Теоретико-операторный подход к алгоритму Берлекэмпа–Месси–Сакаты[1]

В.М. Деундяк, А.М. Пеленицын

1. Введение. Исходная версия алгоритма Берлекэмпа–Месси (BM-алгоритма) для полиномов от одной переменной была изложена Берлекэмпом в 1968 году [1, с. 193] в качестве элемента конструкции декодера кодов Боуза–Чоудхудри–Хоквингема над конечным полем. Месси [2] предложил свою интерпретацию алгоритма, как процесса построения линейного регистра сдвига минимальной длины, генерирующего заданную последовательность элементов конечного поля. BM-алгоритм нашёл многочисленные применения в различных областях математики, обзор последних наиболее важных результатов содержится в [3]. В связи с декодированием алгебро-геометрических кодов появилась необходимость обобщения BM-алгоритма на полиномы нескольких переменных. Впервые такое обобщение предложил С. Саката [4], [5] и его теперь принято называть алгоритмом Берлекэмпа–Месси–Сакаты (BMS-алгоритмом). Приложения этого алгоритма к актуальным задачам помехоустойчивого кодирования обсуждаются в [6]. В [7] представлена реализация кодека для одного класса алгебро-геометрических кодов с использованием двумерного BMS-алгоритма.

Задачи, которые решают как BM-алгоритм, так и BMS-алгоритм, имеют теоретико-операторную природу, которая исследуется в настоящей работе. Теоретико-операторный подход к рассматриваемым алгоритмам позволяет перейти от поиска полиномов к поиску последовательностей, подобно тому, как в теории помехоустойчивого кодирования осуществляется переход от декодирования во временной области к декодированию в частотной области [8]. Основным результатом настоящей работы является основанная на теоретико-операторном подходе новая версия BMS-алгоритма, которая является в теоретическом отношении более прозрачной, чем оригинальная версия С. Сакаты, более удобна для программной реализации и может быть использована при построении эффективных декодеров для широкого класса алгебро-геометрических кодов.

2. Одномерная задача Берлекэмпа. Пусть $\boldsymbol{Z}$ — множество целых чисел, $\boldsymbol{N}_0$ — множество неотрицательных целых чисел, $\boldsymbol{F}$ — некоторое фиксированное (необязательно конечное) поле. *Последовательностью u над полем $\boldsymbol{F}$* будем называть отображение $u\colon \boldsymbol{Z} \to \boldsymbol{F}$. Для каждой последовательности u определим её *носитель*:

$$\operatorname{supp}(u) = \{k \in \boldsymbol{Z} \mid u_k \neq 0\}.$$

Введём линейное пространство последовательностей с конечным носителем:

$$\ell^0(\boldsymbol{Z}) = \{\, u\colon \boldsymbol{Z} \to \boldsymbol{F} \mid |\operatorname{supp}(u)| < \infty \,\}$$

и его подпространство последовательностей с конечным носителем и нулевыми элементами для отрицательных индексов:

$$\ell^0(\boldsymbol{Z}_+) = \{\, u \in \ell^0(\boldsymbol{Z}) \mid k < 0 \Rightarrow u_k = 0 \,\}.$$

[1] Принято к публикации в журнале «Известия вузов. Северо-Кавказский регион», сер. Естественные науки.

Для последовательностей $u \in \ell^0(\boldsymbol{Z}_+)$, отличных от тождественно нулевой последовательности 0, определим *степень u*:

$$d(u) = \max\{k \mid u_k \neq 0\}.$$

Положим $d(0) = -\infty$, подразумевая обычные арифметические свойства $-\infty$.

Для любого $k \in \boldsymbol{N}_0$ определим оператора сдвига:

$$\tau_k\colon \ell^0(\boldsymbol{Z}) \to \ell^0(\boldsymbol{Z}), \quad (\tau_k u)_j = u_{j-k}.$$

Для любой последовательности $f \in \ell^0(\boldsymbol{Z}_+)$ определим оператор Ганкеля:

$$H^{(f)} : \ell^0(\boldsymbol{Z}) \to \ell^0(\boldsymbol{Z}), \qquad (H^{(f)}u)_j = \sum_{k\in\boldsymbol{Z}} f_k u_{j+k}$$

Далее будут рассматриваться уравнения типа $H^{(f)}u = 0$, однако в действительности мы сможем обеспечить равенство нулю лишь части элементов последовательности в левой части, и, чтобы учесть это, введём специальное семейство проекторов:

$$Q_{k,m} : \ell^0(\boldsymbol{Z}) \to \ell^0(\boldsymbol{Z}_+)\,, \qquad k, n \in \boldsymbol{N}_0,\ k \le m,$$

по формуле

$$(Q_{k,m}u)_j = \begin{cases} u_j, & k \le j \le m, \\ 0, & j < k,\, j > m, \end{cases}$$

где $u \in \ell^0(\boldsymbol{Z})$. Для $k > m$ положим $Q_{k,m} = O$ (нулевой оператор).

Для каждой последовательности $f \in \ell^0(\boldsymbol{Z}_+)$ определим семейство линейных операторов, зависящих от двух параметров $k, m \in \boldsymbol{N}_0$:

$$B^{(f)}_{k,m} : \ell^0(\boldsymbol{Z}_+) \to \ell^0(\boldsymbol{Z}_+),$$

по формуле:

$$B^{(f)}_{k,m} u = Q_{k,\,m}\, \tau_k\, H^{(f)}\, u.$$

Заметим, что при $k > m$ имеет место равенство $B^{(f)}_{k,m} = O$ для любой f.

Задача B (задача Берлекэмпа). Пусть дана последовательность $u \in \ell^0(\boldsymbol{Z}_+)$. Требуется найти последовательность f, такую что:

1) выполнено

$$B^{(f)}_{d(f),d(u)} u = 0 \tag{1}$$

2) $d(f) \in \boldsymbol{N}_0$ минимальна.

Для данной последовательности $u \in \ell^0(\boldsymbol{Z}_+)$ будем говорить, что решается задача **B**(u). Видно, что задача **B**(u) представляет собой операторное уравнение, снабжённое некоторым оптимизационным требованием. Решению этой задачи, сформулированной в несколько другой форме, посвящён классический алгоритм Берлекэмпа–Месси [8, с. 208].

В некоторых приложениях, где возникает задача **B**(u), достаточно узнать значение $d(f)$: например, оно даёт определённую характеристику псевдослучайных последовательностей, используемых при поточном шифровании [9, с. 260]. В других случаях требуется узнать и f — так обстоит дело, к примеру, при более тонком анализе псевдослучайных последовательностей [9, с. 261], а также в задачах декодирования кодов

БЧХ [8, с. 211]. Мы будем считать, что результатом решения задачи $\mathbf{B}(u)$ является последовательность f.

Покажем, что задача $\mathbf{B}(u)$ имеет решение для любой последовательности $u \in \ell^0(\boldsymbol{Z}_+)$. Для этого достаточно убедиться, что множество решений уравнения (1) не пусто. Действительно, выбрать из возможных решений уравнения (1) последовательность с минимальной степенью будет возможно, в силу того что множество $\boldsymbol{N}_0$, которому принадлежат степени последовательностей, вполне упорядочено, то есть в каждом его подмножестве имеется минимальный элемент. Итак, если последовательность u ($\in \ell^0(\mathbf{Z}_+)$) является нулевой, то положим $f = 0$. В случае ненулевой последовательности u

$$B^{(f)}_{d(u)+1,d(u)} = O$$

для любой последовательности f, если $d(f)=d(u)+1$ (см. замечание при определении $B^{(f)}_{k,m}$). Полагая

$$f = (\ldots , 0, 1, 0, \ldots),$$

где 1 стоит в позиции $d(u)+1$, получим выполненным уравнение (1).

Поясним принцип работы алгоритма Берлекэмпа–Месси из [8] применительно к решению сформулированной выше задачи $\mathbf{B}(u)$. Для этого введём следующее обозначение: для любой последовательности $v \in \ell^0(\boldsymbol{Z}_+)$ и $r \in \boldsymbol{N}_0$ обозначим

$$v^{(r)} = Q_{0,\,r}v.$$

Алгоритм Берлекэмпа–Месси решает набор задач $\mathbf{B}(u^{(r)})$ последовательно для $r \in [0, d(u)]_{\boldsymbol{Z}}$ (на последней итерации алгоритма, при $r = d(u)$, имеет место совпадение задач $\mathbf{B}(u^{(r)})$ и $\mathbf{B}(u)$). Таким образом, получается набор (необязательно различных) последовательностей $\{f^{(r)}\}_{r=0}^{d(u)}$. На r-ой итерации $f^{(r)}$ либо полагается равным $f^{(r-1)}$ (решение задач $\mathbf{B}(u^{(r-1)})$ и $\mathbf{B}(u^{(r)})$ совпадают), либо вычисляется с помощью $f^{(r-1)}$ и $f^{(j)}$, где

$$j = \max\{i \mid i < r-1 \wedge f^{(i)} \neq f^{(r-1)}\}.$$

3. Многомерная задача Берлекэмпа. *n-мерной последовательностью* или *n-последовательностью* будем называть отображение $u : \boldsymbol{Z}^n \to \boldsymbol{F}$. Для каждой n-последовательности u определён её *носитель*:

$$supp(u) = \{\, \boldsymbol{k} \in \boldsymbol{Z}^n \mid u_{\boldsymbol{k}} \neq 0 \,\}.$$

Введём два отношения порядка на $\boldsymbol{N}_0^n$. Частичный порядок $\le_{\mathrm{P}}$ определим соотношением

$$\boldsymbol{m} \le_{\mathrm{P}} \boldsymbol{k} \Longleftrightarrow \forall\, i \quad m_i \le k_i.$$

В качестве второго отношения порядка можно взять любой *мономиальный порядок* $<$, то есть такой полный линейный порядок на $\boldsymbol{N}_0^n$, что

$$\forall\, \boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \boldsymbol{N}_0^n \quad \boldsymbol{u} < \boldsymbol{v} \Rightarrow \boldsymbol{u} + \boldsymbol{w} < \boldsymbol{v} + \boldsymbol{w}$$

(см. [10, с. 7]). Под операцией + подразумевается покоординатная сумма элементов («точек») $\boldsymbol{N}_0^n$. Например, $<$ можно определить так:

$$\boldsymbol{m} < \boldsymbol{k} \Longleftrightarrow (\sum_i m_i < \sum_i k_i) \vee$$
$$\vee((\sum_i m_i = \sum_i k_i) \wedge$$
$$\wedge(\exists j \,\forall i : \quad (j < i) \to ((m_i = k_i) \wedge (m_j < k_j)))).$$

Всюду далее мы предполагаем фиксированным некоторый мономиальный порядок <. Запись $\boldsymbol{k} \le \boldsymbol{m}$ означает $(\boldsymbol{k} < \boldsymbol{m}) \vee (\boldsymbol{k} = \boldsymbol{m})$.

Введём обозначения для линейных пространств финитных последовательностей:

$$\ell^0(\boldsymbol{Z}^n) = \{\, u : \boldsymbol{Z}^n \to \boldsymbol{F} \mid |supp(u)| < \infty \,\},$$
$$\ell^0(\boldsymbol{Z}_+{}^n) = \{\, u \in \ell^0(\boldsymbol{Z}^n) \mid u_{\boldsymbol{k}} = 0 \text{ для } \boldsymbol{k} \in \boldsymbol{Z}^n \setminus \boldsymbol{N}_0^n \,\}.$$

Для каждой n-последовательности u из $\ell^0(\boldsymbol{Z}_+{}^n)$, отличной от тождественно нулевой 0, определим *степень u*:

$$d(u) = \max\{\boldsymbol{k} \in \boldsymbol{Z}^n \mid u_{\boldsymbol{k}} \neq 0\},$$

где максимум берётся по отношению <. Положим $d(0) = -\infty$. Если $F \subset \ell^0(\boldsymbol{Z}_+{}^n)$ — конечно, то

$$d(F) = \{\, d(f) \mid f \in F \,\}.$$

Оператор сдвига в направлении $\boldsymbol{k} \in \boldsymbol{N}_0^n$ определяется так:

$$\tau_{\boldsymbol{k}} : \ell^0(\boldsymbol{Z}^n) \to \ell^0(\boldsymbol{Z}^n), \qquad (\tau_{\boldsymbol{k}}\, u)_{\boldsymbol{j}} = u_{\boldsymbol{j}-\boldsymbol{k}}.$$

Для любой n-последовательности $f \in \ell^0(\boldsymbol{Z}_+{}^n)$ определим оператор Ганкеля:

$$H^{(f)} : \ell^0(\boldsymbol{Z}^n) \to \ell^0(\boldsymbol{Z}^n),$$

по формуле:

$$(H^{(f)}u)_{\boldsymbol{j}} = \sum_{\boldsymbol{k}\in\boldsymbol{Z}^n} f_{\boldsymbol{k}} u_{\boldsymbol{j}+\boldsymbol{k}} \,.$$

Введём семейство проекторов:

$$Q_{\boldsymbol{k},\,\boldsymbol{m}} : \ell^0(\boldsymbol{Z}^n) \to \ell^0(\boldsymbol{Z}_+{}^n) \quad \boldsymbol{k}, \boldsymbol{m} \in \boldsymbol{N}_0{}^n$$

по формуле:

$$(Q_{\boldsymbol{k},\boldsymbol{m}}u)_{\boldsymbol{j}} = \begin{cases} u_{\boldsymbol{j}+\boldsymbol{k}}, & \boldsymbol{k} \le_{\mathrm{P}} \boldsymbol{j} \le \boldsymbol{m}, \\ 0, & \boldsymbol{j} \in \boldsymbol{Z}^n \setminus \{\boldsymbol{i} \mid \boldsymbol{k} \le_{\mathrm{P}} \boldsymbol{i} \le \boldsymbol{m}\}, \end{cases}$$

где $u \in \ell^0(\boldsymbol{Z}^n)$. Заметим, что множество $\{\, \boldsymbol{j} \mid \boldsymbol{k} \le_{\mathrm{P}} \boldsymbol{j} \le \boldsymbol{m} \,\}$ может быть пусто для некоторых значений $\boldsymbol{k}, \boldsymbol{m}$. В таких случаях полагаем $Q_{\boldsymbol{k},\,\boldsymbol{m}} = O$.

Для каждой n-последовательности $f \in \ell^0(\boldsymbol{Z}_+{}^n)$ определим семейство линейных операторов, зависящих от двух параметров $\boldsymbol{k}, \boldsymbol{m} \in \boldsymbol{N}_0^n$:

$$B_{\boldsymbol{k},\boldsymbol{m}}^{(f)} : \ell^0(\boldsymbol{Z}_+{}^n) \to \ell^0(\boldsymbol{Z}_+{}^n) \qquad B_{\boldsymbol{k},\boldsymbol{m}}^{(f)} u = Q_{\boldsymbol{k},\,\boldsymbol{m}}\, \tau_{\boldsymbol{k}}\, H^{(f)}\, u.$$

Пусть $D = \{\boldsymbol{s}^{(i)}\}_{i=0}^{l} \subset \boldsymbol{N}_0^n$. Будем говорить, что D — *множество гиперболического типа*, если выполнено условие:

$$\boldsymbol{s}^{(i)} \le_{\mathrm{P}} \boldsymbol{s}^{(j)} \Rightarrow i = j.$$

Задача B$^{\boldsymbol{n}}$. Пусть дана n-последовательность $u \in \ell^0(\boldsymbol{Z}_+{}^n)$. Требуется найти такое упорядоченное множество $F = \{f^{(i)}\}_{i=0}^{l} \subset \ell^0(\boldsymbol{Z}_+{}^n)$, что

a) $B_{d(f^{(i)}),d(u)}^{f^{(i)}} u = 0, \quad 1 \le i \le l,$

b) $d(F)$ — множество гиперболического типа;

c) $\forall\, g \in \ell^0(\boldsymbol{Z}_+{}^n) : B_{d(g),d(u)}^{(g)} u = 0 \Rightarrow \exists\, i \colon d(f^{(i)}) \le_{\mathrm{P}} d(g).$

В одномерном случае оптимизационное требование — минимизация величины $d(f)$ — формулировалось достаточно просто, так как величина $d(f)$ принадлежала множеству $\boldsymbol{N}_0$, в котором имеется естественный полный порядок. В многомерном случае работа ведётся в $\boldsymbol{N}_0^n$, где очевидным образом определяется только частичный порядок $\le_P$. Минимизация проводится относительно этого частичного порядка (требования (b)–(c)). По этой же причине рассматривается набор операторных уравнений, а не одно уравнение: частично упорядоченное множество разбивается на несколько подмножеств, в каждом из которых имеется свой минимум.

Полный порядок $<$ вводится на $\boldsymbol{N}_0^n$ с определённой долей произвола и служит исключительно для того, чтобы определять степени последовательностей. Авторам не известны способы проведения минимизации относительно этого порядка. Если бы удалось сформулировать и решить такую задачу, то она, вероятно, состояла бы в нахождении *единственной* n-последовательности f.

4. Теоретико-операторная версия BMS-алгоритма. Представим версию BMS-алгоритма [11], основанную на теоретико-операторном подходе.

Определим операцию взятия покомпонентного максимума двух точек $\boldsymbol{m}, \boldsymbol{k} \in \boldsymbol{Z}^n$:

$$\max(\boldsymbol{m}, \boldsymbol{k}) = (\max(m_1, k_1), \ldots, \max(m_n, k_n)).$$

Отметим, что определённый выше на $\boldsymbol{N}_0$ порядок $\le_P$ естественным образом распространяется на $\boldsymbol{Z}^n$ и связан с операцией максимума:

$$(\boldsymbol{m} \le_P \max(\boldsymbol{m},\boldsymbol{k})) \wedge (\boldsymbol{k} \le_P \max(\boldsymbol{m},\boldsymbol{k})).$$

Полный порядок $<$ на $\boldsymbol{N}_0^n$ позволяет для каждой данной точки $\boldsymbol{r} \in \boldsymbol{N}_0^n$, единственным образом определить непосредственно следующую за ней точку $\hat{\boldsymbol{r}} \in \boldsymbol{N}_0^n$.

Для данных $u, f \in \ell^0(\boldsymbol{Z}_+^n)$ последовательность $B_{d(f),d(u)}^{(f)}u$ будем кратко записывать так: $B^{(f)}u$.

Пусть $\boldsymbol{m} \in \boldsymbol{Z}^n$, обозначим:

$$\Sigma_{\boldsymbol{m}} = \{\boldsymbol{k} \in \boldsymbol{Z}^n \mid \boldsymbol{k} \le_P \boldsymbol{m}\}.$$

Множеству $F \subset \ell^0(\boldsymbol{Z}_+^n)$ сопоставим множества точек:

$$\Sigma(F) = \bigcup_{f \in F} \Sigma_{d(f)}$$

$$\Delta(F) = \boldsymbol{N}_0^n \setminus \Sigma(F),$$

$$C(F) = \max\nolimits_{\le P} \Delta(F).$$

Как и BM-алгоритм, BMS-алгоритм решает последовательность задач $\mathbf{B}^{\boldsymbol{n}}(u^{\boldsymbol{r}})$, $\boldsymbol{0} \le_P \boldsymbol{r} \le d(u)$, где

$$u^{\boldsymbol{r}} = Q_{\boldsymbol{0},\boldsymbol{r}}u.$$

Увеличение $\boldsymbol{r}$ ведётся в порядке, заданном $<$. Множество $F^{(\hat{\boldsymbol{r}})}$, которое должно стать решением задачи $\mathbf{B}^{\boldsymbol{n}}(u^{\hat{\boldsymbol{r}}})$ строится на основе $F^{(\boldsymbol{r})}$ и некоторого множества $G^{(\boldsymbol{r})} \subset \bigcup_{\boldsymbol{0} \le \boldsymbol{j} \le \boldsymbol{r}} F^{(\boldsymbol{j})}$, обладающего свойством:

$\forall\, g \in G^{(\boldsymbol{r})} \;\; \exists\, \boldsymbol{s}$:

$$(\boldsymbol{s} < \boldsymbol{r}) \wedge (B^{(g)}u^{\boldsymbol{s}} = 0) \wedge (B^{(g)}u^{\hat{\boldsymbol{s}}} \ne 0) \wedge$$

$$\wedge\ (\boldsymbol{s} - d(g) \in C(F^{(\boldsymbol{r})})). \qquad (2)$$

Алгоритм решения задачи $\mathbf{B}^{\boldsymbol{n}}(u)$.

1. Положим $F = \{\ f^{(1)} = (\ldots, 0\ , (f^{(1)})_{\mathbf{0}} = 1, 0, \ldots)\ \}$, $G = \emptyset$, $F' = \emptyset$, $\boldsymbol{r} := \mathbf{0}$.
2. Для каждой последовательности f из F положить $d_f := (B^{(f)}u)_{\boldsymbol{r}}$.

$$F_{fail} := \{f \in F \mid d_f \neq 0\};$$
$$F_{broke} := \{f \in F_{fail} \mid \nexists\ \boldsymbol{c} \in C(F)\colon \boldsymbol{r} - \boldsymbol{c} \leq_{\mathrm{P}} d(f)\ \};$$
$$D'' := \{\max(d(f), \boldsymbol{r} - \boldsymbol{c}) \mid f \in F_{broke},\ \ \boldsymbol{c} \in C(F)\ \};$$
$$D' := \min_{\leq \mathrm{P}} D'';$$
$$D := \min_{\leq \mathrm{P}}(\Sigma(F) \setminus \Gamma_{\boldsymbol{r}}).$$

3. Для каждой последовательности $f \in F_{fail} \setminus F_{broke}$ положить:

$$h := f - d_f\,(\tau_{d(f) - (\boldsymbol{r} - \boldsymbol{c})}\, g)$$

и добавить h в F'. Последовательность g определена из условия:

$$\boldsymbol{r} - d(f) \leq_{\mathrm{P}} \boldsymbol{s} - d(g).$$

($\boldsymbol{s}$ соответствует g по (2)) Для каждой пары $(f, g) \in F_{broke} \times G$, такой что $\boldsymbol{d}' := \max(d(f), \boldsymbol{r} - (\boldsymbol{s} - d(g))) \in D'$, положить:

$$h := \tau_{\boldsymbol{d}' - d(f)} f - d_f g$$

и добавить h в F'.

Для каждого $\boldsymbol{d} \in D$, если $\nexists\ \boldsymbol{d}' \in D'\colon \boldsymbol{d}' \leq_{\mathrm{P}} \boldsymbol{d}$, то для каждой $f \in F_{broke}$, такой что $d(f) \leq_{\mathrm{P}} \boldsymbol{d}$, положить:

$$h := \tau_{\boldsymbol{d} - d(f)} f$$

и добавить h в F'.

4.

$$F := (F \setminus F_{fail}) \cup F';$$
$$G' := \{\ g \in G \mid \exists\ f \in F_{broke}\colon \boldsymbol{s} - d(g) <_{\mathrm{P}} \boldsymbol{r} - d(f)\ \};$$
$$G := (G \setminus G') \cup \{\ \ d_f^{\,-1} f \mid f \in F_{broke}\ \}.$$

5. $\boldsymbol{r} = \hat{\boldsymbol{r}}$. Если $\boldsymbol{r} \leq d(u)$, переход на шаг 2, иначе остановка алгоритма.

Литература.

1. *Берлекэмп Э.* Алгебраическая теория кодирования. М.: Мир, 1971. 478 с.
2. *Massey J.L.* Shift Register Synthesis and BCH Decoding, // IEEE Trans. Inform. Theory. 1969. Vol. IT-15. No. 1. P. 122–128.
3. *Куракин В.Л.* Алгоритм Берлекэмпа—Месси над коммутативными артиновыми кольцами главных идеалов // Фундаментальная и прикладная математика. 1999. Т. 5, вып. 4. С. 1061–1101.
4. *Sakata S.* Finding a minimal set of linear recurring relations capable of generating a given finite two–dimensional array // J. Symb. Comp. 1988. Vol. 5. Pp. 321–337.
5. *Sakata S.* Extension of the Berlekamp—Massey algorithm to N dimensions // Inform. and Comput. 1990. Vol. 84. No. 2, P. 207–239.
6. *Sakata S.* The BMS algorithm and Decoding of AG Codes // In Sala M. et al. (ed.), Gröbner bases, coding, and cryptography. Springer. 2009. P. 143–163.

7. *Маевский А.Э., Пеленицын А.М.* Реализация программного алгебро-геометрического кодека с применением алгоритма Сакаты // Изв. ЮФУ. Технические науки. 2008. № 8. С. 196–198.

8. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки: Пер. с англ. М.: Мир, 1986. 576 с.

9. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В.* Основы криптографии, 3-е изд. М: Гелиос АРВ, 2005. 480 с.

10. *Cox D.A., Little J.B., O'Shea D.B.* Using Algebraic Geometry, Second Edition. Springer, 2005. 496 p.

11. *Sakata S.* The BMS algorithm // In Sala M. et al. (ed.), Gröbner bases, coding, and cryptography. Springer. 2009. P. 143–163.