1. $I = 1$, $t = n$.
2. Если $q_1 = 1$, то $t = t - 1$,
   иначе $I = I + r_{t-1} + (q_1 - 2)r_{t-2}$, $t = t - 2$.
3. $i = 1$.
4. Если $i = n$, то переход в п. 6,
   иначе если $q_i = i$, то $t = t - 1$ и переход в п. 5,
   иначе если $q_i > i$, то $I = I + r_{t-1} + (q_i - n + t - 1)r_t$, $t = t - 2$ и переход в п. 5.
5. $i = i + 1$ и переход в п. 4.
6. I — результат.

Приведённые алгоритмы реализованы программно на языке Си++ с использованием процессора Intel(R) Pentium(R) 4CPU, работающего с частотой 300 ГГц. В таблице приведено усреднённое по 10000 случайных примеров время работы алгоритмов для $25 \leqslant n \leqslant 31$.

n	Время работы алгоритма 1, с	Время работы алгоритма 2, с
25	0,0055	0,001261
26	0,008729	0,001902
27	0,013972	0,0032
28	0,022783	0,005199
29	0,037049	0,008263
30	0,057267	0,013038
31	0,091838	0,021003

ЛИТЕРАТУРА

1. *Тимошевская Н. Е.* Разработка и исследование параллельных комбинаторных алгоритмов // Прикладная дискретная математика. 2009. № 2(4). С. 96–103.
2. *Андреева Л. Н.* К криптоанализу инволютивных шифров инволюционной подстановки // Вестник Томского госуниверситета. Приложение. 2005. № 14. С. 43–44.

УДК 519.61

ОТСУТСТВИЕ ДИНАМИЧНОСТИ У МЕТОДА РЕШЕТА ЧИСЛОВОГО ПОЛЯ

Ю. Л. Зачёсов, А. М. Гришин

Под динамичностью метода будем понимать способность сохранять свои основные характеристики при существенном изменении входных параметров. Основными характеристиками являются трудоёмкость выполнения алгоритма, ограничения на требуемые вычислительные ресурсы и другие параметры. Характеристика входных параметров — это, как правило, их длина.

На сайте [1] можно найти данные об изменении трудоёмкости выполнения этапов алгоритма факторизации методом квадратичного решета [2] и NFS [3] с 1990 г. в зависимости от размера модуля факторизации. По представленным данным видно, что рассматриваемые алгоритмы требуют для своего выполнения существенных вычислительных ресурсов. Трудоёмкость выполнения алгоритма измеряется в MIPS years или в 1 ГГц CPU years. На сайте [4] можно посмотреть динамику изменения характеристик лучших мировых суперкомпьютеров. Их мощность измеряется в TFlop/s. Для того чтобы можно было сравнивать предлагаемые ресурсы и потребность в них алгоритмов, переведём всё в оценки, измеряемые в 10^k условных операций в секунду (опер/с),

умножая данные из таблиц на $31{,}536 \cdot 10^{12}$ для MIPS years, на $31{,}536 \cdot 10^{15}$ для 1 ГГц CPU years ($\approx 10^9$ — средняя производительность одного процессора Pentium) и на 10^{12} для максимальной полученной производительности по LINPACK в TFlop/s.

Результаты интерполяции и экстраполяции данных представлены на рис. 1 и 2. Видно, что рост производительности суперкомпьютеров отстаёт от роста трудоёмкости алгоритма NSF при увеличении размера его входных данных.

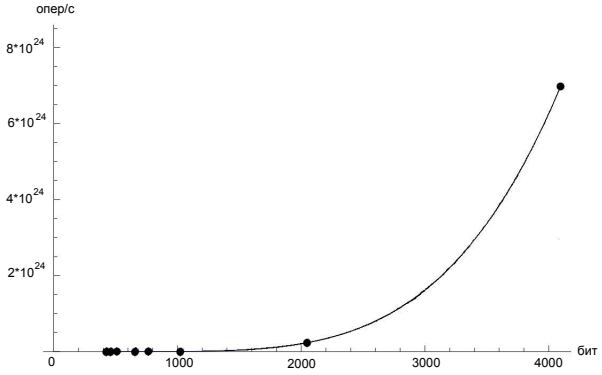

Рис. 1. Рост трудоёмкости алгоритма NSF в зависимости от размера модуля

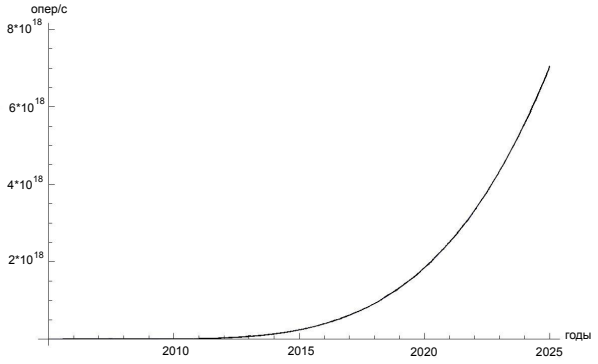

Рис. 2. Предполагаемый рост производительности суперкомпьютеров

Экстраполяция данных трудоёмкости алгоритма NFS при возрастании модуля факторизации и производительности будущих суперкомпьютеров показывает отсутствие динамичности метода NFS.

Так, трудоёмкость факторизации 2048-битного модуля (значение модуля выбрано как далёкое от последних рекордных) стремится к 10^{23} опер/с, в то время как производительность перспективного суперкомпьютера предположительно будет составлять в 2025 г. от 10^{18} до 10^{19} опер/с.

Напрашивается вывод, что примерно с 768-битного модуля метод решета числового поля теряет свою динамичность.

ЛИТЕРАТУРА

1. Информационное сообщение о рекордных факторизациях различных модулей RSA. `http://www.crypto-world.com/FactorRecords.html`.
2. *Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В.* Введение в теоретико-числовые методы криптографии. М.: Лань, 2011. 395 с.
3. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2006. 333 с.
4. Официальная страница Top500. `http://www.top500.org/`.

УДК 519.254

ТОЧНОЕ ВЫЧИСЛЕНИЕ РАСПРЕДЕЛЕНИЙ С ПОМОЩЬЮ ЦЕПЕЙ МАРКОВА

А. М. Зубков, М. В. Филина

Для построения статистических критериев с заданными вероятностями ошибок требуется знание распределений используемых в этих критериях статистик. Как правило, точные формулы слишком громоздки с вычислительной точки зрения. Поэто-