Claude Carlet
Berk Sunar (Eds.)

LNCS 4547

Arithmetic of Finite Fields

First International Workshop, WAIFI 2007
Madrid, Spain, June 2007
Proceedings

Springer

Claude Carlet Berk Sunar (Eds.)

Arithmetic of Finite Fields

First International Workshop, WAIFI 2007
Madrid, Spain, June 2007
Proceedings

Springer

Volume Editors

Claude Carlet
Université Paris 8, Département de mathématiques
2, rue de la Liberté; 93526 - SAINT-DENIS Cedex 02, France
E-mail: claude.carlet@inria.fr

Berk Sunar
Worcester Polytechnic Institute
100 Institute Road, Worcester, MA 01609, USA
E-mail: sunar@wpi.edu

Library of Congress Control Number: 2007928526

CR Subject Classification (1998): E.4, I.1, E.3, G.2, F.2

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-73073-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-73073-6 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12077106 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4547

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Preface

These are the proceedings of WAIFI 2007. The conference was held in Madrid, Spain, during June 21–22, 2007. We are very grateful to the Program Committee members and to the external reviewers for their hard work! The conference received 94 submissions out of which 27 were finally selected for presentation. Each paper was refereed by at least two reviewers, and at least by three in the case of papers (co)-authored by Program Committee members. All final decisions were taken only after a clear position was clarified through additional reviews and comments. The Committee also invited Harald Niederreiter and Richard E. Blahut to speak on topics of their choice and we thank them for having accepted.

Special compliments go out to José L. Imaña, the general Co-chair and local organizer of WAIFI 2007, who brought the workshop to beautiful Madrid, Spain. WAIFI 2007 was organized by the department Computer Architecture of Facultad de Informática of the Universidad Complutense, in Madrid. We also would like to thank the General Co-chair Çetin K. Koç for his guidance. Finally, we would like to thank the Steering Committee for providing us with this wonderful opportunity.

The submission and selection of papers were done using the iChair software, developed at EPFL by Thomas Baignères and Matthieu Finiasz. Many thanks for their kind assistance! We also thank Gunnar Gaubatz for his precious help in this matter.

June 2007

Claude Carlet
Berk Sunar

Organization

Steering Committee

Jean-Pierre Deschamps	University Rovira i Virgili, Spain
José L. Imaña	Complutense University of Madrid, Spain
Çetin K. Koç	Oregon State University, USA
Christof Paar	Ruhr University of Bochum, Germany
Jean-Jacques Quisquater	Université Katholique de Louvain, Belgium
Berk Sunar	Worcester Polytechnic Institute, USA
Gustavo Sutter	Autonomous University of Madrid, Spain

Executive Committee

General Co-chairs

José L. Imaña	Complutense University of Madrid, Spain
Çetin K. Koç	Oregon State University, USA

Program Co-chairs

Claude Carlet	University of Paris 8, France
Berk Sunar	Worcester Polytechnic Institute, USA

Financial, Local Arrangements Chairs

Luis Piñuel	Complutense University of Madrid, Spain
Manuel Prieto	Complutense University of Madrid, Spain

Publicity Chair

Gustavo Sutter	Autonomous University of Madrid, Spain

Program Committee

Jean-Claude Bajard	CNRS-LIRMM in Montpellier, France
Ian F. Blake	University of Toronto, Canada
Marc Daumas	CNRS-LIRMM in Perpignan, France
Jean-Pierre Deschamps	University Rovira i Virgili, Spain
Josep Domingo-Ferrer	University Rovira i Virgili, Spain
Philippe Gaborit	University of Limoges, France
Joachim von zur Gathen	B-IT, University of Bonn, Germany
Pierrick Gaudry	LORIA-INRIA, France
Guang Gong	University of Waterloo, Canada
Jorge Guajardo	Philips Research, Netherlands
Anwar Hasan	University of Waterloo, Canada

Çetin K. Koç	Oregon State University, USA
Tanja Lange	Technische Universiteit Eindhoven, Netherlands
Julio López	UNICAMP, Brazil
Gary Mullen	Pennsylvania State University, USA
Harald Niederreiter	National University of Singapore, Singapore
Ferruh Ozbudak	Middle East Technical University, Turkey
Erkay Savaş	Sabanci University, Turkey
Igor Shparlinski	Macquarie University, Australia
Horacio Tapia-Recillas	UAM-Iztapalapa, D.F., Mexico
Apostol Vourdas	University of Bradford, UK

Referees

O. Ahmadi	M. Finiasz	A. Martínez-Ballesté
J. Aragonés	D. Freeman	N. Méloni
R.M. Avanzi	T. Güdü	Y. Nawaz
O. Barenys	C. Güneri	C. Negre
I. Barenys	K. Gupta	T.B. Pedersen
L. Batina	G. Hanrot	M.N. Plasencia
D.J. Bernstein	F. Hess	D. Pointcheval
P. Birkner	K. Horadam	T. Plantard
M. Cenk	L. Imbert	C. Ritzenthaler
J. Chung	S. Jiang	G. Saldamli
V. Daza	T. Kerins	Z. Saygı
C. Ding	D. Kohel	F. Sebe
A. Doğanaksoy	G. Kömürcü	B. Schoenmakers
N. Ebeid	G. Kyureghyan	A. Tisserand
N. El Mrabet	G. Leander	F. Vercauteren
H. Fan	J. Lutz	W. Willems

Sponsoring Institutions

Real Sociedad Matemática Española, Spain.
Ministerio de Educación y Ciencia, Spain.
Facultad de Informática de la Universidad Complutense de Madrid, Spain.
ArTeCs: Architecture and Technology of Computing Systems Group, Universidad Complutense de Madrid, Spain.
Universidad Complutense de Madrid, Spain.

Lecture Notes in Computer Science

For information about Vols. 1–4451

please contact your bookseller or Springer

Vol. 4581: A. Petrenko, M. Veanes, J. Tretmans, W. Grieskamp (Eds.), Testing of Software and Communicating Systems. XII, 379 pages. 2007.

Vol. 4549: J. Aspnes, C. Scheideler, A. Arora, S. Madden (Eds.), Distributed Computing in Sensor Systems. XIII, 417 pages. 2007.

Vol. 4547: C. Carlet, B. Sunar (Eds.), Arithmetic of Finite Fields. XI, 355 pages. 2007.

Vol. 4543: A.K. Bandara, M. Burgess (Eds.), Inter-Domain Management. XII, 237 pages. 2007.

Vol. 4542: P. Sawyer, B. Paech, P. Heymans (Eds.), Requirements Engineering: Foundation for Software Quality. IX, 384 pages. 2007.

Vol. 4541: T. Okadome, T. Yamazaki, M. Makhtari (Eds.), Pervasive Computing for Quality of Life Enhancemanet. IX, 248 pages. 2007.

Vol. 4539: N.H. Bshouty, C. Gentile (Eds.), Learning Theory. XII, 634 pages. 2007. (Sublibrary LNAI).

Vol. 4538: F. Escolano, M. Vento (Eds.), Graph-Based Representations in Pattern Recognition. XII, 416 pages. 2007.

Vol. 4537: K.C.-C. Chang, W. Wang, L. Chen, C.A. Ellis, C.-H. Hsu, A.C. Tsoi, H. Wang (Eds.), Advances in Web and Network Technologies, and Information Management. XXIII, 707 pages. 2007.

Vol. 4534: I. Tomkos, F. Neri, J. Solé Pareta, X. Masip Bruin, S. Sánchez Lopez (Eds.), Optical Network Design and Modeling. XI, 460 pages. 2007.

Vol. 4531: J. Indulska, K. Raymond (Eds.), Distributed Applications and Interoperable Systems. XI, 337 pages. 2007.

Vol. 4530: D.H. Akehurst, R. Vogel, R.F. Paige (Eds.), Model Driven Architecture- Foundations and Applications. X, 219 pages. 2007.

Vol. 4529: P. Melin, O. Castillo, L.T. Aguilar, J. Kacprzyk, W. Pedrycz (Eds.), Foundations of Fuzzy Logic and Soft Computing. XIX, 830 pages. 2007. (Sublibrary LNAI).

Vol. 4528: J. Mira, J.R. Álvarez (Eds.), Nature Inspired Problem-Solving Methods in Knowledge Engineering, Part II. XXII, 650 pages. 2007.

Vol. 4527: J. Mira, J.R. Álvarez (Eds.), Bio-inspired Modeling of Cognitive Tasks, Part I. XXII, 630 pages. 2007.

Vol. 4526: M. Malek, M. Reitenspieß, A. van Moorsel (Eds.), Service Availability. X, 155 pages. 2007.

Vol. 4525: C. Demetrescu (Ed.), Experimental Algorithms. XIII, 448 pages. 2007.

Vol. 4524: M. Marchiori, J.Z. Pan, C.d.S. Marie (Eds.), Web Reasoning and Rule Systems. XI, 382 pages. 2007.

Vol. 4523: Y.-H. Lee, H.-N. Kim, J. Kim, Y. Park, L.T. Yang, S.W. Kim (Eds.), Embedded Software and Systems. XIX, 829 pages. 2007.

Vol. 4522: B.K. Ersbøll, K.S. Pedersen (Eds.), Image Analysis. XVIII, 989 pages. 2007.

Vol. 4521: J. Katz, M. Yung (Eds.), Applied Cryptography and Network Security. XIII, 498 pages. 2007.

Vol. 4519: E. Franconi, M. Kifer, W. May (Eds.), The Semantic Web: Research and Applications. XVIII, 830 pages. 2007.

Vol. 4517: F. Boavida, E. Monteiro, S. Mascolo, Y. Koucheryavy (Eds.), Wired/Wireless Internet Communications. XIV, 382 pages. 2007.

Vol. 4516: L. Mason, T. Drwiega, J. Yan (Eds.), Managing Traffic Performance in Converged Networks. XXIII, 1191 pages. 2007.

Vol. 4515: M. Naor (Ed.), Advances in Cryptology - EUROCRYPT 2007. XIII, 591 pages. 2007.

Vol. 4514: S.N. Artemov, A. Nerode (Eds.), Logical Foundations of Computer Science. XI, 513 pages. 2007.

Vol. 4513: M. Fischetti, D.P. Williamson (Eds.), Integer Programming and Combinatorial Optimization. IX, 500 pages. 2007.

Vol. 4510: P. Van Hentenryck, L. Wolsey (Eds.), Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems. X, 391 pages. 2007.

Vol. 4509: Z. Kobti, D. Wu (Eds.), Advances in Artificial Intelligence. XII, 552 pages. 2007. (Sublibrary LNAI).

Vol. 4508: M.-Y. Kao, X.-Y. Li (Eds.), Algorithmic Aspects in Information and Management. VIII, 428 pages. 2007.

Vol. 4507: F. Sandoval, A. Prieto, J. Cabestany, M. Graña (Eds.), Computational and Ambient Intelligence. XXVI, 1167 pages. 2007.

Vol. 4506: D. Zeng, I. Gotham, K. Komatsu, C. Lynch, M. Thurmond, D. Madigan, B. Lober, J. Kvach, H. Chen (Eds.), Intelligence and Security Informatics: Biosurveillance. XI, 234 pages. 2007.

Vol. 4505: G. Dong, X. Lin, W. Wang, Y. Yang, J.X. Yu (Eds.), Advances in Data and Web Management. XXII, 896 pages. 2007.

Vol. 4504: J. Huang, R. Kowalczyk, Z. Maamar, D. Martin, I. Müller, S. Stoutenburg, K.P. Sycara (Eds.), Service-Oriented Computing: Agents, Semantics, and Engineering. X, 175 pages. 2007.

Vol. 4501: J. Marques-Silva, K.A. Sakallah (Eds.), Theory and Applications of Satisfiability Testing – SAT 2007. XI, 384 pages. 2007.

Vol. 4500: N. Streitz, A. Kameas, I. Mavrommati (Eds.), The Disappearing Computer. XVIII, 304 pages. 2007.

Vol. 4499: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security II. IX, 117 pages. 2007.

Vol. 4497: S.B. Cooper, B. Löwe, A. Sorbi (Eds.), Computation and Logic in the Real World. XVIII, 826 pages. 2007.

Vol. 4496: N.T. Nguyen, A. Grzech, R.J. Howlett, L.C. Jain (Eds.), Agent and Multi-Agent Systems: Technologies and Applications. XXI, 1046 pages. 2007. (Sublibrary LNAI).

Vol. 4495: J. Krogstie, A. Opdahl, G. Sindre (Eds.), Advanced Information Systems Engineering. XVI, 606 pages. 2007.

Vol. 4494: H. Jin, O.F. Rana, Y. Pan, V.K. Prasanna (Eds.), Algorithms and Architectures for Parallel Processing. XIV, 508 pages. 2007.

Vol. 4493: D. Liu, S. Fei, Z. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part III. XXVI, 1215 pages. 2007.

Vol. 4492: D. Liu, S. Fei, Z. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part II. XXVII, 1321 pages. 2007.

Vol. 4491: D. Liu, S. Fei, Z.-G. Hou, H. Zhang, C. Sun (Eds.), Advances in Neural Networks – ISNN 2007, Part I. LIV, 1365 pages. 2007.

Vol. 4490: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part IV. XXXVII, 1211 pages. 2007.

Vol. 4489: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part III. XXXVII, 1257 pages. 2007.

Vol. 4488: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part II. XXXV, 1251 pages. 2007.

Vol. 4487: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), Computational Science – ICCS 2007, Part I. LXXXI, 1275 pages. 2007.

Vol. 4486: M. Bernardo, J. Hillston (Eds.), Formal Methods for Performance Evaluation. VII, 469 pages. 2007.

Vol. 4485: F. Sgallari, A. Murli, N. Paragios (Eds.), Scale Space and Variational Methods in Computer Vision. XV, 931 pages. 2007.

Vol. 4484: J.-Y. Cai, S.B. Cooper, H. Zhu (Eds.), Theory and Applications of Models of Computation. XIII, 772 pages. 2007.

Vol. 4483: C. Baral, G. Brewka, J. Schlipf (Eds.), Logic Programming and Nonmonotonic Reasoning. IX, 327 pages. 2007. (Sublibrary LNAI).

Vol. 4482: A. An, J. Stefanowski, S. Ramanna, C.J. Butz, W. Pedrycz, G. Wang (Eds.), Rough Sets, Fuzzy Sets, Data Mining and Granular Computing. XIV, 585 pages. 2007. (Sublibrary LNAI).

Vol. 4481: J. Yao, P. Lingras, W.-Z. Wu, M. Szczuka, N.J. Cercone, D. Ślęzak (Eds.), Rough Sets and Knowledge Technology. XIV, 576 pages. 2007. (Sublibrary LNAI).

Vol. 4480: A. LaMarca, M. Langheinrich, K.N. Truong (Eds.), Pervasive Computing. XIII, 369 pages. 2007.

Vol. 4479: I.F. Akyildiz, R. Sivakumar, E. Ekici, J.C.d. Oliveira, J. McNair (Eds.), NETWORKING 2007. Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet. XXVII, 1252 pages. 2007.

Vol. 4478: J. Martí, J.M. Benedí, A.M. Mendonça, J. Serrat (Eds.), Pattern Recognition and Image Analysis, Part II. XXVII, 657 pages. 2007.

Vol. 4477: J. Martí, J.M. Benedí, A.M. Mendonça, J. Serrat (Eds.), Pattern Recognition and Image Analysis, Part I. XXVII, 625 pages. 2007.

Vol. 4476: V. Gorodetsky, C. Zhang, V.A. Skormin, L. Cao (Eds.), Autonomous Intelligent Systems: Multi-Agents and Data Mining. XIII, 323 pages. 2007. (Sublibrary LNAI).

Vol. 4475: P. Crescenzi, G. Prencipe, G. Pucci (Eds.), Fun with Algorithms. X, 273 pages. 2007.

Vol. 4474: G. Prencipe, S. Zaks (Eds.), Structural Information and Communication Complexity. XI, 342 pages. 2007.

Vol. 4472: M. Haindl, J. Kittler, F. Roli (Eds.), Multiple Classifier Systems. XI, 524 pages. 2007.

Vol. 4471: P. Cesar, K. Chorianopoulos, J.F. Jensen (Eds.), Interactive TV: a Shared Experience. XIII, 236 pages. 2007.

Vol. 4470: Q. Wang, D. Pfahl, D.M. Raffo (Eds.), Software Process Dynamics and Agility. XI, 346 pages. 2007.

Vol. 4469: K.-C. Hui, Z. Pan, R.C.-k. Chung, C.C.L. Wang, X. Jin, S. Göbel, E.C.-L. Li (Eds.), Technologies for E-Learning and Digital Entertainment. XVIII, 974 pages. 2007.

Vol. 4468: M.M. Bonsangue, E.B. Johnsen (Eds.), Formal Methods for Open Object-Based Distributed Systems. X, 317 pages. 2007.

Vol. 4467: A.L. Murphy, J. Vitek (Eds.), Coordination Models and Languages. X, 325 pages. 2007.

Vol. 4466: F.B. Sachse, G. Seemann (Eds.), Functional Imaging and Modeling of the Heart. XV, 486 pages. 2007.

Vol. 4465: T. Chahed, B. Tuffin (Eds.), Network Control and Optimization. XIII, 305 pages. 2007.

Vol. 4464: E. Dawson, D.S. Wong (Eds.), Information Security Practice and Experience. XIII, 361 pages. 2007.

Vol. 4463: I. Măndoiu, A. Zelikovsky (Eds.), Bioinformatics Research and Applications. XV, 653 pages. 2007. (Sublibrary LNBI).

Vol. 4462: D. Sauveron, K. Markantonakis, A. Bilas, J.-J. Quisquater (Eds.), Information Security Theory and Practices. XII, 255 pages. 2007.

Vol. 4459: C. Cérin, K.-C. Li (Eds.), Advances in Grid and Pervasive Computing. XVI, 759 pages. 2007.

Vol. 4453: T. Speed, H. Huang (Eds.), Research in Computational Molecular Biology. XVI, 550 pages. 2007. (Sublibrary LNBI).

Vol. 4452: M. Fasli, O. Shehory (Eds.), Agent-Mediated Electronic Commerce. VIII, 249 pages. 2007. (Sublibrary LNAI).

¥562.00元

Table of Contents

Structures in Finite Fields

Efficient Implementation and Architectures

Efficient Finite Field Arithmetic

Classification and Construction of Mappings over Finite Fields

Curve Algebra

Cryptography

Codes

Discrete Structures

Explicit Factorizations of Cyclotomic and Dickson Polynomials over Finite Fields

Robert W. Fitzgerald and Joseph L. Yucas

Southern Illinois University Carbondale

Abstract. We give, over a finite field F_q, explicit factorizations into a product of irreducible polynomials, of the cyclotomic polynomials of order $3 \cdot 2^n$, the Dickson polynomials of the first kind of order $3 \cdot 2^n$ and the Dickson polynomials of the second kind of order $3 \cdot 2^n - 1$.

Keywords: finite field, cyclotomic polynomial, Dickson polynomial.

1 Introduction

Explicit factorizations, into a product of irreducible polynomials, over F_q of the cyclotomic polynomials $Q_{2^n}(x)$ are given in [4] when $q \equiv 1 \pmod 4$. The case $q \equiv 3 \pmod 4$ is done in [5]. Here we give factorizations of $Q_{2^n r}(x)$ where r is prime and $q \equiv \pm 1 \pmod r$. In particular, this covers $Q_{2^n 3}(x)$ for all F_q of characteristic not 2, 3. We apply this to get explicit factorizations of the first and second kind Dickson polynomials of order $2^n 3$ and $2^n 3 - 1$ respectively.

Explicit factorizations of certain Dickson polynomials have been used to compute Brewer sums [1]. But our basic motivation is curiosity, to see what factors arise. Of interest then is how the generalized Dickson polynomials $D_n(x, b)$ arise in the factors of the cyclotomic polynomials and how the Dickson polynomials of the first kind appear in the factors of both kinds of Dickson polynomials.

Let q be a power of an odd prime and let $v_2(k)$ denote the highest power of 2 dividing k. We will only consider the case where r is prime and $q \equiv \pm 1 \pmod r$. We recall the general form of the factors of cyclotomic polynomials in this case (see [4] 3.35 and 2.47).

Proposition 1. *Let $L = v_2(q^2 - 1)$, and work over F_q.*

1. *Suppose $q \equiv 1 \pmod r$. Then:*
   (a) *For $0 \le n \le v_2(q-1)$, $Q_{2^n r}(x)$ is a product of linear factors.*
   (b) *For $v_2(q-1) < n \le L$, $Q_{2^n r}(x)$ is a product of irreducible quadratic polynomials.*
   (c) *For $n > L$, $Q_{2^n r}(x) = \prod f_i(x^{2^{n-L}})$, where $Q_{2^L r}(x) = \prod f_i(x)$.*
2. *Suppose $q \equiv -1 \pmod r$. Then:*
   (a) *For $0 \le n \le L$, $Q_{2^n r}(x)$ is a product of irreducible quadratic factors.*
   (b) *For $n > L$, $Q_{2^n r}(x) = \prod f_i(x^{2^{n-L}})$, where $Q_{2^L r}(x) = \prod f_i(x)$.*

C. Carlet and B. Sunar (Eds.): WAIFI 2007, LNCS 4547, pp. 1–10, 2007.

2 Factors of Cyclotomic Polynomials

As before, $L = v_2(q^2-1)$ and $r = 2s+1$ be a prime. Let $\Omega(k)$ denote the primitive kth roots of unity in F_{q^2}.

We will often use the following, which is equation 7.10 in [4]. For $m \geq 0$

$$D_{2m}(x,c) = D_m(x^2 - 2c, c^2).$$

Lemma 1. *Suppose $q \equiv -1 \pmod{r}$. Let N denote the norm $F_{q^2} \to F_q$.*

1. *If $q \equiv 3 \pmod 4$ and $\rho \in \Omega(2^n)$, for $n \leq L$, then*

$$N(\rho) = \begin{cases} 1, & \text{if } 2 \leq n < L \\ -1, & \text{if } n = L. \end{cases}$$

2. *If $\omega \in \Omega(r)$ then $N(\omega) = 1$.*
3. *If $\alpha \in F_{q^2}$ and $N(\alpha) = a$ then $\alpha + a/\alpha \in F_q$.*

Proof. (1) Since $q-1 \equiv 2 \pmod 4$, $L-1$ is the highest power of 2 dividing $q+1$. Let $\rho \in \Omega(2^L)$. Now $N(\rho) = \rho^{q+1}$ so that $N(\rho)^2 = \rho^{2(q+1)} = 1$ and $N(\rho) = \pm 1$. If $N(\rho) = 1$ then $\rho^{q+1} = 1$ and $2^L = o(\rho)$ divides $q+1$, a contradiction. Hence $N(\rho) = -1$. If $\omega \in \Omega(2^n)$ for $n < L$, then ω is an even power of ρ and so $N(\omega) = 1$.

(2) $N(\omega)^r = N(\omega^r) = 1$ and, as r is prime, the only rth root of unity in F_q is 1. So $N(\omega) = 1$.

(3) We have $\alpha\alpha^q = a$ so that $\alpha + a/\alpha = \mathrm{tr}(\alpha) \in F_q$. □

Theorem 1. *1. Suppose $q \equiv -1 \pmod{r}$ and $q \equiv 3 \pmod 4$.*

(a) $Q_r(x) = \prod_{a \in S_1}(x^2 - ax + 1)$ and $Q_{2r}(x) = \prod_{a \in S_1}(x^2 + ax + 1)$, where S_1 is the set of roots of $1 + \sum_{i=1}^{s} D_i(x,1)$

(b) For $2 \leq n < L$, $Q_{2^n r}(x) = \prod_{a \in S_n}(x^2 + ax + 1)$, where S_n is the set of roots of $1 + \sum_{i=1}^{s}(-1)^s D_{2^{n-1}i}(x,1)$.

(c) For $n \geq L$, $Q_{2^n r}(x) = \prod_{b \in T_L}(x^{2^{n-L+1}} + bx^{2^{n-L}} - 1)$, where T_L is the set of roots of $1 + \sum_{i=1}^{s}(-1)^s D_{2^{L-1}i}(x,-1)$.

2. Suppose $q \equiv -1 \pmod{r}$ and $q \equiv 1 \pmod 4$.

(a) $Q_r(x) = \prod_{a \in S_1}(x^2 - ax + 1)$ and $Q_{2r}(x) = \prod_{a \in S_1}(x^2 + ax + 1)$.

(b) For $2 \leq n \leq L$,

$$Q_{2^n r}(x) = \prod_{\rho \in \Omega(2^{n-1})} \prod_{b \in T(\rho)} (x^2 + bx + \rho),$$

where $T(\rho)$ is the set of roots in F_q of $1 + \sum_{i=1}^{s}(-1)^i D_{2^{n-1}i}(x,\rho)$.

(c) For $n > L$, $Q_{2^n r}(x) = \prod_{\rho \in \Omega(2^{L-1})} \prod_{b \in T(\rho)} (x^{2^{n-L+1}} + bx^{2^{n-L}} + \rho)$.

3. Suppose $q \equiv 1 \pmod{r}$ and $q \equiv 3 \pmod 4$.

(a) $Q_r(x) = \prod(x - \omega)$, $Q_{2r}(x) = \prod(x + \omega)$ and $Q_{4r}(x) = \prod(x^2 + \omega)$, with each product over $\Omega(r)$.

(b) For $3 \le n < L$,

$$Q_{2^n r}(x) = \prod_{\omega \in \Omega(r)} \prod_{c \in U_n} (x^2 + c\omega x + \omega^2)$$

where U_n *is the set of roots in* F_q *of* $D_{2^{n-2}}(x, 1)$.

(c) For $n \ge L$,

$$Q_{2^n r}(x) = \prod_{\omega \in \Omega(r)} \prod_{d \in V_L} (x^{2^{n-L+1}} + d\omega x - \omega^2)$$

where V_L *is the set of roots in* F_q *of* $D_{2^{L-2}}(x, -1)$.

4. Suppose $q \equiv 1 \pmod r$ *and* $q \equiv 1 \pmod 4$.

(a) $Q_r(x) = \prod_{\omega \in \Omega(r)} (x - \omega)$.

(b) For $1 \le n < L$,

$$Q_{2^n r}(x) = \prod_{\omega \in \Omega(r)} \prod_{\rho \in \Omega(2^n)} (x + \omega\rho)$$

(c) For $n \ge L$,

$$Q_{2^n r}(x) = \prod_{\omega \in \Omega(r)} \prod_{\rho \in \Omega(2^{L-1})} (x^{2^{n-L+1}} + \omega\rho).$$

Proof. (1) If $\omega \in \Omega(r)$ then $N(\omega) = 1$ and $\omega + 1/\omega \in F_q$ by Lemma 1. So

$$Q_r(x) = \prod_{\omega \in \Omega(r)} (x - \omega) = \prod (x^2 - ax + 1),$$

is a factorization over F_q, where a runs over all distinct $\omega + \omega^{-1}$. The quadratic factors are irreducible by Corollary 1. Also,

$$\begin{aligned} 1 + \sum_{i=1}^{s} D_i(a, 1) &= 1 + \sum_{i=1}^{s} (\omega^i + \omega^{-i}) \\ &= \omega^{-s} \left(\sum_{j=0}^{2s} \omega^j \right) = 0. \end{aligned}$$

As $\deg(1 + \sum D_i(x, 1)) = s$, the a are all of the roots. Further,

$$Q_{2r}(x) = Q_r(-x) = \prod (x^2 + ax + 1),$$

which completes the proof of (1)(a).

For (1)(b), the case $n = 2$ can be checked directly. So suppose $3 \le n < L$. Note that $a_2 = \rho\omega + (\rho\omega)^{-1}$ as $\rho^{-1} = -\rho$. Let $\rho_n \in \Omega(2^n)$ and set $a_n = \rho\rho_n\omega + (\rho\rho_n\omega)^{-1}$. We claim that $a_n \in F_q$ and that $a_n^2 = 2 - a_{n-1}$ (with a_{n-1}

defined via a different choice of ω). Namely, $N(\rho\rho_n\omega) = 1$ as $n < L$ and so $a_n \in F_q$. And

$$\begin{aligned} a_n^2 &= \rho^2\rho_n^2\omega^2 + (\rho^2\rho_n^2\omega^2)^{-1} + 2 \\ &= -\rho_{n-1}\omega^2 - (\rho_{n-1}\omega^2)^{-1} + 2 = 2 - a_{n-1}. \end{aligned}$$

Then inductively,

$$Q_{2^n r}(x) = \prod(x^4 + a_{n-1}x^2 + 1) = \prod(x^2 + a_n x + 1)(x^2 - a_n x + 1),$$

where again the quadratic factors are irreducible over F_q. Lastly, again by induction, the a_n are roots of

$$1 + \sum_{i=1}^{s}(-1)^i D_{2^{n-2i}}(-(x^2-2), 1) = 1 + \sum_{i=1}^{s}(-1)^i D_{2^{n-1i}}(x, 1).$$

This has degree $2^{n-1}s$ and there are $2^{n-1}s = \frac{1}{2}\deg Q_{2^n r}(x)$ many a_n's. So the a_n's are all of the roots of the above polynomial.

We finish the proof of (1) by checking the case $n = L$ (the cases $n > L$ then follow from Corollary 1). Now $N(\rho\rho_L\omega) = -1$ by Lemma 1, so that $b = \rho\rho_L\omega - (\rho\rho_L\omega)^{-1} \in F_q$. And $b^2 = -a_{L-1} - 2$. Hence

$$x^4 + a_{L-1}x^2 + 1 = (x^2 + bx - 1)(x^2 - bx - 1)$$

is an irreducible factorization over F_q. Lastly, b is a root of

$$1 + \sum_{i=1}^{s}(-1)^i D_{2^{L-2i}}(-(x^2+2), 1) = 1 + \sum_{i=1}^{s}(-1)^i D_{2^{L-1i}}(x, -1).$$

As before, the b's are all of the roots.

(2) First note that $L = v_2(q-1) + 1$ so that $\Omega(2^n) \subset F_q$ for $n < L$. The factorization of $Q_r(x)$ and $Q_{2r}(x)$ is the same as in (1). For (2)(b), again the case $n = 2$ can be checked directly. For $2 < n < L$ we work by induction. Set $b_n = \rho_n(\omega + \omega^{-1})$, for $\rho_n \in \Omega(2^n)$. Then $b_n \in F_q$ and $b_n^2 = b_{n-1} + 2\rho_{n-1}$. Note that the set of b_{n-1}'s is closed under multiplication by -1. Hence we need only check that

$$x^4 - a_{n-1}x^2 + \rho_{n-1} = (x^2 + b_n x + \rho_n)(x^2 - b_n x + \rho_n).$$

Further, b_n is a root of

$$1 + \sum_{i=1}^{s}(-1)^i D_{2^{n-2i}}(x^2 - 2\rho_{n-1}, \rho_{n-2}) = 1 + \sum_{i=1}^{s}(-1)^i D_{2^{n-1i}}(x, \rho_{n-1}).$$

Set $\delta_{\rho_{n-1}}(x) = 1 + \sum_{i=1}^{s}(-1)^i D_{2^{n-1i}}(x, \rho_{n-1})$. Fix a ρ_{n-1} and pick a ρ_n with $\rho_n^2 = \rho_{n-1}$. To complete the proof of (2)(b) we need to check that the b_n's are all of the roots of $\delta_{\rho_{n-1}}(x)$ in F_q.

For $n = 2$, $\deg \delta_{\rho_1} = 2s$ which is the number of b_2's so δ_{ρ_1} has no other roots. Inductively assume that

$$\delta_{\rho_{n-1}}(x) = \prod (x - b_n) \cdot h(x),$$

where $h(x)$ is a product of non-linear factors. Then

$$\delta_{\rho_n}(x) = \delta_{rho_{n-1}}(x^2 - 2\rho_n) = \prod (x^2 - 2\rho_n - b_n) \cdot h(x^2 - 2\rho_n).$$

Now $x^2 - 2\rho_n - b_n$ splits in F_q iff $2\rho_n + b_n$ is a square in F_q. The b_n's in $T(\rho_n)$ are $\pm\rho_n(\omega + \omega^{-1})$. And $2\rho_n + \rho_n(\omega + \omega^{-1}) = \rho_n(\omega^r + \omega^{-r})^2$ is a square (in fact, the square of a b_{n+1}) while $2\rho_n - \rho_n(\omega + \omega^{-1}) = -\rho_n(\omega^r - \omega^{-r})^2$ is not a square (as $\omega^r - \omega^{-r} \notin F_q^2$). Hence the roots of δ_{ρ_n} in F_q are precisely the b_{n+1}'s.

(2)(c) The case $n = L$ must be done separately as $\rho_L \notin F_q$. Set $b_L = \rho\rho_L(\omega - \omega^{-1})$. As in the proof of (a), $(\omega - \omega^{-1})^2 \in F_q \setminus F_q^2$. And $\rho_{L-1} \in F_q \setminus F_q^2$. Hence $\rho_{L-1}(\omega - \omega^{-1})^2 \in F_q^2$ and its square root, b_L, is in F_q. Also $b_L^2 = -b_{L-1} + 2\rho_{L-1}$. Then

$$x^4 + b_{L-1}x^2 + \rho_{L-2} = (x^2 + b_L x + \rho_{L-1})(x^2 - b_L x + \rho_{L-1}),$$

giving the desired factorization. Further, $b_{L-1} = -b_L^2 + 2\rho_{L-1}$ so that b_L is a root of

$$1 + \sum_{i=1}^{s} (-1)^i D_{2^{L-2i}}(-(x^2 - 2\rho_{L-1}), \rho_{L-2}) = 1 + \sum_{i=1}^{s} (-1)^i D_{2^{L-1-i}}(x, \rho_{L-1}).$$

As before, these are all of the roots in F_q. Finally, the cases $n > L$ follow from Corollary 1.

(3) As $q \equiv 1 \pmod{r}$, we have $\Omega(r) \subset F_q$. The factorizations for Q_r and Q_{2r} are clear and that of Q_{4r} follows from Corollary 1. We do the case $n = 3 < L$ (the case $n = 3 = L$ will follow from the case $n = L$ to be done later). Let $\rho_3 \in \Omega(2^3)$. Then $\rho_3 \in F_{q^2} \setminus F_q$, $N(\rho_3) = 1$ as $n < L$, and $c_3 = \rho_3 + \rho_3^{-1} \in F_q$. Also $c_3^2 = \rho + \rho^{-1} + 2 = 2$. A typical factor of Q_{4r} can be written as $x^2 + \omega^4$ and we have

$$x^4 + \omega^4 = (x^2 + c_2\omega x + \omega^2)(x^2 - c_2\omega x + \omega^2),$$

giving the desired factorization of $Q_{2^3 r}(x)$. Note that $c_3 = \pm\sqrt{2}$, the roots of $D_2(x, 1) = x^2 - 2$.

Now suppose $3 < n < L$ and work inductively. We have $N(\rho_n) = 1$ so that $c_n = \rho_n + \rho_n^{-1} \in F_q$. And $c_n^2 = c_{n-1} + 2$. A typical factor of $Q_{2^{n-1}r}(x)$ can be written as $x^2 - c_{n-1}\omega^2 x + \omega^4$ and we have

$$x^4 - c_{n-1}\omega^2 x^2 + \omega^4 = (x^2 + c_n\omega x + \omega^2)(x^2 - c_n\omega x + \omega^2),$$

giving the desired factorization. Further, c_n is a root of $D_{2^{n-3}}(x^2 - 2, 1) = D_{2^{n-2}}(x, 1)$. A counting argument shows the c_n's are all of the roots.

Next suppose $n = L$. We have $N(\rho_L) = -1$ so that $c_L = \rho_L - \rho_L^{-1} \in F_q$. And $c_L^2 = c_{L-1} - 2$. Then

$$x^4 - c_{L-1}\omega^2 x^2 + \omega^4 = (x^2 + c_L\omega x - \omega^2)(x^2 - c_L\omega x - \omega^2),$$