An algebraic approach to primality proving

In Section 1, I give a rather simple theorem that enables rapid primality proving for numbers of the form $n = kb^3+b+1$ with factorization fractions $f = \log(b)/\log(n-1)$ as small as $f = 2/7 \approx 28.57\%$. Section 2 comments on this theorem. In Section 3, I indicate how computer algebra was used to generate 11 polynomials that enable proofs below 26% for primes of the form $n = kb^{50}+b^{13}+1$. After performing the usual Pocklington tests to prove that every divisor of n is congruent to 1 modulo b^{13}, the extra cost is negligible, since it is merely linear in $\log(n)$, assuming FFT multiplication. At 10,000 decimal digits, the proofs are typically 1,000 times faster than would be achieved by numerical use of a Lenstra–Lenstra–Lovász (LLL) method. The certificates are typically 1,000 times smaller, since they contain algebraic formulas that replace the huge numerical expressions required for a certificate obtained with LLL. Section 4 indicates the systematic methods by which I constructed these polynomials and how they may be applied to primes of the special form $n = kb^{4c-2} + b^c + 1$, to get even closer to the 25% limit. Section 5 contains a summary and suggestions for future work.

1 A theorem at 28.57% factorization

Let $n = kb^3 + b + 1$, with integers $k > 0$ and $b > 3k^2$. Suppose that for each prime $q|b$ we find an integer a with $a^{n-1} \equiv 1 \pmod{n}$ and $\gcd(a^{(n-1)/q} - 1, n) = 1$.

Theorem (Broadhurst, 28.57%). With the above conditions, n is prime if and only if $(b+1)^2 - 4(kb-1)$ is not a square and $P(x) = k + x^2 + x^3$ has no integer root.

Proof. If $(b+1)^2 - 4(kb-1) = s^2$, for integer s, then $4n = (b^2+b+2)^2 - (sb)^2$ and n is composite. If $P(-r) = 0$, for integer r, then $n = (rb+1)(b(rb-1)(r-1)+1)$ is composite. Thus each of the two conditions is necessary. Now we show that they are sufficient to prove that n is prime. By Pocklington's theorem we know that every divisor of n is congruent to 1 modulo b. Thus there exists a pair of integers, y and z, such that $n = (yb+1)(zb+1)$ and $m \geq y \geq z \geq 0$, where $m = (n-1)/b$. If n is prime, then $z = 0$ and $y = m$. Since $yzb+y+z = m = kb^2+1$, there exists an integer $t > 0$ such that $y + z = tb + 1$ and $yz = kb - t$. Hence $(tb+1)^2 - 4(kb-t) = (y-z)^2$ is a square. Since it is not a square for $t = 1$, we have $t \geq 2$, $y > b$ and $z < k$. Let $d = zb + 1$ be any divisor of n with $0 \leq z < k$. Then d

divides both $P(-m) = -kn(n-2)$ and $m - z = (n-d)/b$. Hence $d|P(-z)$. Assume that $P(x)$ has no integer root. Then $|P(-z)/d|$ is a positive integer and hence $(zb)^2 < d^2 \le |P(-z)|^2 \le 3(k^2 + z^4 + z^6)$. Defining $Q(x) = 3(k^2 + x^4 + x^6) - (xb)^2$, we conclude that $Q(z) > 0$. However, $Q(k) \le 9k^6 - k^2b^2 < 0$, since $b > 3k^2$, and $Q(1) = 3(k^2 + 2) - b^2 < b + 6 - b^2 = (3-b)(2+b) < 0$, since $b > 3$. Thus $Q(x)$ has a zero for $0 < x < 1$ and a zero for $x > k$. By Descartes' rule of signs [*La Géométrie*, 1637], it can have no other zero at positive x. Hence there is no integer z with $1 \le z < k$ and $Q(z) > 0$. Hence $z = 0$ and n is prime.

2 Comments on the theorem

Since $k < (b/3)^{1/2}$, we may achieve a proof of primality for a factorization fraction $f = \log(b)/\log(n-1)$ arbitrarily close to $f = 1/(3 + \frac{1}{2}) = 2/7 \approx 28.57\%$.

Let $f(c) = c/(4c-2)$. Pocklington's tests prove primality for a fraction $f(1) = 1/2$, the square test of Brillhart, Lehmer and Selfridge (BLS) enables us to reach $f(2) = 2/6 = 1/3$. For primes of a general form, Konyagin and Pomerance showed how to use a cubic, defined by a continued fraction, to reach $f(3) = 3/10$. Here, for primes of a special form, we have already reached $f(4) = 4/14 = 2/7 \approx 28.57\%$, with a much simpler cubic. After the Pocklington tests are completed, we need provide only two small prime witnesses, p and q, showing that $(b+1)^2 - 4(kb-1)$ is not a quadratic residue modulo p and that $P(x)$ is not congruent to 0 modulo q for any integer $x \in [0, q-1]$.

Note that there are many extensions of this method. For example, the form $n = kb^3 + b - 1$ needs two square tests, after the Lucas–Lehmer tests have established that all factors are congruent to ± 1 modulo b. But then the same cubic, $P(x) = k + x^2 + x^3$, will complete the proof that there are no factors of the form $d = zb \pm 1$ with $0 < z < k$.

Another extension is to consider the forms $n = kb^3 + lb \pm 1$, using a cubic polynomial $P(x) = k + lx^2 + x^3$, again for either choice of sign. After the Pocklington and square tests, the proof goes as above, if we demand that $b^2 > 3(1 + k^2l^2 + k^4)$. (The theorem used the condition $b > 3k^2$ in the case $l = 1$.) In any case, it is clear that for large b the operative criterion is $b/k > \max(k, |l|)$, since any small constants are easily absorbed by a few additional square tests. Note that we can achieve a primality proof with a factorization fraction $f = 2/7$ whenever $l^2 < k^2 < b$.

By far the most interesting question, to my mind, is how to progress nearer to 25% than $f(4) = 2/7$ for primes of a special form.

3 Algebraic polynomials to reach 25.99%

Let us pause to consider the three improvements already made on the Coppersmith–Howgrave-Graham (CHG) method. First we used a square test to generate a BLS upper limit for z. This was my suggestion, in late 2004. It makes a significant difference in present work, since the upper limit of n/b^3 on z is noticeably smaller than $n^{1/2}/b$. Secondly, we followed John Renze's recent use of Descartes' rule of signs to replace the less efficient methods originally used in CHG proofs, as will shortly be explained. Finally, we chose a special form for which there was a polynomial whose L_2-norm is far smaller than would be expected from a generic LLL upper bound. Not only did we avoid lattice methods; we also greatly improved on the limits that are expected for more general forms of primes. Together, these three features make for a whole new ball game. This is the first inning.

Already, I have achieved a proof with a factorization fraction slightly below $f(13) = 13/50 = 26\%$, at ten thousand decimal digits, using a form $n = kb^{50} + b^{13} + 1$, by finding a series of efficient polynomials, in closed form, for arbitrary k and b. Here is how it was done.

Suppose that we wish to prove the primality of $n = kb^{4c-2} + b^c + 1$, with $c > 1$. We assume that the Pocklington tests have established that every divisor of n is of the form $d = zb^c + 1$. We may thus write $n = (yb^c + 1)(zb^c + 1)$ with $y \geq z \geq 0$. Our aim is to show that $z = 0$ is the only way of doing this. Since $yzb^c + y + z = kb^{3c-2} + 1$, there exits an integer $t > 0$ such that $y + z = tb^c + 1$ and $yz = kb^{2c-2} - t$. Thus $(tb^c + 1)^2 - 4(kb^{2c-2} - t)$ is a square. We test that this is not a square for $t = 1$ and hence conclude that $t \geq 2$. Thus $y > b^c$ and $z < kb^{c-2}$.

Then (by cunning methods, shortly to be revealed) we find a polynomial $P_{h,u}(x)$ with degree $h - 1$, integer coefficients, $P_{h,u}(0) \neq 0$, and the CHG property that for each $i \in [0, u-1]$ its ith derivative, $P^{(i)}_{h,u}(x)$, satisfies $P^{(i)}_{h,u}(b^{-c})/i! = 0 \bmod n^{u-i}$. Note that b is coprime to n and hence has an inverse modulo any power of n. Note also that $i!$ is cancelled by the ith derviative, $i!\binom{j}{i}x^{j-i}$, of x^j for each term in $P_{h,u}(x) = \sum_j c_j x^j$.

It follows that for every divisor $d = zb^c + 1$ of n we have $d^u | P_{h,u}(-z)$. To prove this, we simply make the Taylor expansion

$$P_{h,u}(-z) = \sum_{i=0}^{h-1}(-z - b^{-c})^i P_{h,u}^{(i)}(b^{-c})/i!$$

and observe that $-z - b^{-c} = -d/b^c$ and that b is coprime to d.

We define $Q_{h,u}(x) = h\sum_j (c_j x^j)^2 - (xb^c)^{2u}$, check that $P_{h,u}(x)$ has no integer root and conclude that $Q_{h,u}(z) > 0$. To prove this, we note that $zb^c < d$, $d^u \le |P_{h,u}(-z)|$ and $|P_{h,u}(-z)|^2 \le h\sum_j (c_j z^j)^2$.

Next we find (if we are able) two real numbers X and Y, with $0 < X < Y$, $Q_{h,u}(X) < 0$ and $Q_{h,u}(Y) < 0$. It follows from Descartes' rule of signs that n has no factor zb^c+1 with $z \in [X, Y]$. This is a significant improvement on earlier CHG methods, which relied on an unnecessarily strong condition, namely $h\sum_j (c_j Y^j)^2 < (Xb^c)^{2u}$, yielding significantly smaller ranges than those covered in this work.

To complete the proof of primality we need a chain of such polynomials to exhaust the range $z \in [1, kb^{c-2}]$ and hence prove that $z = 0$ and n is prime. I shall describe a chain of 11 polynomials that I found for the case $c = 13$ and $b \gg k$, so as to dip below 26%, with no need to know the numerical values of b and k until the algebraic construction is completed and only a few trivial numerical tests remain for any particular primality proof. These polynomials turn out to be special cases of the first 11 polynomials of a master sequence that allow one to progress even closer to the 25% barrier than the target of this section, which is 26%.

For proofs of primes of the form $n = kb^{50} + b^{13} + 1$, I begin, for small z, with

$$P_{4,1}(x) = kb^{11} + x^2 + x^3$$

which obviously has $u = 1$, since $P_{4,1}(b^{-13}) = b^{-39}n$. To each polynomial in the chain, I associate a logarithmic range $\log(z)/\log(b) \in [n_1, n_2]$ in which it is useful for proving the absence of factors, provided that the polynomial has no integer roots and that $b \gg k$. (I shall arrange for these ranges to overlap, so that the neglect of k is benign and is remedied in the proving code.) I indicate the range of a polynomial by the index pair (n_1, n_2). In this case the indices are $I_{4,1} = (-2, 13/2)$, which means that we eliminate factors $zb^{13} + 1$ with z running from 1 to $O(b^{13/2})$. To determine the indices, I study the polynomial $Q_{h,u}(x) = h\sum_j (c_j x^j)^2 - (xb^{13})^{2u}$, where c_j is the coefficient of x^j in $P_{h,u}(x)$, and determine, logarithmically, its two zeros at real positive x, for asymptotic b. Recall that Descartes tells us that there are no more than two such zeros. I have arranged that there shall be precisely two. The easiest way to find them is to assume, in the first instance, that n_1 and n_2 are determined by c_0 and c_{h-1}, respectively, and then to check that the other coefficients of the polynomial do not modify the conclusions. (The skill is to find polynomials which make both of the final checks work.) In this case, with $u = 1$, we have $c_0 = O(b^{11})$ and hence $11 = n_1 + 13$, while $c_3 = O(b^0)$ gives $3n_2 = n_2 + 13$. Clearly $c_2 = 1$ does not modify the conclusion that $I_{4,1} = (-2, 13/2)$.

For the next step, I use

$$P_{6,2}(x) = k^2 b^{37} + k(3b^{13}x - 1)(x + 1) + b^2 x^3 (x + 1)^2$$

with degree $h-1 = 5$ and index $u = 2$, as may be verified by computing $P_{6,2}(b^{-13}) = b^{-63}n^2$ and $P^{(1)}_{6,2}(b^{-13}) = (3b^{-37}+5b^{-50})n$. Writing the weights of the coefficients c_j as the vector $V_{6,2} = [37, 13, 13, 2, 2, 2]$, for $j = 0 \ldots 5$, our first guess for the range comes from solving $37 = 2(n_1 + 13)$ and $5n_2 + 2 = 2(n_2 + 13)$, which suggest that $I_{6,2} = (11/2, 8)$. To verify that this is correct we must add the corresponding multiples of the vector $N_6 = [0, 1, 2, 3, 4, 5]$. For example $V_{6,2} + 8N_6 = [37, 21, 29, 26, 34, 42]$ has its largest component at $j = 5$, as we assumed, to determine $n_2 = 8$, while $2V_{6,2} + 11N_6 = [74, 37, 48, 37, 48, 59]$ has its largest component at $j = 0$, as we assumed, to determine $n_1 = 11/2$. Conveniently, the beginning of the range $I_{6,2} = (11/2, 8)$ overlaps with the end of the previous range $I_{4,1} = (-2, 13/2)$, allowing scope for modest values of k, which was ignored in our logarithmic calculations.

Next comes

$$\begin{aligned} P_{8,3}(x) &= k^3 b^{61} + k^2 b^{37} x(3x + 4) + k b^{26} x^3 (x + 1) + k^2 b^{24}(x - 1) \\ &\quad + k b^{13} x^2 (x + 1)(5x + 3) - k^2 b^{11} + b^2 x^4 (x + 1)^3 - kx(x + 1)(2x + 1) \end{aligned}$$

with index $u = 3$ verified by computing $P_{8,3}(b^{-13}) = b^{-89}n^3$,

$$P^{(1)}_{8,3}(b^{-13}) = \left(4b^{-63} + 7b^{-76}\right) n^2, \quad P^{(2)}_{8,3}(b^{-13})/2 = 3b^{-63} n \left(n + (2b^{13} + 3)(b^{13} + 2)\right).$$

The weight vector $V_{8,3} = [61, 37, 37, 26, 26, 2, 2, 2]$ suggests that $61 = 3(n_1 + 13)$ and $7n_2 + 2 = 3(n_2 + 13)$. Then the checks

$$\begin{aligned} 4V_{8,3} + 37N_8 &= [244, 185, 222, 215, 252, 193, 230, 267], \\ 3V_{8,3} + 22N_8 &= [183, 133, 155, 144, 166, 116, 138, 160], \end{aligned}$$

with $N_8 = [0, 1, 2, 3, 4, 5, 6, 7]$, confirm our first guess that $I_{8,3} = (22/3, 37/4)$. Conveniently, this has an overlap with $I_{6,2} = (11/2, 8)$.

I forbear from printing further polynomials; they will be available in Pari-GP code when the certificate generator is written. Here I characterize the rest of my algebraic path to 25.99% in terms of the ranges covered and the weight vectors that accomplish this covering.

I found a 9th-order polynomial, $P_{10,4}(x)$, proven to have $u = 4$, with

$$V_{10,4} = [87, 63, 63, 52, 39, 28, 28, 4, 4, 4], \quad I_{10,4} = (35/4, 48/5)$$

and an 11th-order polynomial, $P_{12,5}(x)$, proven to have $u = 5$, with

$$V_{12,5} = [111, 87, 87, 76, 63, 52, 52, 28, 28, 4, 4, 4], \quad I_{12,5} = (46/5, 61/6).$$

A pattern is becoming clear. The previous 5 examples have weight vectors that end with small multiples of 2 and taper to these values in decrements of 0, 11, 13, or $11 + 13 = 24$. Moreover $I_{2u+2,u}$ is of the form $(n_1(u), n_2(u))$, where $un_1(u)$ gives the sequence $-2, 11, 22, 35, 46$, with alternating steps of 13 and 11, while $(u + 1)n_2(u)$ gives $13, 24, 37, 48, 61$, with alternating steps of 11 and 13. The ubiquity of 11 and 13 results from the fact that the building blocks of the target are $K = kb^{11}$ and $B = b^{13}$, giving $n = KB^3 + B + 1 = kb^{50} + b^{13} + 1$, chosen so as to achieve very rapid proofs with factorization fraction $f(13) = 13/(3 \times 13 + 11) = 26\%$. (It is one of those happy accidents of experimental mathematics that the quest for 26% led me to the twin primes $c = 13$ and $c - 2 = 11$, making it very easy to spot the pattern in this particular chain and then to generalize it.)

Studying the pattern thus far, one spots a game of leap-frog, by writing out the first 5 ranges numerically:

$$(-2.00, 6.50), (5.50, 8.00), (7.33, 9.25), (8.75, 9.60), (9.20, 10.17).$$

Note that $I_{10,4} \approx (8.75, 9.60)$ is redundant, since $I_{8,3}$ overlaps $I_{12,5}$, assuming that b is sufficiently large. (It might, however, be a good idea to leave $P_{10,4}$ in the code, as an option, in case the powers of k eat away at the overlap, for modest values of b.)

Next comes a polynomial $P_{14,6}(x)$ with degree 13 and weight vector

$$V_{14,6} = [137, 113, 113, 102, 89, 78, 65, 54, 54, 30, 30, 6, 6, 6],$$

and range $I_{14,6} = (59/6, 72/7) \approx (9.83, 10.29)$. Now let us remind ourselves of how far we must go. The target zone of 26% requires us to reach $z = O(b^{11})$. It might appear that progress is becoming slow, with $n_2(6) - n_2(5) \approx 10.29 - 10.17 = 0.12$. However, the next member of the series has

$$V_{16,7} = [161, 137, 137, 126, 113, 102, 89, 78, 78, 54, 54, 30, 30, 6, 6, 6],$$

with $I_{16,7} = (70/7, 85/8) \approx (10.00, 10.63)$. In general, $I_{2u+2,u} = (n_1(u), n_2(u))$ with

$$n_1(2j) = \frac{24j - 13}{2j},\ n_2(2j) = \frac{24j}{2j+1},\ n_1(2j+1) = \frac{24j-2}{2j+1},\ n_2(2j+1) = \frac{24j+13}{2j+2}.$$

For $u = 6 \ldots 10$ the ranges $I_{2u+2,u}$ form the sequence

$$(9.83, 10.29), (10.00, 10.63), (10.38, 10.67), (10.44, 10.90), (10.70, 10.91)$$

with the larger of the indices showing a tendency to freeze at even values of u. For example, $n_2(10) = 120/11 \approx 10.91$ is scarcely better than $n_2(9) = 109/10 = 10.90$. But we do not care about that, since we can leap-frog even values of $u > 2$, using the 6 polynomials with $u = 1, 2, 3, 5, 7, 9$ to reach $z = O(b^{109/10})$.

Finally, I obtained a 23rd order polynomial $P_{24,11}(x)$ with weight vector

$$\begin{aligned} V_{24,11} &= [261, 237, 237, 226, 213, 202, 189, 178, 165, 154, 141, 130, \\ &\quad 130, 106, 106, 82, 82, 58, 58, 34, 34, 10, 10, 10] \end{aligned}$$

and range $I_{24,11} = (118/11, 133/12) \approx (10.73, 11.08)$, as may be confirmed by computing the vectors

$$\begin{aligned} 12V_{24,11} + 133N_{24} &= [3132, 2977, 3110, 3111, 3088, 3089, 3066, 3067, \\ &\quad 3044, 3045, 3022, 3023, 3156, 3001, 3134, 2979, \\ &\quad 3112, 2957, 3090, 2935, 3068, 2913, 3046, 3179], \\ 11V_{24,11} + 118N_{24} &= [2871, 2725, 2843, 2840, 2815, 2812, 2787, 2784, \\ &\quad 2759, 2756, 2731, 2728, 2846, 2700, 2818, 2672, \\ &\quad 2790, 2644, 2762, 2616, 2734, 2588, 2706, 2824] \end{aligned}$$

where N_{24} has $i-1$ as its ith component. Note carefully that the last component of the first test vector is larger than all the others, while in the second test vector the first component is the largest. (It is amusing to note how flat the two test vectors are. This is my algebraic version of LLL, in logarithmic form.)

Since $n_2(11) = 133/12 = 11 + \frac{1}{12}$, we may now prove primality for a probable prime $n = kb^{50} + b^{13} + 1$, with $b \gg k$, using 7 polynomials, namely those with $u = 1, 2, 3, 5, 7, 9, 11$, whose ranges

$$\begin{gathered}(-2, 13/2), (11/2, 8), (22/3, 37/4), (46/5, 61/6),\\ (10, 85/8), (94/9, 109/10), (118/11, 133/12)\end{gathered}$$

overlap and exhaust all possible factors $zb^{13} + 1$ with $0 < z < kb^{11}$.

This chain enables one to prove primality in a few minutes, after the Pocklington tests are completed. We simply find 8 small primes that certify the square test and the absence of integer roots of the 7 polynomials, with degrees $h - 1 = 2u + 1 = 3, 5, 7, 11, 15, 19, 23$. Then the proof is completed by checking 14 inequalities, at the overlapping endpoints for which Descartes' rule of signs exhausts factors. The certificating code occupies a few kilobytes.

Such efficiency is to be contrasted with numerical methods, where more than 80 polynomials might be required, if the LLL bounds were truly indicative of their ranges of utility. When I gave this problem to my numerical client/server CHG set-up, with a set of 82 polynomials selected according to their LLL bounds, and no appeal to Descartes' sign rule, it took 75 CPUhours to prove a single prime with 10,000 digits and generate a 26 MB certificate. By algebraic means, I have now increased the speed by a factor of about 1,000 and decreased the storage by a factor of about 1,000.

Most importantly, the polynomials developed for this case are the first 11 of a truly generic chain, whose continuation allows one to get even closer to the 25% barrier, as I shall now explain.

4 The master chain

Based on the above example, I found a construction for a sequence of master polynomials, $F_u(y, B, C)$, that solve the problem of approaching 25%. To prove a prime of the form $n = kb^{4c-2} + b^c + 1$, with an integer $c > 1$, one may use the chain

$$P_{2u+2,u}(x) = b^{2[u/2]} \frac{F_u(xb^c, b^c, kb^{4c-2})}{b^{2uc+c}}$$

where $[u/2]$ is the integer part of $u/2$. (With $c = 13$ we shall recover the results of the previous section.) The chain begins with

$$\begin{aligned}
F_1(y,B,C) &= y^2(y+B)+C,\\
F_2(y,B,C) &= y^3(y+B)^2+g_1(y,B,2)C+C^2,\\
F_3(y,B,C) &= y^4(y+B)^3+g_1(y,B,3)y(y+B)C+h_1(y,B,3)C^2+C^3,\\
g_1(y,B,u) &= (3y-1)(y+B)+(u-2)Gy,\\
h_1(y,B,u) &= g_1(y,B,2)+(u-2)G, \quad G \equiv By+2y-1.
\end{aligned}$$

The general form is

$$\begin{aligned}
F_u(y,B,C) &= y(y^2+By)^u+G_u(y,B,C)+H_u(y,B,C)+C^u,\\
G_u(y,B,C) &= \sum_{r=1}^{[u/2]} g_r(y,B,u)(y^2+By)^{u-2r}C^r,\\
H_u(y,B,C) &= \sum_{r=1}^{[(u-1)/2]} h_r(y,B,u)C^{u-r},
\end{aligned}$$

where g_r and h_r are polynomials in y, with degree $2r$, and in B, with degree r. (It turns out that they are also polynomials in u, with degree r, which is why I include u as an argument, rather than a subscript.)

Denoting the coefficients of y^s in g_r and h_r by $g_{r,s}(B,u)$ and $h_{r,s}(B,u)$, respectively, I specify the leading coefficients of y^{2r} by

$$g_{r,2r}(B,u) = B(u-2r)+2(u-r)+1, \quad h_{r,2r}(B,u) = 2r+1$$

and, for $s < 2r$, I further require that $g_{r,s}$ and $h_{r,s}$ are polynomials in B with degrees $d_{r,s}$ subject to the powerful constraint

$$d_{r,s} \le \min(r, s+1, 2r-s+1)$$

which drastically limits the non-zero Taylor coefficients. I further specify that

$$g_r(0,0,u) = 0, \quad h_r(0,0,u) = (-1)^r \binom{u-r-1}{r}.$$

Finally, I require that the limit

$$\lim_{\lambda\to 0} \frac{F_u(1+\lambda, B, n\lambda-1-B)}{\lambda^u}$$

exists, for arbitrary B and n. For each $u \leq 11$, I found that there is a unique solution to this master CHG condition allowed by the constraints on the Taylor coefficients given above. Moreover, I found that the coefficients of this unique solution are integers.

It is wonderfully convenient to have a master CHG condition that defines the polynomials, since then the problem of determining F_u reduces to linear algebra with a matrix of integers that specify the contributions of undetermined Taylor coefficients to partial derivatives that vanish in the limit $\lambda \to 0$. By conjecture, there is a unique set of integers that solves the master CHG condition. Hence we may find them, modulo a small set of primes, using the `matsolvemod` routine of Pari-GP and then construct the integers using the Chinese remainder theorem.

From the solutions with $u \leq 11$, I infer that both $g_r(y,B,u)$ and $h_r(y,B,u)$ are polynomials in Gu of degree r and that the rth derivative with respect to u is $G^r y$ in the case of g_r and G^r in the case of h_r. Hence we need only go up to $u = 3r-1$ to determine g_r and h_r for all u. From the very simple matrices with $u \leq 5$, I obtained

$$\begin{aligned}
g_2(y,B,u) &= (u-2)(u-3)yG^2/2 + (u-4)HG + y(y+B)I,\\
h_2(y,B,u) &= (u-3)(u-4)G^2/2 + (u-4)(4y-1)(y+B)G + g_2(y,B,4),\\
H &\equiv (3y-1)(y+B) + y(y-1)^2,\\
I &\equiv (7y-2)(y+B) - 2(y-1)^2.
\end{aligned}$$

Similarly, the results for $u \leq 8$ determine g_3 and h_3, while those for $u \leq 11$ determine g_4 and h_4. In all cases, $g_r(y,B,2r) = h_r(y,B,2r)$. Thus the code that records the first 11 polynomials contains only the 8 master formulas for $g_r(y,B,u)$ and $h_r(y,B,u)$ with $r \leq 4$ and the 3 specific formulas for $g_5(y,B,10)$, $g_5(y,B,11)$ and $h_5(y,B,11)$. It is encouraging to note that the largest coefficient in these 3 specific cases is merely 7355. Had I resorted to `matsolvemod` these particular solutions would have been very easy to find. In fact, I used far more laborious methods, to establish that I had obtained the unique solutions with the weight vectors characterized below.

For every divisor $d = zb^c + 1$ of $n = kb^{4c-2} + b^c + 1$, with $c > 1$, we have ensured, via the master CHG condition, that $d^u | P_{2u+2,u}(-z)$. Now we need to look at the ranges which these polynomials cover. The weight vectors of $P_{2u+2,u}(x)$ have the pattern

$$\begin{aligned}
V_{4,1} &= [c-2,0,0,0],\\
V_{6,2} &= [3c-2,c,c,2,2,2],\\
V_{8,3} &= [5c-4,3c-2,3c-2,2c,2c,2,2,2],
\end{aligned}$$

$$\begin{aligned}
V_{10,4} &= [7c-4, 5c-2, 5c-2, 4c, 3c, 2c+2, 2c+2, 4, 4, 4],\\
V_{12,5} &= [9c-6, 7c-4, 7c-4, 6c-2, 5c-2, 4c, 4c, 2c+2, 2c+2, 4, 4, 4],\\
V_{14,6} &= [11c-6, 9c-4, 9c-4, 8c-2, 7c-2, 6c,\\
&\quad 5c, 4c+2, 4c+2, 2c+4, 2c+4, 6, 6, 6],\\
V_{16,7} &= [13c-8, 11c-6, 11c-6, 10c-4, 9c-4, 8c-2, 7c-2, 6c,\\
&\quad 6c, 4c+2, 4c+2, 2c+4, 2c+4, 6, 6, 6].
\end{aligned}$$

Observe that $V_{2u+2,u}$ always contains the weight $(u-1)c$, which occurs twice when u is odd. The weight vector begins with $(2u-1)c - 2[(u+1)/2]$ and then the weight decreases with special decrements of $2c-2$ and 0, initially, followed by regular alternating decrements of $c-2$ and c, as long as the result does not fall below $(u-1)c$. The weight vector ends with $2[u/2]$ and then, moving to the left, the weight increases with the special increment 0, initially, followed by regular alternating increments of 0 and $2c-2$, as long as the result does not rise above $(u-1)c$. Note that the difference in weight between the first and last components is $u(c-2)+(u-1)c$, whatever the parity of u.

When $b \gg k$, the algebraic polynomial $P_{2u+2,u}(x)$ is a good candidate for exhausting factors of the form zb^c+1 with $\log(z)/\log(b) \in [n_1(u), n_2(u)]$, where

$$n_1(u) = \frac{(u-1)c - 2[(u+1)/2]}{u}, \quad n_2(u) = \frac{uc - 2[u/2]}{u+1}$$

have the desired overlap property that $n_2(u) - n_1(u+1) = 2/(u+1) > 0$. However we must also check that the indices derived from the first and last components of the tapering weight vector are not modified by any of the intermediates weights. If N_h denotes the h-component vector whose ith component is $i-1$, the range tests come from computing the vectors

$$R_u = (u+1)(V_{2u+2,u} + n_2(u)N_{2u+2}), \quad L_u = u(V_{2u+2,u} + n_1(u)N_{2u+2})$$

whose components are integers. The range is correct if the last component of R_u is its largest and the first component of L_u is its smallest. (Note that we did these tests for the case $c=13$ and $u=11$ at the final stage of the concrete analysis in the previous section.) Both tests succeed for $c>1$ and $2(c+[c/2])+1 \geq u \geq 1$, with an upper limit on u that is larger than the value required for the primality tests.

Finally, observe that the upper limit imposed by the square test is $z < kb^{c-2}$. Hence, with $b \gg k$, we exhaust the range as soon as $n_2(u) > c-2$, which occurs when $2[(u+1)/2] > c-2$, i.e. for the first odd value of u greater than $c-3$. (With $c = 13$, this is indeed $u = 11$.) The odd values of c are hence more interesting, since they give proofs at a smaller factorization percentage for a given limit on the number of polynomials that we have the patience to generate.

Suppose that we have the master polynomials up to $u = 2j+1$ and set $c = u+2$. Then we can achieve a primality proof with a factorization fraction less than $f(c) = c/(4c-2) = (2j+3)/(8j+10)$. To estimate how far below $f(c)$ we may get, we look at the last Cartesian inequality, and require that $b^{2[u/2]}z^{h-1} \ll (zb^c)^u$, at $z = kb^{c-2}$. Setting $u = 2j+1$, $h = 2u+2$, and $c = u+2$, we see that this becomes the condition

$$b^{2j}(kb^{2j+1})^{4j+3} \ll (kb^{4j+4})^{2j+1}$$

which conveniently simplifies to $k^{2j+2} \ll b$. Provided that everything else works out (as can be checked in a concrete numerical case) we appear to be able to get slightly below $f(2j+3)$, approaching a fraction

$$F(j) = \frac{2j+3}{8j+10+\frac{1}{2j+2}}$$

when k gets close to the danger zone with $k^{2j+2} = O(b)$. It is amusing to note that $F(0) = 3/(10+\frac{1}{2}) = 2/7 = f(4)$, which is achievable by use of the theorem. However one chooses to do it, 28.57% seems to be the limit using only the master cubic.

In the example of the previous section, I chose $j = 5$, having to hand the first $2j+1 = 11$ master polynomials. This made for comfortable proofs slightly below $f(13) = 13/50 = 26\%$. In fact we might push our luck and aim to get close to $F(5) = 13/(50+\frac{1}{12}) \approx 25.96\%$. At the cost of solving the linear algebra for $F_{13}(y, B, C)$, we can get comfortably to $f(15) = 15/58 \approx 25.86\%$ and with more boldness close to $F(6) = 15/(58+\frac{1}{14}) \approx 25.83\%$. Note that we do not need the master polynomial at $u = 12$, which we may easily leap-frog, just as we avoided the even values of $u > 2$ in the example at $c = 13$. However the master polynomials with $u = 4, 6, 8, 10$ were decidedly useful in determining the polynomial dependence in u of large classes of Taylor coefficients, so as to reduce the size of the linear algebra problem at $u > 10$.

5 Summary and comments

For $u \leq 11$, I have constructed master polynomials, $F_u(y, B, C)$, with integer-valued Taylor coefficients, limited by simple rules. By specifying a few of these coefficients, I constructed the rest from the master CHG condition that the limit

$$\lim_{\lambda\to 0}\frac{F_u(1+\lambda,B,n\lambda-1-B)}{\lambda^u}$$

exists, for arbitrary B and n. For each $u \leq 11$, there was a unique solution to this condition. I conjecture that, with the system of constraints that I have given, this will continue to be the case at higher degrees and hence that the process may be continued by efficient use of the `matsolvemod` and `chinese` routines of Pari-GP, without further recourse to the laborious methods that I used to ensure uniqueness for $u \leq 11$.

The first polynomial, $F_1(y,B,C) = y^2(y+B)+C$, enables one to achieve proofs at 28.57% factorization, as shown by the theorem. Using the polynomials with $u = 1,2,3,5,7,9,11$, I achieved fast compact proofs below 26% at 10,000 digits. Scaling this up to 100,000 digits seems to be a routine matter: the cost of finding a target goes as the cube of the number of digits; the cost of the BLS tests goes as its square; the cost of my final tests is merely linear in the number of digits, using FFT multiplication. At 10,000 digits, I estimate that I have speeded up the CHG method by a factor of 1,000, for primes of a special form with 26% factorization. The size of a certificate is reduced by a factor of about 1,000, in comparison with the output from numerical LLL methods.

In the course of obtaining the first 11 master polynomials, I found rules for the dependence of Taylor coefficients on u that indicate to me the possibility of a recursive algorithm. Thus far, I achieved this only partially, yet very usefully, since large classes of Taylor coefficients for $u > 11$ are already determined algebraically by those found for $u \leq 11$. Ultimately, one might hope that someone will find a closed expression for the whole family of three-variable polynomials.

Finally, I remark on the special form of prime chosen to illustrate the method, namely $n = kb^{4c-2} + b^c + 1$, which enables one to get below a factorization fraction $f(c) = c/(4c-2)$ with $b \gg k$ and u values up to smallest positive odd integer greater than $c-3$. This specific form was chosen for pedagogical purposes. In fact, the master polynomials $F_u(y,B,C)$ are applicable to a wider class of problem. Their definition is Taylored (if I may use the pun) to produce a nicely tapering weight vector for primes of the form $n = C + B \pm 1$ where $\gcd(B^4, C)$ is especially large. I indicated in Section 2 how to extend the proof method at 28.57% to forms such as $n = kb^3 + lb \pm 1$, using essentially the same cubic polynomial. Similar extensions are possible at lower factorization percentages. As already indicated, the examples given here are merely the first inning of a whole new ball game.

Of one thing one may be sure: there is absolutely nothing in this work that indicates any hope of actually reaching 25%, when the rules of the game start with the theorems of Pocklington or Morrison. However, I do find it rewarding that anyone who chooses to try may get, with relative ease, below 26%, for primes of special forms, now that I have completed the hard work of finding an algebraic definition of the master polynomials.

In conclusion, I am deeply grateful to John Renze, whose recognition of the power of Descartes' rule of signs underpins the utility of the master polynomials which I have here defined and partially elucidated. It now seems to me that there were two very significant dates in the 17th century for would-be primality provers. Everyone knows about Fermat's little theorem, from his letter to Frenicle de Bessy in 1640. I find it remarkable that Descartes' *La Géométrie* of 1637 should provide another vital clue. Relations between Fermat and Descartes were fraught with difficulty. How pleasant, therefore, to see them work here in harmony, with Fermat providing the vital input to the BLS method of primality proving and now Descartes providing a welcomed improvement to the CHG method.

David Broadhurst, February 17, 2006