RZ 3018 (# 93064) 04/20/98
Computer Science/Mathematics 17 pages

Research Report

Asymptotic Bounds on Differential Probabilities

Philip Hawkes

Department of Mathematics
University of Queensland
Australia

Luke O'Connor

IBM Research Division
Zurich Research Laboratory
8803 Rüschlikon
Switzerland

Asymptotic Bounds on Differential Probabilities

Philip Hawkes

Department of Mathematics, University of Queensland, Australia

Luke O'Connor

IBM Research Division, Zurich Research Laboratory, 8803 Rüschlikon, Switzerland

Abstract

Let $\mathrm{Pr}_{\otimes,\pi}(\alpha \to \beta)$ be the probability of a differential approximation to the n-bit permutation π, determined with respect to the group $(Z_2^n, \otimes)$. The probability is determined from the difference table $T_{\otimes,\pi}$ for which $T_{\otimes,\pi}(\alpha,\beta) = 2^n \cdot \mathrm{Pr}_{\otimes,\pi}(\alpha \to \beta)$. We show that the distribution of $T_{\otimes,\pi}(\alpha,\beta)$ asymptotically follows a Poisson distribution. Let $M_{\otimes,\pi} = \max_{\alpha,\beta \neq I} T_{\otimes,\pi}(\alpha\beta)$ where I is the identity of $(Z_2^n, \otimes)$, and define $B_n = \ln N^2 / \ln \ln N^2$ where $N = (2^n - 1)$. Our main results are to show that with high probability for a random permutation π, $\Pr(2B_n \le M_{\otimes,\pi} < 2n) \sim 1, \otimes = \oplus$, and $\Pr(M_{\otimes,\pi} < 2B_n) \sim 1, \otimes \in \{\boxplus, \odot\}$, where $\boxplus$ and $\odot$ denote modular addition and modular multiplication. Thus XOR differences admit higher probability approximations for random permutations than differences with respect to $\boxplus$ and $\odot$. Further, with high probability, the best differential probability for a random 64-bit permutation with respect to XOR differences lies in the interval $[2^{-58.6}, 2^{-57}]$.

1 Introduction

Differential approximations are the basis of differential cryptanalysis (DC) [2, 7], a well-known chosen-plaintext attack. The success of DC depends primarily on the probability of the differential approximation(s) used in the attack. The basis of this paper is a study of the distribution of probabilities for differential approximations to n-bit permutations, with particular emphasis on bounding on the maximum probability of an approximation.

Differential approximations are defined with respect to an Abelian group operation $(Z_2^n, \otimes)$, with the *difference* of two group elements X, X^* defined as $\Delta(X, X^*) = X \otimes (X^*)^{-1}$, also denoted ΔX. A *differential approximation* predicts a propagation of differences $\Delta X = \alpha \to \Delta Y = \beta$ from the input X to the output Y of an operation (for example, a permutation). For an n-bit permutation π, we denote the probability of the differential approximation $\Delta X = \alpha \to \Delta\pi(X) = \beta$ by $\Pr_{\otimes,\pi}(\alpha \to \beta)$. The choice of operation used to define differences is typically defined by the group operations(s) used to combine the key into the cipher. Consequently, we consider differences defined with respect to three groups commonly used in block cipher design: $(Z_2^n, \oplus)$, bitwise exclusive-OR (XOR); $(Z_2^n, \boxplus)$, modular addition; and $(Z_2^n, \odot)$, multiplication modulo (2^n+1) where 2^n+1 is prime and $0\ldots0 \equiv 2^n$. Our investigation is motivated by the results of experiments on uniformly selected n-bit permutations, $4 \le n \le 8$, shown in Table 1. Observe that approximations with respect to XOR differences yield higher probabilities with respect to the other differences. While this phenomenon is quite likely to be known by many researchers[1], this is the first paper which analyses it mathematically. In summary, we determine an asymptotic approximation to the distribution of $\Pr_{\otimes,\pi}(\alpha \to \beta)$, obtain bounds on maximum probabilities for approximations with respect to the three group operations, and from these bounds conclude that with high probability that XOR differences yield higher the probability approximations to an n-bit permutation than differences with respect to $\boxplus$ and $\odot$. The similarities for the group operations $\boxplus$ and $\odot$ are accounted for by the fact that their respective groups are isomorphic.

n	4	5	6	7	8
av. max. $\boxplus$	0.2771	0.1617	0.0919	0.0515	0.0284
av. max. $\odot$	0.2764	-	-	-	0.0283
av. max. $\oplus$	0.4186	0.2487	0.1426	0.0806	0.0443

Table 1: The average maximum probability for differential approximations to uniformly selected n-bit permutations, $4 \le n \le 8$, where differences are defined with respect to $\boxplus$, $\odot$ and $\oplus$ respectively. Note that differences with respect to $\odot$ are only defined for n when $2^n + 1$ is prime.

The probability of the best differential approximation can vary greatly according to the group operations used to define the differences. For example, the S-box $S(x) = 45^x \bmod 257$ used in SAFER K-64 [9] admits approximations of probability 1/2 for $\oplus$, while the approximations with respect to $\boxplus$ and $\odot$ are significantly lower. To reduce the probability of approximations to these S-boxes, distinct group operations are used to combine subkeys into the cipher before and after the S-boxes. In particular, SAFER K-64 uses the $\oplus$ and $\boxplus$ operations or vice versa. To analyze the resulting structure, approximations were proposed which use distinct group operations when defining input and output differences. These mixed approximations are known as *quasi-differentials* [10].

The probability of a differential approximation to a fixed mapping is determined from the difference table. Let $(Z_2^n, \otimes)$ be an Abelian group of order 2^n with identity element I, and let $N = (2^n - 1)$. The *difference table* for the n-bit permutation π with respect to $\otimes$ is the $N \times N$ table where, for $\alpha, \beta \in Z_2^n \setminus \{I\}$,

$$T_{\otimes,\pi}(\alpha, \beta) = |\{(X, X^*) : \Delta(X, X^*) = \alpha, \ \Delta(\pi(X), \pi(X^*)) = \beta\}|, \quad (1)$$

[1]For example, this observation was stated by M. Dichtl during a seminar presented at Isaac Newton Institute, 1996.

and differences Δ are defined with respect to $\otimes$. We note that $\Pr_{\otimes,\pi}(\alpha \to \beta) = 2^{-n} \cdot T_{\otimes,\pi}(\alpha, \beta)$. The relevant quantity for DC is the maximum difference table entry $M_{\otimes,\pi} = \max_{\alpha,\beta \neq I} T_{\otimes,\pi}(\alpha,\beta)$. For example, the column for $n = 8$ of Table 1 indicates that the difference tables for 8-bit mappings with respect to $\otimes \in \{\odot, \boxplus\}$ yielded a average maximum table entry between 7 and 8, while the average maximum XOR entry was between 10 and 12. The value 10 appears to be a critical value separating the maximum table entries with respect to $\boxplus$ and $\odot$ from the maximum table entries with respect to $\oplus$.

Our investigation proceeds as follows. First we reduce the problem of enumerating $T_{\otimes,\pi}(\alpha,\beta)$ to a counting problem on graphs. This reveals that the distribution of values for $T_{\otimes,\pi}(\alpha,\beta)$ over the n-bit permutations π depends only on n and the orders of α and β with respect to $\otimes$. This counting problem is combined with the inclusion-exclusion principle to obtain the distribution of probabilities for a differential approximation. Furthermore, we show that if π is a uniformly selected n-bit permutation, then

$$\begin{array}{rcll} \Pr\left(T_{\otimes,\pi}(\alpha,\beta) = 2t\right) & \sim & e^{-\frac{1}{2}} \cdot \frac{1}{2}^t/t! & \text{if ord } \alpha = \text{ord } \beta = 2, \\ \Pr\left(T_{\otimes,\pi}(\alpha,\beta) = t\right) & \sim & e^{-1}/t! & \text{otherwise,} \end{array}$$

uniformly for $0 \leq t \leq \frac{2^{n/2}}{2\ln(\ln n)}$, as $n \to \infty$. These distributions asymptotically follow the Poisson distribution $\Pr[X = t] = e^{-\mu} \cdot \mu^t/t!$, with $\mu = \frac{1}{2}$ if ord α = ord $\beta = 2$ and with $\mu = 1$ otherwise. Consequently, we call these asymptotic approximations the *Poisson approximation (PA)* to the distribution of entries for $T_{\otimes,\pi}(\alpha,\beta)$. As the results of the PA are dependent on the order of the input and output differences and not on the group itself, the PA also applies to quasi-differentials.

Note that all elements of $(Z_2^n - \{0\}, \oplus)$ have order 2, while almost all elements of $(Z_2^n - \{I\}, \otimes)$, $\otimes \in \{\boxplus, \odot\}$, have order greater than 2. ¿From these asymptotic distributions for $T_{\otimes,\pi}(\alpha,\beta)$ and the distribution of elements in the corresponding groups, we determine asymptotic approximations to the distribution of values in difference tables with respect to $\oplus$, $\boxplus$ and $\odot$. We also determine the variance in the number of entries of size $2t$ in difference tables with respect to $\oplus$. ¿From these asymptotic results we derive the following two bounds for uniformly selected π.[2] If B_n is defined as $B_n = \ln N^2/\ln\ln N^2$ where $N = (2^n - 1)$, then

$$\begin{array}{rcll} \Pr\left(2B_n \leq M_{\otimes,\pi} < 2n\right) & \sim & 1, & \otimes = \oplus \\ \Pr\left(M_{\otimes,\pi} < 2B_n\right) & \sim & 1, & \otimes \in \{\boxplus, \odot\}. \end{array}$$

Equivalently, the fraction of n-bit permutations that do not satisfy these bounds tends to 0 as n increases. Some relevant values of B_n are given in Table 2. For example, if $n = 8$,then with high probability the maximum XOR entry is between $2 \cdot \lceil B_8 \rceil = 10$ and $2 \cdot 8 = 16$, while the maximum entry with respect to modular addition and modular multiplication is less than $2 \cdot \lceil B_8 \rceil = 10$. This agrees with our experiment results for $n = 8$. We conclude that for all but a decreasing fraction of permutations, $\oplus$ differences yield higher probability differential approximations when compared to $\boxplus$ and $\odot$ differences. Similar bounds on the maximum table entry can be obtained for differential approximations for other group operations, and likewise for quasi-differentials. The dominant factor in bounding the maximum entry is the fraction of entries for which the orders of α and β is two with respect to the appropriate group operation(s).

The success of DC depends on the average of the probabilities for the differential approximation $\Delta P \to \Delta C_{R-1}$ over all the keys, which is known as the *average-key probability*. If a differential approximation has an average-key probability p_Δ, then the data complexity for DC using this approximation is inversely proportional to $p_\Delta - 1/N$. Our bounds show that with high probability, the best differential probability for a random 64-bit permutation with respect to XOR differences lies in the interval $[2^{-58.6}, 2^{-57}]$. It follows that average-key probabilities should lie well below 2^{-57}. However, block ciphers often have a iterative structure which allows for differential approximations with higher probabilities than expected for a random permutation. For example, the 13-round differential

[2] The upper bound on $M_{\oplus,\pi}$ was determined by [11].

n	8	16	32	64	128	256	512	1024
B_n	4.6	7.2	11.7	20.8	34.3	60.4	108.1	195.6
$2 \cdot \lceil B_n \rceil$	10	16	24	42	70	122	218	392

Table 2: The values of $B_n = \ln N^2 / \ln\ln N^2$, $N = (2^n - 1)$ for several n.

approximation used by Biham and Shamir for DC of the Data Encryption Standard (DES) [12, 3] has an average-key probability of more than $2^{-47.2}$. The corresponding data complexity is less than $2^{-9.8} \approx 1.1 \times 10^{-3}$ times the data complexity predicted above. We suggest that block cipher proposals ensure that all average-key probabilities are below 2^{-57}. More rounds can be added to iterated ciphers to decrease average-key probabilities. However, the reduction in the speed of the cipher will also have to be considered.

2 An Equivalent Graph Theory Problem

We let $\Pi^{(n)}$ denote the set of n-bit permutations, and write $\pi \in_R \Pi^{(n)}$ to denote a uniformly selected n-bit permutation. The problem of determining the distribution of entries for $T_{\otimes,\pi}$ can be considered as an enumeration problem: count the number of edge-preserving mappings between two appropriately defined directed graphs, given below. Recall that the set of n-bit blocks is denoted Z_2^n and can represented by the set $\{0, 1, \ldots, 2^n - 1\}$.

Definition 1 For a group $(Z_2^n, \otimes)$ of order 2^n and a non-trivial (non-identity) difference $\alpha \in Z_2^n$ there is an associated directed graph $D_\alpha = (V, E_\alpha)$, $|V| = 2^n$, where each vertex $v \in V$ has a unique label $l(v) \in Z_2^n$ and $E_\alpha = \{(u, v) \mid l(u) \otimes (l(v))^{-1} = \alpha\}$. The *directed edges* or *arcs* of D_α represent the ordered pairs (X, X^*) for which $\Delta(X, X^*) = \alpha$. We will call D_α the *difference graph* of α with respect to $\otimes$. □

As a result of the group property, every vertex of D_α and D_β has indegree and outdegree one. Consequently, the arcs of D_α and D_β form cycles.[3]

Corollary 1 The directed graph D_α consists of $\frac{2^n}{\operatorname{ord}\alpha}$ labeled disjoint cycles of length ord α. □

Let $D_\alpha = (V, E_\alpha)$ and $D_\beta = (V, E_\beta)$ be the difference directed graphs representing any two differences $\alpha, \beta \in Z_2^n$. For a permutation $\pi \in \Pi^{(n)}$ we define

$$d_{\otimes,\pi}(D_\alpha, D_\beta) \quad = \quad |\{(u, v) \in E_\alpha \mid (u^*, v^*) \in E_\beta,\ l(u^*) = \pi(l(u)), l(v^*) = \pi(l(v))\}|\,.$$

If $d_{\otimes,\pi}(D_\alpha, D_\beta) = t$, then π is said to *map t arcs of D_α onto D_β*. Now, $d_{\otimes,\pi}(D_\alpha, D_\beta)$ is the number of arcs from D_α mapped to arcs of D_β by π, or alternatively, $d_{\otimes,\pi}(D_\alpha, D_\beta)$ is the number of pairs (X, X^*) such that $\Delta(X, X^*) = \alpha$ and $\Delta(\pi(X), \pi(X^*)) = \beta$. Thus, the entries of a difference table for π with respect to $\otimes$ can be considered as the number of arcs preserved from a mapping between two difference graphs.

Lemma 1 For all non-trivial differences $\alpha, \beta \in Z_2^n$ and $\pi \in \Pi^{(n)}$, $T_{\otimes,\pi}(\alpha, \beta) = d_{\otimes,\pi}(D_\alpha, D_\beta)$. □

Example 1 Consider $(Z_2^3, \boxplus)$, the group of addition modulo 8. The directed graphs D_1, D_2 representing the differences $\Delta(X, X^*) = 1$ and $\Delta(X, X^*) = 2$ are shown in Figure 1. Notice that the arcs of D_1 and D_2 form cycles of length 8 and 4 respectively, as ord $1 = 8$ and ord $2 = 4$ with respect to $\boxplus$. Let $\pi \in \Pi^{(3)}$ be the permutation $(3, 0, 7, 1, 2, 5, 4, 6)$. Then the only arcs of D_1 mapped by π to arcs of D_2 are the arcs labeled by $(3, 2)$ and $(7, 6)$ of D_1 which are mapped to the arcs labeled by $(1, 7)$ and $(6, 4)$ respectively of D_2. Consequently $T_{\boxplus,\pi}(1, 2) = d_{\boxplus,\pi}(D_1, D_2) = 2$. □

[3] A cycle is usually assumed to have length greater than three, but in this paper it is useful to extend the definition to include cycles of length two. A cycle of length two on the vertices $\{v_0, v_1\}$ consists of the arcs $\{(v_0, v_1), (v_1, v_0)\}$, and is also considered as an *undirected edge*.

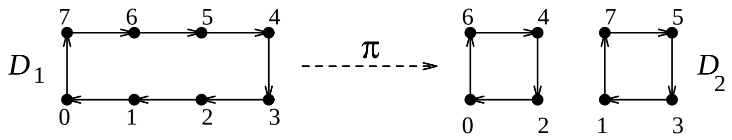

Figure 1: The directed graphs D_1 and D_2 representing the two differences $\Delta(X, X^*) = 1$ and $\Delta(X, X^*) = 2$ using the 3-bit $\boxplus$ operation to define the differences.

From Corollary 1, the structure of D_α and D_β depends only on the orders of α and β, and the order of the group, that is, 2^n. If ord $\alpha =$ ord $\beta = a$, then both D_α and D_β are comprised of disjoint cycles of length a, and thus D_α is isomorphic to D_β. Consequently, the distribution of values for $d_{\otimes,\pi}(D_\alpha, D_\beta)$ over $\pi \in \Pi^{(n)}$ depends only on the orders of α, β and 2^n. That is, if ord $\alpha =$ ord γ and ord $\beta =$ ord δ, then $\Pr(d_{\otimes,\pi_1}(D_\alpha, D_\beta) = t) = \Pr(d_{\otimes,\pi_2}(D_\gamma, D_\delta) = t)$ for each t, $0 \le t \le 2^n$, when $\pi_1, \pi_2 \in_R \Pi^{(n)}$ are independent. We may then make the following definition.

Definition 2 Let $(Z_2^n, \otimes)$ be an Abelian group of order 2^n. For $a = 2^r$, $b = 2^s$, $1 \le r \le n$, $1 \le s \le n$, and $0 \le t \le 2^n$, define

$$p_t(2^n, a, b) \stackrel{\text{def}}{=} \Pr\left(d_{\otimes,\pi}(D_\alpha, D_\beta) = t \mid \pi \in_R \Pi^{(n)}\right),$$

where $\alpha, \beta \in Z_2^n$ are any elements such that ord $\alpha = a$ and ord $\beta = b$. Note: $p_t(2^n, a, b) = p_t(2^t, b, a)$. □

Now, the expected distribution of values in $T_{\otimes,\pi}$ depends only the distribution of (element) orders in $(Z_2^n, \otimes)$. In the group $(Z_2^n, \oplus)$, all the nonzero elements have order 2, and the resulting directed graphs D_α consist of 2^{n-1} cycles of length 2. However, in the group $(Z_2^n, \boxplus)$ there are 2^{a-1} elements of order 2^a, $1 \le a \le n$, and the identity (0) has order one. For $2^n + 1$ prime, the groups $(Z_2^n, \odot)$ and $(Z_2^n, \boxplus)$ are isomorphic, and thus have the same distribution of orders.

Corollary 2 Let $\otimes \in \{\boxplus, \odot\}$. Then there are 2^{2a-2} entries in $T_{\otimes,\pi}(\alpha, \beta)$ for which ord $\alpha =$ ord $\beta = 2^a$, $1 \le a \le n$, and 2^{a+b-1} entries for which $\{\text{ord } \alpha, \text{ord } \beta\} = \{2^a, 2^b\}$, $1 \le a < b \le n$. □

To obtain the expected distribution of entries in a difference table for $\otimes \in \{\oplus, \boxplus, \odot\}$, we need only determine $p_t(2^n, a, b)$ for $a = 2^r$, $b = 2^s$, $1 \le r \le n$, $1 \le s \le n$, and $0 \le t \le 2^n$, and apply Corollary 2. We now cast this enumeration problem in terms of the *inclusion-exclusion principle (IEP)* (see for example Hall [6]).

Let α and β be elements of $(Z_2^n, \otimes)$, and let $D_\alpha = (V, E_\alpha)$ and $D_\beta = (V, E_\beta)$ be their respective (difference) graphs. For each edge $uv \in E_\alpha$ define A_{uv} as $A_{uv} = \left\{\pi \in \Pi^{(n)} \mid (\pi(u), \pi(v)) \in E_\beta\right\}$, which is the set of permutations π that preserve the edge uv of D_α in D_β. Then, by the inclusion-exclusion principle, the number of permutations π that preserve exactly t edges from D_α in D_β is

$$P_t = \sum_{i=0}^{j-t} (-1)^i \binom{t+i}{i} S_{t+i}, \qquad S_k = \sum_{\substack{\mathcal{Y} \subseteq E_\alpha \\ |\mathcal{Y}| = k}} \left| \bigcap_{uv \in \mathcal{Y}} A_{uv} \right|, \tag{2}$$

and it follows that $p_t(2^n, a, b) = P_t/(2^n!)$. In the case of XOR differences ($\otimes = \oplus$) it is known [11] that

$$P_{2t} \sim \binom{2^{n-1}}{t}^2 \cdot 2^t \cdot t! \cdot \frac{(2^{n-1} - t)!}{e^{1/2}}. \tag{3}$$

In this case determining an exact expression for P_t is assisted by the fact that ord $\alpha =$ ord $\beta = 2$, and the sets A_{uv} are 'independent' in the sense that uv is the only edge incident on u and v. For a general group operation $\otimes \neq \oplus$, most groups elements α will have ord $\alpha > 2$, and hence induce a difference graph for which there exist sets $A_{u_1v_1}, A_{u_2,v_2}$ and $u_1 = u_2$. Dependence between the A_{uv} sets considerably complicates the expressions for P_t, as we show next for $p_t(2^n, 2, 4)$ and $p_t(2^n, 4, 4)$.

Lemma 2 For $n \geq 2$, $p_t(2^n, 2, 4) = p_t(2^n, 4, 2) = \sum_{i=0}^{2^{n-1}-t}(-1)^k\binom{t+i}{i}S_{t+i}^{(n)}(2, 4)$ for $0 \leq t \leq 2^{n-1}$, and $p_t(2^n, 4, 4) = \sum_{i=0}^{2^n-t}(-1)^k\binom{t+i}{i}S_{t+i}^{(n)}(4, 4)$ for $0 \leq t \leq 2^n$, where

$$S_k^{(n)}(2,4) =$$
$$\left(\sum_{j=\lceil\frac{k}{2}\rceil}^{\min(k,2^{n-2})}\binom{2^n-4}{j}\cdot\binom{j}{k-j}\cdot 2^{3j}\right)\cdot\binom{2^{n-1}}{k}\cdot k!\cdot(2^n-2k)!,\qquad 0\leq k\leq 2^{n-1}, \tag{4}$$
$$S_k^{(n)}(4,4) =$$
$$\sum_{\substack{\chi=(f,g,h,i)\\ e(\chi)=k}}\left(\sum_{j=\lceil\frac{f}{2}\rceil}^{\min(f,k*)}\binom{k^*}{j}\cdot\binom{j}{f-j}\cdot 2^{3j}\right)^2\cdot\binom{2^{n-4}}{k*}^2\cdot\frac{4^z\cdot(k^*!)^2\cdot f!}{g!\cdot h!\cdot i!}\cdot(2^n-p(\chi))!,$$

for $0 \leq k \leq 2^n$, where $k^* = 2^{n-2} - (g+h+i)$, $p(\chi) = 2f + 3g + 4h + 4i$, $z = f + 2g + 2h - i$, and $\left\lceil\frac{f}{2}\right\rceil + g + h + i \leq 2^{n-2}$. For $2^{n-1}+1 \leq t \leq 2^n$, $p_t(2^n, 2, 4) = 0$.

Proof. Apply the definition of S_k in (2) directly. $\square$

For general $a, b > 4$ the expression for $S_k = S_k^{(n)}(a, b)$ becomes increasing difficult to determine exactly, and we therefore consider an asymptotic approximation. We denote $\pi(\mathcal{Y}) = \{(u^*, v^*) \mid l(u^*) = \pi(l(u)), l(v^*) = \pi(l(v)), (u, v) \in \mathcal{Y}\}$, so that we can represent $\cap_{uv\in\mathcal{Y}}A_{uv} = \{\pi \mid \pi(\mathcal{Y}) \subseteq E_\beta\}$. Observe that S_k is defined in terms of *preserved edges* , but it may be further decomposed into terms of *preserved vertices* . Observe that a set of k edges is incident on at least k vertices (a cycle) and at most $2k$ vertices (disjoint edges). Let $p(\mathcal{Y})$ be the number of vertices which are incident to the edges of $\mathcal{Y}$, where $k \leq p(\mathcal{Y}) \leq 2k$. For $k \leq j \leq 2k$, define

$$\phi(k, j) \;=\; \sum_{\substack{\mathcal{Y}\subseteq E_\alpha,\\ |\mathcal{Y}|=k,\ p(\mathcal{Y})=j}} |\{\pi \mid \pi(\mathcal{Y}) \subseteq E_\beta\}|\,,$$

such that S_k can be expressed as $S_k = \sum_{j=k}^{2k}\phi(k, j)$. As it turns out, $S_k \sim \phi(k, 2k)$, meaning that S_k is dominated by the term mapping disjoint edges D_α to edges to disjoint edges in D_β. In Appendix A we formally prove (Corollaries 7 and 9) that for $k = o(2^{n/2})$,

$$\phi(k, 2k) = \frac{N!}{k!}\cdot(1 + o(1))\,, \qquad S_k = \frac{N!}{k!}\cdot(1 + o(1))\,. \tag{5}$$

Recalling that $N = (2^n - 1)$, the approximation is valid for any k which is asymptotically bounded by $2^{n/2}$. For example, $k \leq \frac{2^{n/2}}{\ln(\ln n)}$ would suffice.

3 The Poisson Approximation

In this section we determine an asymptotic approximation to $p_t(2^n, a, b)$. In all our asymptotic approximations we shall assume that $n \to \infty$. Suppose that for each $n \geq 0$, $g_t(n)$ and $h_t(n)$ are defined for $t \in S(n)$, for example, $S(n) = \{0, 1, \ldots, 2^n\}$. We say that $g_t(n) \sim h_t(n)$ *uniformly for* $t \in R(n) \subseteq S(n)$ if

$$\max_{t\in R(n)}\left|\frac{g_t(n)}{h_t(n)} - 1\right| = o(1),$$

that is, for all $t \in R(n)$, $g_t(n)$ is always approaching $h_t(n)$ as $n \to \infty$. The approximation in (3) can be refined to provide the following asymptotic approximation to $p_{2t}(2^n, 2, 2)$:

Corollary 3 For $n \geq 1$, $p_{2t}(2^n, 2, 2) \sim e^{-\frac{1}{2}} \cdot \frac{1}{2}^t/t!$ uniformly for $0 \leq t \leq \frac{2^{n/2}}{2\ln(\ln n)}$. □

Corollary 3 indicates that if ord $\alpha =$ ord $\beta = 2$, then the distribution of smaller values in $T_{\otimes,\pi}(\alpha, \beta)$ can be approximated using the Poisson distribution with $\mu = 1/2$. Our main result is to determine an asymptotic approximation to the distribution as n increases when ord $\alpha > 2$ or ord $\beta > 2$. This approximation is derived using the following asymptotic result. Suppose that there are a sequence of sets $T^{(n)}$, and for each n there are $j(n)$ subsets $B_i \subset T^{(n)}$, $1 \leq i \leq j(n)$, with P_k and S_k defined as above.

Theorem 1 (Bender [1]) If for some $\mu > 0$, $S_k \sim |T^{(n)}| \cdot \mu^k/k!$ uniformly for $0 \leq k \leq l(n) \leq j(n)$, where $l(n)$ is some function which goes to infinity with n, then $P_t \sim |T^{(n)}| \cdot e^{-\mu} \cdot \mu^t/t!$, uniformly for $0 \leq t \leq m(n)$, if $l(n) - m(n)$ tends to infinity with n. □

Theorem 1 can be applied to determining asymptotic approximations to $p_t(2^n, a, b)$ from asymptotic approximations to S_k. For example, in Lemma 3, asymptotic approximations to $p_t(2^n, 2, 4) = p_t(2^n, 4, 2)$ are determined from asymptotic approximations to the values of S_k given in Lemma 2.

Lemma 3 As $n \to \infty$, $p_t(2^n, 2, 4) = p_t(2^n, 4, 2) \sim e^{-1}/t!$ uniformly for $0 \leq t \leq \frac{2^{n/2}}{2\ln(\ln n)}$.

Proof. Consider the expression for S_k when $a = 2$ and $b = 4$ given in Lemma 2. First, we obtain upper and lower bounds on the summation $\sum_{j=\lceil k/2 \rceil}^{k} \binom{2^{n-2}}{j} \cdot \binom{j}{k-j} \cdot 2^{3j}$, to show that

$$\sum_{j=\lceil k/2 \rceil}^{k} \binom{2^{n-2}}{j} \cdot \binom{j}{k-j} \cdot 2^{3j} \quad = \quad 2^k \cdot \binom{2^n}{k} \cdot \left(1 + O(k^2/2^n)\right),$$

for $k = o(2^{n/2})$. After substituting this back into (4), we then go on to show that for $k = o(2^{n/2})$,

$$S_k \quad = \quad \frac{2^n!}{k!} \cdot \left(\prod_{i=0}^{k-1} \left(1 + \frac{i+1}{2^n - 2i - 1}\right)\right) \cdot \left(1 + O(k^2/2^n)\right),$$

If $k = o(2^{n/2})$, then

$$1 \;\leq \prod_{i=0}^{k-1} \left(1 + \frac{i+1}{2^n - 2i - 1}\right) \leq \left(1 - \frac{k}{2^n - 2k}\right)^k \leq \; 1 + O\left(\frac{k^2}{2^n - 2k}\right) = 1 + O(k^2/2^n),$$

and thus $\prod_{i=0}^{k-1} \left(1 + \frac{i+1}{2^n - 2i - 1}\right) = 1 + o(k^2/2^n)$. Therefore, for $k = o(2^{n/2})$,

$$S_k = \frac{2^n!}{k!} \cdot \left(1 + O(k^2/2^n)\right).$$

If $0 \leq k \leq \frac{2^{n/2}}{\ln(\ln n)} = o(2^{n/2})$, then the error term $O(k^2/2^n)$ is upper bounded by $O(1/(\ln(\ln n))^2) = o(1)$. Thus $S_k \sim 2^n!/k! = \left|\Pi^{(n)}\right| \cdot 1^k/k!$ uniformly for $0 \leq k \leq \frac{2^{n/2}}{\ln(\ln n)}$, which we define to be $l(n)$. Hence, we can apply Theorem 1 with $\mu = 1$. Let $m(n) = l(n)/2$, noting that $l(n) - m(n) = l(n)/2$, which goes to infinity with n. Therefore $P_t \sim 2^n! \cdot e^{-1}/t!$ and $p_t(2^n, 2, 4) \sim e^{-1}/t!$ for $0 \leq t \leq m(n) = \frac{2^{n/2}}{2\ln(\ln n)}$. □

This asymptotic approximation extends to the remaining cases for which $a > 2$ or $b > 2$.

Theorem 2 Let $\{a_n\}$ and $\{b_n\}$ be any two sequences such that $a_n = 2^{r_n}$, $b_n = 2^{s_n}$, $1 \leq r_n \leq n$ and $2 \leq s_n \leq n$. Then, $p_t(2^n, a_n, b_n) \sim e^{-1}/t!$ uniformly for $0 \leq t \leq \frac{2^{n/2}}{2\ln(\ln n)}$.

Proof. Corollary 9 in Appendix A shows that $S_k \sim 2^n!/k! = |\Pi^{(n)}|/k!$ for $k = o(2^{n/2})$. The remainder of the proof follows the last paragraph of the proof of Lemma 3. $\square$

Corollary 4 Let $(Z_2^n, \otimes)$ be an Abelian group of order 2^n and $\alpha, \beta \in Z_2^n$ be non-trivial differences. If $\pi \in_R \Pi^{(n)}$, then

$$\begin{array}{rll} \Pr\left(T_{\otimes,\pi}(\alpha,\beta) = 2t\right) & \sim e^{-\frac{1}{2}} \cdot \frac{1}{2}^t/t! & \text{if ord } \alpha = \text{ord } \beta = 2, \\ \Pr\left(T_{\otimes,\pi}(\alpha,\beta) = t\right) & \sim e^{-1}/t! & \text{otherwise,} \end{array}$$

uniformly for $0 \le t \le \frac{2^{n/2}}{2\ln(\ln n)}$. $\square$

We call the asymptotic approximations in Corollary 4 the *Poisson approximation (PA)* to the distribution of entries for $T_{\otimes,\pi}(\alpha,\beta)$. The probabilities $\Pr(T_{\otimes,\pi}(\alpha,\beta) = t$, $0 \le t \le 11$, predicted by the PA are listed in Table 3. Let $\mathbf{E}[X]$, $\mathbf{Var}[X] = \mathbf{E}[X^2] - (\mathbf{E}[X])^2$ and $\sigma[X] = \sqrt{\mathbf{Var}[X]}$ denote the expectation, variance and standard deviation of the random variable X. It is known that if the distribution of values for X is Poisson, then $\mathbf{Var}[X] = \mathbf{E}[X] = \mu$. For example, if ord $\alpha > 2$ or ord $\beta > 2$ then $\mathbf{Var}[T_{\otimes,\pi}(\alpha,\beta)] \sim \mathbf{E}[T_{\otimes,\pi}(\alpha,\beta)] \sim 1$. A little algebraic manipulation reveals that the distribution of values for $\mathbf{P}_{\otimes,\pi}(\alpha,\beta)$ has $\mathbf{E}[\mathbf{P}_{\otimes,\pi}(\alpha,\beta)] \sim 1/2^n$ and $\sigma[\mathbf{P}_{\otimes,\pi}(\alpha,\beta)] \sim \eta/2^n$, where $\eta = \sqrt{2}$ if ord α = ord $\beta = 2$ and $\eta = 1$ otherwise. This indicates that the probabilities for a differential approximation $\Delta X = \alpha \to \Delta\pi(X) = \beta$ where ord α = ord $\beta = 2$ are distributed $\sqrt{2}$ times as far from $1/2^n$ as the probabilities for other differential approximations. Consequently, differential approximations for which ord α = ord $\beta = 2$ are more likely to have higher probabilities.

t	$\Pr(T_{\otimes,\pi}(\alpha,\beta) = t)$		t	$\Pr(T_{\otimes,\pi}(\alpha,\beta) = t)$	
	ord α = ord $\beta = 2$	ord $\alpha > 2$ or ord $\beta > 2$		ord α = ord $\beta = 2$	ord $\alpha > 2$ or ord $\beta > 2$
0	0.606531	0.367879	6	0.0126361	0.000510944
1	-	0.367879	7	-	7.29920×10^{-5}
2	0.303265	0.18394	8	0.00157951	9.12399×10^{-6}
3	-	0.0613132	9	-	1.01378×10^{-6}
4	0.0758163	0.0153283	10	0.000157951	1.01378×10^{-7}
5	-	0.00306566	11	-	9.21616×10^{-9}

Table 3: The probabilities $\Pr(T_{\otimes,\pi}(\alpha,\beta) = t]$, $0 \le t \le 11$, predicted by the Poisson approximation. Note that $T_{\otimes,\pi}(\alpha,\beta)$ must be even if ord α = ord $\beta = 2$.

4 Bounding the Maximum Difference Table Entry

In this section we use the PA to obtain probabilistic bounds on the maximum difference table entry with respect to the three group operations. The expected distribution of entries in the differences tables can be predicted using the PA. The expected distribution of entries in the difference tables with respect to $\oplus$ is approximated using a Poisson distribution with $\mu = \frac{1}{2}$, as all non-trivial elements have order two. The expected distribution of entries in the difference tables with respect to $\boxplus$ and $\odot$ is approximated using a Poisson distribution with $\mu = 1$, as there is only one pair (α, β) with ord α = ord $\beta = 2$. We determine the expectation and variance of $\theta_t(T_{\otimes,\pi})$, defined to be the fraction of entries in $T_{\otimes,\pi}$ that are equal to t, $0 \le t \le 2^n$.

Corollary 5 For $\pi \in_R \Pi_{2^n}$, $\mathbf{E}[\theta_{2t}(T_{\oplus,\pi})] \sim e^{-\frac{1}{2}} \cdot \frac{1}{2}^t/t!$ and $\mathbf{E}[\theta_t(T_{\otimes,\pi})] \sim e^{-1}/t!$ uniformly for $0 \le t \le \frac{2^{n/2}}{2\ln(\ln n)}$ where $\otimes \in \{\boxplus, \odot\}$. $\square$

This information is sufficient for obtaining upper bounds on the maximum entry in differences tables with respect to the three group operations. However, to obtain our lower bound on the maximum entry in differences tables with respect to $\oplus$, the variance of $\theta_{2t}(T_{\oplus,\pi})$ is required. We have not attempted to determine the variance in $\theta_t(T_{\otimes,\pi})$ for $\otimes \in \{\boxplus, \odot\}$ as the counting problem is very complex, and this variance is not required for the results of this paper.

Lemma 4 For $\pi \in_R \Pi_{2^n}$,

$$\mathbf{Var}[\theta_{2t}(T_{\oplus,\pi})] \sim \frac{1}{(2^n-1)^2} \cdot e^{-\frac{1}{2}} \cdot \frac{1}{2}^t/t! \cdot \left(1 - e^{-\frac{1}{2}} \cdot \frac{1}{2}^t/t!\right),$$

uniformly for $0 \le t \le o(\sqrt{N})$.

Proof. See Appendix B. □

For nontrivial α, β define $\Psi^{(t)}_{\alpha,\beta}$, $0 \le t \le 2^{n-1}$, where $\Psi^{(t)}_{\alpha,\beta} = 1$ if $T_{\oplus,\pi}(\alpha,\beta) = 2t$ and $\Psi^{(t)}_{\alpha,\beta} = 0$ otherwise. It follows that $\Psi^{(t)} = \sum_{\alpha,\beta \ne I} \Psi^{(t)}_{\alpha,\beta} = (2^n-1)^2 \cdot \theta_{2t}(T_{\oplus,\pi})$ is the number of entries of size $2t$ in the differences table $T_{\oplus,\pi}$. Note that $\mathbf{E}[\Psi^{(t)}] = (2^n-1)^2 \cdot \mathbf{E}\left[\theta_{2t}(T_{\oplus,\pi})\right] \sim (2^n-1)^2 \cdot e^{-\frac{1}{2}} \cdot \frac{1}{2}^t/t!$ uniformly for $0 \le t \le \frac{2^{n/2}}{2\ln(\ln n)}$. Similarly,

$$\mathbf{Var}\left[\Psi^{(t)}\right] = (2^n-1)^4 \cdot \mathbf{Var}[\theta_{2t}(T_{\oplus,\pi})] \sim (2^n-1)^2 \cdot \frac{e^{-\frac{1}{2}}}{2^t \cdot t!} \cdot \left(1 - \frac{e^{-\frac{1}{2}}}{2^t \cdot t!}\right) \sim \mathbf{E}[\Psi^{(t)}] \cdot \left(1 - \frac{e^{-\frac{1}{2}}}{2^t \cdot t!}\right)$$

drawing on the result of Lemma 4. Recall that we defined $B_n = \ln N^2/\ln\ln N^2$, where $N = (2^n-1)$. Observe that the Poisson approximation (Corollary 4) holds for $0 \le t \le 2B_n$, as $2B_n \le \frac{2^{n/2}}{2\ln(\ln n)}$ when $n \ge 8$.

Lemma 5 If $\pi \in_R \Pi^{(n)}$, then $\Pr(2B_n \le M_{\oplus,\pi} < 2n) \sim 1$.

Proof. O'Connor [11] proved that $\Pr(M_{\oplus,\pi} \ge 2n) = o(1)$. Denote $\Psi = \Psi^{(B_n)}$, and observe that $\mathbf{Var}[\Psi] \sim \mathbf{E}[\Psi]$ as B_n increases with n. Chebychev's inequality (see for example [4]) is applied to show that

$$\Pr(M_{\oplus,\pi} < 2B_n) \le \Pr(\Psi = 0) \le \Pr(|\Psi - \mathbf{E}[\Psi]| \ge \mathbf{E}[\Psi]) \le \frac{\mathbf{Var}[\Psi]}{(\mathbf{E}[\Psi])^2} \sim \frac{1}{\mathbf{E}[\Psi]}.$$

The expected number of entries $2B_n$ in the differences tables with respect to $\oplus$ is equal to

$$\mathbf{E}[\Psi] = (2^n-1)^2 \cdot \mathbf{E}[\theta_{2B_n}(T_{\oplus,\pi})] \sim N^2 \cdot \frac{e^{-\frac{1}{2}}}{2^{B_n} \cdot B_n!}$$

By applying Stirling's formula for $n!$ (see, for example [5, page 213]),

$$B_n! \sim \left(\frac{B_n}{e}\right)^{B_n} \cdot \sqrt{2\pi B_n} = \frac{(\ln N^2)^{\ln N^2/\ln\ln N^2}}{(e \cdot \ln\ln N^2)^{B_n}} \cdot \sqrt{2\pi B_n},$$

where $(\ln N^2)^{\ln N^2/\ln\ln N^2} = (e^{\ln\ln N^2})^{\ln N^2/\ln\ln N^2} = e^{\ln N^2} = N^2$. Consequently,

$$\Pr(M_{\oplus,\pi} < 2B_n) \le \frac{1}{\mathbf{E}[\Psi]} \sim \frac{1}{N^2} \cdot \frac{2^{B_n}}{e^{-\frac{1}{2}}} \cdot \frac{N^2 \cdot \sqrt{2\pi B_n}}{(e \cdot \ln\ln N^2)^{B_n}} = e^{\frac{1}{2}} \cdot \frac{\sqrt{2\pi B_n}}{((e/2) \cdot \ln\ln N^2)^{B_n}} = o(1),$$

as $\sqrt{2\pi B_n} = o\left(((e/2) \cdot \ln\ln N^2)^{B_n}\right)$. Therefore, the probability that the maximum entry is either less than $2B_n$ or greater than or equal to $2n$ is $o(1)$, and $\Pr(2B_n \le M_{\oplus,\pi} < 2n) \sim 1$. □

Lemma 6 If $\pi \in_R \Pi^{(n)}$, then $\Pr(M_{\otimes,\pi} < 2B_n) \sim 1$, where $\otimes \in \{\boxplus, \odot\}$.

Proof. Assume $\otimes \in \{\boxplus, \odot\}$. Let $\Omega^{(t)} = (2^n-1)^2 \cdot \theta_t(T_{\otimes,\pi})$ denote the number of entries t in the differences table with respect to $\otimes$, and in particular denote $\Omega = \Omega^{(2B_n)}$. Recall that $\mathbf{E}[\Omega] = (2^n-1)^2 \cdot \mathbf{E}[\theta_{2B_n}(T_{\otimes,\pi})] \sim N^2 \cdot e^{-1}/(2B_n)!$. By applying Stirling's formula for $n!$,

$$(2B_n)! \sim \left(\frac{2B_n}{e}\right)^{2B_n} \cdot \sqrt{2\pi \cdot (2B_n)} = \left(\frac{2\ln N^2}{e \cdot \ln\ln N^2}\right)^{2B_n} \cdot 2\sqrt{\pi B_n} = \frac{(\ln N^2)^{2\ln N^2/\ln\ln N^2}}{((e/2)\cdot \ln\ln N^2)^{2B_n}} \cdot 2\sqrt{\pi B_n},$$

where $(\ln N^2)^{2\ln N^2/\ln\ln N^2} = (e^{\ln\ln N^2})^{2\ln N^2/\ln\ln N^2} = e^{2\ln N^2} = N^2$. Thus

$$\begin{aligned}\mathbf{E}[\Omega] &\sim N^2 \cdot \frac{e^{-1}}{N^4} \cdot \left((e/2)\cdot \ln\ln N^2\right)^{2\ln N^2/\ln\ln N^2} \cdot \frac{1}{2\sqrt{\pi B_n}} \\ &= \frac{e^{-1}}{2\sqrt{\pi B_n}} \cdot \left(\frac{((e/2)\cdot\ln\ln N^2)^{2/\ln\ln N^2}}{(N^2)^{1/\ln N^2}}\right)^{\ln N^2} = \frac{e^{-1}}{2\sqrt{\pi B_n}} \cdot \left(\underbrace{\frac{((e/2)\cdot\ln\ln N^2)^{2/\ln\ln N^2}}{e}}_{y(N)}\right)^{\ln N^2},\end{aligned}$$

and we can show that $y(N) \leq 1$. Therefore,

$$\mathbf{E}[\Omega] \sim \frac{e^{-1}}{2\sqrt{\pi B_n}} \cdot y(N)^{\ln N^2} = o(1)$$

as B_n increases with n. Now, for $2B_n \leq t \leq \frac{2^{n/2}}{2\ln(\ln n)}$, $\mathbf{E}[\Omega^{(t)}] \leq \mathbf{E}[\Omega]/(2B_n)^{t-2B_n}$. (The value of $\mathbf{E}[\Omega^{(t)}]$ is insignificant for $t > \frac{2^{n/2}}{2\ln(\ln n)}$). Therefore, the expected number of entries greater than or equal to $2B_n$ in a difference table with respect to $\otimes$ is

$$\sum_{t\geq 2B_n} \mathbf{E}[\Omega^{(t)}] \leq \sum_{t\geq 2B_n} \frac{1}{(2B_n)^{t-2B_n}} \cdot \mathbf{E}[\Omega] = \mathbf{E}[\Omega] \cdot \sum_{i\geq 0} \frac{1}{(2B_n)^i} = \frac{\mathbf{E}[\Omega]}{1-1/(2B_n)} \sim \mathbf{E}[\Omega] = o(1).$$

Note that the probability that $M_{\otimes,\pi} \geq 2B_n$ is less than the expected number of entries of size $t \geq 2B_n$. Therefore, $\Pr(M_{\otimes,\pi} \geq 2B_n) = o(1)$ as $n \to \infty$. □

The bounds on $M_{\otimes,\pi}$ correspond to bounds on the maximum probability of an approximation. For example, the probability of the best approximation with respect to XOR differences is in the range $[2^{-58.6}, 2^{-57}]$ for a random 64-bit permutation and in the range $[2^{-121.9}, 2^{-120}]$ for a random 128-bit approximation. The values $2^{-58.6}$ and $2^{-121.9}$ are also upper bounds on the probability of approximations with respect to $\boxplus$ or $\odot$ for random 64-bit and 128-bit permutations respectively. Further bounds on the maximum entry can be obtained for difference tables with respect to other group operations, and these bounds will rely primarily on the fraction of entries in the difference table for which both elements have order 2.

A similar approach can be applied to bound the maximum probability of a quasi-differential. For example, consider the quasi-differentials which use $\oplus$ to define input differences and $\boxplus$ to define output differences. Difference tables for quasi-differentials are defined in much the same way as (1). We note that ord $\alpha = 2$ for all non-trivial input differences α, while for the output differences, ord $\beta = 2$ only if $\beta = 2^{n-1}$. Consequently there are $(2^n - 1) = N$ entries for which ord $\alpha =$ ord $\beta = 2$. Now, N is approximately $(2^{n/2}-1)^2$, so the maximum entry M for the approximations $\alpha \to 2^{n-1}$ can be bounded in much the same way as bounding the maximum XOR entry for a random $n/2$-bit permutation. Consequently, for a random n-bit permutation, we can bound M by $\Pr(2B_{n/2} \leq M \leq 2n/2 = n) \sim 1$. The maximum entry over the remaining approximations is upper bounded by $2B_n$, and thus the maximum entry in the table is lower bounded by $2B_{n/2}$ and upper bounded by $\max(n, 2B_n)$. For example, the maximum table entry for a random 64-bit permutation is between 24 and 64, corresponding to probabilities in the range $[2^{-59.4}, 2^{-58}]$.

Finally, Lemma 5 and Lemma 6 combine to confirm our initial observation that in general XOR differences yield higher probability approximations than differences with respect to modular addition and modular multiplication.

Corollary 6 If $\pi \in_R \Pi^{(n)}$, then $\Pr(M_{\oplus,\pi} > M_{\otimes,\pi}) \sim 1$, for $\otimes \in \{\boxplus, \odot\}$. □

5 Conclusion

We have shown that with high probability, XOR differences yield better differential approximations than differences with respect to modular addition and modular multiplication. Furthermore, we have also been able to find asymptotic approximations to the distribution of entries in differences tables, and find bounds on the maximum differences tables entry with respect to these three group operations. Further bounds on the maximum entry can be obtained for difference tables with respect to other group operations, and these bounds will rely primarily on the fraction of entries in the difference table for which both elements have order 2. The Poisson approximation (Corollary 4) can also be applied to quasi-differentials and the maximum probability can be similarly bounded.

The distribution of entries in difference tables has previously been predicted using a "balls-in-bins" model [8], summarized as follows. In modeling differences tables with respect to XOR, we let the "balls" represent the *unordered* pairs of difference α and let the "bins" represent the possible non-trivial output differences. If the 2^{n-1} input pairs of input difference α (the "balls") can be allocated randomly and independently to any of the (2^n-1) "bins", then the resulting distribution approaches a Poisson distribution with parameter $\mu = \frac{2^{n-1}}{2^n-1} \sim \frac{1}{2}$. In modeling differences tables with respect to $\boxplus$ or $\odot$, we let the "balls" represent the *ordered* pairs of difference α and let the "bins" represent the possible non-trivial output differences. If the input pairs of input difference α (the "balls") can be allocated randomly and independently to any of the (2^n-1) "bins", then the resulting distribution approaches a Poisson distribution with parameter $\mu = \frac{2^n}{2^n-1} \sim 1$. Our results add validity to the "balls-in-bins" approach for predicting the distribution of difference table entries less than $\frac{2^{n/2}}{2\ln(\ln n)}$.

6 Appendix A

Recall the counting problem posed in §2, along with the definitions required for applying Theorem 1. To simplify further proofs, we derive an alternative expression for $\phi(k,j)$. For a set $\mathcal{Y}$ of arcs, define the directed graph $D(\mathcal{Y}) = (V_{\mathcal{Y}}, \mathcal{Y})$, where $V_{\mathcal{Y}} = \{u, v \mid (u,v) \in \mathcal{Y}\}$. Recall that D_α and D_β are composed of disjoint cycles. As $D(\mathcal{Y})$ is a subgraph of D_α it follows that $D(\mathcal{Y})$ consists of disjoint cycles of length a and disjoint paths of length less than a, where a *path of length* L is a set of L connected arcs, $\{(u_{i_0}, u_{i_1}), (u_{i_1}, u_{i_2}), \ldots, (u_{i_{L-1}}, u_{i_L})\}$, where the vertices $u_{i_0}, \ldots, u_{i_L}$ are distinct. In each path there is a unique element with indegree zero and out degree one (for example, vertex u_{i_0}), which we call the *head vertex* of the path. For each $\mathcal{Y} \subseteq E_\alpha$ define the *length vector* $\mathcal{L}_a(\mathcal{Y}) = \chi = (\chi_1, \ldots, \chi_a)$, where

$$\begin{aligned} \chi_i &= (\#\text{ disjoint paths in } D(\mathcal{Y}) \text{ of length } i),\ 1 \le i \le a-1, \\ \chi_a &= (\#\text{ disjoint cycles in } D(\mathcal{Y})). \end{aligned}$$

For a length vector χ we define $h(\chi) = \sum_{i=0}^{a} \chi_i$, $e(\chi) = \sum_{i=0}^{a} i \cdot \chi_i$ and $p(\chi) = h(\chi) + e(\chi) - \chi_a$. Note that if $\mathcal{L}_a(\mathcal{Y}) = \chi$ then $h(\chi)$ is the total number of disjoint paths and cycles in $\mathcal{Y}$, $e(\chi)$ is the number of arcs in $\mathcal{Y}$ and $p(\chi) = p(\mathcal{Y}) = |V_{\mathcal{Y}}|$.

Lemma 7 If $\mathcal{Y} \subseteq E_\alpha$, $\mathcal{Y}^* \subseteq E_\beta$ and $D(\mathcal{Y})$ and $D(\mathcal{Y}^*)$ are isomorphic then $\mathcal{L}_a(\mathcal{Y}) = \mathcal{L}_a(\mathcal{Y}^*)$. If $\mathcal{Y}, \mathcal{Y}^* \subseteq E_\alpha$ and $\mathcal{L}_a(\mathcal{Y}) = \mathcal{L}_a(\mathcal{Y}^*)$, then $D(\mathcal{Y})$ and $D(\mathcal{Y}^*)$ are isomorphic and $|\{\pi \mid \pi(\mathcal{Y}) \subseteq E_\beta\}| = |\{\pi \mid \pi(\mathcal{Y}^*) \subseteq E_\beta\}|$. □

Assume that $a = \text{ord } \alpha \le \text{ord } \beta = b$. Let $\mathcal{Y}_\chi \subseteq E_\alpha$ be a representative subset of E_α for which $\mathcal{L}_a(\mathcal{Y}_\chi) = \chi$ and suppose that $\pi(\mathcal{Y}_\chi) \subseteq E_\beta$ for some $\pi \in \Pi_{2^n}$. As π is a permutation, the subgraphs $D(\mathcal{Y}_\chi)$ and $D(\pi(\mathcal{Y}_\chi))$ are, by definition, isomorphic. Therefore $\mathcal{L}_a(\pi(\mathcal{Y}_\chi)) = \mathcal{L}_a(\mathcal{Y}_\chi) = \chi$ by Lemma 7. Let $F_{\alpha,\beta}$ denote the set of possible length vectors which exist for both subsets of E_α and subsets of E_β. Note that $\chi_a = 0$ for all $\chi \in F_{\alpha,\beta}$ where ord $\alpha \neq$ ord β. ¿From Lemma 7, it follows that $|\{\pi \mid \pi(\mathcal{Y}) \subseteq E_\beta\}| = |\{\pi \mid \pi(\mathcal{Y}_\chi) \subseteq E_\beta\}|$ for all $\mathcal{Y} \subseteq E_\alpha$ such that $\mathcal{L}_a(\mathcal{Y}) = \chi$. Therefore,

$\phi(k,j)$ can be expressed as

$$\begin{aligned}\phi(k,j) &= \sum_{\substack{\mathcal{Y}\subseteq E_\alpha,\\ |\mathcal{Y}|=k,\ p(\mathcal{Y})=j}} |\{\pi \mid \pi(\mathcal{Y}) \subseteq E_\beta\}| \\ &= \sum_{\substack{\chi\in F_{\alpha,\beta}\\ e(\chi)=k,\ p(\chi)=j}} |\{\mathcal{Y}\subseteq E_\alpha \mid \mathcal{L}_a(\mathcal{Y})=\chi\}|\cdot|\{\pi \mid \pi(\mathcal{Y}_\chi)\subseteq E_\beta\}| \\ &= \sum_{\substack{\chi\in F_{\alpha,\beta}\\ e(\chi)=k,\ p(\chi)=j}} \gamma_{\alpha,\chi}\cdot|\{\pi \mid \pi(\mathcal{Y}_\chi)\subseteq E_\beta\}|. \end{aligned} \tag{6}$$

where $\gamma_{\alpha,\chi} = |\{\mathcal{Y}\subseteq E_\alpha \mid \mathcal{L}_a(\mathcal{Y})=\chi\}|$. Now, if $\pi(\mathcal{Y}_\chi)\subseteq E_\beta$, then $\pi(\mathcal{Y}_\chi)$ can be any subset of E_β for which $\mathcal{L}_a(\pi(\mathcal{Y}_\chi))=\chi$ and there are $\gamma_{\beta,\chi}$ such subsets. Let $\mathcal{Y}^*_\chi\subseteq E_\beta$ be any such subset. Then

$$\begin{aligned}|\{\pi|\pi(\mathcal{Y}_\chi)\subseteq E_\beta\}| &= \sum_{\mathcal{Y}^*\subseteq E_\beta} |\{\pi|\pi(\mathcal{Y}_\chi)=\mathcal{Y}^*, \mathcal{L}_a(\mathcal{Y}^*)=\chi\}| \\ &= |\{\mathcal{Y}^*\subseteq E_\beta|\mathcal{L}_a(\mathcal{Y}^*)=\chi\}|\cdot\left|\left\{\pi|\pi(\mathcal{Y}_\chi)=\mathcal{Y}^*_\chi\right\}\right| \;=\; \gamma_{\beta,\chi}\cdot\left|\left\{\pi|\pi(\mathcal{Y}_\chi)=\mathcal{Y}^*_\chi\right\}\right|,\end{aligned}$$

and substitution into (6) reveals

$$\phi(k,j) = \sum_{\substack{\chi\in F_{\alpha,\beta}\\ e(\chi)=k,\ p(\chi)=j}} \gamma_{\alpha,\chi}\cdot\gamma_{\beta,\chi}\cdot\left|\left\{\pi|\pi(\mathcal{Y}_\chi)=\mathcal{Y}^*_\chi\right\}\right|.$$

We now determine the last factor in the above equation, that is, the number of permutations $\pi\in\Pi_{2^n}$ such that $\pi(\mathcal{Y}_\chi)=\mathcal{Y}^*_\chi$. There are $a^{\chi_a}\cdot\chi_a!$ ways to map the cycles of $\mathcal{Y}_\chi$ to the cycles of $\mathcal{Y}^*_\chi$ and $\chi_i!$ ways to map the paths of length i of $\mathcal{Y}_\chi$ to the cycles of length $\mathcal{Y}^*_\chi$ for $1\le i\le a-1$. Finally, there are and $(2^n-j)!$ ways to map the remaining vertices of D_α onto the remaining vertices of D_β. Thus, $\left|\left\{\pi|\pi(\mathcal{Y}_\chi)=\mathcal{Y}^*_\chi\right\}\right| = a^{\chi_a}\cdot\chi!\cdot(2^n-j)!$ and

$$\phi(k,j) = \sum_{\substack{\chi\in F_{\alpha,\beta}\\ e(\chi)=k,\ p(\chi)=j}} \gamma_{\alpha,\chi}\cdot\gamma_{\beta,\chi}\cdot a^{\chi_a}\cdot\chi!\cdot(2^n-j)!.$$

Our task now is to determine $\gamma_{\alpha,\chi}$ and $\gamma_{\beta,\chi}$ for each $\chi\in F_{\alpha,\beta}$. For small a and b this is not very difficult. For example, the exact expressions for S_k in Lemma 2 are derived using this method. However, in general, determining an exact expression for $\gamma_{\alpha,\chi}$ and $\gamma_{\beta,\chi}$ is a difficult task and an asymptotic approximation is sufficient. This asymptotic approximation is developed from an asymptotic approximation to $\phi(k,2k)$ and bounds on the remaining terms.

Let $D_1=(V,E_1)$ and $D_2=(V,E_2)$ be digraphs on $|V|=N$ vertices such that D_1 consists of N/a disjoint cycles of length a and D_2 consists of N/b disjoint cycles of length b. Assume that $a=2^r$, $b=2^s$, $r\ge1$, $s\ge1$ and consequently N is even. Let $F_{1,2}$ denote the set of possible length vectors which exist for both subsets of E_1 and subsets of E_2. For $i\in\{1,2\}$ define $\gamma_{i,\chi}=|\{\mathcal{Y}\subseteq E_i \mid \mathcal{L}_a(\mathcal{Y})=\chi\}|$. Define S_k and $\phi(k,j)$ as in 3. Let $F^*_{1,2}$ denote the set of a-tuples $\chi\in F_{1,2}$ such that $\chi_a=0$, and denote

$$\phi^*(k,j) = \sum_{\substack{\chi\in F^*_{1,2}\\ e(\chi)=k,\ p(\chi)=j}} \gamma_{1,\chi}\cdot\gamma_{2,\chi}\cdot a^{\chi_a}\cdot\chi!\cdot(N-j)!,$$

with $S^*_k=\sum_{j=k}^{2k}\phi^*(k,j)$. Note that if $a\ne b$ then $F^*_{1,2}=F_{1,2}$, $\phi^*(k,j)=\phi(k,j)$ and $S^*_k=S_k$. The three main steps of our approximation are to develop asymptotic approximations to $\phi(k,2k)$, then S^*_k and finally S_k for $k=o(\sqrt{N})$.

To obtain our asymptotic approximation to $\phi(k,2k)$, we first determine the number of ways to select k single disjoint arcs from a cycle of length a. Let $D=(V,E)$ be a cycle of length $a\ge2$. Let

$f_{a,k}$ denote the number of subsets $\mathcal{Y} \subseteq E$ which consist of k single disjoint arcs, $k \geq 0$. Note that $f_{a,k} = 0$ when $k > \lfloor a/2 \rfloor$. The following expression for $f_{a,k}$ is derived using recurrence relations, although the proof is not included here. Lemma 9 is also given without proof.

Lemma 8 For $a \geq 2$, $0 \leq k \leq \lfloor a/2 \rfloor$, $f_{a,k} = \frac{a}{a-k}\binom{a-k}{k}$. □

Lemma 9 Suppose that $\chi = (k, 0 \ldots)$ where $0 \leq k \leq N/2$. Then $f_{N,k} \leq \gamma_{i,\chi} \leq \binom{N}{k}$. for $i \in \{1, 2\}$. □

The following asymptotic approximations are used frequently (without reference) in obtaining our asymptotic approximations.

Lemma 10 If $k = o(\sqrt{N})$ and $t = o(\sqrt{N})$ as $N \to \infty$, then

$$\binom{N}{k} = \frac{N^k}{k!} \cdot \left(1 + o\left(k^2/N\right)\right), \qquad N! = N^k \cdot (N-k)! \cdot \left(1 + 0\left(k^2/N\right)\right),$$
$$(N-k)^t = N^k \cdot \left(1 + 0\left(kt/N\right)\right), \qquad \frac{N}{N-k} = 1 + 0\left(k/N\right).$$

□

Corollary 7 Suppose that a and b are even. For $N \geq 2$, and $k = o(\sqrt{N})$, $\phi(k, 2k) = \frac{N!}{k!} \cdot \left(1 + O\left(k^2/N\right)\right)$.

Proof. Recall that $\phi(k, 2k) = \gamma_{1,\chi} \cdot \gamma_{2,\chi} \cdot k! \cdot (N-2k)!$, where $\chi = (k, 0, \ldots, 0)$. ¿From Lemma 9, a lower bound on $\phi(k, 2k)$ is determined by

$$\phi(k, 2k) \;\geq\; f^2_{N,k} \cdot k! \cdot (N-2k)! \;=\; \left(\frac{N}{N-k}\right)^2 \cdot \binom{N-k}{k}^2 \cdot k! \cdot (N-2k)! \;=\; \frac{N!}{k!} \cdot (1 + O(k^2/N)),$$

for $k = o(\sqrt{N})$. ¿From Lemma 9, the following upper bound on $\phi(k, 2k)$ is obtained:

$$\phi(k, 2k) \;\leq\; \binom{N}{k}^2 \cdot k! \cdot (N-2k)! \;=\; \frac{N^{2k}}{(k!)^2} \cdot k! \cdot (N-2k)! \cdot (1 + O(k^2/N)) \;=\; \frac{N!}{k!} \cdot (1 + O(k^2/N)),$$

for $k = o(\sqrt{N})$. Consequently, $\phi(k, 2k) = \frac{N!}{k!} \cdot (1 + O(k^2/N))$ for $k = o(\sqrt{N})$. □

The next step is to show that $S^*_k = \frac{N!}{k!} \cdot \left(1 + O\left(k^2/N\right)\right)$ for $k = o(\sqrt{N})$. For any a-tuple χ with $h(\chi) = h$, define $\binom{h}{\chi} = \frac{h}{\chi!}$.

Lemma 11 For each $\chi \in F^*_{1,2}$, $\gamma_{1,\chi} \leq \binom{N}{h}\binom{h}{\chi}$ and $\gamma_{2,\chi} \leq \binom{N}{h}\binom{h}{\chi}$ where $h = h(\chi)$.

Proof. Recall that $\chi_a = 0$ for all $\chi \in F^*_{1,2}$. Denote $G_{1,\chi} = \{\mathcal{Y} \subset E_1 \mid \mathcal{L}_a(\mathcal{Y}) = \chi\}$, so that $\gamma_{1,\chi} = |G_{1,\chi}|$. For each $\chi \in F_{1,2}$ we construct a set $H_{1,\chi}$ of subsets of E_1 such that $G_{1,\chi} \subseteq H_{1,\chi}$.

Any subset $\mathcal{Y} \in G_{1,\chi}$ can be partitioned into the h disconnected paths denoted $\mathcal{Y}_1, \ldots, \mathcal{Y}_h$. Note that there are h vertices corresponding to the heads of the paths $\mathcal{Y}_1, \ldots, \mathcal{Y}_h$. Let $A = \{u_{i_1}, \ldots, u_{i_h}\} \subseteq V$ be any subset of h vertices. There are $\binom{N}{h}$ such subsets A. If $\mathcal{Y} \in G_{1,\chi}$ then the subset of head vertices of the paths in $\mathcal{Y}$ must be one of these subsets. For each set A construct subsets of E_1 as follows. Partition A into subsets $A_1, \ldots, A_{a-1}$ such that A_l contains χ_l vertices, $1 \leq l \leq a-1$. There are $\frac{h}{\chi!} = \binom{h}{\chi}$ such partitions. For each l, $1 \leq l \leq a-1$, construct χ_l paths of length l so that each vertex of A_l is the head vertex of a chain of length l. Let $\mathcal{Y}$ be the union of all such paths, and $H_{1,\chi}$ be the union of all subsets $\mathcal{Y}$ constructed using this method. There are $\binom{N}{h} \cdot \binom{h}{\chi}$ choices of subsets A and partitions $A_1, \ldots, A_{a-1}$ to create such sets $\mathcal{Y}$. Therefore $|H_{1,\chi}| \leq \binom{N}{h} \cdot \binom{h}{\chi}$. Note that each $\mathcal{Y} \in G_{1,\chi}$ will be constructed using some subset A and partition $A_1, \ldots, A_{a-1}$. Consequently, $G_{1,\chi} \subseteq H_{1,\chi}$ and $\gamma_{1,\chi} = |G_{1,\chi}| \leq |H_{1,\chi}| \leq \binom{N}{h} \cdot \binom{h}{\chi}$. Similarly $\gamma_{1,\chi} \leq \binom{N}{h} \cdot \binom{h}{\chi}$. □

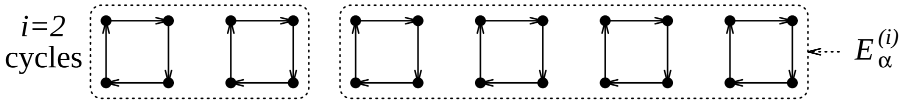

Figure 2: Constructing the set of arcs $E_\alpha^{(i)}$ from E_α. In this figure, ord $\alpha = 4$ and $i = 2$.

Lemma 12 For $k > 0$, and $1 \le h \le k$, with $j = k + h$,

$$\sum_{e(\chi)=k, p(\chi)=j} \binom{h}{\chi} = \sum_{e(\chi)=k, h(\chi)=h} \binom{h}{\chi} = \binom{k-1}{h-1},$$

where the summation is over all possible a-tuples χ with non-negative integer coefficients. □

Corollary 8 Suppose that $N \ge 0$, $a = 2^r$ and $b = 2^s$ such that $a|N$ and $b|N$. For $k = o(\sqrt{N})$, $S_k^* = \frac{N!}{k!} \cdot \left(1 + O\left(k^2/N\right)\right)$.

Proof. Consider $\phi^*(k,j)$ where $0 \le j \le 2k$ and thus $1 \le h = h(\chi) = j - k \le k$. Note that if $k = o(\sqrt{N})$ then $j = o(\sqrt{N})$ and $h = o(\sqrt{N})$. Similarly, if something is $O(k^2/N)$, then it is also $O(j^2/N)$ and $O(h^2/N)$. Recall that $\phi^*(k,j) = \sum \gamma_{\alpha,\chi} \cdot \gamma_{\beta,\chi} \cdot \chi! \cdot (N-j)!$ where the summation is over $\{\chi \in F_{1,2}^* \mid e(\chi) = k,\ p(\chi) = j\}$, and thus

$$\begin{aligned}\phi^*(k,j) &\le \sum \left[\binom{N}{h} \cdot \binom{h}{\chi}\right]^2 \cdot \chi! \cdot (N-j)! = \sum \frac{N^{2h}}{(h!)^2} \cdot \frac{h!}{\chi!} \cdot \binom{h}{\chi} \cdot \chi! \cdot (N-j)! \cdot (1 + O(k^2/N)) \\ &= \frac{N^j}{N^{j-2h} \cdot h!} \cdot (N-j)! \cdot \left(\sum \binom{h}{\chi}\right) \cdot (1 + O(k^2/N)) = \frac{N!}{h!} \cdot \left(\sum \binom{h}{\chi}\right) \cdot (1 + O(k^2/N)).\end{aligned}$$

Note that $F_{1,2}^*$ is a subset of all possible a-tuples χ with non-negative integer coefficients. Thus, Lemma 12 provides the following upper bound:

$$\sum_{\substack{\chi \in F_{1,2}^* \\ e(\chi)=k,\ p(\chi)=j}} \binom{h}{\chi} \le \sum_{e(\chi)=k,\ p(\chi)=j} \binom{h}{\chi} = \binom{k-1}{h-1}.$$

Set $m = j - 2h$. Now, we can show that

$$\begin{aligned}\phi^*(k,j) &\le \frac{N!}{h!} \cdot \frac{1}{N^{j-2h}} \cdot \binom{k-1}{h-1} \cdot \left(1 + O\left(k^2/N\right)\right) \\ &= \frac{N!}{k!} \cdot \frac{k!}{(k-m)!} \cdot \binom{k-1}{k-1-m} \cdot \frac{1}{N^m} \cdot \left(1 + O\left(k^2/N\right)\right) \le \frac{N!}{k!} \cdot \frac{k^{2m}}{N^m} \cdot \left(1 + O\left(k^2/N\right)\right),\end{aligned}$$

for $k = o(\sqrt{N})$. Thus S_k^* is upper bounded by

$$S_k^* = \sum_{j=k+1}^{2k} \phi^*(k,j) \le \sum_{m=1}^{k} \frac{N!}{k!} \cdot \frac{k^{2m}}{N^m} \cdot \left(1 + O\left(k^2/N\right)\right) = \frac{N!}{k!} \cdot \left(1 + O\left(k^2/N\right)\right),$$

for $k = o(\sqrt{N})$. Finally, $S_k^* \ge \phi(k, 2k) = \frac{N!}{k!} \cdot \left(1 + O\left(k^2/N\right)\right)$, for $k = o(\sqrt{N})$, following from Corollary 7. Therefore $S_k^* = \frac{N!}{k!} \cdot \left(1 + O\left(k^2/N\right)\right)$, for $k = o(\sqrt{N})$. □

Corollary 9 Suppose that $n \ge 0$, $a = 2^r$, $b = 2^s$, $1 \le r \le n$ and $2 \le s \le n$. Then $S_k = \frac{2^n!}{k!} \cdot \left(1 + O\left(k^2/2^n\right)\right)$ for $k = o(2^{n/2})$.

Proof. If $a \neq b$, then $S_k = S_k^* = \frac{2^n!}{k!} \cdot (1 + O(k^2/2^n))$ for $k = o(2^{n/2})$ as shown in Corollary 8. Suppose $a = b > 2$, and $\chi_a = i > 0$. Let $E_\alpha^{(i)}$ be the arc set E_α excluding i cycles as shown in Figure 2. Define $\overline{\chi} = (\overline{\chi}_1, \ldots, \overline{\chi}_a)$ by $\overline{\chi}_i = \chi_i$, $1 \leq i \leq a-1$, $\overline{\chi}_a = 0$. Then,

$$\gamma_{\alpha,\chi} \;=\; |\{\mathcal{Y} \subseteq E_\alpha \mid \mathcal{L}_a(\mathcal{Y}) = \chi\}| \;=\; |\{\mathcal{Y} \subseteq E_\alpha \mid \mathcal{L}_a(\mathcal{Y}) = (0,\ldots,0,i)\}| \cdot \left|\left\{\mathcal{Y} \subseteq E_\alpha^{(i)} \mid \mathcal{L}_a(\mathcal{Y}) = \overline{\chi}\right\}\right|.$$

The first term is the number of ways to choose i cycles from $2^n/a = 2^{n-r}$ cycles, and thus

$$|\{\mathcal{Y} \subseteq E_\alpha \mid \mathcal{L}_a(\mathcal{Y}) = (0,\ldots,0,i)\}| \;=\; \binom{2^{n-r}}{i}.$$

We define $\gamma_{\alpha,\overline{\chi}}^{(i)} = \left|\left\{\mathcal{Y} \subseteq E_\alpha^{(i)} \mid \mathcal{L}_a(\mathcal{Y}) = \overline{\chi}\right\}\right|$, so that $\gamma_{\alpha,\chi} = \binom{2^{n-r}}{i} \cdot \gamma_{\alpha,\overline{\chi}}^{(i)} = \gamma_{\beta,\chi}$. Note that provided $k \leq 2^{n-r}$, $0 \leq \chi_a \leq \lfloor k/a \rfloor$. Define $F_\alpha = \{\mathcal{L}_a(\mathcal{Y}) = \chi \mid \mathcal{Y} \subseteq E_\alpha^{(i)}\}$ and let F_α^* denote the set of a-tuples $\chi \in F_\alpha$ such that $\chi_a = 0$. Therefore

$$\begin{aligned} S_k \;&=\; \sum_{\chi \in F_{1,2}, e(\chi) = k} \left(\binom{2^{n-r}}{\chi_a} \cdot \gamma_{\alpha,\overline{\chi}}^{(i)}\right)^2 \cdot a^{\chi_a} \cdot \chi! \cdot (2^n - j)! \\ &=\; \sum_{i=0}^{\lfloor k/a \rfloor} \binom{2^{n-r}}{i}^2 \cdot a^i \cdot i! \cdot \sum_{\overline{\chi} \in F_\alpha^*, e(\overline{\chi}) = k - ia} \gamma_{\alpha,\overline{\chi}}^2 \cdot \overline{\chi}! \cdot (2^n - j - ia)!. \end{aligned}$$

We can apply Corollary 8 to determine the summation over F_α^* with $N = 2^n - ia$. Thus, for $k - ia = o(\sqrt{2^n - ia})$,

$$\sum_{\overline{\chi} \in F_\alpha^*, e(\overline{\chi}) = k - ia} \gamma_{\alpha,\overline{\chi}}^2 \cdot \overline{\chi}! \cdot (2^n - j - ia)! = \frac{(2^n - ia)!}{(k - ia)!} \cdot \left(1 + O\left((k - ia)^2/2^n - ia\right)\right).$$

Note that if $k = o(2^{n/2})$, then $k - ia = o(\sqrt{2^n - ia})$, and $O((k-ia)^2/2^n - ia) = O(k^2/2^n)$. Therefore, if $k = o(2^{n/2})$, we can show that

$$\begin{aligned} S_k \;&=\; \sum_{i=0}^{\lfloor k/a \rfloor} \binom{2^{n-r}}{i}^2 \cdot a^i \cdot i! \cdot \frac{(2^n - ia)!}{(k - ia)!} \cdot \left(1 + O\left(k^2/2^n\right)\right) \\ &=\; \frac{2^n!}{k!} \cdot \left(\sum_{i=0}^{\lfloor k/a \rfloor} \underbrace{\frac{k!}{(k - ia)!} \cdot \frac{1}{i! \cdot a^i} \cdot (2^n)^{-i(a-2)}}_{v(2^n,a,k,i)}\right) \cdot \left(1 + O\left(k^2/2^n\right)\right), \end{aligned}$$

and $v(2^n, a, k, i) \leq \binom{k}{i} \cdot \left(\frac{k^{a-1}}{a \cdot (2^n)^{a-2}}\right)^i$. Thus, an upper bound for S_k is

$$\begin{aligned} S_k \;&\leq\; \frac{2^n!}{k!} \cdot \sum_{i=0}^{\lfloor k/a \rfloor} \binom{k}{i} \cdot \left(\frac{k^{a-1}}{a \cdot (2^n)^{a-2}}\right)^i \cdot \left(1 + O\left(k^2/2^n\right)\right) \\ &\leq\; \frac{2^n!}{k!} \cdot \left(1 + \frac{k^{a-1}}{a \cdot (2^n)^{a-2}}\right)^k \cdot \left(1 + O\left(k^2/2^n\right)\right) \\ &=\; \frac{2^n!}{k!} \cdot \left(1 + O\left(\frac{k^a}{a \cdot (2^n)^{a-2}}\right)\right) \cdot \left(1 + O\left(k^2/2^n\right)\right) \;=\; \frac{2^n!}{k!} \cdot \left(1 + O\left(k^2/2^n\right)\right), \end{aligned}$$

for $k = o(2^{n/2})$, provided that $a > 2$. Note that $S_k \geq S_k^* = \frac{2^n!}{k!} \cdot (1 + O(k^2/2^n))$, and therefore $S_k = \frac{2^n!}{k!} \cdot (1 + O(k^2/2^n))$ for $k = o(2^{n/2})$. □

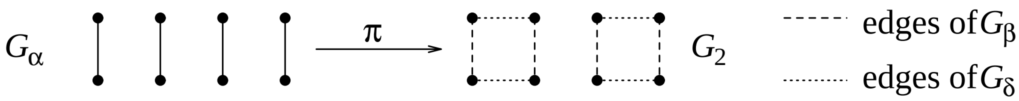

Figure 3: The undirected graphs G_α and $G_2 = (V, E_2)$ where $E_2 = E_\beta \cup E_\delta$.

7 Appendix B

Lemma 13 For $\pi \in_R \Pi_{2^n}$,

$$\mathbf{Var}[\theta_{2t}(T_{\oplus,\pi})] \sim \frac{1}{(2^n-1)^2} \cdot e^{-\frac{1}{2}} \cdot \frac{1}{2}^t/t! \cdot \left(1 - e^{-\frac{1}{2}} \cdot \frac{1}{2}^t/t!\right),$$

uniformly for $0 \le t \le \frac{2^{n/2}}{2\ln(\ln n)}$.

Sketch of Proof. Observe that $\mathbf{Var}\left[\Psi^{(t)}\right] = (2^n-1)^4 \cdot \mathbf{Var}[\theta_{2t}(T_{\oplus,\pi}]$, and $\mathbf{Var}\left[\Psi^{(t)}\right]$ is determined from $\mathbf{Var}\left[\Psi^{(t)}\right] = \mathbf{E}\left[(\Psi^{(t)})^2\right] - (\mathbf{E}[\Psi^{(t)}])^2$. We determine $\mathbf{E}\left[(\Psi^{(t)})^2\right]$ from

$$\begin{aligned}\mathbf{E}\left[(\Psi^{(t)})^2\right] &= \mathbf{E}\left[\left(\sum \Psi^{(t)}_{\alpha,\beta}\right)^2\right] = \sum \mathbf{E}\left[\left(\Psi^{(t)}_{\alpha,\beta}\right)^2\right] + \sum_{\delta\neq\beta} \mathbf{E}\left[\Psi^{(t)}_{\alpha,\beta}\cdot\Psi^{(t)}_{\alpha,\delta}\right] \\ &\quad + \sum_{\delta\neq\alpha} \mathbf{E}\left[\Psi^{(t)}_{\alpha,\beta}\cdot\Psi^{(t)}_{\delta,\beta}\right] + \sum_{\alpha\neq\delta,\beta\neq\epsilon} \mathbf{E}\left[\Psi^{(t)}_{\alpha,\beta}\cdot\Psi^{(t)}_{\delta,\epsilon}\right],\end{aligned} \tag{7}$$

where the summation is over the nontrivial differences α, β, δ and ϵ in the subscripts of $\Psi^{(t)}$. Now,

$$\sum \mathbf{E}\left[\left(\Psi^{(t)}_{\alpha,\beta}\right)^2\right] = \sum \mathbf{E}\left[\Psi^{(t)}_{\alpha,\beta}\right] = \sum \Pr\left(T_{\oplus,\pi}(\alpha,\beta) \ge 2t\right) \sim (2^n-1)^2 \cdot e^{-\frac{1}{2}} \cdot \frac{1}{2^t \cdot t}, \tag{8}$$

for $0 \le t \le \frac{2^{n/2}}{2\ln(\ln n)}$. However, the remaining terms must be determined using different graph enumeration problems. Consider $\mathbf{E}\left[\Psi^{(t)}_{\alpha,\beta}\cdot\Psi^{(t)}_{\alpha,\delta}\right]$ where α, β and δ are non-trivial differences such that $\beta \neq \delta$. Note that $\Psi^{(t)}_{\alpha,\beta}\cdot\Psi^{(t)}_{\alpha,\delta} = 1$ only if $d_{\oplus,\pi}(D_\alpha, D_\beta) = 2t$ and $d_{\oplus,\pi}(D_\alpha, D_\delta) = 2t$, and

$$\begin{aligned}\mathbf{E}\left[\Psi^{(t)}_{\alpha,\beta}\cdot\Psi^{(t)}_{\alpha,\delta}\right] &= \Pr\left(\Psi^{(t)}_{\alpha,\beta}\cdot\Psi^{(t)}_{\alpha,\delta} = 1\right) \\ &= \Pr\left(d_{\oplus,\pi}(D_\alpha, D_\beta) = 2t \text{ and } d_{\oplus,\pi}(D_\alpha, D_\delta) = 2t\right) \\ &= \frac{1}{2^n!}\cdot\left|\left\{\pi \in \Pi^{(n)} \mid d_{\oplus,\pi}(D_\alpha, D_\beta) = 2t, d_{\oplus,\pi}(D_\alpha, D_\delta) = 2t\right\}\right|.\end{aligned}$$

We consider all the edges to be undirected, that is $(u,v) = (v,u)$. Let G_α be the undirected graph with the same edge set as D_α. Similarly define G_β and G_δ. Define $G_2 = (V, E_2)$ where $E_2 = E_\beta \cup E_\delta$. Observe that G_2 consists of 2^{n-2} unordered cycles of length four, as shown in Figure 3. Note that $d_{\oplus,\pi}(D_\alpha, D_\beta) = d_{\oplus,\pi}(D_\alpha, D_\delta) = 2t$ if π maps $2t$ (undirected) edges of G_α onto G_2 such that exactly t edges are mapped onto G_β and exactly t edges are mapped onto G_δ. We apply the IEP twice to determine

$$\left|\left\{\pi \in \Pi^{(n)} \mid d_{\oplus,\pi}(D_\alpha, D_\beta) = 2t, d_{\oplus,\pi}(D_\alpha, D_\delta) = 2t\right\}\right|,$$

and our approximation will require two applications of Theorem 1. Suppose that $\mathcal{Y}_1 \subseteq E_\alpha$ with $|\mathcal{Y}_1| = k$ (considering the edges to be undirected, so this is the equivalent of 2k directed edges). For each $e \in E_\alpha \setminus \mathcal{Y}_1$ define $B_e(\mathcal{Y}_1) = \left\{\pi \in \Pi^{(n)} \mid \pi(\mathcal{Y}_1) \subseteq E_\beta, \pi(\{e\}) \subseteq E_\delta\right\}$. By the IEP, the number of permutations π that preserve exactly t edges from G_α in G_δ and for which $\pi(\mathcal{Y}_1) \subseteq E_\beta$ is

$$Q_t(\mathcal{Y}_1) \;=\; \sum_{i \geq 0} \binom{t+i}{i} \cdot S_{t+i}(\mathcal{Y}_1), \qquad S_t(\mathcal{Y}_1) \;=\; \sum_{\mathcal{Y}_2 \subseteq E_\alpha \setminus \mathcal{Y}_1, |\mathcal{Y}_2|=t} \cap_{e \in \mathcal{Y}_2} B_e(\mathcal{Y}_1).$$

By applying the IEP a second time, the number of permutations π that preserve exactly k edges from G_α in G_β and preserve exactly t edges of G_α in G_δ is

$$P_t(k) \;=\; \sum_{i \geq 0} \binom{k+i}{i} \cdot R_{k+i}(t), \qquad R_t(k) \;=\; \sum_{\mathcal{Y}_1 \subseteq E_\alpha, |\mathcal{Y}_1|=k} Q_t(\mathcal{Y}_1).$$

Using a similar approach to that used in Appendix A, and repeated application of Theorem 1 with $\mu = \frac{1}{2}$, we show that

$$\begin{aligned} S_t(\mathcal{Y}_1) \;&\sim\; \frac{2^n!}{(2^n)^k} \cdot \frac{1}{2^t \cdot t!}, \qquad & \Rightarrow\; Q_t(\mathcal{Y}_1) \;&\sim\; \frac{2^n!}{(2^n)^k} \cdot \frac{e^{-\frac{1}{2}}}{2^t \cdot t!}, \\ \Rightarrow\; R_t(k) \;&\sim\; \frac{2^n! \cdot e^{-\frac{1}{2}}}{2^t \cdot t!} \cdot \frac{1}{2^k \cdot k!}, \qquad & \Rightarrow\; P_k(t) \;&\sim\; \frac{2^n! \cdot e^{-\frac{1}{2}}}{2^t \cdot t!} \cdot \frac{e^{-\frac{1}{2}}}{2^k \cdot k!}, \end{aligned}$$

where the approximation to $P_k(t)$ is uniform for for $0 \leq t \leq \frac{2^{n/2}}{2\ln(\ln n)}$ and $0 \leq k \leq \frac{2^{n/2}}{2\ln(\ln n)}$. Therefore

$$\mathbf{E}\left[\Psi^{(t)}_{\alpha,\beta} \cdot \Psi^{(t)}_{\alpha,\delta}\right] \;=\; \mathbf{E}\left[\Psi^{(t)}_{\alpha,\beta} \cdot \Psi^{(t)}_{\delta,\beta}\right] \;=\; \frac{P_t(t)}{2^n!} \;\sim\; \left(\frac{e^{-\frac{1}{2}}}{2^t \cdot t!}\right)^2, \tag{9}$$

uniformly for $0 \leq t \leq \frac{2^{n/2}}{2\ln(\ln n)}$.

We determine $\mathbf{E}\left[\Psi^{(t)}_{\alpha,\beta} \cdot \Psi^{(t)}_{\delta,\epsilon}\right]$ where $\alpha \neq \delta$ and $\beta \neq \epsilon$ in a similar way. We consider all the edges to be undirected, as above. Define $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ where $E_1 = E_\alpha \cup E_\delta$ and $E_2 = E_\beta \cup E_\epsilon$. Observe that G_1 and G_2 consists of 2^{n-2} unordered cycles of length four, as for G_2 in Figure 3 Now, $d_{\oplus,\pi}(D_\alpha, D_\beta) = d_{\oplus,\pi}(D_\alpha, D_\delta) = 2t$ if π maps $2t$ (undirected) edges of G_1 onto G_2 such that exactly t edges are mapped from G_α onto G_β and exactly t edges are mapped from G_δ onto G_ϵ. Once again we apply the IEP and Theorem 1 twice to show that for all α, β, δ and ϵ such that $\alpha \neq \delta$ and $\beta \neq \epsilon$,

$$\mathbf{E}\left[\Psi^{(t)}_{\alpha,\beta} \cdot \Psi^{(t)}_{\delta,\epsilon}\right] \;\sim\; \left(\frac{e^{-\frac{1}{2}}}{2^t \cdot t!}\right)^2, \tag{10}$$

uniformly for $0 \leq t \leq \frac{2^{n/2}}{2\ln(\ln n)}$. The proof is very involved, so it is not shown here. The values (9) and (10) are substituted back into (7), to obtain $\mathbf{E}\left[(\Psi^{(t)})^2\right]$. ¿From Corollary 5 we obtain the asymptotic approximation $(\mathbf{E}[\Psi^{(t)}])^2 \;=\; \left((2^n-1)^2 \cdot \mathbf{E}[\theta_{2i}(T_{\oplus,\pi})]\right)^2 \;\sim\; (2^n-1)^4 \cdot \left(e^{-\frac{1}{2}}/(2^t \cdot t!)\right)^2$, for $0 \leq t \leq \frac{2^{n/2}}{2\ln(\ln n)}$. The lemma is proven by substituting the value into the expression for $\mathbf{Var}\left[\Psi^{(t)}\right]$, resulting in

$$\mathbf{Var}\left[\Psi^{(t)}\right] \;\sim\; (2^n-1)^2 \cdot \frac{e^{-\frac{1}{2}}}{2^t \cdot t!} \cdot \left(1 - \frac{e^{-\frac{1}{2}}}{2^t \cdot t!}\right),$$

from which $\mathbf{Var}\left[\theta_{2t}(T_{\oplus,\pi})\right] = (2^n-1)^{-4} \cdot \mathbf{Var}\left[\Psi^{(t)}\right]$ is determined. □

References

[1] E. A. Bender. Asymptotic methods in enumeration. *SIAM Review*, 16(4):485–515, 1974.

[2] E. Biham and Shamir A. Differential cryptanalysis of DES-like cryptosystems. *Advances in Cryptology, CRYPTO'90, Lecture Notes in Computer Science, vol. 537, A. J. Menezes and S. A. Vanstone ed., Springer-Verlag*, pages 2–21, 1991.

[3] E. Biham and A. Shamir. Differential cryptanalysis of the full 16-round DES. Technical Report 708, Technion, Israel Institute of Technology, Haifa, Israel, 1991. Also presented at Advances in Cryptology, CRYPTO'92, Lecture Notes in Computer Science, vol. 740, E. F. Brickell ed., Springer-Verlag, pages 487-496, 1993.

[4] W. Feller. *An Introduction to Probability Theory and its Applications.* New York: Wiley, 3rd edition, Volume 1, 1968.

[5] R. P. Grimaldi. *Discrete and Combinatorial Mathematics: An Applied Introduction. Second Edition.* Addison Wesley Publishing Company, 1989.

[6] M. Hall. *Combinatorial Theory.* New York: Wiley-Interscience, 1986.

[7] X. Lai, J. Massey, and S. Murphy. Markov ciphers and differential cryptanalysis. *Advances in Cryptology, EUROCRYPT'91, Lecture Notes in Computer Science, vol. 547, D. W. Davies ed., Springer-Verlag*, pages 17–38, 1991.

[8] J. Lee, H. M. Heys, and S. E. Tavares. Resistance of a CAST-like encryption algorithm to linear and differential cryptanalysis. *Designs, Codes and Cryptography*, 12(3):267–282, 1997.

[9] J. Massey. SAFER K-64: A byte-oriented block-ciphering algorithm. *Fast Software Encryption, Lecture Notes in Computer Science, vol. 809, R. Anderson ed., Springer-Verlag*, pages 1–17, 1994.

[10] J. Massey. SAFER K-64: One year later. *Fast Software Encryption, Lecture Notes in Computer Science, vol. 1008, B. Preneel ed., Springer*, pages 212–241, 1995.

[11] L. J. O'Connor. On the distribution of characteristics in bijective mappings. *Advances in Cryptology, EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, T. Helleseth ed., Springer-Verlag*, pages 360–370, 1994.

[12] National Bureau of Standards. Data Encryption Standard. FIPS PUB 46, Washington, D. C. (January 1977).