POWER ROOTS OF POLYNOMIALS OVER ARBITRARY FIELDS

Vincenzo Acciaro

TR-228, SEPTEMBER 1993

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

Power Roots of Polynomials over Arbitrary Fields

Vincenzo Acciaro*

Abstract

Let F be an arbitrary field, and $f(x)$ a polynomial in one variable over F of degree ≥ 1. Given a polynomial $g(x) \neq 0$ over F and an integer $m > 1$ we give necessary and sufficient conditions for the existence of a polynomial $z(x) \in F[x]$ such that $z(x)^m \equiv g(x) \pmod{f(x)}$. We show how our results can be specialized to $\mathbb{R}$, $\mathbb{C}$ and to finite fields. Since our proofs are constructive it is possible to translate them into an effective algorithm when F is a computable field (e.g. a finite field or an algebraic number field).

1991 Mathematics Subject Classification: 30C10,12E05

1 Introduction

Let F be an arbitrary field, $f(x)$ a polynomial in one variable over F of degree ≥ 1, $g(x)$ a nonzero polynomial over F and $m > 1$ an integer.

In [3] Miller gave some sufficient conditions for the existence of a polynomial $z(x) \in F[x]$ such that $z(x)^m \equiv g(x) \pmod{f(x)}$, when F is $\mathbb{R}$ or $\mathbb{C}$ – it is explicitly stated in his paper that the conditions given are not necessary.

In our paper we extend Miller's results by giving necessary and sufficient conditions for the existence of an m^{th} root in $F[x]/(f(x))$, when F is any field, not necessarily $\mathbb{C}$ or $\mathbb{R}$. While the methods used by Miller in [3] are analytical, ours are purely algebraic.

Moreover, since all the proofs given here are constructive, it is possible to translate them into an effective algorithm when F is a computable field (e.g. an algebraic number field or a finite field).

We can summarize the results of this paper in the following theorem :

*School of Computer Science, Carleton University, Ottawa, ONT, K1S 5B6, Canada.
Research supported in part by NSERC grant A2415

THEOREM 1 *Let F be a field, and $m > 1$ a positive integer, $char(F) \not| m$ if $char(F) > 0$. Let $g(x), f(x)$ be polynomials over F, with $g(x) \neq 0$ and* $\deg f(x) \geq 1$. *In $F[x]$ the congruence*

$$z(x)^m \equiv g(x) \pmod{f(x)} \tag{1}$$

admits a solution if and only if for every irreducible factor $p(x)$ of $f(x)$: if $l \geq 0$ denotes the highest power of $p(x)$ dividing $g(x)$ and $k \geq 1$ denotes the highest power of $p(x)$ dividing $f(x)$, then either

(i). $k \leq l$, or

(ii). $m \mid l$ and $y(x)^m \equiv g(x)/p(x)^l \pmod{p(x)}$ is solvable for $y(x)$.

When $char(F) \mid m$ the situation is more complex – we will consider this case in Section 2.2. We will prove Theorem 1 in Section 2. In Sections 3, 4 and 5 we will show how to specialize Theorem 1 to $\mathbb{C}$, $\mathbb{R}$ and to finite fields.

2 The method

We can assume without loss of generality that $f(x)$ is monic, since if $z(x)^m \equiv g(x) \pmod{f(x)}$ holds, then $z(x)^m \equiv g(x) \pmod{cf(x)}$ holds for any $c \in F$. The method discussed in this paper can be summarized as follows:

(i). Factor $f(x)$ into monic irreducibles obtaining $f(x) = p_1(x)^{e_1} \ldots p_n(x)^{e_n}$

(ii). Solve each of the congruences $z_i(x)^m \equiv g(x) \pmod{p_i(x)}$ for $z_i(x)$, $i \in \{1, \ldots, n\}$;

(iii). Lift the solutions obtained in the previous step from $F[x]/(p_i(x))$ to $F[x]/(p_i(x)^{e_i})$;

(iv). Combine the solutions of the previous step using the Chinese Remainder Theorem to obtain a solution of the original congruence.

Step (iv) does not present any technical difficulty, since it relies on the well known isomorphism [4, page 95]:

$$F[x]/(f(x)) \cong F[x]/(p_1(x)^{e_1}) \times \ldots \times F[x]/(p_n(x)^{e_n})$$

When $p(x)$ is a monic irreducible polynomial $F[x]/(p(x)) \cong F(\alpha)$ where α is any root of $p(x)$: the actual isomorphism is given by $k(x) + (p(x)) \mapsto$

$k(\alpha)$. It follows that Step (ii), that is the extraction of an m^{th} root of $g(x)$ modulo $p(x)$, is equivalent to the extraction of an m^{th} root of $g(\alpha)$ in $F(\alpha)$.

Therefore, the rest of this section will be devoted to explaining how Step (iii), i.e. the lifting process, can be accomplished.

Fundamental to the entire process is the concept of the p-adic expansion of a polynomial f [4, page 189]. Given $f, p \in F[x]$,with $\deg p \geq 1$, there exist unique polynomials $g_0, g_1, \ldots, g_t \in F[x]$ such that $\deg g_i < \deg p$ and $f = g_0 + g_1 p + g_2 p^2 + \ldots + g_t p^t$. The polynomials g_i can be computed recursively as follows:

- $g_0 := f \bmod p$
- $g_{i+1} := (f - \sum_{k=0}^{i} g_k p^k)/p^{i+1} \bmod p$.

The lifting method is based on the following lemma, freely adapted from [2, page 16].

LEMMA 1 *Let p be an irreducible element of $F[x]$. Let $G(y)$ be a polynomial with coefficients in $F[x]$. Assume that there is an element $f_0 \in F[x]$, with $\deg f_0 < \deg p$, such that $G(f_0) \equiv 0 \pmod{p}$ and $G'(f_0) \not\equiv 0 \pmod{p}$. Given any positive integer k there is a unique polynomial $f_{k-1} \in F[x]$ of degree less than $\deg p^k$ such that $G(f_{k-1}) \equiv 0 \pmod{p^k}$ and $f_{k-1} \equiv f_0 \pmod{p}$.*

PROOF: We show how to construct a sequence of polynomials $f_1, \ldots f_{k-1} \in F[x]$ such that for all $n \in \{1, \ldots, k-1\}$:

(i). $G(f_n) \equiv 0 \pmod{p^{n+1}}$

(ii). $f_n \equiv f_{n-1} \pmod{p^n}$

(iii). $\deg f_n < \deg p^{n+1}$

We prove that the sequence (f_n) exists and is unique by induction on n. If f_1 satisfies (ii) and (iii) then it must be of the form $f_0 + b_1 p$, with $\deg b_1 < \deg p$. When we expand $G(f_1)$ we obtain

$$G(f_1) = G(f_0 + b_1 p) = G(f_0) + G'(f_0) b_1 p + w$$

where w is a polynomial divisible by p^2. Since $p \mid G(f_0)$ by assumption, we can write $G(f_0) \equiv a_0 p \pmod{p^2}$ where $\deg a_0 < \deg p$. So, in order to get $G(f_1) \equiv 0 \pmod{p^2}$ we must have $a_0 p + G'(f_0) b_1 p \equiv 0 \pmod{p^2}$, i.e. $a_0 + G'(f_0) b_1 \equiv 0 \pmod{p}$. The last congruence has a unique solution

$(\mathrm{mod}\ p)$ for b_1 since by hypothesis $G'(f_0) \not\equiv 0 \pmod{p}$. Then $f_1 = f_0 + b_1 p$ is the unique polynomial satisfying (i), (ii) and (iii) with $n = 1$.

Next, assume that $f_1, f_2, \ldots, f_{n-1}$ are known, and we want to find f_n. By (ii) and (iii) we need $f_n = f_{n-1} + b_n p^n$ with $\deg b_n < \deg p$. We expand $G(f_n)$ obtaining

$$G(f_n) = G(f_{n-1} + b_n p^n) \equiv G(f_{n-1}) + G'(f_{n-1}) b_n p^n \pmod{p^{n+1}}$$

Since $G(f_{n-1}) \equiv 0 \pmod{p^n}$ by the inductive hypothesis, we obtain

$$G(f_{n-1}) \equiv a_{n-1} p^n \pmod{p^{n+1}}$$

and the condition $G(f_n) \equiv 0 \pmod{p^{n+1}}$ becomes

$$a_{n-1} p^n + G'(f_{n-1}) b_n p^n \equiv 0 \pmod{p^{n+1}}$$

that is

$$a_{n-1} + G'(f_{n-1}) b_n \equiv 0 \pmod{p}$$

Since $f_{n-1} \equiv f_0 \pmod{p}$ it follows that

$$G'(f_{n-1}) \equiv G'(f_0) \not\equiv 0 \pmod{p}$$

and so the previous congruence has a unique solution $(\mathrm{mod}\ p)$ for b_n. Then $f_n = f_{n-1} + b_n p^n$ is the unique polynomial satisfying (i), (ii) and (iii). □

Our objective is to solve the congruence:

$$y(x)^m \equiv g(x) \pmod{p(x)^k} \tag{2}$$

where $p(x)$ is a monic irreducible factor of $f(x)$.

Let $y_0(x)$ be a solution of $y(x)^m \equiv g(x) \pmod{p(x)}$; clearly if such an element $y_0(x)$ does not exist (2) can not admit any solution.

If $m y_0(x)^{m-1} \not\equiv 0 \pmod{p(x)}$ we can use the construction given in Lemma 1 with $G(y) := y(x)^m - g(x)$ to obtain a sequence of polynomials $y_1(x), y_2(x), \ldots$ such that $y_i(x)^m \equiv g(x) \pmod{p(x)^{i+1}}$. A solution of (2) is then given by $y_{k-1}(x)$, and this solution is unique, modulo $p(x)^k$.

If $m y_0(x)^{m-1} \equiv 0 \pmod{p(x)}$ the lifting argument can not be applied, although (2) may still have a solution.

Let us assume therefore that $m y_0(x)^{m-1} \equiv 0 \pmod{p(x)}$. Since $F[x]/(p(x))$ is a field this may happen only in two cases: if $y_0(x) \equiv 0 \pmod{p(x)}$ or if $char(F) \mid m$. We discuss the first case in Section 2.1 and the second case in Section 2.2.

2.1 Lifting of zero

It is easy to see that the zero polynomial is a solution of $y(x)^m \equiv g(x) \pmod{p(x)}$ if and only if $p(x) \mid g(x)$. The following lemma deals with this case.

LEMMA 2 *Assume that $p(x) \mid g(x)$. Let l be the highest power of $p(x)$ dividing $g(x)$. If $k \leq l$ the zero polynomial is a solution of (2). If $k > l$ (2) admits a solution if and only if $m \mid l$ and*

$$y(x)^m \equiv g(x)/p(x)^l \pmod{p(x)^{k-l}} \tag{3}$$

admits a solution. In this case if $\hat{y}(x)$ denotes a solution of (3) then $\hat{y}(x)p(x)^{l/m}$ is a solution of (2).

PROOF: If $k \leq l$ the zero polynomial is obviously a solution of (2), so we will suppose that $k > l$.

Assume that $\hat{y}(x)^m \equiv g(x)/p(x)^l \pmod{p(x)^{k-l}}$. This is equivalent to $p(x)^k \mid \hat{y}(x)^m p(x)^l - g(x)$. Thus, if $m \mid l$ we can write the last relation as $p(x)^k \mid \hat{y}(x)^m p(x)^{(l/m)m} - g(x)$, and so $\hat{y}(x)p(x)^{l/m}$ is a solution of (2).

On the other hand, suppose that $k > l$ and (2) admits a solution. Let the $p(x)$-adic expansion of $g(x)$ be $a_1(x)p(x)^l + a_2(x)p(x)^{l+1} + \ldots$, with $a_1(x) \neq 0$. Let $\overline{y}(x) = b_1(x)p(x)^r + \ldots$ be a solution of (2), with $b_1(x) \neq 0$. Then the $p(x)$-adic expansion of $\overline{y}(x)^m$ is $(b_1(x)^m \bmod p(x))p(x)^{rm} + \ldots$.

Since $b_1(x) \not\equiv 0$ and $\deg b_1(x) < \deg p(x)$ it follows that $b_1(x) \not\equiv 0 \pmod{p(x)}$ and therefore $b_1(x)^m \not\equiv 0 \pmod{p(x)}$, since $p(x)$ is prime. Now $\overline{y}(x)^m \equiv g(x) \pmod{p(x)^k}$ if and only if $(b_1(x)^m \bmod p(x))p(x)^{rm} + \ldots$ and $a_1(x)p(x)^l + \ldots$ coincide up to the term in $p(x)^{k-1}$. Since $a_1(x) \neq 0$ and $b_1(x)^m \bmod p(x) \neq 0$ it follows that $l = rm$ and so $m \mid l$ as asserted. □

COROLLARY 1 *Under the assumptions of the previous lemma, if $char(F) \nmid m$ and $k > l$ (2) admits a solution if and only if $m \mid l$ and $y(x)^m \equiv g(x)/p(x)^l \pmod{p(x)}$ admits a solution.*

PROOF: The Corollary follows immediately from Lemma 1 since the right hand side of (3) is not divisible by $p(x)$. □

Note that if $p(x) \mid g(x)$ and at the same time $char(F) \mid m$, we can use Lemma 2 to reduce this case to the case $p(x) \nmid g(x)$ and $char(F) \mid m$, which is handled in the next section.

2.2 The exponent m is a multiple of $char(F)$

In this section we will assume that $p(x) \not| g(x)$. When $q = char(F) > 0$ the map $a \mapsto a^q$ is always an endomorphism of F. It follows that if $a(x) = a_0 + a_1x + \ldots + a_nx^n$ is a polynomial over F then $a(x)^q = a_0^q + a_1^q x^q + \ldots + a_n^q x^{nq}$. We will use this fact frequently in this section.

LEMMA 3 *Let $q = char(F)$, $q \neq 0$. Assume that $m = q^t$ for some positive integer t, and $m \geq k$. If (2) admits a solution, then every solution of $y(x)^m \equiv g(x) \pmod{p(x)}$ is a solution of (2).*

PROOF: Let us assume that (2) admits a solution $y_1(x)$. Let $y_0(x)$ be a solution of $y(x)^m \equiv g(x) \pmod{p(x)}$. Then $(y_0(x) - y_1(x))^m = y_0(x)^m - y_1(x)^m \equiv 0 \pmod{p(x)}$. Since $p(x)$ is prime and $k \leq m$ it follows that $p(x)^k \mid (y_0(x) - y_1(x))^m$ and therefore $y_0(x)^m \equiv y_1(x)^m \pmod{p(x)^k}$, i.e. $y_0(x)^m \equiv g(x) \pmod{p(x)^k}$. □

NOTE: Therefore, to test if (2) is solvable, it is enough to find *any* solution of $y(x)^m \equiv g(x) \pmod{p(x)}$ and check if it satisfies (2). Clearly if $y(x)^m \equiv g(x) \pmod{p(x)}$ does not admit any solution then (2) does not admit any solution.

LEMMA 4 *Let $q = char(F)$, $q \neq 0$. Assume that $m = q^t$ for some positive integer t.*

If $m \mid k$ (2) admits a solution if and only if $g(x) \bmod p(x)^k$ is a polynomial in x^m and all its coefficients have an m^{th} root in F.

If $m \not| k$ let $w := \lfloor k/m \rfloor$, let $s := k \bmod m$, let $z(x) := g(x) \bmod p(x)^{mw}$ and $r(x) := (g(x) - z(x))/(p(x)^{mw}) \bmod p(x)^s$. Then (2) admits a solution if and only if $z(x)$ is a polynomial in x^m, all its coefficients have an m^{th} root in F and $j(x)^m \equiv r(x) \pmod{p(x)^s}$ admits a solution.

PROOF: Let $g_0(x) + g_1(x)p(x)^m + \ldots$ be the $p(x)^m$-adic expansion of $g(x)$.

If $y(x)$ is an m^{th} root of $g(x)$ modulo $p(x)^k$ and $y_0(x) + y_1(x)p(x) + \ldots$ is its $p(x)$-adic expansion then $y(x)^m = y_0(x)^m + y_1(x)^m p(x)^m + \ldots$ and this expression must coincide with the $p(x)^m$-adic expansion of $y(x)^m$.

Let us assume first that $m \mid k$. It can be seen that in this case (2) is satisfied if and only if

$$g_0(x) + g_1(x)p(x^m) + \ldots + g_{k/m-1}(x)p(x^m)^{k/m-1} = y_0(x)^m + y_1(x)^m p(x)^m + \ldots + y_{k/m-1}(x)^m p(x)^{m(k/m-1)}$$

Therefore $g_i(x)$ must be the m^{th} power of $y_i(x)$, for $i = 0, \ldots, k/m - 1$. But then $g(x) \bmod p(x)^k$ is the m^{th} power of a polynomial $y(x)$, i.e. it must be a polynomial in x^m and each of its coefficients must have an m^{th} root in F — it is easy at this point to find the actual polynomial $y(x)$.

Assume next that $m \not| k$. The argument used above tells us that $g_i(x) = y_i(x)^m$ for $i = 0, \ldots, \lfloor k/m \rfloor - 1$, and $g_i(x) \equiv y_i(x)^m \pmod{p(x)^s}$ for $i = \lfloor k/m \rfloor$, as asserted. Since $s < m$, the last congruence can be handled using Lemma 3. □

Note that Lemma 3 and Lemma 4 are valid for any field of characteristic $q > 0$. When the map $a \mapsto a^q$ is an automorphism of F (i.e. if F is a perfect field) we can say much more, as the next theorem shows.

THEOREM 2 *Let F be a perfect field of characteristic q. Assume that $m = q^t$ for some integer t. Then (2) admits a solution for any $k \geq 1$.*

PROOF: When F is perfect the map $a \mapsto a^q$ is an automorphism of any finite extension of F, and so is the map $a \mapsto a^m$ since m is a power of q.

Let A be the F-algebra $F[x]/(p(x)^k)$. This algebra is clearly finite dimensional over F.

As a consequence of Nakayama's lemma (see [6, Section 4.2]) the endomorphism $a \mapsto a^m$ of A is onto if and only if the induced endomorphism of $A/rad(A)$ given by $a + rad(A) \mapsto a^m + rad(A)$ is onto.

But $A/rad(A) \cong F[x]/(p(x))$ and by what we have just said the induced map $a + (p(x)) \mapsto a^m + (p(x))$ is surjective.

Therefore (2) admits a solution for any $k \geq 1$. □

REMARK: When $q \mid m$ but m is not a power of q, write m as $q^t r$, with $q \not| r$. Write (2) as $(y(x)^{q^t})^r \equiv g(x) \pmod{p(x)^k}$.

Set $z(x) := y^{q^t}$ and solve $z(x)^r \equiv g(x) \pmod{p(x)^k}$ for $z(x)$. Finally solve $y(x)^{q^t} \equiv z(x) \pmod{p(x)^k}$ for $y(x)$ to obtain a solution of (2).

3 The complex case

In $\mathbb{C}[x]$ an irreducible polynomial $p(x)$ can have only degree 1, and therefore we can take $p(x) = x - \alpha$, with $\alpha \in \mathbb{C}$. We recall here that $\mathbb{C}[x]/(x - \alpha) \cong \mathbb{C}$ under the isomorphism $g(x) + (x - \alpha) \mapsto g(\alpha)$.

If $p(x) \not| g(x)$, the congruence $y(x)^m \equiv g(x) \pmod{p(x)}$ always admits a (nonzero) solution and this solution can be lifted to a solution modulo $p(x)^k$.

If $g(x) \equiv 0 \pmod{p(x)}$ then (2) admits a solution if and only if the conditions imposed by Lemma 2 are satisfied. We summarize our results in the following theorem:

THEOREM 3 *In $\mathbb{C}[x]$ the congruence (1) admits a solution if and only if for every common root α of $f(x)$ and $g(x)$ either the multiplicity of α in $g(x)$ is greater than or equal to the multiplicity of α in $f(x)$ or else m divides the multiplicity of α in $g(x)$.*

4 The real case

In $\mathbb{R}[x]$ an irreducible polynomial $p(x)$ can have only degree 1 or 2. Assume first that $p(x) \not| g(x)$.

If $\deg p(x) = 1$, then we can take $p(x) = x - \alpha$, with $\alpha \in \mathbb{R}$; then $\mathbb{R}[x]/(p(x)) \cong \mathbb{R}$ under the isomorphism $g(x) + (p(x)) \mapsto g(\alpha)$. Then $y(x)^m \equiv g(x) \pmod{p(x)}$ admits a solution unless $g(\alpha) < 0$ and m is even. Moreover this solution can always be lifted to a solution modulo $p(x)^k$.

If $\deg p(x) = 2$, then $\mathbb{R}[x]/(p(x)) \cong \mathbb{C}$. In this case $y(x)^m \equiv g(x) \pmod{p(x)}$ admits a nonzero solution and this solution can be lifted to a solution modulo $p(x)^k$.

Assume next that $p(x) \mid g(x)$. If $\deg p(x)$ is 1 or 2 then (2) admits a solution if and only if the conditions imposed by Lemma 2 are satisfied. We summarize our results in the following theorem:

THEOREM 4 *In $\mathbb{R}[x]$ the congruence (1) admits a solution if and only if the following holds for every (real or complex) root α of $f(x)$: if l denotes the multiplicity of α in $g(x)$ and k the multiplicity of α in $f(x)$, then either*

(i). $k \leq l$, or

(ii). $m \mid l$, and whenever α is real either $(g/p^l)(\alpha) > 0$ or else m is odd.

5 Finite fields

When K is a finite field there is an easy criterion to decide if an element a has an m^{th} root in it, namely let $e := (|K| - 1)/(m, |K| - 1)$ and test if a^e is equal to 1 or not: in the first case a has exactly $(m, |K| - 1)$ roots in the field, in the second case it has no roots. We summarize our results in the following theorem:

THEOREM 5 *Let F be a finite field of characteristic q. Write m as $q^t r$ with $q \not| r$. In $F[x]$ the congruence (1) admits a solution if and only if the following holds for every irreducible factor $p(x)$ of $f(x)$: if $d := \deg p(x)$, $e := (|F|^d - 1)/(r, |F|^d - 1)$, l is equal to the highest power of $p(x)$ dividing $g(x)$ and k is equal to the highest power of $p(x)$ dividing $f(x)$, then either*

(i). $k \leq l$, or

(ii). $m \mid l$ and $(g(x)/p(x)^l)^e \equiv 1 \pmod{p(x)}$.

We would like to add the fact that when F is a finite field there are very efficient algorithms for factoring polynomials over F [1, 5], for computing the roots of polynomials over F [7, 5] and for taking m^{th} roots of elements of F [8].

Acknowledgements

The author wishes to thank Prof. J.D. Dixon for his invaluable advice and extremely helpful comments.

References

[1] E.R. Berlekamp, 'Factoring polynomials over large finite fields', *Math. Comp. 24* (1970), 713-735.

[2] N. Koblitz, *P-adic numbers, p-adic analysis and zeta functions,* second edition, (Springer-Verlag, Berlin, Heidelberg, New York, 1984).

[3] J.B. Miller, 'Power roots of polynomials', *Bull. Austral. Math. Soc. Vol. 47* (1993), 163-168.

[4] S. Lang, *Algebra,* third edition, (Addison-Wesley, Reading, Mass., 1993).

[5] R. Lidl and H. Niederreiter, *Finite Fields,* Encyclopedia of Math. and its Applications 20, (Addison-Wesley, Reading, Mass., 1983).

[6] R.S. Pierce, *Associative Algebras,* (Springer-Verlag, Berlin, Heidelberg, New York, 1982).

[7] M.O. Rabin, 'Probabilistic algorithms in finite fields', *SIAM J . Comp. Vol. 9, No.2* (1980), 273-280.

[8] K.S. Williams and K. Hardy, 'A refinement of H.C. Williams' q-th root algorithm', to appear in *Math. Comp.*

School of Computer Science, Carleton University
Recent Technical Reports

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. J. Oommen, K. Zhang and W. Lee, February 1992 (Revised July 1993)

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

TR-222 **Time-Message Trade-Offs for the Weak Unison Problem**
Amos Israeli, Evangelos Kranakis, Danny Krizanc and Nicola Santoro, March 1993

TR-223 **Anonymous Wireless Rings**
Krzysztof Diks, Evangelos Kranakis, Adam Malinowski, and Andrzej Pelc, April 1993

TR-224 **A consistent model for noisy channels permitting arbitrarily distributed substitutions, insertions and deletions**
B.J. Oommen and R.L. Kashyap, June 1993

TR-225 **Mixture Decomposition for Distributions from the Exponential Family Using a Generalized Method of Moments**
S.T. Sum and B.J. Oommen, June 1993

TR-226 **Switching Models for Non-Stationary Random Environments**
B. John Oommen and Hassan Masum, July 1993

TR-227 **The Probability of Generating Some Common Families of Finite Groups**
Vincenzo Acciaro, September 1993