Comparison of Polynomial-Oriented Computer Algebra Systems

(Preliminary Report)

Robert H. Lewis and Michael Wester

Exact symbolic computation with polynomials and matrices over polynomial rings has wide applicability to many fields ([Her96], [LeN98]). By "exact symbolic" we mean computation with polynomials whose coefficients are integers (of any size), rational numbers, or finite fields, as opposed to coefficients that are "floats" of a certain precision. Such computation is part of most computer algebra systems ("CA systems"). Over the last dozen years several large CA systems have become widely available, such as Axiom, Derive, Macsyma, Maple, Mathematica, and Reduce. They tend to have great breadth, be produced by profit-making companies, and be relatively expensive. However, most if not all of these systems have difficulty computing with the polynomials and matrices that arise in actual research. Real problems tend to produce large polynomials and large matrices that the general CA systems cannot handle ([LeN98]).

In the last few years several smaller CA systems focused on polynomials have been produced at universities by individual researchers or small teams. They run on Macs, PCs, and workstations. They are freeware or shareware. Several claim to be much more efficient than the large systems at exact polynomial computations. The list of these systems includes CoCoA, Fermat, MuPAD, Pari-GP, and Singular ([CoC], [Fer], [MuP], [Par], [Sin]).

In this paper we compare these small systems to each other and to one of the large systems (Maple) on a set of problems involving exact symbolic computation with polynomials and matrices. The problems here involve:

- the ground rings Z, Q, Z/p, other finite fields
- basic arithmetic of polynomials over the ground ring
- basic arithmetic of rational functions over the ground ring
- polynomial evaluation (substitution)
- matrix normal forms
- determinant, characteristic polynomial
- gcd of multivariate polynomials
- resultants

In the near future we will add Gröbner bases and factorization of polynomials.

Table 1: Macintosh PPC, 233 Mhz 604e, 240 meg RAM. All times are in seconds unless otherwise noted.

Benchmark		**CoCoA**	**Fermat**	**Maple**	**MuPAD**	**Pari-Gp**	**Singular**
A:	divide factorials	5.8	1.50	10.00	56.82	3.766	48.0
A′:	$\sum_{i=1}^{1000} 1/i$	0.83	0.150	0.200	0.583	0.083	2.7
B:	gcd(big integers)	29.0	11.33	13.0	18.12	5.20	9.2
C:	$\sum_{i=1}^{10} iyt^i/(y+i\ t)^i$	452.0	0.076	0.466	1.367	CR, 17 mins	NA
D:	$\sum_{i=1}^{10} iyt^i/(y+\|5-i\|\ t)^i$	48.0	0.400	1.0	6.28	0.833	NA
F:	gcd(2-var polys)	2.5	0.050	0.083	2.2	0.200	0.60
G:	gcd(3-var polys)	27.5	1.18	9.9	14.72	KD, 60 mins	814.0
G_p:	G mod 181	7.5	0.367	12.0	13.02	KD, 60 mins	55.0
H:	det(rank 80 Hilbert)	KD, 50 mins	22.8	189.0	219.2	9.33	CR, 30 mins
I:	invert rank 40 Hilbert	5.83	3.38	32.0	45.3	1.73	NA
J:	check rank 40 Hilbert	4.17	1.63	11.0	11.93	0.700	UN
K:	invert rank 70 Hilbert	36.7	41.9	392.0	393.9	15.20	NA
L:	check rank 70 Hilbert	23.3	14.5	165.0	76.9	4.95	UN
M_1:	rank 26 sparse, det	KD, 60 mins	0.038	1.2	4.4	0.038	KD, 120 min
M_2:	rank 101 sparse, det	UN	478.0	GU, 66 mins	CR, 270.0	CR, 16.0	UN
N:	eval poly at rationals	NA	44.4	GU, 50.0	KD, 95 mins	KD, 150 mins	NA
O_1:	three dets (average)	1965.0	37.8	GU, 175.0	KD, 101 mins	KD, 60 mins	CR, 52.0
O_2:	two gcds	CR, 120 mins	281.8	UN	UN	UN	UN
P:	det(rank 101)	0.64	0.183	51.0	232.7	0.250	1.62
P_p:	P mod 181	0.64	0.267	15.0	998.2	0.483	0.430
P′:	det(less sparse rank 101)	0.67	0.32			3.87	5.47
P'_p:	P′ mod 181	0.67	0.422			1.30	0.57
Q:	charpoly(P)	KD, 60 mins	3.52	KD, 60 mins	3052.0	0.450	CR, 480.0
Q_p:	Q mod 181	KD, 50 mins	1.78	181.0	144.3	0.433	CR, 480.0
Q′:	charpoly(P′)	UN	44.1			331.0	UN
Q'_p:	Q′ mod 181	UN	13.5			540.0	UN
S:	Hermite form, rank 20	NA	1.75	56.0	71.13	0.383	NA
T:	Hermite form, sparse	NA	1.13	KD, 90 mins	KD, 60 mins	0.583	NA
U:	Smith form, rank 20	NA	0.250	3.00	NA	0.150	NA
V:	Smith form, rank 60	NA	32.8	323.0	NA	15.23	NA
W_1:	Smith form, rank 101	NA	0.150	87.0	NA	3.35	NA
W_2:	Smith form rank 401	NA	15.8	KD, 100 mins	NA	238.0	NA
X:	gcd, finite field	NA	0.917	BG, 519.0	KD, 480 mins	BG, 16 mins	620.0
Y:	det, finite field	NA	0.025	KD, 30 mins	10.90	0.038	899.0

Abbreviations:

BG (bug encountered)	The program hit a bug, stopped, and gave a useless error message.
CR (crashed)	The program or machine crashed.
GU (gave up)	The program gave up on the problem, but did not crash.
KD (killed)	We gave up and stopped the program after a long amount of time (given).
NA (not available)	The command or facility is not available in the system.
UN (unable)	We could not do this test because a prerequisite test failed, or a simpler one of the same kind failed.
VM (virtual memory)	The machine had only 64 Mb of RAM. Virtual memory kicked in, resulting in disk thrashing and a big slow down.
<blank>	Sorry, we didn't get it done in time!

Notes:

• Maple is of course not a small system of this type. It is here for comparison.

• Some systems have several ways to compute determinant, characteristic polynomial, Smith form, or Hermite form. We made an effort to try all the methods that were documented, and then reported the fastest time.

• Choice of Systems: We chose only programs that are complete systems and do not require any money up front. We also wanted systems that seemed to have recent versions.

Details:

A: For $i = 1$ thru 100 do $(1000 + i)!/(900 + i)!$

B: Let $x = 13 \cdot 17 \cdot 31$ and $y = 13 \cdot 19 \cdot 29$. Then for $i = 1$ thru 200 do $\gcd(x^{300+(i \mod 181)}, y^{200+(i \mod 183)})$.

D: $\displaystyle\sum_{i=1}^{10} \frac{i\ y\ t^i}{(y + |5 - i|\ t)^i}$. This way, there are common denominators.

F: $p = (x^2 - 3xy + y^2)^4(3x - 7y + 2)^5$ and $q = (x^2 - 3xy + y^2)^3(3x - 7y - 2)^6$. Compute $\gcd(p, q)$.

G, G_p:
$p = (7yx^2z^2 - 3xyz + 11(x + 1)y^2 + 5z + 1)^4(3x - 7y + 2z - 3)^5$ and
$q = (7yx^2z^2 - 3xyz + 11(x + 1)y^2 + 5z + 1)^3(3x - 7y + 2z + 3)^6$
Compute $\gcd(p, q)$ and $\gcd(p \bmod 181, q \bmod 181)$.

H-L: Hilbert matrices, $h_{ij} = 1/(i + j - 1)$. J and L are to check that the inverse times the matrix is the identity.

M_1, M_2: The matrices are created according to a certain pattern that comes up in graph theory. The n-case is a sparse $(n^2+1) \times (n^2+1)$ matrix containing n symbolic variables. M_1 takes the determinant of the 5-case, i.e., a 26×26 sparse matrix. The answer has 101 terms. M_2 is likewise for the 10-case, i.e., a 101×101 sparse matrix with 10 variables. The answer has about 85000 terms.

N: The problem arises in image analysis. *res* is a 156 term polynomial in 14 symbolic variables, including $q_1, \ldots, q_4$. The test is to evaluate *res* at $q_i = s_i,\ i = 1, \ldots, 4$, where each s_i is a rational function in the variables of roughly 50 terms. The result should be 0.

O_1 and O_2: In van der Waerden's classic "Modern Algebra", there is a chapter on resultants. One example involves three homogeneous polynomials f, g, and h of degree two in three variables. Each polynomial has six coefficients that are independent parameters, for a total of 18 parameters. These parameters are placed in three sparse 15×15 matrices d_1, d_2, and d_3. The resultant of f, g, and h is $\gcd(\det(d_1), \det(d_2), \det(d_3))$.

O_1 is the three determinants, and O_2 is their gcd. The answer has about 34000 terms.

P – Q′: Take the rank 101 matrix in M_2 and replace the variables with small positive integers. This yields a sparse integer matrix where the nonzero entries lie on 10 diagonals. P is to take its determinant, P_p its determinant mod 181. Q and Q_p compute its characteristic polynomial. Next, duplicate each diagonal, yielding a less sparse matrix with 20 diagonals. P′, P'_p, etc. are analagous.

S, T: Hermite form (integers). S is of a certain random dense rank 20 matrix of integers. T is the Hermite form of the matrix from P.

U – W_2: Smith forms (integer). U is of the same matrix as S. V is a dense rank 60 matrix with an interesting Smith form. W_1 is the matrix from P. W_2 is the 20-case of the pattern from M_1 with integers again substituted for the variables (a 401×401 matrix).

X and Y: The point is to work over finite fields. In MuPAD notation:

```
G := Dom::GaloisField(17027, 2, poly(t^2+1, [t], IntMod(17027))):
p := poly((7*t*y*x^2*z^2 - 3*t + t*x*y*z + 11*(x + 1 + t)*y^2 + 5*z + t + 1)^4*
          (3*t*x - 7*t*y + 2*z - 3*t + 1)^5, [x,y,z], G):
q := poly((7*t*y*x^2*z^2 - 3*t + t*x*y*z + 11*(x + 1 + t)*y^2 + 5*z + t + 1)^3*
          (3*t*x - 7*t*y + 2*z + 3*t - 1)^6, [x,y,z], G):
```

X is to find gcd(p, q) (after p and q are fully expanded of course).

Y is to modify the 26×26 example of M_1. We replace the 5 variables in that test with t, x, y, z, making t subject to $t^2 + 1 = 0$ and working mod 17027. Compute the determinant of this matrix.

Benchmark		CoCoA	Fermat	Maple	MuPAD	Pari-Gp	Singular
A:	divide factorials	1.0	2.33		1.38	1.87	24.0
A′:	$\sum_{i=1}^{1000} 1/i$	0.130	0.142		0.120	0.060	0.13
B:	gcd(big integers)	21.7	16.25		3.50	3.840	0.62
C:	$\sum_{i=1}^{10} iyt^i/(y+it)^i$	250.0	0.032		1.35	0.280	NA
D:	variant of C	28.0	0.226		0.777	0.110	NA
F:	gcd(2-var polys)	1.3	0.033		0.337	0.660	5.2
G:	gcd(3-var polys)	19.0	1.13		3.59	KD, 45 mins	156.0
G_p:	G mod 181	1.6	0.730		3.91	KD, 60 mins	17.5
H:	det(rank 80 Hilbert)	KD, 45 mins	23.21		49.0	6.49	CR, 2 mins
I:	invert rank 40 Hilbert	4.0	3.82		15.2	1.49	NA
J:	check rank 40 Hilbert	3.0	2.12		5.49	0.880	NA
K:	invert rank 70 Hilbert	24.0	49.46		82.6	9.83	NA
L:	check rank 70 Hilbert	15.0	18.6		17.2	3.07	NA
M_1:	rank 26 sparse, det	KD, 45 mins	0.025		2.88	0.170	CR, 27 mins
M_2:	rank 101 sparse, det	UN	KDVM, 15 mins		KDVM, 15 mins	CRVM, 3 mins	UN
N:	eval poly at rationals	KDVM, 40 mins	20.0		KDVM, 20 mins	KD, 40 mins	NA
O_1:	three dets (average)	500.0	VM, 168.1		KDVM, 30 mins	KDVM, 25 mins	KDVM, 25 m
O_2:	two gcds	693.0	VM, 263.0		UN	UN	UN
P:	det(rank 101)	0.46	0.42		35.8	0.850	1.05
P_p:	P mod 181	0.50	0.550		291.2	0.220	0.16
P′:	det(less sparse rank 101)	0.50	0.85		36.2	1.10	1.65
P'_p:	P′ mod 181	0.550	0.630		293.4	1.87	0.21
Q:	charpoly(P)	KD, 40 mins	2.43		663.9	0.720	KDVM, 30 m
Q_p:	Q mod 181	KD, 50 mins	1.35		44.23	0.660	1840.0
Q′:	charpoly(P′)	UN	16.6		121.6	113.2	UN
Q'_p:	Q′ mod 181	UN	1.80		508.6	210.0	KDVM, 30 m
S:	Hermite form, rank 20	NA	2.37		21.68	0.610	NA
T:	Hermite form, sparse	NA	1.09		576.0	2.30	NA
U:	Smith form, rank 20	NA	0.254		NA	0.600	NA
V:	Smith form, rank 60	NA	36.7		NA	KD, 30 mins	NA
W_1:	Smith form, rank 101	NA	0.500		NA	1.81	NA
W_2:	Smith form, rank 401	NA	11.9		NA	110.2	NA
X:	gcd, finite field	NA	0.961		KD, 40 mins	KD, 40 mins	KD, 60 mins
Y:	det, finite field	NA	0.014		3.65	0.220	284.0

Versions of the Software Used in These Tests:

CoCoA 3.7
Fermat 2.4.5
Maple V, R4
MuPAD 1.4
Pari-Gp 2.0.12 alpha

Feedback and Future Work:

- Tests with Gröbner bases and factorization of polynomials.

- Other platforms, especially Sun workstations.

- The actual code used in the tests will be posted in a few weeks to the URL http://www.fordham.edu/lewis/cacomp.html. If you try the tests and get noticeably different results, please let us know.

Prof. Robert H. Lewis
Department of Mathematics
Fordham University
Bronx NY 10458
rlewis@murray.fordham.edu

Michael Wester
Cotopaxi
1801 Quincy, SE
Albuquerque, New Mexico 87108
wester@math.unm.edu

References

[CoC] CoCoA, anonymous FTP at ftp.dm.unipi.it:/pub/alpi-cocoa/cocoa.

[Fer] Fermat, http://www.bway.net/~lewis/.

[Her96] Willy Hereman, "Computer algebra: lightening the load", Physics World, Volume 9, Number 3, March 1996, 47-52.

[LeN98] Robert H. Lewis and George Nakos, "Solving the Six-Line Problem with the Dixon Resultant", in "High Performance Symbolic Computation and Challenges of Computer Algebra", 1998 IMACS ACA Conference, Prague.

[MuP] MuPAD, anonymous FTP at athene.uni-paderborn.de:unix/MuPAD.

[Par] Pari-Gp, anonymous FTP at ftp://megrez.math.u-bordeaux.fr/pub/pari.

[Sin] Singular, http://www.mathematik.uni-kl.de/~zca/Singular/Welcome.html.

[Wes94] Michael Wester, "A Review of CAS Mathematical Capabilities", Computer Algebra Nederland Nieuwsbrief, Number 13, December 1994, ISSN 1380-1260, 41-48.