# NOTE ON SYSTEMS OF POLYNOMIAL EQUATIONS OVER FINITE FIELDS

Vincenzo Acciaro

TR-221, MARCH 1993

School of Computer Science, Carleton University
Ottawa, Canada, KIS 5B6

# Note on systems of polynomial equations over finite fields

Vincenzo Acciaro
(acciaro@scs.carleton.ca)
School of Computer Science, Carleton University
Ottawa, Canada, K1S 5B6
and
Dipartimento di Informatica, Bari, Italy

**Abstract**

Let $F$ be a finite field of $q$ elements and characteristic $p$ (so $q = p^n$ for some $n \geq 1$) and let $\Gamma := \{f_i(x_1, \ldots, x_r) = 0 | i = 1, \ldots, s\}$ be a system of polynomial equations with coefficients in $F$.

In this paper we relate the structure of the $F$-algebra $F[x_1, \ldots, x_r]/(f_1(x_1, ..., x_r), \ldots, f_s(x_1, \ldots, x_r), x_1^q - x_1, \ldots, x_r^q - x_r)$ to the roots of $\Gamma$ in $F^r$.

# 1 Introduction and definitions

Let $F$ be a finite field of $q$ elements and characteristic $p$, and let

$$\Gamma := \{f_i(x_1, \ldots, x_r) = 0 | i = 1, \ldots, s\}$$

be a system of $s$ polynomial equations in $r$ variables with coefficients in $F$. Consider the $F$-algebra $A := F[x_1, \ldots, x_r]/I$, where

$$I := (f_1(x_1, \ldots, x_r), \ldots, f_s(x_1, \ldots, x_r), x_1^q - x_1, \ldots, x_r^q - x_r)$$

In this paper we show that the number of distinct solutions of $\Gamma$ in $F^r$ equals the dimension $k$ of the algebra $A$ over $F$.

Furthermore, given the regular representation of the algebra $A$, we show that the roots of $\Gamma$ in $F^r$ can be obtained as the eigenvalues of the images of $x_m$, $m \in \{1, \ldots, r\}$.

The special case of a single polynomial deserves particular attention — it is enough to think about the implications in areas such as cryptography and coding theory — we devote to this case the last section of our paper.

# 2 The main theorems

THEOREM 1 *The algebra $A$ is finite dimensional and commutative.*

PROOF Indeed $A$ is spanned by the elements

$$x_1^{i_1} x_2^{i_2} \ldots x_r^{i_r} + I \quad (i_1, \ldots, i_r = 0, \ldots, q-1)$$

and therefore its dimension over $F$ is bounded by $q^r$. The commutativity of $A$ is inherited from the commutativity of $F[x_1, \ldots, x_k]$. □

THEOREM 2 *The algebra $A$ is semisimple.*

PROOF Remember that in a commutative finite dimensional algebra the radical consists of all the nilpotent elements [3, pag.162].
In order to prove that $A$ is semisimple, all we need to show is that $A$ does not contain any nonzero nilpotent element or, in other words, $rad(A) = (0)$. For this purpose, let

$$g := \sum a_{i_1, i_2, \ldots, i_r} x_1^{i_1} x_2^{i_2} \ldots x_r^{i_r} + I$$

be an element of $A$. We have

$$g^q = \sum (a_{i_1,i_2,\ldots,i_r})^q \; x_1^{i_1 q} x_2^{i_2 q} \ldots x_r^{i_r q} + I = g$$

since $a^q = a$ for all $a \in F$ and $x_i^q \equiv x_i \pmod{I}$ for $i \in \{1, \ldots, r\}$.
It is now clear that if $g^m = 0$ for some $m \geq 1$ then $g = 0$, so 0 is the only nilpotent element in $A$. □

THEOREM 3 *The algebra $A$ is a direct product of fields isomorphic to $F$*

PROOF Any commutative semisimple algebra is a direct product of fields [4, page 54]. Therefore

$$A \cong F_1 \times \ldots \times F_k$$

say, where each $F_i$ is an extension field of $F$. Assume that a field $F_i$ in the decomposition of $A$ is a proper extension field of $F$. Because $F_i$ is finite, it must contain a primitive element, that is an element $t$ whose order in the multiplicative group $F_i^*$ of $F_i$ is exactly $|F_i| - 1$. Consider the element $(0, \ldots, 0, t, 0, \ldots, 0)$ in $A$: its order is strictly greater than $q-1$, which contradicts the fact that for any $g \in A$ we have $g^q = g$. □

THEOREM 4 *The dimension $k$ of $A$ over $F$ is equal to the number of distinct roots of $\Gamma$ in $F^r$.*

PROOF For each root $\alpha_j := (\alpha_{j_1}, \ldots, \alpha_{j_r})$ of $\Gamma$ there is a surjective $F$-algebra homomorphism $\nu_{\alpha_j} : A \to F$ in which $x_i + I \mapsto \alpha_{j_i}$, and conversely, each surjective homomorphism $A \to F$ has this form.
Now we show that there are exactly $k$ surjective $F$-algebra homomorphisms $A \to F$. Since $A$ is a direct product of $k$ fields isomorphic to $F$ we can assume $A = Fe_1 \oplus \ldots \oplus Fe_k$ where the elements $e_1, \ldots, e_k$ form a complete set of primitive orthogonal idempotents in $A$. It is easy to see that there are at least $k$ surjective $F$-algebra homomorphisms $A \to F$, where the $i^{th}$ one maps the element $e_i$ to 1 and $e_j$ to 0 for $j \neq i$. Conversely, let $\nu : A \to F$ be a surjective $F$-algebra homomorphism. Now, any ring homomorphism must map an idempotent to an idempotent, and therefore there are only two possibilities for $\nu(e_i)$, namely 0 or 1. Let us assume that for $i \neq j$ we have $\nu(e_i) = \nu(e_j) = 1$ : then $e_i e_j = 0$ and $\nu(e_i e_j) = 1$, contradicting the fact that in any ring homomorphism 0 must be mapped to 0. □

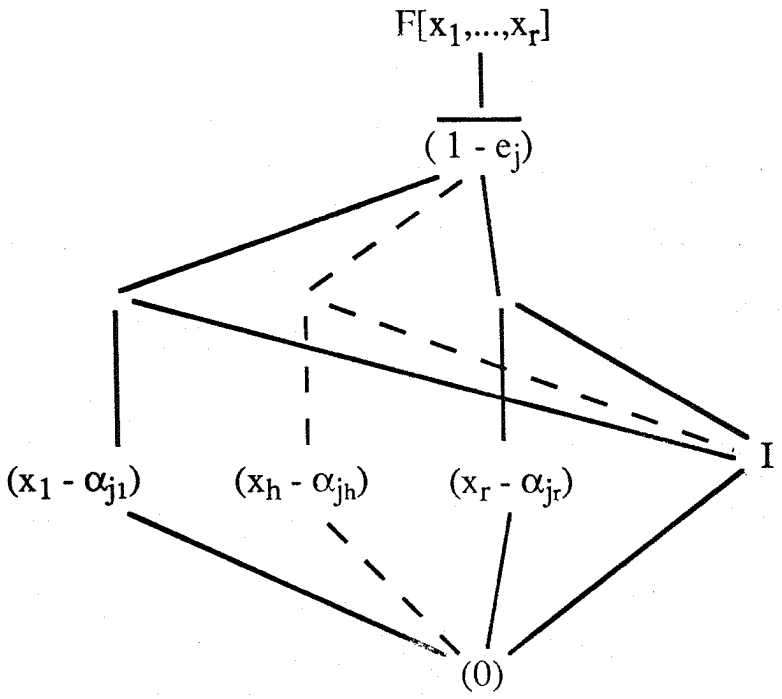


Figure 1: Relation among the ideals

We have seen in the last proof that there is a one to one correspondence between the idempotents $e_j$ and the roots of the system $\Gamma$. Let $\overline{(1-e_j)}$ be the preimage under the natural map $F[x_1,\ldots,x_r] \to F[x_1,\ldots,x_r]/I$ of the ideal generated by $1-e_j$ in $A$, and let $(\alpha_{j_1},\ldots,\alpha_{j_r})$ be the root associated to $e_j$.

Figure 1 helps one to visualize the relation holding among the ideals $I$, $\overline{(1-e_j)}$ and the ideals generated by $x_1-\alpha_{j_1}$ , ..., $x_r-\alpha_{j_r}$.
Note that $\overline{(1-e_i)}$ is maximal in $F[x_1,\ldots,x_r]$ (see also [5, pag. 12] ).

# 3 Roots of $\Gamma$ as eigenvalues of linear transformations

Let us assume that we are given a regular matrix representation $R$ of $A$, with respect to an $F$-basis $(b_1,\ldots,b_k)$. Since

$$A = Fe_1 \oplus \ldots \oplus Fe_k$$

there is an $F$-basis of $A$, namely $(e_1,\ldots,e_k)$, such that each element of $A$ is represented as a diagonal matrix.

Let $M$ be the matrix of transition between the two basis.
Let $E$ be the natural epimorphism $F[x_1,\ldots,x_k] \to F[x_1,\ldots,x_k]/I$.
The argument used to prove theorem 2.4 shows that if $a \in A$ then

$$R(a) = M \cdot diag(\nu_1(a),\ldots,\nu_k(a)) \cdot M^{-1}$$

Therefore the element $x_j$ is mapped by $R \circ E$ to

$$M \cdot diag(\alpha_{1_j},\ldots,\alpha_{k_j}) \cdot M^{-1}$$

and clearly each $\alpha_{m_j}$ is an eigenvalue of $R \circ E(x_j)$.

# 4 The algebra $A$ as a tensor product of algebras

Let $J_i$ be the ideal generated by the polynomial $x_i^q - x_i$ in $F[x_i]$ $(i = 1,\ldots,k)$.
Consider the regular matrix representation $R_i$ of the algebra $A_i := F[x_i]/J_i$ with respect to the basis $(x_i^0 + J_i, x_i^1 + J_i, \ldots, x_i^{q-1} + J_i)$.
It is easily seen that the element $x_i + J_i$ is sent by $R_i$ to the matrix

$$\begin{pmatrix} 0 & & & \\ 1 & & & 1 \\ & \cdot & & \\ & & \cdot & \\ & & 1 & 0 \end{pmatrix}$$

Let $J := J_1 + J_2 + \ldots + J_r$. The algebra $F[x_1,\ldots,x_r]/J$ is isomorphic to $A_1 \otimes A_2 \otimes \ldots \otimes A_r$, and under this isomorphism the element $x_1^{i_1} x_2^{i_2} \ldots x_r^{i_r} + J$ is sent to the Kronecker product

$$R_1(x_1^{i_1}) \otimes R_2(x_2^{i_2}) \otimes \ldots \otimes R_r(x_r^{i_r}) = R_1(x_1)^{i_1} \otimes R_2(x_2)^{i_2} \otimes \ldots \otimes R_r(x_r)^{i_r}$$

of the $r$ matrices.

An easy computation shows that the eigenvalues of each matrix $R_i(x_i)$ are precisely the elements of $F$, each with multiplicity one - this implies that each $R_i(x_i)$ can be put in diagonal form. Therefore using a suitable *fixed basis*, each element $x_1^{i_1} x_2^{i_2} \ldots x_r^{i_r} + J$ is represented as a diagonal matrix, and in particular to each element $f_m(x_1,\ldots,x_r) + J$ there corresponds a diagonal

matrix whose zeroes on the main diagonal are in one to one correspondence with the zeroes of $f_m(x_1, \ldots, x_r)$ in $F^r$.
It follows that:

> *the number of solutions of the system* $\Gamma$ *is equal to the dimension of the intersection of the nullspaces corresponding to the linear transformations* $f_m(x_1, \ldots, x_r) + J \quad (m = 1, \ldots, s)$.

# 5 The case of a single polynomial

Let us assume that $s = 1$, that is the system consists of a single equation $f(x_1, \ldots, x_r) = 0$. The algebra isomorphism given by

$$x_1^{i_1} \ldots x_r^{i_r} + J \mapsto R_1(x_1)^{i_1} \otimes \ldots \otimes R_r(x_r)^{i_r}$$

allows one to consider $f(x_1, \ldots, x_r) + J$ as a linear transformation acting on the space of all the elements $g(x_1, \ldots, x_r) + J$ by left multiplication.

**Note 1.** Since our field $F$ has $q$ elements, and the minimal polynomial of $f(x_1, \ldots, x_r) + J$ splits completely in $F$, the minimal polynomial (in a variable $z$) of $f(x_1, \ldots, x_r)^{q-1} + J$ splits into at most two factors in $F$, the factors being $z$ and $z - 1$. Therefore the problem of determining whether $f(x_1, \ldots, x_r)$ has zeroes in $F^r$ can be restated as:

> *is the minimal polynomial of* $f(x_1, \ldots, x_r)^{q-1} + J \neq z - 1$ *?*

**Note 2.** It is easy to see that the linear transformation corresponding to $f(x_1, \ldots, x_r) + J$ is singular if and only if there is a nonzero polynomial $g(x_1, \ldots, x_r)$ in $F[x_1, \ldots, x_r]$ such that $f(x_1, \ldots, x_r)g(x_1, \ldots, x_r) \in J$ (imagine $g(x_1, \ldots, x_r) + J$ to be an eigenvector in the vector space $F[x_1, \ldots, x_r]/J$): but this simply amounts to say that $f(x_1, \ldots, x_r)$ is a divisor of zero in the algebra $F[x_1, \ldots, x_r]/J$.

**Note 3.** Another way to look at this case is the following: consider in $F[x_1, \ldots, x_r]/J$ the monogenic ideal $L$ generated by $f(x_1, \ldots, x_r) + J$. Given a basis $\mathcal{B}$ for $L$, it is possible to extend $\mathcal{B}$ to a basis of $F[x_1, \ldots, x_r]/J$,

such that, with respect to the new basis, each element of $F[x_1, \ldots, x_r]/J$ is represented as

$$\begin{pmatrix} E & * \\ 0 & D \end{pmatrix}$$

with the submatrix $D$ giving a representation of $A$ isomorphic to the regular representation. Over this basis $f(x_1, \ldots, x_r) + J$ is represented as a matrix

$$T = \begin{pmatrix} S & * \\ 0 & 0 \end{pmatrix}$$

where the matrix $S$ has full rank, and the nullity of the matrix $T$ gives the number of solutions of the equation $f(x_1, \ldots, x_r) = 0$ in $F^r$.

# 6 Open problems

Buchberger's Grobner basis algorithm [2] gives a computational method to test ideal membership, which would allow one to construct the regular representation of $A$, and consequently find the roots of $\Gamma$ in $F^r$. Unfortunately, this algorithm is characterized by a very bad worst case execution time [1].

In the case of a single polynomial equation, the generators of the ideal $I$ assume a very neat form. Is it possible in this case to compute the dimension of the algebra $A$ (number of roots in $F^r$) or its regular representation (which would allow one to compute the value of the roots) without using the Grobner basis machinery?

# Acknowledgements

The author wishes to thank Prof. J.D. Dixon for suggesting the problem and for his invaluable advice and comments.

# References

[1] D. Bayer and M. Stillman *On the Complexity of Computing Syzygies.* in Computational Aspects of Commutative Algebra, L. Robbiano (ed.), Academic Press, 1989.

[2] B. Buchberger. *Grobner Basis: An Algorithmic Method in Polynomial Ideal Theory.* in Recent Trends in Multidimensional System Theory, N.K. Bose (ed.), D. Reidel Publ. Comp., 1985.

[3] C.W. Curtis and I. Reiner *Representation theory of finite groups and associative algebras.* John Wiley & sons, Inc., 1962.

[4] I.N. Herstein *Noncommutative rings.* Carus mathematical monograph number fifteen, The Mathematical Association of America, 1968.

[5] W. Fulton *Algebraic curves.* W.A. Benjamin, Inc. 1969.

## School of Computer Science, Carleton University
## Recent Technical Reports

**TR-179** **Parallel Algorithms for Determining K-width-Connectivity in Binary Images**
Frank Dehne and Susanne E. Hambrusch, September 1990

**TR-180** **A Workbench for Computational Geometry (WOCG)**
P. Epstein, A. Knight, J. May, T. Nguyen, and J.-R. Sack, September 1990

**TR-181** **Adaptive Linear List Reorganization under a Generalized Query System**
R.S. Valiveti, B.J. Oommen and J.R. Zgierski, October 1990

**TR-182** **Breaking Substitution Cyphers using Stochastic Automata**
B.J. Oommen and J.R. Zgierski, October 1990

**TR-183** **A New Algorithm for Testing the Regularity of a Permutation Group**
V. Acciaro and M.D. Atkinson, November 1990

**TR-184** **Generating Binary Trees at Random**
M.D. Atkinson and J.-R. Sack, December 1990

**TR-185** **Uniform Generation of Combinatorial Objects in Parallel**
M.D. Atkinson and J.-R. Sack, January 1991

**TR-186** **Reduced Constants for Simple Cycle Graph Separation**
Hristo N. Djidjev and Shankar M. Venkatesan, February 1991

**TR-187** **Multisearch Techniques for Implementing Data Structures on a Mesh-Connected Computer**
Mikhail J. Atallah, Frank Dehne, Russ Miller, Andrew Rau-Chaplin, and Jyh-Jong Tsay, February 1991

**TR-188** **Generating and Sorting Jordan Sequences**
Alan Knight and Jörg-Rüdiger Sack, March 1991

**TR-189** **Probabilistic Estimation of Damage from Fire Spread**
Charles C. Colbourn, Louis D. Nel, T.B. Boffey and D.F. Yates, April 1991

**TR-190** **Coordinators: A Mechanism for Monitoring and Controlling Interactions Between Groups of Objects**
Wilf R. LaLonde, Paul White, and Kevin McGuire, April 1991

**TR-191** **Towards Decomposable, Reusable Smalltalk Windows**
Kevin McGuire, Paul White, and Wilf R. LaLonde, April 1991

**TR-192** **PARASOL: A Simulator for Distributed and/or Parallel Systems**
John E. Neilson, May 1991

**TR-193** **Realizing a Spatial Topological Data Model in a Relational Database Management System**
Ekow J. Otoo and M.M. Allam, August 1991

**TR-194** **String Editing with Substitution, Insertion, Deletion, Squashing and Expansion Operations**
B John Oommen, September 1991

**TR-195** **The Expressiveness of Silence: Optimal Algorithms for Synchronous Communication of Information**
Una-May O'Reilly and Nicola Santoro, October 1991

**TR-196** **Lights, Walls and Bricks**
J. Czyzowicz, E. Rivera-Campo, N. Santoro, J. Urrutia and J. Zaks, October 1991

**TR-197** **A Brief Survey of Art Gallery Problems in Integer Lattice Systems**
Evangelos Kranakis and Michel Pocchiola, November 1991

**TR-198** **On Reconfigurability of Systolic Arrays**
Amiya Nayak, Nicola Santoro, and Richard Tan, November 1991

**TR-199** **Constrained Tree Editing**
B. John Oommen and William Lee, December 1991

**TR-200** **Industry and Academic Links in Local Economic Development: A Tale of Two Cities**
Helen Lawton Smith and Michael Atkinson, January 1992

**TR-201** **Computational Geometry on Analog Neural Circuits**
Frank Dehne, Boris Flach, Jörg-Rüdiger Sack, Natana Valiveti, January 1992

**TR-202** **Efficient Construction of Catastrophic Patterns for VLSI Reconfigurable Arrays**
Amiya Nayak, Linda Pagli, Nicola Santoro, February 1992

**TR-203** **Numeric Similarity and Dissimilarity Measures Between Two Trees**
B. John Oommen and William Lee, February 1992

**TR-204** **Recognition of Catastrophic Faults in Reconfigurable Arrays with Arbitrary Link Redundancy**
Amiya Nayak, Linda Pagli, Nicola Santoro, March 1992

**TR-205** **The Permutational Power of a Priority Queue**
M.D. Atkinson and Murali Thiyagarajah, April 1992

**TR-206** **Enumeration Problems Relating to Dirichlet's Theorem**
Evangelos Kranakis and Michel Pocchiola, April 1992

**TR-207** **Distributed Computing on Anonymous Hypercubes with Faulty Components**
Evangelos Kranakis and Nicola Santoro, April 1992

**TR-208** **Fast Learning Automaton-Based Image Examination and Retrieval**
B. John Oommen and Chris Fothergill, June 1992

**TR-209** **On Generating Random Intervals and Hyperrectangles**
Luc Devroye, Peter Epstein and Jörg-Rüdiger Sack, July 1992

**TR-210** **Sorting Permutations with Networks of Stacks**
M.D. Atkinson, August 1992

**TR-211** **Generating Triangulations at Random**
Peter Epstein and Jörg-Rüdiger Sack, August 1992

**TR-212** **Algorithms for Asymptotically Optimal Contained Rectangles and Triangles**
Evangelos Kranakis and Emran Rafique, September 1992

**TR-213** **Parallel Algorithms for Rectilinear Link Distance Problems**
Andrzej Lingas, Anil Maheshwari and Jörg-Rüdiger Sack, September 1992

**TR-214** **Camera Placement in Integer Lattices**
Evangelos Kranakis and Michel Pocchiola, October 1992

**TR-215** **Labeled Versus Unlabeled Distributed Cayley Networks**
Evangelos Kranakis and Danny Krizanc, November 1992

**TR-216** **Scalable Parallel Geometric Algorithms for Coarse Grained Multicomputers**
Frank Dehne, Andreas Fabri and Andrew Rau-Chaplin, November 1992

**TR-217** **Indexing on Spherical Surfaces Using Semi-Quadcodes**
Ekow J. Otoo and Hongwen Zhu, December 1992

**TR-218** **A Time-Randomness Tradeoff for Selection in Parallel**
Danny Krizanc, February 1993

**TR-219** **Three Algorithms for Selection on the Reconfigurable Mesh**
Dipak Pravin Doctor and Danny Krizanc, February 1993

**TR-220** **On Multi-label Linear Interval Routing Schemes**
Evangelos Kranakis, Danny Krizanc, and S.S. Ravi, March 1993

**TR-221** **Note on Systems of Polynomial Equations over Finite Fields**
Vincenzo Acciaro, March 1993