Polar Codes for Channel and Source Coding

THÈSE N° 4461 (2009)
PRÉSENTÉE LE 15 JUILLET 2009
À LA FACULTÉ INFORMATIQUE ET COMMUNICATIONS
LABORATOIRE DE THÉORIE DES COMMUNICATIONS
PROGRAMME DOCTORAL EN INFORMATIQUE, COMMUNICATIONS ET INFORMATION

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
POUR L'OBTENTION DU GRADE DE DOCTEUR ÈS SCIENCES

PAR

Satish Babu KORADA

acceptée sur proposition du jury:
Prof. M. Hasler, président du jury
Prof. R. Urbanke, Dr N. Macris, directeurs de thèse
Prof. E. Arikan, rapporteur
Prof. A. Montanari, rapporteur
Prof. E. Telatar, rapporteur

Suisse
2009
Abstract

The two central topics of information theory are the compression and the transmission of data. Shannon, in his seminal work, formalized both these problems and determined their fundamental limits. Since then the main goal of coding theory has been to find practical schemes that approach these limits.

Polar codes, recently invented by Arıkan, are the first “practical” codes that are known to achieve the capacity for a large class of channels. Their code construction is based on a phenomenon called “channel polarization”. The encoding as well as the decoding operation of polar codes can be implemented with $O(N \log N)$ complexity, where $N$ is the blocklength of the code.

We show that polar codes are suitable not only for channel coding but also achieve optimal performance for several other important problems in information theory. The first problem we consider is lossy source compression. We construct polar codes that asymptotically approach Shannon’s rate-distortion bound for a large class of sources. We achieve this performance by designing polar codes according to the “test channel”, which naturally appears in Shannon’s formulation of the rate-distortion function. The encoding operation combines the successive cancellation algorithm of Arıkan with a crucial new ingredient called “randomized rounding”. As for channel coding, both the encoding as well as the decoding operation can be implemented with $O(N \log N)$ complexity. This is the first known “practical” scheme that approaches the optimal rate-distortion trade-off.

We also construct polar codes that achieve the optimal performance for the Wyner-Ziv and the Gelfand-Pinsker problems. Both these problems can be tackled using “nested” codes and polar codes are naturally suited for this purpose. We further show that polar codes achieve the capacity of asymmetric channels, multi-terminal scenarios like multiple access channels, and degraded broadcast channels. For each of these problems, our constructions are the first known “practical” schemes that approach the optimal performance.

The original polar codes of Arıkan achieve a block error probability decaying exponentially in the square root of the block length. For source coding, the gap between the achieved distortion and the limiting distortion also vanishes exponentially in the square root of the blocklength. We explore other polar-like code constructions with better rates of decay. With this generalization,
we show that close to exponential decays can be obtained for both channel
and source coding. The new constructions mimic the recursive construction of
Arikan and, hence, they inherit the same encoding and decoding complexity.
We also propose algorithms based on message-passing to improve the finite
length performance of polar codes.

In the final two chapters of this thesis we address two important problems
in graphical models related to communications. The first problem is in the area
of low-density parity-check codes (LDPC). For practical lengths, LDPC codes
using message-passing decoding are still the codes to beat. The current anal-
ysis, using density evolution, evaluates the performance of these algorithms
on a tree. The tree assumption corresponds to using an infinite length code.
But in practice, the codes are of finite length. We analyze the message-passing
algorithms for this scenario. The absence of tree assumption introduces corre-
lations between various messages. We show that despite this correlation, the
prediction of the tree analysis is accurate.

The second problem we consider is related to code division multiple ac-
cess (CDMA) communication using random spreading. The current analysis
mainly focuses on the information theoretic limits, i.e., using Gaussian in-
put distribution. However in practice we use modulation schemes like binary
phase-shift keying (BPSK), which is far from being Gaussian. The effects of
the modulation scheme cannot be analyzed using traditional tools which are
based on spectrum of large random matrices. We follow a new approach using
tools developed for random spin systems in statistical mechanics. We prove a
tight upper bound on the capacity of the system when the user input is BPSK.
We also show that the capacity depends only on the power of the spreading
sequences and is independent of their exact distribution.

Keywords: Polar codes, low-complexity schemes, channel coding, source
coding, Wyner-Ziv problem, Gelfand-Pinsker problem, multi-terminal scenar-
ios, exponent of polar codes, Reed-Muller Codes, belief propagation, LDPC
codes, density evolution, CDMA communication, statistical mechanics, inter-
opolation method.
Résumé

Les deux sujets centraux de la théorie de l'information sont la compression et la transmission des données. Shannon, dans son travail fondamental, formalisa ces deux problèmes et détermi- na les limites théoriques ultimes associées. Depuis, le but principal de la théorie du codage a été de trouver des schémas de faible complexité qui s’approchent de ces limites.

Les codes polaires (polar codes), inventés récemment par Arıkan, sont les premiers codes pratiques qui atteignent la capacité, pour une large classe de canaux. La construction de ces codes est basée sur un phénomène appelé “polarisation du canal”. Les opérations de codage, et de décodage basé sur une méthode d’éliminations successives, peuvent être implémentées avec une complexité $O(N \log N)$ où $N$ est la longueur du code.

Comme nous le montrons, les codes polaires sont non seulement bien adaptés pour le codage de canal, mais atteignent la performance optimale de plusieurs autres problèmes importants en théorie de l’information. Le premier problème que nous considérons est le codage de source avec pertes. Nous construisons des codes polaires qui atteignent la limite ultime donnée par la fonction de distorsion de Shannon pour une large classe de sources. Nous montrons que cette performance optimale est atteinte en choisissant un code polaire adapté au “canal-test” qui apparaît naturellement dans l’expression de Shannon pour la fonction de distorsion. L’opération de codage combine l’algorithme d’éliminations successives d’Arıkan avec un nouvel ingrédient crucial appelé “l’arrondi aléatoire”. Les deux opérations, le codage et le décodage, peuvent être implémentées avec une complexité de $O(N \log N)$. Il s’agit du premier schéma qui est de faible complexité tout en atteignant la limite ultime donnée par la fonction de distorsion.

Nous construisons aussi des codes polaires qui sont optimaux pour les problèmes de Wyner-Ziv et de Gelfand-Pinsker. Dans ces deux problèmes, la performance optimale est atteinte grâce à des codes “emboités”, et les codes polaires s’appliquent de façon très naturelle dans ce contexte. Nous montrons aussi que les codes polaires sont optimaux pour les canaux asymétriques, pour des scénarios multi-terminaux comme le canal à accès multiple et le canal broadcast dégradé. Pour chacun de ces problèmes, nos constructions sont les premières connues qui soient de faible complexité tout en atteignant la perfor-

iii
mance optimale.

Les codes polaires initiaux d’Arıkan, pour le codage de canal, atteignent une probabilité d’erreur de bloc décroissant exponentiellement avec la racine carrée de la taille du bloc. Pour le codage de source, la différence entre la distorsion atteinte et la limite ultime décroît aussi exponentiellement en fonction de la racine carrée de la longueur du bloc. Nous explorons d’autres constructions de codes polaires avec de meilleurs taux de décroissance. Avec ces généralisations, nous montrons que des décroissances quasi-exponentielles peuvent être obtenues pour ces deux situations. Les nouvelles constructions mimiquent la construction récursive d’Arıkan, et donc héritent de la même complexité de codage et décodage. Nous proposons aussi des algorithmes basés sur la propagation de messages pour améliorer la performance des codes polaires pour les longueurs finies.

Les deux chapitres finaux de cette thèse s’attachent à deux problèmes importants concernant les modèles sur les graphes pour les communications. Le premier est dans le domaine des codes de parité de basse densité (LDPC). Pour des longueurs utilisées dans la pratique, les codes LDPC avec le décodeur de propagation de messages, restent encore les codes à battre. L’analyse, utilisant l’évolution de densité, évalue la performance de ces algorithmes sur un arbre. L’hypothèse de l’arbre correspond à l’utilisation d’un code de longueur infinie, mais en pratique ceux-ci sont de longueur finie. Nous analysons la propagation de messages pour ce dernier scenario. Sans l’hypothèse de l’arbre des corréations entre les messages sont introduites. Nous montrons que malgré ces corrélations, la prédiction de l’analyse sur l’arbre est correcte.

Le second problème que nous considérons est relié au canal à accès multiple par répartition en code (CDMA) avec étalement aléatoire. L’analyse usuelle porte essentiellement sur les entrées à distribution Gausienne. Néanmoins, en pratique on utilise des schémas de modulation par déplacement de phase (par exemple BPSK) qui sont loins d’être Gaussiens. Les effets de ces modulations ne peuvent pas être analysés avec les outils traditionnels qui sont basés sur la théorie des grandes matrices aléatoires. Nous suivons une nouvelle approche utilisant les méthodes développées pour les systèmes de spin aléatoires en mécanique statistique. Nous prouvons une borne supérieure optimale sur la capacité du système pour des entrées BPSK. Nous montrons aussi qu’il y a une capacité dépend seulement de la puissance des séquences d’étalement et est indépendante du détail de la distribution.

Mots clés: codes polaires, schémas de faible complexité, codage de canal, codage de source, problème de Wyner-Ziv, problème de Gelfand-Pinsker, scénarios multi-terminaux, exposants des codes polaires, codes de Reed-Muller, propagation de messages, codes LDPC, évolution de densité, communication CDMA, mécanique statistique, méthode d’interpolation.
Contents

Abstract i
Résumé iii
Acknowledgments v
Contents vii

1 Introduction 1
  1.1 Source and Channel Model . . . . . . . . . . . . . . . . . . . 2
  1.2 Existing Low-Complexity Schemes . . . . . . . . . . . . . . 3
    1.2.1 Channel Coding . . . . . . . . . . . . . . . . . . . . . . 4
    1.2.2 Source Coding . . . . . . . . . . . . . . . . . . . . . . 7
  1.3 Polar Codes . . . . . . . . . . . . . . . . . . . . . . . . . . . 9
  1.4 Contribution of this Thesis . . . . . . . . . . . . . . . . . . 10
    1.4.1 Polar Codes: Low-Complexity Schemes with optimal
          performance . . . . . . . . . . . . . . . . . . . . . . . . . . . 11
    1.4.2 Improved Polar Codes . . . . . . . . . . . . . . . . . . . 12
    1.4.3 Rigorous Results for Graphical Models . . . . . . . . . 13
  1.5 Organization of the Thesis . . . . . . . . . . . . . . . . . . . 15
  1.6 Notation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 16
  1.7 Useful Facts . . . . . . . . . . . . . . . . . . . . . . . . . . . 17

2 Channel Coding: A Review 21
  2.1 Basic Channel Transform . . . . . . . . . . . . . . . . . . . . 22
  2.2 Recursive Application of the Basic Transform . . . . . . . . 24
  2.3 Channel Polarization . . . . . . . . . . . . . . . . . . . . . . 28
  2.4 Polar Codes Achieve Channel Capacity . . . . . . . . . . . . . 30
  2.5 Complexity . . . . . . . . . . . . . . . . . . . . . . . . . . . . 35
    2.5.1 Encoding and Decoding . . . . . . . . . . . . . . . . . . . 35
    2.5.2 Code Construction . . . . . . . . . . . . . . . . . . . . . 36
  2.6 Simulation Results and Discussion . . . . . . . . . . . . . . . 38
  2.A Appendix . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 39
## 3 Source Coding

- **3.1 Rate-Distortion** .......................................................... 41
- **3.2 Successive Cancellation Encoder** .................................. 42
- **3.3 Polar Codes Achieve the Rate-Distortion Bound** ........... 45
- **3.4 Value of Frozen Bits Does Not Matter** ......................... 51
- **3.5 Simulation Results and Discussion** ............................. 55
- **3.A Appendix** ................................................................... 57

## 4 Multi-Terminal Scenarios

- **4.1 Wyner-Ziv Problem** ................................................... 60
- **4.2 Gelfand-Pinsker Problem** ........................................... 64
- **4.3 Lossless Compression and Slepian-Wolf Problem** ........... 68
- **4.4 One-Helper Problem** .................................................. 71
- **4.5 Non-Binary Polar Codes** ............................................ 72
  - **4.5.1 Asymmetric Channels** .......................................... 73
  - **4.5.2 Degraded Broadcast Channels** ............................... 73
  - **4.5.3 Multiple Access Channels** .................................... 75
- **4.A Appendix** ................................................................... 77

## 5 Exponent of Polar Codes

- **5.1 Channel Transform using an $\ell \times \ell$ Matrix** ............. 82
- **5.2 Polarizing Matrices** ..................................................... 85
- **5.3 Exponent of Source Coding** ........................................ 88
- **5.4 Exponent of Channel Coding** ...................................... 91
- **5.5 Duality of Exponents** ................................................. 92
- **5.6 Bounds on Exponent** .................................................. 95
  - **5.6.1 Lower Bound** ....................................................... 96
  - **5.6.2 Upper Bound** ....................................................... 97
  - **5.6.3 Improved Upper Bound** ........................................ 98
- **5.7 Construction Using BCH Codes** .................................. 100
- **5.A Appendix** ................................................................... 104

## 6 Extensions and Open Questions

- **6.1 RM Codes as Polar Codes and Some Consequences** ....... 109
  - **6.1.1 Minimum Distance of Polar Code** .......................... 110
  - **6.1.2 Dumer's Recursive Decoding** ............................... 112
- **6.2 Performance under Belief Propagation** ......................... 112
  - **6.2.1 Successive Decoding as a Particular Instance of BP** ... 112
  - **6.2.2 Overcomplete Representation: Redundant Trellises** ... 114
  - **6.2.3 Choice of Frozen Bits** ........................................ 115
- **6.3 Compound Channel** .................................................... 116
- **6.4 Non-Binary Polar Codes** ............................................ 117
- **6.5 Matrices with Large Exponent** .................................... 118
- **6.6 Complexity Versus Gap** ............................................ 118
## Contents

7 Exchange of Limits ........................................ 119  
7.1 Introduction ............................................. 119  
7.2 Expansion ................................................ 121  
7.3 Case of Large Variable Degree ............................ 123  
7.4 Case of Small Variable Degree ............................ 128  
7.5 Extensions ................................................. 136  

8 Capacity of CDMA ........................................ 137  
8.1 Introduction ............................................... 137  
8.2 Statistical Mechanics Approach ........................... 139  
8.3 Communication Setup ...................................... 142  
8.4 Tanaka's Conjecture ....................................... 143  
8.5 Concentration of Capacity ................................. 144  
8.6 Independence of Capacity with respect to the Spread-  

### Bibliography ................................. 157  
### Curriculum Vitae ............................ 167