FUN-ECM プロジェクト

FUN-ECM Project

山本健太 石川夏樹 小野嘉翔 九島拓実 土田祐介 辻田陸

Kenta Yamamoto　Natsuki Ishikawa　Yoshiharu Ono　Takumi Kushima　Yusuke Tsuchida　Riku Tsujita

統計班

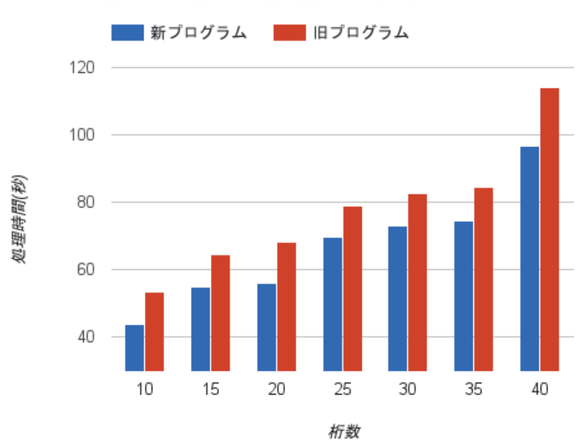
活動目的

本プロジェクトではECMNETへのランクインを目標に掲げている。そのためには100桁以上の数を扱い、またECMで非常に重要な加算公式を莫大な量(例えば57桁の素因数分解で200万回)を行うため、処理時間が非常にかかる。処理時間をいかに削減するかがECMNETランクインへのカギとなる。私たちは処理時間に着目し評価を行った。

活動内容

統計班は本プロジェクトで昨年度作成されたECMプログラムと今年度作成したECMプログラムの比較と評価を行った。各ECMプログラムで10～40桁の素数を入力した時の処理時間の比較を行った。その結果、今年度作成したECMプログラムの処理時間は昨年度作成されたECMプログラムよりもすべての桁数で処理性能の向上が確認された。向上率は平均して約15%、最大で10桁時に18%も上回った。この結果は射影班によって導入された射影変換によって削減された計算コストによる影響が非常に大きいと推測される。

図1 H27年度・H26年度のECMプログラムの桁数ごとの処理時間比較グラフ



活動成果

今年度のECMプログラムは昨年度のものよりも約15%処理時間が低減し、大きな桁を扱う場合でも結果が確認されるため、射影変換とエドワーズ曲線の導入は効果的であることが確認できた。

射影班

活動目的

ECMプログラムの高速化を図るために、ECMプログラムに射影変換を導入することにした。

射影変換とは

射影変換とは、乗算等の計算量は増えるものの、除算を行う回数を減らすことができる手法である。具体的には、座標平面上の点に対し、3つの変数用いて表現する手法である。

射影変換の効果

ECMでの除算は乗算に比べて約28倍ものコストがかかるため、除算を減らすことで全体の計算コストを減らすことが可能になるため、射影変換を導入した。乗算に対する逆元計算、2乗算のコスト比は、乗算をM、逆元計算をI、2乗算をSと置いたとき、I=27.5M、S=0.8Mとなる。ECMプログラム内の加算公式一回の計算コスト比は、昨年度射影変換前のプログラム:I+2M+S=30.3M、今年度射影変換前のプログラム:2I+6M=61M、昨年度射影変換後のプログラム:12M+2S=13.6M、今年度射影変換後のプログラム:11M+S=11.8Mとなる。今年度の射影変換後のプログラムは昨年よりも約15%もコストを削減することができた。

図2 加算公式 1 回分の計算コスト式

昨年度射影変換前	$: I + 2M + S$	$\approx 30.3M$
今年度射影変換前	$: 2I + 6M$	$\approx 61M$
昨年度完成版	$: 12M + 2S$	$\approx 13.6M$
今年度完成版	$: 11M + S$	$\approx 11.8M$

掛け算 (M): M

逆元計算 (I) $\approx 27.5M$

2 乗算 (S) $\approx 0.8M$

図3 加算公式 1 回分の計算コスト式

ヴァイエルシュトラス方程式: $y^2 = x^3 + ax + b$

$P = (x_1, y_1), Q = (x_2, y_2), P + Q = (x_3, y_3)$

$$\begin{aligned} \lambda &= \frac{y_1 - y_2}{x_1 - x_2} \\ x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$

除算をなくすことができる

エドワーズ曲線: $x^2 + y^2 = 1 + dx^2y^2$

$P = (x_1, y_1), Q = (x_2, y_2), P + Q = (x_3, y_3)$

$$\begin{aligned} x_3 &= \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2} & x_1 &= \frac{X_1}{Z_1}, y_1 = \frac{Y_1}{Z_1} \\ y_3 &= \frac{y_1y_2 + x_1x_2}{1 - dx_1x_2y_1y_2} & x_2 &= \frac{X_2}{Z_2}, y_2 = \frac{Y_2}{Z_2} \\ & & x_3 &= \frac{X_3}{Z_3}, y_3 = \frac{Y_3}{Z_3} \end{aligned}$$

$$\begin{aligned} X_3 &= Z_1Z_2(X_1Y_2 + Y_1X2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2) \\ Y_3 &= Z_1Z_2(Y_1Y_2 + X_1X2)(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2) \\ Z_3 &= (Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2) \end{aligned}$$

新たに導入した楕円曲線

今年度のECMプログラムでは昨年のECMプログラムで使用していたヴァイエルシュトラス方程式から、エドワーズ曲線に変更した。エドワーズ曲線ではヴァイエルシュトラス方程式より射影変換の恩恵をより多く得られる。

活動成果

射影変換とエドワーズ曲線の導入により、従来の15%のコスト削減に成功した。