УДК 621.391.251:681.3.06

Кубицкий В.И.

ДЕКОДИРОВАНИЕ ДВОЙНОЙ ОШИБКИ КОДОМ ЛАГРАНЖА

ГосНИИ «Аэронавигация» (Россия, Москва)

Показано, как с помощью кода Лагранжа можно исправлять двойные недвоичные ошибки. Разработаны алгоритмы декодирования, использующие различные процедуры вычисления контрольных символов. Выводятся ключевые уравнения синдромов кода Лагранжа для этих алгоритмов.

Известны описанные Питерсоном [1] и Берлекэмпом [2] эффективные для кодов Боуза-Чоудхури-Хоквингема (БЧХ-кодов) алгоритмы декодирования, согласно которым декодирование разбивается на следующие основные этапы:

1) вычисление синдрома;

2) вычисление элементарных симметрических функций;

3) определение номеров позиций ошибок;

4) вычисление значений ошибок.

В [3] показано, что коды Лагранжа изоморфны кодам Рида-Соломона (РС-кодам), которые являются частным случаем БЧХ-кодов. Поэтому очевидно, что для декодирования кодов Лагранжа характерны этапы, на которые разбивается декодирование БЧХ-кодов. Однако коды Рида-Соломона отличаются от кодов Лагранжа процессами кодирования и декодирования, что объясняется тем, что сравниваемые коды представляют кодовые векторы одного и того же q-мерного пространства E_q, представленные в различных базисах. Этот факт может служить основой для модификации преобразований в процессах кодирования и декодирования кодов Лагранжа. Поэтому одним из важных представляется решение задачи разработки и модификации процедур и алгоритмов декодирования кодов Лагранжа.

В [4, 5] выведены ключевые уравнения синдромов кодов Лагранжа при декодировании многократных ошибок с использованием различных алгоритмов вычисления контрольных символов. Однако в этих работах не описана последовательность вычислений при декодировани определённого количества ошибок.

В [6, 7] предложены алгоритмы и устройство декодирования одиночной ошибки кодом Лагранжа, из которых видно, что при таком декодировании не требуется вычисление элементарных симметрических функций, т.е. отсутствует один из этапов алгоритмов декодирования Питерсона-Берлекэмпа.

Рассмотрим декодирование двойной ошибки кодом Лагранжа.

Пусть кодовое слово определяется полиномом

$$f(x)=\sum_{i=0}^{s+4} f_i\, L_{S\cup T}^{(i)}(x),$$

где f_i - символ кодового слова; $L_{S\cup T}^{(i)}(x)$ – фундаментальные полиномы Лагранжа; $S=\{x_0,\ldots,x_s\}$ – множество информационных узлов мощности k; $T=\{\beta_1,\beta_2,\beta_3,\beta_4\}$ – множество контрольных узлов мощности 4.

Введём ошибки δ_{i_1} и δ_{i_2} в i_1-ю и i_2-ю позиции кодового слова соответственно. Тогда искажённый полином будет иметь вид:

$$\tilde{f}(x)=f(x)+\delta_{i_1}(x)+\delta_{i_2}(x)=$$

$$=\sum_{i=0}^{s+4} f_i\, L_{S\cup T}^{(i)}(x)+\delta_{i_1}\, L_{S\cup T}^{(i_1)}(x)+\delta_{i_1}\, L_{S\cup T}^{(i_1)}(x)=$$

$$=\sum_{i=0}^{s+4} \tilde{f}_i\, L_{S\cup T}^{(i)}(x).$$

Исправить ошибку можно с помощью алгоритмов, основанных на разработанных в [4] алгоритмах вычисления контрольных символов при декодировании

кода Лагранжа. Здесь рассмотрим декодирование с использованием последовательных алгоритмов А2 и А3.

Последовательный алгоритм декодирования А2

Этот алгоритм заключается в выполнении следующих действий.

1) вычисляются значения искаженного полинома в контрольных узлах.
Для 1-го контрольного узла имеем:

$$f^*(\beta_1) = \sum_{i=0}^{s} \tilde{f}_i \, L_S^{(i)}(\beta_1) =$$

$$= -\sum_{i=0}^{s} \tilde{f}_i \prod_{l=2}^{4} (x_i - \beta_l)/(\beta_1 - \beta_l).$$

При вычислении значений искажённого полинома $\tilde{f}(x)$ во 2-ом, 3-ем и 4-ом контрольных узлах кроме информационных символов $\tilde{f}_i$ принятой кодовой последовательности используются вычисленные значения $f^*(\beta_1)$, $f^*(\beta_2)$, $f^*(\beta_3)$ этого полинома в предыдущих контрольных узлах:

$$f^*(\beta_2) = [\sum_{i=0}^{s} \tilde{f}_i + f^*(\beta_1)] \, L_{S_1}^{(i)}(\beta_2),$$

$$f^*(\beta_3) = [\sum_{i=0}^{s} \tilde{f}_i + f^*(\beta_1) + f^*(\beta_2)] \, L_{S_2}^{(i)}(\beta_3),$$

$$f^*(\beta_4) = [\sum_{i=0}^{s} \tilde{f}_i + f^*(\beta_1) + f^*(\beta_2) + f^*(\beta_3)] \, L_{S_3}^{(i)}(\beta_4),$$

где $S_1 = S \cup \{\beta_1\}$, $S_2 = S \cup \{\beta_1, \beta_2\}$, $S_3 = S \cup \{\beta_1, \beta_2, \beta_3\}$,

$$L_{S_1}^{(i)}(\beta_2) = -\prod_{l=3}^{4} (x_i - \beta_l)/(\beta_2 - \beta_l),$$

$$L_{S_2}^{(i)}(\beta_3) = -(x_i - \beta_4)/(\beta_3 - \beta_4),$$

$$L_{S_3}^{(i)}(\beta_4) = -1;$$

2) определяются значения невязок:

$$R_1 = \tilde{f}(\beta_1) - f^*(\beta_1),$$
$$R_2 = \tilde{f}(\beta_2) - f^*(\beta_2),$$
$$R_3 = \tilde{f}(\beta_3) - f^*(\beta_3),$$
$$R_4 = \tilde{f}(\beta_4) - f^*(\beta_4),$$

где $\tilde{f}(\beta_1)$, $\tilde{f}(\beta_2)$, $\tilde{f}(\beta_3)$, $\tilde{f}(\beta_4)$ - значения контрольных символов принятого сообщения.

Если $R_1 = R_2 = R_3 = R_4 = 0$, то ошибок нет;

3) вычисляются величины синдромов:

$$Q_0 = R_1 + R_2 + R_3 + R_4,$$
$$Q_1 = R_1\beta_1 + R_2\beta_2 + R_3\beta_3 + R_4\beta_4,$$
$$Q_2 = R_1\beta_1^2 + R_2\beta_2^2 + R_3\beta_3^2 + R_4\beta_4^2,$$
$$Q_3 = R_1\beta_1^3 + R_2\beta_2^3 + R_3\beta_3^3 + R_4\beta_4^3.$$

Переходим к определению места и величины ошибок;

4) вычисляется определитель матрицы:

$$|M| = \begin{vmatrix} Q_0 & Q_1 \\ Q_1 & Q_2 \end{vmatrix} = Q_0Q_2 - Q_1^2.$$

Если $|M| \neq 0$, то количество ошибок равно 2, и выполняем пункт 5 данного алгоритма. Если $|M| = 0$, то количество ошибок не больше 1, и выполняем пункты 6 (формула 2) и 7 (формула 4) данного алгоритма. Эти условия следуют из теоремы 9.9 [1];

5) определяются нормализованные элементарные симметрические функции.

Выполняется известным из [1] способом, используя соотношения

$$Q_0\sigma_2 + Q_1\sigma_1 + Q_2 = 0,$$
$$Q_1\sigma_2 + Q_2\sigma_1 + Q_3 = 0.$$

Эти уравнения будут разрешимы, если матрица

$$M = \begin{bmatrix} Q_0 & Q_1 \\ Q_1 & Q_2 \end{bmatrix}$$

будет невырожденной, т. е. определитель матрицы $|M| \neq 0$ (теорема 9.9 из [1]).

При $|M| \neq 0$ вычисляются элементарные симметрические функции

$$\sigma_1 = \frac{\begin{vmatrix} Q_0 & -Q_2 \\ Q_1 & -Q_3 \end{vmatrix}}{|M|} = \frac{Q_1Q_2 - Q_0Q_3}{Q_0Q_2 - Q_1^2},$$

$$\sigma_2 = \frac{\begin{vmatrix} -Q_2 & Q_1 \\ -Q_3 & Q_2 \end{vmatrix}}{|M|} = \frac{Q_1Q_3 - Q_2^2}{Q_0Q_2 - Q_1^2}.$$

Вычисление величин σ_1 и σ_2 можно также производить с помощью итеративного алгоритма Берлекэмпа [2];

6) определяются номера позиций искажённых символов.

Реализуется с помощью алгоритма Ченя [8] или *непосредственным решением* уравнения

$$\widetilde{x}^2 + \sigma_1\widetilde{x} + \sigma_2 = 0. \qquad (1)$$

Известен и более быстрый, по сравнению с алгоритмом Ченя, метод Берлекэмпа [2], который, однако не работает в простом поле. В [9–12] предложены методы, также позволяющие ускорить процедуру Ченя.

Обычная формула для решения квадратных уравнений не работает в поле $GF(2^m)$. Поэтому для непосредственного способа решения уравнения (1) можно привести ссылки на следующие литературные источники [2, 13–15], в которых освещается вопрос о разложении многочленов над конечными полями.

Если имела место только одна ошибка, то номер ошибочного узла определяется из соотношений

$$Q_0 = \delta_{i_1}\widetilde{x}_{i_1}^0, \qquad Q_1 = \delta_{i_1}\widetilde{x}_{i_1} = Q_0\widetilde{x}_{i_1}.$$

Отсюда

$$\widetilde{x}_{i_1} = Q_1/Q_0; \qquad (2)$$

7) вычисляются величины ошибок.

Решая систему из двух уравнений

$$\delta_{i_1} + \delta_{i_2} = Q_0, \qquad \delta_{i_1}\widetilde{x}_{i_1} + \delta_{i_2}\widetilde{x}_{i_2} = Q_1,$$

получим

$$\left.\begin{aligned} \delta_{i_1} &= (Q_0\widetilde{x}_{i_2} - Q_1)/(\widetilde{x}_{i_2} - \widetilde{x}_{i_1}) \\ \delta_{i_2} &= (Q_1 - Q_0\widetilde{x}_{i_1})/(\widetilde{x}_{i_2} - \widetilde{x}_{i_1}) \end{aligned}\right\}. \qquad (3)$$

Если произошла одна ошибка, то

$$\delta_{i_1} = Q_0; \qquad (4)$$

8) производится коррекция искажённых символов:

$$f_{i_1} = \widetilde{f}_{i_1} - \delta_{i_1}, \qquad f_{i_2} = \widetilde{f}_{i_2} - \delta_{i_2}.$$

Последовательный алгоритм декодирования А3

Для реализации этого алгоритма необходимо выполнить следующие вычисления.

1) вычисляются значения искажённого полинома в контрольных узлах.

Для 1-го контрольного узла имеем:

$$f^*(\beta_1) = \sum_{i=0}^{s}\widetilde{f}_i\, L_S^{(i)}(\beta_1) =$$

$$= -\sum_{i=0}^{s}\widetilde{f}_i \prod_{l=2}^{4}(x_i - \beta_l)/(\beta_1 - \beta_l).$$

При вычислении значений искажённого полинома $\widetilde{f}(x)$ во 2-ом, 3-ем и 4-ом контрольных узлах кроме информационных символов $\widetilde{f}_i$ используются значения $\widetilde{f}(\beta_1)$, $\widetilde{f}(\beta_2)$, $\widetilde{f}(\beta_3)$ контрольных символов принятой кодовой последовательности:

$$f^*(\beta_2) = [\sum_{i=0}^{s}\widetilde{f}_i + \widetilde{f}(\beta_1)]\, L_{S_1}^{(i)}(\beta_2),$$

$$f^*(\beta_3) = [\sum_{i=0}^{s}\widetilde{f}_i + \widetilde{f}(\beta_1) + \widetilde{f}(\beta_2)]\, L_{S_2}^{(i)}(\beta_3),$$

$$f^*(\beta_4) = [\sum_{i=0}^{s}\widetilde{f}_i + \widetilde{f}(\beta_1) + \widetilde{f}(\beta_2) + \widetilde{f}(\beta_3)]\, L_{S_3}^{(i)}(\beta_4),$$

где $S_1 = S \cup \{\beta_1\}$, $S_2 = S \cup \{\beta_1, \beta_2\}$,

$S_3 = S \cup \{\beta_1, \beta_2, \beta_3\}$,

$$L_{S_1}^{(i)}(\beta_2) = -\prod_{l=3}^{4}(x_i - \beta_l)/(\beta_2 - \beta_l),$$

$$L_{S_2}^{(i)}(\beta_3) = -(x_i - \beta_4)/(\beta_3 - \beta_4),$$

$$L_{S_3}^{(i)}(\beta_4) = -1;$$

2) определяются значения невязок:

$$R_1 = \tilde{f}(\beta_1) - f^*(\beta_1),$$
$$R_2 = \tilde{f}(\beta_2) - f^*(\beta_2),$$
$$R_3 = \tilde{f}(\beta_3) - f^*(\beta_3),$$
$$R_4 = \tilde{f}(\beta_4) - f^*(\beta_4),$$

где $\tilde{f}(\beta_1)$, $\tilde{f}(\beta_2)$, $\tilde{f}(\beta_3)$, $\tilde{f}(\beta_4)$ - значения контрольных символов принятого сообщения.

Если $R_1 = R_2 = R_3 = R_4 = 0$, то ошибок нет;

3) вычисляются величины синдромов:

$$Q_0 = R_4,$$
$$Q_1 = R_4\beta_4 + R_3(\beta_3 - \beta_4),$$
$$Q_2 = R_4\beta_4^2 + R_3(\beta_3^2 - \beta_4^2) + R_2(\beta_2 - \beta_3)(\beta_2 - \beta_4),$$
$$Q_3 = R_4\beta_4^3 + R_3(\beta_3^3 - \beta_4^3) + R_2(\beta_2 - \beta_3)(\beta_2 - \beta_4)(\beta_2 + \beta_3 + \beta_4) + R_1(\beta_1 - \beta_2)(\beta_1 - \beta_3)(\beta_1 - \beta_4);$$

4) вычисление определителя матрицы $|M|$, определение нормализованных элементарных симметрических функций (σ_1, σ_2), места ($\tilde{x}_{i_1}$, $\tilde{x}_{i_2}$) и величины (δ_{i_1}, δ_{i_2}) ошибок, исправление искажённых символов производится аналогично последовательному алгоритму А2.

На рис. 1 показана блок-схема алгоритма программы исправления двойной ошибки по алгоритму А3 (при $L^{(i)}(x) = const$, $\beta_3 = 1$, $\beta_4 = 0$).

В табл. 1 приведены формулы для определения количества операций в поле $GF(2^m)$ при вычислении синдромов Q_μ (с учётом операций при вычислении невязок R_j) с использованием различных алгоритмов вычисления контрольных символов (параллельного - А1, последовательных - А2, А3).

Анализируя таблицу, приходим к выводу о том, что применение последовательных алгоритмов при коррекции двойных ошибок уменьшает объём вычислений по сравнению с параллельным алгоритмом. Процедура декодирования упрощается также за счёт возможности анализа величины определителя матрицы синдромов $|M|$.

Таблица 1. Количество операций в поле $GF(2^m)$ при вычислении синдромов Q_μ

Операции	Коэффициент $L^{(i)}(\beta_j)$	Параллельный алгоритм	Последовательный алгоритм	
		алгоритм А1	алгоритм А2	алгоритм А3
$\oplus$	$L^{(i)}(\beta_j) \neq const$	$8n-8$	$7n-4$	$7n$
	$L^{(i)}(\beta_j) = const$	$4n-4$	$4n+2$	$4n-4$
	$L^{(i)}(\beta_j) = const$, $\beta_3 = 1$, $\beta_4 = 0$	$4n-7$	$4n-1$	$4n-7$
$\otimes$	$L^{(i)}(\beta_j) \neq const$	$12n-24$	$3n+9$	$3n+11$
	$L^{(i)}(\beta_j) = const$	$4n-4$	$3n+3$	$3n$
	$L^{(i)}(\beta_j) = const$, $\beta_3 = 1$, $\beta_4 = 0$	$4n-10$	$3n-3$	$3n-6$
$\ominus$	$L^{(i)}(\beta_j) \neq const$	4	3	3
	$L^{(i)}(\beta_j) = const$	0	0	0

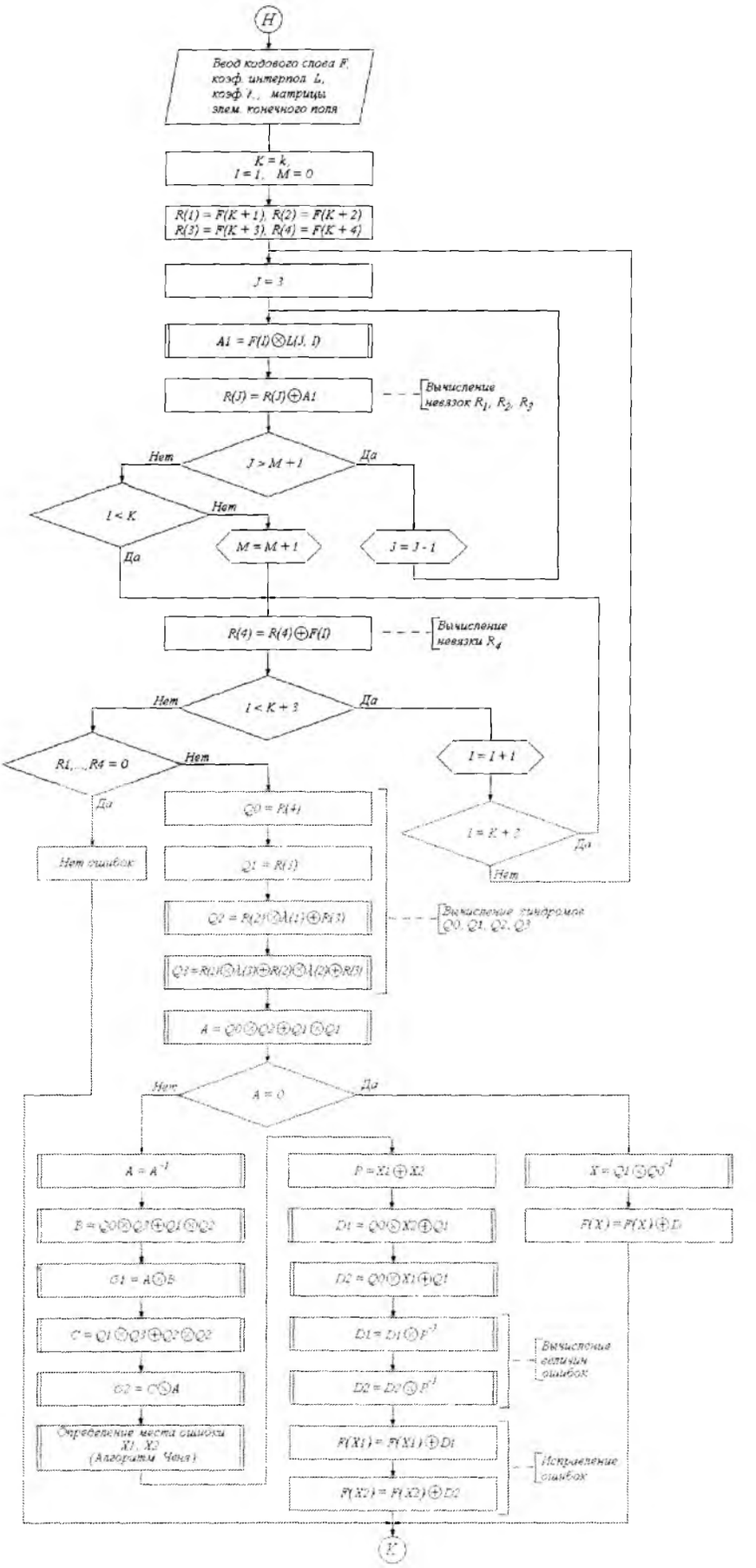

Рис. 1. Блок-схема алгоритма программы декодирования 2-ой ошибки

Выводы

Разработанные математические выражения и алгоритмы декодирования кода Лагранжа позволяют реализовать исправление двойной ошибки программным и аппаратным способами. При этом применение последовательных алгоритмов требует меньшего объёма вычислений по сравнению с параллельным алгоритмом.

Этапы декодирования кода Лагранжа соответствуют этапам алгоритмов декодирования, разработанным Питерсоном-Берлекэмпом. Это даёт возможность использовать известные и эффективные процедуры (например, алгоритм Ченя) при декодировании кода Лагранжа. Возможность анализа величины определителя матрицы синдромов позволяет упростить декодирование.

Список литературы

1. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки: Пер. с англ. /Под ред. Р.Л. Добрушина и С.И. Самойленко. – М.: Мир, 1976. – 596 с.

2. Берлекэмп Э. Алгебраическая теория кодирования. – М.: Мир, 1971. – 477 с.

3. Амербаев В.М. Теоретические основы машинной арифметики. – Алма-Ата: Наука, 1976. – 324 с.

4. Кубицкий В.И. Декодирование многократных ошибок кодами Лагранжа //Проблеми інформатизації та управління: Зб. Наук. праць: Вип. 4 (22). – К.: НАУ, 2007. – С. 86 – 92.

5. Нугманов Р.Н. Процедура исправления многократных ошибок кодом Лагранжа. – Электронная техника. Серия 10. 1979, вып. 1 (13). – С. 7 – 9.

6. Кубицкий В.И. Некоторые алгоритмы коррекции одиночной ошибки кодами с параллельной структурой. – В сб. «Диагностирование энергетических и электронных схем» / АН УССР. Ин-т проблем моделирования в энергетике. – Киев, 1990. – С. 60 – 66.

7. Патент №49052, Украина, МПК (2009) H03M 13/00. Пристрій для декодування одиночних недвійкових помилок / Жуков И.А., Кубицкий В.И., Синельников А.А.; заявл. 24.11.2009, № u 2009 12043; опубл. 12.04.2010. Бюл. №7.

8. Chien R.T. Cyclic decoding procedures for the Bose-Choudhuri-Hocquenghem codes. – IEEE Trans.Inform. Theory, IT-10, 1964. – P. 357 – 363.

9. Gore W. C. Generalized threshold decoding and the Reed-Solomon codes. – IEEE Trans. Inform. Theory, IT-15, 1969. – P. 78 – 81.

10. Gore W.C. Transmitting binary symbols with Reed-Solomon codes. – Proc. 7th Annual Princeton Conf. Information Scinces and Systems, (Dept. of Electrical Engineering, Princeton University, Princeton, NJ, 1973). – P. 495 – 499.

11. Mandelbaum D.A method of coding for multiple errors. – IEEE Trans. Inform. Theory, IT-14, 1968. – P. 518 – 521.

12. Mandelbaum D. Some results in decoding of certain maximal-distance and BCH codes. – Info. and Control, 20, 1973. – P. 232 – 243.

13. Мак-Вильямс Ф. Дж., Слоэн Н. Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ./Под ред. Л. А. Бассалыго. – М.: Связь, 1979. – 744 с.

14. Berlekamp E.R., Rumsey H. and Solomon G. On the solutions of algebraic equations over finite fields. – Inform. Control, 10, 1967. – P. 553 – 564.

15. Berlekamp E.R. Factoring polynomials over large finite fields. – Math. Comp., 24, 1970. – P. 713 – 735.