配布先 : (ﾀﾆ)開3 (小国) (小林)iT

正方乗算器型(256×256)の提案

1. 目的

正方乗算器型(256×256bit)の方式の提案

2. 性能

2-1. 前提

(1) 本メモ添付のﾌﾞﾛｯｸ図
(2) 乗算器 1cyc = 7.5ns 四則演算器 1cyc = 15ns
(3) 余算は、μｺｰﾄﾞにより演算(性能はﾋﾞｯﾄ長 + 8cyc と仮定)
(4) 逆数は、μｺｰﾄﾞにより演算(性能はﾋﾞｯﾄ長 + 8cyc と仮定)

ﾋﾞｯﾄ長	余算	逆数	合計(cyc数)
512bit	520	520	1040
768bit	776	776	1552
1024bit	1032	1032	2064
1280bit	1288	1288	2576
2048bit	2056	2056	4112

2-2. 結果

1024bit /w CRT性能(剰余演算部のみの性能)

pの1ﾓﾝｺﾞﾒﾘ乗算 (X^2 X･Y) '0'ｹｰｽで32cyc '1'ｹｰｽで46cyc
((32+46)×513×0.5)×7.5 + 1552×15 = 0.1733325ms
qの1ﾓﾝｺﾞﾒﾘ乗算(X^2 X･Y) '0'ｹｰｽで20cyc '1'ｹｰｽで24cyc
((20+24)×512×0.5)×7.5 + 1040×15 = 0.10008 ms
0.1733325 + 0.10008 = 0.2734125 ms → 3657件/sec

1024bit 性能

1ﾓﾝｺﾞﾒﾘ乗算 (X^2 X･Y) '0'ｹｰｽで46cyc '1'ｹｰｽで78cyc
平均 ((46+78)×1024×0.5)×7.5 + 2064×15 = 0.50712 ms → 1971件/sec
ﾜｰｽﾄ 78×1024×7.5 + 2064×15 = 0.63000 ms → 1587件/sec

2048bit /w CRT性能(剰余演算部のみの性能)

pの1ﾓﾝｺﾞﾒﾘ乗算 (X^2 X･Y) '0'ｹｰｽで66cyc '1'ｹｰｽで122cyc
((66+122)×1025×0.5)×7.5 + 2576×15 = 0.761265ms
qの1ﾓﾝｺﾞﾒﾘ乗算(X^2 X･Y) '0'ｹｰｽで46cyc '1'ｹｰｽで78cyc
平均 ((46+78)×1024×0.5)×7.5 + 2064×15 = 0.50712 ms
0.761265 + 0.50712 = 1.268385 ms → 788 件/sec

2048bit 性能

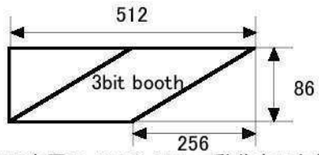
1ﾓﾝｺﾞﾒﾘ乗算 (X^2 X･Y) '0'ｹｰｽで146cyc '1'ｹｰｽで300cyc
平均 ((146+300)×2048×0.5)×7.5 + 4112×15 = 3.48696 ms → 286件/sec
ﾜｰｽﾄ 300 × 2048×7.5 + 4112×15 = 4.66968 ms → 214件/sec

	要求性能 (件/sec)	提案方式 (件/sec)	達成率 (%)
1024bit /w CRT	3600	3657	101.5
1024bit	900	1972	219.1
2048bit /w CRT	900	778	86.4
2048bit	225	286	127.1

3. 消費電力

(1) CSA

CSA概数

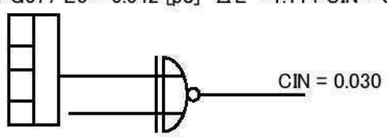


512×86 − 256×86÷2 = 33024

CSAにG358を用い 133.3 MHzで動作させた場合の消費電力を見積もる。
G358 E0 = 0.118 [pJ] ΔEU = 1.121 ΔEC = 1.127
CIN = 0.030
1CSAの消費電力 = (0.118 + 1.121×0.030+1.127×0.030)×133.3×10^6×0.5 = 12359576 [pW]
全CSA = 12359576 × 33024 = 0.409 [W]

(2) booth

FPG180 E0 = 0.065 [pJ] ΔE = 1.122
FPG077 E0 = 0.042 [pJ] ΔE = 1.114 CIN = 0.021



1組の消費電力 = (0.065+1.122×0.021 + 0.042 +1.114×0.030)×133.3×10^6×0.5 = 10929400.3 [pW]
全booth = 10929400.3 × 33024 = 0.361 [W]

(3) ﾗｯﾁ

4012個と仮定
G9F2 E0 = 0.078[pJ] ΔE = 1.140
平均CIN = 0.030
消費電力 = (0.078 + 1.140×0.030)×133.3×10^6×0.5×4012 = 0.030[W]

(1) + (2) + (3) = 0.409 + 0.361 + 0.030 = 0.800 [W]
RSDﾁｪｯｸ 0.800 + 0.018 = 0.818 [W] (詳細は NH-PCIXCC-030 参照)

4. 見積もり

4-1. 乗算器

(1) CSA
11(G358) × 33024 × 1.5 = 545 k ｹﾞｰﾄ
(2) booth
7(C0180 + C077) × 33024 × 1.5 = 347 k ｹﾞｰﾄ
(3) ﾗｯﾁ 5000個 (仮定)
5000 × 7 = 35 k

(1) + (2) + (3) = 927 k ｹﾞｰﾄ

4-2. 四則演算器

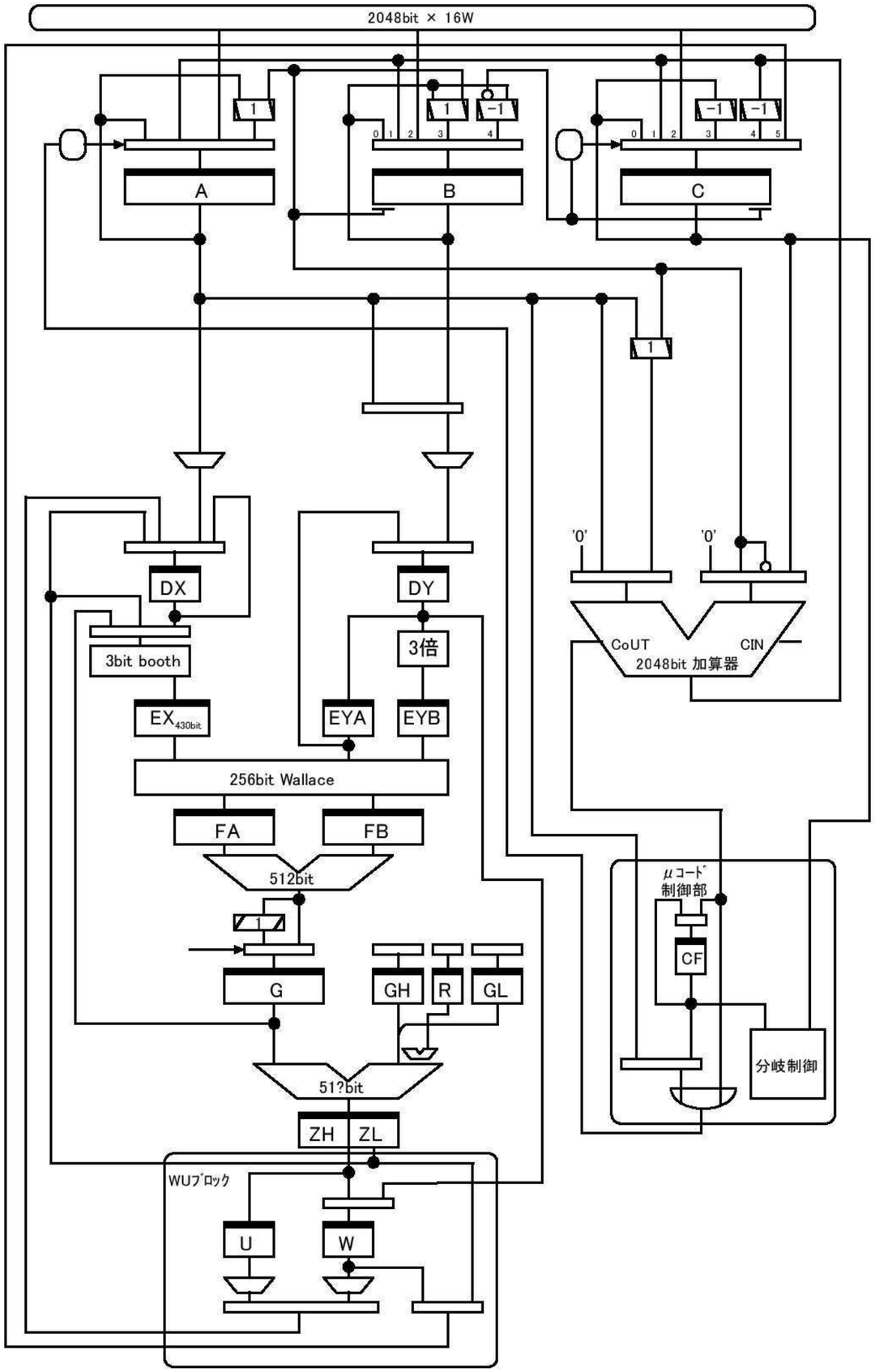
	ICF3				四則演算器			
論理名	ｹﾞｰﾄ数	ﾘﾋﾟｰﾄ数	ﾘﾋﾟｰﾄ数 (2重化)	ｹﾞｰﾄ数	ｹﾞｰﾄ数 ×1.3	ﾘﾋﾟｰﾄ数	ﾘﾋﾟｰﾄ数 (2重化)	ｹﾞｰﾄ数
PCTL	6088	1	2	12176	7914	1	2	15829
PCTL2	2222	1	2	4444	2889	1	2	5777
PDT	3766	64	128	482048	4896	128	256	1253325
PMM	1530	128	256	391680	1989	0	0	0
PAD	1468	16	32	46976	1908	32	64	122138
PSL	376	16	32	12032	489	0	0	0
PMU	828	1	2	1656	1076	0	0	0
PDR	3766	32	32	120512	4896	64	64	313331
PMR	1616	16	16	25856	2101	16	16	33613
PGP	468	2	2	936	608	4	8	4867
PSWCTL	2508	1	1	2508	3260	1	1	3260
PSWD	1838	8	8	14704	2389	16	16	38230
PBUF	500	16	32	16000	650	32	64	41600
			合計	1131528			合計	1831970

1832 kｹﾞｰﾄ

4ﾚｼﾞｽﾀを3ﾚｼﾞｽﾀに減らし 0.75倍とすると 1374 k ｹﾞｰﾄ

4-3. 結果

927 + 1374 = 2301kｹﾞｰﾄ



3bit booth

A_2	A_1	A_0	A_{-1}	W	1倍	2倍	3倍	4倍	負
0	0	0	0	0	0	0	0	0	0
0	0	0	1	1	1	0	0	0	0
0	0	1	0	1	1	0	0	0	0
0	0	1	1	2	0	1	0	0	0
0	1	0	0	2	0	1	0	0	0
0	1	0	1	3	0	0	1	0	0
0	1	1	0	3	0	0	1	0	0
0	1	1	1	4	0	0	0	1	0
1	0	0	0	−4	0	0	0	1	1
1	0	0	1	−3	0	0	1	0	1
1	0	1	0	−3	0	0	1	0	1
1	0	1	1	−2	0	1	0	0	1
1	1	0	0	−2	0	1	0	0	1
1	1	0	1	−1	1	0	0	0	1
1	1	1	0	−1	1	0	0	0	1
1	1	1	1	0	0	0	0	0	0