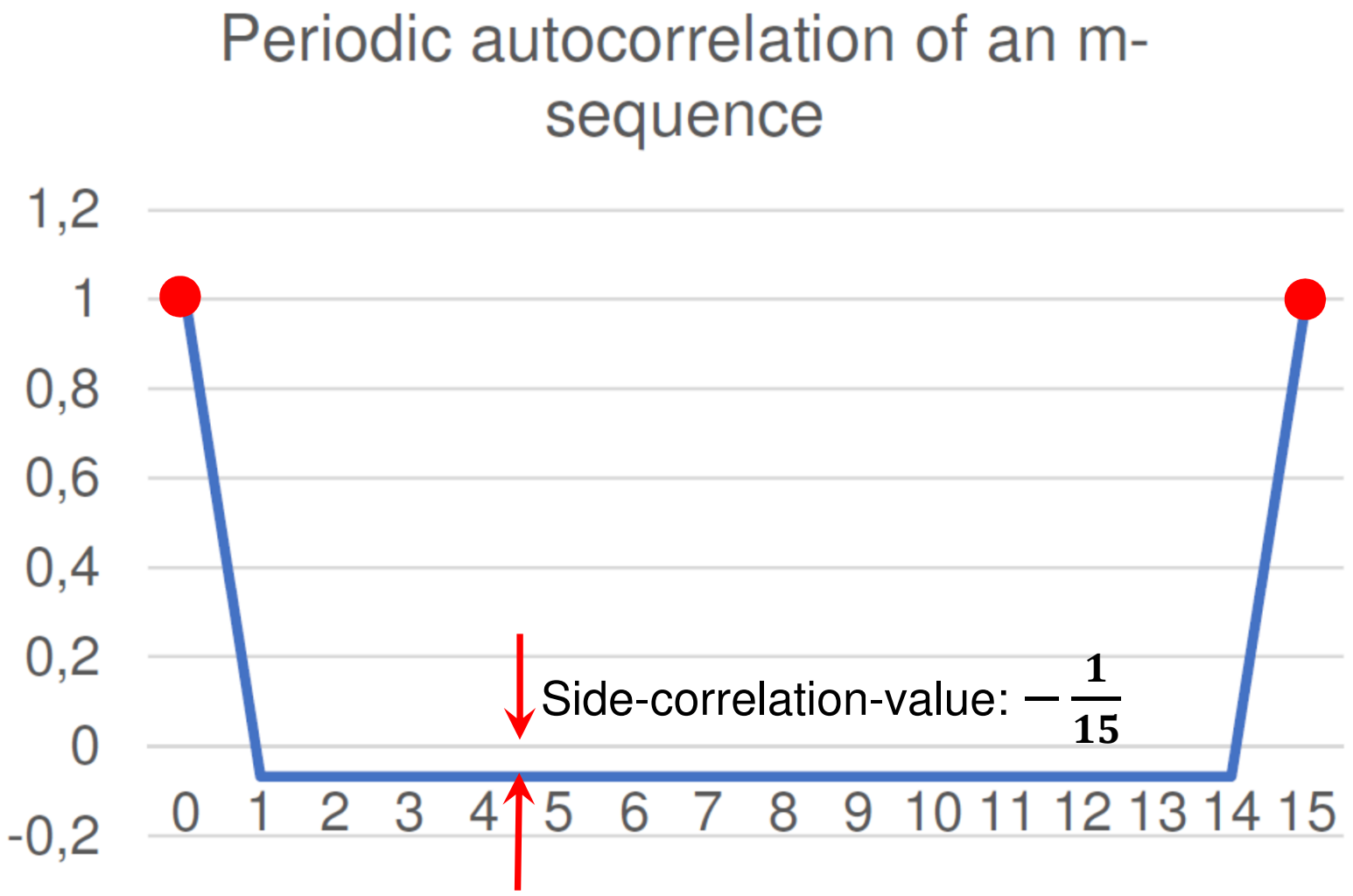
- Any generator polynomial can directly be transferred into a corresponding Linear Feedback Shift Register circuit:



$$p(x) = x^4 + x + 1 \quad \Rightarrow \quad x^4 \equiv x + 1$$

- LFSR: if initialized by any, but the all-zero-state: LFSR runs through all, but the all-zero-state.
- Output sequence is
  - a pseudo random sequence
  - an m-sequence, Length: $L = 2^m - 1$

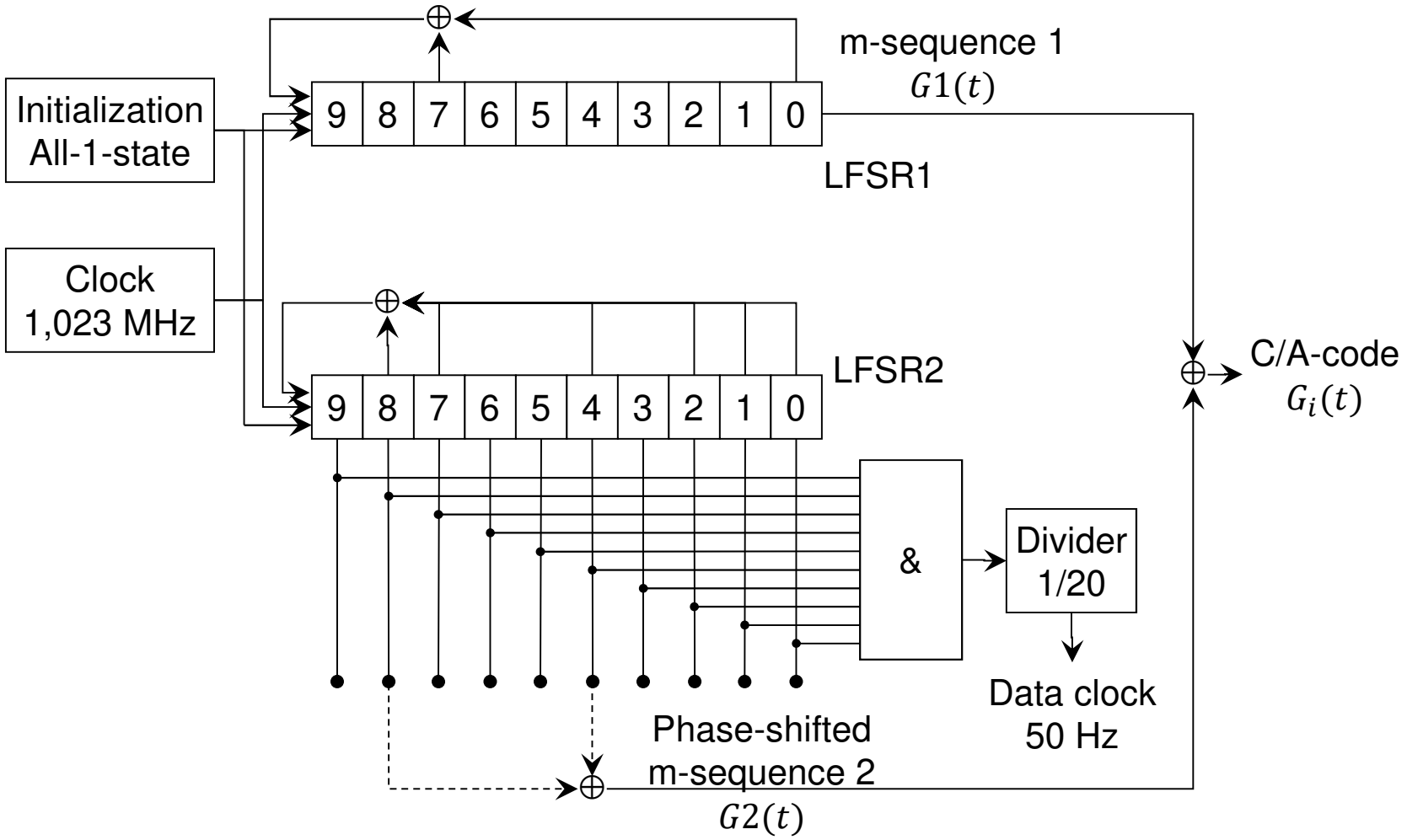
Periodic autocorrelation of m-seq. ($L = 2^4 - 1 = 15$)



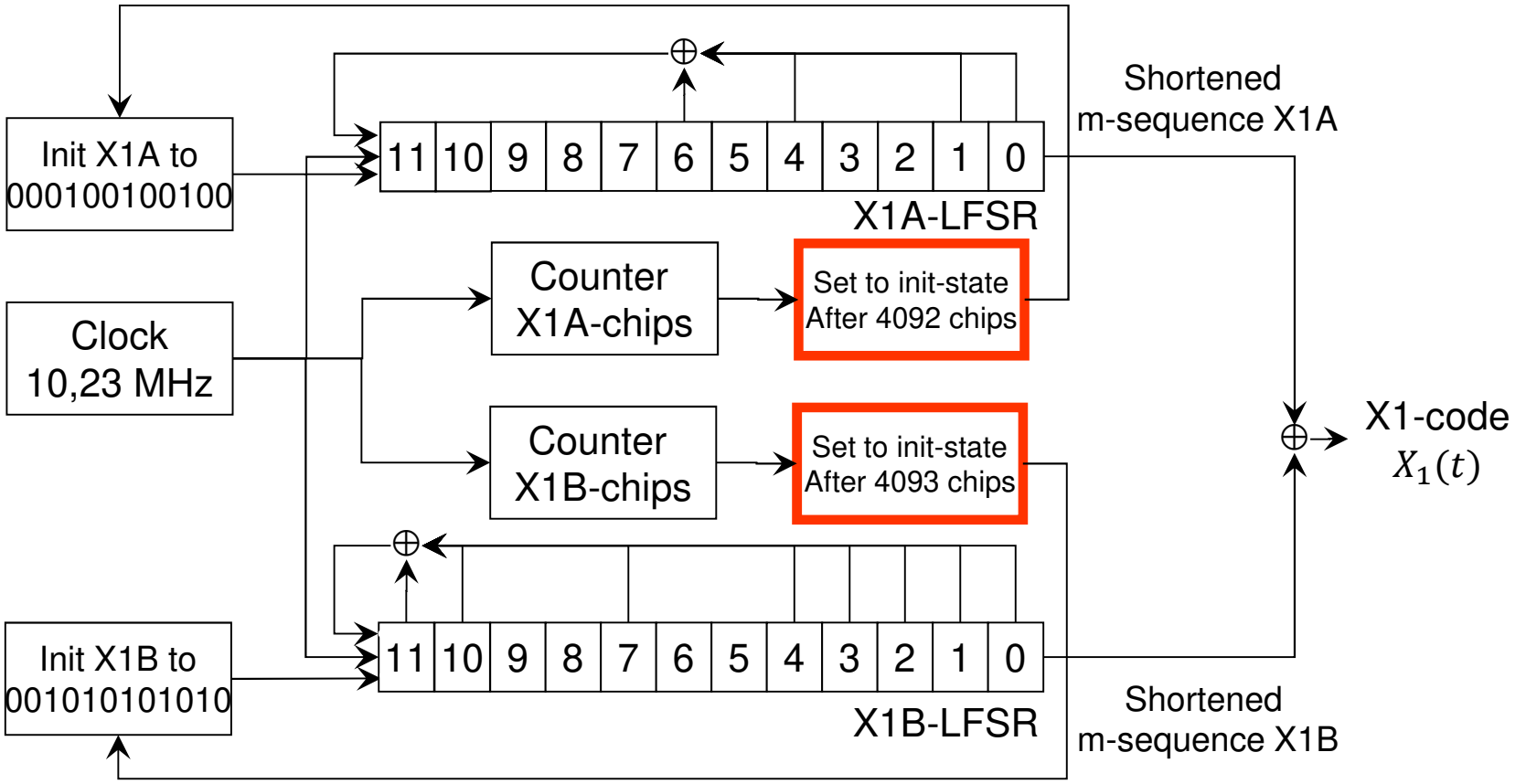
Cross-correlation properties of different sequences

m Number of LFSR stages	$L = 2^m - 1$ Sequence length	# Number of m-sequences	Maximal normalized cross correlation	t absol. cross correlation of Gold sequence	normalized cross correlation of Gold sequence
3	7	2	0,71	5	0,71
4	15	2	0,60	9	0,60
5	31	6	0,35	9	0,29
6	63	6	0,36	17	0,27
7	127	18	0,32	17	0,13
8	255	16	0,37	33	0,13
10	1023	60	0,37	65	0,06
12	4095	144	0,34	129	0,03
15	32767	1800	n.a.	257	0,007843

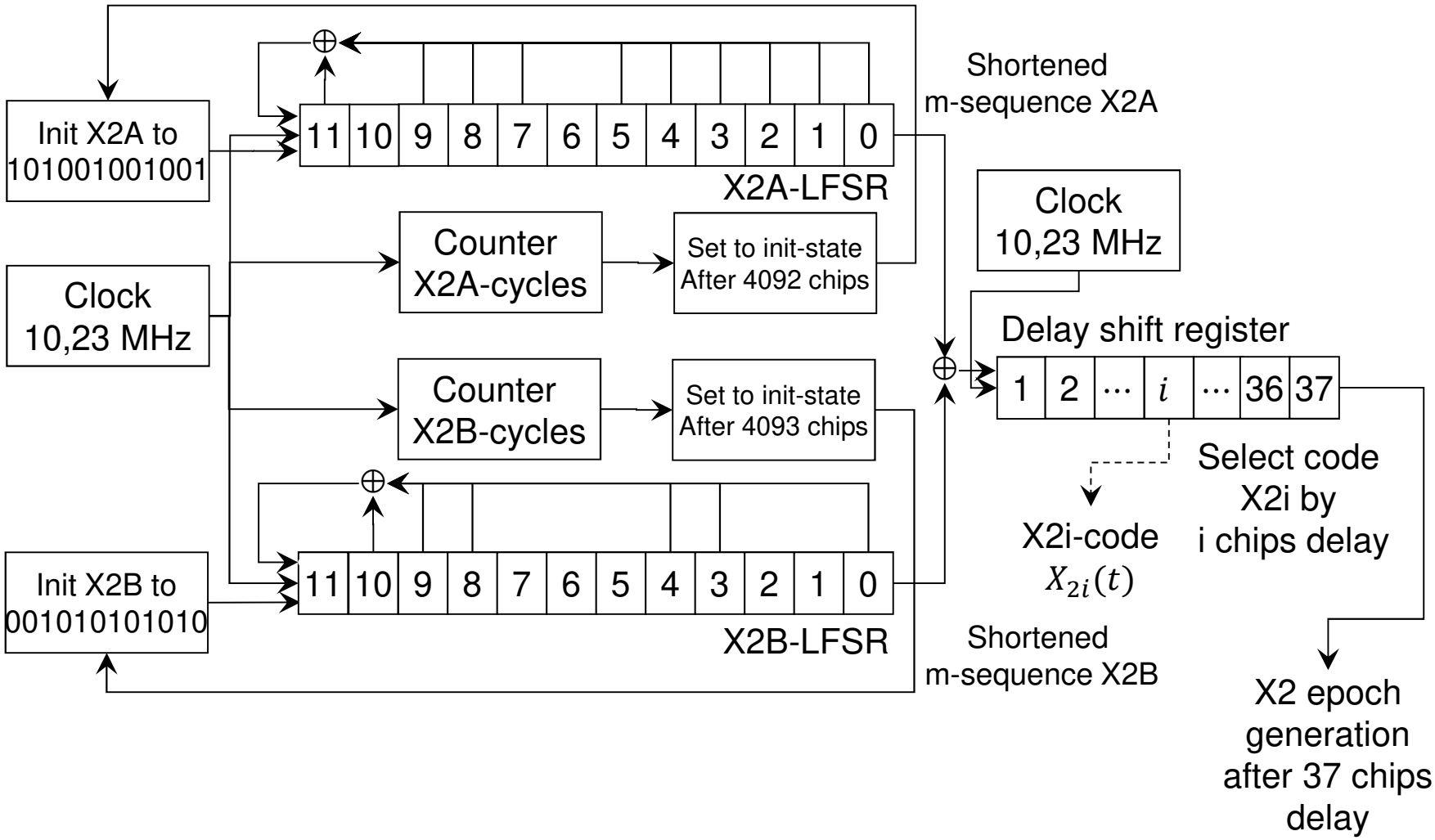
C/A-code generator of GPS



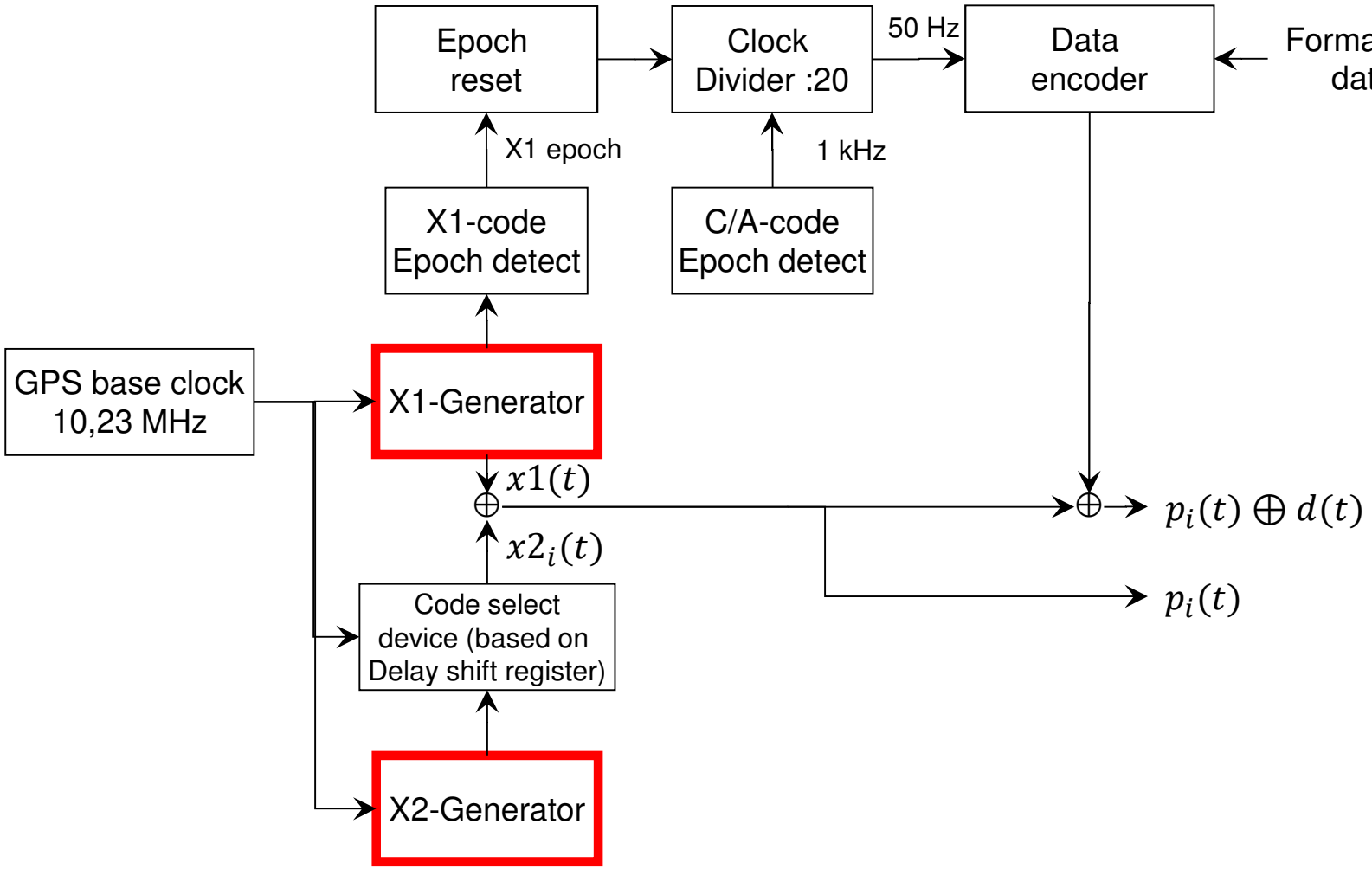
X1-Code Generator for P-code of GPS



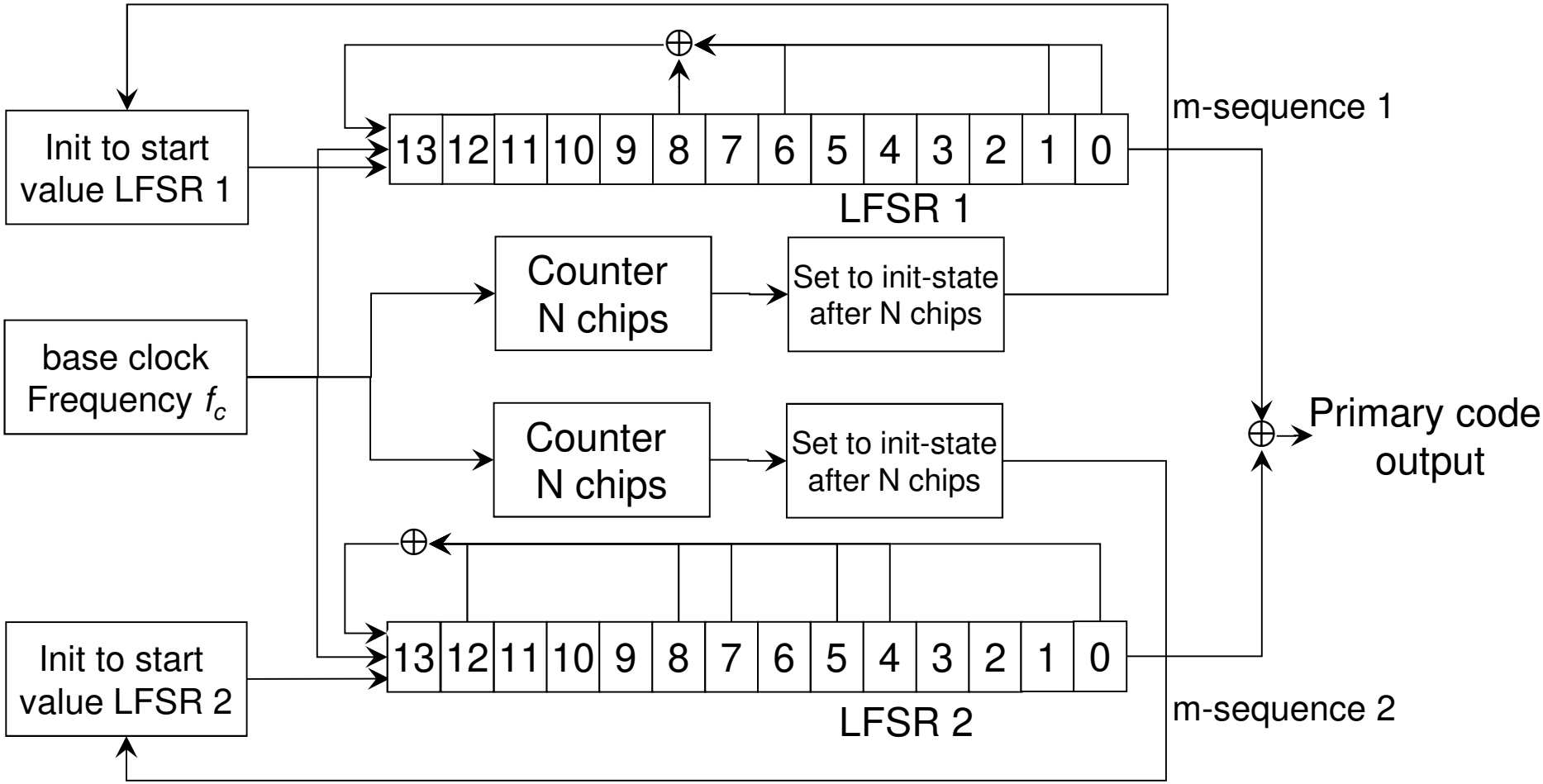
X2i-code generation of GPS P-code



Block diagram of GPS P-code generator

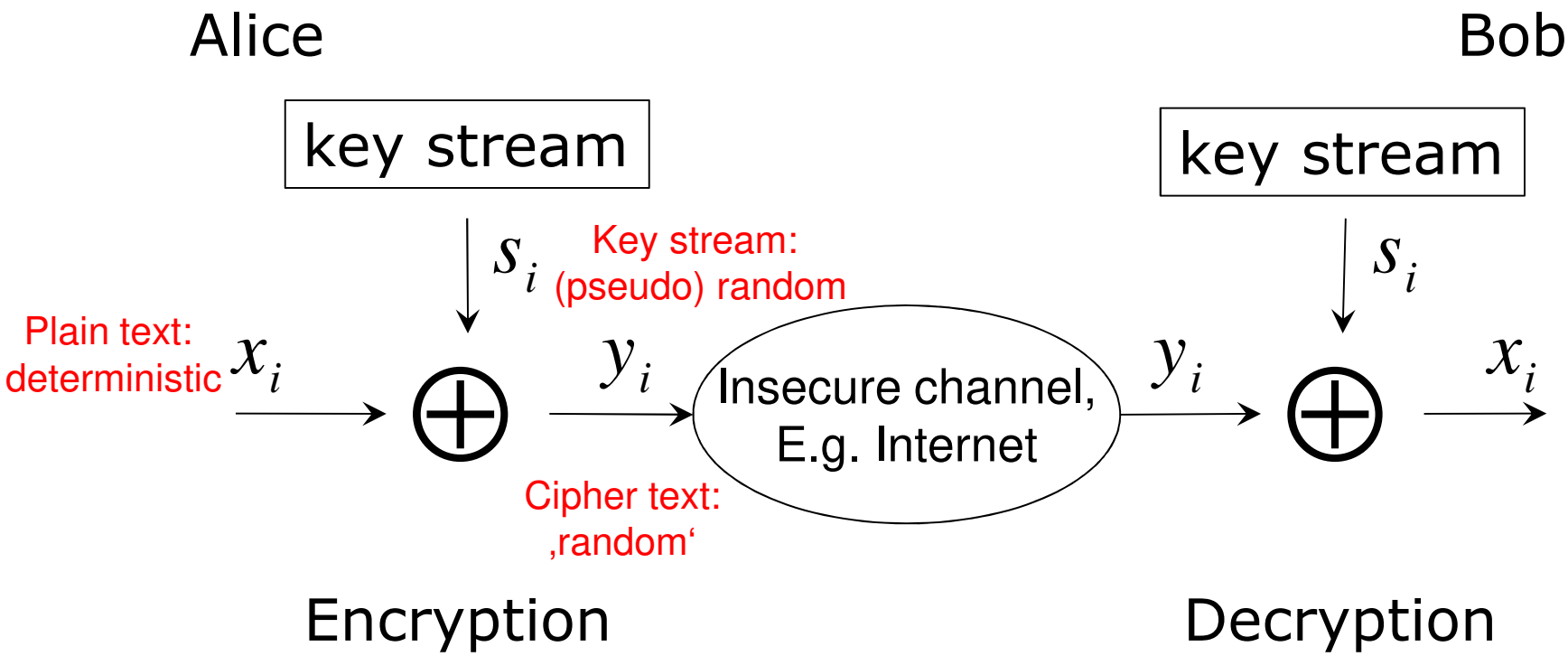


GALILEO Open Service primary code generation

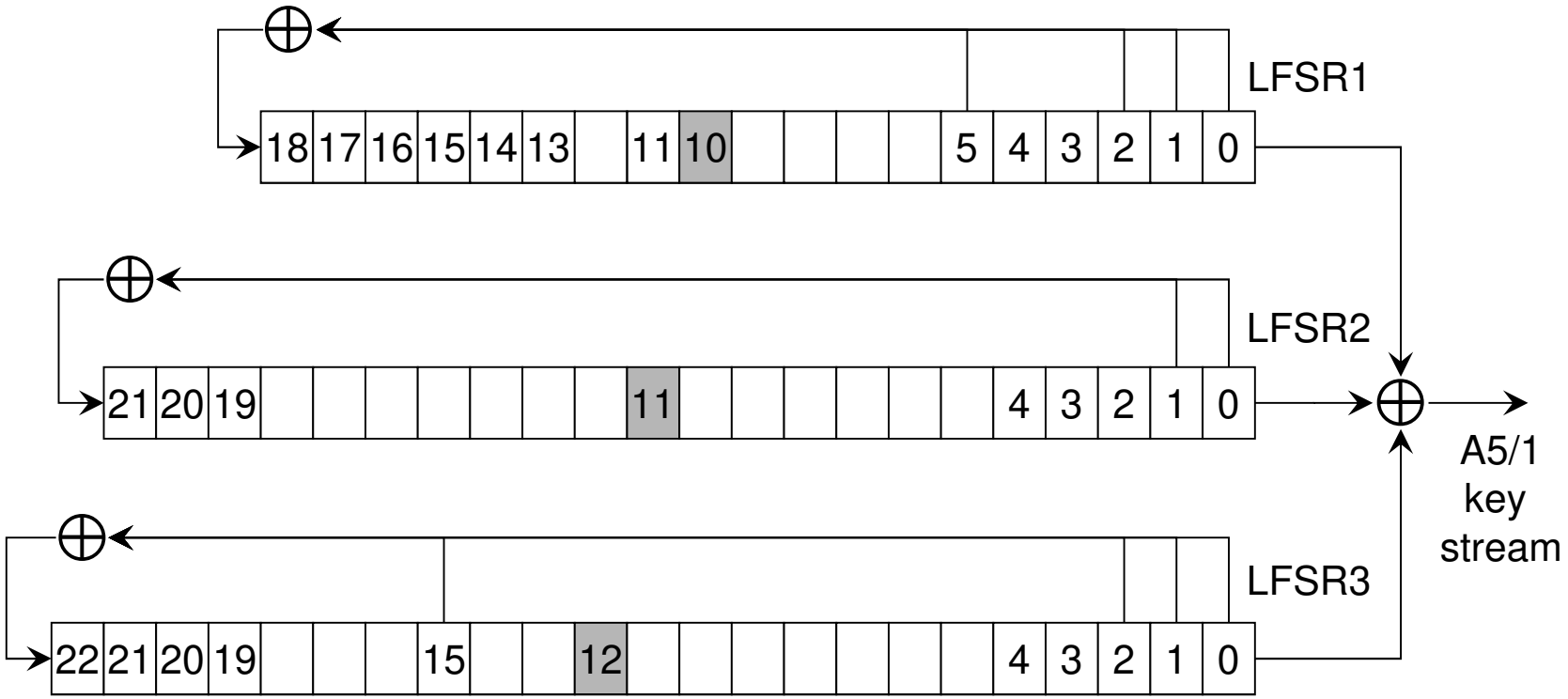


In Galileo: ‚shortened' Gold codes of length $N = k \cdot 1023$ for reasons compatibility between GPS and GALILEO.

LFSRs in cryptography: Stream ciphers

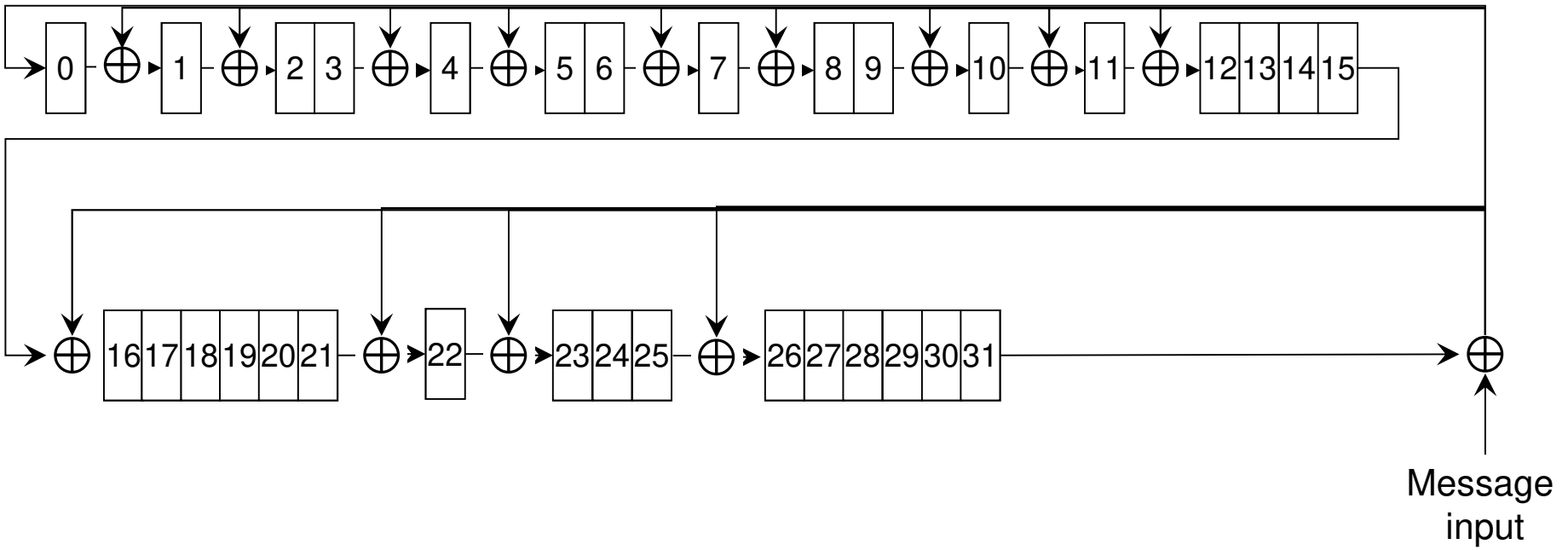


LFSRs in cryptography: A5/1 stream cipher (GSM)



Feedb. Shift Reg. f. Cyclic Redundancy Check

CRC 32bit: $p_{32}(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$



Summary

- „Extension fields“ are limited fields with a great flexibility regarding field size.
- Primitive polynomials defining an Extension Field can straightforward be applied to design a corresponding LFSR.
- LFSRs based on primitive polynomials generate pseudo random sequences (m-sequences) or Gold codes.
- LFSRs have many technical applications:
  - GPS
  - GALILEO
  - Stream ciphers in cryptography
  - Cyclic redundancy checks

Thank you very much for your attention!

References

1. Jean-Marie Zogg: “GPS und GNSS: Grundlagen der Ortung und Navigation mit Satelliten“, May 2014, available at: http://zogg-jm.ch/weitere_publikationen.html
2. Werner Mansfeld: „Satellitenortung und Navigation: Grundlagen, Wirkungsweise und Anwendung globaler Satellitennavigationssysteme“, Vieweg-Teubner Verlag, 2009
3. Spiegel-Online arcticles on GALILEO: several arcticles with publication data ranging from 2011 until 2015.