Темы исследований для студентов

1. Полиномиальная алгебра

1.1. **Поведение при композиции.** Исследуется устойчивость базиса Гребнера (или аналогичного объекта) относительно полиномиальной композиции. Эта задача широко исследовалась Хонгом в середине 1990-х гг. Имеются результаты для базисов Гребнера, редуцированных базисов Гребнера, результантов, инволютивных базисов, некоммутативных базисов Гребнера, а также дифференциальных стандартных базисов. Задача состоит в изучении этих методов и в попытке применить их к универсальным базисам Гребнера, исчерпывающим базисам, граничным базисам, H-базисам и т. д.

[1] Hong H., Groebner Basis Under Composition I, The Journal of Symbolic Computation, 643-663, 25 (5), 1998.
[2] Hong H., Groebner Basis Under Composition II, in Proceedings of ISSAC-1996, 79–85, 1996.
[3] Gutierrez J., and Rubio San Miguel R., Reduces Gröbner Bases Under Composition Journal of Symbolic Computation, vol. 26, 433–444, 1998.
[4] Зобнин А.И.: Поведение дифференциальных стандартных базисов при композиции. «Фундаментальная и прикладная математика», том 13, выпуск 1, стр. 109–134 (2007).

1.2. **Декомпозиция многочленов.** Как алгоритмически проверить, что заданный многочлен является нетривиальной композицией двух других многочленов? На эту тему имеются фундаментальные работы Ритта (1920-е гг.), а также ряд современных результатов. Хочется получить обзор этих методов и, возможно, попытаться применить их в следующей ситуации: сначала мы определяем, что система полиномиальных уравнений допускает декомпозицию, а затем с помощью результатов о поведении при композиции упрощаем задачу вычисления базиса Гребнера этой системы.

[1] J. F. Ritt. Prime and composite polynomials. Trans. Amer. Math. Soc. 23 (1922), no. 1, 51–66.
[2] Michael E. Zieve and Peter Müller. On Ritt's polynomial decomposition theorems. arXiv:0807.3578. 2006. http://www.math.lsa.umich.edu/~zieve/papers/peter.pdf

1.3. **Универсальные базисы.** Известно, что множество всевозможных редуцированных базисов Гребнера заданного идеала конечно. Объединение таких множеств называют универсальным базисом Гребнера. Это определение было введено в начале 1990-х гг. Вайспфеннингом. Недавно появились результаты Н. Васильева и Д. Павлова о так называемых расширенных универсальных базисах Гребнера, которые можно определить достаточно инвариантно. Однако в общем случае алгоритм вычисления расширенного универсального базиса неизвестен. Хотелось бы получить обзор полученных результатов с выяснением известных оценок сложности алгоритмов построения универсального базиса. Можно ли построить универсальный базис быстрее, если известны дополнительные сведения об идеале? (Например, имеются результаты о полиномиальной сложности вычисления универсального базиса для 0-мерных идеалов, а также об алгоритмах для торических идеалов). Что известно про распознавание универсальности базиса? Когда можно построить «частично-универсальные» базисы, которые будут являться базисами Гребнера только при заданных подклассах упорядочений?

[1] V. Weispfennig. Constructing Universal Groebner Bases. In Proceedings of the 5th International Conference on Applied Algebra, 1989.
[2] S. Onn, E. Babson, R. Thomas. The Hilbert zonotope and a polynomial time algorithm for universal Groebner bases, Advances in Applied Mathematics, 30:529–544, 2003. http://ie.technion.ac.il/~onn/Selected/AAM2.pdf
[3] S. Mehta. A New Algorithm for Universal Groebner Basis for Toric Ideals. http://www.cse.iitk.ac.in/users/skmehta/papers/apors03.ps
[4] Н. Васильев, Д. Павлов. Перечисление конечных мономиальных упорядочений и комбинаторика универсальных базисов Гребнера. «Программирование», № 2, 2009, 28–42.

1.4. **Исчерпывающие базисы и системы (Ваня?)** Исчерпывающий базис Гребнера остается базисом Гребнера при любой специализации параметров. Определение также было введено Вайспфеннингом, а затем активно развивалось японскими и испанскими математиками. Имеются алгоритмы, которые по данной системе строят специальное дерево, в узлах которого записаны полиномиальные условия на параметры, а в листьях — получающиеся базисы Гребнера. Такое дерево позволяет решать системы полиномиальных уравнений с параметрами. Нужен подробный обзор этих методов, а также реализация полученных алгоритмов в системе Sage. Можно ли применить эти результаты, например, для компьютерного решения геометрических задач?

[1] Y. Sato and A. Suzuki. An alternative approach to comprehensive Gröbner bases. Journal of Symbolic Computation, ISSAC 2002, vol. 36, number 3–4, pp. 649–667.
[2] Marek Rychlik. Groebner Bases and Comprehensive Groebner Systems. http://marekrychlik.com/node/41
[3] A. Dolzmann, T. Sturm, W. Neun. CGB: Computing Comprehensive Gröbner Bases. http://www.zib.de/Symbolik/reduce/moredocs/cgb.pdf
[4] Публикации A. Montes'a. http://www-ma2.upc.es/~montes.

1.5. **Треугольные разложения (Илья?)** Разложение полиномиальной системы на треугольные множества восходит к работам Ритта и Ву (и иногда называется методом Ву). Считается, что такое использование такого разложения бывает эффективнее при решении систем полиномиальных уравнений, чем применение базисов Гребнера. Требуется сделать обзор имеющихся методов, сравнить алгоритмы треугольного разложения с алгоритмами вычисления базисов Гребнера, указать достоинства и недостатки каждого подхода и, возможно, попытаться описать их в некотором смысле единообразно. Отдельно требуется разобраться с разложениями Томаса, описанными в статье В. П. Гердта.

[1] Hubert E., Notes on triangular sets and triangulation-decomposition algorithms. I: Polynomial Systems, Symbolic and Numerical Scientific Computing 2001, 1–40, 2003.
[2] Aubry P., Lazard D., Moreno Maza M. On the Theories of Triangular Sets. Journal of Symbolic Computation, vol. 28, 105–124, 1999.
[3] V. P. Gerdt. On Decomposition of Algebraic PDE Systems into Simple Subsystems. Acta Appl. Math. 101, 2008, 39–51. http://pin.jinr.ru/pin/pin?c=persons/getDocData&file_id=1097
[4] F. Boulier, C. Chen, O. Golubitsky, F. Lemaire, M. Moreno Maza, W. Pan. Comprehensive triangular decomposition. Proc. 10th International Workshop on Computer Algebra in Scientific Computing (CASC 2007), Bonn, Germany. Lecture Notes in Computer Science, vol. 4770, pp. 73–101 (2007). http://publish.uwo.ca/~ogolubit/ctd.pdf

1.6. **H-базисы.** H-базисы обобщают базисы Гребнера: вместо градуировки алгебры многочленов по мономам используются более грубые градуировки, а вместо редукции — процесс ортогонализации. Нужно дать обзор этим методам, релизовать алгоритмы вычисления этих базисов в системе Sage, указать области применения.

[1] H. M. Möller and T. Sauer. H–bases for polynomial interpolation and system solving. Advances Comput. Math., 12 (2000), 335—362.
[2] H. M. Möller and T. Sauer. H–bases I: The foundation. Curve and Surface fitting. 1999, 325–332.
[3] H. M. Möller and T. Sauer. H–bases II: Applications to numerical problems. Curve and Surface fitting. 1999, 333–342.
[4] T. Sauer. Gröbner bases, H–bases and interpolation. Trans. Amer. Math. Soc., 353 (2001), 2293–2308.
[5] J. M. Peña, T. Sauer. Efficient Polynomial Reduction. http://www.uni-giessen.de/tomas.sauer/Publ/polyLA.pdf

1.7. **Решение больших систем нелинейных уравнений различными методами (Настя?)** Имеется, например, серия полиномиальных уравнений над конечным полем, полученных с помощью криптосистем HFE или AES. Требуется применить различные методы к ее решению (алгоритм Бухбергера, алгоритмы F4 или F5, результанты, треугольные разложения и т.д.) и сравнить эффективность этих алгоритмов следующим образом: систему какой величины сможет решить данный алгоритм за фиксированное время?

[1] The HFE public key encryption and signature. http://www.cryptosystem.net/hfe/
[2] J.-C. Faugère, S. Rahmany. Solving Systems of Polynomial Equations with Symmetries Using SAGBI-Grobner Bases. In Proceedings of the 2009 international symposium on Symbolic and algebraic computation, Seoul Korea, ACM, 2009.
[3] J.-C. Faugère and A. Joux. Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases. Advances in Cryptology - CRYPTO 2003, vol. 2729 of LNCS, pp 44–60. Springer, 2003.

1.8. **Автоматическое доказательство геометрических теорем.** Известно, что метод Ву и базисы Гребнера могут быть применены для автоматического доказательства геометрических теорем, сформулированных в полиномиальном виде. Методы исчерпывающих систем позволяют применять эти алгоритмы также и для решения некоторых геометрических задач. В конце 1980-х гг. вышла книга Чу, где были приведены компьютерные решения более 300 теорем, и были приведены результаты о том, что метод Ву для таких задач эффективнее базисов Гребнера. Сейчас появились новые алгоритмы (F4, F5), благодаря которым ситуация может измениться. Требуется реализовать в какой-либо системе компьютерной алгебры компьютерный решатель таких задач и попытаться повторить исследования Чу.

[1] Chou. S.-C., Mechanical Geometry Theorem Proving, D. Reidel Publishing Company, Dordrecht, 1988.

1.9. **Базисы Гребнера с параметрическими степенями.** Пусть степени некоторых переменных в многочленах данной системы зависят от параметра. Можно ли вычислить в обобщенном виде базис Гребнера для таких систем? Впервые подобные исследования стал проводить Вайспфеннинг.

[1] Weispfenning V., Gröbner Bases for Binomials with Parametric Exponents, in Proceedings of the 7th International Workshop on Computer Algebra in Scientific Computing (CASC-2004), July 12–19, 2004, St. Petersburg, Russia, pp. 467–477 (2004).

1.10. **Лексикографические идеалы.** Пусть $S = k[x_1, \ldots, x_n]$ — кольцо многочленов и $I \lhd S$ — градуированный идеал. Маколей в начале XX века доказал, что найдется *лексикографический идеал* с таким же многочленом Гильберта. Лексикографический идеал можно описать так: вместе с каждым мономом M он содержит и все лексикографически старшие мономы той же степени. Такие идеалы обладают любопытными комбинаторными свойствами и в некотором смысле позволяют описать все возможные размерностные многочлены. Оказывается, обобщение теоремы Маколея справедливо и для некоторых факторколец кольца многочленов. Отдельная задача - явное описание лексикографических идеалов при дополнительных предположениях (например, в кольце многочленов от двух переменных).

[1] J. Memrin, Lexicographic Ideals, Dissertation, 2006.

2. Дифференциальная алгебра

2.1. **Теорема о малой степени и проблема Ритта.** Требуется разобраться в доказательствах теоремы Леви-Ритта-Колчина о малой степени (the Low Power Theorem) (и сопутсвующих леммах о доминировании, о старшем коэффициенте, леммы Леви) и выяснить, какие обобщения она допускает. Также требуется разобраться в известных случаях, при которых задача о построении базиса идеала $[A] : H_A^\infty$ (и, в частности, проблема Ритта) имеет решение. Можно ли получить более простое и доступное доказательство для обыкновенного случая и (или) для случая одной дифференциальной переменной?

[1] Kolchin E.R., Differential Algebra and Algebraic Groups, Academic Press, 1973.
[2] Hubert E., Essential Components of an Algebraic Differential Equation, Journal of Symbolic Computation, vol. 28 (4–5), 657–680, 1999.
[3] Кондратьева М.В., Примеры вычисления образующих дифференциального идеала по характеристическому множеству, Программирование, № 2, 34–37, 2002.
[4] О. Д. Голубицкий, М. В. Кондратьева, А. И. Овчинников. Об обобщённой проблеме Ритта как вычислительной задаче. Фундаментальная и прикладная математика. 2008, т. 14, вып. 4, стр. 109–120. http://mech.math.msu.su/~fpm/ps/k08/k084/k08406.pdf

2.2. **Критерии конечности дифференциальных стандартных базисов (Максим?)** Дифференциальные стандартные базисы в большинстве случаев бесконечны, однако известно несколько важных условий их конечности. Так, для лексикографического упорядочения конечность базиса эквивалентна наличию в идеале квазилинейного многочлена. Однако пока неизвестен алгоритм, проверяющий наличие этого многочлена в идеале. Для beta-упорядочений доказано лишь достаточное условие, а необходимое сформулировано в виде гипотезы, которая полностью пока не доказана. Хочется завершить эти доказательства и получить отрицательные результаты о конечности базисов для других классов упорядочений.

[1] Levi H., On the Structure of Differential Polynomials and on Their Theory of Ideals, Trans. AMS, vol. 51, 532–568, 1942.
[2] O'Keefe K.B., A Property of the Differential Ideal $[y^p]$, Trans. AMS, vol. 94, 483–497, 1960.
[3] Zobnin A.: Admissible Orderings and Finiteness Criteria for Differential Standard Bases. In Proceedings of International Symposium on Symbolic and Algebraic Computation (ISSAC-2005), July 24–27, Beijing, China, pp. 365–372 (2005)

2.3. **Дифференциальные идеалы, порожденные многочленом первого порядка (Максим?)** Из результатов Колчина следует, что в общем случае такой идеал содержит квазилинейный многочлен тогда и только тогда, когда этот идеал радикален. Однако остаются неразобранные Колчиным сингулярные случаи, в которых ответ неизвестен. Требуется разобраться с этими случаями, а также переписать результаты Колчина в современном и доступном виде. Можно ли обобщить эти результаты на случай многочленов больших порядков или случай нескольких многочленов?

[1] Kolchin E.R. On the exponents of differential ideals, Annals of Mathematics, 42:740–777, 1941.

2.4. **Канонические характеристические множества.** В середине 2000-х гг. появились работы О. Голубицкого о построении канонических и универсальных характеристических множеств идеалов, а также о дифференциальном маршруте Гребнера. Требуется изучить эти работы и реализовать алгоритмы построения канонических множеств в системе Sage.

[1] Golubitsky O., Differential Groebner Walk, in Proceedings of International Workshop on Computer Algebra and its Applications to Physics, Dubna, Russia, 114–126, 2001.
[2] O. Golubitsky. Universal characteristic decomposition of radical differential ideals. Journal of Symbolic Computation, 43 (1): pp. 27–45 (2008). http://publish.uwo.ca/~ogolubit/ucdjsc.pdf
[3] O. Golubitsky. Groebner fan and universal characteristic sets of prime differential ideals. Journal of Symbolic Computation, 41 (10): pp. 1091–1104 (2006). http://publish.uwo.ca/~ogolubit/ucsjsc.pdf

2.5. **Эффективность алгоритма Розенфельда-Гребнера.** Известно, что алгоритм Розенфельда-Гребнера имеет очень высокую сложность. Можно ли его распараллелить? Известны результаты о параллелизации треугольных разложений, которые также можно было бы применить. Можно ли переписать Розенфельда-Гребнера в духе линейной алгебры, как это сделано в алгоритме F4? Также требуется реализовать этот алгоритм в системе Sage.

[1] O. Golubitsky, M. Kondratieva, M. Moreno Maza, A. Ovchinnikov. A bound for the Rosenfeld-Groebner algorithm. Journal of Symbolic Computation, 43 (8): pp. 582–610 (2008). http://publish.uwo.ca/~ogolubit/rg.pdf