

A NAGYMÉRTÉKBEN NEMLINEÁRIS FÜGGVÉNYEK SZÁMÁNAK ALSÓ KORLÁTJA

LICSKÓ ILDIKÓ

Budapest

A jelen dolgozatban megkíséreljük a páratlan dimenziójú, nagymértékben nemlineáris függvények és az eggyel magasabb dimenziójú maximálisan nemlineáris függvények számát alulról megbecsülni. A becslésre a nevezett függvénycsoportok közötti összefüggés ad lehetőséget.

1. Bevezetés

A kriptográfia különböző területein alkalmazzák a Boole-függvényeket. A visszacsatolt siftregiszterekkel működő folyamrejtjelező algoritmusok nemlineáris Boole-függvényeket alkalmaznak a kulcsfolyam és a rejtendő adatok egyesítésére. A blokkos típusú rejtjelező algoritmusok az S-dobozok belsejében valamint az egyes iterációs lépésekben a kulcs és a rejtendő szöveg egyesítésére alkalmaznak nemlineáris Boole-függvényeket. A modern rejtjelfejtési módszerekkel, a lineáris és differenciális analízissel szemben csak meghatározott tulajdonságú függvények képesek ellenállni, a függvényeknek ilyen megkívánt matematikai tulajdonságai a lehető legnagyobb mértékű nemlinearitás, a korrelációimmunitás, a kiegyensúlyozottság, stb.

2. Előzetes ismeretek

Az adatokat, információkat általában bináris formában tároljuk, ezért az adatkezeléssel illetve információkezeléssel kapcsolatos feladatokat általában $\{0, 1\}^n$ halmazon valósítjuk meg. $\{0, 1\}^n$ elemei vektorteret alkotnak, amelyet Boole-térnek nevezünk. $\{0, 1\}^n$ -beli vektorok komponensei $\{0, 1\}$ értékűek, tehát egy-egy vektort tekinthetünk úgy is, mint egy egész szám bináris leírását. A Boole-tér i -edik

vektorának komponensei az i egész szám bináris reprezentációját adják. Hivatkozhatunk a vektorokra egy indexelt névvel is, ebben az esetben az indexben megjelenő szám bináris előállítását mutatják a vektor koordinátái. A Boole-tér elemei között a szokásos műveleteket értelmezhetjük: az $\mathbf{a}, \mathbf{b} \in \{0, 1\}^n$ elemek koordinátákkal felírt alakja $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ és $\mathbf{b} = (b_0, b_1, \dots, b_{n-1})$, ekkor az összeadást komponensenként elvégezve az

$$\mathbf{a} + \mathbf{b} = (a_0 + b_0, a_1 + b_1, \dots, a_{n-1} + b_{n-1})$$

eredményt kapjuk, és a skalárszorzatot az

$$\mathbf{a}\mathbf{b} = \bigoplus_{i=0}^{n-1} a_i b_i$$

kifejezés definiálja.

Az $f : \{0, 1\}^n \rightarrow \{0, 1\}$ leképezést Boole-függvénynek nevezzük. A Boole-függvényeket megadhatjuk formulákkal vagy igazságtáblájukkal. Az n -dimenziós (n változós) függvény igazságtáblája 2^n sorból áll és $n + 1$ oszlopot tartalmaz, ahol az első n oszlop a független változók értékét, az $n + 1$ -edik oszlop a hozzájuk tartozó függvényértéket mutatja. Az igazságtábla 2^n sora az adott Boole-tér valamennyi pontját és a hozzájuk tartozó függvényértéket megadja. Az igazságtábla megnevezést a táblázat $n + 1$ -edik oszlopára is használják. Gyakran alkalmazzák a Boole-függvények helyett az általuk generált $\{-1, 1\}$ sorozatot, amelynek jelölése $\bar{f} : \{0, 1\}^n \rightarrow \{-1, 1\}$. A két leképezés kapcsolata:

$$\bar{f}(\mathbf{x}) = (-1)^{f(\mathbf{x})}$$

vagy

$$\bar{f}(\mathbf{x}) = 1 - 2f(\mathbf{x}).$$

A továbbiakban az $\bar{f}(\mathbf{x})$ jelölés mindig az f által generált 2^n elemű $\{-1, 1\}$ sorozatot jelenti.

Az $f(\mathbf{x})$ függvény súlya az igazságtáblájában lévő 1-ek számát jelenti:

$$w(f) = \sum_{\mathbf{x} \in \{0, 1\}^n} f(\mathbf{x}).$$

Az $f(\mathbf{x})$ függvényről azt mondjuk, hogy kiegyensúlyozott, ha igazságtáblájában az 1-ek és a 0-ák száma megegyezik, vagyis $f(\mathbf{x}) = 1$ pontosan ugyanannyi helyen, mint $f(\mathbf{x}) = 0$. Ekkor

$$\sum_{\mathbf{x} \in \{0, 1\}^n} \bar{f}(\mathbf{x}) = 0,$$

és az $f(\mathbf{x})$ súlya: $w(f) = 2^{n-1}$.

Egy f függvényt affin függvénynek neveznek, ha Zsegalkin-polinomja minden $a_i \in \{0, 1\}$ $0 \leq i \leq n-1$ esetén

$$f(x_0, x_1, \dots, x_{n-1}) = a_0 x_0 \oplus a_1 x_1 \oplus \dots \oplus a_{n-1} x_{n-1} \oplus c$$

alakú. Ha $c = 0$ akkor lineáris függvényről beszélünk, és ekkor az $\mathbf{ax}$ lineáris függvényt tekinthetjük az $\mathbf{a}$ konstans vektor és az $\mathbf{x}$ változó skalárszorzataként.

Az f és g függvények távolságát a

$$d(f, g) = w(f \oplus g) = \sum_{\mathbf{x} \in \{0, 1\}^n} (f(\mathbf{x}) \oplus g(\mathbf{x})),$$

míg kettőjük korrelációját a

$$c(f, g) = \sum_{\mathbf{x} \in \{0, 1\}^n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x})} = \bar{f}(\mathbf{x}) \bar{g}(\mathbf{x})$$

kifejezés definiálja. A két függvény közötti távolság és a két függvény közötti korreláció kapcsolata:

$$c(f, g) = \sum_{\mathbf{x} \in \{0, 1\}^n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x})} = 2^n - 2d(f, g).$$

Legyen H egy $m \times m$ méretű mátrix, amelynek elemeire igaz, hogy $h_{ij} \in \{-1, 1\}$ minden $i, j = 0, 1, \dots, m-1$ esetén. H -t Hadamard-mátrixnak nevezzük, ha teljesül, hogy $HH^T = mI$, ahol H^T a H mátrix transzponáltja, és I az m -edrendű egységmátrix. A 2^n -edrendű Hadamard-mátrixot H_n -nel jelöljük, és ezt a mátrixot egyebek között a következő rekurzív eljárás segítségével is előállíthatjuk:

$$H_0 = 1, H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}, n = 1, 2, \dots$$

A H_n mátrix sorait l_i -vel jelöljük $i = 0, 1, \dots, 2^n - 1$. Az i -edik sor l_i , az $\mathbf{ix}$ lineáris függvény által generált $\{-1, 1\}$ sorozat, és ílymódon a H_n mátrix sorai az n -dimenziós tér minden lineáris függvénye által generált $\{-1, 1\}$ sorozatot megjelenítenek.

Az f függvény Walsh-transzformáltja az $\mathbf{a} \in \{0, 1\}^n$, $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ pontban:

$$F(\mathbf{a}) = \sum_{\mathbf{x} \in \{0, 1\}^n} f(\mathbf{x}) (-1)^{\mathbf{ax}},$$

míg az $\bar{f}$ Walsh-transzformáltja

$$\bar{F}(\mathbf{a}) = \sum_{\mathbf{x} \in \{0, 1\}^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{ax}}.$$

$F(\mathbf{a})$ és $\overline{F}(\mathbf{a})$ definíciójában a szummázást a szokásos módon értelmezzük, tehát nem *modulo* 2 összeadásként. Ennek következményeként $F(\mathbf{a})$ és $\overline{F}(\mathbf{a})$ értéke tetszőleges -2^n és 2^n közötti egész értéket vehet fel. Az $\{\overline{F}(\mathbf{a})\}$ egész értékekből álló 2^n elemű halmazt szokás a függvény Walsh-spektrumának nevezni. Az $\overline{F}(\mathbf{a})$ érték tulajdonképpen nem más, mint az f függvénynek az $\mathbf{a}\mathbf{x}$ lineáris függvénnyel mutatott korrelációja, amelyet szintén írhatunk egy skalárszorzat alakjába:

$$(\overline{f}(\mathbf{x})l_{\mathbf{a}}).$$

Az f függvényt maximálisan nemlineárisnak nevezzük*, ha minden $\mathbf{a} \in \{0, 1\}^n$ -re

$$\overline{F}(\mathbf{a}) = \sum_{\mathbf{x} \in \{0, 1\}^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{a}\mathbf{x}} = \pm 2^{\frac{n}{2}},$$

vagyis a függvény Walsh-spektruma azonos abszolút értékű elemekből áll.

Az f függvény nemlinearitásán az f függvénynek az affin függvények halmazától mért távolságát értjük, és N_f -el jelöljük:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{i=1, 2, \dots, 2^n} (\overline{f}(\mathbf{x})l_i).$$

A nemlinearitás legkisebb értéke 0, ez az affin függvények nemlinearitása. Bár a maximálisan nemlineáris függvények a nemlinearitást tekintve igen kedvező tulajdonságúak, mégsem használják ezeket kriptográfiai célra, mert egyéb tulajdonságaik nem megfelelőek. Ezek a függvények például nem kiegyensúlyozottak, és nem is tehetők azzá, nem korrelációimmunisak, csak páros dimenziójú térben léteznek stb.

Az $f : \{0, 1\}^n \rightarrow \{0, 1\}$ függvényt nagymértékben nemlineárisnak nevezzük, ha n páratlan, és az f függvény Walsh-spektrumában levő elemek csak 0 és $\pm C$ értékűek és az elemeknek pontosan a fele nem zérus. A kriptográfiai alkalmazásokban a nagymértékben nemlineáris függvényeket előnyben részesítik a maximálisan nemlineáris függvényekkel szemben, tekintettel arra, hogy egyéb tulajdonságaik is megfelelőek. Például kiegyensúlyozottak, vagy könnyen azzá tehetők, korreláció immunitásuk is jó stb. [3] alapján a nagymértékben nemlineáris függvényekből diszjunkt párokat képezhetünk, amely párok jellemző tulajdonsága, hogy a pár elemei egy adott lineáris függvénnyel sohasem mutatnak azonos abszolút értékű korrelációt. Pontosabban fogalmazva: g_1 és $g_2 : \{0, 1\}^n \rightarrow \{0, 1\}$ nagymértékben nemlineári függvények egy diszjunkt párt alkotnak, ha $(\overline{g}_1(\mathbf{x})l_i) = 0$ -ból következik $(\overline{g}_2(\mathbf{x})l_i) \neq 0$ illetve fordítva. Ilyen párok létezésére szükséges és elégséges feltétel, hogy

$$(\overline{g}_1(\mathbf{x})l_i)^2 + (\overline{g}_2(\mathbf{x})l_i)^2 = 2^{n+1}$$

*Az angol nyelvű irodalomban szokásos megnevezésük: Bent functions.

teljesül minden $i = 0, 1, \dots, 2^n - 1$ -re. Diszjunkt függvénypárok alapján további hasonló tulajdonságú függvénypárok szerkeszthetők az n -dimenziós lineáris függvények segítségével az alábbi módon:

$$\bar{h}_1(i) = \frac{(\bar{g}_1(\mathbf{x})l_i) + (\bar{g}_2(\mathbf{x})l_i)}{2^{n-m}}$$

és

$$\bar{h}_2(i) = \frac{(\bar{g}_1(\mathbf{x})l_i) - (\bar{g}_2(\mathbf{x})l_i)}{2^{n-m}}.$$

Az eredményként előálló $\bar{h}_1$ és $\bar{h}_2$ sorozat két függvény által generált $\{-1, 1\}$ sorozatnak tekinthető, és ez a két függvény kielégíti a

$$(\bar{h}_1(\mathbf{x})l_k)^2 + (\bar{h}_2(\mathbf{x})l_k)^2 = 2^{n+1}$$

feltételt minden $k = 0, 1, \dots, 2^n - 1$ -re.

Az előzőekben említett, nagymértékben nemlineáris függvénypárok mutatják meg a maximálisan nemlineáris és a nagymértékben nemlineáris függvények közötti szoros kapcsolatot. Páros n esetén az $f : \{0, 1\}^n \rightarrow \{0, 1\}$ függvény akkor és csak akkor maximálisan nemlineáris függvény, ha igazságtáblája előállítható két 1-gyel alacsonyabb változós diszjunkt nagymértékben nemlineáris függvénypár igazságtáblájának összefűzésével.

3. Nagymértékben nemlineáris függvények száma

A függvények számának megbecsüléséhez vizsgáljuk először a 3-dimenziós tereket. Ha egy függvénynek egy lineáris függvénnyel vett korrelációja zérus, akkor ez azt jelenti, hogy a függvény igazságtáblájában a függvényértékek fele megegyezik az adott lineáris függvény függvényértékeivel, a pontok másik fele viszont különbözik. Ha a függvény korrelációja egy lineáris függvénnyel 4 vagy -4 értékű, akkor ez azt jelenti, hogy a függvény igazságtáblájában 2 pontban a függvényérték megegyezik a lineáris függvény értékével, 2 pontban különbözik attól, és a maradék 4 pontban vagy megegyezik a lineáris függvénnyel, vagy különbözik attól. Tekintsük a 3-dimenziós tér lineáris függvényeit, és változtassuk meg egy lineáris függvény igazságtáblájában a megfelelő számú függvényértéket.

A háromdimenziós lineáris függvények igazságtáblái:

	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
0x	0	0	0	0	0	0	0	0
1x	0	1	0	1	0	1	0	1
2x	0	0	1	1	0	0	1	1
3x	0	1	1	0	0	1	1	0
4x	0	0	0	0	1	1	1	1
5x	0	1	0	1	1	0	1	0
6x	0	0	1	1	1	1	0	0
7x	0	1	1	0	1	0	0	1

Induljunk ki a legegyszerűbb igazságtáblából, amely a 0x lineáris függvényhez tartozik. A lehetséges módosítások:

1. két pont értékét megváltoztatjuk és hat pont változatlan,
2. hat pont értékét megváltoztatjuk és két pont változatlan,
3. négy pont értékét megváltoztatjuk, négy pont változatlan.

Az első két esetben a módosított függvények mindegyike nagymértékben nemlineáris függvény, a harmadik módszerrel lineáris függvényeket is előállítunk.

Eredeti lin.fgv.	Módosított függvény								Korreláció a lin.függv-ekkel							
	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	l_0	l_1	l_2	l_3	l_4	l_5	l_6	l_7
0x	1	1	0	0	0	0	0	0	4	0	-4	0	-4	0	-4	0
0x	1	0	1	0	0	0	0	0	4	-4	0	0	-4	-4	0	0
0x	1	0	0	1	0	0	0	0	4	0	0	-4	-4	0	0	-4
0x	1	0	0	0	1	0	0	0	4	-4	-4	-4	0	0	0	0
0x	1	0	0	0	0	1	0	0	4	0	-4	0	0	-4	0	-4
0x	1	0	0	0	0	0	1	0	4	-4	0	0	0	0	-4	-4
0x	1	0	0	0	0	0	0	1	4	0	0	-4	0	-4	-4	0
0x	0	1	1	0	0	0	0	0	4	0	0	4	-4	0	0	4
0x	0	0	1	1	1	1	1	1	-4	0	4	0	4	0	4	0
0x	0	1	0	1	1	1	1	1	-4	4	0	0	4	4	0	0
0x	0	1	1	0	1	1	1	1	-4	0	0	4	4	0	0	4
0x	0	1	1	1	0	1	1	1	-4	4	4	4	0	0	0	0
0x	0	1	1	1	1	0	1	1	-4	0	4	0	0	4	0	4
0x	0	1	1	1	1	1	0	1	-4	4	0	0	0	0	4	4
0x	0	1	1	1	1	1	1	0	-4	0	0	4	0	0	4	0
0x	1	0	0	1	1	1	1	1	-4	0	0	-4	4	0	0	-4
0x	0	0	0	0	1	1	1	1	0	0	0	0	8	0	0	0
0x	0	0	0	1	0	1	1	1	0	4	4	0	4	0	0	-4
0x	0	0	0	1	1	0	1	1	0	0	4	-4	4	4	0	0
0x	0	0	0	1	1	1	0	1	0	4	0	-4	4	0	4	0
0x	0	0	0	1	1	1	1	0	0	0	0	0	4	4	4	-4
0x	0	0	1	0	0	1	1	1	0	0	4	4	4	-4	0	0

Ha minden lineáris függvényre az összes lehetséges módosításokat elvégezzük, akkor minden lehetséges nagymértékben nemlineáris függvényt előállítunk, de egy-egy nagymértékben nemlineáris és lineáris függvényt többször is generálunk. Kiválogatva a különböző függvényeket, arra az eredményre jutunk hogy a 3-dimenziós térben a nagymértékben nemlineáris függvények száma 112. Tovább vizsgálódva azt látjuk, hogy ez a 112 függvény 14 függvénycsoportba sorolható úgy, hogy mindegyik csoportban a tagok azonos korrelációs tulajdonságokat mutatnak a lineáris függvényekkel, vagyis egy-egy csoport elemei ugyanazokkal a lineáris függvényekkel adják a nem zérus korrelációt. A 14 függvényhalmazból 7 párt képezhetünk. A függvényhalmaz párokra jellemző, hogy e halmazpár egyik eleméből vett függvény és a halmazpár másik eleméből vett függvény, nevezzük ezeket g_1 és g_2 -nek, kielégítik a

$$(\bar{g}_1(x)l_i)^2 + (\bar{g}_2(x)l_i)^2 = 2^{n+1}$$

feltételt. Vagyis nem találunk olyan nagymértékben nemlineáris függvényt, amelynek ne lenne párja a fenti értelemben.

Bemutatjuk az egyik függvényhalmaz-párt.

A függvényhalmaz-pár első tagja:

Eredeti lin.fgv.	Módosított függvény								Korreláció a lin.függv-ekkel							
	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	l_0	l_1	l_2	l_3	l_4	l_5	l_6	l_7
0x	0	0	1	1	1	1	1	1	-4	0	4	0	4	0	4	0
0x	1	1	0	0	1	1	1	1	-4	0	-4	0	4	0	-4	0
0x	1	1	1	1	0	0	1	1	-4	0	4	0	-4	0	-4	0
0x	1	1	1	1	1	1	0	0	-4	0	-4	0	-4	0	4	0
0x	1	1	0	0	0	0	0	0	4	0	-4	0	-4	0	-4	0
0x	0	0	1	1	0	0	0	0	4	0	4	0	-4	0	4	0
0x	0	0	0	0	1	1	0	0	4	0	-4	0	4	0	4	0
0x	0	0	0	0	0	0	1	1	4	0	4	0	4	0	-4	0

A függvényhalmaz-pár második tagja:

Eredeti lin.fgv.	Módosított függvény								Korreláció a lin.függv-ekkel							
	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	l_0	l_1	l_2	l_3	l_4	l_5	l_6	l_7
1x	0	1	1	0	1	0	1	0	0	-4	0	4	0	4	0	4
1x	1	0	0	1	1	0	1	0	0	-4	0	-4	0	4	0	-4
1x	1	0	1	0	0	1	1	0	0	-4	0	4	0	-4	0	-4
1x	1	0	1	0	1	0	0	1	0	-4	0	-4	0	-4	0	4
1x	1	0	0	1	0	1	0	1	0	4	0	-4	0	-4	0	-4
1x	0	1	1	0	0	1	0	1	0	4	0	4	0	-4	0	4
1x	0	1	0	1	1	0	0	1	0	4	0	-4	0	4	0	4
1x	0	1	0	1	0	1	1	0	0	4	0	4	0	4	0	-4

Mivel ezek a párok egyértelmű kapcsolatban vannak a maximálisan nemlineáris függvényekkel, megbecsülhetjük azok számát is. A 112 függvényből 448 függvény-párt képezhattünk, mindegyik függvénypárból 2 darab 1-el magasabb dimenziójú

maximálisan nemlineáris függvény szerkeszthető, így adódik, hogy a 4-dimenziós, maximálisan nemlineáris függvények száma 896.

Sajnos ezt a konstrukciót magasabb dimenzióban nem alkalmazhatjuk, mivel a lineáris függvények igazságtáblájában végrehajtott módosítások nem csak lineáris vagy nagymértékben nemlineáris függvényeket eredményeznek, hanem egyéb függvényeket is. A szabályosság, ami végül is elvezetne a nagymértékben nemlineáris függvényekhez nem látszik. A további becslési lehetőség érdekében tekintsünk egy példát [7]-ből. Legyen l_i a H_k Hadamard-mátrix i -edik sora. Az $l_0, l_1, \dots, l_{2^k-1}$ $\{-1, 1\}$ sorozatok az összes $\{0, 1\}^k$ -beli, 2^k darab lineáris függvény által generált $\{-1, 1\}$ sorozatok, amelyek mindegyike 2^k elemből áll. Belátható, hogy bármely 2^{k-1} darab, 2^k hosszúságú különböző lineáris függvény által generált $\{-1, 1\}$ sorozat összefűzése (konkatenálása) egy olyan $\{-1, 1\}$ sorozatot eredményez, amelynek generáló függvénye f a $\{0, 1\}^{2^{k-1}}$ téren értelmezett. Az így létrejött $\{-1, 1\}$ sorozathoz tartozó függvényre teljesül, hogy Walsh-transzformáltja a 0 vagy $\pm 2^k$ értéket veszi fel, és ezért nemlinearitása $N_f = 2^{2^{k-1}-1} - 2^{\frac{1}{2}(2^{k-1}-1)}$.

3.1. LEMMA. Jelölje l_i a 2^n -edrendű H_n , és L_j a 2^{2n-1} -edrendű H_{2n-1} Hadamard-mátrix sorait, ahol $i = 0, 1, 2, \dots, 2^n - 1$ és $j = 0, 1, 2, \dots, 2^{2n-1} - 1$. A $g_i : \{0, 1\}^n \rightarrow \{0, 1\}$ és a $G_j : \{0, 1\}^{2n-1} \rightarrow \{0, 1\}$ lineáris függvények $\{-1, 1\}$ sorozataik rendre megfelelnek az l_i és L_j soroknak, azaz $\bar{g}_i = l_i$ és $\bar{G}_j = L_j$ minden i -re és j -re. Az $f : \{0, 1\}^{2n-1} \rightarrow \{0, 1\}$ függvényhez tartozó $\bar{f}$ legyen olyan, amelyet 2^{n-1} darab különböző l_i összefűzésével állítottunk elő. Ekkor az f nagymértékben nemlineáris függvény azzal a G_j lineáris függvénnyel mutat nem zérus korrelációt, amelynek L_j sorát olyan l_i sor generálja, amely előfordul $\bar{f}$ -ban.

Bizonyítás. L_j a j -edik sor H_{2n-1} -ben. Vizsgáljuk meg, milyen komponensek alkotják. Induljunk ki H_n -ből, és tekintsük a rekurzív eljárást:

$$H_n \rightarrow H_{n+1} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix} \rightarrow \dots H_{2n-1} = \begin{bmatrix} H_{2n-2} & H_{2n-2} \\ H_{2n-2} & -H_{2n-2} \end{bmatrix}$$

$$H_n = \begin{bmatrix} l_0 \\ \vdots \\ l_{2^n-1} \end{bmatrix}, H_{2n-1} = \begin{bmatrix} L_0 \\ \vdots \\ L_{2^{2n-1}-1} \end{bmatrix}$$

Az első lépésben a H_{n+1} mátrixot generáljuk. Az eljárásban észrevehetjük, hogy a kiindulási mátrix sorai nem keverednek. Ez azt jelenti, hogy ha tekintjük a H_n mátrix egy l_i sorát, akkor az eljárásban l_i mellé csak l_i vagy $-l_i$ sor kerül. Folytatva az eljárást, H_{2n-1} -ről elmondhatjuk, hogy az L_j sor csak az l_p vagy $-l_p$ $p = j$ modulo 2^n sort tartalmazza H_n -ből. Ez azt jelenti, hogy az L_j sorozat felírható mint l_p vagy $-l_p$ valamilyen sorrendbeli konkatenáltja azaz $L_j = (m_1 l_p, m_2 l_p, \dots, m_{2^{n-1}} l_p)$ és $m_r \in \{-1, 1\}$ minden $r = 1, 2, \dots, 2^{n-1}$ -re. Az f függvényről pedig azt tudjuk, hogy $\bar{f}(x) = (l_{i_1}, l_{i_2}, \dots, l_{i_{2^{n-1}}}) \{i_1, i_2, \dots, i_{2^{n-1}}\} \subset$

$\{0, 1, \dots, 2^n - 1\}$ teljesül. A G_j lineáris függvény és az f korrelációja a két általuk generált $\{-1, 1\}$ sorozat skalárszorzatával számítható:

$$\bar{f}(\mathbf{x})L_j = \sum_{r=1}^{2^{n-1}} (l_{i_r}(l_p m_r)) = \sum_{r=1}^{2^{n-1}} (l_{i_r} l_p) m_r.$$

Az Hadamard-mátrixok tulajdonsága, hogy két sor skalárszorzata zérus, ha a két sor különböző, és 2^n , ha a két sor azonos. Ebből adódik, hogy $\bar{f}(\mathbf{x})L_j = 0$, ha $\bar{f}(\mathbf{x})$ nem tartalmazza azt az l_p sort, amelyik L_j -t generálja, és $\bar{f}(\mathbf{x})L_j = \pm 2^n$, ha l_p előfordul $\bar{f}(\mathbf{x})$ -ben. A H_{2n-1} -et generáló rekurzív eljárás alapján állíthatjuk, hogy egy adott l_p sor (2^{n-1}) -szer szerepel a mátrix sorai között, $\bar{f}(\mathbf{x})$ -et 2^{n-1} különböző sorból állítottuk elő, tehát pontosan $2^{n-1}2^{n-1} = 2^{2n-2} = 2^{(2n-1)-1}$ azon G_j lineáris függvények száma, amelyekkel az f korrelációja nem zérus. $\square$

3.2. TÉTEL. Az $f : \{0, 1\}^{2^{n-1}} \rightarrow \{0, 1\}$ nagymértékben nemlineáris függvények száma legalább

$$2^{2^{n-1}} \frac{(2^n)!}{(2^{n-1})!}.$$

Bizonyítás. A H_n mátrix 2^n sorából kell 2^{n-1} különbözőt kiválasztani. A lehetséges választások száma $\binom{2^n}{2^{n-1}}$. Mivel a negálás nem változtatja a korreláció abszolút értékét, ezért nem csak a kiválasztott sorokat, hanem azok negáltjait is fel lehet használni. Vigyázni kell azonban arra, hogy egy sorozatban nem szerepelhet együtt valamely sor a negáltjával. Ha így tekintjük a sorokat és azok negáltjait, akkor az elkészíthető sorozatok száma egy választásból a negáltakat is figyelembe véve:

$$\binom{2^{n-1}}{0} (2^{n-1})! + \binom{2^{n-1}}{1} (2^{n-1})! + \dots + \binom{2^{n-1}}{2^{n-1}} (2^{n-1})! = (2^{n-1})! 2^{2^{n-1}}.$$

Szorozzuk meg az egy választásból előállítható sorozatok számát a lehetséges választások számával:

$$\binom{2^n}{2^{n-1}} (2^{n-1})! 2^{2^{n-1}} = \frac{(2^n)! (2^{n-1})! 2^{2^{n-1}}}{((2^{n-1})!)^2} = 2^{2^{n-1}} \frac{(2^n)!}{(2^{n-1})!}. \quad \square$$

3.3. TÉTEL. Az $f : \{0, 1\}^{2^n} \rightarrow \{0, 1\}$ maximálisan nemlineáris függvények száma legalább:

$$\frac{(2^n)! 2^{2^n}}{(2^{n-1})!}.$$

Bizonyítás. Minden esetben, amikor kiválasztunk 2^{n-1} sort a H_n mátrixból, tulajdonképpen két halmazt képezünk a sorokból, mégpedig két diszjunkt halmazt, amelyeknek nincs közös eleme. A kiválasztott sorokhoz tartozó nagymértékben nemlineáris függvények korrelációja egy lineáris függvénnyel sohasem veszi

fel ugyanazt az abszolút értéket, mint a megmaradó sorokból képzett függvények korrelációja. Tekintsünk egy függvényt a kiválasztott sorokhoz tartozó függvényhalmazból, legyen ez $g_1 : \{0, 1\}^n \rightarrow \{0, 1\}$, és egy függvényt a meghagyott sorokhoz tartozó függvényekből, legyen ez $g_2 : \{0, 1\}^n \rightarrow \{0, 1\}$. Ekkor a két függvény kielégíti a

$$(\bar{g}_1(\mathbf{x})L_j)^2 + (\bar{g}_2(\mathbf{x})L_j)^2 = 2^{2n}$$

feltételt, vagyis alkalmasak 1-gyel magasabb dimenziós maximálisan nemlineáris függvények szerkesztésére. Mindkét függvényhalmaz elemeinek száma $(2^{n-1})!2^{2^{n-1}}$, és az ezekből készíthető függvénpárok száma $((2^{n-1})!2^{2^{n-1}})^2$. A

$$\bar{h}_1(i) = \frac{(\bar{g}_1(\mathbf{x})L_i) + (\bar{g}_2(\mathbf{x})L_i)}{2^n}$$

és

$$\bar{h}_2(i) = \frac{(\bar{g}_1(\mathbf{x})L_i) - (\bar{g}_2(\mathbf{x})L_i)}{2^n}$$

eljárással minden függvénpárhoz egy további párt készíthetünk, és ezzel az egy függvényhalmaz-párból készíthető függvénpárok száma: $2((2^{n-1})!2^{2^{n-1}})^2$. Egy függvénpárból 1 maximálisan nemlineáris függvény készíthető a $2n$ -dimenziós térben. A negált verziókkal külön nem kell törődni, hiszen a generált nagymértékben nemlineáris függvények negált alakját külön függvényként állítottuk elő. A H_n sorait $\binom{2^n}{2^{n-1}}$ féleképpen választhatjuk ki, tehát

$$\frac{\binom{2^n}{2^{n-1}}}{2}$$

darab függvényhalmaz-párt képezhetünk. Ezzel a szerkeszthető maximálisan nemlineáris függvények száma legalább:

$$\frac{(2^n!)2^{2^n}}{(2^{n-1})!}.$$

□

Összefoglalás

A dolgozatban bemutatott eredmény a páratlan dimenziós nagymértékben nemlineáris függvények és az 1-gyel magasabb dimenziós maximálisan nemlineáris függvények minimális számára ad alsó becslést.

Köszönetnyilvánítás. Köszönetemet szeretném kifejezni Dr. Nemetz Tibor Professzor úrnak, és Pásztorné Varga Katalin egyetemi docens asszonynak, akik értékes szakmai tanácsaikkal segítették munkámat.

Hivatkozások

- [1] Licskó, I., On Highly Nonlinear Functions, *Annales Univ. Sci. Budapest, Sect. Comp.*, **21** (2002), 165–175.
- [2] Licskó, I., Nagymértékben nemlineáris függvények vizsgálata, *Alkalmazott Matematikai Lapok*, **21** (2004), 3–22.
- [3] Licskó, I., Characteristics of Highly Nonlinear Functions, *Periodica Mathematica Hungarica*, Vol. **47** (1–2) (2003), 135–149.
- [4] Pásztor-Varga, K., Boole függvények Boole algebrájának strukturális tulajdonságait felhasználó Boole függvény optimalizációs módszer, *Alkalmazott Matematikai Lapok*, **13** (1987–88), 69–76.
- [5] Seberry, J., Zhang, X. M. and Zheng, Y., Nonlinearity and propagation characteristics of balanced Boolean functions, *Information and Computation*, **119**(1) (1995), 1–13.
- [6] Vajda, I., Buttyán, L., Szekeres, B., *Az algoritmikus adatvédelem módszerei*, Technical University of Budapest, nem publikált kézirat.
- [7] Zhang, X. M. and Zheng, Y., New lower bounds on Nonlinearity and class of highly nonlinear functions, in: *Information Security and Privacy*, Second Australian Conference Sidney, Australia, July 1997, Lecture Notes in Computer Science **1270**, 147–158, **1**(1), 1–13, Springer-Verlag (Berlin, Heidelberg, New York, 1997).

LICKÓ ILDIKÓ
 BUDAPESTI GAZDASÁGI FŐISKOLA
 KERESKEDELMI, VENDÉGLÁTÓIPARI ÉS IDEGENFORGALMI KAR
 INFORMATIKAI INTÉZET
 1054 BUDAPEST,
 V. ALKOTMÁNY UTCA 9–11
 e-mail: licsko_ildiko@t-online.hu

ESTIMATION FOR THE LOWER BOUND ON THE NUMBER OF HIGHLY NONLINEAR FUNCTIONS

ILDIKÓ LICKÓ

This study provides an estimation for the lower bound of the number of highly nonlinear n -dimensional functions if n is odd. The basis of the estimation is the relationship between highly nonlinear odd n -dimensional functions and bent functions in the $(n + 1)$ -dimension.