CORRIGENDA

PHILIP RABINOWITZ, "Gauss-Kronrod integration rules for Cauchy principal value integrals," *Math. Comp.*, v. 41, 1983, pp. 63–78.

On p. 75, every occurrence of the superscript $\mu + 1/2$ in Eq. (68) and on line 11 should be changed to $\mu - 1/2$.

PHILIP RABINOWITZ

Department of Applied Mathematics
The Weizmann Institute of Science
76 100 Rehovot, Israel

G. DUECK & H. C. WILLIAMS, "Computation of the class number and class group of a complex cubic field," *Math. Comp.*, v. 45, 1985, pp. 223–231.

Carsten Eckhardt of Göttingen has pointed out that the algorithm to determine the structure of the Sylow p-subgroup S_p of the class group may only produce a subgroup of S_p. In all of the cases in which this algorithm was run we actually obtained S_p; hence, the results in Section 5 are not affected by this observation. Nevertheless, the complexity result given in the paper has not been proved. This difficulty can be overcome by first extending and improving Algorithm 4.1. We first note that we may assume that $|\Delta|$ is large enough so that $R > 1$ (see, for example, Cusick [1]).

We let $\mathfrak{h}_i$ $(i = 1, 2, \ldots, k)$ be k reduced ideals of $\mathcal{O}_K$ with periods $p_i = p^{\mu_i}$ $(\mu_i \in \mathbf{Z})$, where p is a prime. We put $P = p_1 p_2 \cdots p_k = p^{\mu}$. Given a reduced ideal $\mathfrak{j}$, our new algorithm will either determine t_i $(< p_i)$ $(i = 1, 2, \ldots, k)$ such that (4.1) holds or establish that no such set of t_i's exists. This algorithm executes in $O(\sqrt{PR}|\Delta|^{\epsilon})$ elementary operations. We note that if (4.1) holds, then

$$\mathfrak{j} \prod_{i=1}^{k} \mathfrak{h}_i^{p_i - r_i} \sim \prod_{i=1}^{k} (\mathfrak{h}_i^{m_i})^{q_i}, \tag{1}$$

where $t_i = m_i q_i + r_i$, $m_i \geq 0$, $0 \leq r_i \leq p_i$. When $m_i \neq 0$, we may assume that $r_i < m_i$ and $0 \leq q_i \leq t_i/m_i < p_i/m_i$. Given these bounds on r_i and q_i for a fixed set of values of the m_i's, we let C_1 and C_2 denote the number of ideal classes represented by the left-hand and right-hand side of (1), respectively.

When $P > R$, our approach will be to produce a sorted list J of the $C_1 \times O(R)$ reduced ideals that could be equivalent to the left-hand side of (1). We then determine whether any particular reduced ideal among the C_2 ideal classes represented by the right-hand side of (1) is in J. If none is, then (4.1) has no solution; if one is, then we can easily provide a solution of (1). The number of elementary operations needed to do this is $O(RC_1|\Delta|^{\epsilon}) + O(C_2|\Delta|^{\epsilon})$.

We consider two subcases. If $\sqrt{p} < 2\log_2(\tilde{h}+Y)$, find s (≥ 0) such that $p^s \leq \sqrt{pP/R}$ and $p^{s+1} > \sqrt{pP/R}$ and find n (≥ 0) such that

$$\lambda = \sum_{i=1}^{n} \mu_i \leq s \quad \text{and} \quad \lambda + \mu_{n+1} > s.$$

Put $\gamma = s - \lambda \geq 0$, $m_i = 0$ $(i = 1, 2, 3, \ldots, n)$, $m_{n+1} = p^\gamma$, $m_i = 1$ $(i = n+2, n+3, \ldots, k)$. In this subcase,

$$C_1 \leq m_{n+1} \prod_{i=1}^{n} p_i = p^s \quad \text{and} \quad C_2 \leq p^{-\gamma} \prod_{i=n+1}^{k} p_i = P/p^s.$$

Since $O(RC_1) = O(\sqrt{pPR}), O(C_2) = O(\sqrt{pPR})$, and $\sqrt{p} < 2\log_2(\tilde{h}+Y) < 2\log_2(h+2Y) = O(|\Delta|^\varepsilon)$, we see that we need to perform $O(\sqrt{PR}|\Delta|^\varepsilon)$ elementary operations.

When $\sqrt{p} > 2\log_2(\tilde{h}+Y) > 2\log h \geq 2k$, we put $\rho_i = \sqrt{(p/R^{1/\mu})^{\mu_i}} > 1$ and note that $\rho_1\rho_2\cdots\rho_k = \sqrt{P/R}$. If $M_i = [\rho_i]$ and $N_i = M_i + 1$, we get

$$\prod_{i=1}^{k} M_i < \sqrt{P/R} \quad \text{and} \quad \prod_{i=1}^{k} N_1 > \sqrt{P/R}.$$

Find the *least* value of n (≥ 1) such that

$$\prod_{i=1}^{n} N_i \prod_{i=n+1}^{k} M_i > \sqrt{P/R}.$$

Put $m_i = M_i$ $(i = 1, 2, \ldots, n)$, $m_i = N_i$ $(i = n+1, n+2, \ldots, k)$. Since $N_n/M_n < 2$, we have $\sqrt{P/R} < \prod_{i=1}^{k} m_i < 2\sqrt{P/R}$. Also, $C_1 \leq \prod_{i=1}^{n} m_i$ and

$$C_2 < \prod_{i=1}^{k}(p_i/m_i + 1) < \sqrt{PR}\prod_{i=1}^{k}(1 + m_i/p_i) < \sqrt{PR}\exp\left(\sum_{i=1}^{k} m_i/p_i\right).$$

Since $m_i/p_i < 2/(pR^{1/\mu})^{\mu_i/2}$ and $\sqrt{p} > 2k$, we have $\sum_{i=1}^{k} m_i/p_i = O(1)$.

Thus, in this subcase we need to perform $O(\sqrt{PR}|\Delta|^\varepsilon)$ elementary operations.

When $P < R$, we put $m_i = 0$ $(i = 1, 2, 3, \ldots, k)$. Here we have $C_1 \leq P$ and $C_2 = 1$. If we put $S = \sqrt{PR}$ and use Algorithm 2.1 in the manner suggested in the second case of Algorithm 4.1, we can determine whether or not (4.1) has a solution in

$$O(S|\Delta|^\varepsilon) + O(PR|\Delta|^\varepsilon/S) = O(\sqrt{PR}|\Delta|^\varepsilon)$$

elementary operations.

We also require a simple result from group theory. We let H be an abelian p-group such that

$$H = \langle g_1\rangle \times \langle g_2\rangle \times \cdots \times \langle g_k\rangle,$$

where $|\langle g_i\rangle| = p^{\mu_i}$. Consider g_{k+1}, where $|\langle g_{k+1}\rangle| = p^{\mu_{k+1}}$ and let G be the group $\langle H, g_{k+1}\rangle$. Let λ_{k+1} be the *least* nonnegative integer such that

$$g_{k+1}^{p^{\lambda_{k+1}}} = \prod_{i=1}^{k} g_i^{t_i}, \tag{2}$$

where $t_i = p^{\lambda_i} m_i, (m_i, p) = 1, 0 \leq \lambda_i < \mu_i$. If no such value of λ_{k+1} exists, then $G = H \times \langle g_{k+1} \rangle$; otherwise, let $\mu = \min\{\lambda_1, \lambda_2, \ldots, \lambda_{k+1}\}$ and put

$$g = \left(\prod_{i=1}^{k} g_i^{m_i p^{\lambda_i - \mu}} \right) g_{k+1}^{-p^{\lambda_{k+1} - \mu}}.$$

It is now a simple matter to prove the following

THEOREM. *If* $\mu = \lambda_{k+1}$, *then* $G = H \times \langle g \rangle$; *if* $\mu = \lambda_j$ $(j \neq k+1)$, *then* $G = \langle H_j, g_{k+1} \rangle \times \langle g \rangle$, *where*

$$H_j = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_{j-1} \rangle \times \langle g_{j+1} \rangle \times \cdots \times \langle g_k \rangle.$$

By using this theorem, it is easy to show that if $g_1, g_2, \ldots, g_m$ generate an abelian p-group S_p of order p^n, then we need to utilize $O(nm^2)$ determinations like (2) to find the group structure of S_p. Combining this with our algorithm above and the arguments used in the last paragraph of Section 4, we now see that algorithms for determining h and the class group structure can be developed which will execute in $O(|\Delta|^{1/5+\varepsilon})$ and $O(|\Delta|^{1/4+\varepsilon})$ elementary operations, respectively.

H. C. WILLIAMS

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba R3T 2N2, Canada

1. T.W. CUSICK, "Lower bounds for regulators," *Number Theory Noordwijkerhout 1983*, Lecture Notes in Math., vol. 1068, Springer-Verlag, Berlin, 1984, pp. 63–73.