



为了得到 $T_0$ 和 $T_1$ 的特征值, 分裂过程可递归进行下去, 直到得到可使用QR等串行算法快速求解的小规模问题。图1给出了分而治之算法的任务树。

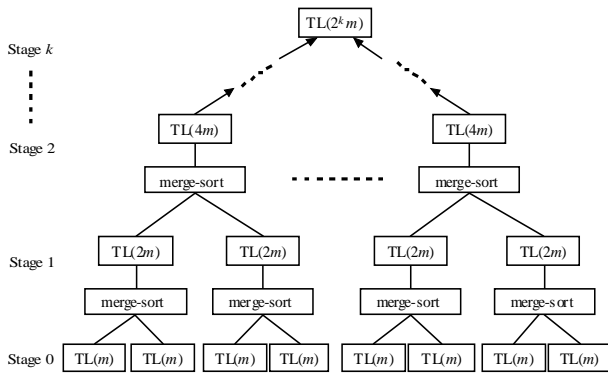


图1 D&C 算法任务树

## 2 MPI 并行算法

尽管分而治之算法逻辑上可看作树, 但树中的节点不能表示并行实现中的处理器, 否则将严重降低算法的并行性。设计并行算法的一个重要目标是使每个进程的计算时间最大化。根据这一原则, 下面给出了一个有效的 MPI 并行算法。

不失一般性, 设三对角矩阵 $T$ 的阶 $n=2^m$ , 处理器数量 $p=2^k$ ,  $s=m-k$ 。MPI并行算法描述如下:

置  $i=1$ , 然后执行下列操作。

第 1 步: 将 $n$ 阶三对角矩阵 $T$ 分解成 $p$ 个阶为  $2^s$  的子矩阵  $T_0, T_1, \dots, T_{p-1}$ , 并分布到处理器  $P_0, P_1, \dots, P_{p-1}$ 。每个处理器独立地计算子矩阵特征值。

第 2 步: 逻辑上将处理器按  $[P_0, \dots, P_{2^i-1}], [P_{2^i}, \dots, P_{2^{i+1}-1}], \dots, [P_{2^{k-1}}, \dots, P_{2^k-1}]$  分成  $2^{k-i}$  组, 每组包含  $2^i$  个处理器。(1) 各组处理器将最近计算的特征值传递给本组最左边的处理器(接收器)。(2) 该接收器对接收到的  $2^{i+s}$  个特征值合并、排序。(3) 接收器将排序后的特征值分发回本组内的所有进程。

第 3 步 (1) 每个处理器得到本组处理器需要处理的  $2^{i+s}$  阶子矩阵。(2) 以第 2 步接收到的  $2^s$  个特征值为初始点, 使用Laguerre迭代近似计算  $2^{i+s}$  阶子矩阵的  $2^s$  个特征值。(3) 置  $i=i+1$ , 若  $i=k$  结束, 否则转第 2 步。

上面算法第 2 步完成 MPI 进程间的消息传递, 这一过程在各进程组间并行进行。但随着  $i$  的增加, 每组中进程数成倍增加, 这使通信代价逐次变大。这样, 当使用的处理器数很大时, 将引起较大的通信开销。第 3 步各进程并行求解相同数量的近似特征值, 但由于求解不同近似特征值时迭代的次数可能不同, 这使该算法潜在地存在着负载不平衡问题。而上述问题是 MPI 并行算法所固有的, 将在混合并行算法中得到改善。

## 3 在 SMP 集群上的混合并行算法

给定一个有效的消息传递算法, 可使用增量过程设计一个有效的混合并行算法。

### 3.1 混合多级并行算法结构

由于 SMP 集群本身具有集群系统的分布存储和 SMP 系统的共享存储两级特性, 与此对应将混合并行算法的设计分解为机群级算法和节点级算法。在机群级算法设计时, SMP 集群系统被作为一个由节点构成的分布存储系统, 算法采用分布消息传递并行。但和纯 MPI 算法中每个处理器运行一个进程不同, 在机群级算法中每个进程映射为一个节点。节点

级算法也称为 SMP 算法, 将集群级算法中分配给每个节点的计算任务映射成一个有效的节点内多线程并行算法。本文的节点级算法基于 OpenMP 的多线程并行。

最简单的 OpenMP 并行是使用 OpenMP 工作共享结构的循环-嵌套并行, 每个线程独立地执行它的循环部分。这种并行又称为细粒度 OpenMP 并行。

另一种 OpenMP 并行称为粗粒度 OpenMP 并行。在粗粒度 OpenMP 并行中, OpenMP 采用 SPMD 并行编程模式, 每个线程本身类似一个 MPI 进程。线程功能的说明依赖库函数 `omp_get_num_threads()` 和 `omp_get_thread_num()`, 它们分别返回并行域内线程数量和执行线程的序号  $id$  (编号为 0 的线程为主线程)。其后根据它们的值对线程功能编码。不同的线程可执行相同或不同的操作, 这样实现了数据和任务的并行。

当将上面两种 OpenMP 并行同 MPI 结合在一起时, 可得到 MPI+细粒度 OpenMP 和 MPI+粗粒度 OpenMP 两种混合并行方式。

### 3.2 MPI+OpenMP 混合并行算法

考虑 $n$ 阶三对角对称矩阵 $T$ 在 $np$ 个 $r$ -路SMP节点上的特征值问题, 不妨设 $n=2^m$ ,  $np=2^d$ ,  $r=2^k$ , 所对应的处理器数量 $s=2^p=2^{d+k}$ 。

首先将上面的 MPI 并行算法直接转换为一个集群级算法。这时矩阵按节点个数分解成 $np$ 个阶为  $2^{m-d}$  的子矩阵并分布在各节点上。相应地, 循环变量 $i$ 对应的循环次数变为 $d$ 。这里将集群算法分为: Cphase1, Cphase2, Cphase3, 分别对应 MPI 算法中的第 1 步、第 2 步和第 3 步。图 2 给出了集群级算法结构。

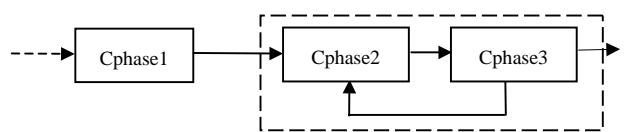


图2 集群级算法结构

为了得到混合并行算法, 须将集群算法中的 Cphase1 和 Cphase2 映射为节点内的 OpenMP 多线程并行。

(1) 映射 Cphase1 为 OpenMP 多线程并行

Cphase1 完成节点内  $2^{m-d}$  阶子矩阵的特征值求解。这类似于 MPI 并行, 需构造一个 OpenMP 粗粒度并行算法。将 Cphase1 在节点内的线程并行对应的各操作步表示为 Nphase1、Nphase2 和 Nphase3。对 Nphase1 而言, 由于节点内所有线程共享内存, 因此矩阵在线程间分解时, 需计算每个线程的数组范围, 并得到数组区域到线程的映射。而 Nphase2 是通过数据复制完成特征值的合并-排序和在线程间的散播, 从而避免了通信开销。在 Nphase3 中每个线程通过Laguerre迭代完成近似特征值的计算。

(2) 映射 Cphase3 为一个多线程的 OpenMP 并行

Cphase3 由节点内进程通过Laguerre迭代计算  $2^{m-d}$  个近似特征值。这对应着一个循环结构, 可使用 OpenMP 工作共享制由多个线程通过细粒度并行完成。在缺省调度(static)方式下, OpenMP 制导把循环均匀地分配给节点内所有线程(即节点内的处理器)。但由于Laguerre迭代在计算不同特征值的近似值时, 达到指定精度所执行的迭代次数可能不同, 这样上述的均匀分配将导致线程间的负载不平衡。为了改善负载平衡问题, 同时减少由同步引起的开销, 我们将循环在线程间的分配采用了 `schedule(dynamic, *)` 动态调度方式。类似地, 使用 Nphase 表示 Cphase3 的 OpenMP 并行。

在 Cphase2 中, 由每个进程中的主线程完成特征值的接收、发送以及特征值的合并和排序。这一过程发生在 OpenMP 并行域外。

图 3 给出了完整的混合并行算法结构。

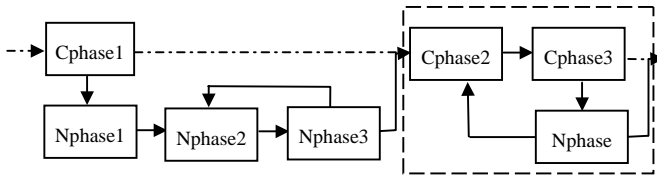


图3 混合并行算法结构

### 3.3 通信开销分析

在三对角矩阵特征问题的D&C并行算法中,外循环*i*的循环次数等于进程数*P*的对数 $\log_2 P$ 。对于含有*r*-路SMP节点的集群系统,混合并行算法的进程数等于节点个数*np*。而MPI并行算法的进程数等于处理器数,即 $np * r$ 。这样混合并行算法的*i*迭代次数仅为MPI算法迭代次数的 $\frac{1}{\log_2 r}$ 。这极大地减少了由Cphase2导致的进程间通信次数,降低了通信开销。

## 4 性能测试

我们通过深腾 6800 系统对混合并行算法和 MPI 算法进行了性能测试和比较。

### 4.1 深腾 6800 系统

深腾 6800 系统整体为 5 万亿次面向网格的超级计算机系统,包括 256 个四路节点。每个节点配置 4 颗 1.3GHz Itanium2 CPU,系统峰值速度为 5.3T Flop/s,内存总容量为 2.6TB。高速连接网络为 Qsnet,点到点通信带宽大于 300MB/s,延迟时间小于 7 $\mu$ s。深腾 6800 软件环境包括 Redhat Linux Advanced Server 2.1 操作系统,支持 OpenMP 制导的 Intel Fortran Compiler7.0 ,C/C++编译器,以及 Intel MPICH1.2.4 并行环境。

### 4.2 MPI 版本和 MPI+OpenMP 版本性能比较

这里仅给出对固定问题规模使用不同处理器在两种版本上的测试结果。测试矩阵为 Toeplitz 矩阵[1,4,1],矩阵规模是 40 000\*40 000。表 1 为纯 MPI 和混合 MPI+OpenMP 并行求解的运行时间。对于混合方式,分别测试了 2 线程和 4 线程的运行情况。而对于 4 个线程,分别给出了动态和静态两种调用方式下的运行时间。表 1 表明,在 4 种情况下,混合模式的并行性能都好于纯 MPI 并行。而在混合模式下,使用 4 线程的并行性能好于 2 线程。在 4 线程情况下,采用动态调度方法的并行性能又好于静态调度方法。并且它们之间的运行时间的差距随着处理器的增加变大。测试结果表明动态调度的多级混合并行算法具有更好的性能。

表 2 是对应的加速比。表中数值表明混合并行算法加速比明显好于 MPI 并行算法加速比。而对于混合并行算法,采用动态调用比静态调用具有更好的加速比。这说明使用动态调用的混合并行算法具有更好的可扩展性。

(上接第 2 页)

有所加重,但加重的部分完全可以通过预处理的办法一次性消除,总之,ESCS 方案所取得的优势是很明显的。

### 参考文献

- Pointcheval D, Stem J. Security Arguments for Digital Signatures and Blind Signatures[J]. Journal of Cryptology, 2000,13(3): 361-396.
- Adams C, Llyod S. Understanding Public Key Infrastructure[M]. New Riders Publishing, 1999.
- Lee B, Kim K. Self-certified Signature[C]. Proc. of Progress in Cryptology: INDOCRYPT'02, Lncs 2551. Springer-Verlag, 2002: 199-214.
- Girault M. Self-certified Public Keys[C]. Proc. of Advances in

表 1 纯 MPI 和 MPI+OpenMP 并行执行时间

节点数 (4-路 节点)	运行时间 (s)			
	纯 MPI	MPI+OpenMP (2 线程)	MPI+OpenMP 静态调度 (4 线程)	MPI+OpenMP 动态调度 (4 线程)
1	17.78	17.00	16.27	15.05
2	10.52	9.59	8.955	8.14
4	5.70	4.89	4.50	3.98
8	2.99	2.46	2.08	1.80
16	1.55	1.29	1.13	0.94
32	0.83	0.64	0.53	0.46

表 2 纯 MPI 和 MPI+OpenMP 并行加速比

节点数 (4-路 节点)	加速比			
	纯 MPI	MPI+OpenMP (2 线程)	MPI+OpenMP 静态调度 (4 线程)	MPI+OpenMP 动态调度 (4 线程)
1	1	1	1	1
2	1.69	1.72	1.72	1.97
4	3.12	3.15	3.34	3.52
8	5.95	5.99	6.79	7.37
16	11.45	11.55	13.94	14.70
32	21.53	21.89	28.97	31.58

## 5 总结

本文建立了一个求解对称三对角特征问题的多粒度混合并行算法,在 SMP 集群系统上得到了理想的并行性能。通过节点内使用共享内存并行模型,减少了通信开销。使用动态调度方式改善了负载平衡。实验表明混合并行算法比纯 MPI 算法具有更好的可扩展性。

### 参考文献

- Li T Y, Zeng Z. The Laguerre Iteration in Solving the Symmetric Tridiagonal Eigenproblem[J]. SIAM J. Science and Statistical Comput., 1994, 15(5): 1145-1173.
- Treffz C, Huanf C C. A Scalable Eigenvalue Solver for Symmetric Tridiagonal Matrices[J]. Parallel Computing, 1995, 21(8): 1213-1240.
- Henty D S. Performance of Hybrid Message Passing and Shared Memory Parallels for Discrete Element Modeling[C]. Proceedings of the 2000 ACM/IEEE Conference on Supercomputing, Dallas, Texas, United States, 2000.
- Bova S W, Breshears C, Cuicchi C, et al. Dual-level Parallel Analysis of Harbor Wave Response Using MPI and OpenMP[J]. Int. J. High Perform Comput. Appl., 2000, 14 (3): 49-64.
- Rabense R, Wellein G. Communication and Optimization Aspects of Parallel Programming Models on Hybrid Architecture[J]. International Journal of High Performance Computing Applications, 2003, 17(1): 49-62.

Cryptology: Eurocrypt'91, LNCS 547. Springer-Verlag, 1991: 490.

- Lee B, Kim K. Self-certificate: PKI Using Self-certified Key[C]. Proc. of Conference on Information Security and Cryptology, 2000: 65-73.
- Chadwick D. An X.509 Role-based Privilege Management Infrastructure[Z]. Business Briefing: Global Infosecurity, 2002.
- Schnorr C P. Efficient Signatures Generation by Smart Cord[J]. Journal of Cryptology, 1991, 4(3): 161-174.
- 杨义先, 孙伟, 钮心忻. 现代密码新理论(第 1 版)(M). 北京: 科学出版社, 2002-08.
- 杨义先, 钮心忻. 网络安全理论与技术(第 1 版)(M). 北京: 人民邮电出版社, 2003-10.