

1. Record Nr.	UNINA9910957331703321
Autore	Storme Leo
Titolo	Current research topics in Galois geometry / / Leo Storme and Jan de Beule, editors
Pubbl/distr/stampa	New York, : Nova Science Publishers, 2012
ISBN	1-62081-363-7
Edizione	[1st ed.]
Descrizione fisica	1 online resource (286 p.)
Collana	Mathematics research developments Cryptography, steganography and data security
Altri autori (Persone)	StormeLeo BeuleJan de
Disciplina	516/.11
Soggetti	Galois theory Geometry, Algebraic
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- CONTENTS -- PREFACE -- References -- CONSTRUCTIONS AND CHARACTERIZATIONS OF CLASSICAL SETS IN $PG(n, q)$ -- Abstract -- 1. Introduction -- 2. Classical Sets with Few Intersection Numbers in $PG(2, q)$ -- 2.1. Conics, Ovals and Hyperovals -- 2.1.1. Known Hyperovals -- Remarks -- 2.1.2. Characterization Theorems of Conics and Related Sets -- 2.2. Maximal Arcs -- 2.2.1. Introduction -- 2.2.2. The Known Constructions of Maximal Arcs -- The Construction by R. Mathon -- The Construction by R. Denniston -- The Constructions by J. A. Thas -- Remark -- 2.2.3. Some Characterization Theorems for Maximal Arcs -- 2.2.4. Maximal Arcs in Small Desarguesian Planes -- 2.3. Hermitian Curves and Unitals -- 2.3.1. Definitions and Constructions -- Remarks -- 2.3.2. Characterization Theorems -- 2.4. Characterizing Subplanes of $PG(2, q)$ -- Remark -- 3. Classical Sets with Few Intersection Numbers in $PG(n, q)$, $n \geq 3$ -- 3.1. Quadrics and Quasi-quadrics -- 3.1.1. Definitions -- 3.1.2. Characterization Theorems -- Remarks -- Remark -- 3.1.3. Ovoids and Generalizations -- 3.2. Hermitian Varieties -- 3.3. Subgeometries -- Open Problems -- References -- SUBSTRUCTURES OF FINITE CLASSICAL POLAR SPACES -- Abstract -- 1. Finite Classical Polar Spaces -- 2. Isomorphisms of Finite Classical Polar Spaces -- 3. Ovoids, Spreads, m -systems and m -ovoids -- 3.1. Ovoids -- 3.2. Spreads -- 3.3. m -

Systems -- 3.4. m-Ovoids -- 4. Partial Ovoids and Partial Spreads --
 4.1. Partial Ovoids -- 4.2. Partial Spreads -- 5. Covers and Blocking
 Sets -- 5.1. Covers -- 5.2. Blocking Sets -- References -- BLOCKING
 SETS IN PROJECTIVE SPACES -- Abstract -- 1. Introduction and De
 nitions -- 2. History and Basic Bounds -- 3. Natural Constructions --
 3.1. Subgeometry -- 3.2. Cone and Projection -- 3.3. Directions and
 the Generalized Rédei Construction -- 4. Linear Blocking Sets -- 5.
 More Constructions.
 5.1. Planar Constructions -- 5.2. Sporadic Constructions in Higher
 Dimensions -- 5.3. More Constructions in Higher Dimensions -- 5.4.
 The Mazzocca, Polverino, Storme Constructions -- 5.5. Some
 Interesting Examples Obtained by the MPS Construction -- 6. Af ne
 Blocking Sets -- Acknowledgm ents -- References -- LARGE CAPS IN
 PROJECTIVE GALOIS SPACES -- 1. What Is a Cap? -- 2. Classical
 Examples -- 3. Exceptional Caps -- The Ternary Case -- When $q \geq 3$ --
 4. The Link to Linear Codes -- 5. General Bounds -- 6. Recursive
 Constructions -- 7. Families of Caps in Fixed Dimension -- The Case of
 Projective Dimension $d = 4$ -- Projective Dimension $d \geq 5$ over F_5 --
 Higher Dimensions -- 8. Concrete Bounds -- 9. The Atoms of Cap
 Theory -- The Complete 14-cap in $PG(3, 4)$ -- A 66-cap in $PG(4, 5)$ -- A
 132-cap in $PG(4, 7)$ -- A 208-cap in $PG(4, 8)$ -- A 195-cap in $PG(5, 5)$ --
 A 434-cap in $PG(5, 7)$ -- 10. An Asymptotic Problem -- 11. Additive
 Codes and Quantum Caps -- 12. A Problem in Additive Number Theory
 -- A Global Approach -- Acknowledgm ents -- References -- THE
 POLYNOMIAL METHOD IN GALOIS GEOMETRIES -- Abstract -- 1.
 Introduction -- 2. Combinatorial Nullstellensatz -- 3. Nullstellensatz
 atze for Lower Dimensional Subspaces? -- 4. Lacunary Polynomials --
 5. Vector Spaces of Polynomials and Functions over F_q -- 6. Field
 Extensions as Vector Spaces -- 7. Algebraic Curves over Finite Fields --
 8. Resultant of Polynomials in Two Variables -- 9. Open Problems --
 10. Final Comments -- Acknowledgments -- References -- FINITE
 SEMIFIELDS -- 1. Introduction and Preliminaries -- 1.1. De nition and
 First Properties -- 1.2. Projective Planes and Isotopism -- 1.3. Spreads
 and Linear Sets -- 1.4. Dual and Transpose of a Semi eld, the Knuth
 Orbit -- 2. Semi elds: A Geometric Approach -- 2.1. Linear Sets and the
 Segre Variety -- 2.2. BEL-construction -- 3. Rank Two Semi elds.
 4. Symplectic Semi elds and Commutative Semi elds -- 5. Rank Two
 Commutative Semi elds -- 5.1. Translation Generalized Quadrangles
 and Eggs -- 5.2. Semi eld Flocks and Translation Ovoids -- 6. Known
 Examples and Classi cation Results -- 6.1. Classi cation Results for Any
 q -- 6.2. Classi cation Results for Small Values of q -- 7. Open
 Problems -- References -- CODES OVER RINGS AND RING GEOMETRIES
 -- Abstract -- 1. Projective and Af ne Hjelmslev Spaces -- 2.
 Coordinate Hjelmslev Geometries -- 3. Multisets of Points in Projective
 Hjelmslev Geometries and Linear Codes over Finite Chain Rings -- 3.1.
 Multisets of Points in $PHG(R_k, R)$ -- 3.2. Linear Codes over Finite Chain
 Rings -- 3.3. Equivalence of Multisets of Points and Linear Codes --
 3.4. Some Classes of Codes De ned Geometrically -- 4. Arcs in
 Projective Hjelmslev Planes -- 4.1. The Maximal Arc Problem -- 4.2. A
 General Upper Bound on the Size of an Arc -- 4.3. Constructions for
 Arcs -- 4.4. $(k, 2)$ -Arcs -- 4.5. Dual Constructions -- 4.6.
 Constructions Using Automorphisms -- 4.7. Tables for Arcs in
 Geometries over Small Chain Rings -- 5. Blocking Sets in Projective
 Hjelmslev Planes -- 5.1. General Results -- 5.2. Rédei Type Blocking
 Sets -- Acknowledgments -- References -- GALOIS GEOMETRIES AND
 CODING THEORY -- Abstract -- 1.0 Linear Codes over Finite Fields --
 1.01. General De nitions -- 1.12. Automorphisms of Linear Codes --
 1.13. The Spectrum of a Linear Code -- 1.14. Generalized

HammingWeights -- 2.0 Arcs in Galois Geometries -- 2.01. Multiarcs and Minihypers -- 2.02. Equivalence of Multisets -- 2.03. Arcs and Codes -- 2.14. Weight Hierarchy and Generalized Spectra for Arcs -- 2.25. Constructions for Arcs -- Sum of Multisets -- Restriction to a Subspace -- Projections of Arcs -- The Dual Construction for Arcs -- 3.0 Arcs and Linear MDS Codes -- 3.01. Introduction to Arcs and Linear MDS Codes. 3.72. The Largest Arcs in Galois Geometries -- 3.73. Arcs in $PG(2, q)$ -- 3.124. Results in Higher Dimensions -- 3.175. Open Problems -- 4.0 Minihypers and the Griesmer Bound -- 4.01. A Geometrical Proof of the Griesmer Bound -- 4.12. Minihypers and the Belov-Logachev-Sandimirov Construction -- 5.0 Saturating Sets in Galois Geometries and Covering Radius -- 5.61. Open Problems -- 6.0 Extension Results -- 6.01. The Extension Result of Hill and Lizak -- 6.72. Diversity and Extendability -- 6.83. Extension Results Depending on Divisibility and Quasi-divisibility -- 7.0 Codes Arising from Incidence Matrices of Galois Geometries -- 7.01. Linear Codes Defined by Incidence Matrices of Galois Geometries -- 7.02. Small Weight Codewords -- 8.0 A Geometrical Result Obtained via Linear Codes -- Acknowledgments -- References -- APPLICATIONS OF GALOIS GEOMETRY TO CRYPTOLOGY -- Abstract -- 1. Introduction -- 1.1. Cryptography -- 1.2. Galois Geometry in Cryptography -- 2. Secret Sharing Schemes -- 2.1. Model for Secret Sharing -- 2.2. Linear Secret Sharing Schemes -- 2.3. Ideal Secret Sharing Schemes -- 2.4. Efficient Linear Secret Sharing Schemes -- 2.5. Specific Families of Access Structures -- 2.6. Secret Sharing Schemes with Extended Capabilities -- 2.6.1. Multiplicative Linear Secret Sharing Schemes -- 2.6.2. Multisecret Sharing Schemes -- 3. Authentication Codes -- 3.1. A-codes -- 3.2. A2-codes -- 3.3. Research Approaches -- 3.4. Geometric Constructions -- 4. Key Predistribution Schemes -- 4.1. Requirements -- 4.2. KPSs Based on Geometry -- 5. Multivariate Equation Systems -- 5.1. Multivariate Cryptography -- 5.1.1. Digital Signatures -- 5.1.2. The Oil and Vinegar Signature Scheme -- 5.1.3. Kipnis and Shamir's Cryptanalysis of the Oil and Vinegar Signature Scheme -- 5.2. Algebraic Cryptanalysis -- 6. The Advanced Encryption Standard -- 6.1. The Design of AES. 6.1.1. The AES S-box -- 6.1.2. Diffusion in AES -- 6.2. Geometric Properties of AES -- 6.2.1. The Group Generated by AES -- 6.2.2. The AES Difference Table -- 6.2.3. The BES Representation of AES -- 7. Concluding Remarks -- Acknowledgments -- References -- GALOIS GEOMETRIES AND LOW-DENSITY PARITY-CHECK CODES -- Abstract -- Introduction -- Constructions -- Structure of This Article -- 1. Low-Density Parity-Check Codes -- 2. Decoding of LDPC Codes -- 2.1. The Sum-product Algorithm -- 3. Assessing the Quality of an LDPC Code -- 4. Finite Incidence Structures and LDPC Codes -- 5. LDPC Codes from Linear Spaces -- 5.1. LDPC Codes Derived from Affine Spaces -- 5.2. LDPC Codes Derived from Projective Spaces -- 5.3. Variations and Concluding Remarks -- 6. LDPC Codes from Partial Linear Spaces -- 6.1. LDPC Codes Derived from Generalized Quadrangles -- Further Results -- 6.2. LDPC Codes from Triangle-Free Geometries -- Further Constructions and Concluding Remarks -- 7. Open Problems -- Acknowledgments -- References -- Index.

Sommario/riassunto

Galois geometry is the theory that deals with substructures living in projective spaces over finite fields, also called Galois fields. This collected work presents current research topics in Galois geometry, and their applications. Presented topics include classical objects, blocking sets and caps in projective spaces, substructures in finite classical polar spaces, the polynomial method in Galois geometry, finite semifields, links between Galois geometry and coding theory, as well as links

between Galois geometry and cryptography. (Imprint: Nova)
