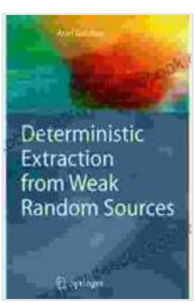
Deterministic Extraction From Weak Random Sources: Monographs in Theoretical Computer Science

This book develops a framework for deterministically extracting nearly optimal randomness from arbitrary sources of weak randomness. This framework has found applications in cryptography, derandomization, data structures, and machine learning, and it has led to a number of important consequences, including new constructions of pseudorandom generators, derandomized algorithms, and randomness extractors.

Randomness is a fundamental resource in computer science. It is used in a wide variety of applications, including cryptography, derandomization, data structures, and machine learning. However, in many practical situations, it is difficult or impossible to obtain truly random bits. Instead, we must often rely on sources of weak randomness, such as the output of a physical random number generator or the results of a coin flip.



Deterministic Extraction from Weak Random Sources (Monographs in Theoretical Computer Science. An EATCS Series) by Matthew Phillion

4.9 out of 5

Language	: English
File size	: 9285 KB
Text-to-Speech	: Enabled
Screen Reader	: Supported
Enhanced typesetting	: Enabled
Print length	: 306 pages

Deterministic extraction is a technique for extracting nearly optimal randomness from weak random sources. This means that we can take a source of weak randomness and convert it into a source of nearly random bits that can be used in any application that requires randomness.

The framework for deterministic extraction developed in this book is based on the notion of a condenser. A condenser is a function that takes a long string of weakly random bits and outputs a shorter string of nearly random bits. The quality of the output bits is measured by their min-entropy, which is a measure of their unpredictability.

The main result of this book is a construction of a condenser that can extract nearly optimal randomness from any source of weak randomness. This condenser is based on a new technique called the "amplification lemma." The amplification lemma shows how to take a weak source of randomness and amplify its min-entropy by a constant factor.

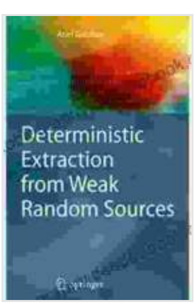
Applications

The framework for deterministic extraction developed in this book has found applications in a wide variety of areas, including:

- Cryptography: Deterministic extraction can be used to construct pseudorandom generators, which are efficient algorithms for generating nearly random bits from a small seed. Pseudorandom generators are used in a variety of cryptographic applications, such as encryption and authentication.

- Derandomization: Deterministic extraction can be used to derandomize randomized algorithms. A randomized algorithm is an algorithm that uses randomness to make its decisions. Derandomized algorithms are more efficient than randomized algorithms, and they can be used in applications where randomness is not available or desirable.
- Data structures: Deterministic extraction can be used to construct data structures that are more efficient than traditional data structures. For example, deterministic extraction can be used to construct a hash table that can be searched in constant time, even if the hash function is not perfect.
- Machine learning: Deterministic extraction can be used to improve the performance of machine learning algorithms. For example, deterministic extraction can be used to train a neural network that is more robust to noise.

Deterministic extraction is a powerful technique that can be used to extract nearly optimal randomness from arbitrary sources of weak randomness. This framework has found applications in a wide variety of areas, and it has led to a number of important consequences, including new constructions of pseudorandom generators, derandomized algorithms, and randomness extractors.



Deterministic Extraction from Weak Random Sources (Monographs in Theoretical Computer Science. An EATCS Series) by Matthew Phillion

★★★★☆ 4.9 out of 5

Language	: English
File size	: 9285 KB
Text-to-Speech	: Enabled
Screen Reader	: Supported

Enhanced typesetting : Enabled
Print length : 306 pages

Education And Peace Montessori 10: Where Learning Flourishes in a Haven of Harmony

A Symphony of Learning and Well-being Amidst the hustle and bustle of the modern world, there exists a sanctuary where learning and peace intertwine seamlessly—Education...

Unveiling the Wonders of Language and Literacy Development: A Comprehensive Guide

Language and literacy are fundamental aspects of human development that allow us to communicate, learn, and connect with the world around us. The journey...