# Multi-Output Galois Field Sum of Products Synthesis with New Quantum Cascades

PORTLAND QUANTUM LOGIC GROUP

**Mozammel H A Khan**

East West University, BANGLADESH

**Marek A Perkowski**

Korea Advanced Institute of Science and Technology, KOREA

**Pawel Kerntopf**

Warsaw University of Technology, POLAND

# Agenda

- Previous Works
- Our Motivation
- MV Quantum Logic
- Ternary Galois Field Logic
- New Generalization of Ternary Toffoli Gate
- New Generalized Reversible Ternary Gate
- GFSOP Synthesis with Ternary Toffoli Gates
- GFSOP Synthesis with New Ternary Gates
- Experimental Results
- Conclusion

# Previous Works

## Reed-Muller Like Expression and Integer Fields

References (non-exhaustive) mentioned in the text

[1, 8, 12, 14 - 18, 20 - 25, 27, 31, 33, 36, 28 - 41]

Sorry!!! Full References are not mentioned here

### Summary

- Mainly Reed-Muller like expression
- Some Galois and Integer Field based
- Mainly quaternary or higher-valued
- Not Quantum technology based
- No benchmark exists. Converted binary benchmark into quaternary by grouping two bits

# Previous Works (Continued)

## MV Quantum Logic

- A. Muthukrishnan, and C. R. Stroud, Jr., "Multivalued logic gates for quantum computation", *Physical Review A,* Vol. 62, No. 5, Nov. 2000, 052309/1-8.

MV logic for QC system. Realization with linear ion trap devices. Too large circuits

- J. L. Brylinski and R. Brylinski, "Universal Quantum Gates", (to appear in *Mathematics of Quantum Computation*, CRC Press, 2002) LANL e-print quant-ph/010862.

Universality on ***n***-qudit gates. No design algorithm given

# Previous Works (Continued)
## MV Quantum Logic (continued)

- P. Picton, "A Universal Architecture for Multiple-Valued Reversible Logic", *Multiple-Valued Logic - An International Journal,* Vol. 5, 2000, pp. 27-37.

Universal architecture for MV reversible logic. Not quantum

- A. De Vos, B. Raa, and L. Storme, "Generating the group of reversible logic gates", *Journal of Physics A: Mathematical and General*, Vol. 35, 2002, pp. 7063-7078.

Proposed two ternary 1*1 gates and two ternary 2*2 gates. No synthesis method proposed

# Previous Works (Continued)

## MV Quantum Logic (continued)

- P. Kerntopf, "Maximally efficient binary and multi-valued reversible gates", *Booklet of 10th Intl Workshop on Post-Binary Ultra-Large-Scale Integration Systems (ULSI),* Warsaw, Poland, May 2001, pp. 55-58.

Proposed reversible MV gates. No synthesis method proposed

- M. Perkowski, A. Al-Rabadi, and P. Kerntopf, "Multiple-Valued Quantum Logic Synthesis", *Proc. of 2002 International Symposium on New Paradigm VLSI Computing,* Sendai, Japan, December 12-14, 2002, pp. 41-47.

Proposed quantum realization of MV Toffoli gate

# Previous Works (Continued)

## MV Quantum Logic (continued)

- A. Al-Rabadi, K. Dill, U. Kalay, (Ph.D. Theses). A. Mishchenko, A. Khlopotine, M. Perkowski and others at Portland State University since 1996 – research on GFSOP minimization and cascades.

# Summary

- Gates proposed without synthesis algorithm
- Some methods proposed but they produce too large circuits far from reality

# Previous Works (Continued)

## Galois Field Based Quantum Logic Synthesis

- A. Al-Rabadi, “Synthesis and Canonical Representations of Equally Input-Output Binary and Multiple-Valued Galois Quantum Logic: Decision Trees, Decision Diagrams, Quantum Butterflies, Quantum Chrestenson Gate, Multiple-Valued Bell-Einstein-Podolsky-Rosen Basis States”, Technical Report #2001/008, ECE Dept, PSU, 2001.

- A. Al-Rabadi, “Novel Methods for Reversible Logic Synthesis and Their Application to Quantum Computing”, *Ph. D. Thesis*, PSU, Portland, Oregon, USA, October 24, 2002.

# Previous Works (Continued)

## Galois Field Based Quantum Logic Synthesis Continued)

- A. Al-Rabadi, L. W. Casperson, M. Perkowski and X. Song, “Multiple-Valued Quantum Logic”, *Booklet of 11th Workshop on Post-Binary Ultra-Large-Scale Integration Systems (ULSI)*, Boston, Massachusetts, May 15, 2002, pp. 35-45.

- A. Al-Rabadi and M. Perkowski, “Multiple-Valued Galois Field S/D Trees for GFSOP Minimization and their Complexity”, *Proc. 31st IEEE Int. Symp. on Multiple-Valued Logic,* Warsaw, Poland, May 22-24, 2001, pp. 159-166.

# Previous Works (Continued)

## Galois Field Based Quantum Logic Synthesis (continued)

- M. Perkowski, A. Al-Rabadi, P. Kerntopf, A. Mishchenko, and M. Chrzanowska-Jeske, “Three-Dimensional Realization of Multivalued Functions Using Reversible Logic”, *Booklet of 10th Int. Workshop on Post-Binary Ultra-Large-Scale Integration Systems (ULSI),* Warsaw, Poland, May 2001, pp. 47- 53.

# Previous Works (Continued)

## Galois Field Based Quantum Logic Synthesis (continued)

### Summary

- Galois quantum matrices were proposed for swap and Toffoli gates without the proof that they can be built from only 1*1 and 2*2 gates
- Several regular structures for MV quantum logic were proposed, including cascades, but these cascades do not allow realization of powers of GFSOP and thus non-universal
- Canonical expansion of Post literals and arbitrary functions were shown

# Previous Works (Continued)

## Galois Field Based Quantum Logic Synthesis (continued)

### Summary (continued)

- No constructive method for GFSOP and cascade minimization were given, nor programs were written for them

- Factorized reversible cascades and complex gates were not proposed

# Our Motivation

- Very little has been published on synthesis algorithm for multi-output MV quantum circuit
- It is very important to look for efficient methods to synthesize multi-output GFSOP functions using quantum cascades
- We concentrate on quantum cascaded realization of ternary GFSOP functions

# Our Motivation (continued)

- We propose a new generalization of ternary Toffoli gate
- We propose a new complex ternary gate
- We propose GFSOP synthesis using cascade of Toffoli gates
- We propose factorized GFSOP synthesis using cascade of new complex gates

# MV Quantum Logic

MV quantum logic manipulates ***qudits***

Qudit states can be photon's polarization or an elementary particle's spin

Logic 0, 1, 2 are different ***qutrit*** states

Qutrit states are $|0\rangle, |1\rangle, |2\rangle$

# MV Quantum Logic (continued)

*Qudits* exit in a linear superposition of states and are characterized by a wavefunction.

It is possible to have slant 45° light polarizations corresponding to the linear superposition of

$$\psi = \frac{1}{2}\left[\sqrt{2}\left|0\right\rangle + \sqrt{2}\left|1\right\rangle\right]$$

# MV Quantum Logic (continued)

In ternary logic, the notion for the superposition is

$$\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$$

Measurement of these intermediate states yields that the qutrit is in one of the basis states $|0\rangle$ , $|1\rangle$ , or $|2\rangle$

**Entanglement:** Pairs of qutrits represent nine distinct states

$|00\rangle$, $|01\rangle$, $|02\rangle$, $|10\rangle$, $|11\rangle$, $|12\rangle$, $|20\rangle$, $|21\rangle$, $|22\rangle$

as well as all possible superpositions of the states

# MV Quantum Logic (continued)

Entanglement Example:

Two qutrits are:

$$\psi_1 = \alpha_1|0\rangle + \beta_1|1\rangle + \gamma_1|2\rangle$$

$$\psi_2 = \alpha_2|0\rangle + \beta_2|1\rangle + \gamma_2|2\rangle$$

These two qutrits together represent

$$\psi_{12} = \psi_1 \otimes \psi_2 = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \Lambda \ + \gamma_1\gamma_2|22\rangle$$

Quantum computing concepts are difficult

# MV Quantum Logic (continued)

Anything that changes a vector of qudit states can be considered as an operator

In a quantum circuit, wires do not carry ternary constants but correspond to 3-tuples of complex values, $\alpha$, $\beta$, and $\gamma$

Quantum logic gates map the complex values on their inputs to complex values on their outputs

# MV Quantum Logic (continued)

Operation of quantum gates is described by (unitary) matrix operations

Any quantum circuit is a composition of parallel and serial connections of blocks

- Serial connection of blocks corresponds to multiplication of their (unitary) matrices
- Parallel connection corresponds to Kronecker multiplication of their matrices

# Ternary Galois Field Logic

Elements of Ternary Galois Field $T = \{0, 1, 2\}$

Ternary Galois Field Operations

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| $\bullet$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

# Ternary Galois Field Logic (continued)

## Reversible Ternary Shift Operations

| Input | Operator Names, Symbols, and Equations | | | | | |
|---|---|---|---|---|---|---|
| Input $A$ | **B** $A$ | **SS** $A' = A + 1$ | **DS** $A'' = A + 2$ | **SlS** $A''' = 2A$ | **SlSS** $A^{\#} = 2A + 1$ | **SlDS** $A^{\wedge} = 2A + 2$ |
| 0 | 0 | 1 | 2 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 | 2 | 0 | 1 |
| 2 | 2 | 0 | 1 | 1 | 2 | 0 |

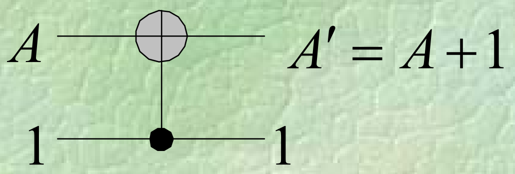
**B**: Buffer, **SS**: Single-Shift, **DS**: Dual-Shift, **SlS**: Self-Shift,
**SlSS**: Self-Single-Sift, **SlDS**: Self-Dual-Shift

## Gate Symbols

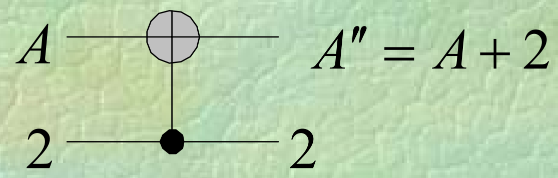

**B** **SS** **DS** **SlS** **SlSS** **SlDS**

# Ternary Galois Field Logic (continued)

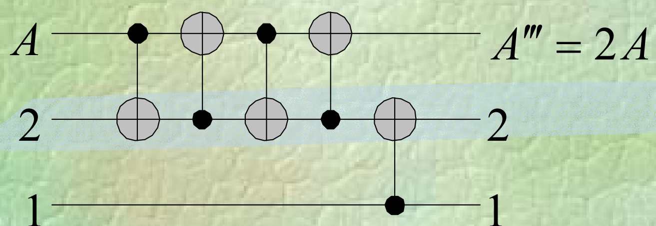
## Quantum Realization of Ternary Shift Gates



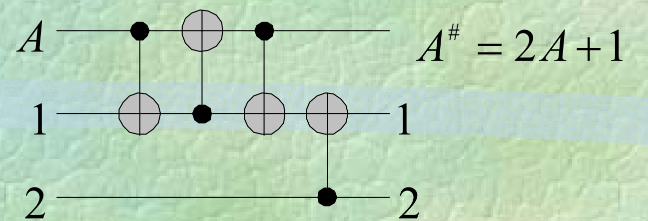

Single-Shift



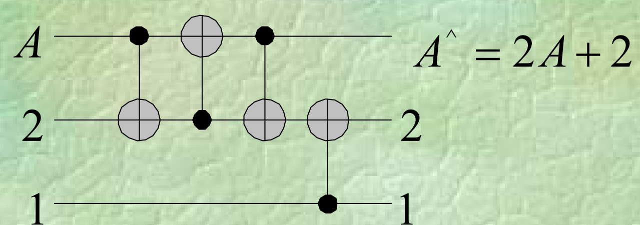

Dual-Shift




Self-Shift




Self-Single-Shift




Self-Dual-Shift

# Ternary Galois Field Logic (continued)

Conversion of one shift form to another shift form using ternary shift gates

| Input | Output | | | | | |
|---|---|---|---|---|---|---|
| | $A$ | $A'$ | $A''$ | $A'''$ | $A^{\#}$ | $A^{\wedge}$ |
| $A$ | | **SS** | **DS** | **SIS** | **SISS** | **SIDS** |
| $A'$ | **DS** | | **SS** | **SISS** | **SIDS** | **SIS** |
| $A''$ | **SS** | **DS** | | **SIDS** | **SIS** | **SISS** |
| $A'''$ | **SIS** | **SISS** | **SIDS** | | **SS** | **DS** |
| $A^{\#}$ | **SISS** | **SIDS** | **SIS** | **DS** | | **SS** |
| $A^{\wedge}$ | **SIDS** | **SIS** | **SISS** | **SS** | **DS** | |

# Ternary Galois Field Logic (continued)

GF3 Basic Literals of a Variable *A*

$$\{1, 2, A, A', A'', A''', A^{\#}, A^{\wedge}, A^{2}\}$$

All ternary literals, except $A^2$, are reversible

Reversible literal multiplied by 2 yield another reversible literal

$2 \cdot 1 = 2$ $\quad 2 \cdot 2 = 1$ $\quad 2A = A'''$ $\quad 2A' = A^{\wedge}$

$2A'' = A^{\#}$ $\quad 2A''' = A$ $\quad 2A^{\#} = A''$ $\quad 2A^{\wedge} = A'$

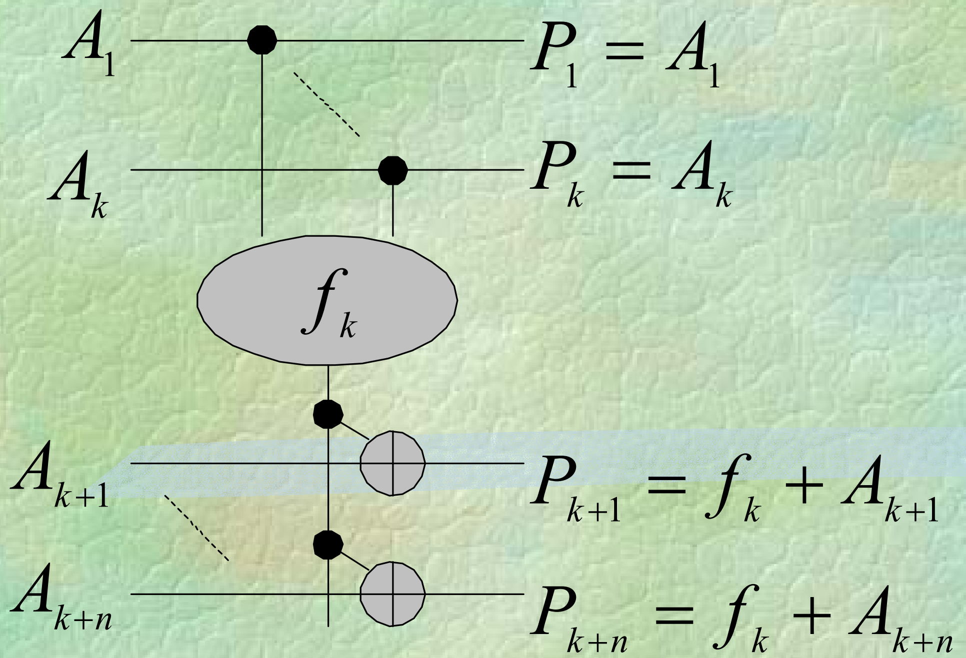
# Ternary Galois Field Logic (continued)

A ternary literal may have a power of only 2

$$A^3 = A \qquad A^4 = A^3 A = A^2$$

Ternary GFSOP $2 + AB'' + B^2 C' + A' C''$

# New Generalization of Ternary Toffoli Gate

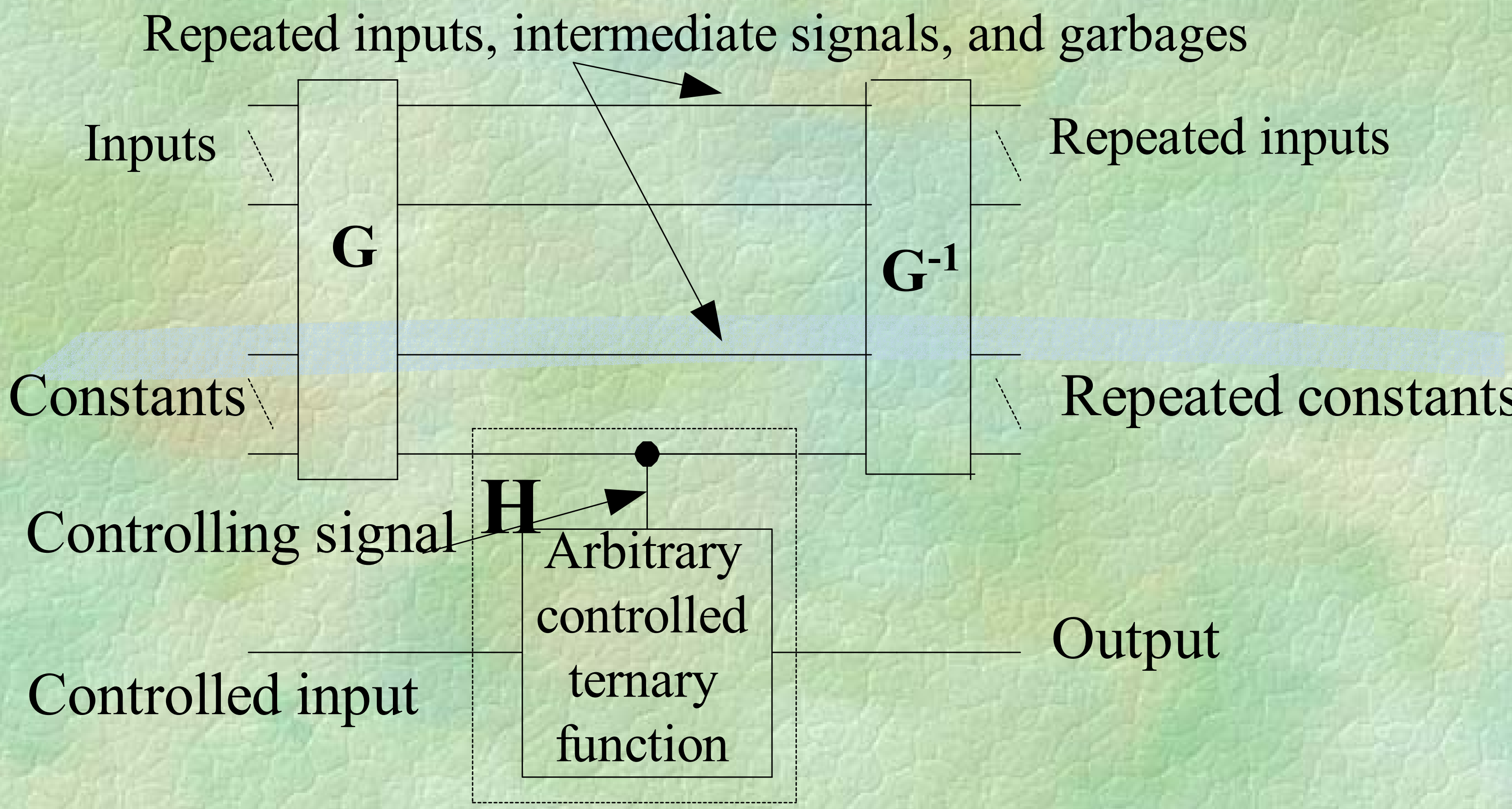



$f_k$ is an arbitrary ternary function of the input variables $A_1, A_2, \Lambda\ , A_k$

Depending on $f_k$ and the value of ***n*** many possible gates can be constructed

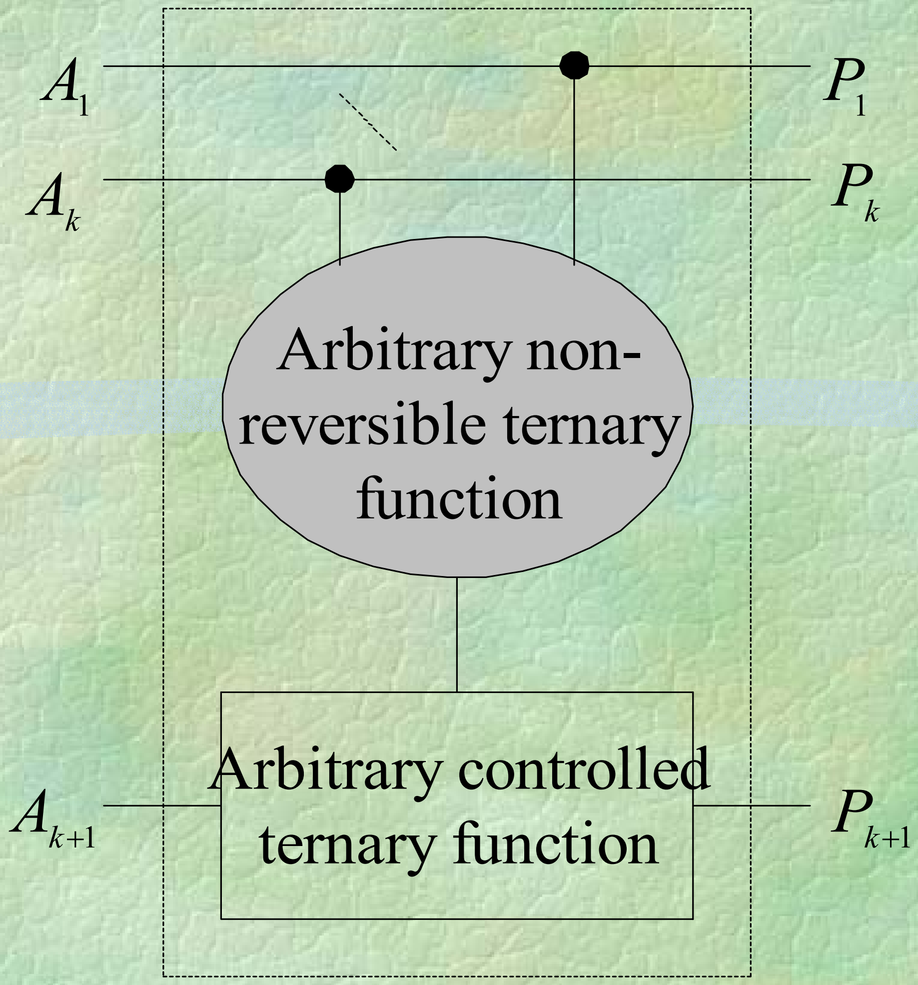
# New Generalization of Ternary Toffoli Gate (continued)

## Principle of creating arbitrary reversible gates



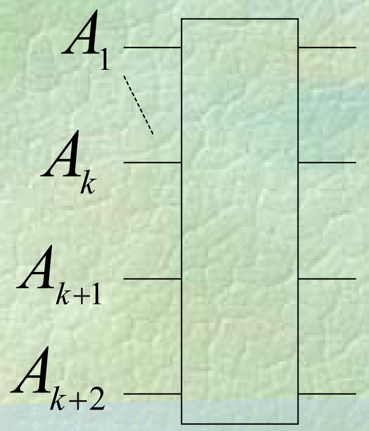
# New Generalization of Ternary Toffoli Gate (continued)

## Creating generalized ternary Toffoli gate



# New Generalized Reversible Ternary Gate

## Generalized Reversible Ternary Gate




$$P_1 = A_1$$

$$P_k = A_k$$

$$P_{k+1} = f_k A_{k+1} + A_{k+2}$$

$$P_{k+2} = f_k^* A_{k+1}^* + A_{k+2}^*$$

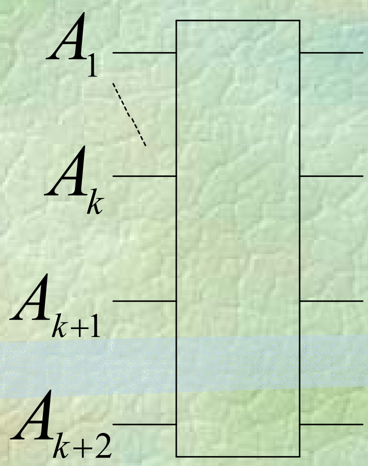
$f_k$ is an arbitrary ternary function of the input variables

$A_1, A_2, \Lambda\ , A_k$ $\qquad f_k^* \in \{f_k', f_k''\}$ $\qquad A_i^* \in \{A_i', A_i''\}$

- Depending on $f_k$ and the choice of the shift, many possible gates can be constructed

# New Generalized Reversible Ternary Gate (continued)

## Special Case of the Generalized Gate




$$P_1 = A_1$$

$$P_k = A_k$$

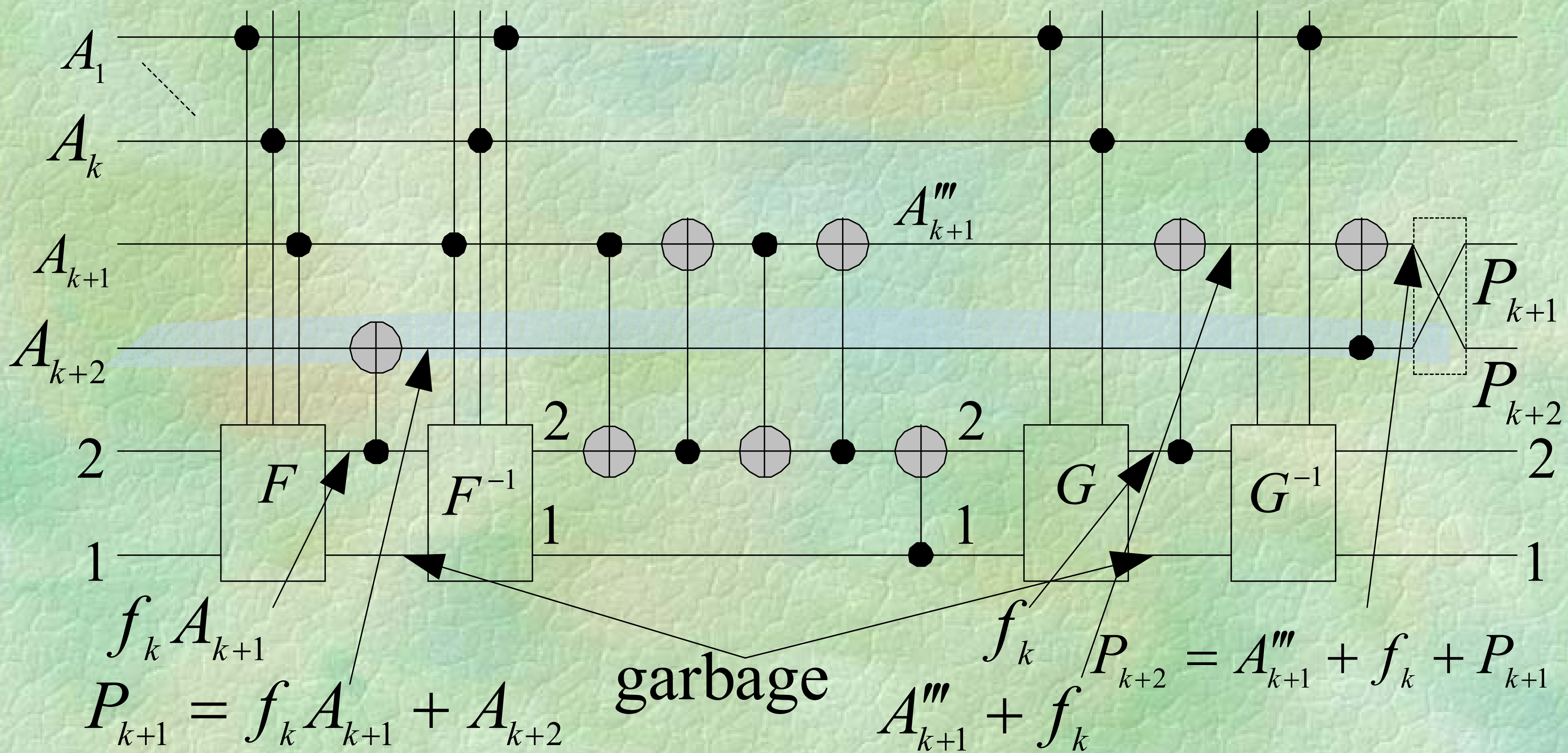
$$P_{k+1} = f_k A_{k+1} + A_{k+2}$$

$$P_{k+2} = f_k'' A'_{k+1} + A'_{k+2}$$

$$= P_{k+1} + A'''_{k+1} + f_k$$

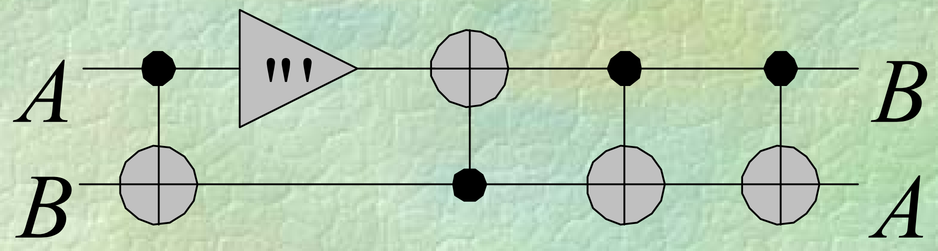
# New Generalized Reversible Ternary Gate (continued)

## Quantum Realization of the Gate



# New Generalized Reversible Ternary Gate (continued)

## Quantum Realization of Ternary Swap Gate



# New Generalized Reversible Ternary Gate (continued)

## Different Modes of Operation of the Gate

| Mode | $A_{k+1}A_{k+2}$ | $P_{k+1}$ | $P_{k+2}$ |
|---|---|---|---|
| A | 00 | 0 | $f_k$ |
| B | 01 | 1 | $f_k'$ |
| C | 02 | 2 | $f_k''$ |
| D | 10 | $f_k$ | $f_k^{\wedge}$ |
| E | 11 | $f_k'$ | $f_k'''$ |
| F | 12 | $f_k''$ | $f_k^{\#}$ |
| G | 20 | $f_k'''$ | 1 |
| H | 21 | $f_k^{\#}$ | 2 |
| I | 22 | $f_k^{\wedge}$ | 0 |

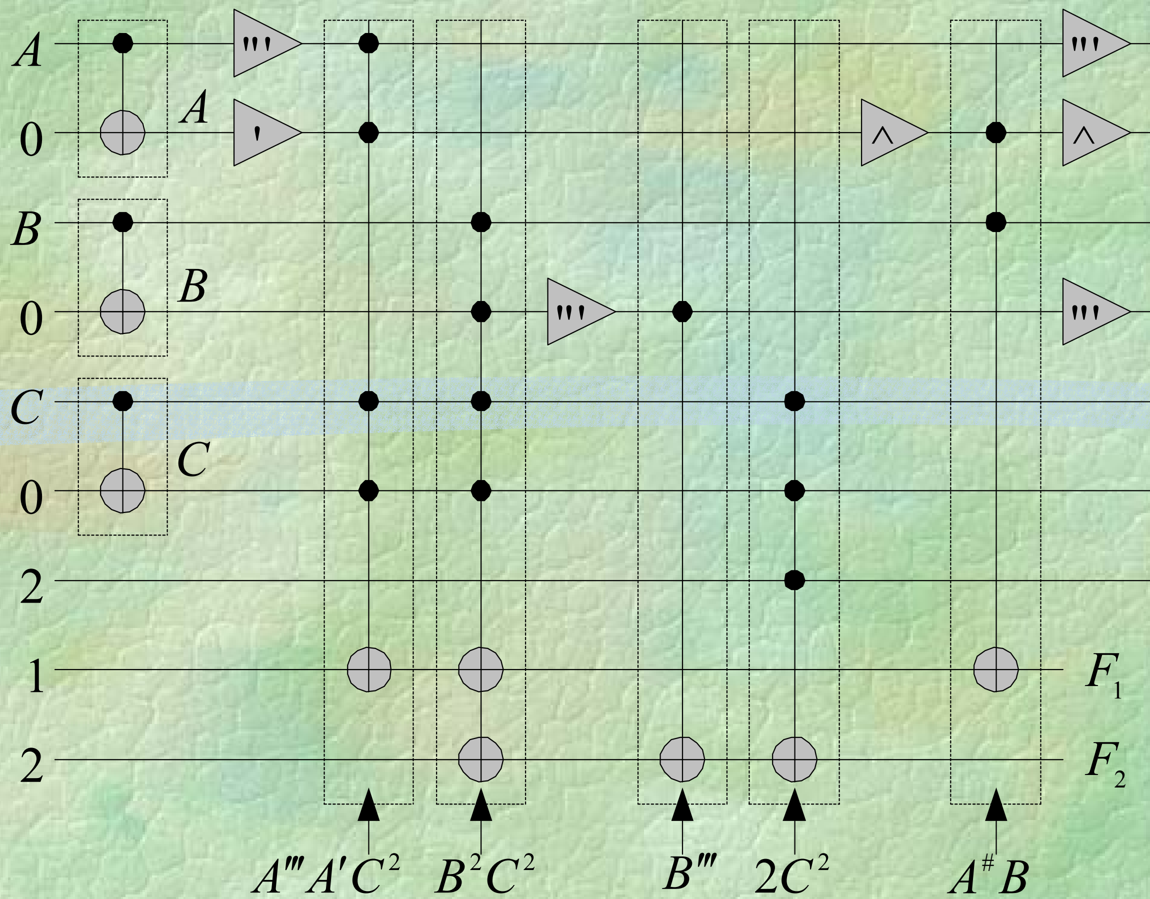
# New Generalized Reversible Ternary Gate (continued)

## Different Modes of Operation of the Gate (continued)

| Mode | $A_{k+1}A_{k+2}$ | $P_{k+1}$ | $P_{k+2}$ |
|---|---|---|---|
| J | $0G$ | $G$ | $G+f_k$ |
| K | $1G$ | $f_k+G$ | $f_k^{\wedge}+G$ |
| L | $2G$ | $f_k'''+G$ | $G'$ |
| M | $G0$ | $f_kG$ | $f_k'G'+G''$ |
| N | $G1$ | $f_kG+1$ | $f_k'G'+G$ |
| O | $G2$ | $f_kG+2$ | $f_k''G'$ |
| P | $GF$ | $f_kG+F$ | $f_kG+F+G'''+f_k$ |

# GFSOP Synthesis with Ternary Toffoli Gates

## General Pattern of a Cascade




$F_1 = 1 + A'''A'C^2 + B^2C^2 + A^{\#}B$ $\quad F_2 = 2 + B^2C^2 + B''' + 2C^2$

# GFSOP Synthesis with Ternary Toffoli Gates (continued)

**Theorem.** *Any ternary GFSOP function can be realized in a cascade of reversible ternary Toffoli, ternary Swap, and 5 ternary shift gates using at most* $2n+2+m$ *(optimistically* $2n+1+m$*) quantum wires, where **n** is the number of input variables and **m** is the number of outputs.*

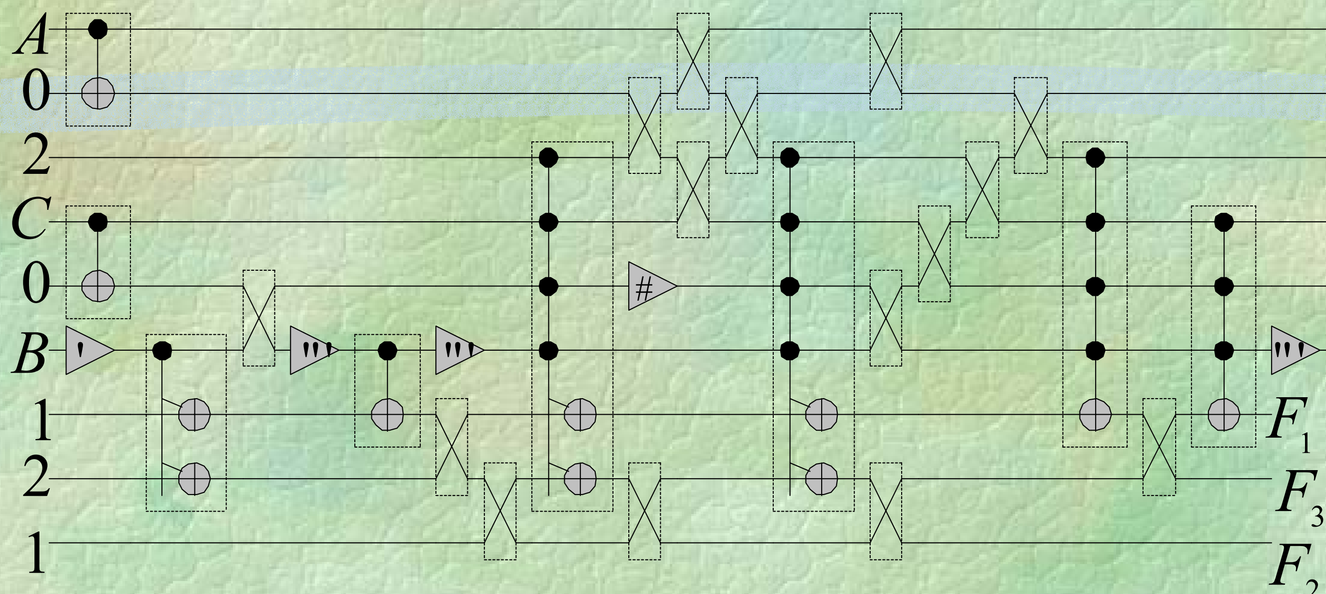
# GFSOP Synthesis with Ternary Toffoli Gates (continued)

## Realization Example

$$F_1 = 1 + 2B'C^2 + A^2B'''$$

$$F_2 = 1 + B' + A^2B'''C + C'''$$

$$F_3 = 2 + 2B'C^2 + 2A^2B''' + B' + A^2B'''C$$




Toffoli gates = 8, Swap gates = 15, Shift gates = 5

# GFSOP Synthesis with New Ternary Gates

Algorithm

*1.1 Factorize the given GFSOPs to satisfy the structure of operating mode P.*

*1.2 If not possible, factorize the given GFSOPs to satisfy the structure of any of the operating modes of J, K, L, M, N, and O.*

*1.3 If not possible, factorize the given GFSOPs to satisfy the structure of any of the operating modes of D, E, and F.*

*1.4 If not possible, factorize the given GFSOPs to satisfy the structure of any of the operating modes of A, B, C, G, H, and I.*

# GFSOP Synthesis with New Ternary Gates (continued)

Algorithm (continued)

*2. Create a node of the implementation graph for the selected mode of operation. Determine the input of that node.*

*3. Repeat steps 1 and 2 recursively for the inputs of the created node until all inputs become constant.*

*4. If any output of a node is garbage, use local mirror to convert it into constant. Convert output constants into other constants, if needed for one of the next gates, using shift gates.*

*From the implementation graph, realize the quantum cascade. Use variable and product ordering to reduce the number of swap gates.*

# GFSOP Synthesis with New Ternary Gates (continued)

## Algorithm (continued)

5. *From the implementation graph, realize the quantum cascade. Use variable and product ordering to reduce the number of swap gates.*

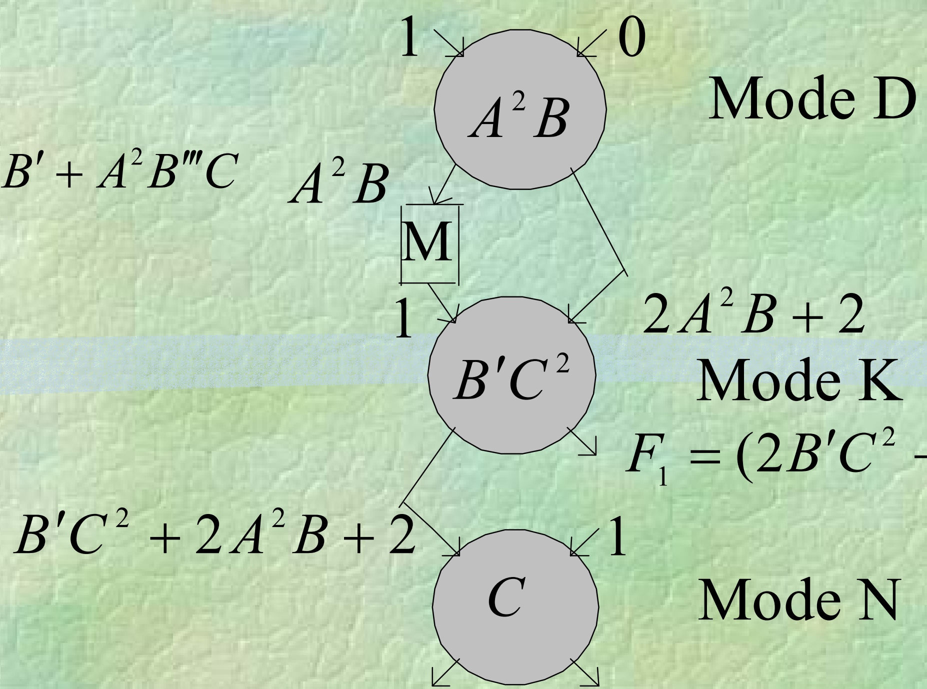
# GFSOP Synthesis with New Ternary Gates (continued)

## Realization Example

$$F_1 = 1 + 2B'C^2 + A^2B'''$$

$$F_2 = 1 + B' + A^2B'''C + C'''$$

$$F_3 = 2 + 2B'C^2 + 2A^2B''' + B' + A^2B'''C$$




$$F_1 = (2B'C^2 + 2) + (2A^2B + 2)$$

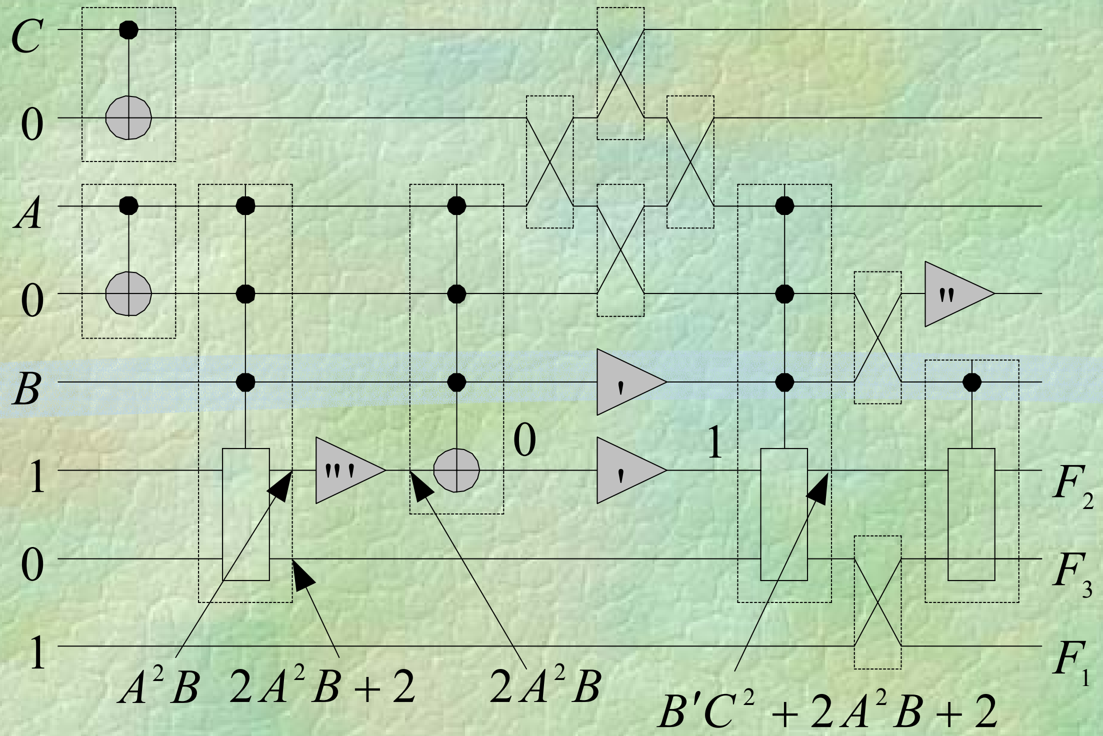
$$F_2 = C(B'C^2 + 2A^2B + 2) + 1$$

$$F_3 = (C+1)(B'C^2 + 2A^2B + 2 + 1) + (B'C^2 + 2A^2B + 2)$$

Implementation graph

# GFSOP Synthesis with New Ternary Gates (continued)

## Realization Example (continued)




New gates = 3, Toffoli gates = 3, Swap gates = 6,
Shift gates = 4

Quantum cascaded realization

# Experimental Results

- No known ternary GFSOP benchmark
- 7 small experimental functions

| Name | GFSOP Expression |
|---|---|
| kpk01 | $F_1 = A'B'C'' + B' + A'B$ , $F_2 = A'B'C'' + A'B + A'C''$ |
| kpk02 | $F_1 = BC'D'E + AB'D'E + D'E$ , $F_2 = BC'D'E + AB'D'E + D'E''' + B'''C' + A'''B' + 2$ |
| kpk03 | $F_1 = AB'$ , $F_2 = AB' + BC'$ , $F_3 = AB' + AC''$ , $F_4 = AB' + AC'' + AD'$ |
| kpk04 | $F = AC + AD'' + B'C + B'D'' + A'B'' + CD$ |
| kpk05 | $F_1 = 1 + A'BCD'$ , $F_2 = 1 + A'BCD' + A'C + B'''D'$ , $F_3 = B'''C + BD' + AC''$ , $F_4 = 1 + BD' + AC''$ |
| kpk06 | $F_1 = A^{\#}B'C^2 + A^2B^2$ , $F_2 = 2 + A''B'C^2 + A^2B^2$ |
| kpk07 | $F_1 = 1 + 2B'C^2 + A^2B'''$ , $F_2 = 1 + B' + A^2B'''C + C'''$ , $F_3 = 2 + 2B'C^2 + 2A^2B''' + B' + A^2B'''C$ |

# Experimental Results (continued)

| Func. Name | Cascade of Toffoli Gates | | | Cascade of New Gates | | | |
|---|---|---|---|---|---|---|---|
| | Toff. Gates | Swap Gates | Shift Gates | New Gates | Toff. Gates | Swap Gates | Shift Gates |
| kpk01 | 4 | 3 | 6 | 3 | 0 | 2 | 5 |
| kpk02 | 6 | 12 | 12 | 3 | 2 | 10 | 9 |
| kpk03 | 4 | 9 | 7 | 4 | 0 | 15 | 6 |
| kpk04 | 6 | 14 | 7 | 6 | 10 | 25 | 20 |
| kpk05 | 6 | 13 | 8 | 4 | 0 | 12 | 5 |
| kpk06 | 6 | 6 | 5 | 2 | 3 | 5 | 5 |
| kpk07 | 8 | 15 | 5 | 3 | 3 | 6 | 4 |

# Experimental Results (continued)

- For multi-output GFSOP the quantum cascades of new ternary gates are more efficient than the quantum cascades of ternary Toffoli gates

- For single-output GFSOP the quantum cascades of ternary Toffoli gates are more efficient than the quantum cascades of new ternary gates

- No comparable work exists to compare with

# Conclusion

## Our Achievement

- We used five (except buffer) reversible ternary unary operators (only three were previously used)

- We propose quantum realization of these ternary unary operators (shift gates)

# Conclusion (continued)

## Our Achievement (continued)

- We propose a new ternary generalization of Toffoli gate with discussion of its quantum realization

- We propose a new generalized reversible ternary gate with discussion of its quantum realization

- We propose quantum realization of a ternary swap gate for the first time.

# Conclusion (continued)

## Our Achievement (continued)

- We propose GFSOP-based reversible logic synthesis method using quantum cascade of ternary Toffoli gates
- We propose GFSOP-based reversible logic synthesis method using quantum cascade of new ternary gates
- The realization methods automatically accomplish the conversion of non-reversible ternary function to reversible ternary function

# Conclusion (continued)

## Our Achievement (continued)

- For synthesis with new gates, a graph-based data structure (called implementation graph) is introduced
- For synthesis with new gates, local mirror is used to convert garbage output into constants for reuse
- For both methods, variable ordering and product ordering are used to reduce the number of ternary swap gates

# Conclusion (continued)

## Our Achievement (continued)

- Quantum cascade of new gates yields better result for multi-output GFSOP
- Quantum cascade of Toffoli gates yields better result for single-output GFSOP
- Using smarter factorization techniques would improve the quality of quantum cascades of new gates

# Conclusion (continued)

## Our Achievement (continued)

- Proposed multi-output GFSOP synthesis methods
  - Applicable to all kinds of existing polynomial expansions
  - Applicable to all new expansions involving operations of powers, multiplications, sums and reversible one-argument functions
- The proposed methods allow to synthesize Galois-like Circuits for realistic-sized multi-output functions (similar to ESOP algorithms),
  - in contrast to the existing reversible logic synthesis methods that work only for few-variable single-output functions.

# Conclusion (continued)

## Future Research

- Investigating more efficient algorithm for reducing the number of swap gates in the cascades

- Developing smarter factorization technique for the cascade of new gates

# Conclusion (continued)

Future Research

- Developing method for multi-output GFSOP minimization

- Creating a good library of ternary GFSOP benchmark functions.

# Acknowledgements

Professor Soonchil Lee

Dr. Jae-Seung Lee

Professor Radomir Stankovic

Professor Tsutomu Sasao

Professor Bogdan Falkowski

Dr. Anas Al-Rabadi