Generalized Characteristic Polynomials

John Canny

543 Evans Hall,
Computer Science Division,
University of California, Berkeley

Abstract

We generalize the notion of characteristic polynomial for a system of linear equations to systems of multivariate polynomial equations. The generalization is natural in the sense that it reduces to the usual definition when all the polynomials are linear. Whereas the constant coefficient of the characteristic polynomial of a linear system is the determinant, the constant coefficient of the general characteristic polynomial is the *resultant* of the system. This construction is applied to solve a traditional problem with efficient methods for solving systems of polynomial equations: the presence of infinitely many solutions "at infinity". We give a single-exponential time method for finding all the isolated solution points of a system of polynomials, even in the presence of infinitely many solutions at infinity or elsewhere.

1 Introduction

In this paper we attack a traditional problem of efficient methods for solving systems of polynomial equations over the complex numbers: the presence of infinitely many solutions "at infinity". The methods of [Laz], [Ren] and [Can] all give single-exponential time bounds for the problem of solving polynomial systems, in fact these are the only methods that have better than double-exponential time performance. But these methods are all based on the u-resultant [Wae] and are only applicable to systems of homogeneous polynomials having finitely many solutions.

In many applications, one would like to find the solutions of a system of n *non-homogenous* polynomial equations $g_i = 0$. It is possible to homogenize the g_i's by introducing an extra variable x_0, multiplying each term in g_i by a power of this variable to make the total degree of the term equal to the degree of g_i. Let f_i denote the homogeneous polynomial obtained from g_i in this way. Then every solution of the system $g_i = 0$, $i = 1, \ldots, n$ leads to a solution for $f_i = 0$ having $x_0 = 1$. However, the homogenizing process can produce extraneous solutions for the homogeneous system which have $x_0 = 0$ and do not correspond to solutions of $g_i = 0$. In fact there may be infinitely many of these solutions "at infinity" even if the original system has only a finite number of solutions. For reasons explained in section 3 of this paper, the presence of an infinite number of solutions causes all the u-resultant based methods to fail.

Thus the methods of [Laz], [Ren] and [Can] may not work on some systems of non-homogeneous equations, even those having a finite number of solutions. In this paper we give a u-resultant based method with single-exponential running time which succeeds even in the presence of an infinity of solutions. It does not matter whether these solutions are at infinity or elsewhere, and we obtain all the isolated points in the solution set.

In fact, our main theorem holds in a much more general context. We show that for n polynomials with a solution set in a certain $(n + m - 1)$-dimensional space, we can recover all the parts of the solution set that have the "right" dimension, i.e. dimension $= m - 1$. For this result, we make use of a construction called the *generalized characteristic polynomial* or GCP of a system of polynomials f_i. The characteristic polynomial nomenclature is used because our general construction reduces to the usual definition of characteristic polynomial when all the f_i are linear.

The generalized characteristic polynomial can also be easily computed. The methods of [Ren] and [Can] for resultant computation actually compute a GCP (or something very close to it) as a side effect. So it comes essentially free with these methods. We give a definition of the generalized characteristic polynomial in section 2, and briefly sketch an algorithm for it.

In section 3 we prove that the GCP has the desired properties, using some basic results about dimension of algebraic sets. We show that while the resultant may vanish identically in the presence of solutions of excess dimension, the lowest degree coefficient of the GCP still contains information about the components of the right dimension, i.e. those whose dimension equals the dimension of the space minus the number of

polynomials. Finally, we apply these results to the equation solving problem. Using the u-resultant construction and the GCP we obtain a single exponential time algorithm which recovers all isolated solutions to a system of homogeneous polynomials even if the system has solutions of excess dimension.

2 Computation of Generalized Characteristic Polynomials

In this section we give the construction of the generalized characteristic polynomial $C(s)$ for a system of homogeneous polynomials f_i. It is a natural generalization of the characteristic polynomial of a linear system and it equals the latter in the special case where all the f_i are linear. The constant coefficient of $C(s)$ is the (multivariate) resultant of the f_i. This property is analogous to the fact that the constant coefficient of the characteristic polynomial of a linear system is the determinant. Our construction is based on Macaulay's formula for the general resultant [Mac]. Macaulay shows that the resultant equals the quotient of the determinant of a certain matrix A whose entries are coefficients of the polynomials, and a subdeterminant of A.

Suppose we are given n homogeneous polynomials f_i in n variables x_j, and that f_i has degree d_i. We need some notation for monomials of f_i. Let α be an n-tuple of integers, we write x^α for the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

The rows and columns of the matrix A are indexed by the set of monomials in $x_1, \ldots, x_n$ of degree d where

$$d = 1 + \sum_{i=1,\ldots,n} (d_i - 1) \tag{1}$$

and letting X^d denote the set of monomials of degree d, the cardinality of X^d is

$$N = |X^d| = \binom{d+n-1}{d} \tag{2}$$

Definition A polynomial is said to be *reduced* in x_i if its degree (the maximum degree of its monomials) in x_i is less than d_i. A polynomial that is reduced in all variables but one is said simply to be reduced.

Now consider the polynomial

$$F = C_1 f_1 + C_2 f_2 + \cdots + C_n f_n \tag{3}$$

where each C_i is a homogeneous polynomial of degree $d - d_i$ with symbolic coefficients, which is reduced in $x_1, \ldots, x_{i-1}$. F is a homogeneous polynomial of degree d, and so has N coefficients. There are also, in total, exactly N coefficients in the C_i. To see this,

imagine for the moment that each f_i equals $x_i^{d_i}$. Then every monomial in F is a multiple of a monomial from exactly one of the C_i's. For the monomial cx^α, let j be the smallest index i such that x^α is not reduced in x_i. Then cx^α is a multiple of a monomial from C_j and from no other C_i.

Since the coefficients of F are linear functions of the coefficients of the C_i via (3), this determines a linear map A from coefficients of the C_i to coefficients of F. Each non-zero entry in the matrix A is a coefficient of some f_i. This defines the matrix A that we mentioned earlier.

More concretely, if we index rows and columns of A by elements of X^d, then the row corresponding to x^α represents the polynomial

$$\frac{x^\alpha}{x_i^{d_i}} f_i \tag{4}$$

where i is the smallest j such that x^α has degree at least d_j in x_j.

The determinant of A vanishes if the f_i have a common zero, and it is therefore a multiple of the resultant R of the system [Mac]. We can write $\det(A) = MR$, where M is an additional factor which we would like to remove. Macaulay shows that M is the determinant of a certain submatrix of A, in fact the submatrix of elements whose row and column indices are not reduced. Thus he obtains the simple formula $R = \det(A)/\det(M)$.

Having given a brief sketch of what a multivariate resultant is, we can now give the construction of generalized characteristic polynomials:

Definition The *generalized characteristic polynomial* (or GCP), $C(s)$ of a system of homogeneous polynomials $f_1, \ldots, f_n$ in $x_1, \ldots, x_n$ is the resultant of $\hat{f}_1, \ldots, \hat{f}_n$, where $\hat{f}_i = f_i - s x_i^{d_i}$.

We do not claim this to be a novel construction. But what has not previously been observed is that it is both inexpensive to compute, and that it can be used to recover all the isolated zeros of a system of polynomials, as shown in the next section.

Inspection of the matrices A and M shows that the coefficients of $x_i^{d_i}$ in f_i always appear on the leading diagonals. So the determinant of the matrix $\hat{A}$ for the new system $\hat{f}_i$ is actually the characteristic polynomial (in the usual sense) of A, i.e. $\det(\hat{A}) = \det(A - sI) = \mathrm{CharPoly}(A)(s)$, where $\mathrm{CharPoly}(A)(s)$ denotes the characteristic polynomial of A in the variable s. The same holds true for M, so that the *generalized* characteristic polynomial of the f_i is given as

$$C(s) = \frac{\mathrm{CharPoly}(A)(s)}{\mathrm{CharPoly}(M)(s)} \tag{5}$$

Now A is an $N \times N$ matrix, while M has $N - D$ rows and columns, where

$$D = \sum_i \prod_{j \neq i} d_j \tag{6}$$

is the number of reduced rows (or columns). This implies than CharPoly$(A)(s)$ has degree N and CharPoly$(M)(s)$ has degree $N - D$, so that the GCP $C(s)$ has degree D. To compute a characteristic polynomial using Newton's identity [Csa] takes $O(N^4)$ arithmetic operations. For large problems, N is much larger than D, and so it seems that computation of all N coefficients of CharPoly$(A)(s)$ in (5) is wasteful. But we can use the fact that if the quotient of two polynomials has degree D, then that quotient depends only on the D most significant coefficients of those polynomials. So it is possible to compute $C(s)$ by computing only the first D coefficients of CharPoly$(A)(s)$ and CharPoly$(M)(s)$. Using the Newton identity, this can be done with $O(N^3D)$ operations.

3 Main Properties

We next prove our main result, that the GCP $C(s)$ contains all the information needed to recover the proper components of the zeros set of the f_i. This result gives as an immediate corollary, a method for finding all the zeros of a system of n non-homogeneous polynomials in n variables, even if such a system has infinitely many solutions "at infinity". The method is based on the u-resultant [Wae], but unlike previous methods [Laz], [Ren], [Can] does not require that there be only finitely many solutions at infinity.

To begin, we give some definitions and basic results on dimension of algebraic sets. We will not define the dimension of an algebraic set, but detailed definitions are given in [Mum] chapter 1. In what follows, we assume that variable values range over the complex numbers C.

Definition The set of common zeros of a system of polynomials $f_1, \ldots, f_n$ in $x_1, \ldots, x_m$ is called an *algebraic set* and is denoted $V(f_1, \ldots, f_n) \subset C^m$. An algebraic set $V(f)$ defined by a single polynomial (which is not identically zero) is called a *hypersurface.* If f is linear, then $V(f)$ is called a *hyperplane.*

If all the f_i are homogenous, it is more convenient to work with the projective space P^{m-1}, formed by identifying points in C^m which are scalar multiples of each other. That is, a "point" in P^{m-1} corresponds to all points in C^m of the form $\lambda(p_1, \ldots, p_m)$, where the $p \in C^m$ is a non-zero constant vector, and λ ranges over all complex values. Points in P^{m-1} are sometimes called solution "rays" for this reason. P^{m-1} has dimension $m-1$ and is compact. We use the same notation, $V(f_1, \ldots, f_n) \subset P^{m-1}$ for an algebraic set defined by homogenous polynomials f_i.

Definition An algebraic set is said to be *reducible* if it can be expressed as a finite union of proper subsets which are algebraic. An algebraic set which is not reducible is *irreducible.*

Any algebraic set can always be expressed as a finite union of irreducible algebraic subsets called *components.* Many results in algebraic geometry apply only to irreducible algebraic

sets, and in much of what follows, we work with the individual components of an algebraic set.

Definition Let Z be the intersection of m hypersurfaces in n-dimensional affine or projective space. A component W of Z is said to be *proper* if it has dimension $n-m$. A component of dimension greater than $n-m$ is said to be an *excess* component.

And in fact all components of an intersection must be either proper or excess by the following lemma:

Lemma 3.1 *If f_i are m non-homogeneous polynomials in n variables, (or homogeneous in $n+1$ variables), then every component of $V(f_1,\ldots,f_m)$ has dimension at least $n-m$.*

For a proof, see for example [Mum] corollary 3.14. Our main result is that if $C(s)$ is arranged in powers of s, then its lowest degree coefficient vanishes on the projection of all proper components of the intersection. We start with n polynomials $f_i(u_1,\ldots,u_m,x_1,\ldots,x_n)$, which are homogenous in the x_j. Then:

Theorem 3.2 *Let $Z = V(f_1,\ldots,f_n) \subset C^m \times P^{n-1}$, and let W be a proper component of Z, so that the dimension of W is $m-1$. Let $C(u_1,\ldots,u_m)(s)$ be the generalized characteristic polynomial of the f_i, as polynomials in the x_j. Arranging the GCP in powers of s, let $C_k(u_1,\ldots,u_m)$ be its coefficient of lowest degree. If $\pi_u : C^m \times P^n \to C^m$ denotes projection on u_i-coordinates, then $C_k(\pi_u(p)) = 0$ for all $p \in W$.*

Proof The GCP is the resultant of the polynomials $\hat{f}_i = f_i - sx_i^{d_i}$. With the addition of the complex variable s, the zeros set of the $\hat{f}_i$, call it Z', lies in $C^m \times P^{n-1} \times C$. Since $\hat{f}_i$ and f_i are identical when $s=0$, the intersection of Z' and the hypersurface $s=0$ is exactly $Z \times \{0\}$. So for every component W of Z, we have $W \times \{0\} \subset Z'$. If W is a *proper* component it has dimension $m-1$, but by the dimension lemma, every component of Z' has dimension at least m. So $W \times \{0\}$ must be contained in some component W' of dimension m.

Because every point of W' has an m-dimensional neighborhood, and because the intersection of this neighborhood with the hypersurface $s=0$ is $(m-1)$-dimensional, it follows that for every point $p \in W \times \{0\}$, there is a sequence of points (p_j) in $W' - W \times \{0\}$ which converges to p. Writing $C(u_1,\ldots,u_m)(s)$ now for the GCP of the f_i, or equivalently the resultant of the $\hat{f}_i$, then $C(\pi_u(q))(\pi_s(q)) = 0$ for any point q in Z', where π_s denotes projection on the s-coordinate. In particular $C(\pi_u(p_j))(\pi_s(p_j)) = 0$ for all j. Dividing this polynomial through by $\pi_s(p_j)^k$ (which is non-zero), and letting C_i denote the coefficient of s^i in the GCP, we obtain

$$C_k(\pi_u(p_j)) + \sum_{i=k+1,\ldots,D} (\pi_s(p_j))^{i-k} C_i(\pi_u(p_j)) = 0 \qquad (7)$$

for all p_j, where C_k is the lowest degree non-vanishing coefficient of $C(s)$, and D is the degree of $C(s)$. This expression is a polynomial in the coordinates of the p_j, and is therefore a continuous function of the coordinates. Since it is zero for all $p_j \to p$, it must be zero at p. But the point p has s-coordinate zero, so the summation over i vanishes, and we conclude that $C_k(\pi_u(p))$ must equal zero. □

We can restate the theorem succinctly as:

$$\pi_u(\bigcup W_i) \subset V(C_k) \subset \pi_u(V(f_1, \ldots, f_n)) \tag{8}$$

The second containment follows because $\pi_u(V(f_1, \ldots, f_n)) = V(C_0)$, where C_0 is the resultant of the f_i. If $k = 0$ it is trivially true, whereas $k > 0$ implies $C_0 = 0$, so that $V(C_0) = C^m$.

Conjecture We conjecture that if Z_i is *any* component of $V(f_1, \ldots, f_n)$, then its projection intersects $V(C_k)$:

$$V(C_k) \cap \pi_u(Z_i) \neq \phi \tag{9}$$

The prove the conjecture, one needs to show that if Z is an excess component, for small enough ϵ, $V(\hat{f}_1, \ldots, \hat{f}_n) \cap V(s = \epsilon)$ has a proper component "near" to Z. The intuition behind this is that if just one of the coefficients of $x_i^{d_i}$ in f_i is changed slightly, it causes each component of the intersection to either "move" slightly, or to be cut into components of lower dimension, which are all contained within that component. In either case, every point of the new intersection is close to some point of the old intersection. Applying this inductively to each f_i, we eventually obtain a new intersection with only proper components, such that each of its components is near to one of the original components.

It is also reasonable to conjecture that the degree of vanishing of $C(u_1, \ldots, u_m)(s)$, at some point $u_i = p_i$ is a measure of the intersection multiplicity (in some appropriate sense) of the surfaces defined by the f_i. For example, we could consider the intersection multiplicity of the surfaces $f_i(p_1, \ldots, p_m, x_1, \ldots, x_n) = v$ in $C^n \times C$.

3.1 Application to Equation Solving

The main theorem of this section can be applied to the following problem: Given n non-homogeneous polynomials g_i in n variables, $x_1, \ldots, x_n$ find all the isolated solution points of the system $g_i = 0$. By isolated solution points, we mean those points that are not contained in some higher-dimensional component of the solution set. The system has an equal number of equations and variables, and so the proper components of $V(g_1, \ldots, g_n)$ are zero-dimensional, i.e. points.

Since the methods we will use apply to homogeneous polynomials, we must produce a homogenous system from the g_i by introducing an additional variable x_0. For each

polynomial g_i of degree d_i we produce a homogeneous polynomial f_i of degree d_i by multiplying terms of g_i of degree δ_i by $x_0^{(d_i-\delta_i)}$. Then if $(p_1,\ldots,p_n) \in C^n$ is a solution of the original system, $\lambda(1,p_1,\ldots,p_n) \in P^n$ is a solution ray of the homogeneous system.

In fact there is a one-to-one correspondence between solution points of the original system and solution rays of the homogeneous system which have $x_0 \neq 0$. However, there may be solutions of the homogeneous system which have $x_0 = 0$, called "solutions at infinity" which have no counterpart in the original system. There may in fact be excess components of the intersection at infinity, even if the original system has only proper solutions.

The presence of excess components at infinity causes the methods of [Laz], [Ren] and [Can] to fail, and there is no easy way to ensure that the given system has only proper solutions at infinity. The methods just mentioned are the only polynomial equation-solving methods that have single exponential bounds. They are based on the u-resultant which we now describe. Using the GCP, we can give a u-resultant style method with single-exponential time bounds which succeeds even in the presence of excess solutions at infinity or elsewhere.

To a system of n homogeneous polynomials f_i in $n+1$ variables, we add the linear polynomial

$$u_0x_0 + u_1x_1 + \cdots + u_nx_n \tag{10}$$

where the coefficients $u_0,\ldots,u_n$ are indeterminates. We call this last polynomial the *u-form*. We now have a system of $n+1$ polynomials in $n+1$ variables, and the resultant of such a system is a polynomial $R(u_0,\ldots,u_n)$ called the u-resultant.

Suppose now that $\lambda(p_0,\ldots,p_n)$ is a solution ray of the system f_i. Then it will also satisfy the u-form if and only if

$$p_0u_0 + \cdots + p_nu_n = 0 \tag{11}$$

.

So the system as a whole has a solution, and therefore the resultant $R(u_0,\ldots,u_n)$ will vanish, whenever $p_0u_0 + \cdots + p_nu_n = 0$. This implies that $(p_0u_0 + \cdots + p_nu_n)$ *divides* $R(u_0,\ldots,u_n)$. Similarly, every other solution ray of the f_i leads to a corresponding linear factor of the u-resultant. By computing the u-resultant and factoring it over the complex numbers, we can obtain the coordinates of all the solution rays. This is the essence of the methods in [Laz], [Ren], and [Can] although they differ in how the factorization is computed.

But suppose now that $V(f_1,\ldots,f_n)$ has a component of dimension 1 (or higher). It is a standard result [Mum] corollary 3.30, that two projective varieties in the same space always intersect if the sum of their dimensions is at least the dimension of the space. For any fixed set of values of the u_i, the equation $u_0x_0 + \cdots + u_nx_n = 0$ defines a variety of dimension at least $n-1$ in P^n, and this must always intersect an excess solution of the f_i, irrespective of the value of the u_i. So the polynomial $R(u_0,\ldots,u_n)$ must be zero for

all values of the u_i, i.e. it is identically zero. This is why the u-resultant methods fail if there are excess components in the solution set.

To get around this problem, we compute the GCP of the f_i and the u-form. We consider the f_i as defining an algebraic set in $C^{n+1} \times P^n$, where a point's coordinates are the u_i's followed by the x_j's. Now for each isolated solution ray $\lambda p \in P^n$ there must be an n-dimensional hyperplane in $V(f_1, \ldots, f_n, u\text{-}form) \subset C^{n+1} \times P^n$ given by equation (11), and the equations $x_i = p_i$. Furthermore, each such hyperplane is irreducible, being defined by linear equations, and is of proper dimension.

By the main theorem of the last section, if $C_k(u_0, \ldots, u_n)$ is the lowest degree non-vanishing coefficient of the GCP, then it must vanish on the projection of every proper component of the solution set of the f_i. Here the proper components each correspond to one of the solution rays. For each solution ray λp, $C_k(u_0, \ldots, u_n)$ must vanish for all u_i satisfying equation (11). This implies that $(p_0 u_0 + \cdots + p_n u_n)$ is a linear factor of $C_k(u_0, \ldots, u_n)$. So once again we can find the solution rays of f_i by factoring a polynomial in $u_0, \ldots, u_n$, but instead of the u-resultant $R(u_0, \ldots, u_n)$ which would be zero in such cases, we factor $C_k(u_0, \ldots, u_n)$ which is always non-vanishing.

We observe next that C_k factors completely into linear factors. This is because for all sufficiently small $s = \epsilon$, there are $D = \deg(C_k)$ solution rays of $\hat{f}_i = 0$, and for each there is a corresponding hyperplane in $V(C(\epsilon)) \subset C^{n+1}$. As $\epsilon \to 0$ these hyperplanes approach limits (by compactness of the Grassmanian of hyperplanes in C^{n+1}) which must all lie in $V(C(s)/s^k)$ and therefore lie in $V(C_k)$ within the slice $s = 0$. Since there are D such limiting hyperplanes, counting multiplicities, C_k factors into D linear factors.

The equation solving methods of [Ren] and [C88] avoid explicit computation of $R(u_0, \ldots, u_n)$, since it has so many coefficients ($O(d^{n^2})$ if all polynomials have degree d). Instead, they compute certain specializations of it. For example in [C88] the solutions not at infinity can be found with the following specializations: $R_0(v,t) = R(v, t, t^2, \ldots, t^n)$ and $R_i^+(v,t) = R(v, t, \ldots, t^i + 1, \ldots, t^n)$ and $R_i^-(v,t) = R(v, t, \ldots, t^i - 1, \ldots, t^n)$, for $i = 1, \ldots, n$. Making these specializations *before* the resultant is computed means that all arithmetic is done on polynomials in two variables v and t, and so the number of coefficients is at most $O(d^{2n})$.

We can make the same specializations of the u_i's before computing the GCP. The arguments in [C88] which show that the resultant is non-vanishing for the above specializations, also apply to the lowest degree coefficient of the GCP. So it is impossible for example, that the lowest degree coefficient of the specialization of $C(s)$ could be some other coefficient than C_k. Since C_k factors completely into linear factors, the methods of [Ren] and [C88] for factorizing the u-resultant from its specializations still apply to C_k and its specializations. So, to summarize, the isolated solution points of a system of polynomials can be found using [Ren] or [C88] by replacing each resultant with the lowest degree coefficient of the corresponding GCP.

4 Conclusions

We described a new construction called the generalized characteristic polynomial, which is a useful adjunct to the multivariate resultant. The GCP can be used in situations where resultant-based methods fail because of the presence of components of excess dimension in the solution set of a system of polynomials. It provides a means for systematically perturbing a polynomial system away from a "bad" or excess intersection, and for recovering the proper components of the intersection, which are robust with respect to this perturbation.

The GCP can be obtained naturally from certain resultant algorithms. We showed that it can be computed as a quotient of the characteristic polynomials of two square matrices. By judicious use of Newton's identity for characteristic polynomials, the quotient can be found by computing only some of the coefficients of the matrix characteristic polynomials. This provides an significant reduction in the cost of computing the GCP. But there is still much that can be done to improve the running time of both resultant and GCP algorithms. Our algorithm required $O(N^4)$ operations as a function of the matrix size, whereas in the special case of two homogeneous polynomials, the (Sylvester) resultant can be computed with $O(N \log^2 N)$ operations. It should be possible to improve the GCP bounds to quadratic or pseudo-linear.

References

[Can] Canny J. F., "A New Algebraic Method for Motion Planning and Real Geometry", Proc. 28th IEEE Symp. FOCS, Los Angeles, (1987), pp 39-48.

[C88] Canny J. F. "Some Algebraic and Geometric Computations in PSPACE", to appear in Proc. ACM STOC, Chicago (May 1988).

[Csa] Csanky L., "Fast Parallel Matrix Inversion Algorithms" SIAM J. Comp., Vol. 5, No. 4, (Dec. 1976) pp 618-623.

[Laz] Lazard D., "Résolution des Systèmes d'Équations Algébriques", Theor. Comp. Sci. vol 15, (1981).

[Mac] Macaulay F. S., "Some Formulae in Elimination" Proc. London Math. Soc. (1) 35 (1902) pp. 3-27.

[Mum] Mumford D., "Algebraic Geometry I, Complex Projective Varieties", Springer-Verlag, New York, (1976).

[Ren] Renegar J., "On the Worst Case Arithmetic Complexity of Approximating Zeros of Systems of Polynomials", Tech. Rept. School of Operations Research and Industrial Engineering, Cornell U. (May 1987).

[Wae] van der Waerden B. L., "Modern Algebra", (third edition) F. Ungar Publishing Co., New York (1950).

[Wie] Wiedemann D.H. "Solving Sparse Linear Equations over Finite Fields", IEEE Trans. Information Theory, vol. IT-32, No 1, (Jan. 1986).