Beschrijving Algoritmes

Roel Matthysen - October 16, 2012

The concept of optimal coefficients was introduced in [1], and their significance for the approximate computation of multidimensional integrals of arbitrary multiplicity s was indicated. Various algorithms for computing s-dimensional optimal coefficients modulo p where p is he number of nodes of the quadrature formula were obtained in [1]-[3]. The realization of these algorithms required the execution of $O(p^2)$ or $O(p^{1+1/3})$ elementary arithmetic operations.
In this note we present more economical algorithms for $p = 2^n$ whose realization requires the execution of $O(p)$ or $O(p \ln p)$ operations.
Let n and s be positive integers, and $x_1, ..., x_s$ odd integers. Summations over odd integers m is indicated by $\sum_m^*$. For $v = 1, ..., n$ we define the function $h_v(x_1, x_2, ..., x_s)$ by

$$h_v(x_1, x_2, ..., x_s) = \frac{1}{2^v} \sum_{m=1}^{2^v}{}^* \left(2n - 2v + \frac{1}{||mx_1/2^v||}\right) \cdots \left(2n - 2v + \frac{1}{||mx_s/2^v||}\right)$$

where $||mx_j/2^v||$ is the distance from $mx_j/2^v$ to the nearest integer.
Take $a_{11} = ... = a_{s1} = 1$. Suppose that $v \geq 2$ and that the odd integers $a_{1v-1}, ..., a_{sv-1}$ are known for $2 \leq v \leq n$ we define $a_{1v}, ..., a_{sv}$ by the equalities

$$a_{1v} = a_{1v-1} + 2^{v-1} z_1', ..., a_{sv} = a_{sv-1} + 2^{v-1} z_s'$$

where $z_1', ...z_s'$ are the variables at which the function

$$h_v(a_{1v-1} + 2^{v-1} z_1', ..., a_{sv-1} + 2^{v-1} z_s')$$

attains a minimum as the variables $z_1, ..., z_s$ run through the values 0 and 1 independently.

THEOREM 1. *For an arbitrary positive integer n the integer $a_1, ..., a_s$ defined by the equalities $a_1 = a_{1n}, ..., a_s = a_{sn}$ are optimal coeffecients modulo $p = 2^n$.*

Proof. For $v = 1, ..., n$ we introduce the notation

$$h_v = h_v(a_{1v}, a_{2v}, ..., a_{sv}).$$

$$H_v = \sum_{k=1}^{v-1} \sum_{m=1}^{2^k}{}^* \frac{1}{||ma_{1k}/2^k|| \cdots ||ma_{sk}/2^k||} + (2^{n+1} - 2^v) h_v.$$

De notatie h_v duidt rekening houdend met de definities hierboven op de waarde van het minimum van $h_v(a_{1v-1} + 2^{v-1} z_1', ..., a_{sv-1} + 2^{v-1} z_s')$

Observing that if $v \geq 2$, then

$$\frac{1}{2}\sum_{z=0}^{1}\frac{1}{||m(a+2^{v-1}z)/2^v||} \leq 2+\frac{1}{||ma/2^{v-1}||} \tag{1}$$

Dit is logisch omdat de maximale waarde van $1/||x||$ gelijk is aan 2. De maximale waarde van de som aan de linkerkant is dus gelijk aan 2, kleiner dan het rechterlid.

for odd a and m, we get

$$h_v \leq \frac{1}{2^s}\sum_{z_1,\ldots z_s=0}^{1} h_v(a_{1v-1}+2^{v-1}z_1, \ldots, a_{sv-1}+2^{v-1}z_s)$$

h_v is de waarde van het minimum, en is dus kleiner of gelijk aan de gemiddelde waarde van h_v. De som in het rechterlid kan dan opgesplitst worden in $\sum_{z_1,\ldots,z_s=0}^{1}\frac{1}{2}h_v(\ldots)$. Door alle paren samen te nemen die enkel verschillen in één z-waarde en (1) toe te passen

$$\leq \frac{1}{2^v}\sum_{m=1}^{2^v}{}^{*}\left(2n-2v+2+\frac{1}{||ma_{1v-1}/2^{v-1}||}\right)\cdots\left(2n-2v+2+\frac{1}{||ma_{sv-1}/2^{v-1}||}\right)$$

$2n-2v+2+\ldots$ wordt $2n-2(v-1)+\ldots$, en de termen voor $m=2^{v-1}+1, 2^{v-1}+3, \ldots$ zijn gelijk aan de termen voor $m=1,3,\ldots$. De sommatie valt dus uiteen in twee gelijke van $m=1..2^{v-1}$

$$= h_{v-1} \tag{2}$$

Since $a_{11}=\cdots=a_{s1}=1$, it follows that

$$h_1 = \frac{1}{2}\sum_{m=1}^{2}{}^{*}\left(2n-2+\frac{1}{||m/2||}\right)\cdots\left(2n-2+\frac{1}{||m/2||}\right) = 2^{s-1}n^s,$$

and, consequently, 2 gives us that

$$h_n \leq h_{n-1} \leq \cdots \leq h_1 \leq 2^{s-1}n^s$$

We now estimate the quantities H_v. Obviously,

$$H_1 = (2^{n+1}-2)h_1 = (2^n-1)2^s n^s < (2n)^s 2^n$$

Bij $v=1$ valt de sommatie uit de definitie van H_v weg.

Since

$$h_v = \frac{1}{2^v}\sum_{m=1}^{2^v}{}^{*}\left(2n-2v+\frac{1}{||ma_{1v}/2^v||}\right)\cdots\left(2n-2v+\frac{1}{||ma_{sv}/2^v||}\right)$$

we get for $v \geq 2$ that

$$\begin{aligned} H_v &\leq \sum_{k=1}^{v-2}\sum_{m=1}^{2^k}{}^{*}\frac{1}{||ma_{1k}/2^k||\cdots||ma_{sk}/2^k||} + 2^{v-1}h_{v-1} + (2^{n+1}-2^v)h_v \\ &\leq \sum_{k=1}^{v-2}\sum_{m=1}^{2^k}{}^{*}\frac{1}{||ma_{1k}/2^k||\cdots||ma_{sk}/2^k||} + (2^{n+1}-2^{v-1})h_{v-1} = H_{v-1} \end{aligned}$$

De eerste lijn volgt uit het weglaten van $k = v - 1$ uit de sommatie. De tweede lijn volgt dan uit het feit dat $h_v \leq h_{v-1}$. NOTA: mijns inziens zou de gelijkheid in de eerste lijn enkel opgaan in het geval $v = n + 1$. De tweede ongelijkheid komt wel voor uit de vorige resultaten.

and, consequently

$$H_n \leq H_{n-1} \leq \cdots \leq H_1 < (2n)^s 2^n \tag{3}$$

According to the definition of a_j and a_{jk},

$$a_1 \equiv a_{1k}, \ldots, a_s \equiv a_{sk} \pmod{2^k}$$

for $k = 1, \ldots, n$. But then it is obvious that

$$\sum_{m=1}^{2^n-1} \frac{1}{||ma_1/2^n|| \cdots ||ma_s/2^n||} = \sum_{k=1}^{n} \sum_{m=1}^{2^k}{}^{*} \frac{1}{||ma_1/2^k|| \cdots ||ma_s/2^k||}$$

$\frac{1}{2^n}, \frac{2}{2^n}, \ldots, \frac{2^{n-1}-1}{2^n} = \frac{1}{2}, \frac{1}{4}, \frac{3}{4}, \frac{1}{8}, \frac{3}{8}, \frac{5}{8}, \ldots$

$$= \sum_{k=1}^{n-1} \sum_{m=1}^{2^k}{}^{*} \frac{1}{||ma_{1k}/2^k|| \cdots ||ma_{sk}/2^k||} + \sum_{m=1}^{2^n}{}^{*} \frac{1}{||ma_{1n}/2^n|| \cdots ||ma_{sn}/2^n||} = H_n$$

De eerste gelijkheid volgt uit het afsplitsen van de term voor $k = n$. De eerste term past dan rechtstreeks in de definitie van H_n, de tweede term komt overeen met $(2^{n+1} - 2^n)h_n = 2^n h_n = \sum_{m=1}^{2^n}{}^{*} \frac{1}{||ma_{1n}/2^n|| \cdots ||ma_{sn}/2^n||}$

Hence by (3),

$$\sum_{m=1}^{2^n-1} \frac{1}{||ma_1/2^n|| \cdots ||ma_s/2^n||} < (2n)^s 2^n \tag{4}$$

NOTA: voor $m = 2^n$ wordt de noemer gelijk aan 0!

We determine b and $b_2, \ldots, b_s$ with the help of the congruences

$$a_1 b \equiv 1, a_2 b \equiv b_2, \ldots, a_s b \equiv b_s \pmod{2^n}$$

De vergelijkingen zijn altijd oplosbaar want a_i is oneven en dus inverteerbaar in de groep mod 2^n. NOTA: Dits is geen stelsel, nadat b bepaald is uit de eerste vergelijking kunnen alle b_i's afzonderlijk bepaald worden.

Then from (4) it follows that

Voor de functie $f(x) = ||x/2^n||$ geldt dat $x = x \pmod{2^n}$. In de groep mod 2^n is $b = a_1^{-1}$ een eenduidig bepaald oneven geheel getal. Vermenigvuldiging van de gehele getallen modulo 2^n met b levert een permutatie op van de gehele getallen modulo 2^n. In de sommatie 4 kan m overal vervangen worden door bm, enkel de volgorde van de sommatie wordt dan omgewisseld.

$$\sum_{m=1}^{2^n-2} \frac{1}{||m/2^n|| \cdot ||b_2 m/2^n|| \cdots ||b_s m/2^n||} < (2n)^s 2^n,$$

NOTA: Schrijffout? Volgens mij zou de sommatie moeten lopen tot $2^n - 1$.

$$\sum_{m=1}^{2^n-1} \frac{1}{m||b_2 m/2^n|| \cdots ||b_s m/2^n||} < (2n)^s,$$

Hier wordt gebruikt dat $m \geq 2^n ||m/2^n||$. In het geval $m \leq 2^{n-1}$ geldt $||m/2^n|| = m/2^n$, in het geval $m > 2^{n-1}$ geldt dat $m = 2^n - b$ met $b < 2^{n-1} < m$. Er geldt dan dat $||m/2^n|| = ||b/2^n|| = b/2^n < m/2^n$.

and consequently, for $m = 1, 2, \ldots, 2^{n-1}$

$$m \left\| \frac{b_2 m}{2^n} \right\| \cdots \left\| \frac{b_s m}{2^n} \right\| > \frac{1}{(2n)^s}.$$

Als de ongelijkheid geldt voor de som, geldt ze ook voor de termen apart aangezien alle termen positief zijn.

Since $p = 2^n$, we have that $2n < 3 \ln p$ and

$3 \ln p = 3n \ln 2 = 2,0974n$.

$$m \left\| \frac{b_2 m}{p} \right\| \cdots \left\| \frac{b_s m}{p} \right\| > \frac{1}{3^s \ln^s p}, \quad 1 \leq m \leq \frac{1}{2} p. \tag{5}$$

As shown in [1] (Corollary 2 of Theorem 7), the estimate (5) implies that if p is prime, then $1, b_2, \ldots, b_s$ and hence also $a_1, \ldots, a_s$, are optimal coefficients modulo p. This optimality condition is not hard to extend also to the case when p is a power of a prime number. But then the theorem obviously follows from (5). $\square$

References

[1] N. M. Korobov. Some problems in the theory of diophantine approximation. *Uspekhi Mat. Nauk.*, (135):83–118, 1967.