유한체에서 Boolean 행렬의 복잡도에 관한 연구

Complexity of Boolean matrices in finite fiels

조 인 호(고려대학교 수학과 교수)
임 종 인(고려대학교 자연과학대 수학과 부교수)
정 석 원(고려대학교 수학과대학원 석사과정)

개 요

공용키암호법의 대표적인 것으로 El Gamal 암호법과 RSA 암호법이 있는데, RSA 암호법은 정수의 인수분해가 어렵다는 것에 안전성을 둔 반면에 El Gamal 암호법은 discrete logarithm을 푸는 것이 어렵다는데 안전성을 두고 있다.[6] 그런데 유한체상에서 멱승과 곱셈이 효율적으로 수행이 된다면 El Gamal 암호법이 RSA 암호법보다 유용하다는 사실을 알게 되었다. 그런데 Coppersmith의 이산로그 알고리즘을 이용하면 $n > 1000$ 이 되어야 El Gamal 암호법이 안전성을 보장 받을 수 있으나 이 경우 복잡도의 증가로 인한 gate수의 급속한 증가로 고속연산전용 VLSI 설계시 어려움이 있다.[3] 그래서 본 논문은 복잡도를 줄일 수 있는 정규기저들의 탐색에 연구의 중점을 두었다.

1. 최적정규기저의 생성

갈로아체 $GF(p^n)$의 기저 N을

$$N = \{\beta, \beta^{p}, \cdots, \beta^{p^{n-1}}\}$$

이라하자. 그러면 $GF(p^n)$ 안의 모든 원소 A는 다음과 같이 유일하게 표시된다.

$$A = \sum_{i=1}^{n-1} a_i \beta^{p^i}, \quad a_i \in GF(p)$$

여기서 A를 벡터 $(a_0, a_1, \cdots, a_{n-1})$로 표시하면, A^2은 $(a_{n-1}, a_0, \cdots, a_{n-2})$가 되어 A의 벡터를 오른쪽으로 한칸씩 옮긴 것이 된다. 그래서 갈로아체 $GF(p^n)$에서의 멱승은 쉽게 구할 수 있다.

또다른 원소 B를

$$B = \sum_{j=1}^{n-1} b_j \beta^{p^j}, \quad b_j \in GF(p)$$

이라 놓자. 그리고 C를 A,B의 곱이라 놓고 그 벡터표현을 $(c_0, c_1, \cdots, c_{n-1})$이라 하자. 그러면 $GF(p)$에 속하는 원소 λ_{ij}가 있어서 다음식을 만족한다.

$$c_k = \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} \lambda_{ij} \cdot a_{i+k} \cdot b_{j+k}, \quad k = 0, 1, \cdots, n-1$$

여기에서 첨자들은 modulo n 의 계산이다. 따라서 $c_0 = A \cdot \lambda \cdot {}^tB$, $\lambda = (\lambda_{ij})$ 라 표현되며, 나머지 C의 계수 c_k들은 A와 B를 k번 옮긴 후 λ와의 곱으로 구할 수 있다. 따라서 다음과 같은 정의를 얻을 수 있다.

정의 1.1 $GF(p^n)$ 에서 C_N을 n x n 행렬 λ의 영아닌 원소의 개수라 하자. 우리는 이때의 C_N을 기저 N에 대한 복잡도라 부른다.

정의 1.2 특별히 $C_N = 2n-1$ 인 경우의 C_N을 최적정규기저라 부른다.

정리 1.1 $f(x) = 1 + x + x^2 + \cdots + x^n$ 이 기약다항식이고, $f(x)$ 의 근 β가 갈로아체 $GF(p^n)$에서 최적정규기저가 되기 위한 필요충분조건은 n+1이 소수이고 p가 Z_{n+1}에서 원시원이 될 때이다.

다음의 표는 $GF(2^n)$ 에서 이 정리를 만족하는 n(≤2000)의 값이다.

2	4	10	12	18	28	36	52	60	66
82	100	106	130	138	148	162	172	178	196
210	226	268	292	316	346	348	372	378	388
418	420	442	460	466	490	508	522	540	546
556	562	586	612	618	652	906	940	946	1018
1060	1090	1108	1116	1122	1170	1186	1212	1228	1236
1258	1276	1282	1290	1300	1306	1372	1380	1426	1450
1452	1482	1492	1522	1530	1548	1570	1618	1620	1636
1668	1692	1732	1740	1746	1786	1860	1866	1876	1900
1906	1930	1948	1972	1978	1986	1996			

이상의 n에 대해서 컴퓨터 실행결과 n = 2 일때를 제외 하고는 self-dual 정규기저가 되지 않았다.

정리 1.2 (1) 2n+1이 소수이고 2가 Z_{n+1}에서 원시원 이거나
(2) 2n+1이 소수이고 $2n+1 \equiv 3 \bmod 4$ 이며 2가 Z_{n+1}에서 quadratic residue를 생성하면 갈로아체 $GF(2^n)$은 최적정규기저를 갖는다.

$2^{2n} \equiv 1 \bmod 2n+1$ 이므로 2n+1이 $2^{2n}-1$을 나눈다. 그러면 갈로아체 $GF(2^{2n})$에 primitive (2n+1)st root of unity β가 존재한다. 이때 α를 $\beta + \beta^{-1}$ 이라 놓으면 α로 만들어진 정규기저

$$N = \{\alpha, \alpha^2, \cdots, \alpha^{2^{n-1}}\}$$

이 최적정규기저가 됨을 위의 정리 1.2로부터 알 수 있다.

$$\alpha^{2^i} \cdot \alpha^{2^j} = (\beta^{2^i} + \beta^{2^i})(\beta^{2^j} + \beta^{2^j})$$

$$= (\beta^{(2^i+2^j)} + \beta^{-(2^i+2^j)}) + (\beta^{(2^i-2^j)} + \beta^{-(2^i-2^j)})$$

2가 Z_{n+1}에서 원시원이면, 적당한 $0 \le k \le 2n-1$ 가 존재해서 $2^i+2^j = 2^k$을 만족한다. 그리고 2가 Z_{n+1}에서 quadratic residue를 생성하면, 2^i+2^j 이 2^k 이거나 -2^k 이 된다. 그러므로 $2^i \not\equiv 2^j \bmod 2n+1$이면, 적당한 k,k'가 존재해서

$$\alpha^{2^i} \cdot \alpha^{2^j} = \alpha^{2^k} + \alpha^{2^{k'}}$$

가 되어

$$\begin{aligned} Tr(\alpha^{2^i} \cdot \alpha^{2^j}) &= Tr(\alpha^{2^k} + \alpha^{2^{k'}}) \\ &= Tr(\alpha^{2^k}) + Tr(\alpha^{2^{k'}}) \\ &= 0 \end{aligned}$$

가 된다.

만약에 2^i 이 2^j 이나 -2^j과 같다면, $2^i \pm 2^j$ 이 둘 중 하나는 0이 아니다. 그러므로

$$2^i + 2^j = 2^k,\ 2^i + 2^j = -2^k,\ 2^i - 2^j = 2^k\ ,\ 2^i - 2^j = -2^k$$

중 한 식이 만족된다. 그러면 우리는

$$\alpha^{2^i} \cdot \alpha^{2^j} = \alpha^{2^k}$$

을 얻을 수 있다. 그러므로

$$\begin{aligned} Tr(\alpha^{2^i} \cdot \alpha^{2^j}) &= Tr(\alpha^{2^k}) \\ &= 1 \end{aligned}$$

이 된다. 따라서 우리는 정리 1.2에서 만들어낸 최적정규기저는 모두 self-dual 정규기저가됨을 알 수 있다. 다음 표는 정리 1.2 (1)을 만족하는 최적정규기저이다.

5	6	9	14	18	26	29	30	33	41
50	53	65	69	74	81	86	89	90	98
105	113	134	146	158	173	174	186	189	194
209	210	221	230	233	245	254	261	270	273
278	281	293	306	309	326	329	330	338	350
354	378	386	393	398	410	413	414	426	429
438	441	459	470	473	509	530	545	554	558
561	585	593	606	614	618	629	638	641	645
650	659	686	690	713	725	726	741	746	749
761	765	774	785	809	810	818	833	834	846
866	870	873	893	930	933	938	950	953	965
974	986	989	993	998	1013	1014	1026	1034	1041
1049	1065	1070	1106	1110	1118	1121	1133	1134	1146
1154	1166	1169	1178	1185	1194	1218	1229	1233	1238
1265	1269	1274	1278	1289	1310	1329	1338	1341	1346
1349	1353	1370	1394	1398	1401	1409	1418	1421	1425
1430	1454	1469	1478	1481	1505	1509	1518	1533	1541
1593	1601	1626	1649	1653	1661	1673	1685	1706	1730
1733	1734	1745	1749	1758	1766	1769	1773	1778	1785
1790	1791	1806	1818	1821	1829	1838	1845	1850	1854
1866	1889	1898	1901	1925	1926	1938	1953	1958	1961
1973	1994								

다음 표는 정리 1.2 (2)를 만족하는 최적정규기저이다.

3	11	23	35	39	51	83	95	99	119
131	135	155	179	183	191	231	239	243	251
299	303	323	359	371	411	419	431	443	483
491	495	515	519	531	543	575	611	615	639
651	659	683	719	723	743	755	771	779	783
791	803	831	879	891	911	923	935	939	975
1019	1031	1043	1055	1103	1119	1155	1199	1211	1223
1251	1271	1275	1295	1323	1331	1355	1359	1439	1443
1451	1463	1499	1511	1539	1559	1583	1659	1679	1703
1755	1763	1779	1791	1811	1835	1859	1863	1883	1923
1931	1955	1959	1965	1993					

이상에서 살펴본바와 같이 모든 가능한 n($\leq$ 2000) 에대해 최적정규기저는 대략 20%정도를 차지하고 있다. 그런데 이 최적정규기저 중 75%가 self-dual 정규기저를 이룬다.

2. 저복잡도정규기저 생성.

1절에서는 복잡도 C_N 이 2n+1 인 최적의 경우를 살펴보았다. 이절에서는 복잡도가 최적은 아니지만 n에 대해 선형적 증가를 갖는 정규기저를 찾는 방법을 소개한다.

정의 2.1 군 G가 가환군이며 n이 정수일 때 G^n을 다음과 같이 정의한다.

$$G^n = \{a^n : a \in G\}$$

보조정리 2.1 kn+1이 소수이고 군 G 가 Z_{kn+1}의 곱셈군이라 하자. 만약 $G = \langle 2, G^n \rangle$ 이고 r이 Z_{kn+1}의 primitive kth root of unity라면, G 의 임의의 원소 β는 적당한 $0 \leq i \leq n-1$ 와 $0 \leq j \leq k-1$ 에 대해서

$$\beta = 2^i r^j$$

으로 유일하게 표현된다.

정리 1.2(2) 에서 2는 quadratic residue를 생성했는데, 위의 보조정리 에서 $G = \langle 2, G^n \rangle$ 은 2가 kth residue를 생성함을 의미한다. 이는 다음과 같은 방법으로 쉽게 알 수 있다. δ를 G의 원시원이라 하자. 그러면 적당한 m이 존재해서 $\delta^m = 2$ 가 된다. 이때 $(m, kn) = k$ 이면 $G = \langle 2, G^n \rangle$ 이 된다. 그리고 δ^n 이 primitive kth root of unity r이 된다.

정리 2.1 kn+1이 소수이고 군 G가 Z_{kn+1}의 곱셈군이라 하자. 만약 $G = \langle 2, G^n \rangle$ 이고 β가 $GF(2^{kn})$ 안에서 primitive (kn+1)st root of unity 라면,

$$\alpha = \sum_{i=0}^{k-1} \beta^{r^i}, \quad r \text{ 은 G의 primitive root of unity}$$

이 $GF(2^n)$ 의 정규기저를 생성한다.

정리 2.2 N이 정리 2.1에서 생성된 정규기저라 하면 복잡도 C_N의 bound는 다음과 같다.
k가 짝수이면 $kn-(k^2-3k+3) \le C_N \le kn-1$ 이고
k가 홀수이면 $(k+1)n-(k^2-k+1) \le C_N \le (k+1)n-k$ 이다.

정리 2.3 먼저 정리 2.1의 조건이 만족한다고 하자. 그리고

$$f(x) = (x^{t1} - x^{j1})(x^{j2} - 1) - (x^{t2} - x^{j2})(x^{j1} - 1)$$
$$g(x) = x^{j1+t2} - x^{t1} - x^{j1} + 1$$
$$h(x) = k\text{th cyclotomic 다항식 } Q_k(x)$$

라 놓고, $1 \le t_1, j_1, t_2, j_2 \le k-1, t_1 \ne j_1, t_2 \ne j_2, t_1 \ne t_2, j_1 \ne j_2$에 대해서 GF(kn+1)[x] 안에서 gcd(f,h) = 1 이고, k 가 홀수일 때 $1 \le t_1, j_1, t_2 \le k-1, t_1 \ne t_2$에 대해서 GF(kn+1)[x] 안에서 gcd(g,h) = 1 이면 정규기저는 정리2.2의 최소 복잡도를 가진다.

정리 2.4 k=3,4에 대해서 n이 1보다 클 때, 정리 2.1에서 만든 정규기저는 복잡도 C_N이 4n-7 이다.

(증명) 먼저 k=3 인 경우부터 해보자. k가 3이므로 t_1과 j_1는 1아니면 2이다. 그리고 t_2, j_2도 1또는 2의 값을 갖는다. 그래서

$$f(x) = (x^2-x)(x^2-1)-(x-x^2)(x-1)$$
$$= x(x-1)^2(x+2)$$

가 된다. 그런데 $Q_3(x) = x^2+x+1$ 은 임의의 GF(3n+1)위에서 1이나 -2를 근으로 갖지 않는다. 따라서 $\gcd(f, Q_3(x)) = 1$이다. 이 경우 k가 홀수이므로 g(x)와의 공통인수도 생각해봐야 한다. 그런데 위와같은 성질에 의해서 우리는

$$g(x) = 2-2x \text{거나 } g(x) = 1-x \text{거나 } g(x) = 1-x^2 \text{ 이거나 } g(x) = 2-2x^2$$

을 얻을 수 있다. 그런데 이 경우 역시 g(x)의 근이 1또는 -2뿐이므로 $Q_3(x)$와는 공통인수를 갖지 않는다. 그러므로 복잡도는 4n-1이다.
이제 k가 4인경우를 해보자. $Q_4(x) = x^2+1$이고 유리수체 위에서는 $(f(x), Q_4(x)) = 1$ 이다. 따라서 $f(x) \equiv Ax+B \bmod x^2+1$이 된다. 여기서 $|A| + |B| \le 6$ 이고 A와 B는 동시에 0은 아니다. Q[x] 안에서 $(f(x), Q_4(x)) = 1$ 이므로, Z[x] 안에 f'(x)와 Q'(x)가 있어서

$$f(x)f'(x) + Q_4(x)Q'(x) = m \ , \ m \in Z^+$$

을 만족한다. 이 식은 GF(4n+1)[x] 에서도 성립하므로, 만약 4n+1이 m을 나누지 않는다면 $(f(x), Q_4(x)) = 1$ 이 된다. $A^2(x^2+1)-(Ax-B)(Ax+B) = A^2+B^2 \le 36$ 이므로 4n+1이 36을 나눈다고 해보자. 그러면 A,B가 모두 짝수이므로 36을 나누는 소수는 2,3 또는 5 뿐이다. 그런데 4n+1 형태는 5이다. 그러므로 Ax+B = 2x+4가 된다. 그런데 x^2+1 이 -2를 근으로 갖지 않기위한 필요충분조건은 $(-2)^2+1 = 5 \not\equiv 0 \bmod(4n+1)$ 이므로 4n+1이 5만 아니면 정리가 성립한다. 즉 n>1 이면 정리가 성립한다.

다음의 표는 k가 3일 때 저복잡도를 가지는 GF(2^n) 과 primitive kth root of unity r in GF(kn+1)을 나타낸 것이다.

n	r	n	r	n	r	n	r	n	r
20	47	22	37	46	96	54	104	76	134
92	116	94	238	102	289	116	226	124	284
126	327	140	400	166	139	180	129	182	40
204	65	206	366	214	465	220	296	236	227
244	425	246	320	252	27	276	125	284	632
286	260	294	545	302	384	332	304	340	652
356	86	364	151	374	33	390	420	404	217
412	300	430	346	484	759	494	1444	510	884
516	1273	526	639	542	1362	564	1259	566	397
574	1681	580	356	582	371	596	152	620	1406
622	834	644	1341	662	647	676	975	684	1855
694	449	710	468	734	285	740	543	750	708
756	2186	764	1303	780	1106	782	1284	790	464
796	689	812	2351	822	2250	852	835	886	903
892	1643	894	2046	902	1327	916	2153	932	1696
934	2389	972	247	1006	239	1012	2291	1022	2093
1062	1871	1076	914	1084	1813	1086	852	1102	57
1124	2718	1156	1785	1172	258	1182	2384	1190	3467
1214	422	1230	3216	1236	498	1244	948	1284	2713
1292	224	1302	3844	1334	822	1340	2208	1342	2206
1364	902	1366	2017	1406	112	1414	298	1420	1647
1446	237	1494	505	1502	3715	1516	1744	1532	377
1534	4423	1540	2857	1550	3864	1574	717	1596	3109
1604	1888	1644	2131	1652	2674	1662	3850	1670	2907
1686	3146	1700	3486	1726	1497	1742	451	1774	1282
1804	1224	1812	2271	1814	2588	1852	1827	1884	4912
1886	4194	1916	5418	1942	1350	1950	5273	1956	5091
1974	5494								

다음의 표는 k가 4일 때 저복잡도를 가지는 GF(2^n)과 primitive kth root of unity r in GF(kn+1)을 나타낸 것이다.

n	r	n	r	n	r	n	r	n	r
7	12	9	31	13	30	15	11	25	10
37	105	43	80	45	162	49	183	67	187
70	228	73	138	79	203	87	213	88	311
97	115	115	48	127	301	139	118	144	553
153	578	154	194	163	149	165	555	169	26
175	566	177	96	193	317	199	215	205	295
207	583	213	333	219	151	235	844	258	678
262	623	265	958	274	341	277	354	279	214
288	186	300	1152	307	632	319	113	325	1250
343	668	345	366	363	497	370	1016	373	88
400	1561	405	166	409	316	417	1449	423	1449
433	1323	435	59	465	61	469	137	472	1558
475	1683	487	589	493	259	499	1585	507	992
513	244	517	164	532	372	535	419	553	1130
555	1431	559	1021	567	1287	568	290	573	1693
577	1621	583	2225	589	633	597	2104	609	915
637	357	655	472	669	2127	673	1834	685	656
697	167	699	2194	709	416	715	1202	727	2031
739	1222	759	281	762	2574	772	2696	784	56
804	1781	813	1598	828	2906	853	1942	865	2008
867	2466	882	808	883	548	889	2614	895	364
903	1027	918	1309	925	2422	927	1609	949	3055
958	361	963	1305	969	502	979	3082	997	481
1000	3102	1003	1230	1005	3298	1023	1059	1033	3400
1039	1761	1054	2306	1057	2082	1063	561	1072	3761
1087	3741	1089	66	1093	1904	1099	505	1114	2577
1123	2280	1129	1474	1159	2593	1197	3308	1203	2945
1204	1291	1219	4158	1234	4088	1239	359	1243	223
1269	4219	1297	2734	1308	2253	1315	4434	1327	1804
1348	665	1369	74	1375	1115	1389	2478	1393	3556
1423	1193	1429	3301	1435	3363	1437	4943	1453	796
1467	1042	1470	1098	1507	1801	1513	3221	1525	247
1543	2447	1549	2007	1557	1523	1569	1033	1579	1963
1597	4297	1599	1302	1617	2977	1630	2364	1642	3038
1663	752	1675	1721	1677	4559	1683	2217	1690	4986
1695	5786	1698	709	1707	1625	1717	5871	1729	6654
1737	6017	1753	2480	1767	6881	1777	304	1782	767
1807	3572	1809	2502	1813	5042	1837	2061	1869	1652
1870	1408	1885	2867	1887	2931	1893	3830	1894	6037
1897	3270	1905	2038	1917	5377	1929	4764	1939	6945
1947	4411	1954	5253	1957	5792	1960	198	1963	6094
1969	7557	1975	4555	1987	679				

이상에서 살펴본 바와 같이 모든 가능한 n(<2000) 에 대해서 최적은 아니지만 복잡도가 상당히 작은 정규기저를 찾았다. 이들은 전체 경우 중 17%를 차지한다. 우리는 k를 조금크게 하면 위의 경우보다는 복잡도가 좀 크지만 n에 선형적으로 증가하는 정규기저를 찾을 수 있을 것이다.

참 고 문 헌

1. R.C.Mullin, I.M.Onyszchuk and S.A.Vanstone, "Optimal normal bases in GF(p^n)", Discrete Applied Mathematics 22, Dec. 1987, pp 149 - 161.
2. David W.Ash, Ian F.Blake and Scott A.Vanstone, "Low complexity normal bases", Discrete Applied Mathematics 25, Aug. 1988, pp 191 - 210.
3. C.C.Wang, "Exponentiation in finite fields", 1985, UCLA.
4. Rudolf Lidl, Introduction to finite fields and their applications, 1986, Cambridge Univ. Press.
5. S.Lang, Algebra, 2nd ed., Addison-Wesley, 1984.
6. Dominic Welh, Codes and Crytography, Clarendon press, 1989.
7. A.Lempel, M.J.Weinberger, "Self complementary normal bases in finite fields, SIAM J.DISC.Math., vol.1, No.2, May 1988, pp 193 - 198.
8. H.Cohen, A course in algorithmic algebraic number theory, Lecture note.