Distribution of Boolean Functions of 6 Variables According to the Frequency of Walsh Coefficients

Erdener Uyan, Ali Doğanaksoy

***Abstract*—This paper further investigates the problem of counting Boolean functions with specified number s of specified Walsh coefficients ω, discussed by Uyan et al. [?]. In that paper, the complete and exact counts for all s and ω values were presented for Boolean functions of up to 5 variables. Here, we extend these results to 6 variables by employing the idea of affine equivalence.**

***Index Terms*—Counting, Boolean functions, Walsh coefficients.**

I. Introduction

COUNTING Boolean functions meeting expected criteria has often taken a considerable amount of attention in cryptography mainly because of its importance in defining and bounding the search space for such functions. There are still open problems in literature that requires counting. Finding the number of bent functions or the number of maximum nonlinear balanced Boolean functions are such two problems. Solving these problems is hard primarily due to their computational complexity cost. When the number of variables increases, the size of the whole Boolean function set expands exponentially. In that case, a useful tool to analyze large function domains is affine equivalence classes.

On the other hand, finding relations among Walsh coefficients can help trivializing many questions concerning the main cryptographic features of Boolean functions such as nonlinearity, correlation immunity, resiliency or even algebraic immunity. Papers by Carlet et. al. [**?**], [**?**], and by Maitra and Pasalic [**?**] are some examples where such relations were studied. This work however tries to find such relations focusing on the frequencies of absolute values of Walsh coefficients.

The study in [**?**] focuses on obtaining general results to help counting n-variable Boolean functions with specified values in their Walsh spectrum. Exact and complete counts are listed only for $n \leq 5$, but for larger values of n, partial counts are given. For instance, the number of functions having $(2^n - 4)$ zeros in their Walsh spectrum is given to be $2\binom{2^n}{3}$. This work is dedicated to grouping the set of Boolean functions of 6 variables with respect to the quantity of their Walsh coefficients and giving exact and complete table of their cardinalities. Furthermore, we provide the number of functions for each level of nonlinearity, which was previously given in Fuller's Ph.D. thesis [**?**] as well.

E. Uyan is with the Institute of Applied Mathematics, METU, Ankara, TURKEY e-mail: uerdener@metu.edu.tr.

A. Doğanaksoy is with the Department of Mathematics, METU, Ankara, TURKEY e-mail: aldoks@metu.edu.tr.

II. Preliminaries

The mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called an n-variable Boolean function. The set of all n-variable Boolean functions $\mathcal{B}_n$ has 2^{2^n} elements. The primary representation of a Boolean function f is its *truth table*, the vector formed by 2^n $f(a)$ values evaluated at each $a \in \mathbb{F}_2^n$. Another representation of a Boolean function is its *Walsh spectrum*, the vector formed by 2^n $W_f(a)$ values evaluated at each $a \in \mathbb{F}_2^n$, where

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x}, a \in \mathbb{F}_2^n. \quad (1)$$

Equation (**??**) is called the Walsh-Hadamard transform. Each $W_f(a)$ is named a *Walsh coefficient*, which implies the correlation between f and a linear function $x \in \mathcal{B}_n$ at point $a \in \mathbb{F}_2^n$. Note that a Walsh spectrum represents a Boolean function uniquely just like its truth table.

A prominent cryptographic property of a Boolean function f is its nonlinearity, $nl(f)$, which is its minimum distance to the set of all n-variable linear functions. Nonlinearity is simply computed by means of the Walsh spectrum as follows.

$$nl(f) = 2^{n-1} - \frac{|W_f(a)_{max}|}{2} \quad (2)$$

Equation (2) implies that the absolute values of Walsh coefficients give enough information about nonlinearity. We therefore find the distribution of functions in $\mathcal{B}_6$ with respect to the absolute values of their Walsh coefficients.

III. Distribution of $\mathcal{B}_6$ with respect to Walsh coefficients

In this section, the framework and the algorithms to complete the distribution of 6-variable Boolean functions with respect to their Walsh Coefficients will be explained.

A. Framework and Derived Results

The following two definitions were introduced in [**?**].

- The set of Boolean functions f such that $\#\{\alpha \in \mathbb{F}_2^n | \, |W_f(\alpha)| = \omega\} = s$ is denoted by $\mathcal{S}(n, s, \omega)$, where n,s and ω are nonnegative integers with $n \geq 1$ and ω, $s \leq 2^n$.
- The chart whose (s, ω) entry contains the cardinality of $\mathcal{S}(n, s, \omega)$ is called the *function distribution table* of $\mathcal{B}_n$, denoted by FDT_n (e.g. Table **??** shows FDT_3).

FDT_n for $n \leq 5$ were provided completely in [**?**]. Since there are 2^{64} functions in $\mathcal{B}_6$, it is not feasible to do an exhaustive search to create the complete FDT_6. However,

TABLE I
FDT_3

$s \setminus \lvert\omega\rvert$	0	2	4	6	8
0	128	128	144	128	240
1	0	0	0	128	16
2	0	0	0	0	0
3	0	0	0	0	0
4	112	0	112	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	16	128	0	0	0
8	0	0	0	0	0

using Propositon 4.6 and 4.13 in [**?**], half of FDT_6, where $|\omega| \geq 32$, can easily be formed.

Proposition 1. ***(4.6 in [?])*** *Let $\omega = 2^n - 2k$ such that $k < 2^{n-2}$. Then, $|\mathcal{S}(n,1,\omega)| = 2^{n+1}\binom{2^n}{k}$ and $|\mathcal{S}(n,s,\omega)| = 0$ for all $s > 1$.*

TABLE II
FDT_6, $|\omega| > 32$ †

$\lvert\omega\rvert \setminus s$	**0**	**1**	**2**	**...**	2^n
34	18426325641727123456	20418431982428160	0	0	0
36	18440618544114823168	6125529594728448	0	0	0
38	18445062555781586944	1681517927964672	0	0	0
40	18446323694227560448	420379481991168	0	0	0
42	18446648893449478144	95180260073472	0	0	0
44	18446724685138055168	19388571496448	0	0	0
46	18446740548514734080	3525194817536	0	0	0
48	18446743507160384512	566549167104	0	0	0
50	18446743994193879040	79515672576	0	0	0
52	18446744064112832512	9596719104	0	0	0
54	18446744072733614080	975937536	0	0	0
56	18446744073628223488	81328128	0	0	0
58	18446744073704218624	5332992	0	0	0
60	18446744073709293568	258048	0	0	0
62	18446744073709543424	8192	0	0	0
64	18446744073709551488	128	0	0	0

† For readability, this is a transposed version of the conventional FDT_n seen in [**?**]

Note that the value 128 in the last row of Table **??** corresponds to the number of affine functions in $\mathcal{B}_n$

Proposition 2. ***(4.13 in [?])*** *Let $\omega = 2^{n-1}$. Then,*

1) $|\mathcal{S}(n,s,\omega)| = 0$ *for* $s = 3$ *and* $s \geq 5$
2) $|\mathcal{S}(n,4,\omega)| = 2\binom{2^n}{3}$
3) $|\mathcal{S}(n,2,\omega)| = \beta$
4) $|\mathcal{S}(n,1,\omega)| = \alpha$
5) $|\mathcal{S}(n,0,\omega)| = 2^{2^n} - [\alpha + \beta + 2\binom{2^n}{3}]$, *where*

$\alpha = \mu(\omega) - \left[2\beta + 4 \cdot 2\binom{2^n}{3}\right]$ *and*
$\beta = \left[\binom{2^{n+1}}{2} - 2^n\right]\binom{2^{n-1}}{2^{n-2}} - \binom{4}{3}2\binom{2^n}{3}$ *for* $n \geq 4$.

For the remaining values of FDT_6, we exploit previously known affine classification of $\mathcal{B}_6$. In the next section, a brief introduction on affine equivalence will be given.

B. Affine Equivalence Classes in $\mathcal{B}_6$

Two Boolean functions f and g are called *affine equivalent* if $f(x) = g(Ax+a) \oplus bx \oplus c$, where A is a nonsingular binary $n \times n$ matrix, $a, b \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$.

The set of affine equivalent functions is called an affine *equivalence class*. Many cryptographic features are preserved by affine equivalence such as algebraic degree, nonlinearity or more importantly, the absolute values of Walsh coefficients.

Proposition 3. ***([?]) For every two affine equivalent functions, the distribution of the absolute values of their Walsh spectrum is equal.***

In 1991, Maiorana [**?**] discovered 150.357 equivalence classes in $\mathcal{B}_6$. This classification was later confirmed by the works of Braeken et. al. [**?**], Fuller [**?**], and Langevin [**?**]. We used the data, specifically the representative and the cardinality of each class from [**?**] to create FDT_6 by means of the following algorithm.

Algorithm 1 Complete FDT_6 for $\omega < 32$

Input: $(f_1, c_1), (f_2, c_2), ..., (f_{150357}, c_{150357})$ ▷ Representatives and cardinalities of equivalence classes in $\mathcal{B}_6$
Output: FDT_6

```
ω ← 0
for s ← 0, 2^6 do                                   ▷ Initialize the table
    while ω ≤ 2^6 do
        FDT_6[s][ω] ← 0
        ω ← ω + 2
    end while
end for
for i ← 1, 150357 do                                ▷ Main loop
    WalshSpectrum_i ← abs(WHT(f_i))
    [U, C] ← Count_Unique(WalshSpectrum_i)†
    for j ← 1, length(U) do
        if U[j]<32 then
            FDT_6[C(j)][U(j)] ← FDT_6[C(j)][U(j)] + c_i
        end if
    end for
end for
return FDT_6
```

† ▷ Count_Unique is any procedure that can give unique elements and their respective counts from an input vector.

In order to simplify numbers obtained by this algorithm, we define the normalized versions of $|\mathcal{S}(n,s,\omega)|$ and FDT_n to be as follows.

- $|\overline{\mathcal{S}(n,s,\omega)}| = \frac{|\mathcal{S}(n,s,\omega)|}{2^{n+1}}$
- $\overline{FDT_n}$ is the *normalized function distribution table* of $\mathcal{B}_n$ such that its (s,ω) entry contains $|\overline{\mathcal{S}(n,s,\omega)}|$.

Note that, these definitions are appropriate since $bx \oplus c$ part

TABLE III
FDT_6, $|\omega| = 32$

$s \setminus \lvert\omega\rvert$	**32**
0	143626699006838909
1	488451200955648
2	37868060664
3	0
4	651
5	0
...	0
64	0

in the definition of affine equivalence contributes 2^{n+1} number of times for all functions in an equivalence class as $b \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$. In other words, all $|\mathcal{S}(n,s,\omega)|$ values must be divisible by the factor 2^{n+1}.

As an encyclopedic reference, the output of Algorithm **??** is given as $\overline{FDT_6}$ in Appendix **??**. In order to ease its readability and to cut the excess of zeros appearing when $17 \leq s \leq 64$ and $16 \leq \omega \leq 30$, the table is divided into two parts and shortened. One of the important values of this table is the one corresponding to $(s,\omega) = (64,8)$ entry of the table where 42.386.176, the number of 6-variable bent functions divided by 2^{6+1} is seen.

Using the same data and Algorithm **??**, a modified version of the Algorithm **??**, we were able to obtain a survey on the number of functions for each level of nonlinearity, which was also given in [**?**].

Algorithm 2 Number of functions for each nonlinearity in $\mathcal{B}_6$

Input: $(f_1,c_1),(f_2,c_2),...,(f_{150357},c_{150357})$ ▷ Representatives and cardinalities of eq. classes in $\mathcal{B}_6$
Output: Number of Functions per Nonlinearity

1: **for** $nl \leftarrow 0,26$ **do** ▷ Initializing the table
2: $f_{counts}[nl] \leftarrow 0$
3: **end for**
4: **for** $i \leftarrow 1,150357$ **do** ▷ Main loop
5: $WalshSpectrum_i \leftarrow abs(WHT(f_i))$
6: $W_{max} \leftarrow MAX(WalshSpectrum_i)*$
7: $nl = 2^{n-1} - \frac{W_{max}}{2}$
8: $f_{counts}[nl] \leftarrow f_{counts}[nl] + c_i$
9: **end for**
10: **return** f_{counts}

The output of Algorithm **??** is shown as Table **??**, which has been ordered from the highest nonlinearity level of 28 to the lowest 0 value. Note that, the counts below the nonlinearity 16 are equal to the values in $s = 1$ column of Table **??**. This is basically due to the fact that there is a single Walsh value in this part of FDT_n is maximal in the spectrum.

IV. Conclusion and Further Study

In this paper, we have presented the distribution of Boolean functions of 6 variables according to the frequency of Walsh coefficients by means of affine equivalence classes in $\mathcal{B}_6$. Previously, the exact distributions were given in [**?**] for functions with 5 or less variables. The idea of affine equivalence enabled us to lessen the number of functions to check in $\mathcal{B}_6$, from 2^{64} to only $150357 \approx 2^{17.2}$. We have presented two algorithms using the data of representatives and cardinalities of each class; one to complete the function distribution table and one to create the table showing the number of functions per nonlinearity.

FDT_7 can be studied for further analysis. However, according to Hou [**?**], there are about 2^{65} affine equivalence classes in $\mathcal{B}_7$. This makes the algorithms presented here inefficient. In order to find answers for the entries of FDT_7, more efficient algorithms should be found.

TABLE IV
Number of functions for each Nonlinearity

nl(f)	# f
28	5425430528
27	347227553792
26	1617838297055232
25	103868560519987200
24	1305039828998603264
23	3821934098435833856
22	5097726702198767616
21	4011570131804454912
20	2291582136636334080
19	1087405010755682304
18	458313050588725248
17	176395152249028608
16	62526600834171264
15	20418431982428160
14	6125529594728448
13	1681517927964672
12	420379481991168
11	95180260073472
10	19388571496448
9	3525194817536
8	566549167104
7	79515672576
6	9596719104
5	975937536
4	81328128
3	5332992
2	258048
1	8192
0	128

Acknowledgment

The authors would like to thank Zülfükar Saygı and Çağdaş Çalık for their valuable contributions and feedback.

References

[1] A. Braeken, Y. Borissov, S. Nikova, B. Preneel, Classification of boolean functions of 6 variables or less with respect to some cryptographic properties., Automata, Languages and Programming. Springer Berlin Heidelberg, 2005. 324-334.
[2] C. Carlet, D. K. Dalai, K. C. Gupta, S. Maitra, Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction, Information Theory, IEEE Transactions on 52 (7), pp. 3105–3121, 2006.
[3] C. Carlet, P. Sarkar, Spectral domain analysis of correlation immune and resilient Boolean functions, Finite Fields and Their Applications 8 (1) pp.120–130, 2002.
[4] J. Fuller, Analysis of affine equivalent Boolean functions for cryptography, Ph.D. Thesis, QUT, Australia, 2003.
[5] X. D. Hou, AGL (m, 2) acting on R (r, m)/R (s, m), Journal of Algebra 171.3, pp. 921-938, 1995.
[6] P. Langevin, Classification of Boolean functions under the affine group http://langevin.univ-tln.fr/project/agl/agl.html, 2009.
[7] J. Maiorana, A Classification of the Cosets of the Reed-Muller Code R(1,6). Mathematics of Computation 57 (195), pp. 403414, 1991.
[8] S. Maitra, E. Pasalic, Further constructions of resilient Boolean functions with very high nonlinearity., IEEE Transactions on Information Theory 48 (7) pp.1825–1834, 2002.
[9] B. Preneel, Analysis and Design of Cryptographic Hash Functions, Ph.D. Thesis, KU Leuven, Belgium, 1993.
[10] E. Uyan, Ç. Çalık, A. Doğanaksoy, "Counting Boolean functions with specified values in their Walsh spectrum", Journal of Computational and Applied Mathematics, ISSN 0377-0427, http://dx.doi.org/10.1016/j.cam.2013.06.035, 2013.

APPENDIX

TABLE A - $\overline{FDT_6}, |\omega| \leq 30$

$s \setminus \lvert\omega\rvert$	0	2	4	6	8	10	12	14
0	72621222574527744	72057602467610624	72620544008126464	72057622083079424	72622095976660224	72057689154119936	72625034638355584	72142467633545216
1	0	0	0	0	0	662473154560	24023638388736	747614794924032
2	10583322640	0	0	0	0	9130356619776	207318618759168	2995695843194880
3	1722169774080	0	0	279982080	0	44785297890816	719428478963712	7242174646990080
4	18251051857920	0	0	242534476800	2961685440	209499448052160	2188257251009760	11859982725648960
5	87944051220480	0	0	72571355136	91554140160	581080576462848	4396261821235200	13938338817220608
6	266917829165568	0	0	5049693798912	5278134677760	1547109348830976	7844919431271552	12540151435773696
7	769143475666944	0	0	1041773322240	118695723612480	2917542785935680	10411747357832352	9616702651727040
8	2138149299686400	0	0	46160060567040	6868914011366 40	5100761866346496	12066003006382080	6865856427064320
9	4252057890877440	0	0	22294693048320	3207474708480	6941532029071360	11379448548235264	4128919532236800
10	6105590049226752	3563462590464	5375655936	318935587815936	209504767128384	8710898218998528	9359218987896960	1648147202994432
11	8202945889861632	0	0	34485840764928 0	3289041327882240	8950279657439232	5771002952171520	3562930997821 44
12	11169686287323648	17618712330240	173133918720	1147171079476800	13059723162336144	9129127308123648	4124139956982528	31220241776640
13	11950669988167680	13439139840 0	0	1634668654510080	13074183198720	7456265936437248	1301540936048640	1612696780800
14	9472893446016000	10751311872000	11087290368000	3155879210803200	72426209050944 0	6917940343480320	962121643130880	22855680
15	6560061945163776	28670164992	260859303936	3799950102336192	9483549226012848	4811912521887744	312211255867392	10303340544
16	4761952300046592	590073040908288	286056593956224	59661067007324 16	29265523912590336	3886013057246208	113765111566848	0
17	3019781441617920	0	8090362183680	64173068660736 00	4959042600960	2320173419397120	4676820664320	0
18	1421987940696960	2137171158958080	2903602090072320	7885495224337920	302041308119040	1434637361332224	207628438929408	0
19	487272272578560	2167009782497280	120229064847360	6729634715811840	3691807869173760	674302121902080	53756559360	0
20	184216244655744	1362013145579520	12934924056375552	9404376692368896	9531988828669440	296361927622656	107513118720	0
21	117198498816000	6934460358131712	676423606118400	5145082754961408	290808053760	87344169615360	84978881003520	0
22	24292389687552	5486797902458880	24611185665803520	6930253495388160	15474924541440	27830050762752	5375655936	0
23	456630773776000	4270958641152000	1421993706577920	4389266748948480	177256654848000	1451427102720	0	0
24	128100272307840	15327122841354240	19624795765182720	3093122840801280	394568875975680	854505308160	11293655826432	0
25	7570715443200	3923109128945664	1071088413954048	2437301570715648	385255342080	0	0	0
26	99314340475392	8882293960802304	6217932249865728	1516734154801152	8648086487040	0	0	0
27	73120261559296	8271606505078784	250634358374400	724202892492800	50166815784960	0	0	0
28	17335115481600	2729334178099200	753267543104160	618725559029760	72125261493376	2712715264	0	0
29	50189027696640	4319361943142400	7310892072960	145874343444480	684556185600	0	0	0
30	29400528995712	3071917184716800	31322467233792	134730475364352	17263717801344	0	0	0
31	8641366917120	754841031081984	2016	19061180006400	99358640640000	0	0	0
32	16938738915840	1395015149316096	1310636113920	18082642636800	128254086213120	0	0	0
33	1338081024000	117579781079040	0	2153622159360	197107384320	0	0	0
34	2711626444800	218435229250560	0	2814379868160	7552796590080	0	0	0
35	151222321152	11670581035008	0	525278380032	45617816272896	0	0	0
36	46625911584 0	39555770268672	0	302853505024	53903749939200	0	0	0
37	5879623680	1633975418880	0	80634839040	24078458880	0	0	0
38	142153901568	10712646346752	0	0	2019230760960	0	0	0
39	16297290240	1359966289920	0	0	13923508838400	0	0	0
40	16825173120	1207842693120	11293655826432	0	15514367016960	0	0	0
41	1959874560	138871111680	0	0	0	0	0	0
42	840133728	57568315392	84978881003520	5119672320	0	0	0	0
43	209986560	13439139840	0	0	0	0	0	0
44	142178400	9099417600	191545260318720	0	0	0	0	0
45	0	10665984	10695763427328	597295104	0	0	0	0
46	3749760	10543325184	1606894058864 64	0	6089610240	0	0	0
47	0	0	25688915804160	0	1007935488 00	0	0	0
48	241950660	15484842240	51895751792640	0	111866840064	0	0	0
49	0	1142784000	16050995527680	0	0	0	0	0
50	0	0	6288285523968	0	0	0	0	0
51	17498880	1119928320	3226793472000	0	0	0	0	0
52	0	0	376225920000	0	0	0	0	0
53	0	0	179188531200	0	0	0	0	0
54	546840	34997760	34430018560	0	0	0	0	0
55	0	0	5711634432	0	0	0	0	0
56	11160	714240	281981952	0	0	0	0	0
57	0	0	279982080	0	0	0	0	0
58	0	0	104993280	0	0	0	0	0
59	0	0	0	0	0	0	0	0
60	651	41664	4999680	0	0	0	0	0
61	0	0	0	0	0	0	0	0
62	0	0	0	0	0	0	0	0
63	1	64	0	0	0	0	0	0
64	0	0	0	0	42386176	0	0	0

$s \setminus \lvert\omega\rvert$	16	18	20	22	24	26	28	30
0	736401371888883852	78376899729410752	91801043670119456	110117258751722048	125833798480977392	135582604969668032	140532277216848224	142737029667930944
1	5240629419250176	18947976160909824	29921358592984320	27393590186016768	16966291037375232	8345818667585280	3564137512349568	1376946651273984
2	12560023422051840	22835525169348864	17361660563856000	6108505058154240	1292022710254080	186233857770240	18768803969664	1211745943296
3	17917219124686560	15589394844663360	4453518280108128	485968528731840	22914064812240	530580832320	4500024480	10707648
4	16964459254387680	6659042781484800	546544843474560	98370478886 40	161782145280	0	42663936	0
5	10864229316820992	1545493802065920	30350253459456	28222193664	0	0	0	0
6	4861454914971648	155468441216256	699893953920	281148672	291648	0	0	0
7	1513645200518040	5332394704896	11945902080	0	0	0	0	0
8	418173220747800	53756559360	31997952	0	0	0	0	0
9	104723252838400	995491840	0	0	0	0	0	0
10	30139398955008	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	354120459840	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	241284036	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
...	0	0	0	0	0	0	0	0
64	0	0	0	0	0	0	0	0