Mapping Combinational Circuits to Homogeneous Trellis-Constrained Codes

Christian Franck

Definitions

**Combinational Circuits**
A combinational circuit is a memoryless digital circuit in which the output is directly dependent on the input.

**Homogenous Trellis-Constrained Codes (HTCC)** [Frey and McKay, 1997]
An HTCC code is a generalization of Turbo-codes where all bits are constrained. An HTCC code $C_{\cap}$ is defined by constituent codes $C_1$, $C_2$, and a permutation matrix $\pi$, with $c \in C_{\cap} \iff (c \in C_1$ and $\pi c \in C_2)$.

Exemplary Mapping

**Combinational Circuit**

**HTCC Code**

Generalization
- Combinational circuits composed of NAND gates can be mapped to HTCC codes.
- Every combinational circuit can be built using only NAND gates.

Other Gates and Circuits

**XOR gate**

**Full Adder gate**

Cost of $k$-bit XOR gate: $1 + 5k$ nodes, and $8k$ edges.

Cost of $k$-bit Full-Adder gate: $2 + 12k$ nodes, and $4 + 16k$ edges.

Cryptographic Circuits

HTCCs can be used to represent cryptographic circuits for, e.g.,
- SHA256
- SIPHASH
- ...
and circuits for
- the computation of semi-primes, or
- the computation of discrete logarithms.

Circuit Evaluation

**Belief-Propagation Decoding**
Given the inputs, one can compute the outputs using belief-propagation.

**Maximum-Likelihood (ML) Decoding**
A ML-decoder could compute the inputs given the outputs and could for instance be used to break cryptographic functions.

Munich Workshop on Coding and Applications 2017 (MWCA 2017)