

Name: Arnob Bhowmik

Roll: 1907065

Dept. : CSE

A Parasitic Mechanism-Based Filter Pruning Method for Deep Convolutional Neural Networks

Xu Han, Lei Xue, Ying Xu, Keju Huang

The paper introduces a Parasitic Mechanism (PAM)-based filter pruning method for Deep Convolutional Neural Networks (CNNs) aimed at accelerating and compressing CNNs without pre-selected pruning standards. PAM creates parasitic layers attached to CNNs, which intelligently learn and apply pruning standards during training, thus maintaining original CNN performance. The method outperforms traditional pruning approaches in simulations, showcasing better pruning performance and offering a novel, efficient way to compress and accelerate CNNs.

An Algorithm Based on Hitting Set for SAT Problem

Youjun Xu; Yingrui Ma; Zi Li

The paper introduces an algorithm based on the hitting set for solving SAT problems efficiently. It employs the concept of complementarity in binary hitting set trees to evaluate the satisfiability of clause sets without needing redundant clauses or numbering maximum terms. This approach leads to an efficient method for determining the satisfiability of a given problem set, showing superior performance compared to algorithms based on resolution and extension rules. The proposed algorithm, CBHST, demonstrates its effectiveness through comparative analysis with established methods.

Cryptographic Hashing From Strong One-Way Functions

Justin Holmgren, Alex Lombardi

The paper presents a new approach to cryptographic hashing based on the concept of one-way product functions (OWPFs), introducing a family of computational assumptions for constructing hash families with properties akin to those of random oracles. By enhancing one-way functions with batch one-wayness, the authors construct collision-resistant hash families and address the long-standing challenge of deriving such hash functions from basic cryptographic primitives. This research opens a potential path for bypassing black-box separations in cryptography, proposing that OWPFs can be used to build cryptographic primitives in a black-box manner from these enhanced one-way functions.

