Robust HGCD with No Backup Steps

Niels Möller

Lysator academic computer society and KTH, Sweden

International Congress on Mathematical Software 2006

Comparison of gcd algorithms

Algorithm	Time (ms)	# lines	
mpn_gcd	1440	304	GMP-4.1.4 (Weber)
mpn_rgcd	87	1967	"Classical" Schönhage gcd
mpn_bgcd	93	1348	Rec. bin. (Stehlé/Zimmermann)
mpn_sgcd	100	760	1987 alg. (Schönhage/Weilert)
mpn_ngcd	85	733	New algorithm for GMP-5

Questions

Q Where does the complexity come from?

A Accurate computation of the quotient sequence.

Q How to avoid that?

A Stop bothering about quotients.

Outline

Background

- Algorithm comparison
- The half-gcd (HGCD) operation
- Subquadratic HGCD

Quotient based HGCD

- Jebelean's criterion

A robustness condition

Simple subquadratic HGCD

Conclusions

What is HGCD?

Definition (Reduction)

$$\begin{pmatrix} a \\ b \end{pmatrix} = M \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

- Positive integers a, b, α, and β
- Matrix M, non-negative integer elements
- $\det M = 1$

What is HGCD?

Definition (Reduction)

$$\begin{pmatrix} a \\ b \end{pmatrix} = M \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

- Positive integers a, b, α, and β
- Matrix M, non-negative integer elements
- $\det M = 1$

Definition (HGCD, "half gcd")

Input: a, b, of size n

Output: M, size of α, β and M elements $\approx n/2$

What is HGCD?

Definition (Reduction)

$$\begin{pmatrix} a \\ b \end{pmatrix} = M \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

- Positive integers a, b, α, and β
- Matrix M, non-negative integer elements
- $\det M = 1$

Definition (HGCD, "half gcd")

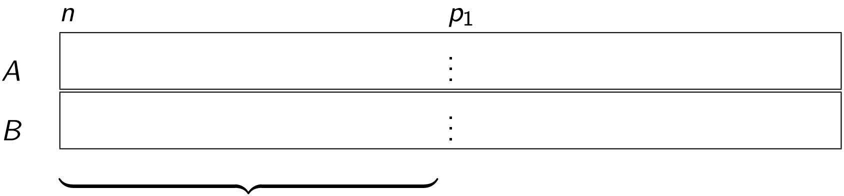
Input: a, b, of size n

Output: M, size of α, β and M elements $\approx n/2$

Fact

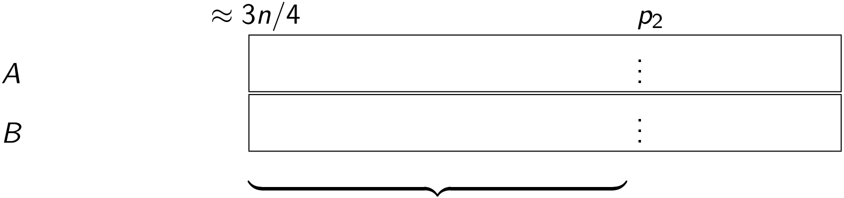
For any reduction, $\gcd(a, b) = \gcd(\alpha, \beta)$

Main idea of subquadratic HGCD



$$M_1 \leftarrow \textsc{hgcd}(\lfloor 2^{-p_1} A \rfloor, \lfloor 2^{-p_1} B \rfloor)$$

$$\begin{pmatrix} A \\ B \end{pmatrix} \leftarrow M_1^{-1} \begin{pmatrix} A \\ B \end{pmatrix}$$



$$M_2 \leftarrow \textsc{hgcd}(\lfloor 2^{-p_2} A \rfloor, \lfloor 2^{-p_2} B \rfloor)$$

$$M \leftarrow M_1 \cdot M_2$$

HGCD algorithm

HGCD(A, B)

$n \leftarrow \#(A, B)$

Select $p_1 \approx n/2$

$M_1 \leftarrow$ HGCD$(\lfloor 2^{-p_1} A \rfloor, \lfloor 2^{-p_1} B \rfloor)$

$(A; B) \leftarrow M_1^{-1}(A; B)$

Perform a small number of divisions or backup steps.

$\triangleright$ A, B are now of size $\approx 3n/4$

Select $p_2 \approx n/4$

$M_2 \leftarrow$ HGCD$(\lfloor 2^{-p_2} A \rfloor, \lfloor 2^{-p_2} B \rfloor)$

$(A; B) \leftarrow M_2^{-1}(A; B)$

Perform a small number of divisions or backup steps.

$\triangleright$ A, B are now of size $\approx n/2$

$M \leftarrow M_1 \cdot M_2$

Return M

HGCD algorithm

HGCD(A, B)

1 $n \leftarrow \#(A, B)$
2 Select $p_1 \approx n/2$
3 $M_1 \leftarrow \text{HGCD}(\lfloor 2^{-p_1} A \rfloor, \lfloor 2^{-p_1} B \rfloor)$
4 $(A; B) \leftarrow M_1^{-1}(A; B)$
5 Perform a small number of divisions or backup steps.
  ▷ A, B are now of size $\approx 3n/4$
6 Select $p_2 \approx n/4$
7 $M_2 \leftarrow \text{HGCD}(\lfloor 2^{-p_2} A \rfloor, \lfloor 2^{-p_2} B \rfloor)$
8 $(A; B) \leftarrow M_2^{-1}(A; B)$
9 Perform a small number of divisions or backup steps.
  ▷ A, B are now of size $\approx n/2$
10 $M \leftarrow M_1 \cdot M_2$
11 Return M

1. Simplify Steps 5 and 9.
2. Eliminate multiplication in Step 8.

Definition (Quotient sequence)

For any positive integers a, b, quotient sequence q_j and remainder sequence r_j are defined by

$$r_0 = a \qquad r_1 = b$$
$$q_j = \lfloor r_{j-1}/r_j \rfloor \qquad r_{j+1} = r_{j-1} - q_j r_j$$

Fact

$$\begin{pmatrix} a \\ b \end{pmatrix} = M \begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix}$$

with

$$M = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_j & 1 \\ 1 & 0 \end{pmatrix}$$

Theorem (Jebelean's criterion)

Let $a > b > 0$, with remainders r_j and r_{j+1},

$$\begin{pmatrix} a \\ b \end{pmatrix} = \underbrace{\begin{pmatrix} u & u' \\ v & v' \end{pmatrix}}_{=M} \begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix}$$

Let $p > 0$ be arbitrary, $0 \le A', B' < 2^p$, and define

$$\begin{pmatrix} A \\ B \end{pmatrix} = 2^p \begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} A' \\ B' \end{pmatrix}$$

$$\begin{pmatrix} R_j \\ R_{j+1} \end{pmatrix} = M^{-1} \begin{pmatrix} A \\ B \end{pmatrix} = 2^p \begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix} + M^{-1} \begin{pmatrix} A' \\ B' \end{pmatrix}$$

For even j, the following two statements are equivalent:

(i) $r_{j+1} \ge v$ *and* $r_j - r_{j+1} \ge u + u'$

(ii) *For any p and any A', B', the jth remainders of A and B are R_j and R_{j+1}.*

Quotient based HGCD

A generalization of Lehmer's algorithm

Define HGCD(a, b) to return an M satisfying Jebelean's criterion.

Example (Recursive computation)

$$
\begin{aligned}
(a; b) &= (858\,824; 528\,747) \\
M_1 &= (13, 8; 8, 5) && \text{No difficulties} \\
(c; d) &= M_1^{-1}(a; b) = 16\,(4009; 194) + (0; 15) \\
M_2 &= \textsc{hgcd}(4009, 194) = (21, 20; 1, 1) \\
M_2^{-1}(4009; 194) &= (129; 65) && \text{Satisfies Jebelean} \\
M &= M_1 \cdot M_2 = (281, 268; 173, 165) \\
M^{-1}(a; b) &= (1764; 1355) && \text{Violates Jebelean}
\end{aligned}
$$

Backup step

Example (Fixing M)

$$(a; b) = (858\,824; 528\,747)$$
$$M = M_1 \cdot M_2 = (281, 268; 173, 165)$$
$$M^{-1}(a; b) = (1764; 1355)$$

Violates Jebelean

M corresponds to quotients $1, 1, 1, 1, 1, 1, 1, 20, 1$.
E.g., $(A; B) = 8\,(a; b) + (1; 7)$ has quotient sequence starting with $1, 1, 1, 1, 1, 1, 1, 20, 2$.

Backup step

Example (Fixing M)

$$(a; b) = (858\,824; 528\,747)$$

$$M = M_1 \cdot M_2 = (281, 268; 173, 165)$$

$$M^{-1}(a; b) = (1764; 1355)$$

Violates Jebelean

M corresponds to quotients $1, 1, 1, 1, 1, 1, 1, 20, 1$.
E.g., $(A; B) = 8\,(a; b) + (1; 7)$ has quotient sequence starting with $1, 1, 1, 1, 1, 1, 1, 20, 2$.

Conclusion

- The quotients are correct for $(a; b)$, but not robust enough.
- Must drop final quotient before returning $\textsc{hgcd}(A, B)$.

A robustness condition

Definition (Robust reduction)

A reduction M of $(a; b)$ is robust iff

$$M^{-1}\left\{\begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} x \\ y \end{pmatrix}\right\} > 0$$

for all "small" $(x; y)$. More precisely, for all $(x; y) \in S$, where

$$S = \{(x; y) \in \mathbb{R}^2, |x| < 2, |y| < 2, |x - y| < 2\} \tag{1}$$

A robustness condition

Definition (Robust reduction)

A reduction M of $(a; b)$ is robust iff

$$M^{-1}\left\{\begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} x \\ y \end{pmatrix}\right\} > 0$$

for all "small" $(x; y)$. More precisely, for all $(x; y) \in S$, where

$$S = \{(x; y) \in \mathbb{R}^2, |x| < 2, |y| < 2, |x - y| < 2\} \tag{1}$$

Theorem

The reduction

$$\begin{pmatrix} a \\ b \end{pmatrix} = \underbrace{\begin{pmatrix} u & u' \\ v & v' \end{pmatrix}}_{=M} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

is robust iff $\alpha \geq 2\max(u', v')$ *and* $\beta \geq 2\max(u, v)$

Sufficient conditions

Corollary

If $\min(\alpha, \beta) > 2 \max M$, *then* M *is robust.*

Lemma (Strong robustess)

Let $n = \#(a, b)$ *denote the bitsize of the larger of* a *and* b. *If* $\# \min(\alpha, \beta) > \lfloor n/2 \rfloor + 1$, *then* M *is robust.*

Theorem (Schönhage/Weilert reduction)

For arbitrary $a, b > 0$, *let* $n = \#(a, b)$ *and* $s = \lfloor n/2 \rfloor + 1$. *There exists a unique strongly robust* M *such that* $\# \min(\alpha, \beta) > s$ *and* $\#|\alpha - \beta| \leq s$.

HGCD with strong robustness

$\textsc{hgcd}(A, B)$

$n \leftarrow \#(A, B)$
$s \leftarrow \lfloor n/2 \rfloor + 1$
$p_1 \leftarrow \lfloor n/2 \rfloor$
$M_1 \leftarrow \textsc{hgcd}(\lfloor 2^{-p_1} A \rfloor, \lfloor 2^{-p_1} B \rfloor)$
$(C; D) \leftarrow M_1^{-1}(A; B) \triangleright \#|C - D| \approx 3n/4$
One subtraction and one division step on $(C; D)$. Update M_1.
$p_2 \leftarrow 2s - \#(C, D) + 1$
$M_2 \leftarrow \textsc{hgcd}(\lfloor 2^{-p_2} C \rfloor, \lfloor 2^{-p_2} D \rfloor)$
return $M_1 \cdot M_2$

- Uses strong robustness
- Returns with $\#|\alpha - \beta| \leq s + 2k$, where k is the recursion depth.
- To compute Schönhage/Weilert reduction, need at most four additional division steps before returning.

HGCD with plain robustness

HGCD(A, B)

$n \leftarrow \#(A, B)$
$s \leftarrow \lfloor n/2 \rfloor + 1$
$p_1 \leftarrow \lfloor n/2 \rfloor$
$M_1 \leftarrow \text{HGCD}(\lfloor 2^{-p_1} A \rfloor, \lfloor 2^{-p_1} B \rfloor)$
$(C; D) \leftarrow M_1^{-1}(A; B) \triangleright \#|C - D| \approx 3n/4$
One subtraction and one division step on $(C; D)$. Update M_1.
$p_2 \leftarrow \#M_1 + 2$
$M_2 \leftarrow \text{HGCD}(\lfloor 2^{-p_2} C \rfloor, \lfloor 2^{-p_2} D \rfloor)$
return $M_1 \cdot M_2$

$$M^{-1}\left\{\begin{pmatrix} A \\ B \end{pmatrix} + \begin{pmatrix} x \\ y \end{pmatrix}\right\} = 2^{p_2} M_2^{-1}\left\{\begin{pmatrix} c \\ d \end{pmatrix} + \underbrace{\begin{pmatrix} \delta c \\ \delta d \end{pmatrix} + 2^{-p_2} M_1^{-1}\begin{pmatrix} x \\ y \end{pmatrix}}_{\text{disturbance } \in S}\right\}$$

Conclusions

Conclusions

- HGCD in terms of correct quotients $\implies$ complexity.
- Reduction matrices are important, quotients are not.
- "Robust reduction" is a powerful notion in analysis and algorithm design.
- Can use either the robustness condition, or Schönhage/Weilert's condition on bitsizes.

Further work

Further analysis and experiments on the HGCD algorithm using plain robustness.