Diss. ETH No. 14961

Algebraic Coding for Iterative Decoding

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZURICH

for the degree of
Doctor of Technical Sciences

presented by
PASCAL O. VONTOBEL

born 21. August 1972
citizen of Oetwil am See (ZH)
dipl. El.-Ing. ETH

accepted on the recommendation of
Prof. Dr. Hans-Andrea Loeliger, examiner
Prof. Dr. R. Michael Tanner, co-examiner
Prof. Dr. Joachim Rosenthal, co-examiner

2003

Abstract

Since the publication of Shannon's 1948 paper "A Mathematical Theory of Communication" the quest has been on to find practical channel coding schemes that live up to the promises given by Shannon. Traditionally, coding theory focused on finding codes with large minimum distance and then to find an efficient decoding algorithm for such a code. In the realm of iterative decoding the picture is reversed: given an iterative decoding algorithm, one has to look out for codes that are suitable for such an algorithm.

To understand iterative decoding algorithms, it is advantageous to have a basic knowledge of factor graphs and the summary-product algorithm. Therefore, in a first step we show how the detection problems in a data transmission system can be modeled very naturally by factor graphs and solved with the help of the most popular instances of the generic summary-product algorithm, namely the sum-product and the max-product algorithm. We also show how different iteratively decodable channel codes fit very naturally into this picture.

For loop-less factor graphs the summary-product algorithm gives back the desired results; for loopy factor graphs the results are only approximations to the desired ones. As we do not want that the summary-product algorithm becomes prohibitively computationally intense, we have to bound the local state space sizes. Under these circumstances, it seems favorable in our applications at hand to perform a sub-optimal algorithm on a loopy factor graph than to perform an optimal algorithm on a loop-less factor graph. One reason for this phenomenon lies in the fact that under the above restrictions much stronger codes can be achieved when allowing factor graphs with cycles than without cycles.

In order to apply the summary-product algorithm successfully, experimental evidences seem to indicate that it is advisable that the factor graph looks locally tree-like, i.e. that there are no short cycles. This helps the messages of the summary-product algorithm to be as independent as possible. To be able to construct factor graphs of codes having these desirable properties, our next step is therefore to consider constructions of graphs having large girth, i.e. graphs whose length of the shortest cycle is large. We then unify different constructions of graphs that have a large girth and we propose some extensions.

Finally, we come to the heart of our thesis, namely the algebraic construction of codes suitable for iterative decoding. Based on graphs with large girth, we propose various algebraic constructions of regular and irregular low-density parity-check codes and turbo codes. Especially by using more complex subcodes than simple parity-check subcodes and by using bit nodes of different degrees, one can obtain a rich class of codes.

Apart from this main line, we treat several topics that are still within the subject at hand. Namely, we discuss why codes which have a loopless Tanner graph representation cannot be asymptotically good; we give a shorter and more intuitive proof of this fact than available in the literature. We unify different algorithms that can be used to perform the sum-product update rule for an indicator function of a subcode, namely the BCJR algorithm, the one-sweep algorithm, and decoding on the dual code. Finally, we propose some variations of a lower bound first given by Tanner on the minimum distance of codes.

Keywords: Digital data transmission, channel coding, iterative decoding, factor graphs, graphs with large girth, finite geometries, summary-product algorithm, sum-product algorithm, max-product algorithm, low-density parity-check codes, turbo codes, algebraic code constructions.

Kurzfassung

Seit der Publikation von Shannons Artikel "A Mathematical Theory of Communication" im Jahre 1948 wird versucht, praktische Kanalcodierungsverfahren zu finden, die die von Shannon aufgezeigen Versprechen einlösen. Traditionelle Codierungsverfahren zielten darauf hin, Codes mit grosser Minimaldistanz zu konstruieren und nachher für diese Codes effiziente Decodieralgorithmen zu finden. In der Welt der iterativen Decodierung liegt das Problem anders: gegeben sei ein iterativer Decodieralgorithmus, finde Codes, die für diesen Algorithmus geeignet sind.

Um iterative Decodieralgorithmen verstehen zu können, ist es von Vorteil, über ein Basiswissen bezüglich Faktor-Graphen und dem Summier-Produkt-Algorithmus zu verfügen. In einem ersten Schritt werden wir deshalb zeigen, wie die Detektionsprobleme, die bei der digitalen Datenübertragung auftreten, auf natürliche Weise durch Faktor-Graphen dargestellt und mit Hilfe von spezifischen Instanzen des generischen Summier-Produkt-Algorithmus' gelöst werden können, nämlich dem Summe-Produkt- und dem Max-Produkt-Algorithmus. Des weiteren zeigen wir, wie verschiedene iterativ decodierbare Codes in dieses Bild passen.

Für Faktor-Graphen ohne Schleifen liefert der Summier-Produkt-Algorithmus die gewünschten Resultate; für Faktor-Graphen mit Schleifen jedoch sind die Resultate nur Approximationen der gewünschten Resultate. Da wir vermeiden wollen, dass die Komplexität des Summier-Produkt-Algorithmus' zu gross wird, verlangen wir, dass die Grösse der lokalen Zustandsräume beschränkt ist. Unter dieser Voraussetzung scheint es in den uns interessierenden Problemkreisen von Vorteil zu sein, einen suboptimalen Algorithmus auf einem Graphen mit Schleifen

anstatt einem optimalen Algorithmus auf einem Graphen ohne Schleifen laufen zu lassen. Ein Grund für dieses Verhalten liegt in der Tatsache, dass unter den obigen Einschränkungen viel stärkere Codes erreicht werden können, wenn Schleifen erlaubt sind als wenn keine Schleifen erlaubt sind.

Experimentelle Resultate deuten darauf hin, dass es zur erfolgreichen Anwendung des Summier-Produkt-Algorithmus' günstig ist, wenn der Faktor-Graph lokal wie ein Baum aussieht, mit anderen Worten, dass er keine kurzen Schleifen besitzt. Dadurch sind die Nachrichten des Summier-Produkt-Algorithmus' so weit unabhängig wie möglich. Damit Konstruktionen von Faktor-Graphen mit diesen gewünschten Eigenschaften möglich werden, betrachten wir in einem nächsten Schritt die Konstruktion von Graphen mit grosser Taillenweite, d.h., Graphen bei denen die Länge der kleinsten Schleife gross ist. Wir vereinheitlichen verschiedene Konstruktionsansätze von Graphen mit grosser Taillenweite und schlagen einige Erweiterungen vor.

Das Herzstück der vorliegenden Arbeit wird dann die algebraische Konstruktion von Codes sein, die für die iterative Decodierung geeignet sind. Basierend auf Graphen mit grosser Taillenweite schlagen wir verschiedene algebraische Konstruktionen von Low-Density-Parity-Check-Codes und von Turbo-Codes vor. Insbesondere die Verwendung von komplexeren Subcodes (verglichen mit einfachen Parity-Check-Subcodes) und von Bitknoten verschiedener Grade liefert eine grosse Klasse von Codes.

Neben diesem Hauptstrang behandeln wir ein paar weitere Gebiete, die zum Themenbereich passen. So erklären wir, warum Codes, die durch schleifenlose Tanner-Graphen repräsentiert werden können, asymptotisch nicht gut sein können; dazu geben wir einen kürzeren und intuitiveren Beweis als in der Literatur verfügbar. Ferner zeigen wir die Gemeinsamkeiten von verschiedenen Algorithmen auf, die für die Durchführung der Summe-Produkt-Aufdatierungsregeln einer Subcode-Indikatorfunktion verwendet werden können; diese Algorithmen sind der BCJR-Algorithmus, der One-Sweep-Algorithmus, und das Decodieren auf dem dualen Code. Schliesslich schlagen wir verschiedene Variationen einer von Tanner eingeführten unteren Schranke für die Minimaldistanz von Codes vor.

Stichworte: Digitale Datenübertragung, Kanalcodierung, iterative Decodierung, Faktor-Graphen, Graphen mit grosser Taillenweite, endliche Geometrien, Summier-Produkt-Algorithmus, Summe-Produkt-Algorithmus, Max-Produkt-Algorithmus, Low-Density-Parity-Check-Codes, Turbo-Codes, algebraische Code-Konstruktionen.