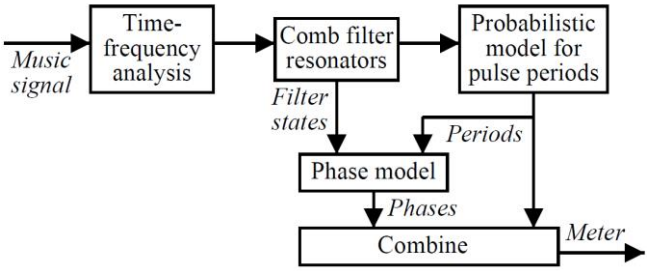

Рис. 1 – Схема построения ритмической картины по алгоритму А.Клапури

Список использованных источников:

1. F. Gouyon, S. Dixon, “A review of automatic rhythm description systems,” *Computer Music Journal*, vol. 29, no. 1, pp. 34–54, 2005.
2. M. Alonso, B. David, and G. Richard, “Tempo and beat estimation of musical signals,” in Proc. International Conference on Music Information Retrieval. Barcelona: Audiovisual Institute, Pompeu Fabra University, 2004, pp. 158–163.
3. S. Dixon, “Automatic extraction of tempo and beat from expressive performances,” Journal of New Music Research, vol. 30, no. 1, pp. 39–58, 2001.
4. E. Scheirer, “Tempo and beat analysis of acoustic musical signals,” J.Acoust. Soc. Am., vol. 103, no. 1, pp. 588–601, 1998.
5. Klapuri, A. Eronen, and J. Astola, “Analysis of the meter of acoustic musical signals,” IEEE Trans. Speech and Audio Processing, 2005.
6. G. Tzanetakis and P. Cook, “Musical genre classification of audio signals,” IEEE Trans. Speech and Audio Processing, vol. 10, no. 5, pp. 293–302, 2002.
7. C. Uhle, J. Rohden, M. Cremer, and J. Herre, “Low complexity musical meter estimation from polyphonic music,” in Proc. AES 25th International Conference. New York: Audio Engineering Society, 2004, pp. 63–68.
8. F. Gouyon, A. Klapuri, S. Dixon, M. Alonso, G. Tzanetakis, C. Uhle, P. Cano, "An experimental comparison of audio tempo induction algorithms" , IEEE Transactions on Speech and Audio Processing, 14(5), 2006.

ФАКТОРИЗАЦИЯ ЧИСЛА ПОСРЕДСТВОМ МОДИФИЦИРОВАННОГО АЛГОРИТМА ШОРА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Кухарчук И. В.

Самаль Д. И. – к-т техн. наук, доцент

Процедура факторизации широко используется в современной криптографии, однако, на сегодняшний день нет эффективных высоких нижних оценок сложности этих алгоритмов. Вопрос о существовании алгоритма факторизации с полиномиальной сложностью на классическом компьютере является одной из важных открытых проблем современной теории чисел. В то же время факторизация с полиномиальной сложностью возможна с использованием квантовых компьютеров, однако существуют определённые технические сложности построения систем с достаточным количеством кубитов для обеспечения приемлемой точности вычислений.

Для решения поставленной задачи нет необходимости в реализации всего алгоритма факторизации при помощи квантовых вычислений, так как это приведёт к несоизмеримому увеличению сложности алгоритма в сравнении с приобретённой скоростью вычисления. Поэтому в нашем случае весь алгоритм разбит на две части: подготовительная часть исполняется на классическом компьютере, а ядро – с учётом специфики квантовых вычислений.

Суть алгоритма факторизации Шора заключается в сведении задачи факторизации к задаче поиска периода функции, так как в случае, если известен период функции, то факторизация осуществляется при помощи алгоритма Евклида за полиномиальное время на классическом компьютере.

Необходимо учитывать то обстоятельство, что алгоритм нахождения периода функции вероятностный, а это в свою очередь требует ввода дополнительных операций по верификации полученного периода на соответствие требованиям достаточности. В нашем случае этими требованиям является чётность полученного периода и проверка на корректность решения путём произведения полученных множителей и сравнение результата с начальным значением. В случае если найденное значение не удовлетворяет требованию, существует необходимость повторного запуска алгоритма поиска периода.

Функция, для которой производится поиск периода, как правило, имеет следующий вид:

$$f(x) = a^x \pmod{M}$$

В приведённой формуле a – некоторый параметр, выбираемый произвольно до старта алгоритма (обычно этим параметром является число 2), M – число, которое необходимо факторизовать. Основным ограничением для данных выбранных параметров является отсутствие у них общих делителей, больших 1.

Согласно алгоритму следующим шагом является выбор необходимого количества кубитов для получения конечного результата с учётом сработавшей конструктивной интерференции. Автор данного алгоритма предлагает использовать следующую формулу для расчёта необходимого количества кубитов:

$$M^2 \le 2q < 2M^2$$

Однако часто в результате применения данной формулы к выбору подходящего количества кубитов возникает проблема необходимости уменьшения их количества ввиду отсутствия технической возможности работать с данным количеством кубитов. Поэтому предлагается использовать следующую формулу для выбора необходимого количества кубитов:

$$M^2 \le 4(qw + qs) < 2M^2$$

В данной формуле qw – количество основных кубитов, а qs – количество вспомогательных. Причём согласно этой формуле количество вспомогательных кубитов предлагается выбирать из расчёта максимальной вместимости значения потенциально найденного периода функции.

Основная вычислительная часть реализована при помощи квантового преобразования Фурье, имеющего следующий вид:

$$A(m,n) = e^{-2\pi i \frac{(m-1)(n-1)}{N}}$$

Гейт для квантового преобразования Фурье реализуется при помощи формулы Эйлера, которая используется с целью упрощения реализации алгоритма.

Особенностью алгоритма Шора является то, что полученный результат в процессе измерения является приближением к реальному значению. Поэтому для получения конечного ответа на поставленную задачу необходимо использовать специальные алгоритмы обработки полученных результатов в процессе вычисления. Для повышения результирующей точности использовался квантовый вариационный метод Монте-Карло. С целью использования вышеуказанного метода необходимо производить определённое количество измерений. Общая статистическая картина редко разнится со временем измерения, так что единожды произведя множественные измерения можно построить общую диаграмму, на основе которой сделать выводы и обосновать выбор критериев для работы алгоритма.

На следующей диаграмме представлены результаты запусков реализованной программы с использованием языка программирования Quipper в пределах интервалов [1..50] для количества вызова алгоритма и [1..6] для количества вызова квантовой подпрограммы.

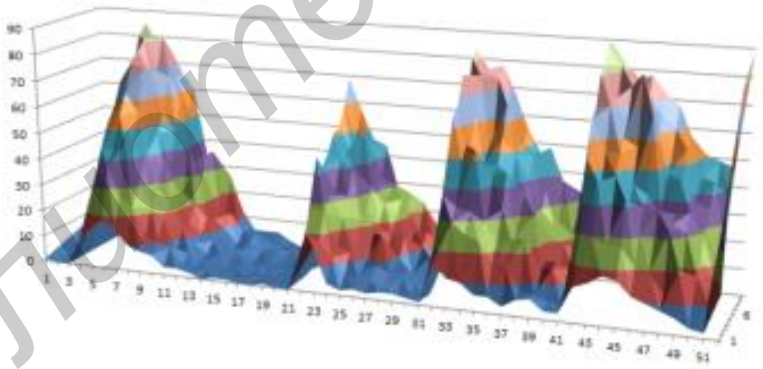

Рис. 1 – Результаты полученных измерений в зависимости от количества запусков основного алгоритма и квантовой подпрограммы

Данное двукратное уменьшение количества кубитов приводит к ~30% потере точности вычисления, однако при использовании корректирующих алгоритмов удаётся достичь лишь 10% потерь.

Список использованных источников:

1. Валиев К. А. Квантовые компьютеры. Надежды и реальность / К. А. Валиев, А. А. Кокин // Уч. метод. пособие для студентов радиотехнических специальностей. – Ижевск, 2001. – 352 с.
2. Душкин, Р. В. Квантовые вычисления и функциональное программирование / Р. В. Душкин // Уч. метод. пособие для студентов радиотехнических специальностей. – Москва, 2014. – 318 с.