CHAPTER 1

EFFICIENT IMPLEMENTATION OF THE RECTIFICATION PROCEDURE USING ZDDS

1.1 Experimental Results

This section presents the experimental results for rectification of finite field circuits, and logic synthesis of the rectification function. An implementation of Algorithm **??** is written using Python programming language, wherein the PolyBori's [2] Python API is used for ZDD based computations. The optimization of ON-set with the DC-set is performed using *sis* tool [3], and the resulting rectification function is mapped using *abc* tool [1]. The experiments are performed on a 3.5GHz Intel Core$^{\text{TM}}$ i7-4770K Quad-Core CPU with 32 GB of RAM.

1.1.1 Mastrovito Multipliers

Table 1.1 presents the results of rectification and synthesis of rectification function for Mastrovito multipliers with operand width k when a gate change bug has occurred in the logic topologically closer to primary inputs.

1.1.2 Point Addition

1.1.3 Montgomery Multipliers

Table 1.1: Mastrovito Multipliers. Checks performed from PI side; bug near inputs (NI); #G: number of gates; BO: set of buggy outputs; CN: target nets; Deb: debugging time; #Chks: number of checks; Tot: total time; A: area; D: delay; (t): time in seconds

k	#G	Rectification					RF Synthesis			
							ON		ON-DC	
		$\lvert BO\rvert$	$\lvert CN\rvert$	Deb(t)	#Chks	Tot(t)	A	D	A	D
4	39	1	16	$<$ 0.01	8	0.01	4.0	3	1.0	1
8	171	4	12	$<$ 0.01	4	0.01	4.0	3	1.0	1
16	804	4	30	0.01	13	0.06	4.0	3	1.0	1
32	2855	3	59	0.01	3	0.17	7.0	3	7.0	3
64	11197	3	34	0.06	4	0.73	7.0	3	7.0	3
96	24521	2	213	0.24	24	1.9	7.0	3	7.0	3
128	43253	2	389	0.83	77	4.24	7.0	3	7.0	3
163	69857	1	931	14.58	578	21.3	52.0	6	52.0	6
233	119465	1	759	12.08	333	24.37	15.0	4	15.0	4
283	189714	1	907	33.98	301	62.82	5.0	3	5.0	3
409	384762	1	1133	61.01	404	161.53	5.0	3	5.0	3
571	827548	2	237	6.74	7	1082.38	6.0	3	6.0	3

Table 1.2: Mastrovito Multipliers. Checks performed from PI side; bug in middle of logic (NM); #G: number of gates; BO: set of buggy outputs; CN: target nets; Deb: debugging time; #Chks: number of checks; Tot: total time; A: area; D: delay; (t): time in seconds

k	#G	Rectification					RF Synthesis			
							ON		ON-DC	
		$\lvert BO\rvert$	$\lvert CN\rvert$	Deb(t)	#Chks	Tot(t)	A	D	A	D
4	39	1	22	$<$ 0.01	8	0.01	5.0	3	5.0	3
8	171	1	51	0.01	29	0.03	8.0	4	8.0	4
16	804	2	38	0.01	12	0.06	19.0	5	19.0	5
32	2855	1	179	0.28	104	0.44	19.0	5	19.0	5
64	11197	1	311	0.72	139	1.4	59.0	7	58.0	7
96	24521	1	685	3.43	342	5.11	64.0	7	64.0	7
128	43253	1	1125	15.29	889	18.69	99.0	11	78.0	22
163	69857	1	1249	21.3	911	28.16	146.0	12	31.0	5
233	119465	1	931	12.59	402	25.07	122.0	11	112.0	11
283	189714	1	2143	89.54	1341	120.59	444.0	15	565.0	16
409	384762	1	1229	65.09	350	167.13	135.0	13	31.0	5
571	827548	1	3043	498.8	1485	1556.69	211.0	12	180.0	14

Table 1.3: Mastrovito Multipliers. Checks performed from PI side; bug near outputs (NO); #G: number of gates; BO: set of buggy outputs; CN: target nets; Deb: debugging time; #Chks: number of checks; Tot: total time; A: area; D: delay; (t): time in seconds

k	#G	Rectification					RF Synthesis			
							ON		ON-DC	
		$\lvert BO\rvert$	$\lvert CN\rvert$	Deb(t)	#Chks	Tot(t)	A	D	A	D
4	39	1	22	< 0.01	8	0.01	25.0	8	26.0	8
8	171	1	51	0.02	29	0.03	44.0	9	52.0	10
16	804	1	145	0.17	72	0.22	87.0	11	78.0	11
32	2855	1	179	0.91	104	1.09	111.0	8	109.0	8
64	11197	1	311	16.99	139	17.93	263.0	9	269.0	12
96	24521	1	572	157.17	381	160.06	3729.0	22	3342.0	21
128	43253	1	731	1178.32	703	1186.93	17200.0	24	ME	ME
163	69857	1	1165	2349.0	799	2364.47	11946.0	26	ME	ME
233	119465	1	931	2660.66	650	2684.23	3055.0	26	ME	ME
283	189714	1	2143	26019.76	1507	26101.89				
409	384762	1	1229	18888.0	1004	19068.2	3194.0	22	ME	ME
571	827548	1	3043	30426.7	1973	31622.95				

Table 1.4: Mastrovito Multipliers. Checks performed from PO side; bug near outputs (NO); #G: number of gates; BO: set of buggy outputs; CN: target nets; Deb: debugging time; #Chks: number of checks; Tot: total time; A: area; D: delay; (t): time in seconds

k	#G	Rectification					RF Synthesis			
							ON		ON-DC	
		$\lvert BO\rvert$	$\lvert CN\rvert$	Deb(t)	#Chks	Tot(t)	A	D	A	D
4	39	1	22	< 0.01	1	0.01	33.0	8	33.0	8
8	171	1	51	< 0.01	1	0.01	24.0	6	39.0	10
16	804	1	145	< 0.01	1	0.05	85.0	11	54.0	7
32	2855	1	179	0.02	1	0.19	108.0	8	106.0	8
64	11197	1	311	0.06	1	0.97	235.0	9	231.0	9
96	24521	1	572	0.16	1	2.47	531.0	10	534.0	10
128	43253	1	731	0.28	1	6.4	683.0	11	694.0	12
163	69857	1	1165	0.4	1	11.57	999.0	12	997.0	12
233	119465	1	931	0.63	1	19.01	907.0	11	905.0	11
283	189714	1	2143	1.61	1	56.51	2088.0	13	2084.0	13
409	384762	1	1229	2.35	1	142.49	1220.0	12	1213.0	12
571	827548	1	3043	6.69	1	1077.62	2966.0	14	2975.0	14

Table 1.5: Point Addition. Checks performed from PI side; bug near inputs (NI); #G: number of gates; BO: set of buggy outputs; CN: target nets; Deb: debugging time; #Chks: number of checks; Tot: total time; A: area; D: delay; (t): time in seconds

k	#G	Rectification					RF Synthesis			
							ON		ON-DC	
		$\lvert BO \rvert$	$\lvert CN \rvert$	Deb(t)	#Chks	Tot(t)	A	D	A	D
4	48	4	15	< 0.01	11	0.01	13.0	5	32.0	11
8	234	8	33	0.03	23	0.04	217.0	19	251.0	25
16	896	16	96	0.53	90	0.6	263.0	19	333.0	30
32	2910	32	159	2.36	120	2.59	432.0	21	607.0	26
64	10646	64	301	24.33	287	25.31	886.0	23	1286.0	34
96	24791	96	463	80.52	406	83.56	1454.0	24	1446.0	95
128	43173	128	639	89.21	206	96.91	5079.0	27	3149.0	47
163	71649	163	914	675.74	905	693.91	4246.0	26	4243.0	43
233	122162	2	1115	4.02	3	23.52	7.0	3	22.0	8
283	207654	283	1160	2051.13	1154	2120.28	3774.0	27	5370.0	31
409	367825	409	823	2186.87	776	2348.94	2701.0	24	ME	ME
571	813354	571	2302	26063.93	2288	27503.6	7942.0	25	9896.0	34

Table 1.6: Point Addition. Checks performed from PI side; bug in middle of logic (NM); #G: number of gates; BO: set of buggy outputs; CN: target nets; Deb: debugging time; #Chks: number of checks; Tot: total time; A: area; D: delay; (t): time in seconds

k	#G	Rectification					RF Synthesis			
							ON		ON-DC	
		$\lvert BO \rvert$	$\lvert CN \rvert$	Deb(t)	#Chks	Tot(t)	A	D	A	D
4	48	1	32	0.01	23	0.01	67.0	14	85.0	10
8	234	2	45	0.05	41	0.06				
16	896	1	181	0.85	135	0.92	526.0	18	598.0	19
32	2910	1	329	4.97	257	5.19	40.0	10	41.0	10
64	10646	1	690	43.35	520	44.34	53.0	10	53.0	9
96	24791	1	841	120.85	606	123.88	57.0	9	57.0	9
128	43173	1	1217	338.28	882	346.08	300.0	10	313.0	14
163	71649	1	1544	743.83	1154	761.93	71.0	8	74.0	8
233	122162	1	1368	764.17	858	784.26	53.0	11	3.0	3
283	207654	1	2402	2969.42	1713	3037.63	1702.0	18	1775.0	18
409	367825	1	1845	2814.62	973	2973.53	16.0	5	15.0	5
571	813354	1	4016	20503.01	2786	21954.25	298.0	13	284.0	14

Table 1.7: Point Addition. Checks performed from PO side; bug in middle of logic (NM); #G: number of gates; BO: set of buggy outputs; CN: target nets; Deb: debugging time; #Chks: number of checks; Tot: total time; A: area; D: delay; (t): time in seconds

k	#G	Rectification					RF Synthesis			
							ON		ON-DC	
		$\lvert BO\rvert$	$\lvert CN\rvert$	Deb(t)	#Chks	Tot(t)	A	D	A	D
4	48	1	32	< 0.01	1	0.02	26.0	6	34.0	8
8	234	2	45	< 0.01	1	0.05	5.0	4	5.0	4
16	896	1	181	0.01	1	0.08	205.0	12	205.0	14
32	2910	1	329	0.02	1	0.26	404.0	14	395.0	13
64	10646	1	690	0.1	1	1.12	790.0	14	820.0	14
96	24791	1	841	0.21	1	3.36	938.0	14	910.0	14
128	43173	1	1217	0.47	1	8.4	1690.0	15	1735.0	15
163	71649	1	1544	0.79	1	18.91	2102.0	16	2075.0	16
233	122162	1	1368	1.08	1	21.05	1453.0	13	1444.0	13
283	207654	1	2402	2.1	1	70.9	2812.0	17	2780.0	18
409	367825	1	1845	3.13	1	161.24	1978.0	14	1978.0	14
571	813354	1	4016	7.93	1	1432.93	3570.0	16	3571.0	16

Table 1.8: Point Addition. Checks performed from PO side; bug near outputs (NO); #G: number of gates; BO: set of buggy outputs; CN: target nets; Deb: debugging time; #Chks: number of checks; Tot: total time; A: area; D: delay; (t): time in seconds

k	#G	Rectification					RF Synthesis			
							ON		ON-DC	
		$\lvert BO\rvert$	$\lvert CN\rvert$	Deb(t)	#Chks	Tot(t)	A	D	A	D
4	48	1	26	< 0.01	9	0.01	33.0	9	19.0	5
8	234	1	73	< 0.01	1	0.02	80.0	11	61.0	7
16	896	1	273	0.01	1	0.16	339.0	13	354.0	13
32	2910	1	341	0.03	1	0.71	476.0	13	491.0	14
64	10646	1	873	0.16	1	7.11	1028.0	13	1032.0	15
96	24791	1	1161	0.41	1	23.08	1769.0	16	1804.0	15
128	43173	1	1791	1.03	1	93.79	3444.0	17	3493.0	17
163	71649	1	2174	117.57	1	257.47	4138.0	17	4060.0	17
233	122162	1	1409	1.32	1	54.33	1643.0	15	1637.0	13
283	207654	1	3410	3.75	1	294.51	5035.0	17	5081.0	17
409	367825	1	2611	4.1	1	276.35	4138.0	15	4139.0	16
571	813354	1	6622	10.85	1	1993.93	6538.0	17	6480.0	19

Table 1.9: Montgomery Multipliers. Checks performed from PI side; bug near inputs (NI); #G: number of gates; BO: set of buggy outputs; CN: target nets; Deb: debugging time; #Chks: number of checks; Tot: total time; A: area; D: delay; (t): time in seconds

k	#G	Rectification					RF Synthesis			
							ON		ON-DC	
		$\vert BO\vert$	$\vert CN\vert$	Deb(t)	#Chks	Tot(t)	A	D	A	D
4	50	4	15	< 0.01	7	0.01	13.0	5	98.0	21
8	222	8	129	0.04	23	0.06	173.0	17	140.0	17
16	931	16	821	1.98	199	2.07	1188.0	22	925.0	24
32	2749	32	1382	1.55	56	1.8	1665.0	25	2467.0	69
64	9587	64	3562	18.63	161	19.57	9400.0	27	5195.0	27
96	20994	96	17417	69.03	180	72.36	14554.0	27	9965.0	26
128	35713	128	1246	133.65	369	137.55	3753.0	25	2931.0	57
163	57489	163	3017	18.86	20	27.9	21559.0	31	ME	ME
233	111189	233	500	229.75	246	242.81	615.0	20	8.0	4
283	170904	283	80412	77.84	30	138.52	216296.0	35	ME	ME
409	340516	8	948	2418.16	792	2509.38	7.0	3	22.0	8

Table 1.10: Montgomery Multipliers. Checks performed from PO side; bug in middle of logic (NM); #G: number of gates; BO: set of buggy outputs; CN: target nets; Deb: debugging time; #Chks: number of checks; Tot: total time; A: area; D: delay; (t): time in seconds

k	#G	Rectification					RF Synthesis			
							ON		ON-DC	
		$\vert BO\vert$	$\vert CN\vert$	Deb(t)	#Chks	Tot(t)	A	D	A	D
4	50	3	22	< 0.01	1	0.01	22.0	8	21.0	8
8	222	5	129	0.03	19	0.04	46.0	9	60.0	10
16	931	5	821	5.17	551	5.24	134.0	12	145.0	11
32	2749	11	1512	17.29	738	17.57	306.0	12	331.0	13
64	9587	32	3796	44.69	349	47.76	559.0	13	559.0	14
96	20994	53	17652	2951.57	11810	2962.49	903.0	12	921.0	14
128	35713	9	1757	0.36	1	7.66	1056.0	12	1057.0	13
163	57489	73	4381	6.07	2	75.08	1636.0	13	1637.0	13
233	111189	5	1006	1.05	1	15.01	1208.0	12	1210.0	12
283	170904	143	80412	87201.68	57188	87279.37	1204.0	12	1238.0	14
409	340516	8	1132	3.81	1	115.85	963.0	12	966.0	11

Table 1.11: Montgomery Multipliers. Checks performed from PO side; bug near outputs (NO); #G: number of gates; BO: set of buggy outputs; CN: target nets; Deb: debugging time; #Chks: number of checks; Tot: total time; A: area; D: delay; (t): time in seconds

k	$\#G$	Rectification					RF Synthesis			
							ON		ON-DC	
		$\lvert BO \rvert$	$\lvert CN \rvert$	Deb(t)	#Chks	Tot(t)	A	D	A	D
4	50	2	28	< 0.01	1	0.01	36.0	9	36.0	9
8	222	1	215	0.01	5	0.02	65.0	10	58.0	10
16	931	1	907	0.01	1	0.11	168.0	10	174.0	12
32	2749	4	2533	0.03	1	0.44	231.0	13	249.0	13
64	9587	4	8914	0.1	1	1.6	217.0	9	216.0	9
96	20994	4	20898	4.36	20	11.17	580.0	11	585.0	12
128	35713	1	5986	206.36	343	231.63	1217.0	16	1199.0	14
163	57489	2	40227	0.99	1	22.22	607.0	11	608.0	11
233	111189	2	2652	1.21	1	43.28	719.0	11	724.0	11
283	170904	2	170335	2.36	1	101.54	636.0	14	619.0	11
409	340516	1	7804	4.54	1	300.9	1017.0	12	1022.0	12

REFERENCES

[1] R. Brayton and A. Mishchenko, *ABC: An Academic Industrial-Strength Verification Tool*, in Comp. Aid. Verif., vol. 6174, 2010, pp. 24–40.

[2] M. Brickenstein and A. Dreyer, *PolyBoRi: A Framework for Gröbner-basis Computations with Boolean Polynomials*, Journal of Symbolic Computation, 44 (2009), pp. 1326–1345.

[3] E. Sentovich *et al.*, *SIS: A System for Sequential Circuit Synthesis*, Tech. Rep. UCB/ERL M92/41, ERL, Dept. of EECS, Univ. of California, Berkeley., 1992.