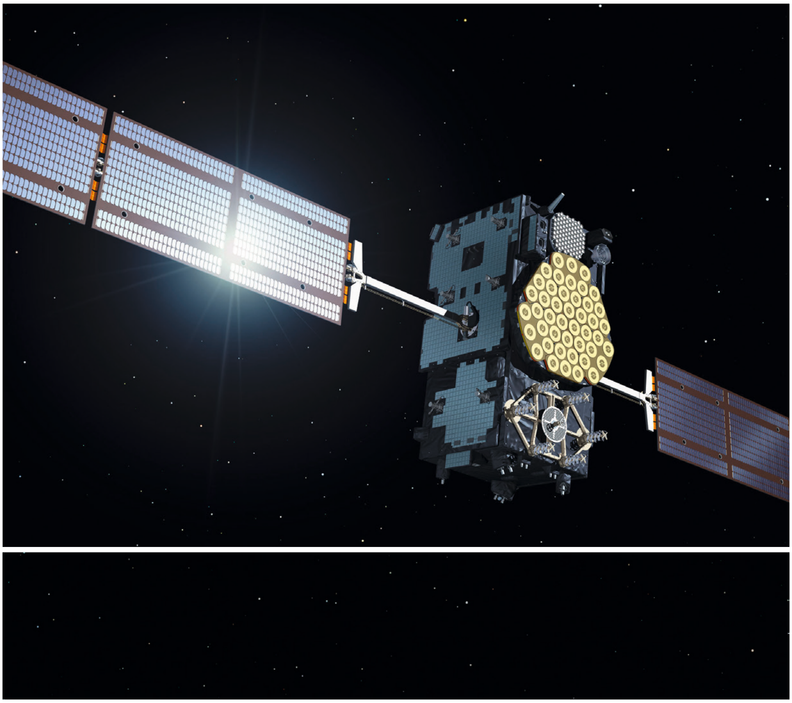
Ulrich Jetzek

# Galois Fields, Linear Feedback Shift Registers and their Applications



HANSER

Jetzek

**Galois Fields,**

**Linear Feedback Shift Registers and their Applications**

Ulrich Jetzek

# Galois Fields, Linear Feedback Shift Registers and their Applications

With 85 illustrations as well as numerous tables, diagrams and examples

Fachbuchverlag Leipzig
im Carl Hanser Verlag

The Author:
**Prof. Dr.-Ing. Ulrich Jetzek**
Fachhochschule Kiel, Fachbereich Informatik und Elektrotechnik,
Institut für Kommunikationstechnik und Embedded Systems

FSC
www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C016439



Cataloging-in-Publication Data is on file with the Library of Congress


Editor: Dipl.-Ing. Natalia Silakova
Production Management: Dipl.-Ing. (FH) Katrin Wulst
Coverconcept: Marc Müller-Bremer, www.rebranding.de, München
Coverdesign: Stephan Rönigk
Typesetting: le-tex publishing services GmbH
Printed and bound by Hubert & Co. GmbH & Co. KG BuchPartner, Göttingen
Printed in Germany

ISBN: 978-3-446-45140-7
E-Book ISBN: 978-3-446-45613-6

*To Carola, Julia, Franziska and Christian*

# Acknowledgements

First of all, I would like to thank all the students I have been working with. All their questions, comments and remarks during my various lectures showed an intense interest in Galois Fields, Linear Feedback Shift Registers and their applications. This was a strong motivation moment to write this book.

Furthermore, I am grateful for the cooperation I had with the editor of Hanser Fachbuchverlag, Mrs. Mirja Werner. From the very beginning she had trust in my idea about this book and always supported me in writing this book. We had several fruitful discussions regarding structure, content and details of this book. I would also like to thank the editor, Mrs. Natalia Silakova, who accompanied me in the finalization phase of this book.

Many other people contributed to this book. Therefore, I would also like to thank all those people who are not mentioned explicitly in this section.

Finally, my thanks go to my family – my wife Carola and my children Julia, Franziska and Christian. They always showed lots of understanding while I was writing this book. And they had lots of patience when I (unfortunately) had no time to share and enjoy together with them.

**Remark:** *The author of this book has written and described the entire content of this book to his best knowledge. However, the author does not take any responsibility for any developments and/or products which may have been developed based on the content of this book. The book is intended as a textbook to get acquainted with Galois Fields, Linear Feedback Shift Registers and their applications. Therefore, the reader is required to make sure by himself whether any software or hardware implementation or any product derived from the content of this book works as wanted.*

# Contents

# 1 Introduction

Digital processing and transmission of data found their way into technical systems many years ago. We may, for example, only need to think of the digital mobile communication standard GSM, which was *the standard* to make mobile phones a mass market product in the mid 1990s. Another example was the invention, development and distribution of digital cameras, which have also been mass market products roughly since the beginning of this millennium.

The current trend we can observe in many areas is digitalization, connecting production chains by means of digital communication between different production steps and digital control of complete production chains.

An important area in the digital world is the world of finite fields, very often called Galois Fields. These fields, in particular the so-called Extension Fields, form the basis for quite a few technical applications, e.g. the technology of Global Navigation Satellite Systems (GNSS), such as the American Global Positioning System (GPS) or the European GALILEO. Therefore, the idea for this book is to build a bridge via the directly connected Linear Feedback Shift Register (LFSR) circuits between the mathematical description of Galois and Extension Fields and various technical applications as illustrated in Figure 1.1.

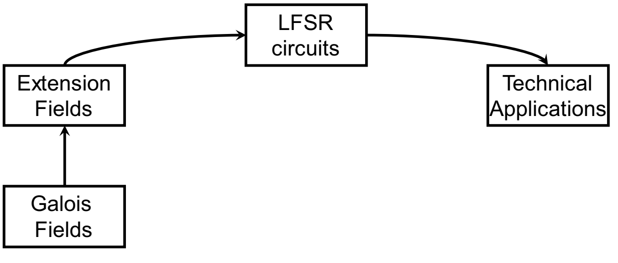



**Figure 1.1** Building the bridge between Galois and Extension Fields and Technical Applications via LFSRs

### Goal of this book

For several years the author of this book has been giving lectures on digital circuit theory, cryptography, mobile communications systems and most recently also on navigation systems. Whereas the explanation of how a register works and what a shift register is seems to be of rather theoretical and academic nature at the first glance, there are numerous examples where linear feedback shift registers are used in various technical systems. Such linear feedback shift registers play a significant role in e.g.

- the US navigation system GPS [1, 2];
- the Crypto system A5/1 used for voice encryption in GSM [3];
- cyclic redundancy checks (CRC) [4];
- the mobile communication standard UMTS [5];
- the mobile communication standard LTE [6].

Although there is a tight mathematical connection between the above mentioned Linear Feedback Shift Registers (LFSRs) and Finite Fields, in particular Galois Fields, the corresponding mathematical background is often not visible to students. Furthermore, LFSRs are often used to generate Pseudo Random Sequences, the so-called m-sequences, which have very specific and important properties. Due to these special properties m-sequences are often applied in technical systems. Therefore the main goals of this book are:

1. To explain what Galois Fields are. We will explain what prime fields are as well as what extension fields are.
2. How to work with Galois Fields, and how to perform operations in Galois Fields.
3. Explain the connection between Galois Fields, in particular extension fields, and linear feedback shift registers.
4. Describe some of the most important technical applications of Galois Fields and LFSRs.

We will start with the mathematical description of Galois Fields. This means that we need to look into how the algebraic structures of groups, rings and fields are defined. We will then have a closer look especially into the mathematical operations over these finite fields. For that purpose, we will need to define modular arithmetic. This concept will further be generalized as the so-called Extension Fields, where modular arithmetic is applied to polynomials.

In order to give the reader a deep insight into these Extension Fields, Chapter 3 of this book is fully dedicated to the principles of working with Extension Fields.

In the following section we will move over from the mathematical perspective towards the transformation of the so-called primitive polynomials into corresponding Linear Feedback Shift Register (LFSR) circuits. It is amazing to see that primitive polynomials, and not only these, can be transformed straight into a corresponding LFSR. This step will be taken in Chapter 4.

The above mentioned LFSRs can be used to generate pseudo random sequences, the so-called m-sequences. These sequences have quite interesting properties, especially when it comes to their periodic autocorrelation. Chapter 5 explains what an m-sequence is, which properties it has and why these properties are well-suited for use in technical systems.

In Chapter 6 we take the last step towards building the above-mentioned bridge: we will look into various technical systems, which are based on Extension Fields and related LFSRs. We will start with the description of the US Satellite Navigation System GPS, and then we will look into cryptographic applications, such as the GSM-stream cipher A5/1 as well as a recent stream cipher called Trivium. As the third big area for applications we will have a close look into Cyclic Redundancy Checks (CRC) and will show that one may easily design an LFSR to perform a CRC calculation rapidly.

In order for the interested reader to try out and test his own knowledge, several exercises are provided for some chapters. Solutions to all given problems are provided in Chapter 7. In addition, this chapter contains a list with several primitive and irreducible polynomials up to the degree $m = 16$.

The book is mainly intended to support students who attend lectures on navigation systems, cryptography, channel coding or mobile communication systems (e.g. on UMTS, LTE or LTE-advanced). However, it shall also support engineers working in the fields mentioned above, who may either need to study Galois Fields and their applications or are possibly simply interested in gaining a deeper understanding of this field.

Since the theory of Galois Fields itself and especially working with Galois Fields is rather abstract, the book is not intended for first-year bachelor students, but rather for students who already had the possibility to deal more intensively with mathematical theories.

## Bibliography

[1] W. Mansfeld, Satellitenortung und Navigation: Grundlagen, Wirkungsweise und Anwendung globaler Satellitennavigationssysteme, Wiesbaden: Vieweg + Teubner, 2009.

[2] J.-M. Zogg, „GPS und GNSS: Grundlagen der Ortung und Navigation mit Satelliten“, Mai 2014. [Online]. Available: http://www.zogg-jm.ch/Dateien/Update_Zogg_Deutsche_Version_Jan_09_Version_Z4x.pdf.

[3] C. Paar und J. Pelzl, Understanding Cryptography – A Textbook for Students and Practitioners, Heidelberg: Springer Verlag, 2010.

[4] H. S. Warren, Jr., Hacker’s Delight, Eddison Wesley, 2013.

[5] H. Holma und A. Toskala, WCDMA for UMTS, West Sussex, England: John Wiley & Sons, Ltd., 2000.

[6] E. Dahlman, S. Parkvall und J. Sköld, 4G – LTE/LTE-Advanced for Mobile Broadband, Academic Press, 2011.

# 2 Finite Groups and Fields

Figure 2.1 shows the basic elements of a Digital Communication System. In order to ensure the confidentiality of data (and other security services) the sender ENcrypts the data while the receiver performs the *reverse operation* – the DEcryption of the received data. In addition, the sender performs channel ENcoding of data in order to protect the data against transmission errors due to noise and interference on the channel. Once again, the receiver performs the *reverse operation*, namely channel DEcoding.

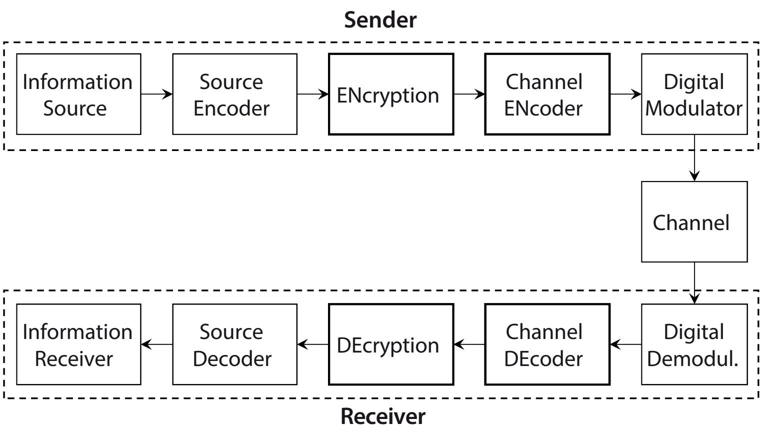



**Figure 2.1** Elements of a Digital Communication System

In many cases ciphering of data as well as channel coding are performed in blocks, i.e. by encrypting and channel encoding of data blocks having a specific size, e.g. 64 bits. These data blocks may also be considered as integer values of a specific length. Therefore, since the data blocks have a finite length, only a finite number of possible elements exists. In case of our example with 64 bit blocks, the number of possible elements is $2^{64}$.

From the sender's perspective mathematical operations performed with these data blocks are usually based on the arithmetic operations "addition" and "multiplication." However, the essential idea which counts for crypto systems as well as for channel coding is that any operation containing two or more elements results in an element WITHIN the finite set of elements. That means that we work with a *fixed bit length*, and any addition or multiplication operation in a finite field yields a result having the *same bit length as each single operand*. In general, this aspect does not work for addition and multiplication when used with real numbers $\mathbb{R}$, since, for example, the multiplication of two integers yields a larger value, which has an *increased bit length*, e.g. $(1000)_2 \cdot (1001)_2 = (1001000)_2$. Therefore, we need a different type of arithmetic in order to ensure the above-mentioned requirement. This is the modular arithmetic used in Galois Fields.

Since the receiver performs the *inverse operations* as compared to those of the sender, i.e. channel DEcoding and DEcryption of data, we need the *inverse operations* for addition and multiplication. These, in case of the arithmetic with real numbers $\mathbb{R}$, are, of course, subtraction (the inverse of addition) and division (the inverse of multiplication). Subtraction remains as an inverse operation with the modular arithmetic used in Galois Fields as well. However, division of integers does not exist within Galois Fields, but rather is "replaced" by what is called multiplicative inversion.

It was Evariste Galois (1811–1832), a French mathematician, who invented the theory of Galois Fields (see Figure 2.2).

**Figure 2.2** Portrait of Evariste Galois [1]

## 2.1 Modular Arithmetic

One important property – if we work with finite sets of elements – is the isolation property, which means that the result c of an operation performed with two group elements a and b is always an element of the given finite set. This property is achieved by applying a modular operation.