#1569420179: *On the Decoding Complexity of Cyclic Codes Up to the BCH Bound*

Property	Change Add	Value
Conference and *track*		**2011 IEEE International Symposium on Information Theory** - *2011 IEEE International Symposium on Information Theory*

Authors	Name	ID	Flag	Affiliation	Email	Country
	Davide Schipani	594695		University of Zurich	davide.schipani@math.uzh.ch	Switzerland
	Michele Elia	553745		Politecnico di Torino	eliamike@tin.it	Italy
	Joachim Rosenthal	151712		University of Zurich	rosenthal@math.uzh.ch	Switzerland

Presenter		presenter not specified
Registration		
Category		Eligible for ISIT Student Paper Award
Title		*On the Decoding Complexity of Cyclic Codes Up to the BCH Bound*
Abstract		THIS PAPER IS ELIGIBLE FOR THE STUDENT PAPER AWARD The standard algebraic decoding algorithm of cyclic codes $[n,k,d]$ up to the BCH bound t is very efficient and practical for relatively small n while it becomes unpractical for large n as its computational complexity is $O(nt)$. Aim of this paper is to show how to make this algebraic decoding computationally more efficient: in the case of binary codes, for example, the complexity of the syndrome computation drops from $O(nt)$ to $O(t\sqrt n)$, and that of the error location from $O(nt)$ to at most $\max \{ O(t\sqrt n), O(t^2\log(t)\log(n)) \}$.
Topics		Coding theory and practice; Communication theory
Session		The program is not yet visible (tpc)
DOI		
Status		accepted

Review manuscript	Document (show)	Pages	File size	Changed	MD5	Similarity score
		4	263,548	February 15, 2011 08:55:37 EST	9b7e6fa071c44d8ecb206b6b5925c3f2	13

Final manuscript		Can upload 5 pages until May 31, 2011 00:00:00 EDT.

Personal notes

Reviews

You are a TPC member for this conference.

2 Reviews

Review 1 (Reviewer B)

Importance	Technical Level	Novelty	Presentation	Recommendation
Extremely Important (5)	Extremely high technical level (5)	Very Novel (4)	Excellent (5)	Strongly Recommend (5)

Strengths (What are the key strengths of this paper?)

The papers deals with the decoding complexity of the class of algebraic error correcting codes that is the most widely used nowadays.
Their possible use in new standards, such as SSD's, is hampered by the
high cost of the evaluation steps in their decoding procedure.
This paper shows that the above-mentioned complexity drops
drastically using the new algorithm by the same authors.

Weaknesses (What are the major weaknesses of this paper?)

The authors sometimes use complacent, somewhat informal, expressions, such as "the big advantage" or "Outstanding is in particular", that show their enthusiasm for their results.
I suggest they reword such sentence to a more sober tone, as fit for
a scientific paper.

They report extensively the literature on cyclic-code decoding with traditional methods. There are other competing methods that should be cited and that are based on polynomial evaluations: decoding with general error locator polynomials ([1] and [3] may suffice) and advanced iterative decoding
([2] may suffice).
I suggest the authors reports on these as well.

[1] @InCollection{
AUTHOR = "T. Mora and E. Orsini",

TITLE = "Decoding cyclic codes: the {C}ooper philosophy",

BOOKTITLE = {Gr{\"o}bner Bases, Coding, and Cryptography},

EDITOR = "M. Sala and T. Mora and L. Perret and S. Sakata and C. Traverso",

PAGES = "69--91",

PUBLISHER = "RISC Book Series, Springer",

ADDRESS = "Heidelberg",

YEAR = "2009"

}

[2] @InCollection{
AUTHOR = "E. Guerrini and A. Rimoldi",

TITLE = "{F}{G}{L}{M}-like decoding: from {F}itzpatrick's approach to recent developments",

BOOKTITLE = {Gr{\"o}bner Bases, Coding, and Cryptography},

EDITOR = "M. Sala and T. Mora and L. Perret and S. Sakata and C. Traverso",

PAGES = "197--218",

PUBLISHER = "RISC Book Series, Springer",

ADDRESS = "Heidelberg",

YEAR = "2009"

}

[3] @Article{ ,

author = "E. Orsini and M. Sala",

title = "Correcting errors and erasures via the syndrome variety",

journal = "J. Pure Appl. Algebra",

year = "2005",

volume = "200",

pages = "191--226",

issues = "1-2",

fjournal = "Journal of Pure and Applied Algebra"

}

Comments and Recommendation (Please give the reasoning for your overall recommendation and any additional comments you wish to add.)

I strongly suggest acceptance because this paper improves
both theoretically and in practice the most important procedure
for nowadays algebraic decoding in industrial application.
Moreover, the paper presentation is crystal clear.

Student Paper Award (This paper is eligible for the student paper award. Do you think it would rank among the top ten papers out of the 500 submitted papers in that category? If so, explain why.)

I believe this paper is eligible for the student paper award.
Such an improvement in a theoretical problem with so deep
applications is very rarely seen.

Review 2 (Reviewer C)

Importance	Technical Level	Novelty	Presentation	Recommendation
Average Importance (3)	Good technical level (4)	Average Novelty (3)	Good (4)	Recommend (4)

Strengths (What are the key strengths of this paper?)

The authors propose computationally efficient probabilistic decoding algorithm for BCH codes correcting up to t=[(d-1)/2] errors, where d is the BCH-designed-distance of the code. Actually, the authors consider (but did not write it clearly) the case when the length n of the code is large (n tends to infinity) and d is not too large (d/n tends to zero). The proposed decoding algorithm consists of the following steps.
1. Compute the syndrome using the Frobenius automorphism like in [6], [21].
2. Apply the classical Berlekamp-Massey algorithm to find error-locator polynomial.
3. Find the roots of the error-locator polynomial using Cator-Zassenhaus probabilistic factorization algorithm, get locations of the errors.
4. Find values of errors (for nonbinary case) using Forney algorithm accelerated by efficient polynomial evaluation algorithm.

Weaknesses (What are the major weaknesses of this paper?)

The authors estimate the expectation of the decoding complexity of their probabilistic algorithm and compare it with maximum decoding complexity of the deterministic classical algorithm. This is not fare. At least it should be clearly explained.

In classical case "good" codes are usually considered, where d/n=cost and n tends to infinity. For good codes the average complexity of the proposed algorithm is n^2 log^2 n and it is larger than the complexity n^2 of the classical algorithms. The authors should emphasize that they consider nonclassical asymptotic when d/n -> 0.

Comments and Recommendation (Please give the reasoning for your overall recommendation and any additional comments you wish to add.)

The proposed algorithm is interesting. I recommend to accept the paper.

Comments.

"Decoding up to the BCH bound" is confusing. One can understand that you correct up to d errors.

The parameter t is not clearly defined. It is written: "Assuming that C has BCH bound t...". One can understand that t is the BCH-designed code distance.

It should be clearly written that the AVERAGE complexity is given.

Page 1. Second column. "the error pattern e(x) has no more than t errors" . May be better to say that e(x) has no more than t nonzero coefficients.

Page 3. First column. In item 1) Generate a random polynomial b(z) of degree t-1 .... Later in Remark 1: b(z)=z. You select polynomial of degree less than t-1. What is it?!

1 Summary review by TPC member

Review 1 (Reviewer A)

TPC recommendation

Strong accept (5)

TPC Recommendation Justification (Please give a justification for your recommendation, especially if the review scores vary widely or your recommendation differs significantly from those of the reviewers.)

This is an excellent paper with a completely new strong result

Student Paper Award (This paper is eligible for the student paper award. The TPC needs to identify 10-15 semifinalists for the award from among the 500 submitted eligible papers. Later the IT Society Awards committee will select up to three winners. If you think this paper is worthy of the award, please send a one page nomination to the TPC cochairs at isit2011@eng.tau.ac.il with "STUDENT AWARD NOMINATION" in the subject header. The TPC co-chairs and IT Society Awards committee will have access to the papers, reviews (including your TPC summary review) and the nominations of the finalists. (You need not write anything in the box here.))

I strongly recommend that the paper be considered for the Student Paper Award. Please see a detailed discussion given by referees B and C.

Discussion

Not a reviewer. Apr 16, 2011 04:20	A TPC MEMBER SUBMITTED THE FOLLOWING NOMINATION OF THIS PAPER FOR THE STUDENT PAPER AWARD: I nominate this paper for the ISIT 2011 Student Paper Award The authors design a novel decoding algorithm for cyclic codes that drastically reduces their decoding complexity if the designed code distance d is small relative to the block length n: More specifically, consider any cyclic code over the field F_{2^p} that has designed distance d with respect to the BCH bound: The new decoding algorithm corrects t = \floor{ (d-1)/2} errors and requires the order of Phi=max{t\sqrt{n}, t^2(log(t))(log(n))} multiplications. Thus, the algorithm reduces the best current complexity estimate O(nt) if t = o(n/ln^2 n): This is a major improvement of the classical decoding, which has employed the conventional Gorenstein-Peterson-Zierler procedure for five decades and has been in place since the invention of the Berlekamp-Massey algorithm. The new algorithm consists of 4 steps, two of which replace the conventional technique as follows: 1. Compute the syndrome using O (t\sqrt{n}) multiplications via the Frobenius automorphism (conventional decoding has complexity O(nt)): 2. Find error-locator polynomial using O(t^2) operations (keep the classical Berlekamp-Massey algorithm). 3. Find error locations using O (Phi) multiplications via the Cantor-Zassenhaus probabilistic algorithm and the Shankís algorithm (the conventional Chien search has complexity O(nt)): 4. Find error values for nonbinary codes (keep the Forney algorithm with some accelerations possible). As an extension to the submitted paper, the authors may consider the probability of failure in the Cantor-Zassenhaus algorithm and detail the number of additions used throughout the algorithm. From the theoretical perspective, it would be interesting to reduce decoding complexity for the BCH codes of a given code rate, in which case the designed distance has the order of n/ log n: In summary, high-rate cyclic codes that have a relatively small minimum distance can be used in numerous applications that require low input/output error rates. In this regard, the proposed algorithm achieves two important goals. It brings a major new development to decoding algorithms of general cyclic codes and Ölls the void for their new applications. I strongly recommend the paper for Student Paper Award.