The Secret Santa problem

Leo Liberti[1] and Franco Raimondi[2]

[1] *LIX, École Polytechnique, F-91128 Palaiseau, France*
liberti@lix.polytechnique.fr
[2] *Dept. of Computer Science, University College London, UK*
f.raimondi@cs.ucl.ac.uk

Abstract. Consider a digraph where the vertices represent people and an arc (i, j) represents the possibility of i giving a gift to j. The basic question we pose is whether there is an anonymity-preserving "gift assignment" such that each person makes and receives exactly one gift, and such that no person i can infer the remaining gift assignments from the fact that i is assigned to give a gift to j. We formalize this problem as a graph property involving vertex disjoint circuit covers, give a polynomial algorithm to decide this property for any given graph and provide a computational validation of the algorithm.

1 Introduction

The problem we deal with is well described by the following Wikipedia [14] entry:

> Secret Santa is a Christmas ritual involving a group of people exchanging anonymous gifts. Participants names are placed in a hat and each person draws a name for whom they are to buy a gift. Presents are then exchanged anonymously. There is usually a gift giving occasion, where all the presents are placed on a table, with the name of the receiver, but not the giver.

We assume that additional constraints may exist in the definition of the problem. For instance, it may be required that self-gifts and gifts between certain pairs of participants should be avoided. These constraints are enforced on a graph model: participants are represented by vertices and the possibility of a participant giving a gift to another participant is represented by an arc between the corresponding vertices.

Previous academic work on the Secret Santa problem is scarce. A secure protocol for the distributed solution of the Secret Santa problem is proposed in [11], with the corresponding implementation being described in [12]. Some published works in social sciences exist [3]. A scholarly discussion ensued in 1999-2001 in the *Mathematical Gazette* [7, 9, 1] focussing on the probability of picking a gift assignment without mutual gifts. This is extended in [8] to deal with more constraints on pairs of people that cannot exchange gifts, and in [13] to include at least a cyclic assignment of given length.

We use a digraph to model arbitrary constraints on the possibility of people exchanging gifts and propose a formalization of the Secret Santa problem as a decision problem on digraphs. Our main result is that the problem of determining whether anonymous gift assignments are possible on a given graph is in **P**. An investigation of anonymous communication channels along the lines of [2] provides further application-driven motivation for studying the Secret Santa problem.

An instance of the Secret Santa Problem is a connected digraph $G = (V, A)$ where V is the set of the participants, and $(i, j) \in A$ if participant i is allowed to make a gift to participant j. If symmetry is assumed (i.e., if we assume that if i can buy a gift for j then j can do the same for i) then A contains pairs of opposing arcs (i, j) and (j, i). In what follows, given a vertex $i \in V$, we let $\delta^+(i) = \{j \in V \mid (i, j) \in A\}$ and $\delta^-(i) = \{j \in V \mid (j, i) \in A\}$. An istance of the Secret Santa problem has a solution if for each person $i \in V$ there exists another assigned person $j \in V$ such that $(i, j) \in A$ such that i makes a gift to j (e.g. if $V| = \{1, 2\}$ and $A = \{(1, 2)\}$ there is no solution, for 2 has no assigned person). We model solutions as follows.

Definition 1.1 *A Vertex Disjoint Circuit Cover (VDCC) for $G = (V, A)$ is a subset $S \subseteq A$ of arcs of G such that: (a) for each $v \in V$ there is a unique $u \in V$, called the predecessor of v and denoted by $\pi_S(v)$, such that $(u, v) \in S$; (b) for each $v \in V$ there is a unique $u \in V$, called the successor of v and denoted by $\sigma_S(v)$, such that $(v, u) \in S$. We denote by $\mathcal{C}$ the set of all VDCCs in G.*

Let $x_{ij} \geq 0$ be real non-negative continuous variables for all $(i, j) \in A$, and consider the equations:

$$\forall i \in V \quad \sum_{j \in \delta^+(i)} x_{ij} = 1 \tag{1}$$

$$\forall i \in V \quad \sum_{j \in \delta^-(i)} x_{ji} = 1. \tag{2}$$

The support of any mapping $x^* : A \to \mathbb{R}^+$ satisfying (1)-(2) defines a VDCC (this follows by total unimodularity of the constraint matrix of (1)-(2)). Assuming G admits at least a VDCC, it is easy to see that x^* defines a permutation on $\{1, \ldots, |V|\}$ and therefore an assignment of maximum size on the undirected (bipartite) graph subjacent to the bipartite digraph $B = (U_1, U_2, A')$ where $U_1 = U_2 = V$ and A' are the same arcs as in A such that their heads are in U_1 and their tails in U_2. The best method for finding such an assignment is reported in [10] (Thm. 16.5) as $O(\nu(B)^{\frac{1}{2}}|A|)$, where $\nu(B)$ is the maximum size of a matching in B. Since in our case $\nu(G) = |V|$, we obtain a total (polynomial) worst-case complexity of $O(|V|^{\frac{1}{2}}|E|)$ for solving the VDCC.

Since gifts must be exchanged anonymously, not all VDCCs are acceptable: e.g. when $V = \{1, 2\}$ and $A = \{(1, 2), (2, 1)\}$, there is a unique VDCC given by $(x_{12}, x_{21}) = (1, 1)$, so each person knows that the other person will make them a gift. Informally, we define a graph G as a Secret Santa graph if it admits at

least a VDCC ensuring gift anonymity; i.e., if knowing a (donor,receiver) pair in the VDCC does not uniquely identify any other (donor,receiver) pair. Such a VDCC is an "acceptable" solution (precise definitions are given in Defn. 2.1).

The rest of the paper is organised as follows: in Section 2 we formalize the Secret Santa problem and discuss a few basic properties. In Section 3 we give a polynomial-time algorithm for deciding whether a given graph has the Secret Santa property or not. In Section 4 we discuss some computational results. Section 5 concludes the paper.

2 Characterisation of anonymity and basic results

Given a connected digraph $G = (V, A)$, let $n = |V|$ and $m = |A|$. We aim to characterize the set $\mathcal{S} \subseteq \mathcal{C}$ of "acceptable" solutions (i.e. anonymity-preserving VDCCs) formally: Secret Santa graphs are those for which $|\mathcal{S}| > 0$. The anonymity requirement on VDCCs reflects the notion of *ignorance* in epistemic logic [4], and is translated in graph-theoretical terms in the following definition.

Definition 2.1 *A graph G is a Secret Santa graph (SESAN) if there exists a VDCC S for G such that for each pair of distinct arcs $a, b \in S \cap A$, there is another VDCC T for G with $a \in T$ and $b \notin T$. The set*

$$\mathcal{V}(S) = \{S\} \cup \{T_{ab} \in \mathcal{C} \mid a \in S \cap T_{ab} \wedge b \in S \setminus T_{ab}\} \tag{3}$$

is a verification family for G, and S is a witness. Elements of a verification family are called acceptable solutions.

By the definition of SESAN, even if a participant knows his/her own gift assignment a, he/she does not gain any knowledge with respect to any other gift assignment b. We define $\mathcal{S}$ as the union of all verification families for G.

Proposition 2.2 *If the graph $G = (V, A)$ contains a vertex v such that $|\delta^-(v)| = 1$ or $|\delta^+(v)| = 1$ then G is not SESAN.*

Proof. Let $\delta^-(v) = \{(u)\}$ (the proof for $\delta^+(v)$ is the same). All VDCCs S will necessarily contain (u, v), thereby contradicting Defn. 2.1.

The converse to Prop. 2.2 is of course false: the complete digraph over three vertices is an example of a graph where $|\delta^-(i)| = |\delta^+(i)| = 2$ for each $i \in \{1, 2, 3\}$, but since there are only two possible VDCCs, G is not SESAN.

Lemma 2.3 *A verification family for $G = (V, A)$ contains at most $\tau(V) = |V|(|V| - 1) + 1$ VDCCs.*

Proof. This follows trivially from Eq. (3), as apart from S there is at most one VDCC for each pair of distinct arcs in S (the fact that $|S| = |V|$ follows trivially from (1)-(2)).

We formally define the Secret Santa problem as follows.

Definition 2.4 Secret Santa Problem *(SESANP). Given a graph* $G = (V, A)$*, decide whether it is SESAN.*

Notice that the SESANP asks for the existence of particular subgraphs (the VDCCs) whose added condition (anonymity) requires checking against $O(m^2)$ similar subgraphs. A naive approach of finding an arbitrary VDCC and then checking over all pairs of arcs whether it is acceptable might yield the answer NO without proving that the graph is not SESAN, for a different initial choice might have yielded a different answer. In order to make this approach work, one would need a complete enumeration of an exponentially large set (that of all VDCCs), suggesting that SESANP might be **NP**-complete. It turns out, however, that SESANP is in **P** (see Sect. 3).

2.1 Some examples

Consider the directed graph obtained from K_4 (in Fig. 1, left) by replacing edge edge with two antiparallel arcs. The second graph on from the left of Fig 1 is a possible witness; a verification family is displayed on the right, therefore the graph is SESAN.

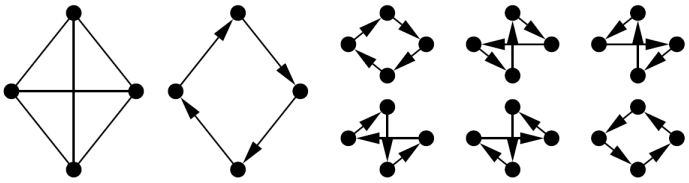

Fig. 1. K_4, a witness and its verification family.

Consider now the graph in Figure 2. This graph is SESAN: it is sufficient to take two equal solutions for K_4, as in Figure 1, to guarantee an acceptable solution. However, not all VDCCs for this graph are acceptable solutions. Indeed, on the right hand side of Figure 2, the arc (i, j) does not guarantee anonymity for the arc (j, i), because there is no other VDCC in which (i, j) appears, and (j, i) does not. In this case the set $\mathcal{S}$ is a proper subset of $\mathcal{C}$.

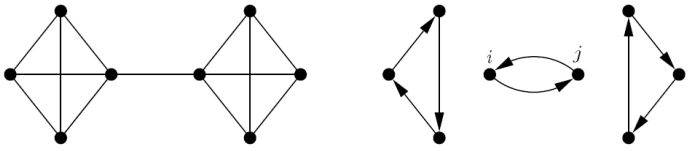

Fig. 2. An instance with two copies of K_4 and a non-anonymous VDCC.

3 A polynomial time algorithm

Algorithm 1 is a polynomial time algorithm for deciding whether a given graph is SESAN. The algorithm is based on the following observation: let T be a VDCC that does not guarantee anonymity. This implies that there exists an arc $a \in T$ such that, for some arc $b \in T$, all the VDCCs of G containing a also contain b. The key observation here is that *all* VDCCs of G containing a cannot satisfy the anonymity requirement (because of the necessary presence of b). The algorithm incrementally builds a set α of arcs that are not permitted and uses this set as additional constraints when looking for possible VDCCs. If no VDCC can be found satisfying the additional constraints given by α the graph is not SESAN.

Let P be the constraint satisfaction problem (1)-(2) such that $x \geq 0$. For $\alpha \subseteq A$ define P^α as P with the added constraints $x_{ij} = 0$ for each $(i,j) \in \alpha$. For given $(i,j),(k,l) \in A$ define P^α_{ijkl} as P^α with the added constraints $x_{ij} = 1$ and $x_{kl} = 0$. Recall $\mathcal{C}$ is the set of all VDCCs and $\mathcal{S}$ is the set of all acceptable solutions. Let $\mathcal{C}^\alpha$ (resp. $\mathcal{S}^\alpha$) be the set of all VDCCs (resp. acceptable solutions) not containing the arcs in α and let $\mathcal{C}^\alpha_{ijkl}$ (resp. $\mathcal{S}^\alpha_{ijkl}$) be the subset of $\mathcal{C}^\alpha$ (resp. $\mathcal{S}^\alpha$) containing (i,j) but not (k,l).

Lemma 3.1 *For any $\alpha \subseteq A$ and distinct $(i,j),(k,l) \in A$, if P^α_{ijkl} is infeasible then no acceptable solution in $\mathcal{S}^\alpha$ contains the arc (i,j).*

Proof. Since P^α_{ijkl} is infeasible, $\forall T \in \mathcal{C}^\alpha\ ((i,j) \in T \rightarrow (k,l) \in T)$, hence $\forall T \in \mathcal{C}^\alpha\ ((i,j) \in T \rightarrow T \notin \mathcal{S}^\alpha)$. This implies that $\forall S \in \mathcal{S}^\alpha\ ((i,j) \notin S)$.

Theorem 3.2 *Alg. 1 correctly solves the SESANP.*

Proof. By Lemma 3.1 and Line 13 in Alg. 1, no arc in α is contained in an acceptable solution. First assume G is SESAN and suppose Alg. 1 fails. This happens either when P^α is infeasible at Line 3 or when $|\alpha| > |A| - |V|$ at Line 2. The former case implies that $\mathcal{C}^\alpha = \emptyset$ and hence $\mathcal{S}^\alpha = \emptyset$, which means that all the acceptable solution must have an arc in α, a contradiction with the construction of α in Lines 11-12. The latter case would imply an acceptable solution with fewer than $|V|$ arcs, again a contradiction as $|T| = |V|$ for all $T \in \mathcal{C}$. Therefore the algorithm terminates with an acceptable solution. Assume now that G is not SESAN. Then for each $\alpha \subseteq A$ (and hence also the sets α generated during the algorithm run) there exist distinct $(i,j),(k,l) \in A$ such that P^α_{ijkl} is infeasible, i.e. $\mathcal{C}^\alpha_{ijkl} = \emptyset$. By Lines 11-12 and 3, the only possibility for $|\alpha|$ not to increase monotonically at each outer iteration is for P^α to be infeasible. Since $|\alpha|$ is bounded above by $|A| - |V|$, in either case the algorithm terminates with `IsSesan` = FALSE.

Note that P, P^α and P^α_{ijkl} are simply instances of the VDCC problem (i.e. the problem of determining whether a given graph has a VDCC) on graphs that are modifications of the original digraph G given by the forced absence of the arcs in α and (k,l) and by the forced presence of the arc (i,j): when these instances are infeasible, the maximum matching mentioned in Sect. 1 has size strictly smaller

Algorithm 1 Polynomial algorithm for solving the SESANP.

Require: $G = (V, A)$.
Ensure: Whether G is SESAN or not.
1: Let $\alpha = \emptyset$, `ExitLoop` = FALSE, `IsSesan` = FALSE
2: **while** $|\alpha| \leq |A| - |V|$ and `ExitLoop` = FALSE **do**
3: **if** P^α is feasible **then**
4: Let S be a solution to P^α
5: Let `ExitLoop` = TRUE
6: **else**
7: Let `IsSesan` = FALSE
8: exit While loop
9: **end if**
10: **for all** $(i, j), (k, l) \in S : (i, j) \neq (k, l)$ **do**
11: **if** P^α_{ijkl} is infeasible **then**
12: Let $\alpha \leftarrow \alpha \cup \{(i, j)\}$
13: Let `ExitLoop` = FALSE
14: exit For loop
15: **end if**
16: **end for**
17: **if** `ExitLoop` = TRUE **then**
18: Let `IsSesan` = TRUE
19: **end if**
20: **end while**
21: **if** `IsSesan` = TRUE **then**
22: G is SESAN
23: **else**
24: G is not SESAN
25: **end if**

than $|V|$. Solving $P, P^\alpha, P^\alpha_{ijkl}$ has the same worst-case polynomial complexity as finding a VDCC in G, namely $O(n^{\frac{1}{2}}m)$.

Lemma 3.3 *Alg. 1 has worst case $O(n^{\frac{5}{2}}m^2)$ time complexity.*

Proof. An n^2 term arises because of the internal loop on the distinct arcs in S (Line 10), as $|S| = |V|$. An m term arises because of the external loop (Line 2), and because $|\alpha|$ increases at each outer iteration (Line 13) unless the algorithm terminates. The remaining $n^{\frac{1}{2}}m$ term refers to the solution of each P^α_{ijkl} problem in Line 11.

Corollary 3.4 *SESANP is in* **P**.

4 Computational results

We tested Alg. 1 on a class of randomly generated graph instances. As the main target application of the SESANP is in communication protocols, communication

between any two agents (gifts between participants) is assumed to be bidirectional. Thus, we generated groups of 20 undirected random graphs with vertex set V and edge generation probability p for various values of $|V|$ and p, and then replaced each edge with two antiparallel directed arcs. Alg. 1 was implemented in AMPL [5] and the ILOG CPLEX 10.1 solver [6] was deployed on the VDCC sub-problems $P^{\alpha}, P^{\alpha}_{ijkl}$. This yields a practical algorithm that is nonpolynomial in the worst case but efficient on the average case, as we solved each sub-problem using the simplex method. Using CPLEX's barrier method yields a polynomial algorithm but is practically less efficient.

The plot in Fig. 3 refers to $|V| \in \{10i \mid 1 \leq i \leq 5\}$ and $p \in \{0.05i \mid 1 \leq i \leq 8\}$. The plot in Fig. 4 refers to $|V| \in \{10+5i \mid 0 \leq i \leq 6\}$ and $p \in \{0.04+0.02i \mid 0 \leq i \leq 10\}$. It took around 4h of user CPU time to solve the 2340 instances on an Intel Core Duo 1.2GHz and 1.5GB RAM running Linux. The plots suggest that the SESAN property is correlated to graph density and graph size.

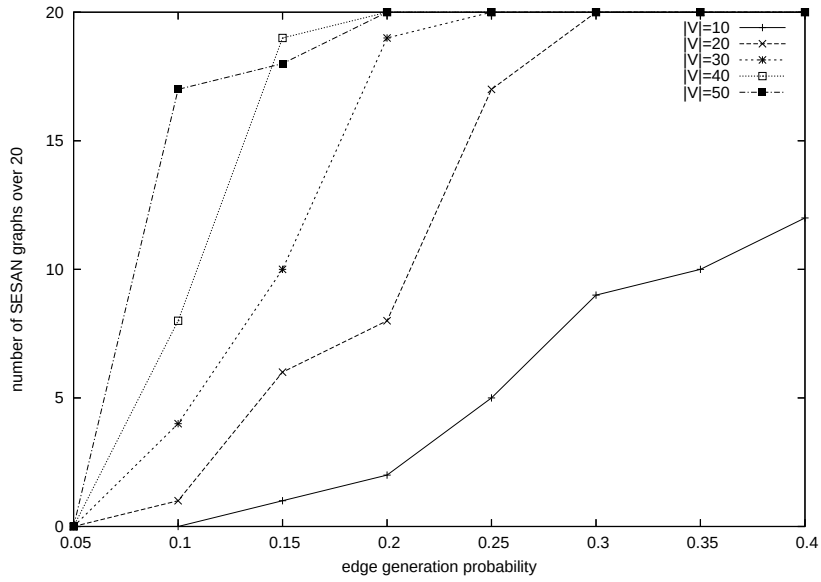

Fig. 3. Proportion of SESAN random graphs with p ranging in $[0.05, 0.4]$.

5 Conclusion

We formalized the Secret Santa problem as a decision problem related to finding subgraphs of a given graph with a particular structure (vertex-disjoint circuit covers) subject to an anonymity condition, and proved that it is in **P**. We pro-

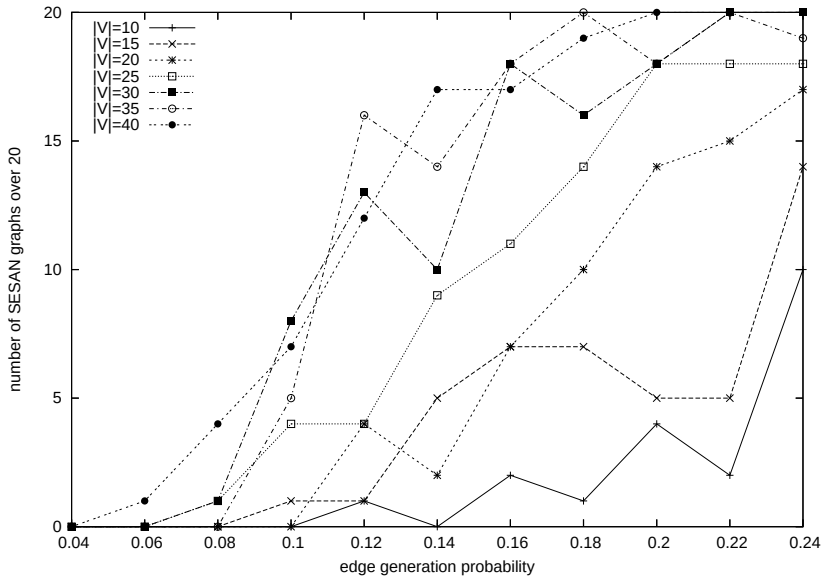

Fig. 4. Proportion of SESAN random graphs with p ranging in $[0.04, 0.24]$.

vided an $O(|V|^{\frac{5}{2}}|A|^2)$ polynomial algorithm and a limited computational study thereof.

Future work will focus on a generalized decision problem: given a graph, a particular graph structure and a particular anonymity property, are there families of subgraphs with the given structure that are anonymous according to the given property? A practical interest is attached, for example, to path-structured subgraphs in the study of networks providing anonymity of the source and/or intermediate vertices.

References

1. A.V. Boyd and J.N.Ridley. The return of Secret Santa. *Mathematical Gazette*, 85(503):307–311, 2001.
2. D. Chaum. The dining cryptographers problem: unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1):65–75, 1988.
3. B. Duncan. Secret Santa reveals the secret side of giving. Technical Report 0601, University of Colorado at Denver, 2006.
4. R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi. *Reasoning about Knowledge*. MIT Press, Cambridge, 1995.
5. R. Fourer and D. Gay. *The AMPL Book*. Duxbury Press, Pacific Grove, 2002.
6. ILOG. *ILOG CPLEX 10.1 User's Manual*. ILOG S.A., Gentilly, France, 2006.
7. K.M. McGuire, G. Mackiw, and C.H. Morrell. The Secret Santa problem. *Mathematical Gazette*, 83(498):467–472, 1999.

8. S. Penrice. Derangements, permanents and christmas presents. *American Mathematical Monthly*, 98(7):617–620, 1991.
9. R. Pinkham. The Secret Santa problem revisited. *Mathematical Gazette*, 85(502):96–97, 2001.
10. A. Schrijver. *Combinatorial Optimization: Polyhedra and Efficiency*. Springer, Berlin, 2003.
11. G. Tel. *Cryptografie, Beveiliging van de digitale maatschappij*. Addison-Wesley, 2002.
12. J. Verelst. Secure computing and distributed solutions to the Secret Santa problem. Master's thesis, Computer Science Dept., University of Utrecht, 2003.
13. M. White. The Secret Santa problem. *Rose-Hulman Institute of Technology Undergraduate Math Journal*, 7(1):paper 5, 2006.
14. Secret Santa. *Wikipedia*, `http://en.wikipedia.org/wiki/Secret_Santa`, 2006.