平成20年度 情報工学コース卒業研究報告要旨

石井（克） 研究室	氏　　名	浜 口 恵 輔
卒業研究題目	素数 p を用いた modulo による 多倍長計算の並列評価	

整数論に関係した問題や特殊な行列の逆行列を求める問題を正確に解くには多倍長演算のような非常に大きな精度を保つ計算が必要であり，必要な桁数が増えるほど，計算時間と使用するメモリ領域は莫大なものとなる．特に整数の問題に限ると素数 p より大きい整数が出てきた場合はこれを p で割った剰余を元の数値の代わりにして計算を行っていくことで計算時間，使用メモリをどこまでも単一精度のままにすることが可能である．そして複数の法 $p_0, p_1, \cdots p_n (p_i$ は素数 $(i = 0, 1, \cdots n))$ を用いることで真値 A の範囲が $0 \leq A < p_0 p_1 \cdots p_n$ であれば，真値を一意に求めることが可能である．1960 年頃にこのような手法が研究されており，この手法の中で複数の法中での計算は完全に独立しているため並列計算することにより，効率的に高精度計算が実行できると期待される．そこで本研究では現在主流となっている並列計算環境を用いて前述の手法の並列性能の評価を行った．

まず掃き出し法による逆行列の計算を浮動小数点型を用いた場合と法 p を用いた場合とで行い，計算結果から法 p を用いた計算での計算結果の正確性について評価を行った．計算を行った行列は要素の値は大きく隣の行の要素との差が極小なものを用い，浮動小数点型には 64bit のものを用いた．法 p = 18446744073709548859 である．それぞれ計算を行った結果，浮動小数点型の場合は 1E-2 の誤差が出たのに対し，法 p を用いた場合は正確に逆行列を求めることができ，法 p を用いた計算の正確性を示すことができた．

次に多倍長と法 p を用いた方法で掃き出し法による逆行列の計算を行い，時間の比較を行った．法 p = 4294967291 である．多倍長での実装は分母と分子に分け計算を行うことで計算結果が正確に求まるようにした．行列を n 次正方行列とすると，[多倍長の乗算時間] $\times (7n^2 - 5n) >$ [法 p を用いた方法での乗算時間] $\times (2n^2 + n) +$ [逆数計算時間] $\times n$ を満たす行列のサイズならば法 p を用いた方法の方が高速である．実際に計測を行った結果，多倍長の乗算時間（128bit × 128bit）が 4.89E-7 秒，法 p を用いた方法での乗算時間が 7.70E-8 秒，逆数計算時間 が 1.57E-6 秒となった．この結果を先程の式に当てはめると $n > 1$ となり，法 p を用いた方法の方が高速であることが分かった．実際に n=2 の場合の行列での計算時間を測定したところ，多倍長では 2.84E-5 秒，法 p を用いた方法では 9.54E-6 秒となり，n=2 以上の行列で多倍長よりも高速に計算できるということを示した．

最後に分散メモリ環境において法 p を用いた方法の並列性の評価を行った．全体の処理はルートプロセスが各プロセスへデータを渡し，各々のプロセスが法 p 表現へ変換，異なる法で計算を行い，計算結果をルートプロセスが収集し真値計算を行う．時間の計測を行うと，通信量 4Kbyte の 1 対 1 通信で 4.06E-5 秒となった．法の個数を n 個とし，通信に集団通信を利用すると通信時間は 4.06E-5 $\log_2 n$ となる．法 p の表現 (32bit) への変換時間は元の値が 128bit の場合 2.24E-6 秒となり，真値の計算時間は法 32 個の場合 1.96E-4 秒となった．乗算，逆数計算時間は逐次の場合と同じである．今回は 5×5 の行列の逆行列を求めることを考えると，逐次の多倍長と比較した場合は常に高速に処理を行うことができた．法の個数が 32 個以上の場合通信時間を隠蔽できるという結果を得た．実際に一つの要素が 512bit の整数値である 5×5 の行列の逆行列を法 32 個で計算した結果，処理時間は多倍長では 4.03 秒，法 p の逐次では 5.89E-3 秒，法 p の並列では 1.79E-3 秒となった．この結果から計算時間が通信時間を隠蔽し，並列効果が出ていることが分かり，法 p を用いた計算は並列計算に向いているこということを示した．