Rose-Hulman Undergraduate Mathematics Journal

Volume 18
Issue 1

Article 18

The Secret Santa Problem Continues

Daniel Crane
Taylor University

Tanner Dye
Taylor University

Rose-Hulman Undergraduate Mathematics Journal

THE SECRET SANTA PROBLEM CONTINUES

Daniel Crane[a] Tanner Dye[b]

Volume 18, No. 1, Spring 2017

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
mathjournal@rose-hulman.edu
scholar.rose-hulman.edu/rhumj

[a]Taylor University
[b]Taylor University

Rose-Hulman Undergraduate Mathematics Journal
Volume 18, No. 1, Spring 2017

THE SECRET SANTA PROBLEM CONTINUES

Daniel Crane Tanner Dye

Abstract. We explore the Secret Santa gift exchange problem. A group of n people draws names at random, giving a gift to the person drawn. First, we examine the probabilities of gift exchanges under various scenarios when everyone draws names at once, similar to Montmort's matching problem. We then consider the probabilities of certain gift exchanges when people take turns drawing names and develop a strategy to maximize the likelihood of receiving a gift from the most generous participant.

Acknowledgements: This work was partially funded by a Taylor University Faculty Mentored Undergraduate Summer Scholarship. We would also like to thank Dr. Case for advising us on our research.

1 Introduction

Secret Santa gift exchanges are a popular Christmas tradition. In a Secret Santa gift exchange, a group of n people draws names at random, with the requirement that a person can not draw him or herself. Then each person gives a gift to the person drawn.

There are several ways to design a Secret Santa gift exchange. Previous work done on these gift exchanges [2, 5, 6, 9, 10] usually operates under the assumption that everyone is equally likely to give a gift to any other person in the gift exchange, which is true when everyone draws a name at once. In Section 2, we summarize some of these results and also apply results proven in other contexts to Secret Santa. We consider cases where everyone is single, where all participants are in families of size k, and where participants are in families of different sizes. The probability of needing to redraw names depends on family size when we do not allow family members to give gifts to each other. Rook polynomials allow for calculation of this probability. Other techniques such as the inclusion-exclusion principle and bounds on permanents of matrices can be used for studying he limiting behavior of these probabilities when the number of participants in the gift exchange increases.

Next, in Section 3, we examine probabilities of allowed gift exchanges when names are drawn one at a time as opposed to all at once as in Section 2, and we then determine which kinds of exchanges are more likely than others. Specifically, we show that the order of drawing names affects to whom each participant is most likely to give a gift. In this type of gift exchange, the probability of any one derangement can be written as a product of terms involving an indicator function, and this allows us to compare the probabilities for two different giver-recipient pairs. We find that each person is most likely to give to the person drawing directly before him, with the first person to draw being most likely to give a gift to the last person to draw. Furthermore, we find that the last person to draw is more likely to give a gift to the second to last person than any other giver-recipient pair.

2 Drawing Names All at Once

In Secret Santa, nobody is allowed to give a gift to himself or herself. We might add the additional constraint that if a participant is in a family of k people (for $k \geq 2$), he may not give to himself or to a family member. We will refer to a gift exchange where no one gives to himself or a family member, as an *allowed arrangement*. When everyone draws names at once, there is a chance that nobody will draw his own name or a family member's name. The probability of this is equal to the number of allowed arrangements divided by total number of arrangements, $n!$. As the number of people approaches infinity, this probability converges to different values depending on the number of people in various family sizes.

2.1 The Simplest Case

When the only restriction is that nobody can draw his own name, the allowed exchanges

are called derangements. The number of possible derangements for n people is

$$d_n = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}, \tag{1}$$

which can be verified using the inclusion-exclusion principle. This allows for a simple proof of our first result by recognizing the Taylor series for e^{-1}. In the following theorem we see that the probability of a derangement approaches e^{-1} as the number of people n increases.

Theorem 2.1. *If d_n is the number of derangements of length n, then*

$$\lim_{n\to\infty} \frac{d_n}{n!} = \frac{1}{e}. \tag{2}$$

This is a well known and easy to prove result known by multiple names, most notably as Montmort's Matching Problem [4].

2.2 Families of k people

Now suppose that all of the n people in a gift exchange are partitioned into families of size k. In that case, the rules require that nobody can give to a member of his own family. In this case, the number of allowed arrangements can be calculated using rook polynomials [3] or using permanents of (0,1) matrices. The number of allowed arrangements is

$$F_k(n) = \sum_{i=1}^{n} (-1)^i R_i * (n-i)!, \tag{3}$$

where R_i is the i^{th} coefficient of the rook polynomial

$$R(x) = \left(\sum_{j=0}^{k} \binom{k}{j}^2 j! x^j \right)^{n/k}.$$

The i^{th} coefficient of a rook polynomial of degree d represents the number of ways to place i non-attacking rooks, meaning no rooks share a row or column, on an $d \times d$ chessboard. In this case, our problem can be represented as the number of ways to place k non-attacking rooks each on n/k separate chessboards.

Alternatively, by letting A be a $(0,1)$ matrix with $k \times k$ blocks of 0s along the diagonal and 1s everywhere else we can calculate the value $F_k(n)$ by taking the permanent of A. This alternate method is used in the proof of out next theorem, which determines the limiting behavior of the probability of an allowed arrangement as n increases.

Theorem 2.2. (Penrice [6]) *If $F_k(n)$ represents the number of allowed arrangements for a gift exchange with n people in families of k, then*

$$\lim_{n\to\infty} \frac{F_k(n)}{n!} = e^{-k}. \tag{4}$$

Penrice's proof involves finding upper and lower bounds on the fraction $F_k(n)/n!$ using inequalities from Minc and Van der Waerden for permanents of (0,1) matrices. Since both of these bounds go to e^{-k}, then the probability does as well.

2.3 The General Case

Of course, large collections of people are rarely all in families of equal size. More generally, for n people, let p_1 be the proportion of the people who are individuals, p_2 be the proportion of the people who are in families of two, and so on so that p_i represents the proportion of people in a family of i. Once again, we can calculate the number of allowed arrangements using rook polynomials or permanents. Letting F_n denote the number of allowed arrangements for this case, we find that

$$F_n = \sum_{i=1}^{n} (-1)^i R_i * (n-i)!,$$

where R_i is the i^{th} coefficient of the rook polynomial

$$R(x) = \prod_{k=1}^{M} \left(\sum_{j=0}^{k} \binom{k}{j}^2 j! x^j \right)^{np_k},$$

and M denotes the largest family size in the collection of participants.

We then come to our next result which applies a known theorem to Secret Santa exchanges.

Theorem 2.3. *If $F_{\overline{x}}(n)$ represents the number of allowed arrangements for a gift exchange with $p_i n$ people in families of size i for each $i \in \mathbb{Z}^+ \cup 0$, then*

$$\lim_{n\to\infty} \frac{F_{\overline{x}}(n)}{n!} = e^{-\overline{x}} \tag{5}$$

where

$$\overline{x} = \sum_{i=1}^{M} i p_i$$

and M denotes the largest family size.

We see that this agrees with our previous results in section 2.2 when we let $p_k = 1$ and $p_i = 0$ for $i \neq k$.

Proof. The proof follows from a special case of a result by Barton given in Margolius [4] and proven by Barton [1]. In Barton's proof, the problem is viewed as two decks of N cards being matched up pairwise. There are S suits in each deck with n_i cards of suit i in deck one and m_i cards of suit i in deck two. A match occurs if a card from deck 1 of suit i is matched up with a card from deck 2 of the same suit.

For our purposes, each deck of cards corresponds to the participants in Secret Santa (one being the givers and one being the receivers). Then $n_i = m_i$ because the givers and receivers are the same collection of people. Each of the S suits corresponds to an individual family of n_i people.

Barton proves that the distribution of the number of matching cards, or in our case the number of people who drew their own name or a family member's name, is asymptotic to a Poisson distribution with parameter

$$\lambda = \frac{1}{N}\sum_{i=1}^{S} n_i m_i.$$

For us, the parameter becomes $\frac{1}{N}\sum_{i=1}^{S} n_i^2$. It can be verified using our previous notation that this becomes

$$\lambda = \sum_{i=1}^{M} i p_i = \overline{x}.$$

So the probability distribution for the number of people j who draw their own or a family member's name is given by

$$\frac{\overline{x}^j}{j!} e^{-\overline{x}}.$$

So the probability that nobody draws his own name or a family member's name ($j = 0$) becomes $e^{-\overline{x}}$. □

3 Drawing One at a Time

We assumed in section 2 that each derangement was equally likely, but few gift exchanges are set up so that everyone draws names at the same time. A more common method of drawing is for everyone to take turns drawing names and for each person to redraw if he gets his own name. In this section, we will assume that everyone is single. In this case, the only problem that might arise is if the last person gets his own name. We will assume that if this happens, then everyone will return the names drawn and they will redraw using the same method. An interesting consequence of this method of drawing names is that different arrangements are no longer equally likely. We find that the order in which people draw determines who each person is most likely to draw.

3.1 Ranking Derangement Classes by Likelihood

First, we will introduce some notation. We use $x \to y$ to indicate that the x^{th} person to draw gives to the y^{th} person. Similarly, we will let $P(x \to y)$ denote the probability that the x^{th} person gives to the y^{th} person. Finally, if α is a derangement, we will let $\alpha(x) = y$ mean

that $x \to y$ for the specific derangement α.

Most of our proofs rely heavily on two ideas. The first is our method for calculating probabilities. One method of computing probabilities when names are drawn one at a time is given by White [10]. We will employ simpler, more illustrative notation for these probabilities.

Lemma 3.1. *Let D_n denote the set of all derangements (allowed gift exchanges) for n people. For a given derangement $\alpha \in D_n$, the probability of α is given by*

$$P(\alpha) = \prod_{i=1}^{n} \frac{1}{n - i + I_\alpha(i)}, \tag{6}$$

where i runs over all of the n people, and $I_\alpha(i)$ is an indicator function that is equal to 1 if the i^{th} person's name is drawn before i draws and equal to 0 if his name has not yet been drawn. To avoid dividing by zero, we define $I_\alpha(n) = 1$.

Proof. The probability of person i drawing a specific name is 1 divided by the number of names left in the hat which i could possibly draw. We find that this number of names is $n - i + 1$ if i has not been drawn and $n - i$ otherwise. Then the probability associated $i \to \alpha(i)$ for a specific derangement α is

$$P(i \to \alpha(i)) = \frac{1}{n - i - I_\alpha(i)}.$$

The probability of the derangement as a whole is the product of such terms,

$$P(\alpha) = \prod_{i=1}^{n} P(i \to \alpha(i)) = \prod_{i=1}^{n} \frac{1}{n - i + I_\alpha(i)}.$$

□

For example, the probability where $n = 5$ people and the derangement

$$\alpha = 1 \to 5 \to 4 \to 2 \to 3 \to 1$$

(where 1 is first to draw, 2 second, and so on) is $(1/4)(1/3)(1/3)(1)(1) = 1/24$.

The second idea we employ is the notion of "pairing up" derangements with each other. We can find a bijection between sets of derangements and compare the probabilities of these derangements. If we can find a bijection between arrangements where $x \to y$ and arrangements where $x \to z$ and every individual arrangement where $x \to y$ is at least as likely as the corresponding arrangement where $x \to z$, then we can conclude that $P(x \to y) \geq P(x \to z)$.

We apply these ideas to prove the next several theorems. The first one involves those who draw names before the k^{th} person.

Theorem 3.2. *For $n \geq 3$ participants, if $i < i+1 < k$ then $P(k \to i) \leq P(k \to i+1)$.*

In everyday language, this conjecture states that a participant is more likely to draw the second person in a pair of consecutive people who had already drawn. A direct consequence of this is that, of all the people who drew before him, he is most likely to draw the person who drew right before him, second most likely to draw the person who drew two people before him, and so on.

Proof. Let A be the set of derangements in D_n where $k \to i$ and B be the set of derangements where $k \to i+1$. Note that $|A| = |B|$ by symmetry. We will set up a bijection from A to B and compare each $\alpha \in A$ to its corresponding derangement $\beta \in B$.

There are three different types of derangements in A (and in B). We will examine each of these three cases.

Case 1: Suppose that $\alpha(y) = i+1$ for some $y < i$. In other words, $i+1$ was drawn before i's turn for the derangement α.

In this case, we will map α to the $\beta \in B$ such that α and β are identical except for the two differences that $\beta(k) = i+1$ and $\beta(y) = i,$. Thus, $P(\alpha)$ and $P(\beta)$ (which are both just products of probabilities of the form $1/(n - i + I_\alpha(x)))$ will agree with each other except possibly at the terms $1/(n - i + I_\alpha(i))$ and $1/(n - (i+1) + I_\alpha(i+1))$.

These terms will be different for the two derangements. For α, $i+1$ drew after he was drawn so $I_\alpha(i+1) = 1$. Meanwhile i drew before he was drawn, so $I_\alpha(i) = 0$.

On the other hand, since i drew after he was drawn in β, then $I_\beta(i) = 1$ and $I_\beta(i+1) = 0$ because he drew a name before his name was drawn.

Thus we have (note that $I_\alpha(j) = I_\beta(j)$ for $j \neq i, i+1$)

$$P(\alpha) = \frac{1}{(n-i)} \frac{1}{(n-(i+1)+1)} \prod_{j=1, j\neq i, j\neq i+1}^{n} \frac{1}{n - j + I_\alpha(j)},$$

whereas

$$P(\beta) = \frac{1}{(n-i+1)} \frac{1}{(n-(i+1))} \prod_{j=1, j\neq i, j\neq i+1}^{n} \frac{1}{n - j + I_\alpha(j)}.$$

Then by inspection, we see that $P(\beta) > P(\alpha)$.

Case 2: Now suppose α is such that $\alpha(i) = i+1$ and $\alpha(i+1) = y$ for some $y \in \{1, ...n\}$. Then map this α to a $\beta \in B$ such that $\alpha = \beta$ except for the following alternations: $\beta(k) = i+1$, $\beta(i) = y$ and $\beta(i+1) = i$.

For α, i draws before he has been drawn (by k) so $I_\alpha(i) = 0$ and $i+1$ draws after he has been drawn (by i). So $I_\alpha(i+1) = 1$. Thus,

$$P(\alpha) = \frac{1}{(n-i)} \frac{1}{(n-(i+1)+1)} \prod_{j=1, j\neq i, j\neq i+1}^{n} \frac{1}{n - j + I_\alpha(j)}.$$

For β, $i+1$ draws before he has been drawn (by k) so $I_\beta(i+1) = 0$ and i also draws before his name is drawn (by $i+1$). So $I_\beta(i) = 0$. Thus,

$$P(\beta) = \frac{1}{(n-i)}\frac{1}{(n-(i+1))}\prod_{j=1,j\neq i,j\neq i+1}^{n}\frac{1}{n-j+I_\alpha(j)}.$$

Once again, we see that $P(\beta) > P(\alpha)$.

Case 3: Now suppose that $\alpha(k) = i$, $\alpha(m) = i+1$ where $m \in \{i+1, ...n\}$; (i.e $i+1$ draws before his name was drawn).

We will map α in this case to the β equal to α except that $\beta(k) = i+1$ and $\beta(m) = i$.

In α, $i+1$ draws before he was drawn so $I_\alpha(i+1) = 0$. The same is true for i so $I_\alpha(i) = 0$. Thus,

$$P(\alpha) = \frac{1}{(n-i)}\frac{1}{(n-(i+1))}\prod_{j=1,j\neq i,j\neq i+1}^{n}\frac{1}{n-j+I_\alpha(j)}.$$

Now for β, both i and $i+1$ drew before they were drawn (by m and k) so $I_\beta(i) = I_\beta(i+1) = 0$ Thus,

$$P(\beta) = \frac{1}{(n-i)}\frac{1}{(n-(i+1))}\prod_{j=1,j\neq i,j\neq i+1}^{n}\frac{1}{n-j+I_\beta(j)}.$$

Note that these probabilities are equal so $P(\alpha) = P(\beta)$ for case 3.

We now show that our mapping is a bijection. For $\beta \in B$, β will have one of the forms described by the three cases above. Then our mapping is invertible and must be a bijection.

Then $P(\alpha) < P(\beta)$ in cases 1 and 2 and $P(\alpha) = P(\beta)$ in case 3. Therefore $P(k \to i) = \sum_i P(\alpha_i) \leq \sum_i P(\beta_i) = P(k \to i+1)$. □

We find that when this inequality is strict whenever we have at least 3 people in our gift excange.

Corollary 3.3. *The inequality in Theorem 3.2 is a strict inequality for $n \geq 3$.*

Proof. Consider, $n = 3$ people and $3 \to 1$. Then we must have $1 \to 2$ and $2 \to 3$. Thus, only case 2 in Theorem 4 holds for $n = 3$ people which shows the inequality proved in Theorem 3.2 must be strict for $n = 3$. For $n \geq 3$, there certainly exists a derangement described by case 2. So there will never be a case where only case 3 holds. This completes the proof. □

From this we see that person k is more likely to give a gift to the $k-1^{st}$ person than to anyone else drawing a name before k.

In the following proof, we consider those who draw names after the k^{th} person. We will find that person k is more likely to draw the last person's name than he is to draw the name of anyone else after k. It is important to note that this is different from our other proofs in that it compares conditional probabilities in which we know information about previous draws.

Theorem 3.4. *For $k < i < n, P(k \to n) \geq P(k \to i)$.*

Proof. Instead of comparing individual derangements, we will compare different ways that the first $k-1$ people could draw and look at who k is most likely to draw. By k's turn, there are three possible cases.
Case 1: If both i and n have already been drawn, then $P(k \to i) = P(k \to n) = 0$.
Case 2: If neither i nor n have been drawn, then k is equally likely to draw either. But if $k \to i$, then there is a chance that $n \to n$, causing a redraw. So for this case $P(k \to n) > P(k \to i)$.
Case 3: The final case is if only one of the two had been drawn. In this case, we can define a bijection from the ways i could be drawn first to the ways that n could be drawn first by switching which one was drawn first and leaving all other draws the same (note that we are pairing up ways the first k people could draw, not complete derangements). From equation 6, corresponding ways of the first k people drawing have equal probabilities, so $P(k \to i) = P(k \to n)$ for this case.
Therefore, $P(k \to n) \geq P(k \to i)$. □

The next theorem tells us that the k^{th} person is more likely to draw the first person than he is to draw the last person. Combined with our previous theorems, this tells us that each person is most likely to draw the name of the person right before him. The one special case is the first person, who is most likely to draw the last person's name.

Theorem 3.5. *For* $1 < k < n, P(k \to 1) \geq P(k \to n)$.

Proof. By symmetry, there are the same number of derangements where $k \to n$ as there are where $k \to 1$. We will pair these up bijectively by splitting them up into two separate cases. We will let A be the set of derangements where $k \to 1$ and let B denote the set of derangements where $k \to n$.

Case 1: Suppose that for some $\alpha \in A, \alpha(i) = n$ for some $1 < i < n$. We can map this α to the derangement $\beta \in B$ identical to α except that $\beta(k) = n$ and $\beta(i) = 1$ From equation (6), we see that $P(\alpha) = P(\beta)$.

Case 2: Now suppose $\alpha(1) = n$ and $\alpha(n) = x$ for some $1 < x < n$. In this case, we can map this α to the derangement $\beta \in B$ such that the only difference between α and β is that $\beta(1) = x$, $\beta(k) = n$, and $\beta(n) = 1$. From equation 6, we see that

$$P(\alpha) = \left(\frac{1}{n-x}\right) \prod_{j=1, j\neq x}^{n} \frac{1}{n-j+I_\alpha(j)}$$

and

$$P(\beta) = \left(\frac{1}{n-x+1}\right) \prod_{j=1, j\neq x}^{n} \frac{1}{n-j+I_\alpha(j)}.$$

So $P(\alpha) > P(\beta)$ for this case.

Since every derangement in A has a probability greater than or equal to the corresponding derangement in B, then the sum of the probabilities for A is greater than or equal to that of B. Therefore, $P(k \to 1) \geq P(k \to n)$. □

The previous three theorems tell us that the k^{th} person to draw is most likely to draw the $k-1^{\text{st}}$ person (and the first person is most likely to draw the last person). However, numerical simulations appear to indicate that the n^{th} person is more likely to draw the $n-1^{\text{st}}$ person than any other person is to draw the person before him. We will prove this in the next two theorems. Theorem 3.7 is the main result and Theorem 3.6 takes care of a special case. We prove the special case first because it is simpler and involves fewer subcases. The main result follows from a similar proof.

Theorem 3.6. *If there are n participants, then $P(n \to n-1) > P(1 \to n)$. This means that the last person is more likely to give to the second to last person than the first person is to give to the last person.*

Proof. Let A be the set of derangements where $n \to n-1$ and let B denote the set of derangements where $1 \to n$. Now suppose that $\alpha \in A$. We will map α to some $\beta \in B$ based on which of the following cases describes α.

Case 1: If $\alpha(1) = n$, then $\alpha = \beta$ for some $\beta \in B$. In this case, we map α to this β. Clearly, $P(\alpha) = P(\beta)$.

Case 2: Suppose that $\alpha(y) = n$ for some $1 < y < n-1$. Suppose $\alpha(1) = x$. Then we can map α to the corresponding derangement $\beta \in B$ where β is identical to α except that $\beta(1) = n, \beta(n) = x,$ and $\beta(y) = n-1$. Then, from equation (6), $P(\alpha)$ and $P(\beta)$ have the form (since $I_\beta(j) = I_\alpha(j)$ for $j \neq x, n-1$)

$$P(\alpha) = \left(\frac{1}{1}\right)\left(\frac{1}{n-x+1}\right)\prod_{j=1, j\neq x, n-1}^{n} \frac{1}{n-j+I_\alpha(j)}$$

and

$$P(\beta) = \left(\frac{1}{2}\right)\left(\frac{1}{n-x}\right)\prod_{j=1, j\neq x, n-1}^{n} \frac{1}{n-j+I_\alpha(j)}.$$

Since $x < n-1$, then algebra gives us

$$\frac{1}{2(n-x)} < \frac{1}{n-x+1}.$$

Then $P(\alpha) > P(\beta)$ for this case.

Case 3: Our last case is if $\alpha(n-1) = n$. Suppose $\alpha(y) = 1$ and $\alpha(1) = x$ (note that it is possible that $x = y$). In this case, we will map α to the $\beta \in B$ such that β is identical to α except that $\beta(1) = n, \beta(y) = n-1, \beta(n-1) = x,$ and $\beta(n) = 1$. Since applying equation (6) gives us the same equations for $P(\alpha)$ and $P(\beta)$ as in case 2, then $P(\alpha) > P(\beta)$ for this case as well.

Therefore, $P(n \to n-1) \geq P(1 \to n)$. □

Theorem 3.7. *For any $1 < k < n, P(n \to n-1) \geq P(k \to k-1)$.*

We already know that the k^{th} person is most likely to give a gift to the $k-1^{\text{st}}$ person. This proof shows that it is more likely that the last person gives a gift to the next to last person than it is for any other person k to give to the $k-1^{\text{st}}$ person.

Proof. We will give an outline for the proof of this theorem. The proof is similar to that for Theorem 7, but with 2 extra cases. Let $A = \{\alpha \in D_n : \alpha(n) = n-1\}$ and let $B = \{\beta \in D_n : \beta(k) = k-1\}$. The five cases for mapping α to a β are:
Case 1: If $\alpha(k) = k-1$, then $\beta = \alpha$. Then $P(\alpha) = P(\beta)$.
Case 2: If $\alpha(k) \neq n, n-1, k-1$ and $\alpha(y) = k-1$ for some $y \neq k-1, n-1$, then we map α to the β identical to α except that $\beta(k) = k-1$, $\beta(n) = \alpha(k)$ and $\beta(y) = n-1$. In this case we find that $P(\alpha) \geq P(\beta)$.
Case 3: This is similar to case 2 except that $\alpha(k) = n$ and $\beta(n) = k$. To ensure a one-to-one, onto map we let $\beta^{-1}(n) = \alpha^{-1}(k)$. For this case, $P(\alpha) \geq P(\beta)$.
Case 4: If $\alpha(n-1) = k-1$ and $\alpha(k) \neq n$, then we map α to a β such that $\beta(k-1) = n-1, \beta(n-1) = \alpha(k-1),$ and $\beta(n) = \alpha(k)$. Once again, $P(\alpha) \geq P(\beta)$.
Case 5: This is the same as case 4 except that $\alpha(k) = n$. We make a similar change in the mapping as we did to change from case 2 to case 3. As in the previous three cases, $P(\alpha) \geq P(\beta)$.
Using similar reasoning to our previous proofs, we find that $P(\alpha) > P(\beta)$ or $P(\alpha) = P(\beta)$ for each of these cases, so $P(n \to n-1) \geq P(k \to k-1)$. □

3.2 Summary

To summarize our results, we have shown that for the k^{th} person to draw, the order from most likely person for him to draw to least likely is the following:

$$k-1, k-2, k-3, ...3, 2, 1, n, (\text{ then } k+1 \text{ to } n-1 \text{ in some order}).$$

We also know that the most likely event in a gift exchange is for the last person to draw the next to last person. As an application, if some (slightly greedy) participant k has a very generous friend g whom k would like to receive a gift from, k may maximize the probability of being selected by g by letting g draw a name last and letting himself draw second to last. We can verify that this is true for the case $n = 4$.

Derangement	Probability	Derangement	Probability	Derangement	Probability
2143	1/9	3412	1/12	4321	1/12
2413	1/9	3142	1/12	4312	1/12
2341	1/18	3421	1/12	4123	1/6

In the above table, we have used the notation $WXYZ$ to imply that $1 \to W$, $2 \to X$, $3 \to Y$, and $4 \to Z$. The three most likely derangements all involve the last person giving to the third person, so this is clearly the most likely giver-recipient pair.

4 Further Work

More work may be done on the Secret Santa problem, particularly in the instance where people draw one at a time. We are confident, but have yet to prove that the k^{th} person is more likely to draw person i than he is to draw person $i+1$ when i and $i+1$ draw somewhere between $k+1$ and $n-1$ (inclusive). Another interesting problem would be to explore how probabilities change drawing one at a time when people are in families of various sizes. A third problem would be to study the value $R(n) = \frac{P(n \to n-1)}{1/(n-1)}$ for n people, which represents how many times more likely the last person is to draw the second to last than you would expect if all outcomes were equally likely. Calculations of $P(n \to n-1)$ for up to 11 people and approximations from simulations for up to 10000 people suggest that $R(n)$ increases as n increases and that $R(n) \to 2$ as $n \to \infty$. Furthermore, it appears (tentatively) that as $n \to \infty$, $\frac{P(n-k \to n-k-1)}{1/(n-1)} \to (k+2)/(k+1)$ for any $0 \leq k \leq n-2$. But at this point, all we have are numerical values from computer simulations that support this conjecture.

Finally, it might be possible to find alternative proofs that are simpler than those we have given for when people draw one at a time. One possible method might be using permanents of matrices to represent the probabilities. Let

$$A = \begin{pmatrix} 0 & 1/(n-1) & 1/(n-2) & \dots & 1/4 & 1/3 & 1/2 & 1 \\ 1/(n-1) & 0 & 1/(n-2) & \dots & 1/4 & 1/3 & 1/2 & 1 \\ 1/(n-1) & 1/(n-2) & 0 & \dots & 1/4 & 1/3 & 1/2 & 1 \\ 1/(n-1) & 1/(n-2) & 1/(n-3) & \dots & 1/4 & 1/3 & 1/2 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ 1/(n-1) & 1/(n-2) & 1/(n-3) & \dots & 0 & 1/3 & 1/2 & 1 \\ 1/(n-1) & 1/(n-2) & 1/(n-3) & \dots & 1/3 & 0 & 1/2 & 1 \\ 1/(n-1) & 1/(n-2) & 1/(n-3) & \dots & 1/3 & 1/2 & 0 & 1 \\ 1/(n-1) & 1/(n-2) & 1/(n-3) & \dots & 1/3 & 1/2 & 1 & 0 \end{pmatrix}.$$

Also, we will let $M_{i,j}$ represent the matrix formed by removing the i^{th} row and the j^{th} column of A. We will let $A_{i,j}$ denote the element in the i^{th} row and the j^{th} column of A.

We find that the probability of some derangement α on the first draw (allowing the last person to draw his own name) is equal to

$$P(\alpha) = \prod_{i=1}^{n} A_{i,\alpha(i)}.$$

Since permanents are used to calculate the sum of all permutations, it follows that

$$P(i \to j) = \frac{A_{i,j} * Per(M_{i,j})}{Per(A)}.$$

In addition to allowing easier computation of probabilities, this might allow for cleaner proofs using known properties of permanents instead of the lengthy proofs using our method.

References

[1] Barton, D.E., "The Matching Distributions: Poisson Limiting Forms and Derived Methods of Approximation". *Journal of the Royal Statistical Society.* Series B, 20(1): 73-92, 1958.

[2] Boyd, A.V., and J.N. Ridley, "The Return of Secret Santa". *The Mathematical Gazette*, 85(503):307-311, 2001.

[3] Grimaldi, Ralph P. *Discrete and Combinatorial Mathematics.* 4th ed. Boston: Addison Wesley Longman, 1998.

[4] Margolius, Barbara H. "The Dinner-Diner Matching Problem". *Mathematics Magazine*, 76(2): 107-118, 2003.

[5] McGuire, Kelly M., George Mackiw, and Christopher H. Morrell. "The Secret Santa Problem". *The Mathematical Gazette*, 83(498):467-472, 1999.

[6] Penrice, Stephen G., "Derangements, Permanents, and Christmas Presents". *The American Mathematical Monthly*, 98(7): 617-620, 1991.

[7] Schrijver, A. "A Short Proof of Minc's Conjecture." *Journal of Combinatorial Theory Series A*, 25(1978) 80-83.

[8] Van Lint, J.H. "Notes on Egoritchev's Proof of the Van der Waerden Conjecture." *Linear Algebra and Its Applications*, 39(1981) 1-8.

[9] Ward, Tony, "Difference Equations, Determinants and the Secret Santa Problem". *The Mathematical Gazette*, 89(514):2-6, 2005.

[10] White, Matthew J., "The Secret Santa Problem". *Rose-Hulman Institute of Technology Undergraduate Math Journal*, 7(1) (Paper 5), 2006.