Рецензия на статью И.В.Латкина и А.В.Селиверстова «О вычислениях над упорядоченными кольцами»

Статья может быть рекомендована к публикации в журнале «Сибирские электронные математические известия» после доработки. Список замечаний и пожеланий см. ниже.

Статья посвящена исследованию сложности вычислений некоторых алгоритмических проблем над некоторыми упорядоченными кольцами с операцией взятия остатка. В частности рассматриваются кольца целых чисел $\mathbb{Z}$, декартово произведение бесконечного числа $\mathbb{Z}$ и ультрастепень $\mathbb{Z}$. Изучается сложность вычисления наибольшего общего делителя, неполного общего частного, а также возможность решения классической NP-полной проблемы о сумме подмножества за полиномиальное время над бесконечной декартовой степенью $\mathbb{Z}$. Последний результат, по мнению рецензента, является наиболее интересным.

Список замечаний и пожеланий по улучшению текста:

1. Введение малоинформативно. Создается впечатление, что исследования по вычислимости и сложности вычислений в алгебраических системах, отличных от кольца $\mathbb{Z}$, ограничиваются статьей Ньюмана и Паули 2018 года и статьей Блюм, Шуба и Смейла 1989 года. В промежутке между 1989 и 2018 годами появилось много работ по данной тематике многих авторов: Ю.Л.Ершов, С.С.Гончаров, А.С.Морозов, Л.Блюм, М.Шуб, С.Смейл, Ф.Кукер, К.Меер, П.Койран, А.Хеммерлинг, А.Г.Мясников, В.Я.Беляев, И.В.Ашаев, А.Н.Рыбалов, М.Прунеску и др. Исследования по сложности вычислений были сконцентрированы в основном вокруг переноса классической теории NP-полноты на произвольные алгебраические системы и вокруг проблем разделения различных классов сложности – типа проблемы $P \neq NP$. Кроме модели Блюм-Шуба-Смейла для изучения сложности вычислений над алгебраическими системами используются S-машины (А. Хеммерлинг) и машины над списочной надстройкой (Ашаев-Беляев-Мясников). Обобщенные регистровые машины, используемые авторами данной статьи, по-видимому являются моделью, эквивалентной вышеупомянутым.

   Список работ по сложности вычислений над алгебраическими системами, которые можно добавить в библиографию:

   (a) Blum L., Cucker F., Shub M., Smale S. Complexity and Real Computation. Springer, 1998.

   (b) Hemmerling A. Computability and complexity over structures // Math. Logic Quarterly, 44, No.1, pp. 1–44, 1998.

   (c) Koiran P. Computing over the reals with addition and order // Theoretical Computer Science, 133, pp. 35–47, 1994.

   (d) Gaßner C. The $P - DNP$ problem for infinite abelian groups // Journal of Complexity, 17, pp. 574–583, 2001.

(e) Meer K. A note on $P \neq NP$ – result for a restricted class of real machines // Journal of Complexity, 8, pp. 451–453, 1992.

(f) Prunescu M. $P \neq NP$ for all infinite Boolean algebras // Math. Logic Quarterly, 49, № 2, pp. 210–213, 2003.

(g) Rybalov A. On the P-NP problem over real matrix rings // Theoretical Computer Science, Vol. 314/1-2, pp. 281–285, 2004.

(h) Рыбалов А.Н. Сложность вычислений в алгебраических системах // Сибирский математический журнал, Т.45, № 6, С. 1365–1377, 2004.

(i) Рыбалов А.Н., Релятивизации вопроса P=NP над полем комплексных чисел // Сибирские электронные математические известия, Т. 1, С. 91–98, 2004.

2. Желательно более подробно описать, что такое обобщенные регистровые машины и чем они отличаются от рассмативаемых ранее моделей. Можно выделить отдельный параграф для этого.

3. Лемма 1 на стр. 147 неочевидна. Требуется ясное и подробное доказательство.

4. Пример 2 на стр. 150. Что за тест Рабина? Имеется ввиду вероятностный тест Рабина-Миллера? Не будет ли этот тест ошибаться на числах Кармайкла? Предлагаю убрать этот пример, так как в доказательстве теоремы 4 на него ссылаются как на полиномиальный алгоритм для проверки простоты чисел, и в то же время в конце примера пишется: «Поэтому работа машины не завершится за полиномиальное время». Более того, в доказательстве теоремы 4, проверка простоты чисел порядка $n \log n$ может быть выполнена за полиномиальное время от n напрямую, последовательным делением на числа, меньшие n. Без всяких хитрых тестов. Ведь обобщенные регистровые машины должны уметь реализовывать классические вычисления с целыми числами.

5. Определение класса NP на стр. 151 некорректно. Что значит «сертификат полиномиальной длины»? Полином, ограничивающий эту длину фиксирован заранее?

6. Авторам предлагается подумать, можно ли, используя технику из доказательства теоремы 4, доказать, что в бесконечной декартовой степени $\mathbb{Z}$ имеет место совпадение аналогов классов P и NP. Эти классы (а в общем случае есть два класса NP) определяются, например, в статье Хеммерлинга. Если удастся доказать P=NP для данной системы, это будет простой естественный пример алгебраической системы, где P=NP. Хеммерлинг в своих работах строил такие системы, но они были достаточно сложные и искусственные. Это лишь пожелание, если доказать не удастся, это не будет препятствием к публикации.