問題適合型高精度計算ライブラリの開発

プロジェクト代表:
長谷川秀彦@筑波大学図書館情報メディア研究科

発表者:
後 保範@早稲田大学

プロジェクトの目的

- 計算誤り検証付きライブラリの開発
- RAS 暗号(1024ビット)の強度推定: 発表
- 自動チューニング機構付き線形計算ライブラリの開発
- 精度保証付き線形計算ライブラリの開発
- ４倍精度線形計算ライブラリの開発

RAS 暗号の強度推定の計画

- 初年度(発表年度)

  RSA暗号ふるい処理の高速化と評価
- ２年度（予定）

  RSA暗号処理プログラムの作成と高速化
- ３年度（予定）

  現1024ビットRSA暗号の強度推定

RAS 暗号の強度推定の背景

(1) 現在の暗号 (RSA暗号)や認証システムは多数桁数(1024ビット,10進309桁)の因数分解の困難さを利用している。

(2) 現在の多数桁数の因数分解の世界記録は、RSA-768(10進232桁)。2010年1月、NTT他5カ国共同、GNFSを使用。

(3) 「暗号の2010年問題」:RSA暗号を含む現在の暗号システムの変更が必要

現在の暗号方式(ハイブリッド暗号)

(1) 公開鍵暗号方式: 秘密鍵の送付が不要
公開鍵で暗号化、秘密鍵で復号化
認証やネットワーク通信に都合が良い
RSA暗号 : 多数桁数因数分解の難しさを利用

(2) 秘密鍵暗号方式(共通鍵): 公開鍵より高速
暗号化と復号化で共通の秘密鍵を使用
代表暗号例: RC4(Netscape)、TLS 1.0

RSA768(232桁)の計算時間

項目	台数･年	比率(%)
ふるい処理	1500	90
0-1行列計算	155	9
利用関数の探査	20	1
代数平方根の計算	1	0
その他	1	0

注) AMD64 (2.2Ghz, 1コア換算)
行列サイズ : 192,796,550 * 192,795,550

代表的なRSA暗号のふるい法

(1) QS (Quadratic Sieve、2次ふるい法)
MPQS (Multiple Polynomial QS,
複数多項式2次ふるい法)が代表的解法
100桁以下ではGNFSより高速な解法

(2) GNFS (General Number Field Sieve、
一般数体ふるい法)。現在、100桁程度以上で最も高速な解法と言われている。

ふるいプログラム(中心部)

```
do 20 k=1,N          :基底数          開始位置(割れる)
      do 10 i=NPL(2,k),LP,NPL(1,k)      :k番目素数
10      V(i) = V(i) + PV(k)     元は乗算(対数で加算)
20 continue
    do 30 i=1,LP        ＜ふるいデータの採取＞
      if( V(i) .ge. PS(i) ) then  累計が基準以上で採用
        ns = ns + 1                ふるいで得たデータ数
        sieve(ns) = LLP + i    取得データのトータル番号
      end if
30 continue
```

次のふるいのため、NPL(2,1)～NPL(2,N)の更新

ふるい処理の特徴

- PC(キャッシュ処理のパソコン)
  高速化のためにはキャッシュ内処理が必須
  LPのサイズはベクトルより数千倍短い
  少し大きな素数(基底)ではLPをはみ出す
- ベクトル計算機(地球シミュレータ(ES))
  LPのサイズはPCの数千倍長く取れる
  ふるいデータの採取(do 30)が遅くネック

注) LP: 1回のふるい処理での配列長

ES2対策(データ採取部分)

- 条件一致(採取)は少ない(1/百万～1/数百億)の特性を利用
- 数万件単位に、基準値を引いた最大値を求める。
- 求めた最大値が正の場合にだけデータ採取処理を行うように変更
- ES2では64K(65,536)単位
- 本対策で、ふるい全体で約3倍の性能向上

ふるい処理の評価法

- 10進m桁からの値を、小さい方からN個の素数基底でのふるい処理で評価

  MPQS：平方剰余となる素数を基底に使用(半分)

  GNFS：イデアル分解(処理の基本は素数基底と同じ)と全素数での基底分解

- ふるいでN個のデータが得られるまでの時間を測定

  通常のふるい処理では、同じ素数(イデアル)のデータが2件得られたら、基底に追加し、処理を短縮。評価を単純化するため、基底の追加はしない。

ふるい測定結果の比較

- PC(1コア)とベクトル計算機(1ノード)で比較
- PC (CPU時間で測定)

  Dell Vostro 200 (Intel Core 2, 2.33Ghz, 2GB)

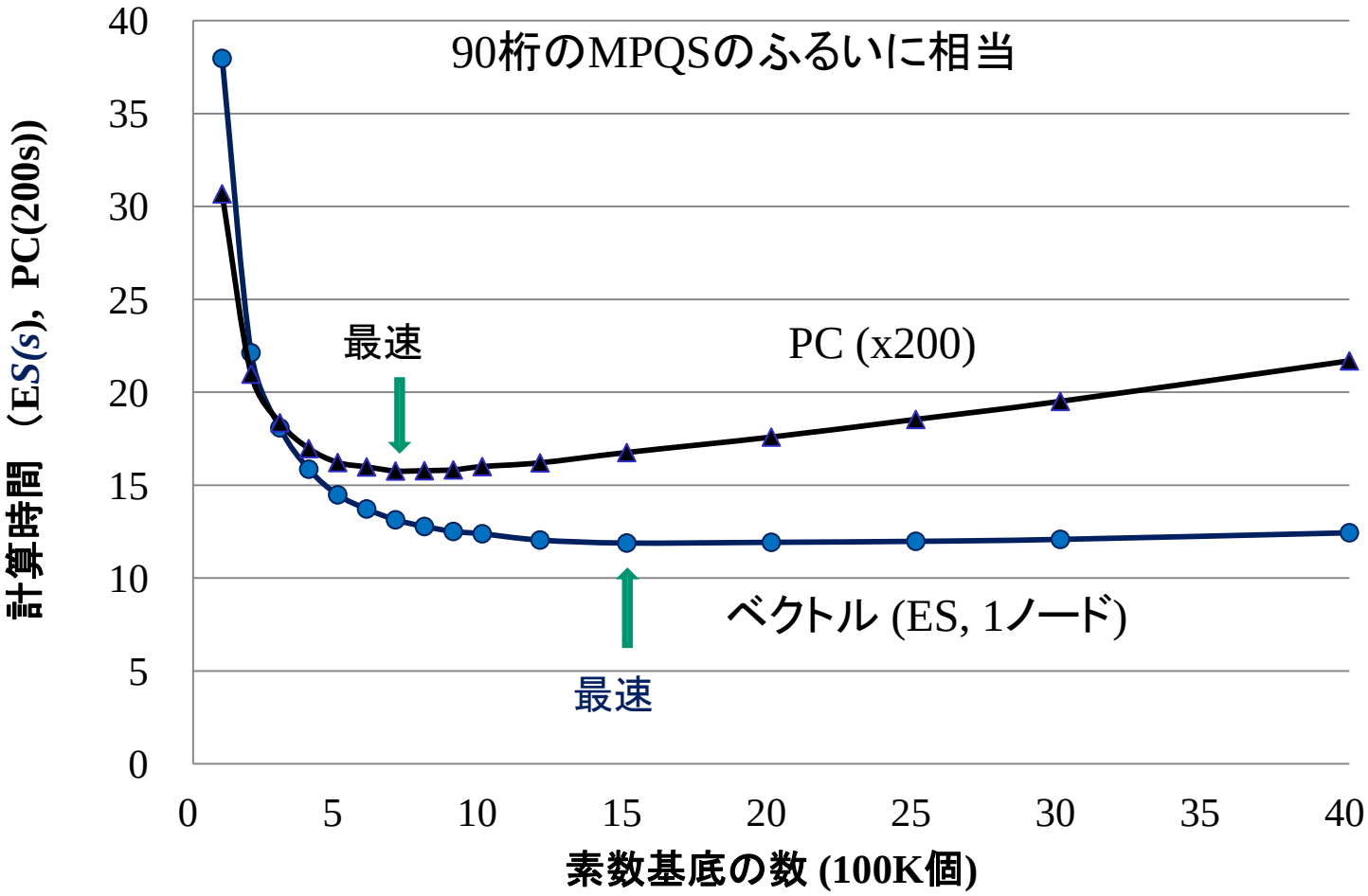
  Windows Vista, g77, -O3オプション
- ベクトル計算機 (経過時間で測定)

  地球シミュレータ (ES2, 1ノード8cpu)

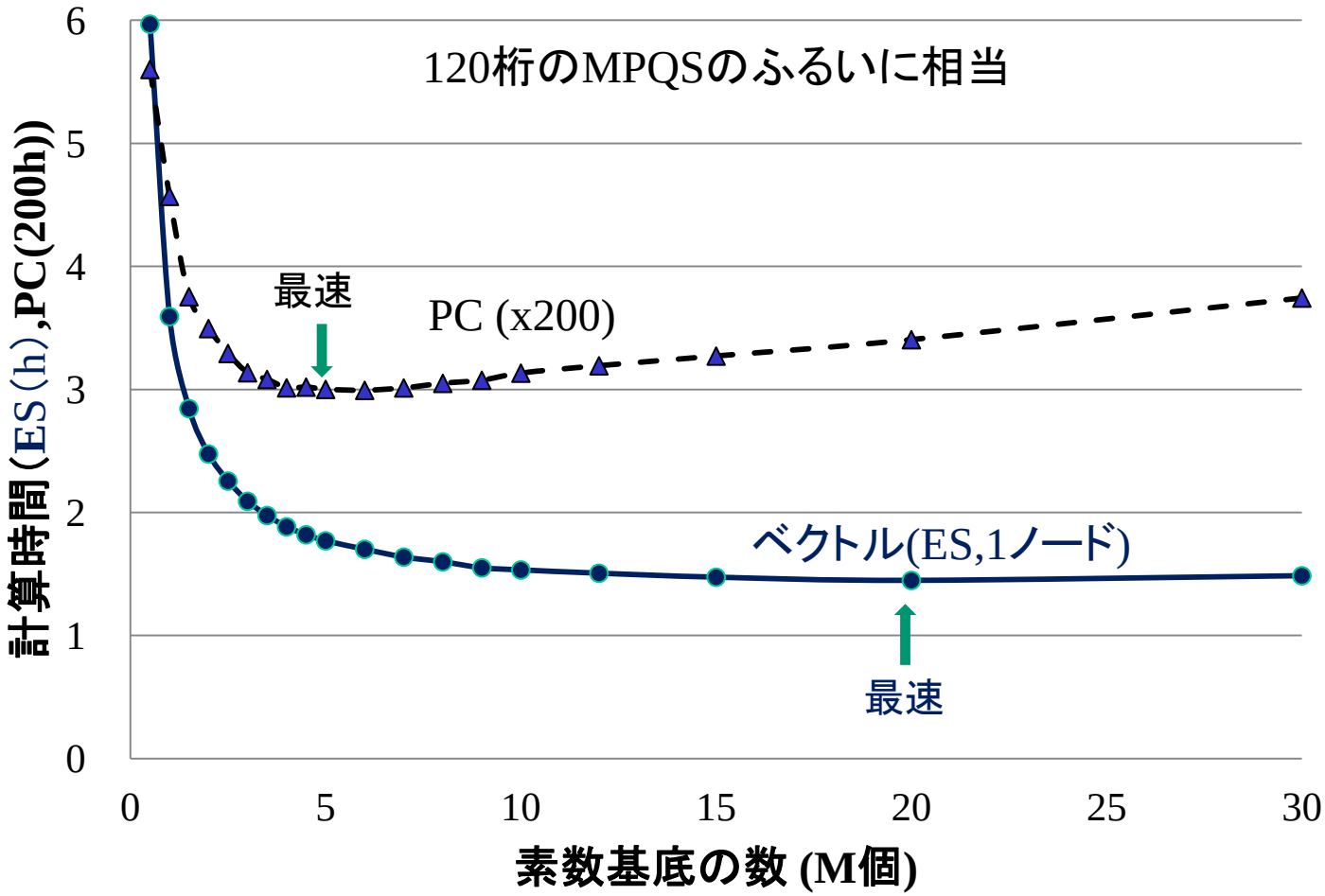
  3.2Gh, 1ノード: 819Gflops, 128GB

  SUPER-UX, 自動ベクトル化FORTRAN+MPI

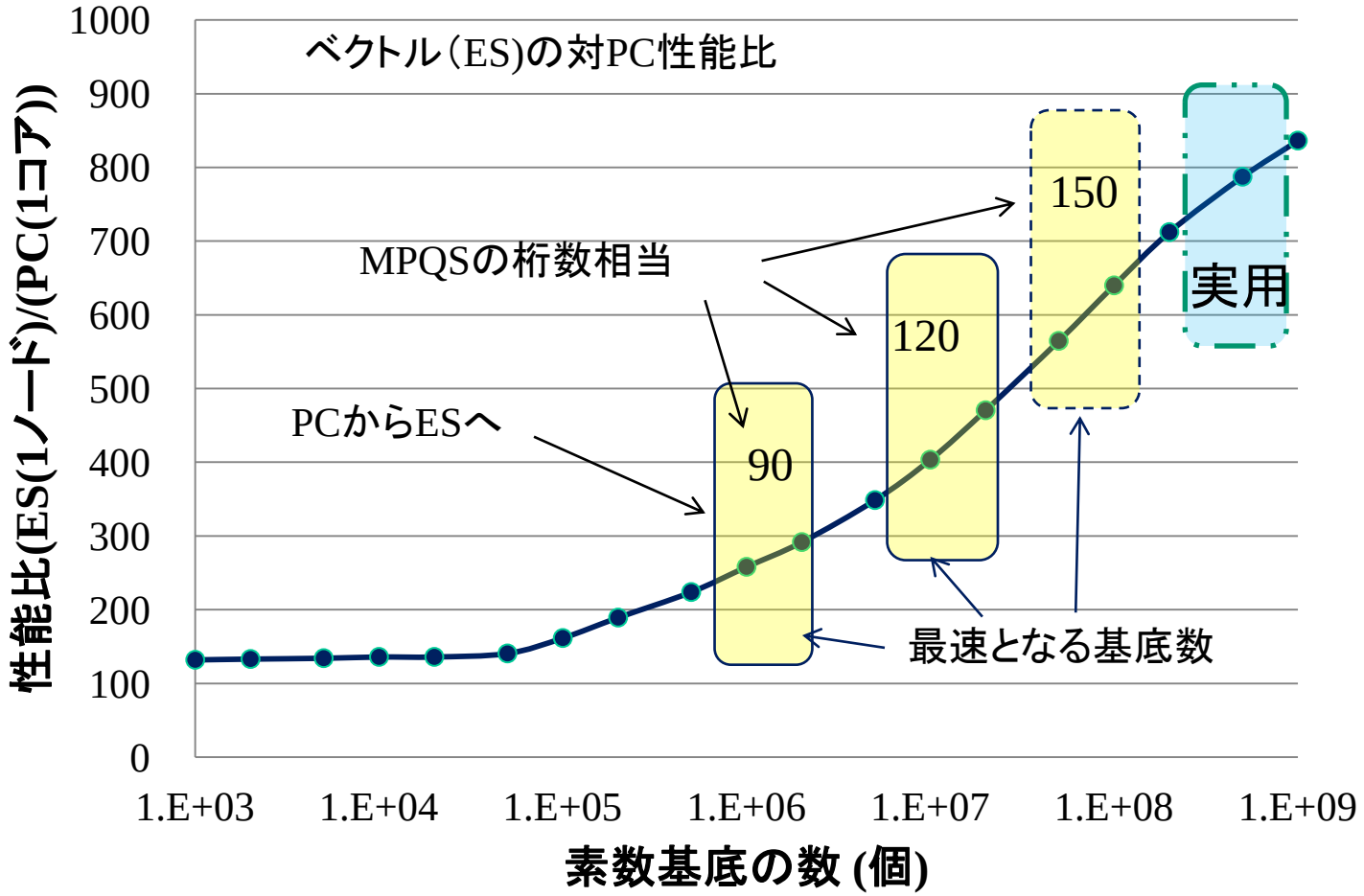
ふるい計算時間(10進45桁)



ふるい計算時間(10進60桁)



ふるいの性能比較


ベクトル(ES)の対PC性能比
性能比(ES(1ノード)/(PC(1コア))
1000
900
800
700
600
500
400
300
200
100
0
1.E+03
1.E+04
1.E+05
1.E+06
1.E+07
1.E+08
1.E+09
素数基底の数 (個)
MPQSの桁数相当
PCからESへ
90
120
150
実用
最速となる基底数

ふるい処理の評価まとめ

- ふるい処理のPC(2.33Ghz)とES2(1ノード)の性能比は200倍～800倍程度
- 分解対象桁数が大きくなると、性能比も大きくなる。実用規模(桁数)では約800倍
- データ採取部に特性を生かした対策を行うことで、処理全体を約3倍高速化できた
- 同じ桁数の分解では、基底の数はPCよりES2の方が大きく、最適な範囲が広い