

# **On Some Properties of Reversible Boolean Functions**

**Pawel Kerntopf, Marek Szyprowski**

**Institute of Computer Science**

**Warsaw University of Technology**

**Warsaw, Poland**

**8<sup>th</sup> International Workshop on Boolean Problems**

**September 18, 2008**

# Overview

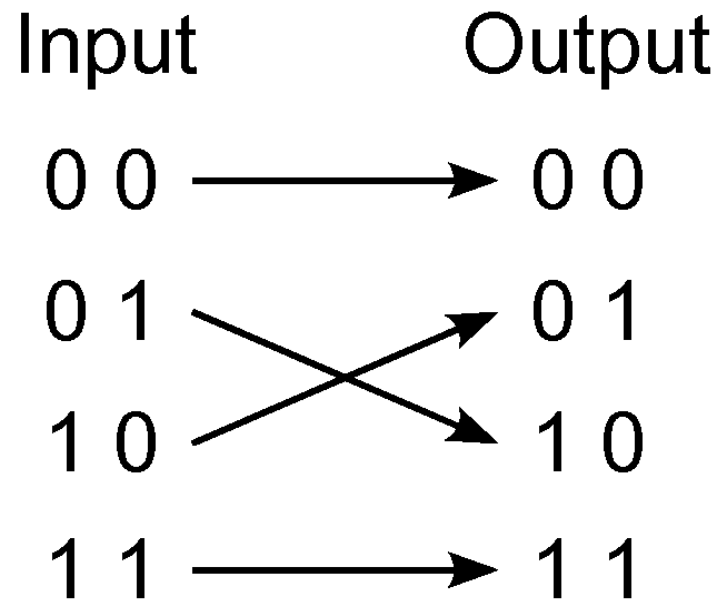
- Motivation
- Reversible functions
- Reversible vs. classical logic circuits
- Basic reversible gates and libraries
- Approaches to synthesis of reversible circuits
- Calculations of all optimal  $3 \times 3$  reversible circuits
- Previous work on decomposition types of reversible circuits
- New decomposition types
- Usage of NOT gates in optimal circuits
- Conclusions and open problems

# Motivation

- Reversible circuits enable to reduce energy dissipation (R. Landauer 1961, C. Bennett 1973)
- Quantum processes are inherently reversible (R. Feynman 1985)
  - ⊙ Logic synthesis for classical reversible circuits is a first step toward synthesis of quantum circuits
- Some important processing tasks are reversible
  - ⊙ Digital signal processing
  - ⊙ Cryptography
  - ⊙ Communication
  - ⊙ Computer graphics

# Reversible functions

- A completely specified  $n$ -input  $n$ -output Boolean function (referred to as  $n \times n$  function) is **reversible** iff it is a bijective mapping, i.e. output rows of its truth table can be obtained by permutation of the input rows.



# Reversible vs. classical circuits

- A circuit (a gate) is **reversible** iff it realizes a bijective mapping of inputs vectors into output vectors of a truth table of the circuit (gate)
  - ⊙ # inputs = # outputs
  - ⊙ reversible circuit consists only of reversible gates
  - ⊙ fan-out of each output = 1
  - ⊙ reversible circuits are cascade circuits
- Realization of arbitrary circuits (including irreversible) sometimes requires
  - ⊙ creation of additional output wires („garbage”)
  - ⊙ application of constant signals to some inputs
  - ⊙ application of temporary storage (i.e. wires that can be changed during computation, but must be restored by end of the computation)

# Basic reversible gates and libraries

⊙ (a) NOT (**N**)

$$a' = 1 \oplus a$$

⊙ (b) CNOT (**C**)

$$a' = a, b' = a \oplus b$$

⊙ (c) Toffoli (**T**)

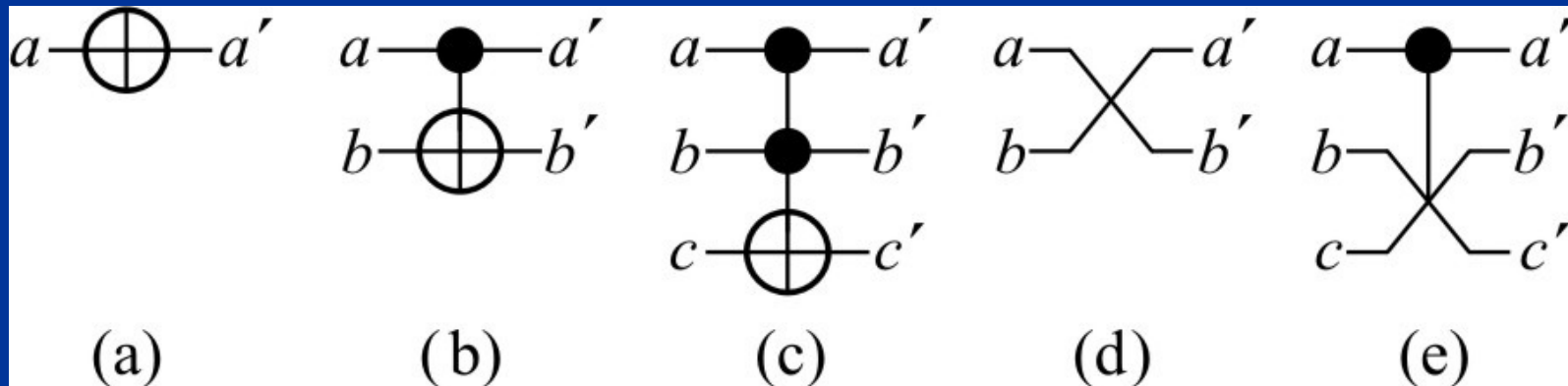
$$a' = a, b' = b, c' = c \oplus ab$$

⊙ (d) SWAP (**S**)

$$a' = b, b' = a$$

⊙ (e) Fredkin (**F**)

$$a' = a, \text{ if } a = 0 \text{ then } b' = b, c' = c, \\ \text{if } a = 1 \text{ then } b' = c, c' = b$$



Basic gate libraries: **NCT**, **NCTS**, **NCTSF**

# Previous work (1)

- **K. Iwama, Y. Kambayashi, S. Yamashita DAC 2002**
  - ⊙ equivalent transformations of reversible circuits
  - ⊙ canonical form
  - ⊙ no synthesis algorithm
- **V.V. Shende, A.K. Prasad, I.L. Markov, J.P. Hayes ICCAD 2002**
  - ⊙ synthesis of optimal 3-wire reversible circuits
  - ⊙ libraries of small optimal ckts.
  - ⊙ decomposition type
- **D.M. Miller, D. Maslov, G. Dueck DAC 2003**
  - ⊙ 2-stage transformation-based algorithm (called also the MMD algorithm) based on truth tables
- **A. Agrawal, N.K. Jha DATE 2004**
  - ⊙ a synthesis algorithm based on PPRM expressions

# Previous work (2)

- **P. Kerntopf DAC 2004**
  - ⊙ a synthesis algorithm based on decision diagrams
- **D.M. Miller, D. Maslov, G. Dueck quant-ph 2006**
  - ⊙ a synthesis algorithm based on RM spectra
- **University of Gent, Belgium and Portland State University, Portland, Oregon, USA 1999-2007**
  - ⊙ algorithms based on group-theoretic results, implemented using GAP tool
- **University of Bremen, Germany 2007-2008**
  - ⊙ algorithms based on SAT instances and quantified Boolean formulas (QBFs), implemented using modern SAT-solvers and QBF-provers

# Calculations of all optimal 3\*3 circuits

## Assumptions:

- Reversible specifications are realized without additional wires
- Libraries: NCT
- Cost of a circuit:
  - ⊙ gate count
  - ⊙ quantum cost (NOT and CNOT - 1, Toffoli gate - 5)

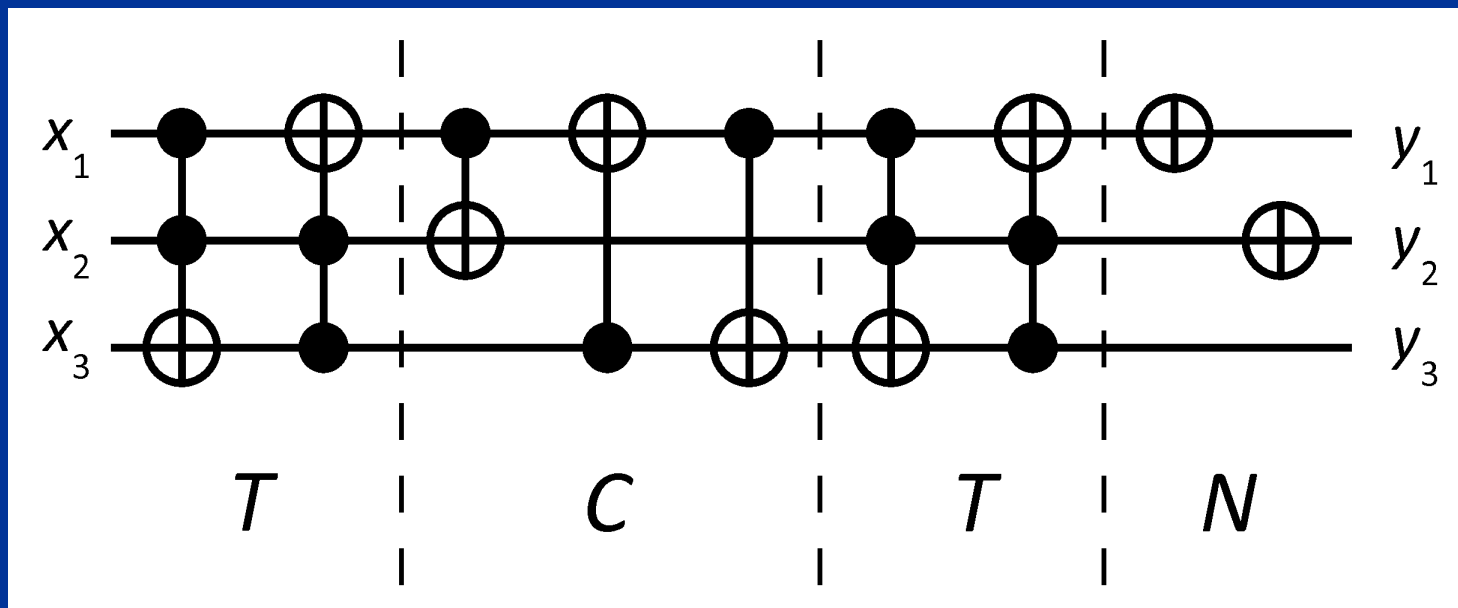
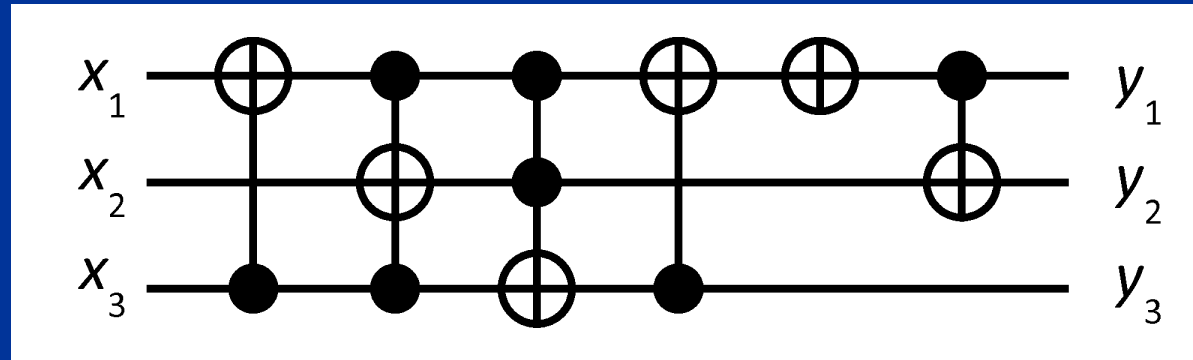
# Number of optimal circuits (gate count)

	average	maximal
3*3 (NCT)	27	1264

---

length of circuits	number of circuits
3	1
4	7
5	59
6	514
7	4603
8	38680
9	338514

# Decomposition type (T|C|T|N)



# Decompositon types (1)

## List of decomposition types

C|N|C

C|N|T / T|N|C

C|T|C|N / N|C|T|C

C|T|C

C|T|N / N|T|C

C|T|N|C / C|N|T|C

N|C|N

N|C|T / T|C|N

C|T|N|T / T|N|T|C

N|T|N

C|N|C|T / T|C|N|C

N|C|N|T / T|N|C|N

T|C|T

C|N|T|N / N|T|N|C

N|C|T|N / N|T|C|N

T|N|T

C|T|N|T / T|N|T|C

N|T|C|T / T|C|T|N

T|C|N|T / T|N|C|T

# Decompositon types (2)

GC	T C T N N T C T	T C N T T N C T	C T C N N C T C	C T N C C N T C	Optimal
13	10				
12	57	3			
11	327	70	36		
10	1609	779	753	6	
9	4820	3896	3748	938	
8	8826	9066	8651	7932	577
7	10340	11071	11225	13099	10253
6	7997	8513	8959	10482	17049
5	4206	4626	4682	5333	8921
4	1580	1715	1706	1913	2780
3	445	472	457	508	625
2	90	96	90	96	102
1	12	12	12	12	12
0	1	1	1	1	1
WA:	7.037	6.854	6.820	6.513	5.866

# Decompositon types (3)

QC	T C T N N T C T	T C N T T N C T	C T C N N C T C	C T N C C N T C	Optimal
Highest:	32	32	23	22	20
WA:	16.542	16.400	14.691	14.388	13.740

# Classification of 3\*3 functions

Let

$f(x_3, x_2, x_1)$  be a 3\*3 Boolean function

$$f(0,0,0) = (a_3, a_2, a_1)$$

$F_n$  is the set of all 3\*3 reversible functions  
for which  $n = a_3 + a_2 + a_1$

# Number of NOT gates (1)

## Gate count

#N	F <sub>0</sub>	F <sub>1</sub>	F <sub>2</sub>	F <sub>3</sub>	Total
0	5040				5040
1		14754	12786	4160	31700
2		354	2328	865	3547
3		12	6	15	33
Total	5040	15120	15120	5040	40320

## Quantum cost

#N	F <sub>0</sub>	F <sub>1</sub>	F <sub>2</sub>	F <sub>3</sub>	Total
0	5040				5040
1		14748	12876	4202	31826
2		366	2238	825	3429
3		6	6	13	25
Total	5040	15120	15120	5040	40320

# Number of NOT gates (2)

Gate count:

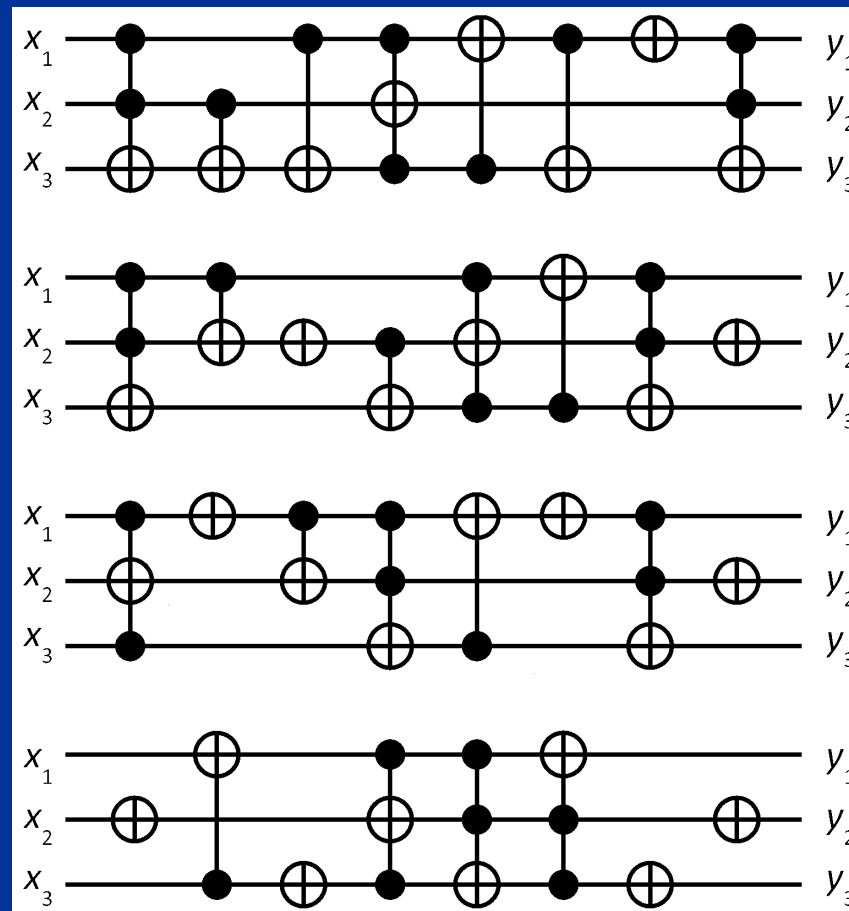
#N	F <sub>0</sub>	F <sub>1</sub>	F <sub>2</sub>	F <sub>3</sub>	Total
0	5040				5040
1		14754	12786	4160	31700
2	429	3867	9210	3203	16709
3		1014	1332	856	3202
4		24	66	6	96
Total	5469	19659	23394	8225	56747

Quantum cost:

#N	F <sub>0</sub>	F <sub>1</sub>	F <sub>2</sub>	F <sub>3</sub>	Total
0	5040				5040
1		14748	12876	4202	31826
2	423	3891	9042	3175	16531
3		948	1212	756	2916
4		24	54	6	84
Total	5463	19611	23184	8139	56397

# Number of NOT gates (3)

Four optimal circuits for the same function





# Conclusions and open problems

- We suppose that the presented experimental results can be used in the future to guide development of heuristic synthesis algorithms
- Open problems:
  - ⊙ How to decompose a reversible function in a way corresponding to a decomposition type?
  - ⊙ How to synthesize reversible functions with many NOT gates in search for minimal cost circuits?
  - ⊙ Is it possible to use templates for finding circuits with many NOT gates?