Galois Fields and their Applications in Global Navigation Satellite Systems

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

16th International Symposium on
Ambient Intelligence and Embedded Systems
September 14th – 16th, 2017

Vaasa University of Applied Sciences, Vaasa, Finland

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
- Summary

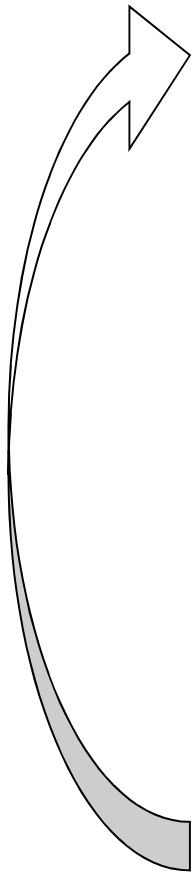
Galois Fields – Finite Fields over primes

- Galois Field is a
  - **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.
  - **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 generate 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 $\boldsymbol{GF(2^m)}$

- Prime Fields (except for $GF(2)$) technically not important, since most technical systems work bit-oriented.
- → **Galois Fields can be extended**, i.e. for any prime p and any positive integer m there exists a finite field $\boldsymbol{GF(p^m)}$.
- Each field element is a polynomial.

$$\left(a_{m-1}x^{m-1} + \quad a_{m-2}x^{m-2} + \quad a_{m-3}x^{m-3} + \quad \cdots + \quad a_1x^1 + \quad a_0x^0\right)$$

$$\text{with } a_i \in 0,1,2,\ldots.,\ p-1 \text{ for } i = 0,1,2,\ldots,m-1$$

$$\left(a_{m-1} \quad a_{m-2} \quad a_{m-3} \quad \cdots \quad a_1 \quad a_0\right)$$

$$\text{with } a_i \in 0,1,2,\ldots.,\ p-1 \text{ for } i = 0,1,2,\ldots,m-1$$

- If $p = 2$, i.e. $GF(2^m)$: all coefficients are equal to ‚0' or ‚1'.

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

$$p(x) = x^4 + x + 1$$

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

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

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

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

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

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

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

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

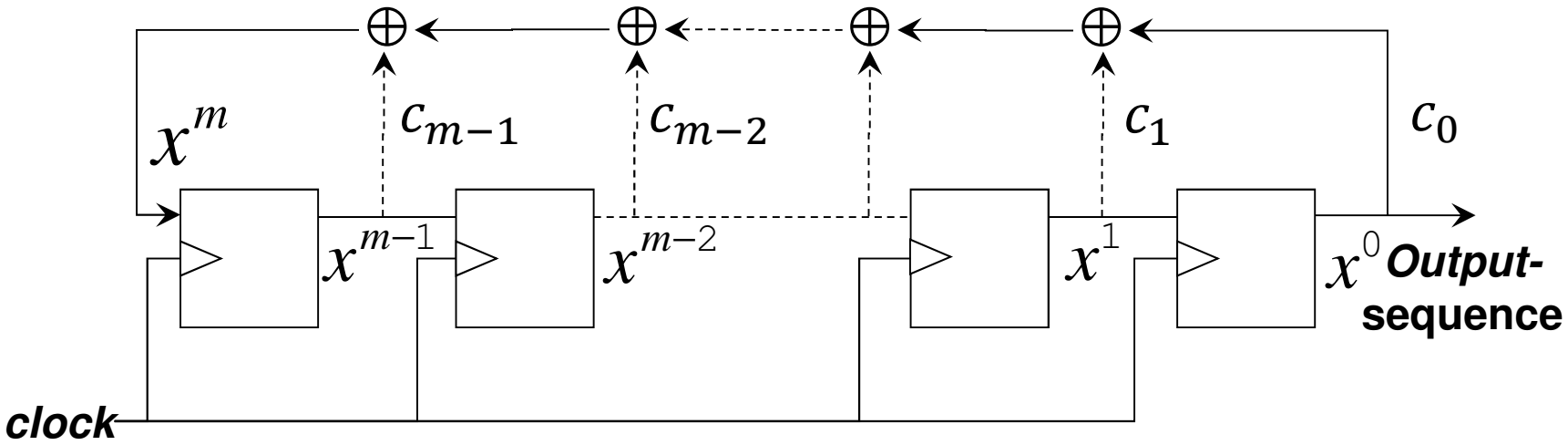
$$\vdots$$

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

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

Lin. Feedback Shift Registers for Ext. Fields $GF(2^m)$

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

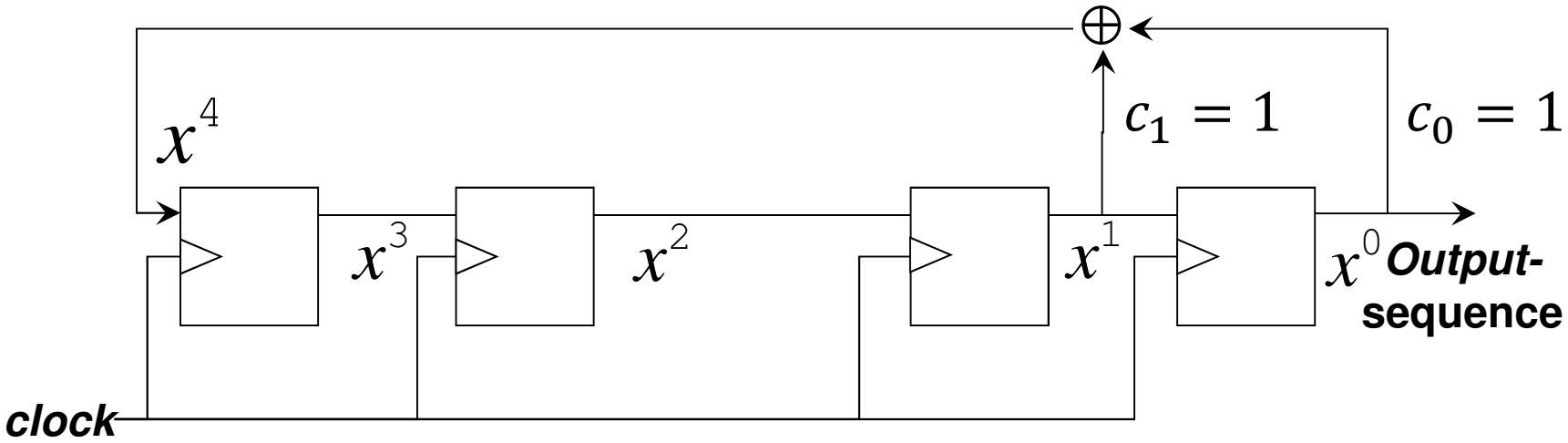


$$p(x) = x^m + \sum_{i=m-1}^{0} c_i \cdot x^i \quad \text{with } c_i \in GF(2) = \{0,1\} \Rightarrow \text{since } \alpha^m + \sum_{i=m-1}^{0} c_i \cdot \alpha^i \equiv 0 \text{ (by definition)} \Rightarrow$$

$$\alpha^m \equiv \sum_{i=m-1}^{0} c_i \cdot \alpha^i \text{ if we replace } \alpha \text{ by } x \quad \Rightarrow x^m \equiv \sum_{i=m-1}^{0} c_i \cdot x^i$$

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

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



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

- Output sequence is
  - a pseudo random sequence
  - an m-sequence, Length: $L = 2^m - 1$, LFSR runs through **all** possible but the all-zero-state!

m-sequence properties

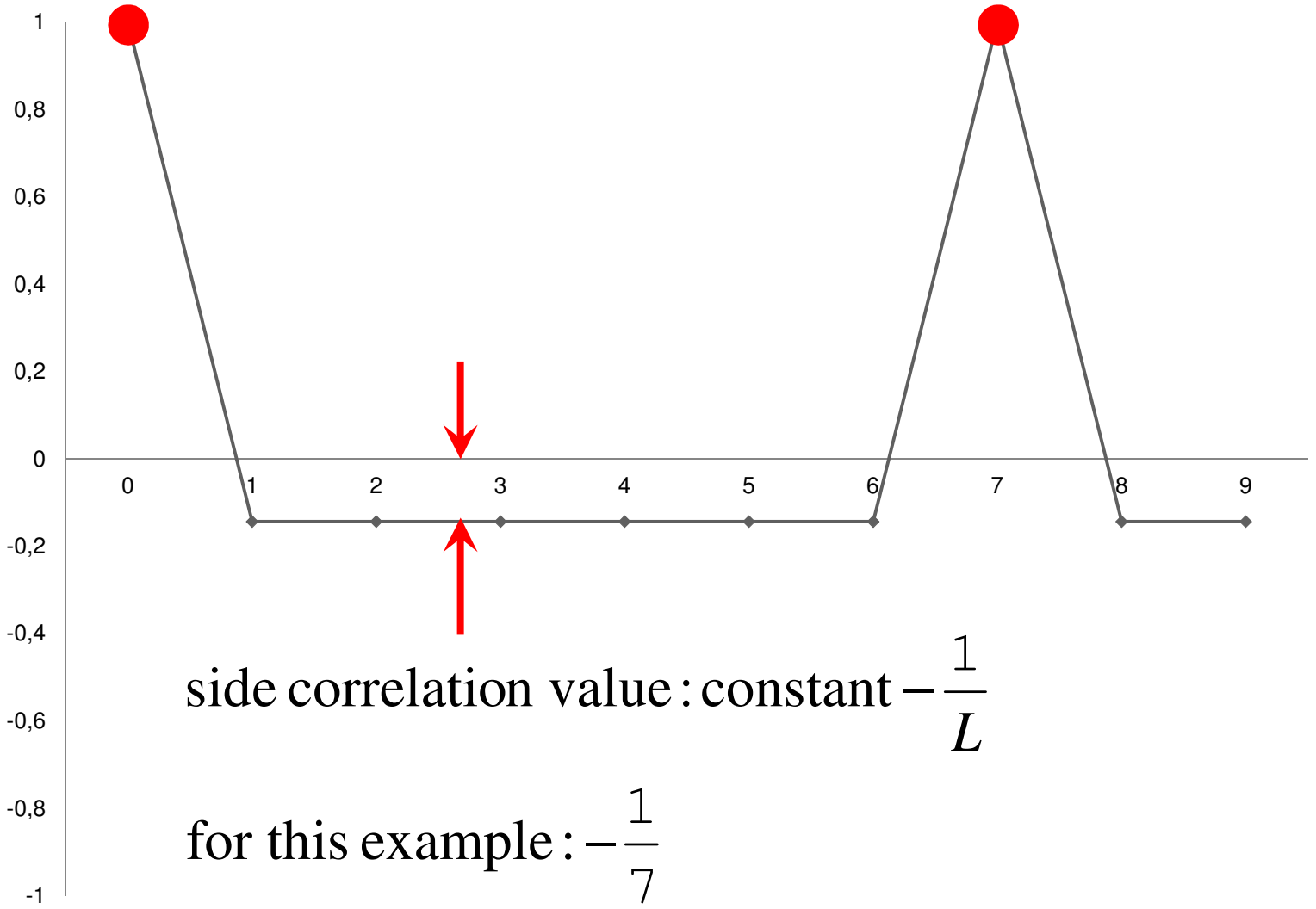
- Balance property:
  - Sequence contains:

$$\frac{L+1}{2} \quad \text{'1' in case of our example: 8 '1'}$$

$$\frac{L-1}{2} \quad \text{'0' in case of our example: 7 '0'}$$

- Run length property (run of length k = sequence of k same symbols) :
  - $\frac{1}{2}$ of all runs: length 1
  - $\frac{1}{4}$ of all runs: length 2
  - $\frac{1}{8}$ of all runs: length 3
  - ….

Periodic autocorrelation of m-sequence (L=7)



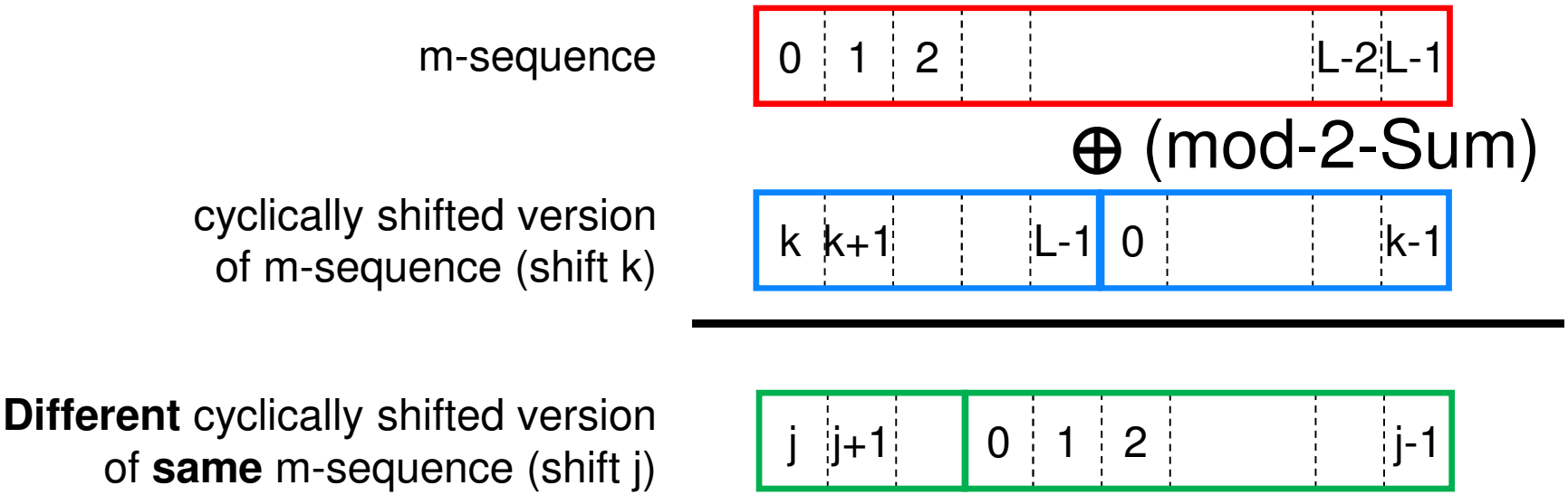
$$\text{side correlation value}: \text{constant} -\frac{1}{L}$$

$$\text{for this example}: -\frac{1}{7}$$

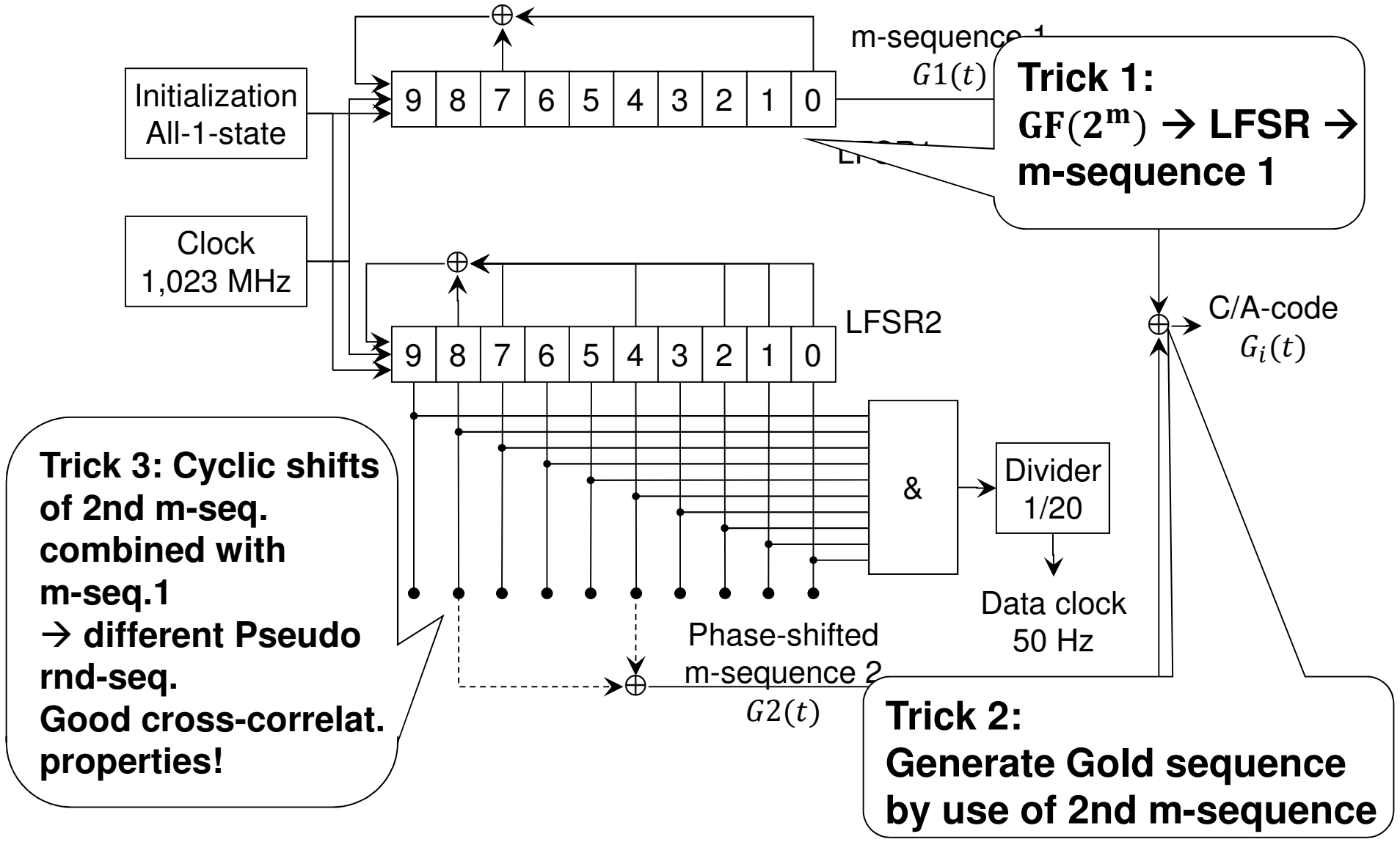
Cross-correlation properties of different sequences

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

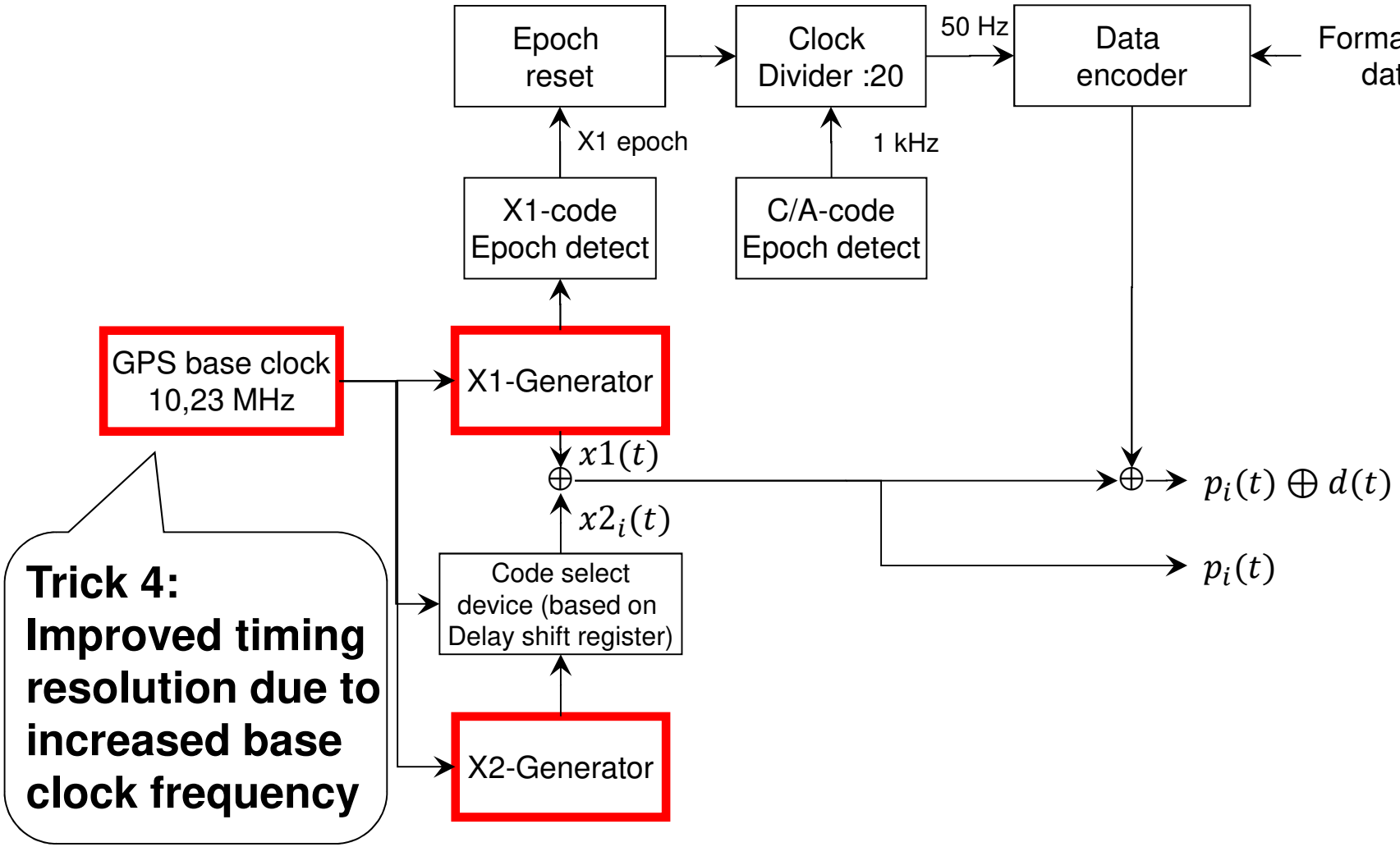
Addition of cyclically shifted m-sequences



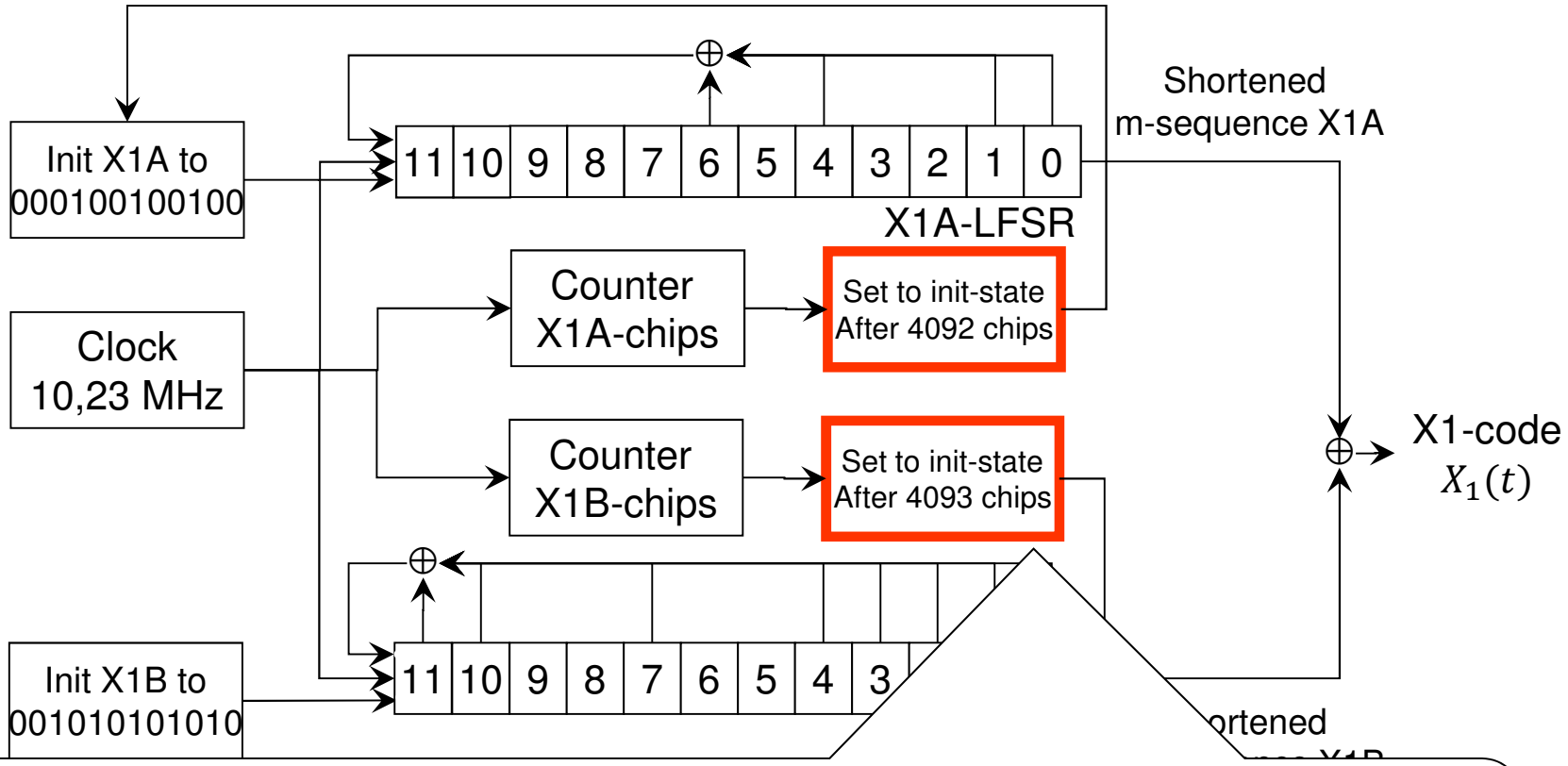
C/A-code generator of GPS



Block diagram of GPS P-code generator

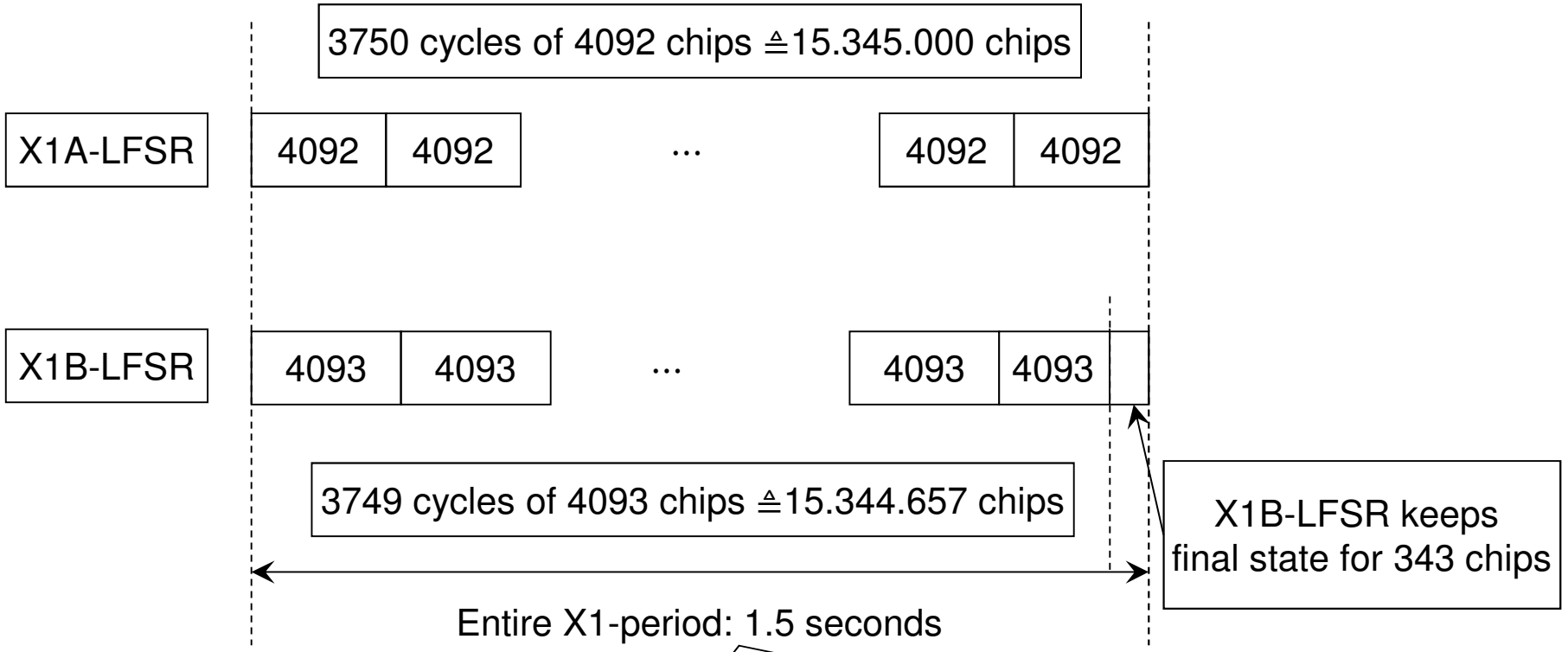


X1-Code Generator (for P-code) of GPS



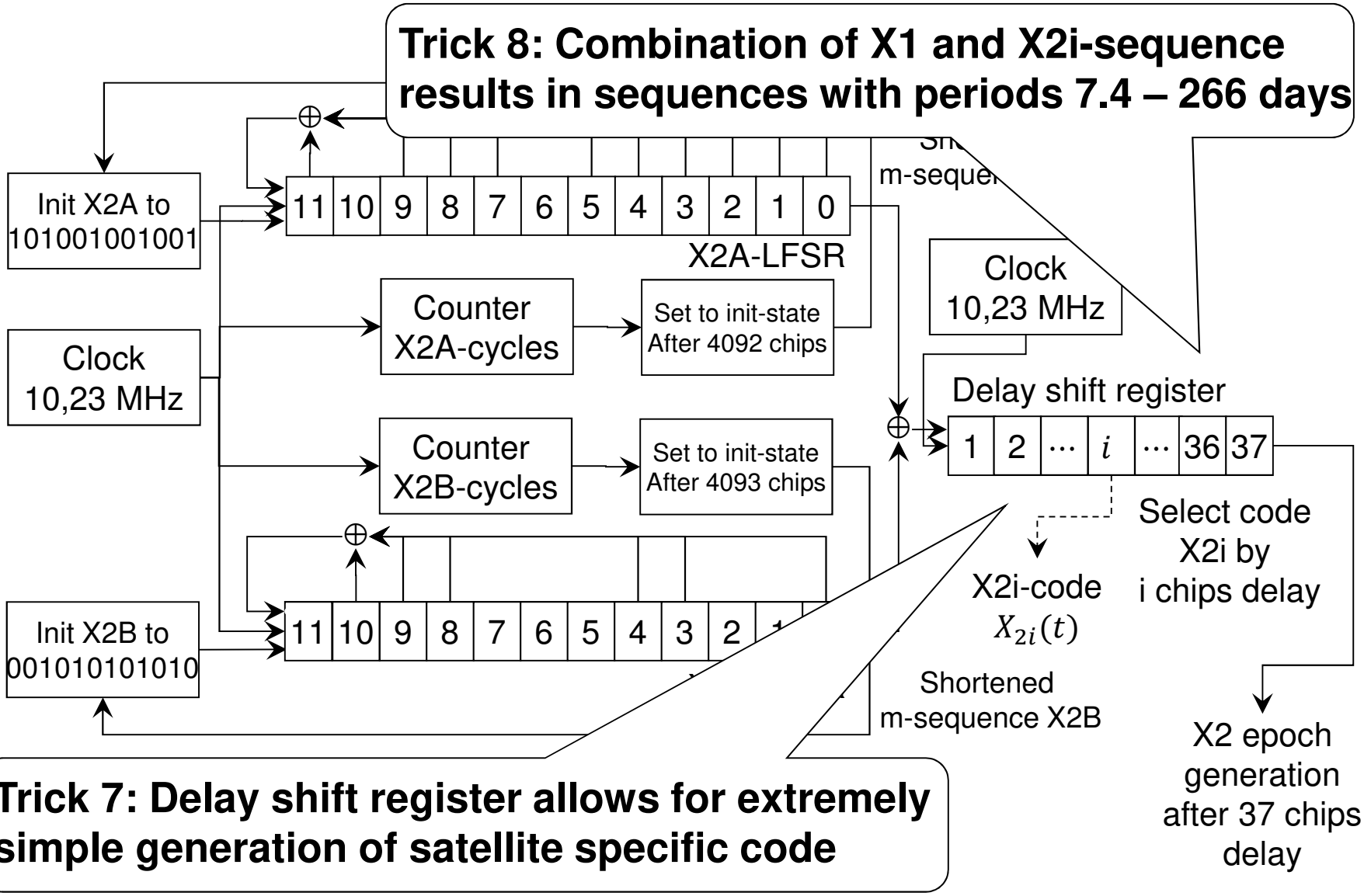
Trick 5: Use of shortened m-sequences →
Resulting sequence: length defined by least common multiplier of the seq.-lengths (4093 prime → 4092x4093=16.748.556)

Timing relations of X1-code generation within GPS

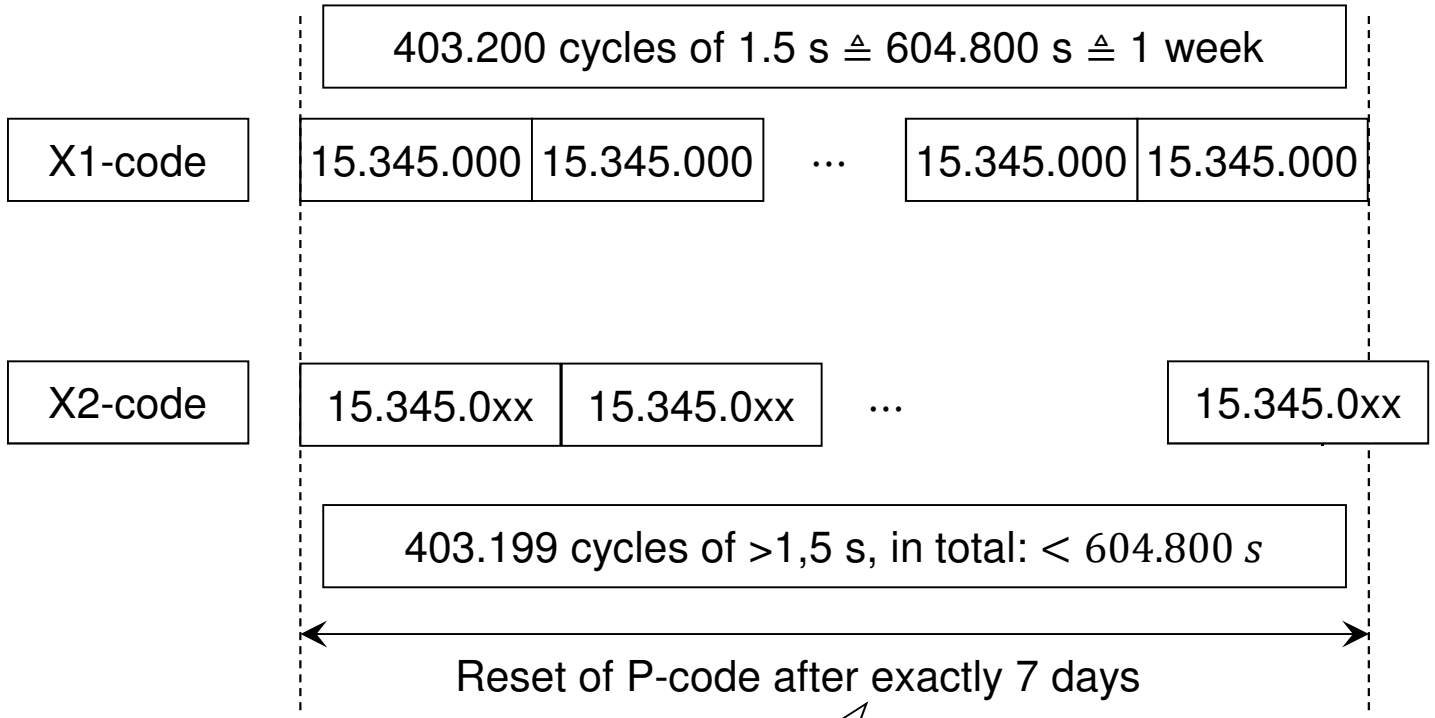


Trick 6: Resulting X1-sequence shortened to exact period of 1.5 seconds ←→ 15.345.000 chips

X2i-code generation of GPS P-code



Timing relations of P-code generation in GPS

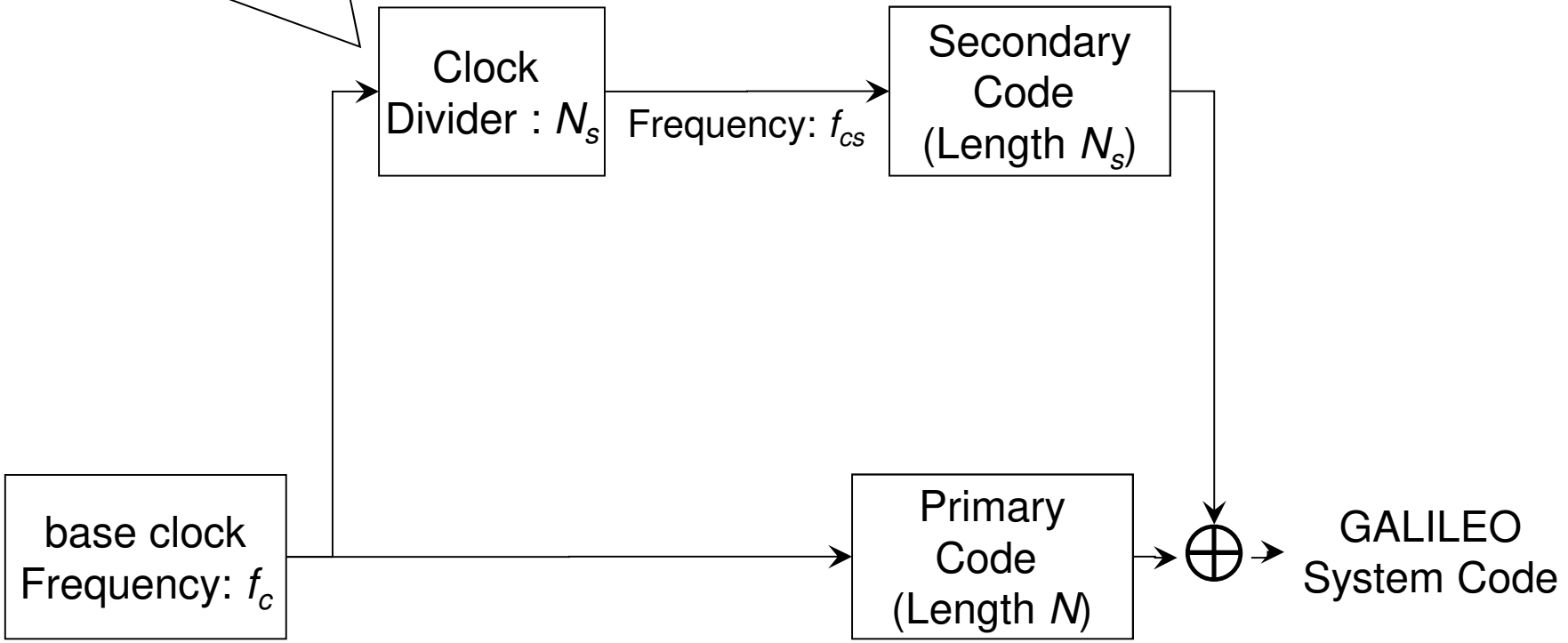


Trick 9: P-code also shortened to match defined timing period of 7 days

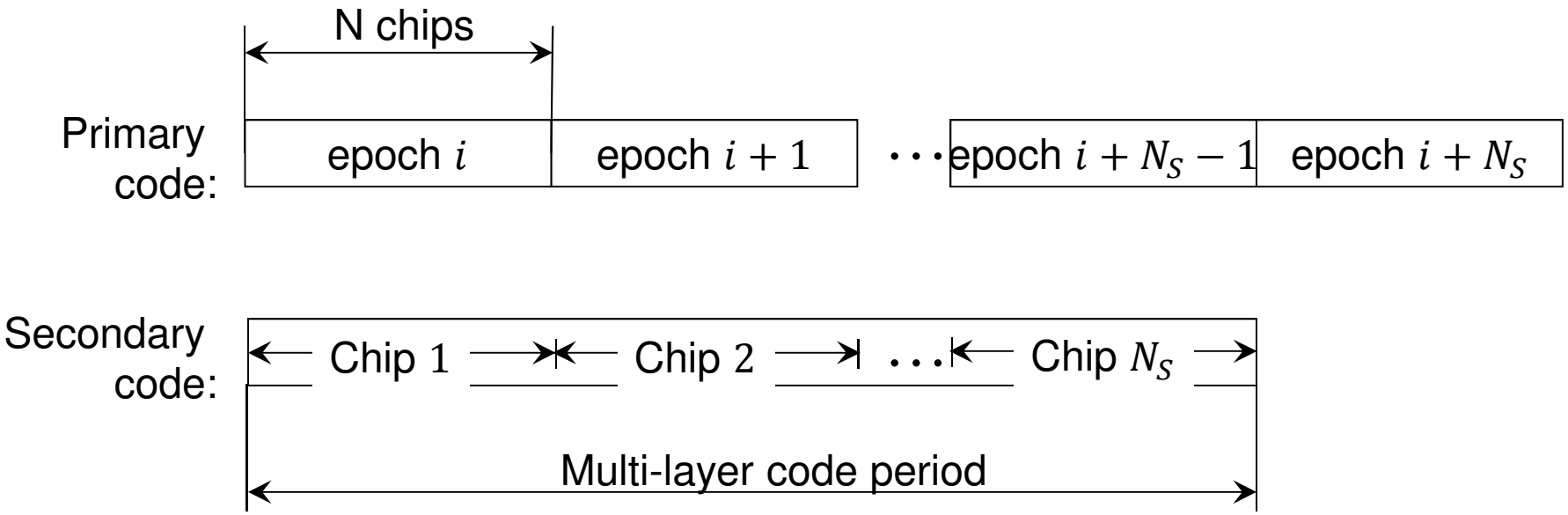
GALILEO multi-layer system code generation

Trick 10: Use of multi-layer code generated by sequences based on DIFFERENT clock frequencies

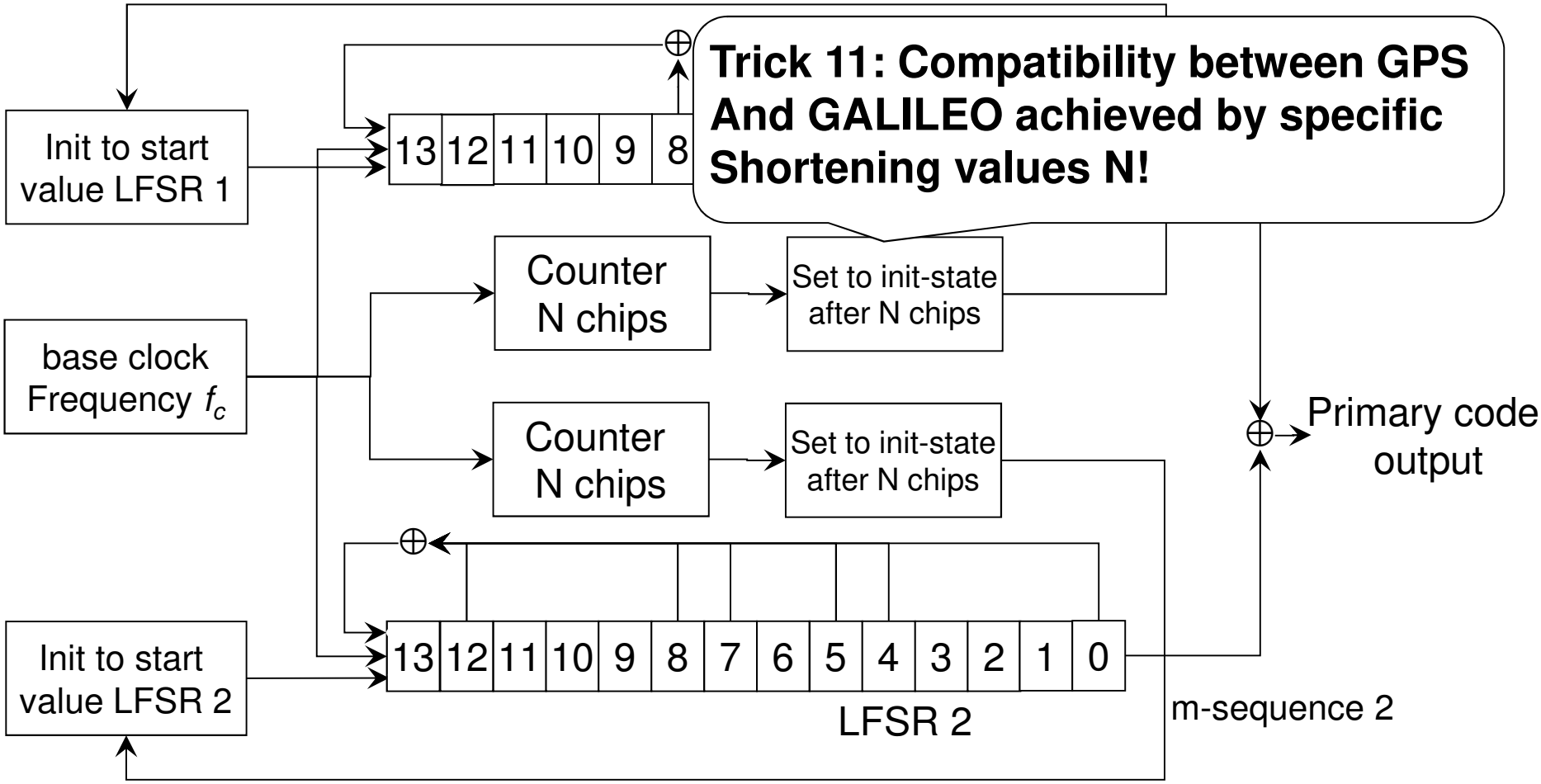
Secondary codes:
fixed sequences of
length 4, 20, 25 or 100 bit



Timing structure of GALILEO system codes



GALILEO Open Service primary code generation



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

Summary

- Extension fields of various degrees are the core for GPS and GALILEO.
- Code generation is always based on m-sequences
- Due to much better crosscorrelation properties Gold codes are applied in GPS.
- In GALILEO a similar idea (multi-layer-codes) is used!
- ‚Simple tricks' lead to generation of very long (pseudo-random)-sequences, which are used within GPS and GALILEO.

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.
4. European Space Agency (ESA): „Space in Videos“ - http://www.esa.int/spaceinvideos/content/search?SearchText=galileo&SearchButton=Go