



剰余系(孫子算経)を用いた 時間デジタル変換回路

群馬大学大学院 理工学府 電子情報部門
小林春夫

koba@gunma-u.ac.jp

<https://kobaweb.ei.st.gunma-u.ac.jp/>

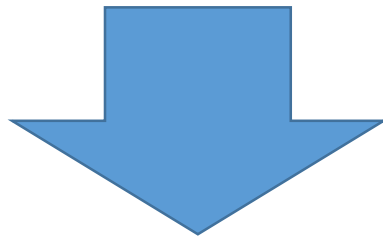
講義資料: <https://kobaweb.ei.st.gunma-u.ac.jp/lecture/lecture.html>

中国の剰余定理

- 中国の算術書『孫子算経』

「3で割ると2余り、5で割ると3余り、
7で割ると2余る数はいくつか」

一般化



中国の剰余定理

答え 23

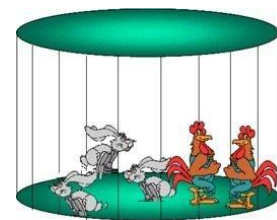


孫子算経

孫子算経

- 「3で割ると2余り、5で割ると3余り、
7で割ると2余る数は何か」 答え 23
➡ 一般化したのが「**中国人の剰余定理**」。

- **鶏兔同籠(けいとどうりゅう)**
「キジとウサギが同じ籠(かご)。頭が35個
足は94本。キジ、ウサギはそれぞれいくらか。」



➡ 日本に入ってきて「**鶴亀算**」となる

- が、孫子算経と孫子兵法とは
直接は関係ないようである。

二人の孫子

「孫武」

戦わずして勝つ



「孫臏 (そんびん)」

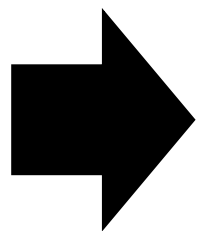
馬を三組ずつ出して勝負する競馬。

相手の上等の馬が出る競走に自分の下等の馬、
中等の馬が出る競走に上等の馬、
下等の馬が出る競走に中等の馬を出させる。



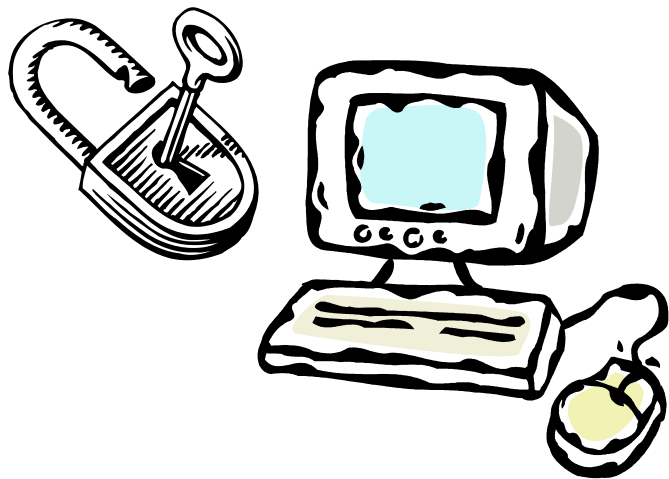
中国の剰余定理のアナログ回路への応用

- ✓ 江戸時代、「百五減算」として伝来
- ✓ 現在、情報セキュリティの暗号化に応用



古典数学によるイノベーション

集積回路に応用



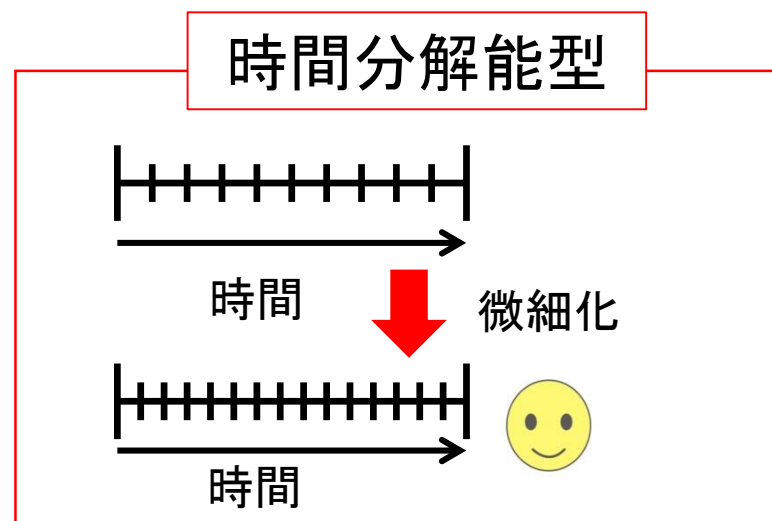
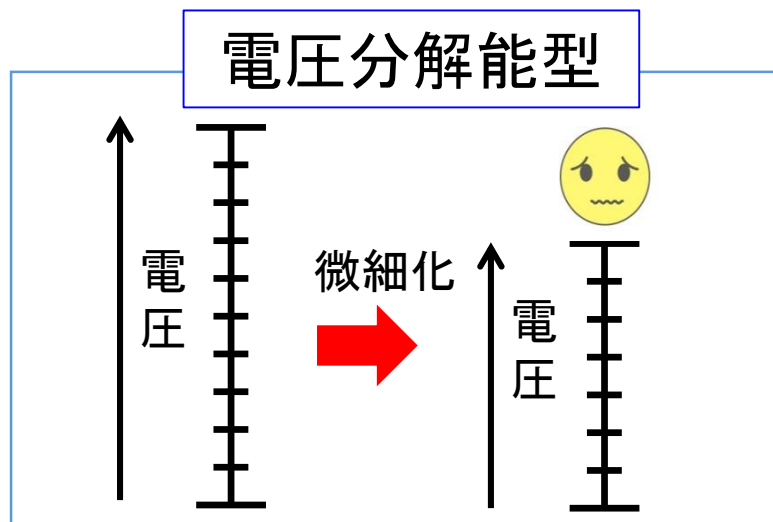
関孝和

研究背景

微細化CMOS LSI



電源電圧の低下
動作スイッチングスピードの向上



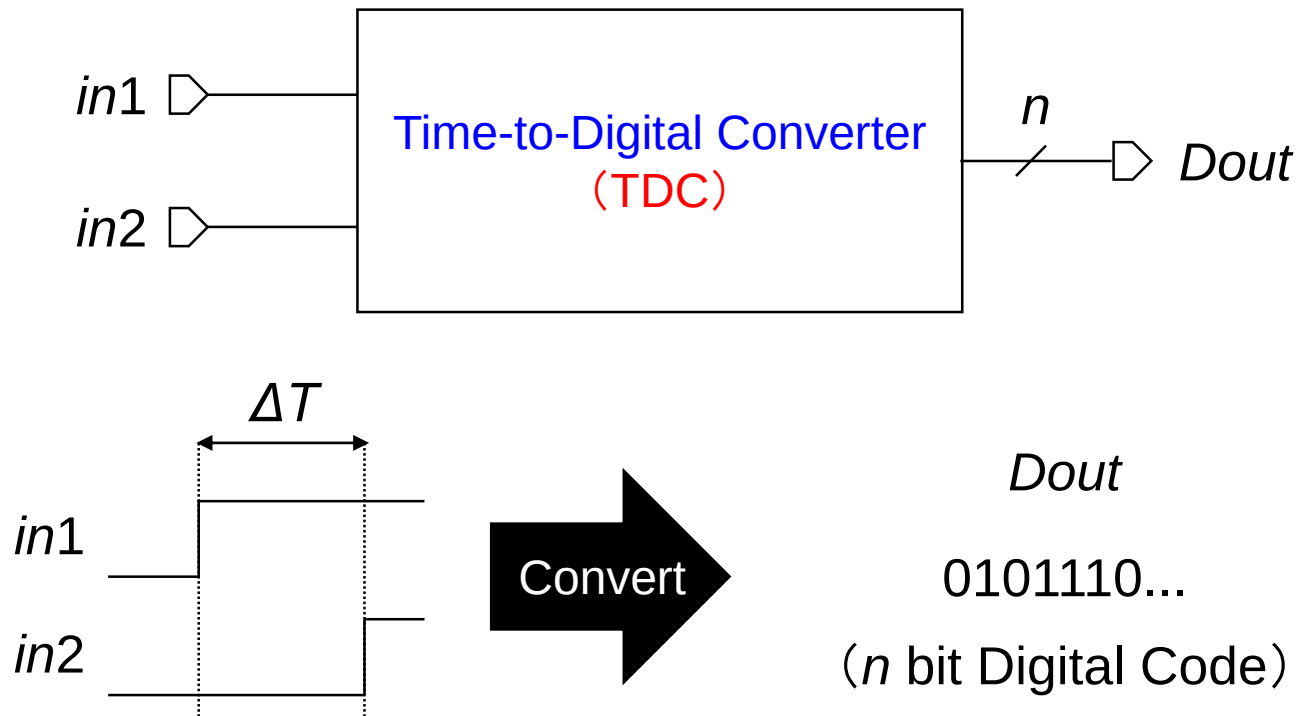
TDC (Time-to-Digital Converter) は2つのデジタル信号の時間差をデジタル値に変換



微細化CMOS LSIにおいて、TDCは時間領域アナログ回路のカギとなる
(センサ回路, All-Digital PLL, ADC, 変調回路等)

タイムデジタイザ回路

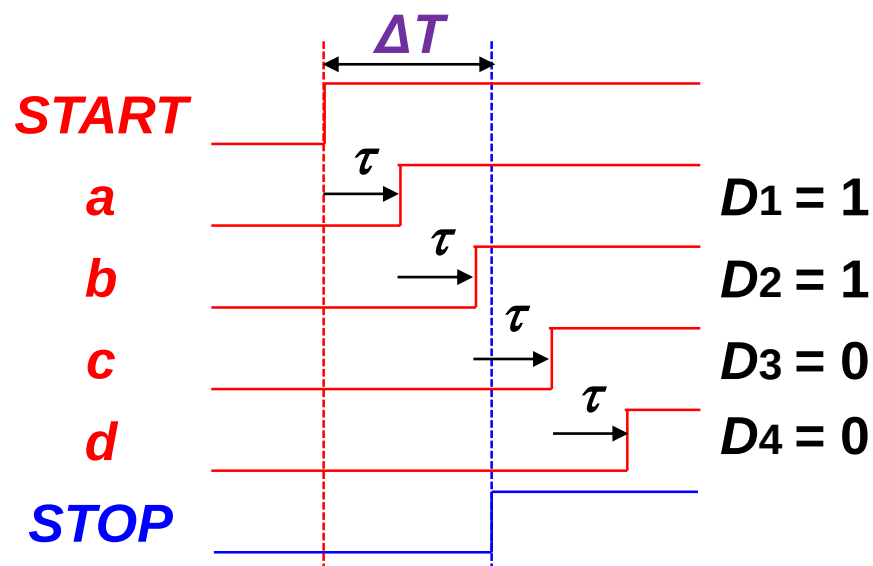
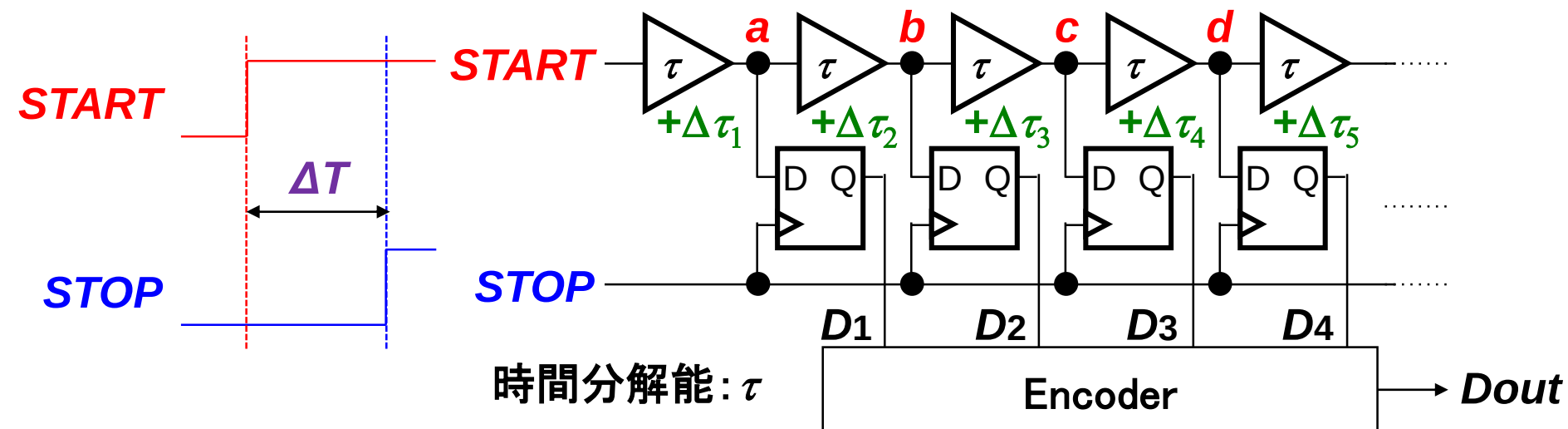
7



2つのデジタル信号間の時間差 ΔT をデジタル値に変換

出力のデジタル値より ΔT を測定可能

フラッシュ型 TDCの構成と動作



● ΔT の大きさに比例したデジタル値 Dout を出力

● 時間分解能 τ

高エネルギー加速器研究機構
素粒子原子核研究所
新井康夫氏による発明

フラッシュ型TDCの回路規模の問題

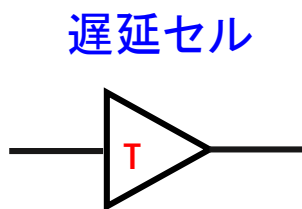
START とSTOP の立ち上がりエッジ間の時間差

測定範囲 $0 < \Delta T < N T$ ΔT

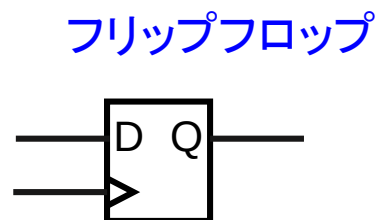
時間分解能 T

$N = 1001$ (千一) のとき

フラッシュ型TDC では大きな回路規模、大きな消費電力



1001個



1001 個

提案する剰余系TDC $1001 = 7 \times 11 \times 13$
 同じ測定範囲、時間分解能で $7 + 11 + 13 = 31$ 個の
 遅延セル、フリップフロップで実現できる

千一個から三十一個へ !!

研究の目的

時間測定回路TDC

- LSIテストシステムのキーコンポーネント
- 時間信号であることを利用



“剰余”が容易に得られる

- 剰余系を利用

フラッシュ型TDCに比べ、
同等性能、小回路規模・低消費電力TDCが
実現できる可能性あり



剰余系TDC回路を検討

剰余系の例

基数 2, 3, 5 互いに素

$$N=2 \times 3 \times 5 = 30$$

0から $N-1(=29)$ までの整数の一つを k

a: k を2で割った余り $a = \text{mod}2(k)$

b: k を3で割った余り $b = \text{mod}3(k)$

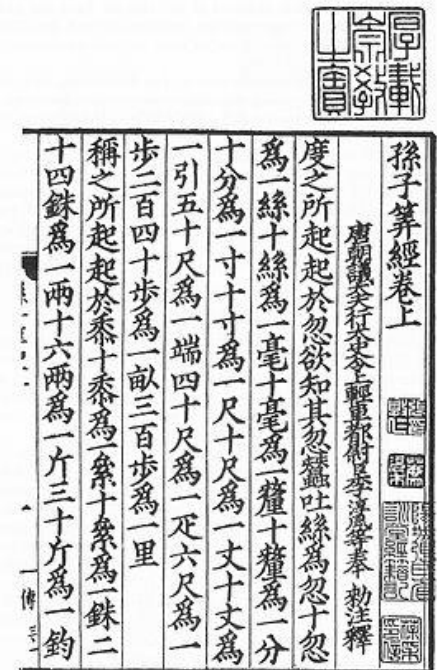
c: k を5で割った余り $c = \text{mod}5(k)$

k と (a, b, c) の組は1対1に対応する。

k を (a, b, c) で表現 ➡ 剰余表現

中国人の剰余定理 (Chinese Remainder Theorem)

(a, b, c) から k を求めるアルゴリズム



剰余定理の例

基数 2, 3, 5 互いに素

$$N=2 \times 3 \times 5 = 30$$

0から $N-1(=29)$ までの整数の一つを k

a : k を 2 で割った余り $a = \text{mod}2(k)$

b : k を 3 で割った余り $b = \text{mod}3(k)$

c : k を 5 で割った余り $c = \text{mod}5(k)$

k と (a, b, c) の組は1対1に対応する。

k を (a, b, c) で表現  剰余表現

剰余定理 (Chinese Remainder Theorem)
(a, b, c) から k を求めるアルゴリズム

自然数 k と剰余表現 (m_1, m_2, m_3) は 1 対 1 対応

m_1	m_2	m_3	k
0	0	0	0
1	1	1	1
0	2	2	2
1	0	3	3
0	1	4	4
1	2	0	5
0	0	1	6
1	1	2	7
0	2	3	8
1	0	4	9
0	1	0	10
1	2	1	11
0	0	2	12
1	1	3	13
0	2	4	14

m_1	m_2	m_3	k
1	0	0	15
0	1	1	16
1	2	2	17
0	0	3	18
1	1	4	19
0	2	0	20
1	0	1	21
0	1	2	22
1	2	3	23
0	0	4	24
1	1	0	25
0	2	1	26
1	0	2	27
0	1	3	28
1	2	4	29

剰余定理は、

この問題を他の整数についても適用できるように一般化したもの。

剰余DCの原理

TDC 回路は信号が時間であることを利用すると“剰余”が容易に得られる。

三つのリング発振回路(遅延 m_1T , m_2T , m_3T)を利用し、発振状態から経過時間 T の測定を行うことが可能で。剰余定理に基づいて、(a, b, c)から k を求め、経過時間 $T = k \times T$ を得る。

例えば、三つのリング発振回路(遅延 $2T$, $3T$, $5T$)を利用し、発振している状態から経過時間 T の測定を行う。

T を $2T$ で割った余りは a

T を $3T$ で割った余りは b

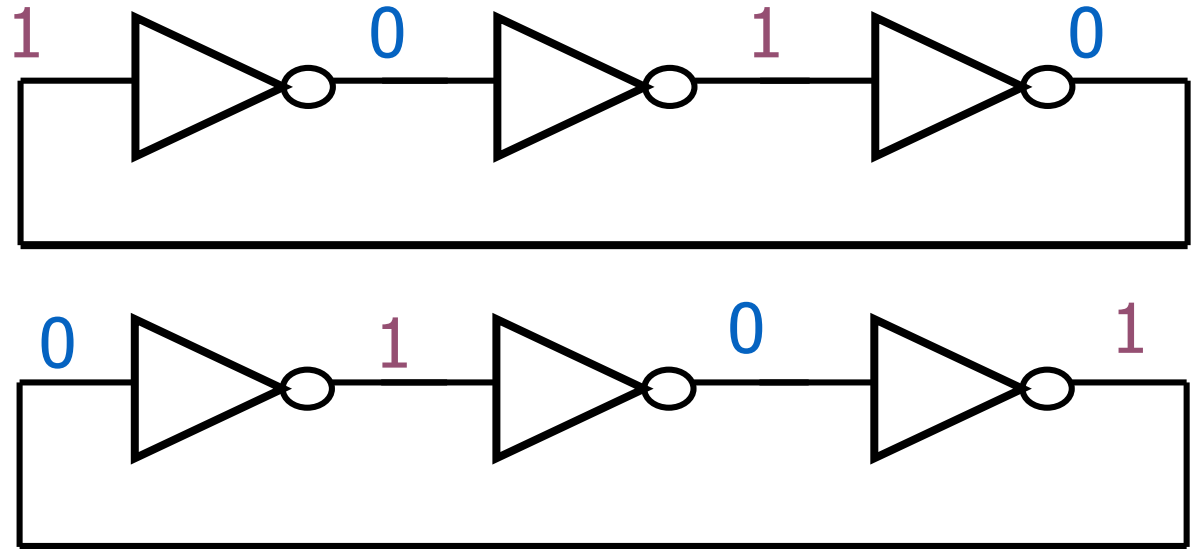
T を $5T$ で割った余りは c

⇒剰余定理で $T = k^*T$

リング発振器 (Ring Oscillator)

奇数個インバータのリング接続

安定状態
なし



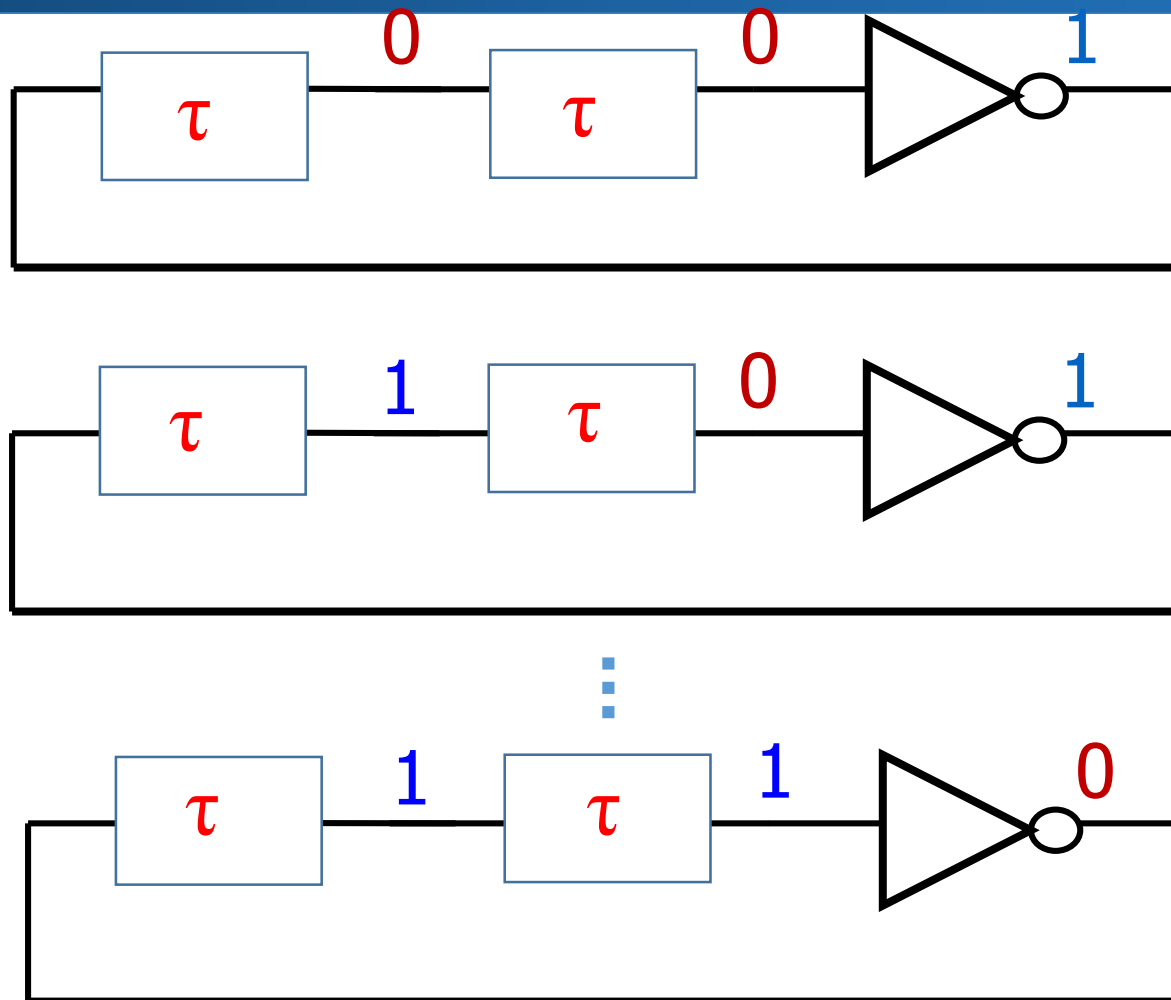
T: インバータ遅延、 $2N+1$ 個のインバータリング接続

周波数 $f = \frac{1}{2(2N+1)T}$ で発振。



メビウスの帯

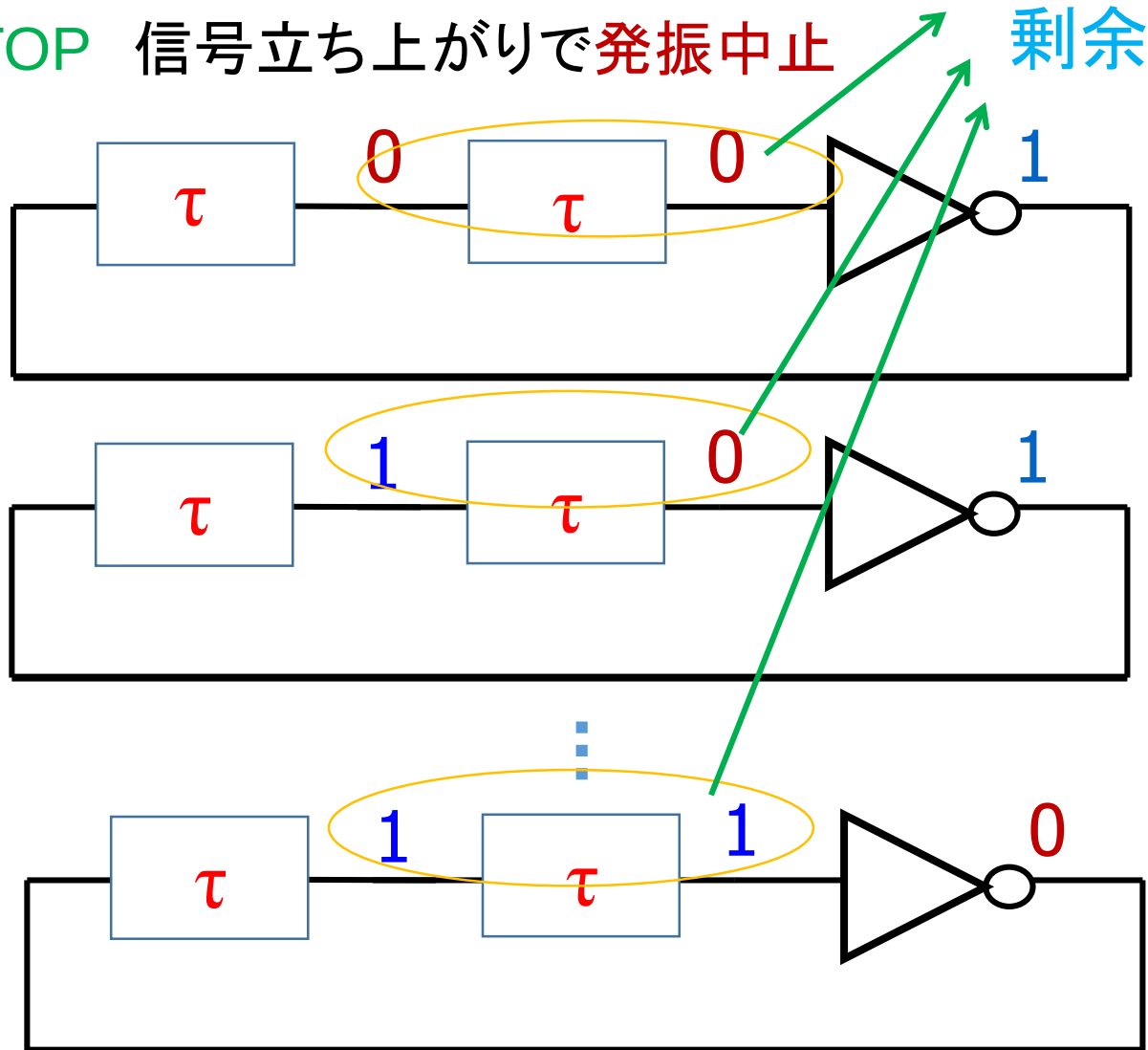
リング発振回路で剰余が容易に得られる



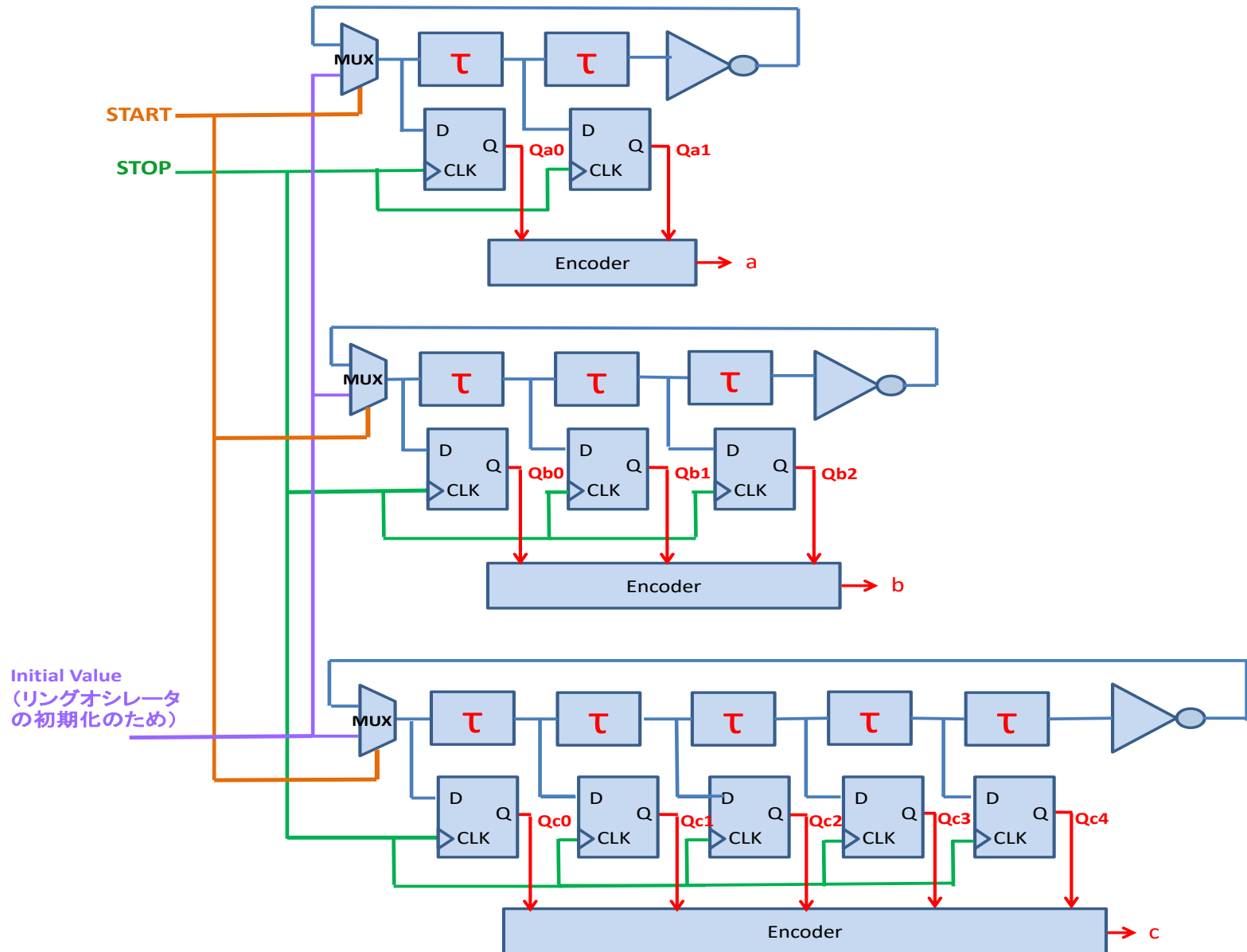
考察 TDCでは取り扱う入力信号が時間信号なので
リング発振回路構成により剰余が容易に得られる。
電圧信号を入力とするADCでは剰余を得るのは簡単ではない。

リング発振回路で剰余を得る

- **START** 信号立ち上がりで発振開始
- **STOP** 信号立ち上がりで発振中止



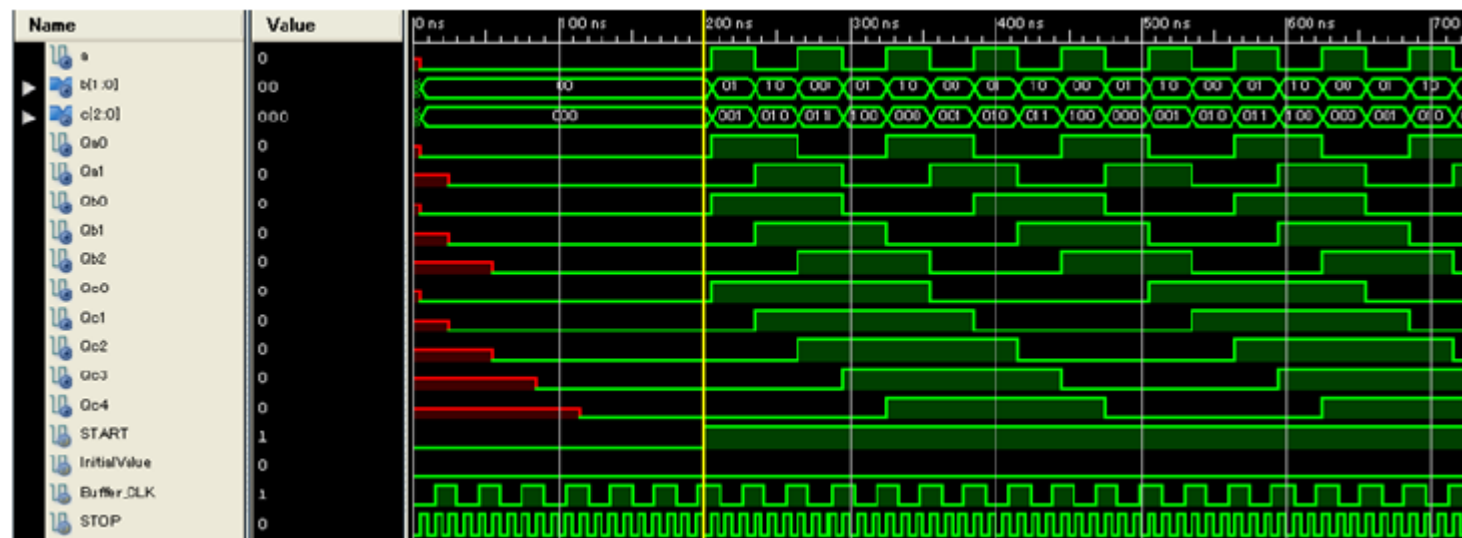
提案する剰余系TDCの回路図



RTL(Register Transfer Level) 検証

回路機能をHDL (Hardware Description Language)で記述し、ISim を使用し、下記条件でシミュレーションを行った:

- ・STOP クロック周波数=100MHz
- ・バッファ遅延 $\tau=30.30\text{ns}$
- ・START 信号がL からH に変化=200ns



タイミングチャート

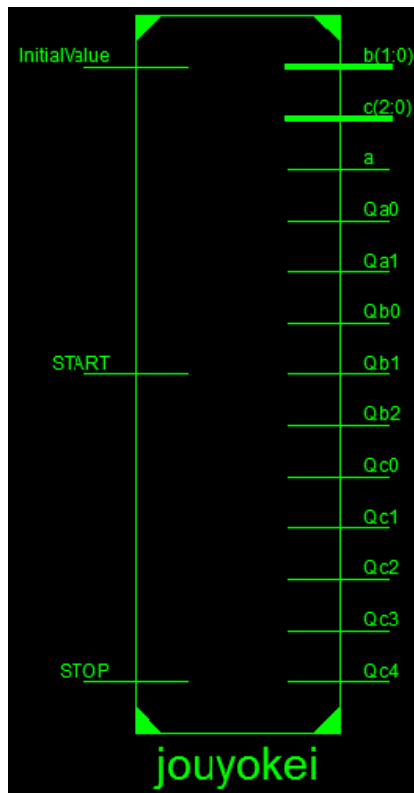
FPGA実装

STOPポートの入力: 100MHz FPGA クロック

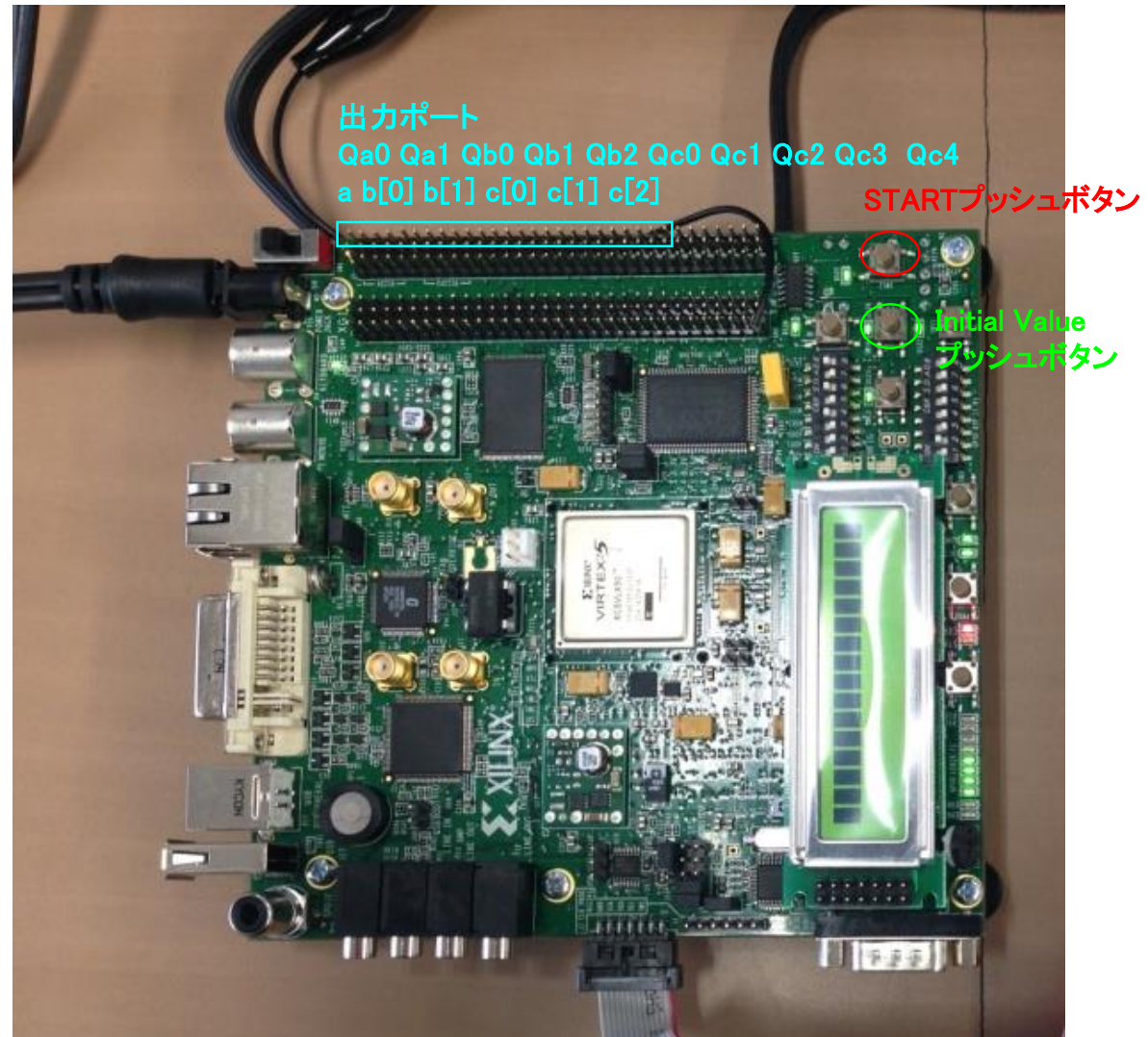
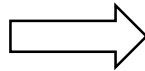
Buffer_CLKポートの入力: 33MHz FPGA クロック(バッファの遅延 $\tau = 30.30\text{ns}$)

入力ポート

出力ポート



ピン配置制約



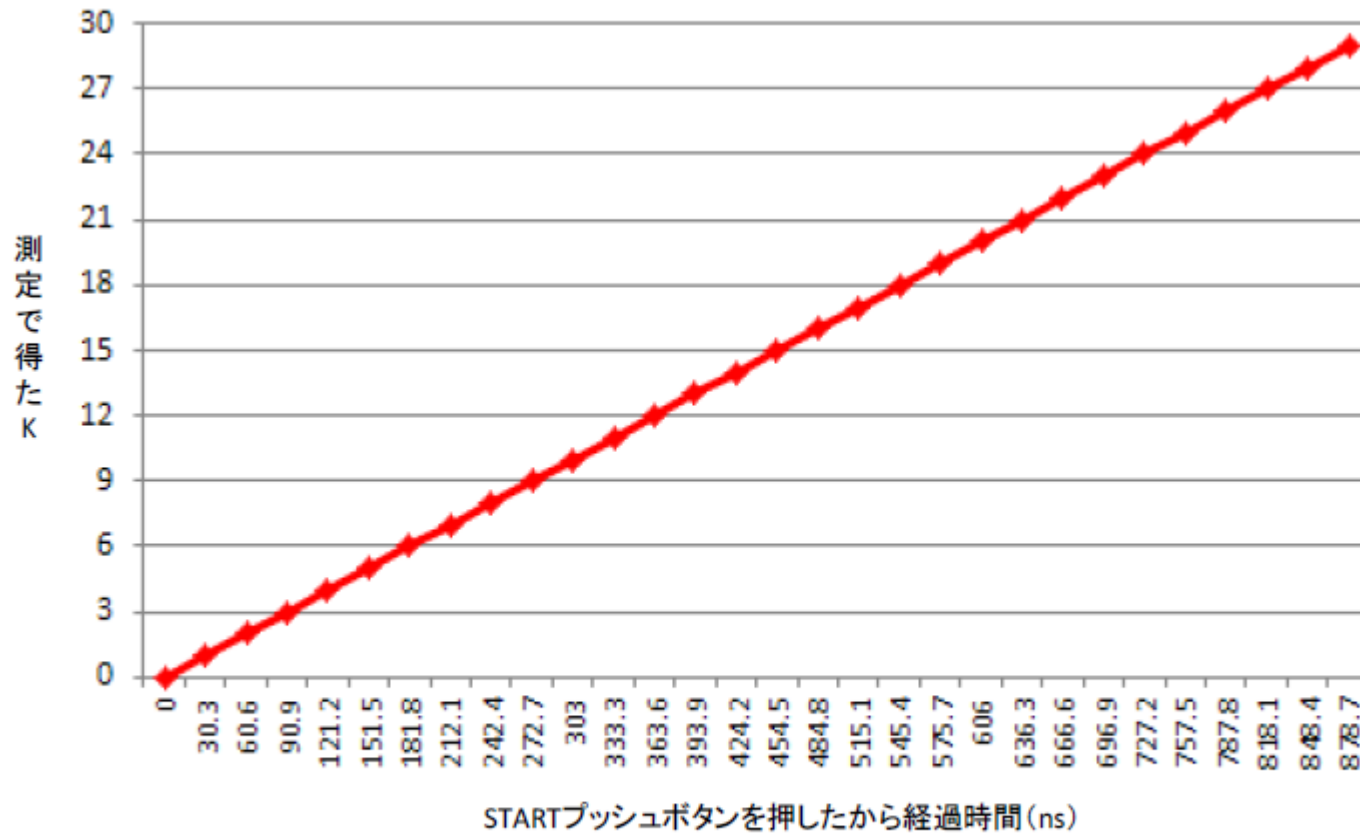
FPGA(Field Programmable Array) 実装

20



FPGA実装 剰余系TDCの評価

剰余系TDC回路はFPGAで実現できることが示された。



経過時間 VS. 測定で得た k

中国人の剰余定理(剰余系)

兵士数を数えるのに使用

群馬大学 阿部優大、小林春夫

Chinese Remainder Theorem



Sun Tzu

Chinese arithmetic book 'Sun Tzu calculation'

孫子算經

"When dividing by 3, its residue is 2,
dividing by 5, its residue is 3,
dividing by 7, its residue is 2.
What is the original number?"

Answer 23

Generalization



Chinese Remainder Theorem



Sun Tzu calculation

How to use Chinese remainder theorem

He used to quickly find out how many soldiers there are.



Sun Tzu

“Divide into 3.”



...



Remainder : 2



How to use Chinese remainder theorem

He used to quickly find out how many soldiers there are.



Sun Tzu

“Divide into 5.”

Remainder : 3



■ ■ ■



How to use Chinese remainder theorem

He used to quickly find out how many soldiers there are.



“Divide into 7.”

Sun Tzu



How to use Chinese remainder theorem

He used to quickly find out how many soldiers there are.



Sun Tzu

“There are 23 people in all
according to
Chinese remainder theorem”



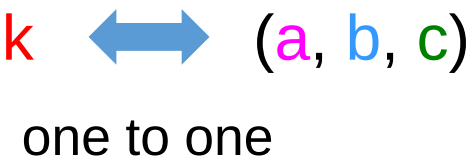
Example of Residue Number System

$23 \% 3 = 2, \quad 23 \% 5 = 3, \quad 23 \% 7 = 2$

- Natural numbers
3, 5, 7 (relatively prime)
 $N=3 \times 5 \times 7=105$
- $k \ (0 \leq k \leq N-1 (=104))$

a : Remainder of k dividing by 3
 b : Remainder of k dividing by 5
 c : Remainder of k dividing by 7

$a=\text{mod}3(k)$
 $b=\text{mod}5(k)$
 $c=\text{mod}7(k)$



Chinese remainder theorem

a	b	c	k
0	0	1	15
1	1	2	16
2	2	3	17
0	3	4	18
1	4	5	19
2	0	6	20
0	1	0	21
1	2	1	22
2	3	2	23
0	4	3	24
1	0	4	25
2	1	5	26
0	2	6	27
1	3	0	28
2	4	1	29

Residue number system

解 説

孫子算経は兵法家の孫子(孫武)より
ずいぶん前の書で、直接は関係ないようである。

<https://kobaweb.ei.st.gunma-u.ac.jp/news/pdf/2014/2014-07-30joyo.pdf>

が、ここでは孫子が兵士の数を素早く数える
という話にした。



グレイコードを用いた 時間デジタル変換回路

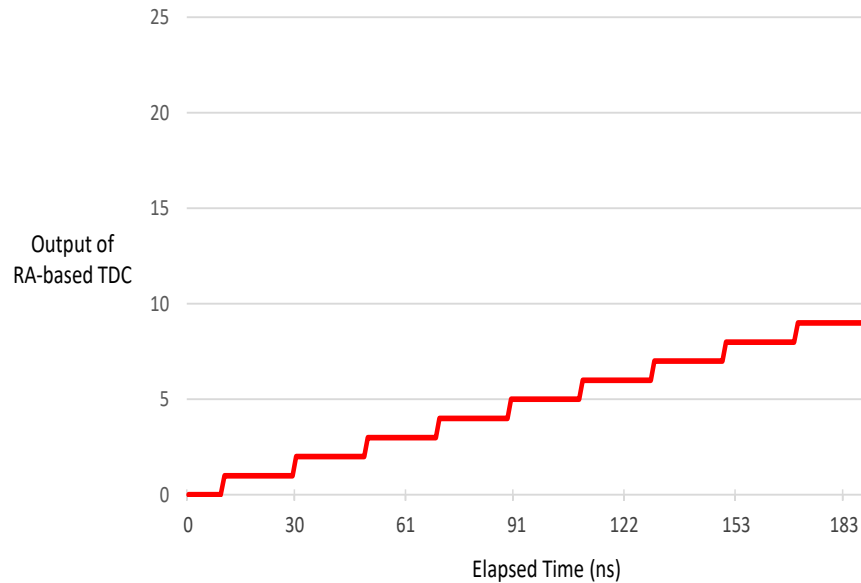
群馬大学大学院 理工学府 電子情報部門

小林春夫

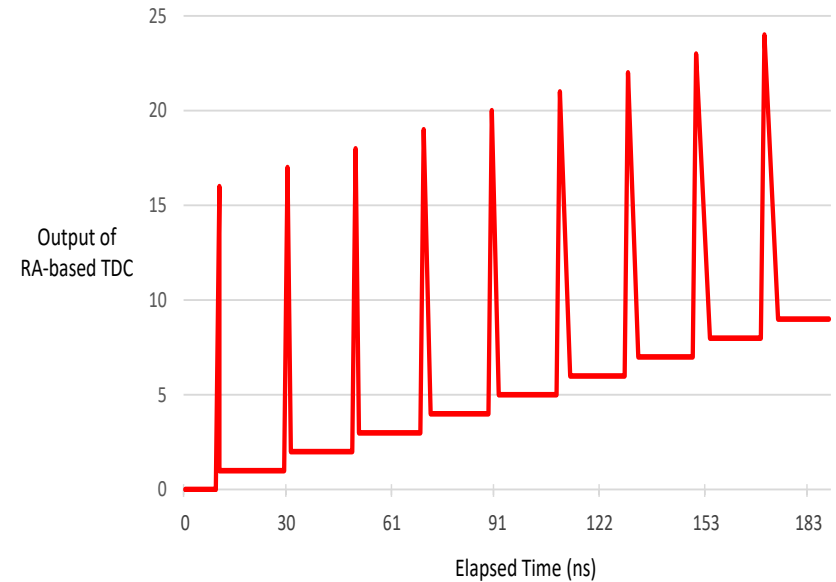
koba@gunma-u.ac.jp

<http://www.el.gunma-u.ac.jp/~kobaweb/>





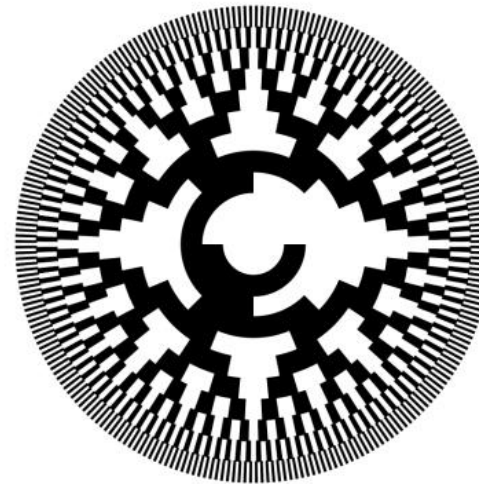
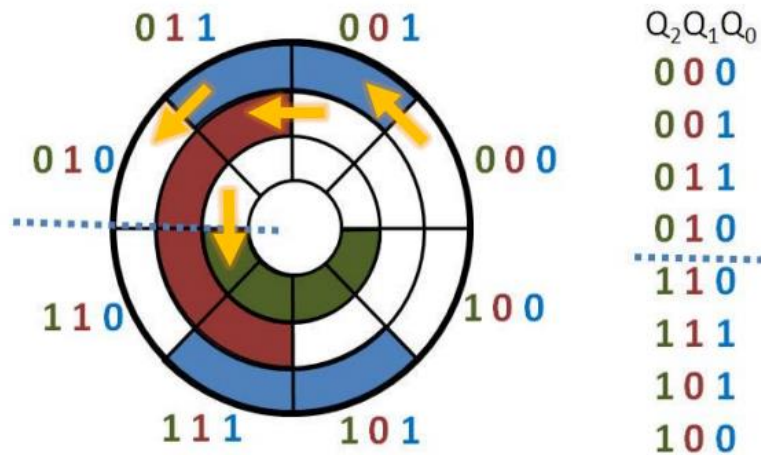
No mismatches among the delay stages



Mismatches exist among the delay stages
(large glitches are observed)

Simulation results with Residue Arithmetic-based TDC
without and with mismatches among delay cells in ring
oscillators.

グレイコード (Gray code)



FRANK GRAY and A. L. Johnson in television booth. Behind the glass panels at sides and top are the photo-electric cells.

グレイコード: 前後に隣接する符号間のハミング距離が必ず1

ベル研究所のフランク・グレイが1947年の特許出願書で最初に使用した。

● Gray code の応用

従来例:

AD変換器、ロータリーエンコーダー

群馬大 小林研究室からの提案 (グリッチ低減のため):

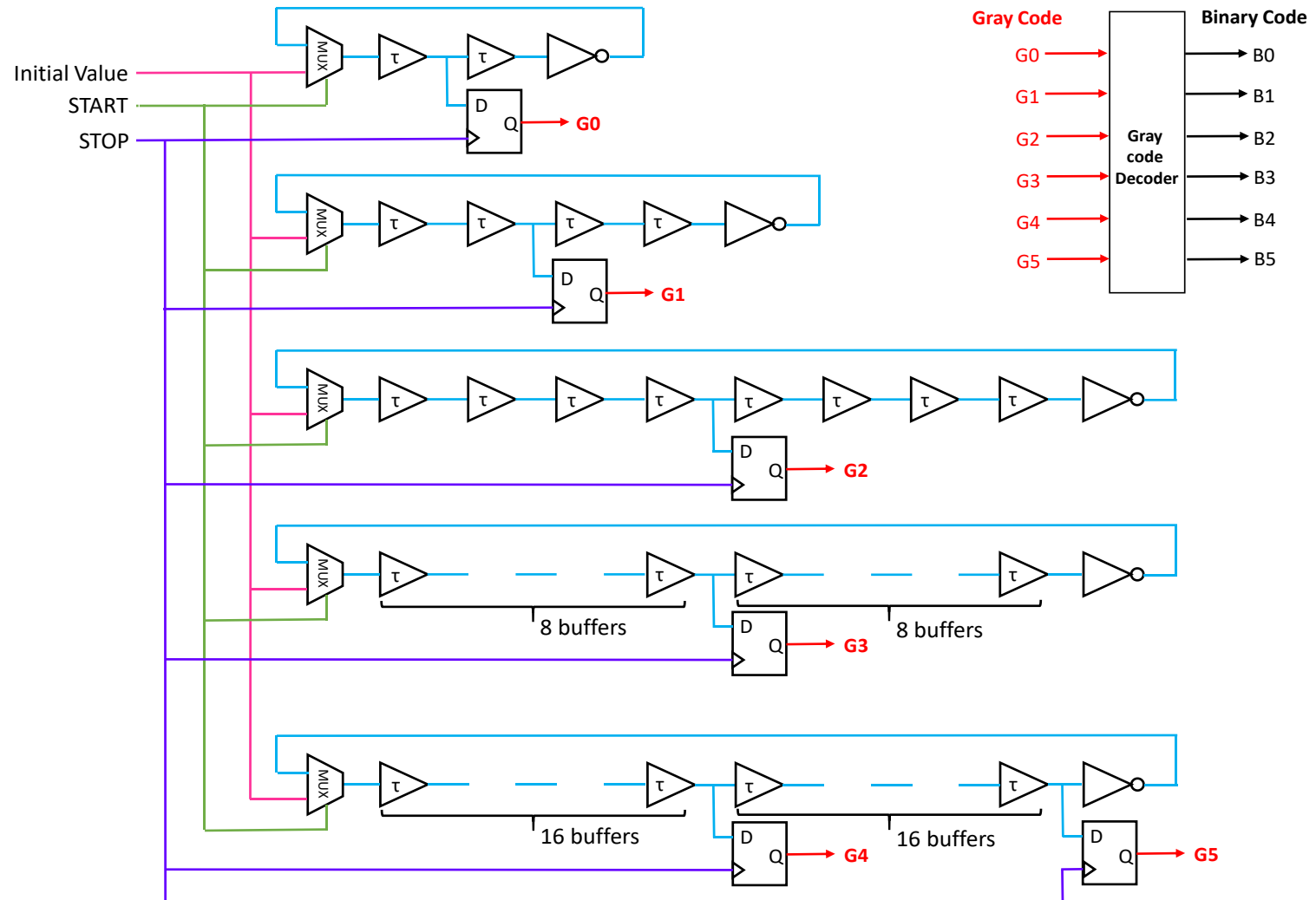
時間デジタイザ回路(TDC)

DA変換器

Binary Code と Gray Code

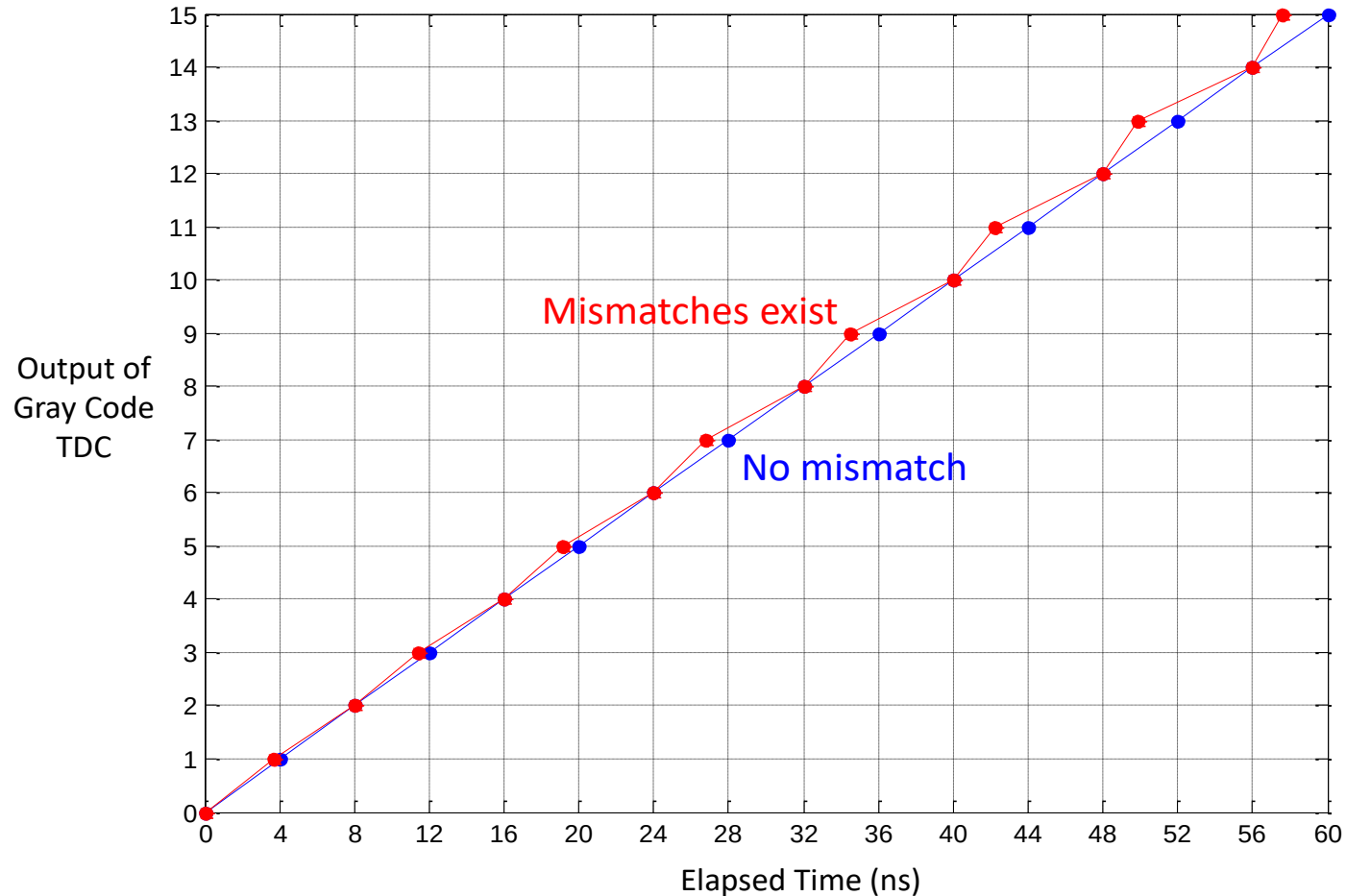
Decimal numbers	Binary Code	Gray Code
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

Gray code TDC



Gray code TDC と回路非理想特性の影響

35



RTL simulation results for 4-bit Gray code based TDC
without and with one delay mismatch.

ハノイの塔とGray code

Binary Code と Gray Code

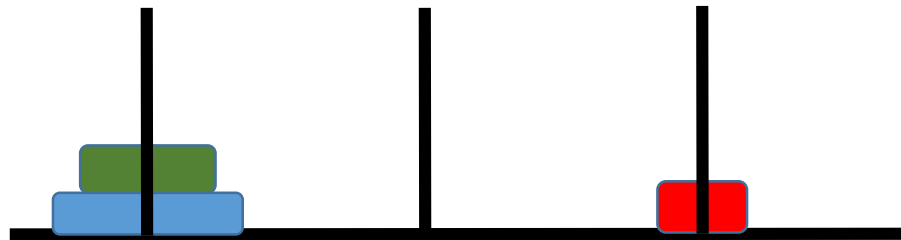
Decimal numbers	Binary Code	Gray Code
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

0: 0 0 0

$$\underline{Q_2 Q_1 Q_0}$$

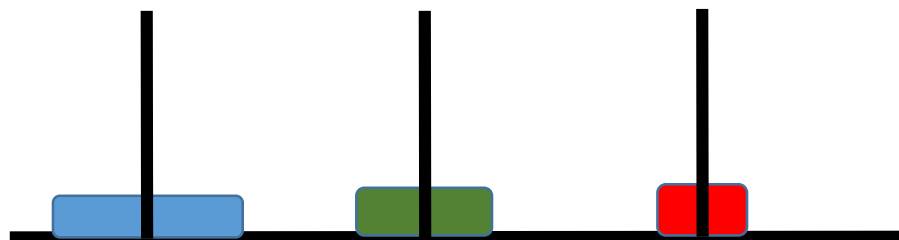
1: 0 0 1

Q_2	Q_1	Q_0
0	0	0
0	0	1
0	1	1
0	1	0
.....		
1	1	0
1	1	1
1	0	1
1	0	0



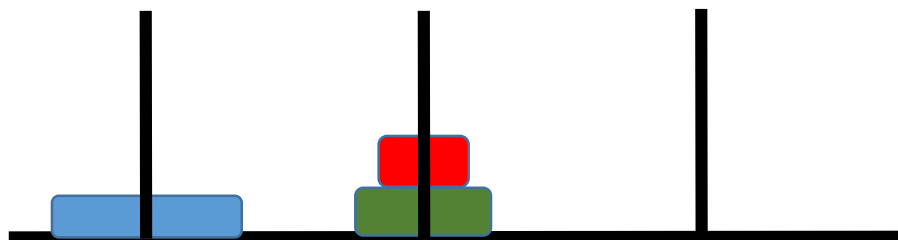
2: 0 1 1

Q_2	Q_1	Q_0
0	0	0
0	0	1
0	1	1
0	1	0
.....		
1	1	0
1	1	1
1	0	1
1	0	0



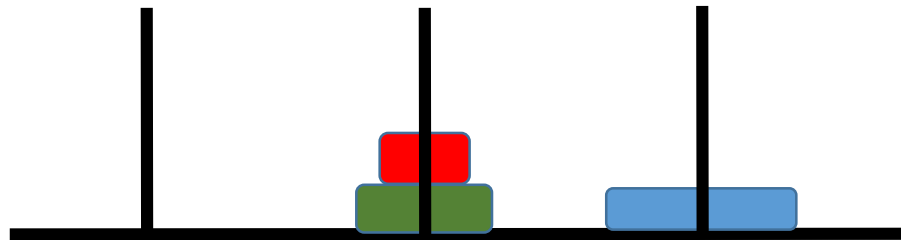
3: 0 1 0

Q_2	Q_1	Q_0
0	0	0
0	0	1
0	1	1
0	1	0
1	1	0
1	1	1
1	0	1
1	0	0



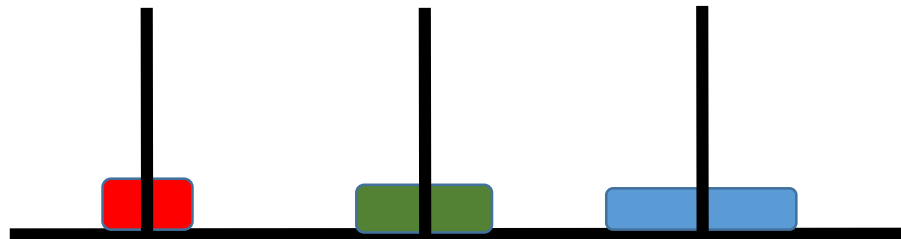
4: 1 1 0

Q_2	Q_1	Q_0
0	0	0
0	0	1
0	1	1
0	1	0
1	1	0
1	1	1
1	0	1
1	0	0



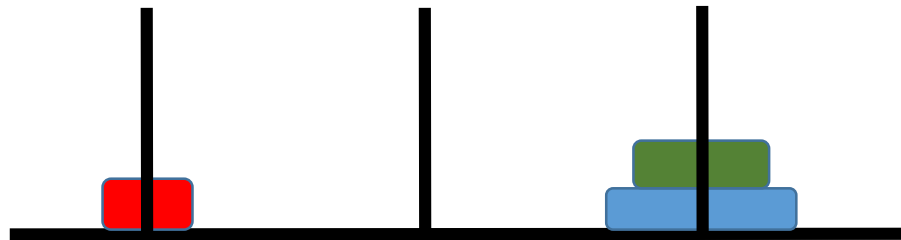
5: 1 1 1

Q_2	Q_1	Q_0
0	0	0
0	0	1
0	1	1
0	1	0
.....		
1	1	0
1	1	1
1	0	1
1	0	0



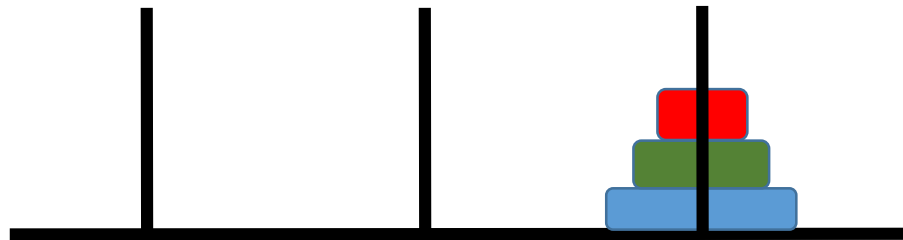
6: 1 0 1

Q_2	Q_1	Q_0
0	0	0
0	0	1
0	1	1
0	1	0
.....		
1	1	0
1	1	1
1	0	1
1	0	0



7: 1 0 0

Q_2	Q_1	Q_0
0	0	0
0	0	1
0	1	1
0	1	0
1	1	0
1	1	1
1	0	1
1	0	0



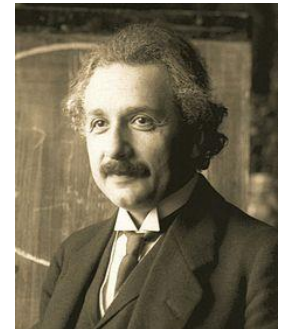
「時間」はミステリアス

往古来今、之を**宙**と謂い
四方上下、之を**宇**と謂う。
淮南子

時間
空間



時空は一体
時間は相対的である。
アインシュタイン



虚数時間
ホーキング博士

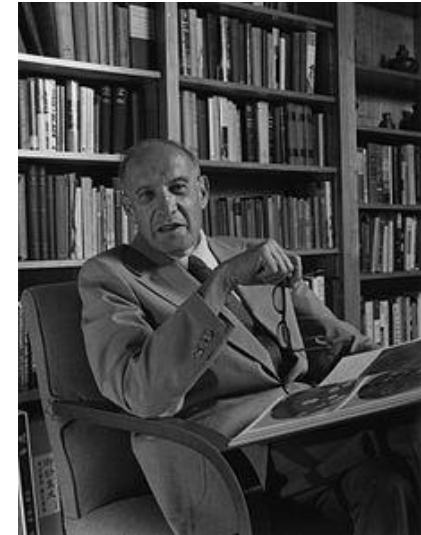


時間は最も貴重な資源

「成果を上げる者は、
仕事からスタートしない。
時間からスタートする。

計画からもスタートしない。
まず、何に時間がとられているかを
知ることからスタートする。

次に、時間を奪おうとする非生産的な要求を退ける。
そして、得られた自由な時間を大きくまとめる」



レポート課題

この講義の内容に関係したことを調べ
その内容について A4レポート用紙2枚程度に
まとめよ。

できるだけ手書きでなくコンピュータを用いよ。

基礎電子情報理工学Ⅰ(小林春夫担当分)

3回目レポート

提出： 2019年12月20日(金)17時まで

GA棟 教養教育① 窓口にレポート提出