

# Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

169

---

Christian Ronse

Feedback Shift Registers

---



Springer-Verlag  
Berlin Heidelberg New York Tokyo 1984

**Editorial Board**

D. Barstow W. Brauer P. Brinch Hansen D. Gries D. Luckham  
C. Moler A. Pnueli G. Seegmüller J. Stoer N. Wirth

**Author**

Christian Ronse  
Philips Research Laboratory Brussels  
2 Av. E. Van Becelaere, B-1170 Bruxelles, Belgium

CR Subject Classifications (1982): B.6.1, E.4

ISBN 3-540-13330-5 Springer-Verlag Berlin Heidelberg New York Tokyo  
ISBN 0-387-13330-5 Springer-Verlag New York Heidelberg Berlin Tokyo

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically those of translation, reprinting, re-use of illustrations, broadcasting, reproduction by photocopying machine or similar means, and storage in data banks. Under § 54 of the German Copyright Law where copies are made for other than private use, a fee is payable to "Verwertungsgesellschaft Wort", Munich.

© by Springer-Verlag Berlin Heidelberg 1984  
Printed in Germany

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.  
2145/3140-543210

# Contents

Introduction . . . . .	3
Part I: General theory . . . . .	5
§ I       Definition . . . . .	5
§ II       The feedback equation . . . . .	8
§ III      The state diagram . . . . .	9
§ IV      Singularity and period . . . . .	10
§ V       The algebraic treatment . . . . .	15
§ VI      Regular elements . . . . .	21
§ VII     The S.S.A. of $\mathcal{O}$ generated by the shift, the identity and the constant absorbants . . . . .	26
§ VIII    Right ideals and flags . . . . .	30
Part II: The linear case . . . . .	45
§ IX      Definition and basic properties . . . . .	45
§ X       The singularity and period in the linear case . . . . .	53
§ XI      Regular sequences . . . . .	56

§ XII	Sequence description by the roots of the characteristic polynomial — Sequence products . . . . .	58
§ XIII	The associated polynomial . . . . .	61
§ XIV	Multipliers and multigrams . . . . .	69
§ XV	Decimation . . . . .	75
§ XVI	An addition formula . . . . .	85
Part III: Randomness properties . . . . .		87
§ XVII	Golomb's three randomness postulates . . . . .	88
§ XVIII	The third postulate in the nonlinear case . . . . .	92
Part IV: Miscellaneous . . . . .		95
§ XIX	Cascade connection of F.S.R.'s . . . . .	95
§ XX	The subtraction operator $\Sigma_\lambda$ . . . . .	101
§ XXI	The operator $\Pi_\lambda$ . . . . .	107
§ XXII	The reverse of an operator in $\mathcal{W}^*$ . . . . .	108
§ XXIII	Affine operators . . . . .	118
§ XXIV	The binary case . . . . .	121
§ XXV	F.S.R. cycles . . . . .	129
§ XXVI	A homomorphism of the de Bruijn graph . . . . .	132
§ XXVII	Some generalizations of F.S.R.'s . . . . .	134
References . . . . .		139
Appendix: F.S.R.'s in a practical environment . . . . .		143