The University of Warwick

THEORY OF COMPUTATION

REPORT NO. 39.

COMPOSITION AND CHARACTERS OF BINARY QUADRATIC FORMS

BY

CONSTANTINOS S ILIOPOULOS

Department of Computer Science
University of Warwick
Coventry CV4 7AL
England

JANUARY 1982

COMPOSITION AND CHARACTERS OF BINARY QUADRATIC FORMS

CONSTANTINOS S. ILIOPOULOS
WARWICK UNIVERSITY
DEPT. OF COMPUTER SCIENCE
COVENTRY CV4 7AL
U.K.

To Spiros - Despina & Vickie - Yiannis

JANUARY 1982

1. INTRODUCTION

In this paper two number theoretic algorithms are presented. The first is an algorithm for composition of binary quadratic forms having running time of $O(M(\log|D|)\log\log|D|)$ elementary operations (for reduced forms with determinant D) improving the upper bound given by Lagarias in [6] by a factor of $O(\log\log|D|/\log|D|)$. This algorithm will appear in [4]. The second algorithm is for evaluation of the genus characters of the form class group $C\ell(D)$. It has running time $O(M(\log|D|)\log|D|)$ elementary operations, asymptotically the same as the upper bound of Lagarias in [6] but the algorithm described here is simpler and has a better implicit constant.

2. BASIC DEFINITIONS-NOTATIONS

Suppose that

$$Q(x,y) = ax^2 + 2bxy + cy^2 \qquad a,b,c \in Z$$

Then Q is called binary quadratic form (or abbreviated form) and it is denoted by $Q = (a,b,c)$. Its determinant D is the integer $D = b^2 - ac$.

If $D > 0$, non-square, then the form $Q = (a,b,c)$ is reduced iff

$$|\sqrt{D} - |a|| < b < \sqrt{D}$$

and if $D < 0$, then the form $Q = (a,b,c)$ is reduced iff

$$|2b| \lesssim |a| \lesssim c$$

Hence a reduced form satisfies

$$O(\|Q\|) = O(|D|) \tag{2.1}$$

where $\|Q\| = \max\{a,b,c\}$.

An integer M is represented by a form Q iff there exist integers m,n such that $Q(m,n) = M$.

3. COMPOSITION

Suppose that $Q_1 = (a_1, b_1, c_1)$, $Q_2 = (a_2, b_2, c_2)$ are properly primitive forms with determinant D (non-square, if D>0). Then the forms Q_1, Q_2 are composed to a properly primitive form Q_3 with the same determinant via a bilinear matrix B, if the following holds:

$$Q_1(x_1,y_1) \cdot Q_2(x_2,y_2) = Q_3(z_1,z_2)$$

with $(z_1,z_2) = B \cdot (x_1\, y_1,\ x_1\, y_2,\ x_2\, y_1,\ x_2\, y_2)^T$ for some bilinear matrix B with integer entries given by

$$B = \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \end{pmatrix}$$

satisfying the conditions:

(i) Unimodularity : The greatest common divisor of Δ_{ij}'s for $1 \leq i < j < 4$ is one, where

$$\Delta_{ij} = \begin{vmatrix} b_{1i} & b_{1j} \\ b_{2i} & b_{2j} \end{vmatrix} = b_{1i}\, b_{2j} - b_{2i}\, b_{1j}$$

(ii) Orientability : $a_1\ \Delta_{12} > 0$, $a_2\ \Delta_{13} > 0$

(Orientability of the matrix B is necessary to distinguish between composition with a form (a,b,c) and composition with its opposite (a, -b, c).

The operation of composition of forms is denoted by

$$Q_1 \circ Q_2 = Q_3 \quad \text{via } B$$

The algorithm described below for composition is based on the constructive proofs of the following lemma and theorem.

LEMMA 3.1 (Dickson [1], p.134)

Suppose that $\gcd(m_1,m_2, \ldots , m_n)=1$. If s divides $m_i\, q_j - m_j\, q_i$ for $1 < i, j < n$, then there exists exactly one solution B(mod s) of the system of equations

$$m_i B = q_i \pmod{s} \quad 1 \leq i \leq n \tag{3.1}$$

Proof

Since $\gcd(m_1, m_2, \ldots, m_n)=1$, there exist integers a_i, $1 \leq i \leq n$ such that

$$\sum_{i=1}^{n} a_i m_i = 1$$

Then

$$B = \sum_{i=1}^{n} a_i q_i \pmod{s}$$

is a solution of the system (3.1) because

$$m_k B = m_k \sum_i a_i q_i \equiv \sum_i a_i m_i q_k = q_k \sum_i a_i m_i \equiv q_k \pmod{s}, 1 \leq k \leq n$$

It is not difficult to see that the above solution is unique (mod s) □

Proofs of the following theorem were given by Gauss ([2] , A.243), Mathews ([7], p.152) and Pall ([8], p.404).

THEOREM 3.2

Suppose that $Q_1 = (a_1, b_1, c_1)$ and $Q_2 = (a_2, b_2, c_2)$ are properly primitive forms with determinant D. Let $\mu = \gcd(a_1, a_2, b_1 + b_2)$, $m_1 = a_1/\mu$, $m_2 = a_2/\mu$, $m_3 = (b_1 + b_2)/\mu$ and $a_3 = m_1 m_2$. Then

(i) The following system has integer coefficients and a unique solution x (mod a_3)

$$\begin{aligned} m_1 x &\equiv b_2 m_1 && \text{(A)} \\ m_2 x &\equiv b_1 m_2 && \text{(B)} \qquad (3.2) \\ m_3 x &\equiv (b_1 b_2 + D)/\mu && \text{(C)} \end{aligned}$$

(ii) Suppose b_3 is the solution of (3.2). Then $Q_3 = (a_3, b_3, *)$ is a form with determinant D and there exists a bilinear matrix B such that $Q_1 \circ Q_2 = Q_3$ via B.

Proof

(i) The system (3.2) has integer coefficients, since

$$b_1 b_2 + D = b_1 b_2 + b_2^2 - a_2 c_2 = b_2 (b_1 + b_2) - a_2 c_2 \equiv 0 \pmod{\mu}$$

Since $\gcd(m_1, m_2, m_3) = 1$ and a_3 divides $m_1 m_2 b_2 - m_2 m_1 b_1$, $m_2(b_1 b_2 + D)/\mu - m_3 b_1 m_2 = - m_1 m_2 c_1$, $m_1(b_1 b_2 + D)\mu - m_3 m_1 b_2 = - m_1 m_2 c_2$, lemma 3.1 applies, and one can find the unique solution $x \pmod{a_3}$ of the system (3.2) by choosing integers s_1, s_2, s_3 such that $s_1 m_1 + s_2 m_2 + s_3 m_3 = 1$

and defining

$$x = s_1 b_2 m_1 + s_2 b_1 m_3 + s_3(b_1 b_2 + D)/\mu$$

(ii) Let $Q_3 = (a_3, b_3, c_3)$. It will be shown that $c_3 = (b_3^2 - D)/\alpha_3$ is integer. Using (C) of (3.2)

$$b_3^2 - D \equiv b_3^2 - (b_1 + b_2)b_3 + b_1 b_2 = (b_3 - b_1)(b_3 - b_2) \pmod{\mu a_3}$$

From (A), (B) follows

$$b_3 - b_1 \equiv 0 \pmod{m_1} \text{ and } b_3 - b_2 \equiv 0 \pmod{m_2}$$

Hence $b_3^2 - D \equiv 0 \pmod{a_3}$ and c_3 is an integer.

It is not difficult to show that $Q_1 \circ Q_2 = Q_3$ via B, with

$$B = \begin{pmatrix} \mu & (b_2-b_3)/\mu & (b_1-b_3)/m_1 & (b_1 b_2 + D - b_3 m_3 \mu)/\mu\, m_1 m_2 \\ 0 & m_1 & m_2 & m_3 \end{pmatrix} . \square$$

ALGORITHM 3.4

INPUT : Two properly primitive forms $Q_1 = (a_1, b_1, c_1)$ and $Q_2 = (a_2, b_2, c_2)$ of the same determinant D

OUTPUT : A properly primitive form $Q_3 = (a_3, b_3, c_3)$ and a bilinear matrix B, which satisfies $Q_1 \circ Q_2 = Q_3$ via B

<u>Begin</u>

1. $\mu \leftarrow \gcd(a_1, a_2, b_1 + b_2)$;

2. $m_1 \leftarrow a_1/\mu$; $m_2 \leftarrow a_2/\mu$; $m_3 \leftarrow (b_1 + b_2)/\mu$;

3. Find s_1, s_2, s_3 such that : $s_1 m_1 + s_2 m_2 + s_3 m_3 = 1$

   <u>Comment</u> This can be done with two applications of the Extended Euclidean algorithm (see Knuth [5])

4. $a_3 \leftarrow m_1 m_2$;

5. $b_3 \leftarrow s_1 b_2 m_1 + s_2 b_1 m_2 + s_3(b_1 b_2 + D)/\mu$;

6. $c_3 \leftarrow b_3^2 - D/a_3$;

7. $B \leftarrow \begin{pmatrix} \mu & (b_2-b_3)/m_2 & (b_1-b_3)/m_1 & (b_1b_2+D-b_3m_3\mu)/\mu m_1 m_2 \\ 0 & m_1 & m_2 & m_3 \end{pmatrix}$

   <u>Return</u> $Q_3 = (a_3, b_3, c_3)$, B;

<u>end</u>. □

<u>THEOREM 3.5</u>

Algorithm 3.4 correctly computes a properly primitive form Q_3 and a bilinear matrix B such that $Q_1 \circ Q_2 = Q_3$ via B in $O(M(\log\|Q\|)\log\log\|Q\|)$ elementary operations, where $\|Q\| = \max\{\|Q_1\|, \|Q_2\|\}$. Moreover $\log\|B\| = O(\log\|Q\|)$.

<u>Proof</u>

The correctness follows from Theorem 3.3.

Step 1 requires $O(M(\log\|Q\|)\log\log\|Q\|)$ elementary operations for an application of the Euclidean algorithm (see [5]). Step 2 requires only $O(M(\log\|Q\|))$ elementary operations for divisions. Step 3 requires $O(M(\log\|Q\|)\log\log\|Q\|)$ elementary operations for two applications of the Extended Euclidean Algorithm. Steps 4-7 require only $O(M(\log\|Q\|)$ elementary operations for multiplications and divisions. Hence the algorithm terminates in $O(M(\log\|Q\|)\log\log\|Q\|)$ elementary operations in worst-case. It follows directly that $\log\|B\| = O(\log\|Q\|)$. □

COROLLARY 3.6

If the forms Q_1, Q_2 of the input of algorithm 3.4 are reduced, then algorithm 3.4 requires $O(M(\log|D|)\log\log|D|)$ elementary operations to compute a properly primitive form Q_3 (not necessarily reduced) and a bilinear matrix B such that $Q_1 \circ Q_2 = Q_3$ via B. Moreover $\log\|B\| = O(\log|D|)$.

Proof

The corollary follows from (2.1) and from Theorem 3.5. □

Lagarias [6] gave an $O(M(\log\|Q\|)\log\|Q\|)$ algorithm for composition of forms, which is based on Dirichlet's method (it makes use of "concordant" or "united" forms).

4. CHARACTERS

The equivalence classes of properly primitive forms with fixed determinant D under composition form an abelian group via $C\ell(D)$ (see [3], section 1.2). An algorithm for evaluation of the genus characters (the character of order 2) of $C\ell(D)$ is given below.

The definition of the genus characters and the algorithm for their evaluation depends on the following lemma.

LEMMA 4.1 (Mathews [7], p.132)

If Q is a properly primitive form, then there exists an integer N represented by Q with gcd(N, 2D) = 1.

Proof

Suppose that Q = (a, b, c). Then let

$$\gcd(a, c, 2D) = \prod_\alpha p_\alpha^{n_\alpha}$$

$$\gcd(a, 2d) = \prod_\alpha p_\alpha^{m_\alpha} \prod_\beta q_\beta^{v_\beta} \qquad (4.1)$$

$$\gcd(c, 2D) = \prod_\alpha p_\alpha^{k_\alpha} \prod_\gamma \tau_\gamma^{t_\gamma} \qquad (4.2)$$

and

$$2D = \prod_\alpha p_\alpha^{e_\alpha} \prod_\beta q_\beta^{u_\beta} \prod_\alpha \tau_\gamma^{z_\gamma} \prod_{i=1}^{\delta} s_i^{h_i} \qquad (4.3)$$

where p_i, q_i, τ_i, s_i are distinct primes and $n_\alpha \leq m_\alpha \leq e_\alpha$, $n_\alpha \leq k_\alpha \leq e_\alpha$, $v_\beta \leq u_\beta$ and $t_\gamma \leq z_\gamma$.

If $x = \pi_\beta \, q_\beta \, \pi_i \, s_i$ and $y = \pi_\gamma \, \tau_\gamma$, then let $N = Q(x,y)$. It is not difficult to show that $\gcd(N, 2D) = 1$. □

<u>Remark</u>

If we partition the s_i's into two disjoint sets, say $\{s_1,\ldots,s_n\}$, $\{s_{n+1},\ldots,s\}$, then $Q(x', y') = N'$ with

$$x' = \pi_\beta \, q_\beta \, s_1 \ldots s_\mu \, , \; y' = \pi_\gamma \, \tau_\gamma \, s_{\mu+1} \ldots s_\delta \quad \text{satisfies } \gcd(N', 2D) = 1. \; \square$$

Now for each prime division p_i of D the character χ_{p_i} is defined such that

$$\chi_{p_i} : C\ell(D) \to \{-1, 1\} \text{ via } \chi_{p_i}(Q) := \chi_{p_i}(N) := \left(\frac{N}{p_i}\right)$$

where Q is a form representing a class of $C\ell(D)$, N is an integer represented by Q with $\gcd(N, 2D) = 1$ and $\left(\frac{N}{p_i}\right)$ is the Legendre symbol. Moreover

$$\chi_{-4}(Q) := \chi_{-4}(N) = (-1)^{(N-1)/2} \text{ when } D \equiv 0,3,4,7 \pmod 8$$

$$\chi_8(Q) := \chi_8(N) = (-1)^{(N^2-1)/8} \text{ when } D \equiv 2,0 \pmod 8$$

$$\chi_{-8}(Q) := \chi_{-4}(Q) \cdot \chi_8(Q) \qquad \text{when } D \equiv 6 \pmod 8$$

where Q, N are as above.

TABLE I
Basis for Genus Characters

Determinant $D = df^2$		Field characters	Ring characters
$d \equiv 1 \pmod 4$	$f \equiv 1 \pmod 4$	$\chi_{p_1}, \ldots, \chi_{p_r}$	$\chi_{q_1}, \ldots, \chi_{q_s}$
	$f \equiv 2 \pmod 4$	$\chi_{p_1}, \ldots, \chi_{p_r}$	$\chi_{q_1}, \ldots, \chi_{q_s}, \chi_{-4}$
	$f \equiv 0 \pmod 4$	$\chi_{p_1}, \ldots, \chi_{p_r}$	$\chi_{q_1}, \ldots, \chi_{q_s}, \chi_{-4}, \chi_8$
$d \equiv 3 \pmod 4$	$f \equiv 1 \pmod 2$	$\chi_{-4}, \chi_{p_1}, \ldots, \chi_{p_r}$	$\chi_{q_1}, \ldots, \chi_{q_s}$
	$f \equiv 2 \pmod 4$	$\chi_{-4}, \chi_{p_1}, \ldots, \chi_{p_r}$	$\chi_{q_1}, \ldots, \chi_{q_s}$
	$f \equiv 0 \pmod 4$	$\chi_{-4}, \chi_{p_1}, \ldots, \chi_{p_r}$	$\chi_{q_1}, \ldots, \chi_{q_s}, \chi_8$
$d \equiv 2 \pmod 8$	$f \equiv 1 \pmod 2$	$\chi_8, \chi_{p_1}, \ldots, \chi_{p_r}$	$\chi_{q_1}, \ldots, \chi_{q_s}$
	$f \equiv 0 \pmod 2$	$\chi_8, \chi_{p_1}, \ldots, \chi_{p_r}$	$\chi_{q_1}, \ldots, \chi_{q_s}, \chi_{-4}$
$d \equiv 6 \pmod 8$	$f \equiv 1 \pmod 2$	$\chi_{-8}, \chi_{p_1}, \ldots, \chi_{p_r}$	$\chi_{q_1}, \ldots, \chi_{q_s}$
	$f \equiv 0 \pmod 2$	$\chi_{-4}, \chi_8, \chi_{p_1}, \ldots, \chi_{p_r}$	$\chi_{q_1}, \ldots, \chi_{q_s}$

THEOREM 4.2

The characters χ_{p_i}, χ_{-4}, χ_8, χ_{-8} are well defined. If the first character of Table I is deleted, then the remaining characters are a basis for the genus characters of $C\ell(D)$ for the appropriate type of D.

Proof

See [7] p.133 and [9], p.143-144. □

ALGORITHM 4.3

INPUT : The set $P = \{P_1, P_2, \ldots, P_\tau\}$ of all odd distinct prime divisors of D and a reduced form Q = (a, b, c) with determinant D.

OUTPUT : $\chi_p(Q)$ $\forall\, p \in P$ and $\chi_{-4}(Q)$, $\chi_8(Q)$, $\chi_{-8}(Q)$ when appropriate.

Begin

1. $m_1 \leftarrow \gcd(a, c, 2D)$;
2. $m_2 \leftarrow \gcd(a, 2D)$;
3. $m_3 \leftarrow \gcd(c, 2D)$;
4. <Compute $R = \{q_1, \ldots, q_m\} \subseteq P$ as in (4.1)>;
5. <Compute $T = \{\tau_1, \ldots, \tau_e\} \subseteq P$ where τ_i as in (4.2)>;
6. <Compute $S = \{s_1, \ldots s_n\} \subseteq P$ where s_i as in (4.3)>;

   Comment The computation of R, T, S is done in the following way : for each $p \in P$ which does not divide m_1, if $p | m_2$, then $p \in R$, if $p | m_3$, then $p \in T$, else $p \in S$.

7. $x \leftarrow$ <the product of all primes in $R \cup S$>;
8. $y \leftarrow$ <the product of all primes in T>;
9. $N \leftarrow ax^2 + 2bxy + cy^2$;

10. <u>For</u> p = 1 <u>until</u> k <u>do</u>

<u>Begin</u>

11. $N_1 \leftarrow N \pmod{p_i}$;

12. $X_{p_i}(Q) \leftarrow N_1^{(p_i-1)/2} \pmod{p_i}$;

<u>Comment</u> The symbol $\left(\frac{N}{p}\right)$ is computed using Euler's criterion

13. <u>end</u>

14. <u>If</u> $D \equiv 0, 3, 4, 7 \pmod 8$ <u>then</u> $X_{-4} \leftarrow (-1)^{(N-1)/2}$;

15. <u>If</u> $D \equiv 0, 2 \pmod 8$ then $X_8 \leftarrow (-1)^{(N^2-1)/8}$;

16. <u>If</u> $D \equiv 6 \pmod 8$ <u>then</u> $X_8 \leftarrow (-1)^{(N-1)/2 + (N^2-1)/8}$;

<u>end</u>

<u>THEOREM 4.4</u>

Algorithm 4.3 correctly computes the characters χ_{p_i} for each p_i odd prime divisor of D and χ_{-4}, χ_8, χ_{-8} when appropriate in $O(\log|D|M(\log|D|))$ elementary operations.

<u>Proof</u>

Lemma 4.1 shows that N has the required properties and Euler's criterion justifies the computation of the χ_{p_i}'s.

Since Q is reduced, steps 1-3 require $O(M(\log|D|)\log\log|D|)$ elementary operations. Steps 4-6 require at most $O(\tau)$, where τ is the number of distinct prime divisors of D. Since $\tau = O(\log|D|/\log\log|D|)$, steps 4-6 require $O(M(\log|D|))$ elementary operations.

Steps 7, 8 require τ multiplications at most and thus $O(M(\log|D|)\log|D|/\log\log|D|)$ elementary operations. Since Q is reduced, step 9 requires $O(M(\log|D|))$ elementary operations.

Step 11 requires $O(M(\log|D|))$ elementary operations and step 12 requires $O(\log p_i\, M(\log p_i))$ elementary operations. Hence loop 10-13 requires

$$O(M(\log|D|)\log|D|/\log\log|D| + \sum_{p|D} \log p\ M(\log p)) = O(\log|D|\ M(\log|D|))$$

elementary operations.

Finally steps 14-15 require only $O(M(\log|D|))$ elementary operations and the theorem follows. □

THEOREM 4.5

Suppose that χ is a genus character expressed in terms of the basis for genus characters specified in Theorem 4. For Q reduced form with determinant D, one can compute $\chi(Q)$ in $O(\log|D|\ M(\log|D|))$ elementary operations

Proof

Suppose that $\{X_i\}$ is the basis of genus characters and $\chi = \prod_i \chi_i^{\alpha_i}$ with $\alpha_i \in \{0, 1\}$. To compute $\chi(Q)$, compute $\chi_i(Q)$ for all the i's using algorithm 4.3 in $O(M(\log|D||\ \log|D|)$ elementary operations and afterwards compute the product of $\chi_i(Q)$'s in $O(\log|D|/\log\log|D|)$ elementary operations, since $\chi_i^{\alpha_i}(Q) = \pm 1$. □

Lagarias in [6] gave an algorithm for evaluation of $\chi(Q)$, which computes a form $Q' = (A, B, C)$ equivalent to Q such that $\gcd(A, 2D) = 1$ and thus $\chi(Q) = \chi(Q') = \chi(Q'(1, 0)) = \chi(A)$ and then evaluates $\chi(A)$ as in algorithm 4.3. Algorithm 4.3 has the same asymptotic complexity as Lagarias' algorithm in [6], but inspection readily shows that it runs faster by a constant factor.

ACKNOWLEDGEMENTS

My best thanks to my supervisor, Dr. Meurig Beynon, for his continuous help. Also thanks to Mrs.Josie Lloyd for typing this paper.

REFERENCES

1. DICKSON, L.E., "Introduction to the theory of numbers", Univ. of Chicago Press, Chicago, 1929.

2. GAUSS, C.F., "Disquisitiones Arithmeticae", 1801; English trans., Yale Univ. Press, New Haven, Conn. 1966.

3. ILIOPOULOS, C.S., "Analysis of an algorithm for composition of binary quadratic forms", J. Algorithms 2, (1982).

4. ILIOPOULOS, C.S., "Algorithms in the theory of integral binary quadratic forms", M.Sc. Thesis, Univ. of Warwick, (1981).

5. KNUTH, D., "Seminumerical Algorithms", Addison-Wesley, Reading, Mass. 1969.

6. LAGARIAS, J.C., "Worst-case Complexity bounds for Algorithms in the theory of quadratic forms", J. Algorithms 1, (1980).

7. MATHEWS, G.B., "Theory of Numbers", 2nd ed., Chelsea, New York, (1961),(reprinted).

8. PALL, G., "Some aspects of Gaussian composition", Acta Arithmetica,24 (1973), pp. 401-409.

9. VENKOV, B.A., "Elementary number theory", English trans. (by Alderson, H.), Wolters-Noordhoff publishing groningen, The Netherlands (1970).