Mapping Combinational Circuits to Homogenous 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.

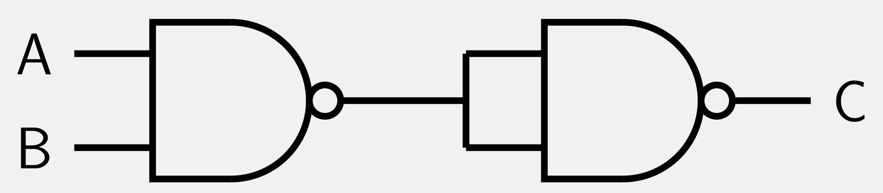
Homogenous Trellis-Constrained Codes (HTCC) [Frey and McKay, 1997]

An HTCC code is a generalization of Turbo-codes where all bits are constrained. An HTCC code $\mathbf{C}_\cap$ is defined by constituent codes $\mathbf{C}_1$, $\mathbf{C}_2$, and a permutation matrix $\boldsymbol{\pi}$, with

$$\mathbf{c} \in \mathbf{C}_\cap \Leftrightarrow (\mathbf{c} \in \mathbf{C}_1 \text{ and } \boldsymbol{\pi}\mathbf{c} \in \mathbf{C}_2).$$

Exemplary Mapping

Combinational Circuit



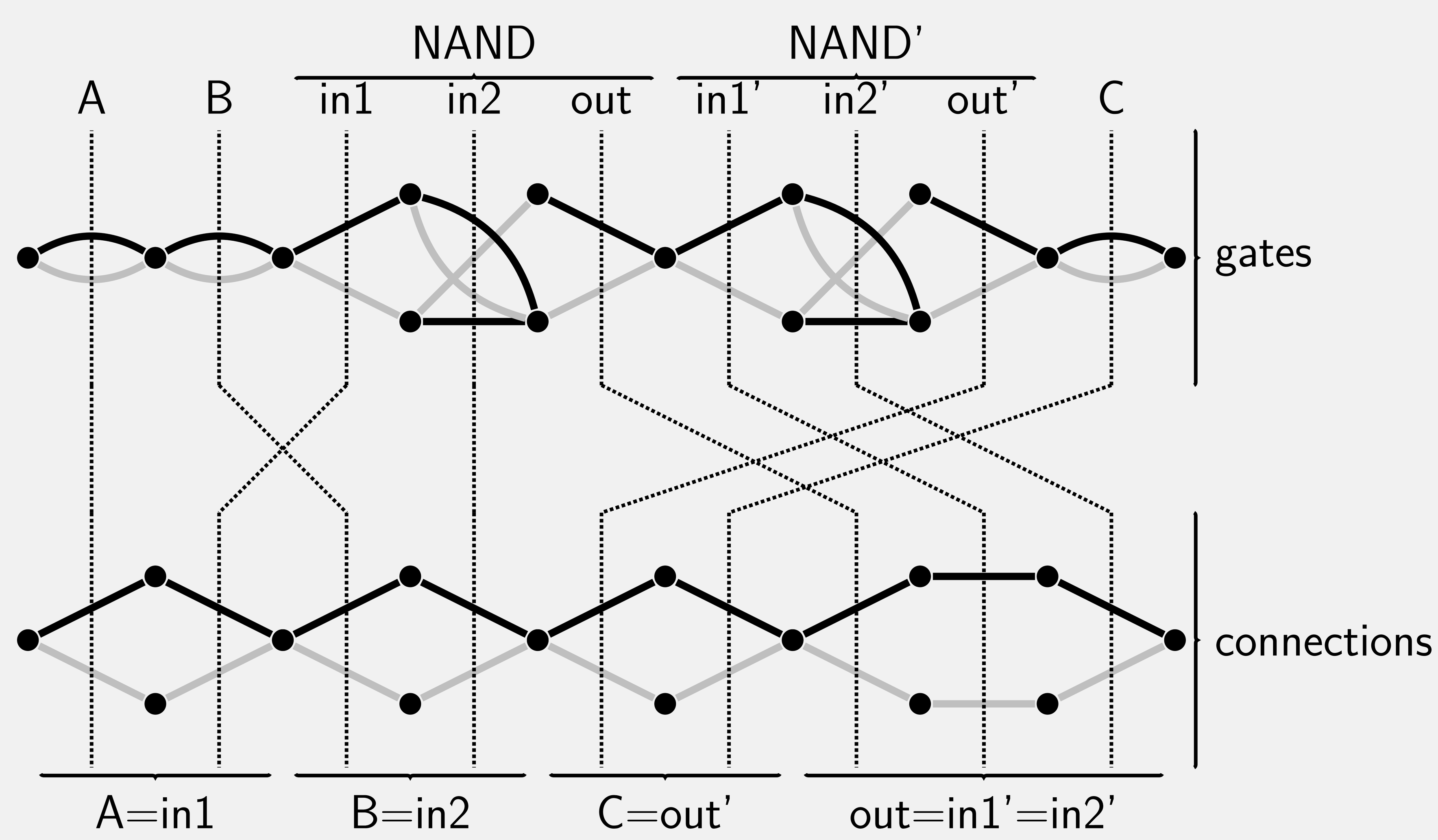
Generalization

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

$\Downarrow$

Every combinational circuit can be mapped to a HTCC Code.

HTCC Code

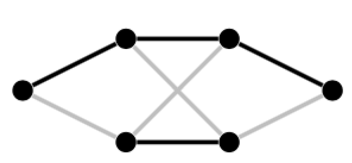


Other Gates and Circuits

XOR gate

in1	in2	out
0	0	0
0	1	1
1	0	1
1	1	0

(a) logic table



(b) trellis

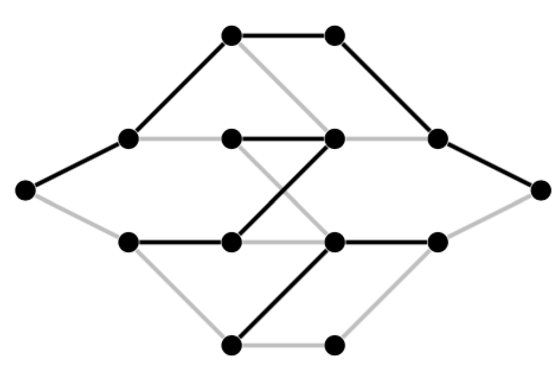
Figure 1: XOR gate

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

Full Adder gate

c_{in}	in1	in2	out	c_{out}
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

(a) logic table



(b) trellis

Figure 3: Full-Adder gate

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)