Irreducible polynomials and Barker sequences

Peter Borwein*
Department of Mathematics and Statistics
Simon Fraser University
Burnaby, B.C. V5A 1S6 Canada
pborwein@cecm.sfu.ca

Erich Kaltofen†
Department of Mathematics, Box 8205
North Carolina State University
Raleigh, North Carolina 27695-8205 USA
kaltofen@math.ncsu.edu

Michael J. Mossinghoff
Department of Mathematics, Box 6996
Davidson College
Davidson, North Carolina 28035-6996 USA
mimossinghoff@davidson.edu

Abstract

A Barker sequence is a finite sequence $a_0, \ldots, a_{n-1}$, each term $\pm 1$, for which every sum $\sum_{k=0}^n a_ka_{n-k}$ with $0 < k < n$ is either 0, 1, or $-1$. It is widely conjectured that no Barker sequences of length $n > 13$ exist, and this conjecture has been verified for the case when $n$ is odd. We show that in this case the problem can in fact be reduced to a question of irreducibility for a certain family of univariate polynomials: No Barker sequence of length $2m + 1$ exists if a particular integer polynomial of degree $4m$ is irreducible over $\mathbb{Q}$. A proof of irreducibility for this family would thus provide a short, alternative proof that long Barker sequences of odd length do not exist. However, we also prove that the polynomials in question are always reducible modulo $p$, for every prime $p$.

1 Introduction

For a positive integer $m$, let $g_m(x)$ denote the polynomial

$$g_m(x) = x^{4m} + x^{4m-2} + \cdots + x^{2m+2} + (-1)^m(2m+1)x^{2m} + x^{2m-2} + \cdots + x^2 + 1.$$ 

Five of the first six of these polynomials factor over the rationals in a nice way—as a product of two irreducible polynomials, each with $\pm 1$ coefficients:

$$g_1(x) = x^4 - 3x^2 + 1 = (x^2 - x - 1)(x^2 + x - 1),$$
$$g_2(x) = x^8 + x^6 + 5x^4 + x^2 + 1 = (x^4 - x^3 + x^2 + x + 1)(x^4 + x^3 + x^2 - x + 1),$$
$$g_3(x) = x^{12} + x^{10} + x^8 - 7x^6 + x^4 + x^2 + 1$$
$$= (x^6 - x^5 + x^4 + x^3 - x^2 - x - 1)(x^6 + x^5 + x^4 - x^3 - x^2 + x - 1),$$
$$g_5(x) = x^{20} + x^{18} + x^{16} + x^{14} + x^{12} - 11x^{10} + x^8 + x^6 + x^4 + x^2 + 1$$
$$= (x^{10} - x^9 + x^8 + x^7 - x^6 + x^5 + x^4 + x^3 - x^2 - x - 1)$$
$$\cdot (x^{10} + x^9 + x^8 - x^7 - x^6 - x^5 + x^4 - x^3 - x^2 + x - 1),$$
$$g_6(x) = x^{24} + x^{22} + x^{20} + x^{18} + x^{16} + x^{14} + 13x^{12} + x^{10} + x^8 + x^6 + x^4 + x^2 + 1$$
$$= (x^{12} - x^{11} + x^{10} - x^9 + x^8 + x^7 - x^6 - x^5 + x^4 + x^3 - x^2 + x + 1)$$
$$\cdot (x^{12} + x^{11} + x^{10} + x^9 + x^8 - x^7 - x^6 + x^5 + x^4 - x^3 + x^2 - x + 1).$$

---

*Research supported in part by NSERC of Canada and MITACS.
†Research supported in part by NSF under Grant CCF-0514585.
One might expect some similar factorizations to appear for larger \( m \), but, curiously, no other polynomials \( g_m(x) \) are even known to be reducible! In fact, the polynomials shown here are the only reducible ones in the sequence up to \( m = 1000 \). In this note, we show how the question of irreducibility for these polynomials is connected to an old and difficult problem in combinatorial optimization involving certain binary sequences with remarkable properties, known as Barker sequences. We show that establishing that \( g_m(x) \) is irreducible for all \( m \geq 7 \) would provide a simple proof that Barker sequences of odd length do not exist. However, we also demonstrate that the polynomials \( g_m(x) \) are reducible mod \( p \), for every prime \( p \). Consequently, many standard tests for irreducibility do not directly apply for these polynomials.

2 Barker Sequences

We begin by recalling the definition of a Barker sequence, and describing some of its properties. For a sequence of integers \( a_0, a_1, \ldots, a_{n-1} \), each one \( \pm 1 \), and for an integer \( k \) with \( |k| < n \), define the \( k \)th aperiodic autocorrelation of the sequence by

\[
c_k = \sum_{i=0}^{n-1-k} a_i a_{i+k}
\]

if \( k \geq 0 \), and similarly set \( c_{-k} = \sum_{i=k}^{n-1} a_i a_{i-k} = c_k \). The value of \( c_0 \) is therefore \( n \), independent of the choice of signs in the \( a_k \). This number is called the peak autocorrelation. The other \( c_k \) are the off-peak autocorrelations, and sequences with especially small off-peak autocorrelations are of great interest in applications in communications. By considering the parity of the number of terms in the sum (1), we see that the best we can possibly achieve is \( |c_k| \leq 1 \) for each nonzero \( k \), so in fact \( c_k = \pm 1 \) if \( n - k \) is odd and \( c_k = 0 \) otherwise. In his 1953 paper [1], Barker asked if there exist sequences \( \{a_k\} \) in which each off-peak autocorrelation \( c_k \) is 0 or \( -1 \), and sequences achieving the more symmetric condition \( |c_k| \leq 1 \) for \( k \neq 0 \) are known today as Barker sequences.

Since negating the terms of a sequence \( \{a_k\} \) does not disturb its autocorrelations, and negating every other term does not affect the magnitudes of its autocorrelations, we may assume that \( a_0 = a_1 = 1 \). With this normalization, there are just eight known Barker sequences. These are displayed in Table 1, where we use + and - to represent +1 and -1, respectively. Only three of these satisfy the more strict condition requested by Barker—the ones of length 3, 7, and 11.

<table>
<thead>
<tr>
<th>( n )</th>
<th>Barker sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>++</td>
</tr>
<tr>
<td>3</td>
<td>+++-</td>
</tr>
<tr>
<td>4</td>
<td>++++</td>
</tr>
<tr>
<td>5</td>
<td>++++-</td>
</tr>
<tr>
<td>7</td>
<td>+++++-</td>
</tr>
<tr>
<td>11</td>
<td>+++++-++++-++</td>
</tr>
<tr>
<td>13</td>
<td>+++++-+++++-+</td>
</tr>
</tbody>
</table>

Table 1: Barker sequences with \( a_0 = a_1 = 1 \).

It is widely conjectured that this list forms the complete set of Barker sequences, but this problem remains open and seems surprisingly hard. Before describing how this problem is related to the polynomials \( g_m(x) \), we first record some properties of Barker sequences. The following results were established by Turyn and Storer [7, 8]; we include the proof here for the reader’s convenience.

**Theorem 1.** Suppose \( a_0, a_1, \ldots, a_{n-1} \) is a sequence of integers with each \( a_i = \pm 1 \), and let \( \{c_k\} \) denote the sequence of its aperiodic autocorrelations. Then

\[
c_k + c_{n-k} \equiv n \mod 4.
\]

Suppose further that the sequence \( \{a_k\} \) is a Barker sequence. If \( n \) is odd, then

\[
a_k a_{n-1-k} = (-1)^{\frac{n-1}{2} + k}
\]

(2)
for $0 \leq k < n$, and $c_k + c_{n-k} = (-1)^{(n-1)/2}$ for $0 < k < n$. If $n$ is even and $n > 2$, then $n = 4m^2$ for some integer $m$, and $c_{n-k} = -c_k$ for $0 < k < n$.

**Proof.** Since $c_k$ records the difference between the number of positive and negative terms in $\sum_{i=0}^{n-1-k} a_ia_{i+k}$, it follows that

$$\prod_{i=0}^{n-k-1} a_ia_{i+k} = (-1)^{(n-k-c_k)/2}$$

for $0 \leq k < n$. Multiplying this product by the same expression with $k$ replaced by $n-k$, we obtain

$$(-1)^{(n-c_k-c_{n-k})/2} = \prod_{i=0}^{k-1} a_ia_{i+n-k} \prod_{i=0}^{n-k-1} a_ia_{i+k} = 1,$$

so $c_k + c_{n-k} \equiv n \mod 4$. On the other hand, multiplying (3) by the same equation where $c_k$ is even, then exactly one of $c_k$ and $c_{n-k}$ is 0, and since $c_k + c_{n-k} \equiv n \mod 4$, it follows that $c_k = (-1)^{(n-1)/2}$ when $k$ is even. Therefore, $c_k + c_{n-k} = (-1)^{(n-1)/2}$ for $0 < k < n$. Further, we see that $c_k + c_{k+1} = (-1)^{(n-1)/2}$ for $0 < k < n$, and combining this with (4) establishes (2).

If $n$ is even, then $c_k = 0$ for even $k \neq 0$, so in particular $c_k + c_{n-k} = 0$ when $n > 2$, and therefore $n \equiv 0 \mod 4$ in this case. It follows then that $c_k + c_{n-k} = 0$ when $n \geq 4$ and $0 < k < n$. Last, since

$$\left( \sum_{i=0}^{n-1} a_i \right)^2 = c_0 + \sum_{k=1}^{n-1} (c_k + c_{n-k}) = n,$$

we see that $n$ is a perfect square in this case. $\square$

Many additional restrictions on Barker sequences are known. Turyn and Storer [7] proved that if the length $n$ of a Barker sequence is odd, then $n \leq 13$, so the complete list for this case appears in Table 1. It follows from this that no additional sequences satisfy Barker’s original requirement for sequences whose off-peak autocorrelations are all 0 or −1, since Theorem 1 implies that any such sequence must have length $n \equiv 3 \mod 4$. For the case when the length is even, several additional restrictions are known on $m$ if $n = 4m^2$: $m$ must be odd and cannot be a prime power [2, sec. 2D and 4C; 5; 9], every prime divisor $p$ of $m$ must satisfy $p \equiv 1 \mod 4$ [4], and if $m > 1$ then in fact $m > 5 \cdot 10^10$ [6]. Thus, any additional Barker sequences must have length exceeding $10^{22}$. More information on Barker sequences, and their connection to other open problems in analysis and number theory, appears in [3].

### 3 A Question of Irreducibility

The proof of Turyn and Storer that no Barker sequences of odd length $n$ exist for $n > 13$ is elementary, though somewhat complicated, and relies on showing that long Barker sequences of odd length must exhibit certain patterns. We describe here a possible alternative route to proving this result, in the hope of spurring further research.

**Theorem 2.** If the polynomial

$$g_m(x) = (-1)^m(2m+1)x^{2m} + \sum_{k=1}^{m} (x^{2m+2k} + x^{2m-2k})$$

is irreducible over $Q$, then no Barker sequence of length $2m+1$ exists.

We require a brief definition before supplying the proof. For a polynomial $f(x)$ with $f(0) \neq 0$, we define its *reciprocal polynomial* $f^*(x)$ by $f^*(x) := x^{\deg f} f(1/x)$. Also, for $f(x) \in Z[x]$ with $f(0) \neq 0$, we say that $f$ is self-reciprocal if $f = \pm f^*$. 

120
Proof of Theorem 2. Suppose \( \{a_k\} \) is a Barker sequence of length \( 2m+1 \), and let \( f_m(x) = \sum_{k=0}^{2m} a_k x^k \). By Theorem 1, the aperiodic autocorrelation \( c_k \) is 0 if \( k \) is odd and \( (-1)^m \) if \( k \neq 0 \) and \( k \) is even. Thus

\[
f_m(x) f_m^*(x) = \sum_{k=-m}^{m} c_{2k} x^{2k+2m} \]

\[
= (2m+1)x^{2m} + \sum_{k=1}^{m} (-1)^m \left( x^{2m+2k} + x^{2m-2k} \right),
\]

and so \( g_m(x) = (-1)^m f_m(x) f_m^*(x) \).

We conjecture that the polynomial \( g_m(x) \) is in fact irreducible for every \( m > 6 \). However, we find that these polynomials are reducible mod \( p \), for every prime number \( p \). This follows immediately from the following more general statement.

Theorem 3. Suppose \( f(x) \) is an even, self-reciprocal polynomial with integer coefficients and \( \deg(f) \geq 4 \). Then \( f(x) \) is reducible mod \( p \) for every prime \( p \).

Proof. If \( f = -f^* \) then \( f(\pm 1) = 0 \) so \( f \) is reducible over \( \mathbb{Q} \). If \( f = f^* \) and \( \deg(f) = 4n+2 \) then \( f(\pm i) = 0 \), so again \( f \) is reducible over \( \mathbb{Q} \) for \( n \geq 1 \). Suppose then that \( f = f^* \) and \( \deg(f) = 4n \) with \( n \geq 1 \), and write \( f(x) = g(x^2) \). Clearly \( f(x) \equiv g(x)^2 \mod 2 \), so suppose \( p \) is an odd prime, and \( g(x) \) is irreducible mod \( p \). Let \( \alpha \) be a root of \( g \) in its splitting field \( \mathbb{F}_{p^{2n}} \) over \( \mathbb{F}_p \), so that

\[
g(x) = \prod_{k=0}^{2n-1} \left( x - \alpha^{p^k} \right).
\]

Let \( \gamma \) be a primitive element of \( \mathbb{F}_{p^{2n}} \), and let \( \alpha = \gamma^t \) for some integer \( t \). Since \( g \) is self-reciprocal, \( \alpha^{-1} \) is also a root of \( g \), so \( \alpha^{-1} = \gamma^{-t} = \alpha^{p^j} = \gamma^{tp^i} \) for some positive integer \( j < 2n \). Then \( \gamma^{tp^i} = \gamma^{-tp^i} = \gamma^t \), so \( \alpha^{p^j-1} = 1 \), and consequently \( j = n \). Therefore \( \gamma^{t(p^{n+1})} = 1 \), so \( (p^n - 1) \mid t \) and thus \( t \) is even. Let \( \beta = \gamma^{t/2} \). Then

\[
f(x) = \prod_{k=0}^{2n-1} \left( x + \beta^{p^k} \right) \prod_{k=0}^{2n-1} \left( x - \beta^{p^k} \right),
\]

and each of these products lies in \( \mathbb{F}_p[x] \).

This result would appear to make the determination of the irreducibility of the polynomials \( g_m(x) \) a more challenging proposition!

References


On a query algorithm for a divisibility problem

Adrian Dumitrescu†
Guangwu Xu†

Abstract

According to an old result of Turán, any \((n+1)\)-subset of \(\{1,2,\ldots,2n\}\) contains a pair of divisible numbers. Ciurea et al. have recently considered a natural algorithmic variant of this classic mathematical result: if the subset is not known, and it is only accessible via a membership oracle, what is the minimum number of questions necessary to identify one such divisible pair? They showed a \(\frac{4}{3}n - O(1)\) lower bound and also designed an algorithm which they conjectured asks no more than \(\frac{4}{3}n + O(1)\) queries, and therefore would be optimal. We reanalyze the proposed algorithm and prove that it comes close to the conjectured value, in asking no more than \((\frac{4}{3} + \frac{5}{108})n + O(1)\) queries; this corrects an error in the old analysis.

1 Introduction

It is well known that any \((n+1)\)-subset of \(\{1,2,\ldots,2n\}\) contains a pair of divisible numbers. This was proved by Turán and Lázár independently, and also by Vásonyi and Wachsberger, see [2] (pp. 194–195). Ciurea et al. [1] have recently considered a natural algorithmic variant of this classic mathematical result: if the subset is not known, and it is only accessible via a membership oracle, what is the minimum number of questions necessary to identify one such divisible pair? Using a simple but efficient pairing strategy for an adversary answering the questions, they proved a \(\frac{4}{3}n - O(1)\) lower bound on the number of queries. They also designed an algorithm which they conjectured asks no more than \(\frac{4}{3}n + O(1)\) queries, and therefore would be optimal. A tentative analysis of the algorithm is given in [1], claiming an upper bound of \((\frac{4}{3} + \frac{5}{108})n + O(1)\) queries. Here we prove that their algorithm comes close to the conjectured value, in asking no more than \((\frac{4}{3} + \frac{5}{108})n + O(1)\) queries. This corrects an error in the analysis in [1].

Theorem 1 In the worst case, \((\frac{4}{3} + \frac{5}{108})n + O(1)\) membership queries suffice to find a divisible pair from an unknown \((n+1)\)-subset of \(\{1,2,\ldots,2n\}\).

2 Proof of Theorem 1

The goal of the algorithm is to find a divisible pair by asking membership questions of the form: Is \(i\) in \(S\)? — where \(S\) is the unknown \((n+1)\)-subset of \(\{1,2,\ldots,2n\}\). We refer to the following query algorithm presented in [1]: the algorithm considers the positive integer numbers \(i = 1, 2, \ldots\) in increasing order until it finds a divisible pair in the subset \(S\). If \(i\) is not probed already, and \(i \leq 2n/3\), \(i\) is probed. If the answer is \(\text{no}\), the algorithm continues with the next number \(i + 1\). If the answer is \(\text{yes}\), \(i\)'s multiples are also probed in increasing order (if not probed already). Observe that any positive answer to a multiple would find a divisible pair and the algorithm stops. When (if) the algorithm reaches numbers \(i > 2n/3\), and \(i \leq n\), if \(i\)'s single multiple \(2i \leq 2n\) has been previously probed (and received a negative answer), there is no point in querying \(i\), \(i\) is skipped, and the algorithm considers \(i + 1\) next. (To avoid repeated oracle membership queries for the same integer, the algorithm remembers all previous answers.)

The purpose of analysis [1], the execution of the algorithm is broken into two stages: the first stage lasts as long as \(i \leq 2n/3\), then possibly (if the algorithm did not terminate by then), the second stage starts. If the algorithm terminates during the first stage, it is shown in [1] that at most \(\frac{4}{3}n + O(1)\) queries are asked. Now assume that the algorithm terminates in the second stage; in this case, all numbers between 1 and \(2n/3\) are probed. Let \(Y\) be the set of such numbers that received a positive (yes) answer, and let \(N\) be the set of probed numbers which received a negative (no) answer during the first stage (\(N\) possibly includes numbers larger than \(2n/3\) which are probed as multiples, in the negative streak that follows a positive answer to some \(i \leq 2n/3\)). Let now \(M = N \cap \{2n/3 + 1, \ldots, 2n\}\). As

*Department of Computer Science, University of Wisconsin-Milwaukee, WI 53201-0784, USA, email: ad@cs.uwm.edu Supported in part by NSF CAREER grant CCF-0444188.
†Department of Computer Science, University of Wisconsin-Milwaukee, WI 53201-0784, USA, email: gux@uwm.edu
shown in [1], proving that $|M| \geq 2|Y| - n/24$ implies an upper bound of $(\frac{1}{16} + \frac{1}{24})n + O(1)$ on the total number of queries. As part of the proof, it is claimed in [1] that $M$ contains two power-of-two multiples for every element in $Y \cap \{1, \ldots, n/2\}$, however this is incorrect: for instance take $y = n/3$ (or more generally $n/4 < y \leq n/3$), and observe that $y$ has only one power-of-two multiple in the interval $\{2n/3 + 1, \ldots, 2n\}$, namely $z = 4y$.

Next we correct this error by making a more careful analysis of this part, and prove instead that $|M| \geq 2|Y| - 5n/108$. Set $m = 2n/3$, and assume $m$ is an integer.\(^1\)

A set of positive integers is said to be multiple-free (or divisor-free) if no element is a multiple of any other. Note that the algorithm ensures that the set of numbers $Y$ (the numbers between 1 and $2n/3$ which received a positive answer) is multiple-free. We establish the following

**Lemma 1** Let $Y \subseteq \{1, \ldots, m\}$ be multiple-free, where $m$ is a positive integer. Let $M$ be the set of multiples of elements in $Y$ among $\{m + 1, m + 2, \ldots, 3m\}$. Then

$$|M| \geq 2|Y| - \frac{5}{72}m - O(1).$$

**Proof.** We partition $Y = \{y_1 < y_2 < \ldots < y_l\}$ into three sets (intervals): $Y_1 = \{y \in Y : 1 \leq y \leq m/2\}$, $Y_2 = \{y \in Y : m/2 < y \leq 2m/3\}$, $Y_3 = \{y \in Y : 2m/3 < y \leq m\}$. For each element $y$ in $Y$, we specify two multiples $u, v$ in $\{m + 1, m + 2, \ldots, 3m\}$, where $u < v$, and then account for the possible overlap to obtain the bound (in a manner similar to the approach in [1]). We have three different cases, depending on whether $y \in Y_1$, $y \in Y_2$, or $y \in Y_3$.

**Case 1:** $y \in Y_1$. Let $k$ be the smallest positive integer, such that $2^ky > m$; clearly $k \geq 2$. Set $u = 2^ky \in (m, 2m]$.

If $u \leq 3m/2$, set $v = 2^{k+1}y \in (2m, 3m]$. If $u > 3m/2$, set $v = 3 \cdot 2^{k-1}y \in (9m/4, 3m]$.

**Case 2:** $y \in Y_2$. Let $u = 2y \in (m, 4m/3]$, and let $v = 4y \in (2m, 8m/3]$.

**Case 3:** $y \in Y_3$. Let $u = 2y \in (4m/3, 2m]$, and let $v = 3y \in (2m, 3m]$.

Denote by $M_i$ the multiples of elements in $Y_i$, for $i = 1, 2, 3$. Denote also by $u_i$ (resp. $v_i$), a $u$ (resp. $v$) multiple in $M_i$. To distinguish the two possibilities for $v$ in Case 1, we denote them by $v_{1a}$ and $v_{1b}$ respectively. The possible overlap of multiples of $y$’s coming from the same or different groups (the sets $Y_1, Y_2, Y_3$) is limited by the multiple-free assumption or by disjointness of the interval ranges; for instance we cannot have, say, $u_1 = v_1$, since $u_1 \leq 2m$, while $v_3 > 2m$; we cannot have, say, $u_1 = u_3$, since $Y$ is multiple-free. In fact, we cannot have overlap between any two $u$’s since $Y$ is multiple-free. It can be verified that there are only four possible types of overlap:

**Case A:** $v_{1a} = v_3$. Let $z$ be a common multiple of this form. We thus have $z = 2^{k+1}y_{1a} = 3y_j \in (2m, 3m]$ for some $i < j$. Since $y_i$ must be divisible by 3, and we have $k_i \geq 2$, $z$ is a multiple of 24 in the interval $(2m, 3m]$, and there are at most $m/24$ such multiples.

**Case B:** $v_2 = v_3$. Let $z$ be a common multiple of this form. We have $4y_i = 3y_j \in (2m, 8m/3]$ for some $i < j$. Since $y_i$ must be divisible by 3, $z$ is a multiple of 12 in the interval $(2m, 8m/3]$. The even multiples of 12 (that is, multiples of 24) in this interval have already been accounted for in Case A, and there are at most $2m/3 + \frac{1}{12} \leq \frac{m}{3}$ odd multiples of 12 in the interval $(2m, 8m/3]$.

**Case C:** $v_{1a} = v_{1b}$. We have $z = 2^{k+1}y_{1a} = 3 \cdot 2^{k-1}y_j \in (9m/4, 3m]$. This leads to $z$ being a multiple of 24 in the interval $(9m/4, 3m]$, and these have been already counted in case A.

**Case D:** $v_{1b} = v_2$. We have $z = 3 \cdot 2^{k-1}y_i = 4y_j \in (9m/4, 8m/3]$ for some $i < j$. Since $y_j$ is a multiple of 3, this leads to $z$ being a multiple of 12 in the interval $(9m/4, 8m/3]$, which are covered by cases A and B already.

Summarizing, the total possible overlap of multiples (cases A,B,C,D) is at most $(\frac{1}{24} + \frac{1}{36})m = \frac{5}{72}m$. We conclude by observing that there is no triple overlap involving two (or more) from the above list of four cases; consequently $|M| \geq 2|Y| - \frac{5}{72}m - O(1)$.\(\square\)

To finish the proof of Theorem 1, recall that $m = 2n/3$, so by Lemma 1, $|M| \geq 2|Y| - \frac{5}{108}n - O(1)$. Therefore the total number of queries is at most $(\frac{1}{4} + \frac{1}{120})n + O(1)$, as claimed.

**Remark.** We believe the inequality in the lemma can be substantially improved for large enough $|Y|$, ideally to $|M| \geq 2|Y| - o(m)$. This would imply a matching (modulo lower order terms) upper bound of $(\frac{1}{4} + o(1))n$ on the

\(^1\)We omit all floor and ceiling signs, since they are not essential and would only complicate the notation; the results would only change plus or minus a constant additive term, which is accounted anyway in the final result.
number of queries done by the algorithm. Note that the inequality cannot be replaced by the stronger $|M| \geq 2|Y|$, as the following example shows: $m = 20$, $Y = \{12, 16, 18, 20\}$, $M = \{24, 32, 36, 40, 48, 54, 60\}$, for which $|M| = 2|Y| - 1$. We concur with [1] in that closing the gap between the upper and the lower bound remains an interesting problem.

References


Abstracts of Recent Doctoral Dissertations in Computer Algebra

Communicated by Ilias Kotsireas

In this issue we continue our new section of the ACM Communications in Computer Algebra on the abstracts of recent doctoral dissertations in Computer Algebra and Symbolic Computation. We encourage all recent Ph.D. graduates (and their supervisors), who have defended in the past year, to submit their abstracts for publication here. We hope you agree that this is a great way to bring attention to the young researchers in our field, and see the new directions of their research. Please send abstracts to the CCA editors <editors_SIGSAM@acm.org> for consideration.

Symbolic Computation Techniques for Solving Large Expression Problems from Mathematics and Engineering

Dr. Wenqin Zhou
Applied Mathematics Department,
University of Western Ontario,
London, Ontario, CANADA.
(publish.uwo.ca/~wzhou25/)

Supervisors: David J. Jeffrey and Gregory J. Reid
External examiner: Ilias S. Kotsireas
Defence date: April 19, 2007

This thesis studies the use of computer algebra methods to solve some large-expression problems from mathematics and engineering. We give several strategies for solving problems from symbolic linear algebra and dynamic systems.

First, we describe new forms for fraction-free LU factoring and QR factoring. These new forms keep both the computation and the output results in the same domain as the input domain and thereby increase the computational efficiency in applications by delaying the appearance of quotients of the input data. To compute the new forms, we use a fraction-free variant of Gaussian elimination to control the growth of matrix entries. We give a complexity analysis for standard domains.

Secondly, we propose a general method, hierarchical representation and signature computing for zero testing, to deal with problems with intermediate or inherent expression swell. For instance, when we use Gaussian elimination to solve large symbolic linear equations, the resulting large expressions can be handled using our general method. We implement a version of LU factoring.
using hierarchical representation with signature computing for zero testing. The LU factoring is the standard one, rather than the fraction-free one described above. We prove that the improved algorithm is much faster than the classical LU factoring algorithm using Gaussian elimination and give associated time complexity analysis and experimental results.

Besides large expression problems from linear algebra, we also explore large expression problems from engineering, especially those arising from analyzing and solving multibody dynamic systems and limit cycle computations. We define a new concept, implicit reduced involutive form, to cope with large expression problems resulting from symbolically pre-processing systems of differential algebraic equations (DAE). We also show how symbolic pre-processing can be combined with numerical integration to solve a problem from limit cycle computations which could not be directly solved because of large expression swell.

The techniques we develop in this thesis are quite general and can be easily applied to other similar areas, such as computing determinants and solving more general DAE models.
Applicable Algebra and Computer Science:  
A Meeting in Honor of Jacques Calmet

http://www.unirioja.es/dptos/dmc/ApplicableAlgebra.shtml

February 28-29, 2008  
Universidad de La Rioja, Logroño, Spain

Communicated by Julio Rubio, julio.rubio@unirioja.es

Speakers

- Teo Mora, Genova University
- Werner Seiler, Kassel University
- Graham Ellis, National University of Ireland
- Francis Sergeraert, Institut Fourier
- Anna Bigatti, Genova University
- Isabel Bermejo, University of La Laguna
- Henry P. Wynn, London School of Economics

Contributed Presentations

- Luis Laita, Un. Politécnica de Madrid
- Eugenio Roanes, Un. Comlutense de Madrid
- Edgar Martínez-Moro, Un. de Valladolid
- Rober Zeier, Harvard School of Engineering and Applied Sciences
- Marc Giusti, LIX, École Polytechnique
- Philippe Gimenez, Un. de Valladolid
- Mehdi Sabhi, Karlsruhe University
Call for Papers: AB 2008
Third International Conference on Algebraic Biology
July 31-August 2, 2008, RISC, Castle of Hagenberg, Austria

The Third International Conference on Algebraic Biology, AB’08, is an international forum to promote discussion and interaction between researchers who apply symbolic computation to various issues in biology / life sciences. The conference covers all aspects of applications of symbolic computation methods in biology.

Important Dates
January 21, 2008  Deadline for submission
March 31, 2008  Notification of acceptance
April 28, 2008  Camera-ready paper submission

Conference Topics
The conference covers all aspects of applications of symbolic computation methods in biology, e.g.

- mathematical modeling
- model identification
- system analysis and design
- system verification
- system synthesis
- etc.

in
- molecular sequence analysis
- molecular structure analysis
- molecular evolution
- genomics
- proteomics
- gene regulation
- gene expression
- gene ontology
- network inference
- etc.

using
- polynomial methods
- group theory
- rewriting
- automated reasoning
- automata theory
- formal language methods
- combinatorics
- graph theory
- artificial intelligence
- hybrid symbolic-numerical methods
- differential algebra
- local analysis
- etc.

in various computing paradigms like
- sequential
- parallel
- distributed
- grid computing
- cellular
- genetic
- etc.

Submission
Authors are invited to submit original papers that have not been submitted for publication elsewhere. Contributions that present recent results (including significant work-in-progress) and identify and explore new directions of research are welcome.

Submitted papers will be peer-reviewed, and the accepted papers will appear in the proceedings before the Conference. The proceedings will be published in the Springer LNCS series. See the conference website for details on the submission format.

Revised versions of selected papers may later be submitted to Mathematics in Computer Science (MCS), Special Issue on Symbolic Computation in Biology, if they substantially extend the ideas and topics published in the Proceeding Volume. See http://www.cbrc.jp/~horimoto/MCS_si/ for details.
Invited Speakers

Keynote Talks: Kiyoshi Asai, Charles Cantor, David Harel.

Conference Chairs
Bruno Buchberger, Katsuhisa Horimoto, Reinhard Laubenbacher, Bud Mishra.

Program Chairs and Proceedings Editors
Katsuhisa Horimoto, Georg Regensburger, Markus Rosenkranz, Hiroshi Yoshida.

Program Committee

Sachiyo Aburatani  Erich Kaltofen  Seth Sullivant
Tatsuya Akutsu    Veikko Keranen    Carolyn L. Talcott
Hirokazu Anai     Hans A. Kestler  Francis Thackeray
Niko Beerenwinkel Reinhard Laubenbacher Ashish Tiwari
Armin Biere       Pierre Lescanne  Hiroyuki Toh
Bruno Buchberger  James F. Lynch  Dongming Wang
Luca Cardelli     Manfred Minimair  Bridget S. Wilson
Gautam Dasgupta   Bud Mishra      Limsoon Wong
Francois Fages    Eugenio Omodeo  Kazuhiro Yokoyama
Hoon Hong         Georg Regensburger Hiroshi Yoshida
Katsuhisa Horimoto Markus Rosenkranz  Ruriko Yoshida
Abdul Jarrah      Stanly Steinberg  

ACA’08
14th International Conference on Applications of Computer Algebra

http://www.risc.uni-linz.ac.at/about/conferences/aca2008/

http://math.unm.edu/aca.html (main ACA page)

July 27–30, 2008

RISC-Linz, Hagenberg, Austria

Communicated by Ilias S. Kotsireas

General Chairs: Vladimir Gerdt (gerdt@jinr.ru)
Wolfgang Windsteiger (wolfgang.windsteiger@risc.uni-linz.ac.at)

Coordination: Bruno Buchberger

Scope:

The ACA series of conferences is devoted to promoting the applications and development of Computer Algebra and Symbolic Computation. Topics include computer algebra and symbolic computation in engineering, the sciences, medicine, pure and applied mathematics, education, communication and computer science. For more information please see http://math.unm.edu/aca.html (main ACA page).

Meeting Format:

The meeting will be run in the standard format where individuals are invited to organize a special session. Individuals can propose a special session by contacting the conference chairs, session proposals will be approved by the ACA board. All paper submissions must be directed to an organizer of an appropriate special session.

ACA 2008 is a part of the RISC Summer 2008 event that consists of conferences and schools organized by RISC in summer 2008:

<table>
<thead>
<tr>
<th>Event</th>
<th>Title</th>
<th>Dates</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTA’08</td>
<td>(Rewrite Techniques and Applications)</td>
<td>July 14–18</td>
<td>Mo–Fr</td>
</tr>
<tr>
<td>ISSAC’08</td>
<td>(International Symposium on Symbolic and</td>
<td>July 20–23</td>
<td>Su–We</td>
</tr>
<tr>
<td></td>
<td>Algebraic Computation)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SFB-SC 08</td>
<td>(Final Conference of the Special Research</td>
<td>July 24–26</td>
<td>Th–Sa</td>
</tr>
<tr>
<td></td>
<td>Area “Scientific Computing”)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACA’08</td>
<td>(Applications of Computer Algebra)</td>
<td>July 27–30</td>
<td>Su–We</td>
</tr>
<tr>
<td>AB’08</td>
<td>(Algebraic Biology)</td>
<td>July 31–Aug. 2</td>
<td>Th–Sa</td>
</tr>
</tbody>
</table>

For more information, please see

http://www.risc.uni-linz.ac.at/about/conferences/summer2008/
AISC 2008 – 9th International Conference on
Artificial Intelligence and Symbolic Computation
Theory, Implementations and Applications
http://events.cs.bham.ac.uk/aisc08/
Birmingham, UK, 31 July – 2 August 2008

Call for Papers


Artificial Intelligence and Symbolic Computation are two views and approaches for automating problem solving, in particular mathematical problem solving. The two approaches are based on heuristics and on mathematical algorithmics, respectively. Artificial Intelligence can be applied to Symbolic Computation and Symbolic Computation can be applied to Artificial Intelligence. Hence, a wealth of challenges, ideas, theoretical insights and results, methods and algorithms arise in the interaction of the two fields and research communities. Advanced tools of software technology and system design are needed and a broad spectrum of applications is possible by the combined problem solving power of the two fields.

Hence, the conference is in the center of interest and interaction for various research communities:

- artificial intelligence,
- symbolic computation,
- computer algebra,
- automated reasoning,
- formal mathematics,
- mathematical knowledge management,
- automated discovery,
- machine learning,
- logic,
- software technology,
- semantic web technology,
- computer-based math teaching and didactics.

Topics. Topics of particular interest of the conference include:

- AI in Symbolic Mathematical Computing
- Computer Algebra Systems and Automated Theorem Provers
- Integration of Logical Reasoning and Computer Algebra
- Symmetries in AI problems,
- Engineering, Industrial and Operations Research Applications
- Foundations and Complexity of Symbolic Computation
- Mathematical Modeling of Multi-Agent Systems
- Programming Languages for Symbolic Computation
- Symbolic Computations for Expert Systems and Machine Learning
- Implementations of Symbolic Computation Systems
- Logic and Symbolic Computing
- Implementation and Performance Issues
• Intelligent Interfaces
• Symbolic Techniques for Document Analysis

Papers on other topics with links to the above research fields and topics will also be welcomed for consideration.

**Proceedings.** The proceedings of the conference will be published as a volume in the series Lecture Notes in Artificial Intelligence (LNAI) by Springer-Verlag. Accepted papers will have to be prepared in LaTeX and formatted according to the requirements of the Springer’s LNAI series (the corresponding style files can be downloaded from [http://www.springer.de/comp/lncs/authors.html](http://www.springer.de/comp/lncs/authors.html) and are the same for LNCS and LNAI).

**Submission.** Theoretical and applied research papers on all topics within the scope of the conference are invited. Submitted papers (in English) must not exceed 15 pages in length (in the LNCS style). The title page should contain the title, author(s) with affiliation(s), e-mail address(es), listing of keywords and abstract plus the topics from the above list to which the paper is related. The program committee (PC) will subject all submitted papers to a peer review. Theoretical papers will be judged on their originality and contribution to their field, and applied papers on the importance and originality of the application. Results must be original and have not been published elsewhere. The web page for electronic submission is at [http://www.easychair.org/AISC08/](http://www.easychair.org/AISC08/).

**Important Dates**

**Programme Committee**
Volker Sorge (University of Birmingham, UK), Chair
Alessandro Armando (University of Genoa, Italy)
Christoph Benzmueller (Universität des Saarlandes, Germany)
Bruno Buchberger (RISC, Austria)
Russell Bradford (University of Bath, UK)
Jacques Calmet (University of Karlsruhe, Germany)
John Campbell (University College London, UK)
Jacques Carette (McMaster University, Canada)
Arjeh Cohen (Eindhoven University of Technology, The Netherlands)
Simon Colton (Imperial College London, UK)
Timothy Daly (Carnegie Mellon, USA)
Lucas Dixon (University of Edinburgh, UK)
William M. Farmer (McMaster University, Canada)
Martin Charles Golumbic (University of Haifa, Israel)
Hoon Hong (North Carolina State University, USA)
Tetsuo Ida (University of Tsukuba, Japan)
Tom Kelsey (University of St Andrews, UK)
Petr Lisoné (Simon Fraser University, Canada)
George Labahn (University of Waterloo, Canada)
Renaud Rioboo (Université Pierre et Marie Curie - LIP6, France)
Karem Sakallah (University of Michigan, USA)
Jrg Siekmann (Universität des Saarlandes, DFKI, Germany)
Elena Smirnova (Texas Instruments, USA)
Stephen M. Watt (University of Western Ontario, Canada)
Wolfgang Windsteiger (RISC, Austria)
Dongming Wang (Beihang University, China and UPMC-CNRS, France)
Call for Papers: Calculemus 2008
July 30 – August 1, 2008, University of Birmingham, UK
http://events.cs.bham.ac.uk/calculemus08/

Calculemus is a series of conferences dedicated to the integration of computer algebra systems (CAS) and systems for mechanised reasoning, the interactive theorem provers or proof assistants (PA) and the automated theorem provers (ATP).

Currently, symbolic computation is divided into several (more or less) independent branches: traditional ones (e.g., computer algebra and mechanised reasoning) as well as newly emerging ones (on user interfaces, knowledge management, theory exploration, etc.) The main concern of the Calculemus community is to bring these developments together in order to facilitate the theory, design, and implementation of integrated systems for computer mathematics that will routinely be used by mathematicians, computer scientists and engineers in their every day business.

For the upcoming Calculemus meeting, which will be held jointly with AISC 2008 and MKM 2008 (confederated in the Conferences on Intelligent Computer Mathematics, CICM 2008) in Birmingham, UK, we seek original research papers on the subjects described above.

Scope
The scope of Calculemus covers all aspects of the interplay of mechanised reasoning and computer algebra, including cross-fertilisation between those two research areas, as well as the development of integrated systems that transcend both computer algebra and theorem proving. Potential areas of interest are:

- Theorem proving in computer algebra (CAS)
- Computer algebra in theorem proving (PA and ATP)
- Case studies and applications that both involve computer algebra and mechanised reasoning
- Representation of mathematics in computer algebra
- Theory, design and implementation of interdisciplinary systems for computer mathematics
- Infrastructure for mathematical services
- Theory exploration techniques

Keynote Speakers
Annie Cuyt (Universiteit Antwerpen)  Thierry Coquand (Goteborg University)

Important Dates
March 07, 2008: Submission deadline
April 11, 2008: Notification of acceptance
April 25, 2008: Camera ready copies due
July 30, 2008: Calculemus 2008 starts in Birmingham, UK

Submission
Please submit your full paper of at most 15 pages prepared with the standard LNCS class style as pdf or ps file via http://www.easychair.org/conferences/?conf=Calculemus2008
on or before March 7, 2008. Detailed formatting instructions will be available at the Calculemus website.

Proceedings
Accepted papers will be published in the LNAI series of Springer.
Differential Algebra and Related Computer Algebra
University of Catania, March 26–29, 2008
An International Conference in Memory of Giuseppa Carrà-Ferro

Communicated by William Sit wyscc@sci.ccny.cuny.edu

Announcement

In agreement with the Department of Mathematics and Computer Science of the University of Catania, we are organizing an international conference on Differential Algebra and Related Computer Algebra in memory of Giuseppa Carrà-Ferro, to be held in Catania, Italy on March 26–29, 2008.

Giuseppa Carrà-Ferro (1952–2007), affectionately known as Pina in close circles, died of cancer on March 22, 2007. Professor Carrà-Ferro is remembered for her contributions to Differential Algebra (differential spectrum and varieties, Kolchin schemes, differential Gröbner bases, differential dimension and multiplicity, automated theorem-proving in differential geometry, differential rankings, characteristic sets, and differential resultants) and to Computer Algebra (super G-bases, involutive division, and graph algorithms).

The major focus of the conference will be Differential Algebra, its computational aspects, and its applications. Topics include, but are not limited to, differential and difference algebra, differential and difference Galois theory, differential algebraic geometry, differential algebraic groups, differential dimension theory and invariants, related model theory, computational differential algebra, dynamical systems, integrability theories, and applications. In addition, the conference will also be open to other topics that are related to the research interest of Carrà-Ferro (see the conference website http://www.dmi.unict.it/carrasymposium). The conference will be structured to include up to 8 invited 40-minute plenary talks and a number of shorter talks of 25 minutes each on state of the art research results. As of this announcement, the following have accepted our invitation for plenary talks:

François Boulier, Université Lille I, France
Xiao-Shan Gao, Chinese Academy of Sciences, China
Evelyne Hubert, INRIA, France
Alexander Levin, Catholic University of America, U. S. A.
Bud Mishra, Courant Institute, New York University, U. S. A.
Michael Singer, North Carolina State University, U. S. A.
Volker Weispfenning, Universität Passau, Germany

Subject to scheduling limitations, the short talks are open to the research community. Interested speakers are required to submit a brief abstract (limited to 2 pages) to the Program Committee (via the website above) no later than November 30, 2007. Acceptance to the short talks will be announced by January 5, 2008. Please visit website for more information.

The abstracts of the invited lectures and other contributions will appear in a special issue of Le Matematiche and will be distributed at the conference.

Program Committee

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jacques Calmet</td>
<td><a href="mailto:calmet@ira.uka.de">calmet@ira.uka.de</a></td>
</tr>
<tr>
<td>Giovanni Gallo</td>
<td><a href="mailto:gallo@DMI.Unict.it">gallo@DMI.Unict.it</a></td>
</tr>
<tr>
<td>Vladimir Gerdt (co-chair)</td>
<td><a href="mailto:gerdt@jinr.ru">gerdt@jinr.ru</a></td>
</tr>
<tr>
<td>Julia Hartmann</td>
<td><a href="mailto:Julia.Hartmann@wr.uni-heidelberg.de">Julia.Hartmann@wr.uni-heidelberg.de</a></td>
</tr>
<tr>
<td>Elizabeth Mansfield</td>
<td><a href="mailto:E.L.Mansfield@kent.ac.uk">E.L.Mansfield@kent.ac.uk</a></td>
</tr>
<tr>
<td>Teo Mora (co-chair)</td>
<td><a href="mailto:theomora@disi.unige.it">theomora@disi.unige.it</a></td>
</tr>
<tr>
<td>François Ollivier</td>
<td><a href="mailto:ollivier@lix.polytechnique.fr">ollivier@lix.polytechnique.fr</a></td>
</tr>
<tr>
<td>Fritz Schwarz</td>
<td><a href="mailto:fritz.schwarz@scai.fraunhofer.de">fritz.schwarz@scai.fraunhofer.de</a></td>
</tr>
<tr>
<td>William Sit (co-chair)</td>
<td><a href="mailto:wyscc@sci.ccny.cuny.edu">wyscc@sci.ccny.cuny.edu</a></td>
</tr>
</tbody>
</table>
Sixth International Workshop on Computer Algebra Systems and Their Applications (CASA 2008)
University of Perugia, Perugia, Italy
June 30 – July 3, 2008

Communicated by Andres Iglesias, iglesias@unican.es

Computer Algebra (also known as Symbolic Computation or Computational Algebra) has found applications in many domains of science such as mathematics, physics, chemistry, engineering, computer science, computational biology, education, etc. The computer algebra systems (CAS) such as Mathematica, Maple, MuPAD, Reduce, Axiom, Lie, Matlab, Scilab, CoCoa, MuMATH, Derive, Pari-GP, SMP, MathCAD, Macsyma, Scratchpad, Magma, Singular, SARAG, Risa/Asir, GAP (and many others that have been developed so far) are becoming more and more popular and now they are valuable tools for teaching, research and industry. This workshop solicits high-quality papers for presentation describing original research results in Computer Algebra Systems and their Applications.

All accepted papers will be published by IEEE Computer Society Press. In addition, the accepted papers will be scheduled for oral presentation. Submission implies the willingness of at least one of the authors to register and present the paper.

The workshop is a part of ICCSA’08, the 2008 International Conference on Computational Science and Applications to be held at the University of Perugia, Perugia (Italy).

International Program Committee
This is the tentative list of Program Committee members of this workshop (still in progress): Bruno Autin (Switzerland), Algimantas Cepulkauskas (Lithuania), Mistushi Fujimoto (Japan), Akemi Galvez (co-chair, Spain), Tetsuo Ida (Japan), Andres Iglesias (chair, Spain), Mariusz Jankowski (USA), Chikara Miyaji (Japan), Alfred G. Noel (USA), Yes Papegay (France), Tomás Recio (Spain), Eugenio Roanes-Lozano (Spain), Haiduke Sarafian (USA), Tadashi Takahashi (Japan), Unal Ufuktepe (Turkey), Ryszard A. Walentynski (Poland), Hitoshi Yanami (Japan), Ali Yazici (Turkey)

Topics
This workshop is intended to cover recent developments (algorithms, programs, packages, extensions, new tools, etc.) for computer algebra systems (CAS). Emphasis will be placed upon the applications of these systems for solving problems in science and engineering. Thus, we accept papers describing research on actual or possible applications of CAS and techniques to other fields (Mathematics, Physics, Chemistry, Engineering, Computer Science, Education, Industry, etc.).

A very remarkable feature of CAS is their capability to handle symbolic, numerical and graphical tasks within a uniform framework. Papers exploring the interaction of these CAS symbolic, numerical and graphical tools to solve complex problems as well as papers describing strategies to combine CAS with other programs and/or packages are also welcomed.

Finally, an exciting new feature of many CAS is the possibility to perform calculations by using remote kernels connected via Internet. Papers discussing the use of this new technology will also be considered.

Important Dates
• January 27, 2008: Draft papers due
• March 31, 2008: Notification of Acceptance
• April 15, 2008: Camera Ready Papers and Pre-registration
• June 30- July 3, 2008: ICCSA 2008 conference, Perugia (Italy)

Submission Of Papers
For paper submission, please refer to the URL:
http://personales.unican.es/iglesias/CASA2008/submission.htm
and follow the instructions indicated there.
Call For Papers: Milestones in Computer Algebra (MICA 2008)
A Conference in Honour of Keith Geddes’ 60th Birthday
Stonehaven Bay, Trinidad and Tobago, May 1–3, 2008

Communicated by Mark Giesbrecht

Keith Geddes’ research has spanned the areas of numerical approximation, algebraic algorithms for symbolic computation, hybrid symbolic-numeric computation and the design and implementation of computer algebra systems. He is perhaps best known as co-founder of the Maple computer algebra system. Through his teaching, research and software, the work of Keith Geddes has touched millions of individuals. In honour of Keith Geddes’ 60th birthday, the 40th year of his scientific career and the 20th anniversary of the founding of Maplesoft, a conference will be held May 1–3, 2008 near Scarborough, Tobago.

The conference will feature invited talks by well known figures in the computer algebra world as well as contributed talks selected by the program committee. The following invited speakers have confirmed their participation:

- Jim Cooper (Maplesoft, Canada)
- Gaston Gonnet (ETH Zurich, Switzerland)
- Michael Monagan (Simon Fraser U., Canada)
- Joel Moses (MIT, USA)
- Peter Paule (RISC Linz, Austria)
- B. David Saunders (U. Delaware, USA)
- David Stoutemyer (Texas Instruments, USA)
- Jan Verschelde (U. Illinois at Chicago, USA)

Call for Papers. Contributions of original research in areas related to Keith Geddes’ career or of related historical interest are invited. Extended abstracts of 4–5 pages should be submitted by February 22, 2008. Please see the website for details. A special issue of the Journal of Symbolic Computation is approved to follow the conference, with a submission deadline of September 1, 2008.

Topics. Topics include, but are not limited to: algebraic algorithms for symbolic computation, hybrid symbolic-numeric computation, numerical approximation, symbolic summation and integration, and the design of symbolic computation libraries and systems.

Important Dates

Program Committee
- Jacques Carette (McMaster U., Canada)
- Robert Corless (U. Western Ontario, Canada)
- James Davenport (U. Bath, UK)
- Jürgen Gerhard (Maplesoft, Canada)
- Mark Giesbrecht, Chair (U. Waterloo, Canada)
- Laureano Gonzalez Vega (U. Cantabria, Spain)
- Hoon Hong (North Carolina State U., USA)
- Erich Kaltofen (North Carolina State U., USA)
- George Labahn (U. Waterloo, Canada)
- Ziming Li (AMSS Academia Sinica, China)

Organizing Committee
- General Chair: Stephen Watt (U. Western Ontario)
- Program Chair: Mark Giesbrecht (U. Waterloo)
- Sponsorship Chair: George Labahn (U. Waterloo)
- Publicity Chair: Ilias Kotsireas (Wilfrid Laurier U.)
- Treasurer: Jim Cooper (Maplesoft)
- Local Arrangements: Bal Swarooop Bhatt
- (U. West Indies, Trinidad & Tobago), and David Jeffrey (U. Western Ontario)

Venue. The conference will be held at the Grafton Beach Resort, located about 8km from Scarborough, the capital of Tobago, and about 8km from the Crown Point international airport.

Sponsorship. The conference is sponsored by the University of Waterloo, and in cooperation with ACM SIGSAM. Support is gratefully acknowledged from Maplesoft, the Ontario Research Centre for Computer Algebra, the University of Waterloo, the University of Western Ontario, the University of the West Indies.

Notice: All aspects of the conference are subject to change without notice. This includes, but is not limited to, dates, locations and speakers.

136
NumAn 2008, Conference in Numerical Analysis
Recent Approaches To Numerical Analysis: Theory, Methods and Applications
Honoring Richard S. Varga on his 80th birthday
September 1-5, 2008, Kalamata, Greece
Communicated by Ilias S. Kotsireas

NumAn provides an opportunity to learn of new developments and to present original research results in all areas of Numerical Analysis such as Theory, Methods and Applications. The program of NumAn 2008 will include invited presentations, contributed research papers and posters, covering theory, methods and applications of Numerical Analysis.

**Proceedings:** Papers presented at the conference may be submitted for publication in a Special Issue of the journal *Applied Numerical Mathematics* published by Elsevier. Details for paper submission to this special issue will be announced at the conference.

**Invited Speakers:**
- Richard S. Varga (USA)
- Claude Brezinski (France)
- Ronald Cools (Belgium)
- Michel Crouzeix (France)
- Vassilios A. Dougalis (Greece)
- Michael Eiermann (Germany)
- Elias Houstis (Greece)
- Volker Mehrmann (Germany)
- Nick Papamichael (Cyprus)
- Panos Pardalos (USA)
- Lothar Reichel (USA)
- Youcef Saad (USA)
- Hans J. Stetter (Austria)
- Daniel B. Szyld (USA)
- Paul Van Dooren (Belgium)

**Important Dates:** Submission of abstracts: (15/03/2008), Notification of acceptance: (15/04/2008)

**Conference contact e-mail:** numan2008@math.upatras.gr

**Organizing Committee:**
G. Akrivis (Ioannina), E. Gallopoulos (Patras), A. Hadjidimos (Volos), I.S. Kotsireas (Waterloo), D. Noutsos (Ioannina), M.N. Vrahatis (Patras).
SCC 2008
First International Conference on Symbolic Computation and Cryptography
http://www.cc4cm.org/scc2008
April 28-30, 2008, Beijing, China,
Communicated by Ilias S. Kotsireas

SCC 2008 is the first of a new series of conferences where research and development in symbolic computation and cryptography may be presented and discussed. It is organized in response to the growing interest in applying and developing methods, techniques, and software tools of symbolic computation for cryptography. The use of lattice reduction algorithms in cryptology and the application of Groebner bases in the context of algebraic attacks are typical examples of explored applications.

INVITED SPEAKERS
• Bruno Buchberger (Johannes Kepler Universitaet Linz, Austria)
• Arjen K. Lenstra (Ecole Polytechnique Federale de Lausanne, Switzerland) (to be confirmed)
• Adi Shamir (Weizmann Institute of Science, Israel)
• Xiaoyun Wang (Tsinghua University and Shandong University, China)

SUBMISSION
Potential participants of SCC 2008 are invited to submit extended abstracts of 3-5 pages or full papers describing their work to be presented at the conference. The submitted extended abstracts and full papers will be reviewed by members of the program committee (PC) for soundness and relevance to the conference. Submission of original research papers is encouraged, while published material and work in progress will also be considered for presentation at the conference. For more information see the conference webpage or e-mail scc2008@cc4cm.org

PUBLICATION
Authors of the extended abstracts and full papers accepted for presentation at the conference will be invited to submit their full and/or revised papers for publication in special issues of Mathematics in Computer Science (MCS - http://www.cc4cm.org/mcs) by Birkhauser/Springer after the meeting. The submitted papers will be formally reviewed by PC members and external referees according to the standard refereeing procedure of MCS.

IMPORTANT DATES

GENERAL CHAIR
Zhiming Zheng (China)

PROGRAM COMMITTEE
Anne Canteaut (France), Jintai Ding (USA), Jean-Charles Faugere, Co-chair (France), Joachim von zur Gathen (Germany), Pierrick Gaudry (France), Jaime Gutierrez (Spain), Hoon Hong (USA), Antoine Joux (France), Martin Kreuzer (Germany), Dongdai Lin (China), Zhuojun Liu (China), Alexander May (Germany), Ludovic Perret (France), Igor Shparlinski (Australia), Rainer Steinwandt (USA), Boaz Tsaban (Israel), Dongming Wang, Co-chair (China/France).

LOCAL ARRANGEMENTS
Shangzhi Li, Chair (China), Jinxi Ma (China), Chenqi Mou (China)
RISC-Linz, a research institute at the Johannes Kepler University, Austria, offers opportunities to researchers to obtain access to its infrastructure and facilities. Access is provided through the project SCIEnce (http://www.symbolic-computation.org) within the 6th Framework Programme of the European Commission.

What we offer.
Within this programme the users can:
- visit RISC-Linz for several weeks, work with and get an advice from the members of the institute on applications of symbolic computation in users work;
- get remote access to the the computing infrastructure and facilities of the institute.

Applications can be submitted any time. For successful applicants, access is free of charge. We provide scientific, technical, administrative, and logistic support, including travel and living expenses.

Who can benefit.
Students and researchers who are interested in using symbolic computation in their work.

For more information and the application procedure please visit the program web page at http://www.risc.uni-linz.ac.at/projects/science/access.
2008 Call for Nominations
ACM SIGSAM
Richard D. Jenks Memorial Prize
for
Excellence in Computer Algebra Software Engineering

Communicated by Mark Giesbrecht, Chair ACM SIGSAM

The third ACM SIGSAM Richard D. Jenks Memorial Prize for excellence in software engineering for computer algebra will be awarded at International Symposium on Symbolic and Algebraic Computation (ISSAC 2008) at RISC Linz, Austria, in July, 2008. The prize will consist of a plaque and a cash award of $1,000.

Nominations, including self nominations, for this prize are hereby solicited. Each nomination should be accompanied by a carefully completed nomination form. Candidates (or their nominators) should arrange to have two to five confidential letters of recommendation submitted by persons who are familiar with the nominee’s software engineering achievements in computer algebra. The letters are an especially important part of the nomination packet. We welcome re-nominations of previously nominated candidates into the current competition.

Please see http://www.sigsam.org/awards/Jenks for more details.

Previous winners have been the SINGULAR team at the University of Kaiserslautern (2004) and Prof. John J. Cannon of The University of Sydney (2006).

Software engineering will be interpreted broadly, but it should be an important component in the work of any nominee. The nominee can be an individual or a team, when the latter is appropriate. Any questions about the suitability of a given body of work for the prize should be directed to a member of the prize committee as listed below.

All nominations must be received by May 1, 2008.

The prize winner will be selected by a committee consisting of the following individuals:

- Barry Trager (co-chair), IBM Research. Email: bmt@watson.ibm.com
- Tony Hearn (co-chair), Rand Corporation. Email: hearn@rand.org
- Mark Giesbrecht, ACM SIGSAM Chair, University of Waterloo. Email: mwg@uwaterloo.ca
- David Musser, Rensselaer Polytechnic Inst. Email: musser@cs.RPI.edu
- Mike Dewar, Numerical Algorithms Group. Email: miked@nag.co.uk

All nominations and supporting papers should be sent by email to jenksprize@sigsam.org by May 1, 2008.