On 1-factorizations of Bipartite Kneser Graphs

Kai Jin[1][0000−0003−3720−5117]

The Hong Kong University of Science and Technology, Hong Kong SAR
cscjjk@gmail.com

Abstract. It is a challenging open problem to construct an explicit 1-factorization of the bipartite Kneser graph $H(v,t)$, which contains as vertices all t-element and $(v-t)$-element subsets of $[v] := \{1,\dots,v\}$ and an edge between any two vertices when one is a subset of the other. In this paper, we propose a new framework for designing such 1-factorizations, by which we solve a nontrivial case where $t=2$ and v is an odd prime power. We also revisit two classic constructions for the case $v=2t+1$ — the *lexical factorization* and *modular factorization*. We provide their simplified definitions and study their inner structures. As a result, an optimal algorithm is designed for computing the lexical factorizations. (An analogous algorithm for the modular factorization is trivial.)

Keywords: Graph Theory: 1-factorization · Modular factorization · Lexical factorization · Bipartite Kneser graph · Perpendicular Array.

1 Introduction

The *bipartite Kneser graph* $H(v,t)$ $(t < v/2)$ has as vertices all t-element and $(v-t)$-element subsets of $[v] := \{1,\dots,v\}$ and an edge between any two vertices when one is a subset of the other. Because it is regular and bipartite, each bipartite Kneser graph admits a 1-factorization due to Hall's Marriage Theorem [15]. (A 1-factor of a graph G is a subgraph in which each node of G has degree 1, and a 1-factorization of G partitions the edges of G into disjoint 1-factors.) For the special case $v=2t+1$, the graph $H(2t+1,t)$ is also known as the *middle level graph* and it admits two explicit 1-factorizations – the *lexical factorization* [17] (see subsection 1.2) and *modular factorization* [10] (see section 4). However, to the best of our knowledge, for decades it remains a challenging open problem to design explicit 1-factorizations for the general bipartite Kneser graphs.

In this paper, we propose a natural framework to attack the open problem. Briefly, it attempts to find a special kind of 1-factorizations called resolvable 1-factorizations. We noticed that the lexical and modular factorizations and any 1-factorization of $H(2t+1,t)$ are resolvable. We also checked (by a *C++* program) that there are no resolvable 1-factorization for $(v,t)=(6,2)$. Therefore, we can only expect for solving part of the open problem by using this framework.

As our main result, Theorem 1 states that finding a resolvable 1-factorization of $H(v,t)$ is equivalent to designing a special type of combinatorial designs, called perpendicular arrays [5,7]. In particular, $\mathsf{CPA}(t,t+d,2t+d)$, where $d=$

$v - 2t$. According to this theorem and by using the known perpendicular arrays found in [26,28], we obtain the first resolvable 1-factorizations of $H(v,t)$ when $t = 2$ and t is an odd prime power or when $(t,d) \in \{3,8\},\{3,32\}$. On the other direction, we use the lexical and modular factorizations to obtain the first explicit constructions of $\mathsf{CPA}(t,t+1,2t+1)$, which are known to be existed in [19].

In addition to the construction of the new factorizations, we conduct a comprehensive study of the existing factorizations of the middle level graph mentioned above, which serves as part of an ongoing effort to solve the general case.

First, we unveil an inner structure of the lexical factorization, which leads to not only the first constructive proof for the fact that the lexical factorization is well-defined, but also an optimal algorithm for the following computational problem: Given i and a t-element subset A, find the unique A' such that (A,A') belongs to the i-th 1-factor of the lexical factorization. The case $i = t+1$ of this problem was studied in [25]. For $i \leq t$ it becomes more difficult and a trivial algorithm takes $O(v^2)$ time in the RAM model (where an atomic operation on a word accounts $O(1)$ time). We improve it to optimal $O(v)$ time (in section 3). (An $O(v)$ time algorithm for this problem on modular factorization is trivial.)

Second, we propose an intuitive definition of the modular factorization (in section 4), which establishes an interesting connection between this factorization and the *inversion number of permutations* (section 5.3 of [18]). As it is simpler than the original definition in most aspects, a few existing results about the modular factorization become more transparent with this new definition.

Also, we prove properties called *variation laws* for the known 1-factorizations.

We will see the alternative definitions, inner structure, and variation laws are important for understanding the existing 1-factorizations. They have not been reported in literature and obtaining them requires nontrivial analysis.

1.1 Motivation & related work

A 1-factor of the bipartite Kneser graph is also known as an antipodal matching in the subset lattice. It is strongly related to the *set inclusion matrix* introduced in [30], which has connections to t-design in coding theory (see [3,12] and the references within). See [25] for its another application in coding theory.

The 1-factorization problem of the middle level graph was motivated by the *middle level conjecture*, which states that all the middle level graphs are Hamiltonian. It was hoped that people can find two 1-factors which form a Hamiltonian cycle [17]. Yet after extensive studies for thirty years the conjecture itself was settled by Mütze [21]; see also [14] for a recent and shorter proof and see [22] for an optimal algorithm for computing such a Hamiltonian cycle. Moreover, Mütze and Su [23] settles the Hamiltonian problem for all the bipartite Kneser graphs.

We give new applications of the 1-factorizations of $H(v,t)$ in hat-guessing games. We show that an optimal strategy in the unique-supply hat-guessing games can be designed from a 1-factorization of $H(v,t)$. To make the strategy easy to play, such a 1-factorization must be simple or at least admit an explicit construction. The details of this application are given in E due to space limits.

1.2 Preliminaries

The *subset lattice* is the family of all subsets of $[v]$, partially ordered by inclusion. Let $\mathcal{P}_t$ denote the t-th layer of this subset lattice, whose members are the t-element subsets of $[v]$. Throughout the paper, denote $d = v - 2t$. Let the words clockwise and counterclockwise be abbreviated as CW and CCW respectively.

A representation of the edges of $H(v,t)$. We identify each edge (A, A') of $H(v,t)$ by a permutation ρ of t $\bigcirc$'s, t $\triangle$'s, and d $\times$'s: the (positions of) t '$\bigcirc$'s indicate the t elements in A; the t '$\triangle$'s indicate the t elements that are **not** in A' (recall that A' has $v-t$ elements); and the '$\times$'s indicate those in $A' - A$. We do not distinguish the edges with their corresponding permutations.

Denote $[t\bigcirc, t\triangle, d\times]$ as the multiset of $2t+d$ characters with t '$\bigcirc$'s, t '$\triangle$'s, and d '$\times$'s. Giving a 1-factorization of $H(v,t)$ is equivalent to giving a **labeling function** f from the $\binom{2t+d}{t,t,d}$ permutations of $[t\bigcirc, t\triangle, d\times]$ to $1, \ldots, \binom{t+d}{d}$ so that

(a) $f(\rho) \neq f(\sigma)$ for those pairs ρ, σ who admit the same positions for t $\bigcirc$'s; and
(b) $f(\rho) \neq f(\sigma)$ for those pairs ρ, σ who admit the same positions for t $\triangle$'s.

If (a) and (b) hold, for fixed i, all edges labeled by i constitute a 1-factor, denoted by $F_{f,i}$, and $F_{f,1}, \ldots, F_{f,\binom{t+d}{d}}$ constitute a 1-factorization of $H(v,t)$.

An example of the labelling function that satisfies (a) and (b) is given in [17]:

The lexical factorization[17]. Let $\rho = (\rho_1, \ldots, \rho_{2t+1})$ be any permutation of $[t\bigcirc, t\triangle, 1\times]$. Arrange $\rho_1, \ldots, \rho_{2t+1}$ in a cycle in CW order. For any ρ_j that equals $\bigcirc$, it is *positive* if there are strictly more $\bigcirc$'s than $\triangle$'s in the interval that starts from the unique $\times$ and ends at ρ_j in CW order. The number of positive $\bigcirc$'s modular $t+1$ is defined to be $f_{\mathsf{LEX}}(\rho)$ (here, we restrict the remainder to $[t+1]$ by mapping 0 to $t+1$). See Fig. 1. It is proved in [17] that f_{LEX} satisfies the above conditions (a) and (b). We provide in section 3 a more direct proof for this. The lexical factorization is $\{\mathcal{L}_1, \ldots, \mathcal{L}_{t+1}\}$, where $\mathcal{L}_i = F_{f_{\mathsf{LEX}},i}$.

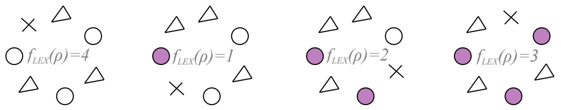


Fig. 1. Illustration of the definition of f_{LEX}. In the graph, the solid circles indicate positive $\bigcirc$'s. Note that the positions of $\bigcirc$'s are identical in all the permutations drawn here. As we see, the four permutations are mapped to different numbers under f_{LEX}.

Note: The original definition [17] of $f_{\mathsf{LEX}}(\rho)$ actually calculates the number of nonnegative $\triangle$'s rather than positive $\bigcirc$'s. For $\rho_j = \triangle$, it is said *nonnegative* if there the number of $\bigcirc$'s is no less than the number of $\triangle$'s in the interval that starts from the unique $\times$ and ends at ρ_j in CW order. Nevertheless, it is clear that the number of nonnegative $\triangle$'s is the same as the number of positive $\bigcirc$'s.

Note: The original definition [17] use $\mathcal{L}_0$ to denote $\mathcal{L}_{t+1}$. In this paper, however, we choose $\mathcal{L}_{t+1}$ instead of $\mathcal{L}_0$ to make it consistent with the case $d > 1$.

2 Construct "resolvable" 1-factorizations of $H(v,t)$

This section introduces resolvable 1-factorizations of $H(v,t)$ and constructs some of them using combinatorial designs called perpendicular arrays (defined below).

Definition 1. *Assume $\{g_A \mid A \in \mathcal{P}_t\}$ is a group of functions where g_A is a bijection from $A^C = [v] - A$ to $[t+d]$ for every $A \in \mathcal{P}_t$. Assume γ is a bijection from the set of all d-element subsets of $[t+d]$ to $1, \ldots, \binom{t+d}{d}$. We define a labeling function $f_{\gamma,g}$ on the edges of $H(v,t)$ as follows: $f_{\gamma,g}(A,A') := \gamma(g_A(A'-A))$.*

Note 1: Throughout, we use $g_A(X)$ to denote $\bigcup_{x \in X} g_A(x)$ for any $X \subseteq A^C$.
Note 2: Function $f_{\gamma,g}$ satisfies condition (a) trivially. Yet in most cases it does not satisfy condition (b) and hence does not define a 1-factorization of $H(v,t)$.

Definition 2. *Let f be the labelling function of a 1-factorization of $H(v,t)$. We say f is* resolvable *if there are $\{g_A \mid A \in \mathcal{P}_t\}$ and γ as mentioned in Definition 1 such that $f(A,A') \equiv \gamma(g_A(A'-A))$. In this case, we call g_A's for $A \in \mathcal{P}_t$ the* resolved functions *of f and we say the 1-factorization defined by f is* resolvable.

Remark 1. Among other merits which make the resolvable 1-factorizations more interesting than the general ones, a resolvable 1-factorization takes only $(t+d)$ over $\binom{t+d}{d}$ fraction of storing space comparing to a general 1-factorization.

The proofs of the following two lemmas are put into A due to space limits.

Lemma 1. *1. Any 1-factorization of $H(v=4,t=1)$ is resolvable.*
2. Any 1-factorization of $H(2t+1,t)$, including the lexical factorization and modular factorization, is resolvable. (This claim is actually trivial.)
3. No 1-factorization of $H(6,2)$ is resolvable. (Will be proved by a program.)

As shown by Lemma 1, there could be $H(v,t)$'s without a resolvable 1-factorization, hence we are not always able to design a resolvable 1-factorization of $H(v,t)$. Nevertheless, the first two claims of Lemma 1 and the results given in the rest part of this section point out that for several cases we can do so.

Lemma 2. *Given $\{g_A \mid A \in \mathcal{P}_t\}$ and γ as above, the following are equivalent:*

(i) function $f_{\gamma,g}(A,A')$ satisfies condition (b); and
(ii) When $A_1 \neq A_2$ and $(A_1,A_1'),(A_2,A_2')$ are two edges in $H(v,t)$, then $g_{A_1}(A_1'-A_1) = g_{A_2}(A_2'-A_2)$ implies that $A_1' \neq A_2'$.

By Lemma 2, it is independent with the choice of γ whether $f_{\gamma,g}(A,A')$ defines a 1-factorization of $H(v,t)$. Therefore, if we want to design a resolvable 1-factorization, the difficulty lies in and only lies in designing $\{g_A \mid A \in \mathcal{P}_t\}$.

By Lemma 2 and Definition 1, $H(v,t)$ has a resolvable factorization if and only if there exist resolved functions $\{g_A \mid A \in \mathcal{P}_t\}$ such that for $A_1 \neq A_2$, $g_{A_1}(A_1'-A_1) = g_{A_2}(A_2'-A_2)$ implies $A_1' \neq A_2'$. The following theorem shows that finding such functions is equivalent to designing some perpendicular arrays.

A *perpendicular array* [5,7] with parameters t, k, v, denoted by $\mathsf{PA}(t, k, v)$, is a $\binom{v}{t} \times k$ matrix over $[v]$, where each row has k distinct numbers and each set of t columns contain each t-element subset of $[v]$ as a row exactly once.

For $d \geq 0$, a $\mathsf{PA}(t, t+d, 2t+d)$ is *complete*, hence denoted by $\mathsf{CPA}(t, t+d, 2t+d)$, if each $(t+d)$-element subset of $[2t+d]$ is also contained in exactly one row.

Theorem 1. *$H(2t+d, t)$ has a resolvable 1-factorization* $\Leftrightarrow \exists \mathsf{CPA}(t, t+d, 2t+d)$.

Proof. $\Rightarrow$: Assume f is the labeling function of a resolvable 1-factorization of $H(v = 2t+d, t)$. Then, $f(A, A') \equiv \gamma(g_A(A' - A))$ for some resolved functions $\{g_A \mid A \in \mathcal{P}_t\}$ and a bijection γ as mentioned in Definition 1.

We construct a matrix M over $[v]$ as follows. For each $A \in \mathcal{P}_t$, we build a row $(a_1^{(A)}, \ldots, a_{t+d}^{(A)})$ in M, where $a_i^{(A)} = g_A^{-1}(i)$ (which belongs to A^C and thus belongs to $[v]$). As $\mathcal{P}_t$ has $\binom{v}{t}$ elements, the size of matrix M is $\binom{v}{t}$ by $k = t+d$.

We now verify that M is a $\mathsf{PA}(t, t+d, 2t+d)$. First, since g_A^{-1} is bijective, $a_1^{(A)}, \ldots, a_{t+d}^{(A)}$ are distinct and so each row of M contains $k = t+d$ distinct numbers. Next, for any t columns $i_1, \ldots, i_t$, we show that

$$\{a_{i_1}^{(A_1)}, \ldots, a_{i_t}^{(A_1)}\} \neq \{a_{i_1}^{(A_2)}, \ldots, a_{i_t}^{(A_2)}\} \tag{1}$$

for any distinct $A_1, A_2 \in \mathcal{P}_t$. Assume $\{j_1, \ldots, j_d\} = [t+d] - \{i_1, \ldots, i_t\}$.

Let $A_1' = A_1 \biguplus \{g_{A_1}^{-1}(j_1), \ldots, g_{A_1}^{-1}(j_d)\}$ and $A_2' = A_2 \biguplus \{g_{A_2}^{-1}(j_1), \ldots, g_{A_2}^{-1}(j_d)\}$. Clearly, $g_{A_1}(A_1' - A_1) = \{j_1, \ldots, j_d\} = g_{A_2}(A_2' - A_2)$, thus $A_1' \neq A_2'$ by Lemma 2. Thus $[v] - A_1' \neq [v] - A_2'$. Because $\{j_1, \ldots, j_d\} \biguplus \{i_1, \ldots, i_t\} = [t+d]$, we know $A_1^C = \{g_{A_1}^{-1}(j_1), \ldots, g_{A_1}^{-1}(j_d)\} \biguplus \{g_{A_1}^{-1}(i_1), \ldots, g_{A_1}^{-1}(i_t)\}$, which implies that $[v] - A_1' = \{g_{A_1}^{-1}(i_1), \ldots, g_{A_1}^{-1}(i_t)\}$. Similarly, $[v] - A_2' = \{g_{A_2}^{-1}(i_1), \ldots, g_{A_2}^{-1}(i_t)\}$. Altogether, $\{g_{A_1}^{-1}(i_1), \ldots, g_{A_1}^{-1}(i_t)\} \neq \{g_{A_2}^{-1}(i_1), \ldots, g_{A_2}^{-1}(i_t)\}$, i.e., (1) holds.

Next, we argue that M is a $\mathsf{CPA}(t, t+d, 2t+d)$. This reduces to proving that each row of M forms a distinct $(t+d)$-element subset of $[2t+d]$, which follows from the fact that the row constructed from A is a permutation of A^C.

$\Leftarrow$: Assume M is a $\mathsf{CPA}(t, t+d, 2t+d)$. First, we construct $\{g_A \mid A \in \mathcal{P}_k\}$. For any row $(a_1, \ldots, a_{t+d})$ of M, assuming that $A^C = \{a_1, \ldots, a_{t+d}\}$, define $g_A(a_i) = i$ for $i \in [t+d]$. Obviously, each g_A for $A \in \mathcal{P}_k$ is defined exactly once.

Below we verify that when $A_1 \neq A_2$, equality $g_{A_1}(A_1' - A_1) = g_{A_2}(A_2' - A_2)$ would imply $A_1' \neq A_2'$. According to Lemma 2, this further implies that for any γ as mentioned in Definition 1, $f_{\gamma,g}(A, A')$ is a labeling function satisfying conditions (a) and (b), and hence $H(2t+d, t)$ has a resolvable 1-factorization.

Suppose to the opposite that $g_{A_1}(A' - A_1) = g_{A_2}(A' - A_2) = \{j_1, \ldots, j_d\}$. Assume $\{i_1, \ldots, i_t\} = [t+d] - \{j_1, \ldots, j_d\}$. Because $g_{A_1}(A' - A_1) = \{j_1, \ldots, j_d\}$, we know $g_{A_1}([v] - A') = \{i_1, \ldots, i_t\}$, so $[v] - A' = \{g_{A_1}^{-1}(i_1), \ldots, g_{A_1}^{-1}(i_t)\}$. Similarly, because $g_{A_2}(A' - A_2) = \{j_1, \ldots, j_d\}$, we get $[v] - A' = \{g_{A_2}^{-1}(i_1), \ldots, g_{A_2}^{-1}(i_t)\}$. Moreover, because M is a $\mathsf{PA}(t, t+d, 2t+d)$ where $\{g_{A_1}^{-1}(i_1), \ldots, g_{A_1}^{-1}(i_t)\}$ and $\{g_{A_2}^{-1}(i_1), \ldots, g_{A_2}^{-1}(i_t)\}$ appear in two rows of M in the columns indexed by $i_1, \ldots, i_t$, these two sets are distinct. Thus $[v] - A' \neq [v] - A'$. Contradiction. □

2.1 Applications of Theorem 1

Lemma 3. *1. For $t = 1$, there is always a $\mathsf{PA}(t, 2t + d, 2t + d)$. (trivial)*
2. [26] For $t = 2$ and an odd prime power $2t + d$, there is a $\mathsf{PA}(t, 2t + d, 2t + d)$.
3. [28] For $t = 3$ and $2t + d \in \{8, 32\}$, there is a $\mathsf{PA}(t, 2t + d, 2t + d)$.

The following lemma is trivial and its proof can be found in A.

Lemma 4. *Any $t+d$ columns of a $\mathsf{PA}(t, 2t+d, 2t+d)$ form a $\mathsf{CPA}(t, t+d, 2t+d)$.*

Lemma 4 points out a way to construct a $\mathsf{CPA}(t, t+d, 2t+d)$. Yet it is unknown whether every $\mathsf{CPA}(t, t+d, 2t+d)$ can be constructed this way. We conjecture so. If so, finding resolvable 1-factorizations reduces to finding $\mathsf{PA}(t, 2t + d, 2t + d)$'s.

The following is a corollary of Lemma 3, Lemma 4, and Theorem 1.

Corollary 1. *Graph $H(2t + d, t)$ has a resolvable 1-factorization when 1. $t = 1$, or 2. ($t = 2$ and $2t+d$ is an odd prime power), or 3. ($t = 3$ and $2t+d \in \{8, 32\}$).*

The constructions of $\mathsf{PA}(t, 2t + d, 2t + d)$ for those pairs of (t, d) discussed in Lemma 3 are explicit and quite simple (see [26,28]). Also, our construction of the resolvable 1-factorization of $H(2t + d, t)$ using a $\mathsf{CPA}(t, t + d, 2t + d)$ is extremely simple (as shown in the proof of Theorem 1). As a result, the resolvable 1-factorizations of $H(2t+d, t)$ mentioned in this corollary are explicit and simple.

Perpendicular arrays have not been studied extensively in literature. In addition to the existence results mentioned in Lemma 3, there do exist $\mathsf{PA}(3, 5, 5)$ and $\mathsf{PA}(t, t + 1, 2t + 1)$ ($t \geq 1$) and some other perpendicular arrays. Yet the construction of $\mathsf{PA}(t, t+1, 2t+1)$ (in [19]) is not explicit and thus not too useful (regarding that we are only interested in explicit factorizations of $H(2t + 1, t)$). A $\mathsf{PA}(3, 5, 5)$ is also useless to us since $5 < 2 \times 3$. Because a $\mathsf{CPA}(t, t + d, 2t + d)$ automatically implies a resolvable 1-factorization of $H(v, t)$, we hope that our results motivate more study on the perpendicular arrays in the future.

Another application of Theorem 1 — construction of $\mathsf{CPA}(t, t + 1, 2t + 1)$. As shown in Lemma 1.2, the lexical and modular factorization of $H(2t + 1, t)$ are both resolvable. The resolved functions of f_{LEX} and f_{MOD} will be demonstrated in the next sections. Using these resolved functions and applying the proof of Theorem 1, we can easily construct two $\mathsf{CPA}(t, t + 1, 2t + 1)$s. Therefore, as byproducts, we obtain (the first) explicit constructions of (complete) $\mathsf{PA}(t, t + 1, 2t + 1)$ (note that [19] only showed the existence of $\mathsf{PA}(t, t + 1, 2t + 1)$).

3 Revisit the lexical factorization

Recall f_{LEX} in subsection 1.2, which is a labeling function of $H(2t + 1, t)$. In this section, we first give $\{g_A\}$ of γ so that $f_{\mathsf{LEX}} = f_{\gamma,g}$. Based on this formula we then show that f_{LEX} satisfies (a) and (b) and thus that it indeed defines a 1-factorization. Moreover, by applying $f_{\mathsf{LEX}} = f_{\gamma,g}$, we design optimal algorithms for solving two fundamental computational problems about this factorization (P1 and P2 below). Finally, we introduce a group of *variation laws* of f_{LEX}.

P1. Given $A \in \mathcal{P}_t$ and $i \in \{1, \ldots, t+1\}$, how do we find the unique A' so that $(A, A') \in \mathcal{L}_i$? In other words, given number i and the positions of $\bigcirc$'s in ρ and suppose $f_{\mathsf{LEX}}(\rho) = i$, how do we determine the position of $\times$ in ρ?

P2. Given a $A' \in \mathcal{P}_{t+1}$ and $i \in \{1, \ldots, t+1\}$, how do we find the unique A so that $(A, A') \in \mathcal{L}_i$? In other words, given number i and the positions of $\triangle$'s in ρ and suppose $f_{\mathsf{LEX}}(\rho) = i$, how do we determine the position of $\times$ in ρ?

3.1 Preliminary lemmas

The two lemmas given in this subsection are trivial; proofs can be found in B.

Given $S = (s_1, \ldots, s_v)$, the j-th $(0 \leq j < v)$ *cyclic-shift* of S is $S^{(j)} := (s_{1+j}, \ldots, s_{v+j})$, where subscripts are taken modulo v (and restricted to $[v]$).

Lemma 5. *Given any sequence S of t of right parentheses ')' and $t+1$ left parentheses '('. There exists a unique cyclic-shift $S^{(j)}$ of S whose first $2t$ parentheses are paired up when parenthesized, and we can compute j in $O(t)$ time.*

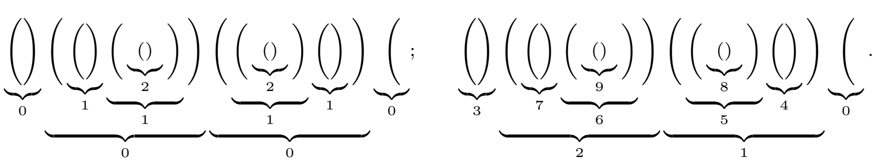
Example 1. Assume $t = 9$, $S = (_1(_2)_3)_4)_5(_6(_7(_8)_9)_{10}(_{11})_{12})_{13}(_{14}(_{15})_{16}(_{17}(_{18})_{19}$.
The unique cyclic-shift in which the first $2t$ parentheses are paired up is:

$$S^{(14)} = \Big(_{15}\Big)_{16}\Big(_{17}\Big(_{18}\Big)_{19}\Big(_{1}(_{2})_{3}\Big)_{4}\Big)_{5}\Big(_{6}\Big(_{7}(_{8})_{9}\Big)_{10}\Big(_{11}\Big)_{12}\Big)_{13}\Big(_{14}.$$

Definition 3. *Given $S = (s_1, \ldots, s_{2t+1})$, t of which are ')' and $t+1$ are '('. It is said* canonical *if its first $2t$ parentheses are paired up when parenthesized.*

Definition 4 (Indices of the $2t+1$ parentheses). *For any canonical parentheses sequence S, we index the $t+1$ left parentheses in S by $0, \ldots, t$ according to the following rule:* ***The smaller the depth, the less the index; and index from right to left for those under the same depth.*** *Here, depth is defined in the standard way; it is the number of pairs of matched parentheses that cover the fixed parenthesis. Moreover,* ***we index the t right parentheses in such a way that any two paired parentheses have the same index.***

For $S^{(14)}$ above, the depth and index are shown below (index on the right).



This definition of indices is crucial to the next lemma and the entire section. For convenience, denote by $\mathsf{depth}(s_i), \mathsf{index}(s_i)$ the depth and index of s_i.

Lemma 6. *When S is canonical, for any $s_l = ($ and $s_r =)$, there are more $)$'s than $($'s in the cyclic interval $\{s_{l+1}, \ldots, s_r\}$ if and only if $\mathsf{index}(s_l) \geq \mathsf{index}(s_r)$.*

3.2 Finding resolved functions $\{g_A\}$ of f_{LEX}

Parenthesis representation. We can represent any $A \subseteq [v]$ by a sequence of parentheses $S = (s_1, \dots, s_v)$ where $s_x =')'$ if $x \in A$ and $s_x =' ('$ if $x \notin A$. For example, $A = \{3, 4, 5, 9, 10, 12, 13, 16, 19\}$ is represented by the S given in Example 1 above. Notice that if $A \in \mathcal{P}_t$, its associate sequence S contains t ')'s.

Definition 5. *Fix $A \in \mathcal{P}_t$ and let S denote its parentheses sequence. We abuse* $\mathsf{index}(s_x)$ *to mean the index of s_x in the unique canonical cyclic-shift of S (uniqueness is by Lemma 5). For any $x \in A^C$ (hence $s_x =' ('$), define $g_A(x) :=$* $\mathsf{index}(s_x)$ *mod* $(t+1)(\in [t+1])$ *(restrict to $[t+1]$ by mapping 0 to $t+1$).*

Because left parentheses have distinct indices, g_A is a bijection as required.

Theorem 2. *Let γ be the natural bijection from all the 1-element subsets of $[t+1]$ to $[t+1]$, which maps $\{x\}$ to x. Define $\{g_A \mid A \in \mathcal{P}_t\}$ as in Definition 5. Then, $f_{\mathsf{LEX}} = f_{\gamma,g}$. In other words, $f_{\mathsf{LEX}}(A, A \cup \{x\}) \equiv g_A(x)$ $(x \in A^C)$.*

Proof. Build the parentheses sequence $S = (s_1, \dots, s_{2t+1})$ of A and the permutation $\rho = (\rho_1, \dots, \rho_{2t+1})$ of $[t\bigcirc, t\triangle, 1\times]$ corresponding to edge $(A, A \cup \{x\})$. Recall that $f_{\mathsf{LEX}}(A, A \cup \{x\}) := p \bmod (t+1) \in [t+1]$, where p is the size of $P = \{\rho_r = \bigcirc \mid \text{there are more } \bigcirc\text{s than } \triangle\text{s in the cyclic interval } (\rho_{x+1}, \dots, \rho_r)\}$. Observe that S can be constructed from ρ by replacing $\bigcirc, \triangle, \times$ to ')','(','('. So, $\{s_r =')' \mid \text{there are more } ')'\text{s than } '('\text{s in the cyclic interval } (s_{x+1}, \dots, s_r)\}$, which equals $\{s_r =')' \mid \mathsf{index}(s_x) \geq \mathsf{index}(s_r)\}$ by Lemma 6 (indices refer to those in the canonical cyclic-shift of S), has the same size as P, so $\mathsf{index}(s_x) = p$. Further by Definition 5, $g_A(x) = \mathsf{index}(s_x) \bmod (t+1)(\in [t+1]) = f_{\mathsf{LEX}}(A, A \cup \{x\})$.

Theorem 3. *f_{LEX} satisfies conditions (a) and (b).*

Proof. Because f_{LEX} equals $f_{\gamma,g}$, applying Note 2 below Definition 1, this labeling function satisfies condition(a). Below we prove that it also satisfies condition (b).

Define the *dual* of ρ, denoted by ρ^*, to be another permutation of $[t\bigcirc, t\triangle, 1\times]$ which is constructed from ρ by swapping the $\triangle$'s with $\bigcirc$'s. As illustrated in Fig. 2, we have (i): $f_{\mathsf{LEX}}(\rho^*) \bmod (t+1) + f_{\mathsf{LEX}}(\rho) \bmod (t+1) = t$ for any ρ .

Consider $t+1$ distinct permutations $\rho^0, \dots, \rho^t$ sharing the same positions of $\triangle$'s. Then, $(\rho^0)^*, \dots, (\rho^t)^*$ share the same positions of $\bigcirc$'s. Using condition (a), $f_{\mathsf{LEX}}((\rho^0)^*), \dots, f_{\mathsf{LEX}}((\rho^t)^*)$ are distinct. So $t - f_{\mathsf{LEX}}((\rho^0)^*) \bmod (t+1), \dots, t - f_{\mathsf{LEX}}((\rho^t)^*) \bmod (t+1)$ are distinct. So $f_{\mathsf{LEX}}(\rho^0) \bmod (t+1), \dots, f_{\mathsf{LEX}}(\rho^t) \bmod (t+1)$ are distinct by (i), i.e., $f_{\mathsf{LEX}}(\rho^0), \dots, f_{\mathsf{LEX}}(\rho^t)$ are distinct. Thus (b) holds. □

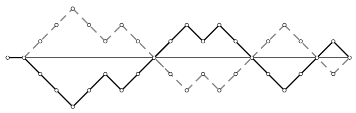


Fig. 2. $f_{\mathsf{LEX}}(\rho^*) \bmod (t+1) + f_{\mathsf{LEX}}(\rho) \bmod (t+1) = t$. The dashed line indicates ρ^*.

Remark 2. In the original proof of Theorem 3 in [17], it proves the existence of bijections g_A's ($A \in \mathcal{P}_t$) such that $f_{\mathsf{LEX}} = f_{\gamma,g}$, yet how to define such g_A's is neither explicitly given, nor implicitly given. As we have seen in Definition 4, giving this definition is not easy, even though the definition of f_{LEX} is known.

There are two advantages of having explicit $\{g_A\}$. First, the ideas we used in defining g_A could be useful in finding resolvable 1-factorizations for the case $v > 2t+1$. Second, to solve P1 and P2 (in the next subsection), it seems necessary to have an explicit definition of $\{g_A\}$ for the efficiency of computation.

3.3 Linear Time Algorithms for P1 and P2

Problem P1 admits a trivial $O(t^2)$ time solution as follows. Given the positions of $\bigcirc$'s in ρ and the number i, we can enumerate the position of the unique $\times$ among the remaining $t+1$ positions and compute $f_{\mathsf{LEX}}(\rho)$ in $O(t)$ time, until that the computed value is i. Problem P2 can be solved symmetrically.

Applying the results in subsection 3.2, we can solve P1 much more efficiently. Briefly, using those indices of parentheses in Definition 4, we can compute $f_{\mathsf{LEX}}()$ for all permutations $\rho^0, \ldots, \rho^t$ in which the positions of $\bigcirc$'s are as given altogether, and then find ρ^j so that $f_{\mathsf{LEX}}(\rho^j) = i$. See the details in Algorithm 1.

```
Input: A set $A \in \mathcal{P}_t$ and a number $i \in [t+1]$.
Output: The set $A' = A \cup \{z\}$ so that $(A, A') \in \mathcal{L}_i$.
    (Integer $z$ indicates the position of $\times$ so that $f_{\mathsf{LEX}}(\rho) = i$.)
Compute the parentheses sequence $S$ of $A$.
Compute the unique $j$ so that the first $2t$ parentheses are paired up in $S^{(j)}$.
Compute the indices of all parentheses in $S' = S^{(j)}$ according to Definition 4.
Find $s'_{z-j} =' ('$ in $S$ with index $(i \bmod (t+1))$ and output $A' = A \cup \{z\}$.
```

Algorithm 1: Computing the unique A' such that $(A, A') \in \mathcal{L}_i$.

Theorem 4. *1. Given a canonical S', we can compute the indices of all parentheses in S' in $O(t)$ time. Therefore, Algorithm 1 solves P1 in $O(t)$ time.*

2. An instance (A', i) of P2 reduces to the instance $([v] - A', j)$ of P1, where i mod $(t+1) + j$ mod $(t+1) = t$. Thus P2 can be solved in $O(t)$ time.

The proof of Theorem 4 is trivial and is omitted due to space limits.

3.4 Variation laws of f_{LEX}

We prove some *variations laws* of f_{LEX} as summarized in Lemma 7, which are comparable to the laws of modular factorization given below in Lemma 9. See B.1 for the details, including the definitions of $\rho^{\times\rightarrowtail\triangle}$, $\rho^{\times\rightarrowtail\bigcirc}$, $\rho^{\bigcirc\leftarrowtail\times}$, and $\rho^{\triangle\leftarrowtail\times}$.

Lemma 7 (Variation laws of f_{LEX}). *Restrict the remainder to $[t+1]$ here.*
When $f_{\mathsf{LEX}}(\rho) \neq t+1$, $f_{\mathsf{LEX}}(\rho^{\times\rightarrowtail\triangle}) = f_{\mathsf{LEX}}(\rho^{\bigcirc\leftarrowtail\times}) = (f_{\mathsf{LEX}}(\rho) - 1)$ mod $(t+1)$.
When $f_{\mathsf{LEX}}(\rho) \neq t$, $f_{\mathsf{LEX}}(\rho^{\times\rightarrowtail\bigcirc}) = f_{\mathsf{LEX}}(\rho^{\triangle\leftarrowtail\times}) = (f_{\mathsf{LEX}}(\rho) + 1)$ mod $(t+1)$.

4 Revisit the modular factorization

This section presents a new and simpler definition of the modular factorization. When a number modulo $t+1$ in this section, the remainder is restricted to $[t+1]$.

The modular factorization[10]. The modular factorization was originally given by $t+1$ 1-factors $\mathcal{M}_1, \ldots, \mathcal{M}_{t+1}$ where $\mathcal{M}_i$ was defined as follows. Consider $A \in \mathcal{P}_t$. Let ΣA indicate the sum of elements in A. Let $y = (\Sigma A + i) \bmod (t+1) (\in [t+1])$. Then, $\mathcal{M}_i(A) := A \cup \{z\}$, where z is the y-th **largest** element in $[v] - A$.

Take $t = 3, v = 7$, and $A = \{2, 4, 6\}$ for example:

For $i = 1$, we have $y = 13 = 1 \pmod 4$ and $z = 7$. So $\mathcal{M}_1(A) = \{2, 4, 6, 7\}$.
For $i = 2$, we have $y = 14 = 2 \pmod 4$ and $z = 5$. So $\mathcal{M}_2(A) = \{2, 4, 5, 6\}$.
For $i = 3$, we have $y = 15 = 3 \pmod 4$ and $z = 3$. So $\mathcal{M}_3(A) = \{2, 3, 4, 6\}$.
For $i = 4$, we have $y = 16 = 4 \pmod 4$ and $z = 1$. So $\mathcal{M}_4(A) = \{1, 2, 4, 6\}$.

Note 1. It is proved in [10] that $\mathcal{M}_i$ is a 1-factor for each i $(1 \leq i \leq t+1)$. Moreover, it is obvious that all the 1-factors $\mathcal{M}_1, \ldots, \mathcal{M}_{t+1}$ are pairwise-disjoint.

Note 2. The origins of modular factorization are murky, said by the authors of [10], who credited it to Robinson, who asked if it is the same as the lexical one.

Note 3. Assume $\mathcal{M}_i(A) = A'$. We can compute A from i and A' symmetrically. Let $x = (\Sigma A' + i) \bmod (t+1) (\in [t+1])$ where $\Sigma A'$ indicates the sum of elements in A'. Then $A = A' - \{z\}$, where z is the x-th **smallest** element in A' [10]. Thus, the problems on modular factorizations analogous to P1 and P2 are easy to solve.

The original definition of the modular factorization above does not explicitly give its labeling function. Such a labeling function will be needed in analyzing the variation laws of the above modular factorization in Lemma 9 below and hence we state it Lemma 8. However, our definition of the modular factorization is **not** given by Lemma 8. The proof of Lemma 8 can be found in C.

Consider any permutation $\rho = (\rho_1, \ldots, \rho_{2t+1})$ of $[t\bigcirc, t\triangle, 1\times]$. For each $i \in [2t+1]$, the *position* of ρ_i is i. Let $O_1^\rho, \ldots, O_t^\rho$ be the positions of t $\bigcirc$'s in ρ and $T_1^\rho, \ldots, T_t^\rho$ the positions t $\triangle$'s. Denote by $\mathsf{rank}^{\circlearrowleft}_{\triangle}(\rho)$ the rank of $\times$ when enumerating all $\triangle$'s and $\times$ in ρ from ρ_{2t+1} back to ρ_1. So, $\mathsf{rank}^{\circlearrowleft}_{\triangle}(\rho) - 1$ is the number of $\triangle$'s with positions larger than the position of $\times$. Denote by $\mathsf{rank}^{\circlearrowleft}_{\bigcirc}(\rho)$ the rank of $\times$ when enumerating all $\bigcirc$'s and $\times$ in ρ from ρ_{2t+1} back to ρ_1.

Lemma 8. *The labeling function of* $\{\mathcal{M}_1, \ldots, \mathcal{M}_{t+1}\}$ *is given by* f_{mod}*, where*

$$f_{\mathsf{mod}}(\rho) := \mathsf{rank}^{\circlearrowleft}_{\triangle}(\rho) - \Sigma_{j=1}^{t} O_j^\rho \pmod{t+1} (\in [t+1]), \text{ or}$$
$$f_{\mathsf{mod}}(\rho) := 1 + \Sigma_{j=1}^{t} T_j^\rho - \mathsf{rank}^{\circlearrowleft}_{\bigcirc}(\rho) \pmod{t+1} (\in [t+1]).$$

We now introduce a labeling function f_{MOD} and proves that $f_{\mathsf{MOD}} \equiv f_{\mathsf{mod}} + C$ for some constant C. Thus we give an alternative yet equivalent definition of the modular factorization, which is $\{F_{f_{\mathsf{MOD}},1}, \ldots, F_{f_{\mathsf{MOD}},t+1}\}$.

Definition 6. *Assume* $\rho = (\rho_1, \ldots, \rho_{2t+1})$ *is any permutation of* $[t\bigcirc, t\triangle, 1\times]$. *Arrange* $\rho_1, \ldots, \rho_{2t+1}$ *in CW order. We count* ***the number of tuples*** $(\times, \bigcirc, \triangle)$

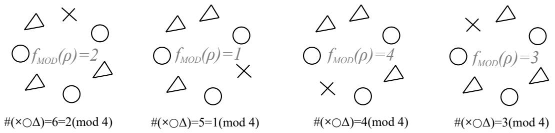


Fig. 3. Illustration of the definition of f_{MOD}. The four permutations drawn here share the same positions of $\bigcirc$'s, and they are mapped to different numbers under f_{MOD}.

which are located in CW order within this cycle of characters (positions may be inconsecutive) (such a tuple is an inversion when we cut the sequence at $\times$). Taken modulo $(t+1)$, the remainder, restricted to $[t+1]$, is $f_{\mathsf{MOD}}(\rho)$. See Fig. 3.

By Definition 6, we establish an interesting connection between the modular factorization and the **inversion number of permutations** (section 5.3 of [18]).

Let $\rho^{\times\to\triangle}$ be constructed from ρ, which swaps $\times$ with its CW next $\triangle$.
Let $\rho^{\times\to\bigcirc}$ be constructed from ρ, which swaps $\times$ with its CW next $\bigcirc$.
Let $\rho^{\triangle\leftarrow\times}$ be constructed from ρ, which swaps $\times$ with its CCW next $\triangle$.
Let $\rho^{\bigcirc\leftarrow\times}$ be constructed from ρ, which swaps $\times$ with its CCW next $\bigcirc$.

Lemma 9 (Variation laws of f_{mod} and f_{MOD}).

$$f_{\mathsf{MOD}}(\rho^{\times\to\triangle}) = f_{\mathsf{MOD}}(\rho^{\bigcirc\leftarrow\times}) = f_{\mathsf{MOD}}(\rho) - 1 \quad (\mathit{mod}\ t+1), \tag{2}$$

$$f_{\mathsf{MOD}}(\rho^{\times\to\bigcirc}) = f_{\mathsf{MOD}}(\rho^{\triangle\leftarrow\times}) = f_{\mathsf{MOD}}(\rho) + 1 \quad (\mathit{mod}\ t+1). \tag{3}$$

$$f_{\mathsf{mod}}(\rho^{\times\to\triangle}) = f_{\mathsf{mod}}(\rho^{\bigcirc\leftarrow\times}) = f_{\mathsf{mod}}(\rho) - 1, \quad (\mathit{mod}\ t+1) \tag{4}$$

$$f_{\mathsf{mod}}(\rho^{\times\to\bigcirc}) = f_{\mathsf{mod}}(\rho^{\triangle\leftarrow\times}) = f_{\mathsf{mod}}(\rho) + 1. \quad (\mathit{mod}\ t+1). \tag{5}$$

Lemma 9 is proved in C. Its corollary below is trivial; proof omitted.

Corollary 2. *Because f_{mod} and f_{MOD} have the same variation law, there is a constant C so that $f_{\mathsf{MOD}} \equiv f_{\mathsf{mod}} + C$. Specifically,* $\begin{cases} C = 0, & t \textit{ is even;} \\ C = (t+1)/2, & t \textit{ is odd.} \end{cases}$

At last, we point out that the resolved functions of f_{mod} or f_{MOD} can easily be deduced according to the original definition of modular factorization.

References

1. Aggarwal, G., Fiat, A., Goldberg, A., Hartline, J., Immorlica, N., Sudan, M.: Derandomization of auctions. In: Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing. pp. 619–625. STOC '05, ACM (2005)
2. Aigner, M.: Lexicographic matching in Boolean algebras. Journal of Combinatorial Theory, Series B **14**(3), 187–194 (1973)
3. Bapat, R.: Moore–Penrose inverse of set inclusion matrices. Lin. Alg. and its App. **318**(1), 35–44 (2000)
4. Ben-Zwi, O., Newman, I., Wolfovitz, G.: Hats, auctions and derandomization. Random Structures & Algorithms **46**(3), 478–493 (2015)

5. Bierbrauer, J., Edel, Y.: Theory of perpendicular arrays. Journal of Combinatorial Designs **2**(6), 375–406 (1994)
6. Butler, S., Hajiaghayi, M., Kleinberg, R., Leighton, T.: Hat guessing games. SIAM Review **51**(2), 399–413 (2009)
7. Colbourn, C., Dinitz, J. (eds.): CRC Handbook of Combinatorial Designs. CRC Press, Inc, 2 edn. (2007)
8. Däubel, K., Jäger, S., Mütze, T., Scheucher, M.: On orthogonal symmetric chain decompositions. CoRR **abs/1810.09847** (2018)
9. Dershowitz, N., Zaks, S.: The cycle lemma and some applications. European Journal of Combinatorics **11**(1), 35–40 (1990)
10. Duffus, D., Kierstead, H., Snevily, H.: An explicit 1-factorization in the middle of the Boolean lattice. J. of Comb. Theory, Series A **65**(2), 334–342 (1994)
11. Ebert, T., Merkle, W., Vollmer, H.: On the autoreducibility of random sequences. SIAM Journal on Computing **32**(6), 1542–1569 (2003)
12. Ghorbani, E., Khosrovshahi, G., Maysoori, C., Mohammad-Noori, M.: Inclusion matrices and chains. J. of Comb. Theory, Series A **115**(5), 878–887 (2008)
13. Greene, C., Kleitman, D.: Strong versions of Sperner's theorem. Journal of Combinatorial Theory, Series A **20**(1), 80–88 (1976)
14. Gregor, P., Mütze, T., Nummenpalo, J.: A short proof of the middle levels theorem. CoRR **abs/1710.08249** (2018)
15. Hall, P.: On representatives of subsets. Journal of the London Mathematical Society **s1-10**(1), 26–30 (1935)
16. Jin, K., Jin, C., Gu, Z.: Cooperation via codes in restricted hat guessing games. In: Inter. Conf. on Autonomous Agents and Multiagent Systems (2019)
17. Kierstead, H., Trotter, W.: Explicit matchings in the middle levels of the Boolean lattice. Order **5**(2), 163–171 (1988)
18. Kleinberg, J., Tardos, E.: Algorithm Design. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA (2005)
19. Kramer, E., Wu, Q., Magliveras, S., Trung, T.: Some perpendicular arrays for arbitrarily large *t*. Discrete Mathematics **96**(2), 101–110 (1991)
20. Ma, T., Sun, X., Yu, H.: A new variation of hat guessing games. In: Computing and Combinatorics. pp. 616–626. Springer Berlin Heidelberg (2011)
21. Mütze, T.: Proof of the middle levels conjecture. Proc. of the London Mathematical Society **112**(4), 677 (2016)
22. Mütze, T., Nummenpalo, J.: A constant-time algorithm for middle levels Gray codes. In: Proc. of the 28th Annual ACM-SIAM Symposium on Discrete Algorithms. pp. 2238–2253. Society for Industrial and Applied Mathematics (2017)
23. Mütze, T., Su, P.: Bipartite kneser graphs are hamiltonian. Combinatorica **37**(6), 1207–1219 (Dec 2017)
24. Neylon, T.: Notes on Raney's lemmas. Tech. rep. (2015)
25. Ordentlich, E., Roth, R.: Low complexity two-dimensional weight-constrained codes. IEEE Transactions on Information Theory **58**(6), 3892–3899 (June 2012)
26. Rao, C.: Combinatorial arrangements analogous to orthogonal arrays. Sankhyā: The Indian Journal of Statistics, Series A **23**(3), 283–286 (1961)
27. Spink, H.: Orthogonal symmetric chain decompositions of hypercubes. CoRR **abs/1706.08545** (2018)
28. Stinson, D., Teirlinck, L.: A construction for authentication/secrecy codes from 3-homogeneous permutation groups. E. J. of Combinatorics **11**(1), 73 – 79 (1990)
29. White, D., Williamson, S.: Recursive matching algorithms and linear orders on the subset lattice. Journal of Combinatorial Theory, Series A **23**(2), 117–127 (1977)
30. Wilson, R.: Incidence matrices of *t*-designs. Lin. Alg. and its App. **46**, 73–82 (1982)

A Proofs omitted in section 2

This appendix contains the proofs of Lemmas 1, 2, and 4.

Restatement of Lemma 1.

1. *Any 1-factorization of* $H(v = 4, t = 1)$ *is resolvable.*
2. *Any 1-factorization of* $H(2t + 1, t)$*, including the lexical factorization and modular factorization (as illustrated in Fig. 4), is resolvable.*
3. *No 1-factorization of* $H(6, 2)$ *is resolvable.*

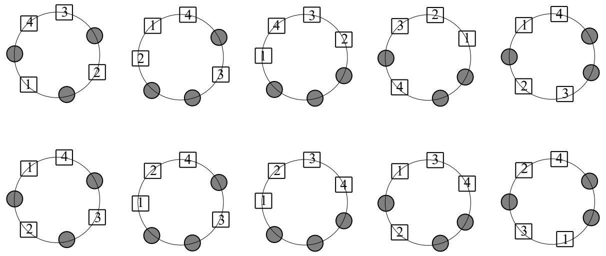


Fig. 4. Top (bottom) shows resolvable functions for f_{MOD} (f_{LEX}) for $v = 7, t = 3$.

Proof (of claim 1 of Lemma 1). Consider any 1-factorization of $H(4, 1)$. Assume its labeling function is f. We shall find $\{g_A \mid A \in \mathcal{P}_1\}$ and γ so that $f = f_{\gamma,g}$.

First, choose γ to be any bijection from the 2-element subset of [3] to [3]. Then, define $g_{\{1\}}$ as follows and define $g_{\{2\}}$, $g_{\{3\}}$, $g_{\{4\}}$ using a similar idea.

Observe that there must exist distinct numbers a, b, c so that $f(\{1\}, \{1, 2, 3\}) = \gamma(\{a, b\})$ and $f(\{1\}, \{1, 2, 4\}) = \gamma(\{a, c\})$ and $f(\{1\}, \{1, 3, 4\}) = \gamma(\{b, c\}$. This is because $\{f(\{1\}, \{1, 2, 3\}), f(\{1\}, \{1, 2, 4\}), f(\{1\}, \{1, 3, 4\})\} = \{1, 2, 3\}$ whereas the preimages of $1, 2, 3$ under γ are the three 2-element subsets of [3].

By choosing a, b, c as the values of $g_{\{1\}}(2), g_{\{1\}}(3), g_{\{1\}}(4)$ respectively,

$$\begin{aligned} f_{\gamma,g}(\{1\}, \{1, 2, 3\}) &= \gamma(g_{\{1\}}(\{2, 3\})) = \gamma(\{a, b\}) = f(\{1\}, \{1, 2, 3\}) \\ f_{\gamma,g}(\{1\}, \{1, 2, 4\}) &= \gamma(g_{\{1\}}(\{2, 4\})) = \gamma(\{a, c\}) = f(\{1\}, \{1, 2, 4\}) \\ f_{\gamma,g}(\{1\}, \{1, 3, 4\}) &= \gamma(g_{\{1\}}(\{3, 4\})) = \gamma(\{b, c\}) = f(\{1\}, \{1, 3, 4\}) \end{aligned}$$

Therefore, it is always possible to find a group of $\{g_A\}$ such that $f = f_{\gamma,g}$. □

Proof (of claim 2 of Lemma 1). Consider any 1-factorization of $H(2t + 1, t)$. Assume its labeling function is f. Choose γ to be the natural bijection from all the 1-element sets of $[t + 1]$ to $[t + 1]$, which maps $\{x\}$ to x. We shall find $\{g_A\}$ so that $f = f_{\gamma,g}$. For any t-subset A of $[2t + 1]$, we define g_A as follows.

$$g_A(x) := f(A, A \cup \{x\}) \quad (\forall x \in A^C). \tag{6}$$

Because f defines a 1-factorization, it satisfies condition (a). Therefore, when x is taken over all elements in A^C, function $f(A, A \cup \{x\})$ would be taken over all numbers in $[t+1]$. This means that g_A is indeed a bijection from A^C to $[t+1]$. Moreover, it is straightforward to see $f_{\gamma,g}(A, A \cup \{x\}) \equiv f(A, A \cup \{x\})$. □

Proof (of claim 3 of Lemma 1). We design a short *C++* program which searches all the resolvable 1-factorizations of $H(6, 2)$ and $H(8, 3)$ by brute force, which can be downloaded at `https://github.com/cscjjk/resolvable-1-factorization`.

For $H(8, 3)$, the program returns many solutions.

For $H(6, 2)$, the program runs in less than five seconds and finds no solution. This shows that there is no resolvable 1-factorization of $H(6, 2)$.

We note that this claim is not so important for this manuscript because no result is depending on this claim. So we only prove it by a *C++* program. □

Restatement of Lemma 2. *Given $\{g_A\}$ and γ, the following are equivalent:*

(i) function $f_{\gamma,g}(A, A')$ satisfies condition (b); and
(ii) When $A_1 \neq A_2$ and $(A_1, A'_1), (A_2, A'_2)$ are two edges in $H(v, t)$, then $g_{A_1}(A'_1 - A_1) = g_{A_2}(A'_2 - A_2)$ implies that $A'_1 \neq A'_2$.

Proof (of Lemma 2). Assume (i) holds. Proving (ii) is equivalent to proving that for A_1, A_2, A'_1, A'_2 such that $A_1 \neq A_2$ and $(A_1, A'_1), (A_2, A'_2)$ are two edges in $H(v, t)$, equality $A'_1 = A'_2 = A'$ implies that $g_{A_1}(A'_1 - A_1) \neq g_{A_2}(A'_2 - A_2)$.

Because condition (b) is satisfied by $f_{\gamma,g}$ whereas $A_1 \neq A_2$ and $A'_1 = A'_2 = A'$, we get $f_{\gamma,g}(A_1, A') \neq f_{\gamma,g}(A_2, A')$, i.e., $\gamma(g_{A_1}(A' - A_1)) \neq \gamma(g_{A_2}(A' - A_2))$. Further since γ is a bijection, $g_{A_1}(A'_1 - A_1) \neq g_{A_2}(A'_2 - A_2)$.

Now we prove (i) from (ii). Assume (ii) holds. For any two distinct edges (A_1, A') and (A_2, A') of $H(v, t)$, we shall prove that $f_{\gamma,g}(A_1, A') \neq f_{\gamma,g}(A_2, A')$, namely, $g_{A_1}(A' - A_1) \neq g_{A_2}(A' - A_2)$. Suppose to the opposite that $g_{A_1}(A' - A_1) = g_{A_2}(A' - A_2)$, we get $A' \neq A'$ according to (ii), which is contradictory. □

Restatement of Lemma 4. *Any $t + d$ columns of a $\mathsf{PA}(t, 2t + d, 2t + d)$ form a $\mathsf{CPA}(t, t + d, 2t + d)$.*

Proof (of Lemma 4). Suppose M' contains any $t+d$ columns of a $\mathsf{PA}(t, 2t+d, 2t+d)$ M. By the definition of perpendicular arrays, M' is still a $\mathsf{PA}(t, t + d, 2t + d)$. Therefore, we only need to show that M' is complete.

Let A_i denote the set of elements in the i-th row of M among those t columns which are not chosen in constructing M'. Because M is $\mathsf{PA}(t, 2t + d, 2t + d)$, sets $A_1, \ldots, A_{\binom{2t+d}{t}}$ go through every t-element subset of $[2t + d]$ exactly once. Therefore, $[2t + d] - A_1, \ldots, [2t + d] - A_{\binom{2t+d}{t}}$ go through every $(t + d)$-element subset of $[2t + d]$ exactly once. However, the elements in each row of M' are respectively $[2t + d] - A_1, \ldots, [2t + d] - A_{\binom{2t+d}{t}}$. Together, M' is complete. □

B Proofs omitted in section 3

Restatement of Lemma 5. *Given any sequence S of t ')'s and $t+1$ '('s. There exists a unique cyclic-shift $S^{(j)}$ of S whose first $2t$ parentheses are paired up when parenthesized, and we can compute j in $O(t)$ time.*

Proof (of Lemma 5). Assume S is a sequence of $v = 2t+1$ parentheses, t of which are ')'s. We are interested in finding a cyclic-shift of S in which the first $2t$ parentheses can be paired up when parenthesizing.

Denote H_i = the number of ')'s − the number of '('s in $s_1, \ldots, s_i$ for each i. Draw points $\{(i, H_i) \mid 0 \le i \le v\}$ in the Cartesian plane, as shown in Fig. 5.

Select the highest point (j^*, H_{j^*}); for a tie, select the rightmost one.

When $j \neq j^*+1$, the cyclic-shift $S^{(j)}$ does not satisfy our requirement. This is because when $j \neq j^*+1$, the one shifted from s_{j^*+1}, which is a left parenthesis, cannot be paired up. When $j = j^*+1$, the cyclic-shift $S^{(j)}$ satisfies our requirement. This is simply illustrated in the figure. To complete, we point out that index j^*+1 can easily be computed in $O(t)$ time.

This lemma also follows from Cycle Lemma [9] or Raney Lemma [24]. □

Restatement of Lemma 6. *When S is canonical, for any $s_l = ($ and $s_r =)$, there are more)'s than ('s in $\{s_{l+1}, \ldots, s_r\}$ $\Leftrightarrow$ $\mathsf{index}(s_l) \ge \mathsf{index}(s_r)$.*

Proof (of Lemma 6). For each i $(0 \le i \le 2t+1)$, denote

H_i = the number of ')'s − the number of '('s in $s_1, \ldots, s_i$, and

H'_i = the number of ')'s − the number of '('s in $s_{i+1}, \ldots, s_{2t+1}$.

To be clear, $H_0 = H'_{2t+1} = 0$. Trivially, we have:

$H_i + H'_i = -1$ (for all i). $\quad \mathsf{depth}(s_l) = -H_l - 1. \quad \mathsf{depth}(s_r) = -H_r.$

We need to discuss two cases depending on which one of l, r is smaller.

- Case 1: $l < r$. Let us count the number of ')'s minus the number of '('s in the interval $s_{l+1}, \ldots, s_r$. This is given by $H_r - H_l$. Therefore, there are more ')'s in this interval $\Leftrightarrow H_r - H_l > 0 \Leftrightarrow -\mathsf{depth}(s_r) + \mathsf{depth}(s_l) + 1 > 0 \Leftrightarrow \mathsf{depth}(s_r) \le \mathsf{depth}(s_l) \Leftrightarrow \mathsf{index}(s_r) \le \mathsf{index}(s_l)$ (when $l < r$).
- Case 2: $r < l$. The number of ')' minus the number of '('s in (cyclic) interval $s_{l+1}, \ldots, s_{2t+1}, s_1, \ldots, s_r$ is given by $H'_l + H_r = -1 - H_l + H_r$. So, there are more ')'s in this interval $\Leftrightarrow -1 - H_l + H_r > 0 \Leftrightarrow \mathsf{depth}(s_l) - \mathsf{depth}(s_r) > 0 \Leftrightarrow \mathsf{depth}(s_r) < \mathsf{depth}(s_l) \Leftrightarrow \mathsf{index}(s_r) \le \mathsf{index}(s_l)$ (when $r < l$).

In either case, the lemma holds. □

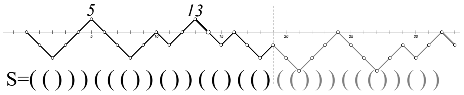

5
13
5
10
15
20
25
30
S=(( ))) ((( )) ( )) (( ) (( ) (( ))) ((( )) ( ))

Fig. 5. Illustration of Lemma 5. This figure draws Example 1.

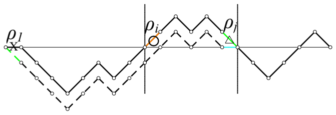


Fig. 6. Illustration of variation laws below. The dotted line indicates $\rho^{\times \rightarrowtail \triangle}$.

B.1 The full version of the variation laws of f_{LEX}

Consider any permutation ρ of $[t\bigcirc, t\triangle, 1\times]$. For any character $\triangle$ or $\bigcirc$ in ρ,

we say it is *CW-balanced* if there are equal number of $\triangle$'s and $\bigcirc$'s in the (cyclic) interval of ρ starting from $\times$ to this character in CW order, and

we say it is *CCW-balanced* if there are equal number of $\triangle$'s and $\bigcirc$'s in the (cyclic) interval of ρ starting from $\times$ to this character in CCW order.

The following lemma is the full version of Lemma 7.

Lemma 10 (Variation laws of f_{LEX}).

1. *$f_{\mathsf{LEX}}(\rho) \neq t+1 \Leftrightarrow$ there is a CW-balanced $\triangle \Leftrightarrow$ there is a CCW-balanced $\bigcirc$.*
2. *$f_{\mathsf{LEX}}(\rho) \neq t \Leftrightarrow$ there is a CW-balanced $\bigcirc \Leftrightarrow$ there is a CCW-balanced $\triangle$.*
3. *When $f_{\mathsf{LEX}}(\rho) \neq t+1$, let $\rho^{\times\rightarrowtail\triangle}$ ($\rho^{\bigcirc\leftarrowtail\times}$) be constructed from ρ by swapping $\times$ with the CW first CW-balanced $\triangle$ (the CCW first CCW-balanced $\bigcirc$). Then,*
$$f_{\mathsf{LEX}}(\rho^{\times\rightarrowtail\triangle}) = f_{\mathsf{LEX}}(\rho^{\bigcirc\leftarrowtail\times}) = (f_{\mathsf{LEX}}(\rho) - 1) \ mod \ (t+1)(\in [t+1]).$$
4. *When $f_{\mathsf{LEX}}(\rho) \neq t$, let $\rho^{\times\rightarrowtail\bigcirc}$ ($\rho^{\triangle\leftarrowtail\times}$) be constructed from ρ by swapping $\times$ with the CW first CW-balanced $\bigcirc$ (the CCW first CCW-balanced $\triangle$). Then,*
$$f_{\mathsf{LEX}}(\rho^{\times\rightarrowtail\bigcirc}) = f_{\mathsf{LEX}}(\rho^{\triangle\leftarrowtail\times}) = (f_{\mathsf{LEX}}(\rho) + 1) \ mod \ (t+1)(\in [t+1]).$$

Proof (of Lemma 10). Without loss of generality, assume that $\rho_1 = \times$. For each i ($1 \leq i \leq v$), define the *height* of ρ_i as the number of $\bigcirc$'s minus the number of $\triangle$'s in $\{\rho_1, \ldots, \rho_i\}$. (So, a $\bigcirc$ is positive if and only if its height is positive.)

Proof of Claim 1. Assume $f_{\mathsf{LEX}}(\rho) \neq t+1$. In this case there exists some $\bigcirc$ with positive height. This implies that there exists a pair of (i,j) such that $\rho_i = \bigcirc$ has a height 1 while $\rho_j = \triangle$ has a height 0, as shown in Fig. 6. Clearly, ρ_j is a CW-balanced $\triangle$ while ρ_i is a CCW-balanced $\bigcirc$. On the other direction, the existence of a CW-balanced $\triangle$ or a CCW-balanced $\bigcirc$ implies the existence of a positive $\bigcirc$, which immediately implies that $f_{\mathsf{LEX}}(\rho) \neq t+1$.

Claim 2 is symmetric to Claim 1; proof omitted. □

Proof of the equations in Claim 3 and Claim 4. Because the four equations are symmetric, we only show the proof of $f_{\mathsf{LEX}}(\rho^{\times\rightarrowtail\triangle}) = f_{\mathsf{LEX}}(\rho) - 1$.

Without loss of generality, assume $\rho_1 = \times$. Let ρ_i be the CW first $\bigcirc$ with height 1. Let ρ_j be the CW first $\triangle$ with height 0, i.e. the CW first CW-balanced $\triangle$. As illustrated in Fig. 6, $\rho^{\times\rightarrowtail\triangle}$ is constructed from ρ by swapping ρ_1 with ρ_j. We shall prove that after the swapping, the number of positive $\bigcirc$'s decreases by 1. This follows from three observations: (i) $\rho_i = \bigcirc$ is positive in ρ (with height 1) but not anymore in $\rho^{\times\rightarrowtail\triangle}$ (with height 0). (ii) For other $\bigcirc$'s in $\rho_2, \ldots, \rho_j$, their heights drop by 1, but their positivity do not change. (iii) For the $\bigcirc$'s in $\rho_{j+1}, \ldots, \rho_{2t+1}$, their heights and positivity stay the same as before. □

C Proofs omitted in section 4

Restatement of Lemma 8. *The labeling function of* $\{\mathcal{M}_i \mid 1 \leq i \leq t+1\}$ *is*

$$f_{\mathsf{mod}}(\rho) := \mathsf{rank}^{\circlearrowright}_{\triangle}(\rho) - \Sigma^t_{j=1} O^{\rho}_j \pmod{t+1} (\in [t+1]), \text{ or} \tag{7}$$

$$f_{\mathsf{mod}}(\rho) := 1 + \Sigma^t_{j=1} T^{\rho}_j - \mathsf{rank}^{\circlearrowright}_{\bigcirc}(\rho) \pmod{t+1} (\in [t+1]). \tag{8}$$

Proof (of Lemma 8). We first state two trivial observations:
($\times$'s position) $+ \Sigma_j O^{\rho}_j + \Sigma_j T^{\rho}_j = 1 + \ldots + (2t+1) = 0(\bmod t+1)$, and
($\times$'s position) $+ \mathsf{rank}^{\circlearrowright}_{\triangle}(\rho) - 1 + \mathsf{rank}^{\circlearrowright}_{\bigcirc}(\rho) - 1 = 2t + 1 = -1(\bmod t+1)$.

By subtraction, $\mathsf{rank}^{\circlearrowright}_{\triangle}(\rho) - \Sigma^t_{j=1} O^{\rho}_j = 1 + \Sigma^t_{j=1} T^{\rho}_j - \mathsf{rank}^{\circlearrowright}_{\bigcirc}(\rho)(\bmod t+1)$. Therefore, the two definitions of f_{mod} given in (7) and (8) are equivalent.

Next, we show that f_{mod} is the labelling function of $\{\mathcal{M}_1, \ldots, \mathcal{M}_{t+1}\}$. Recall that ρ represents the edge (A, A') in the middle level graph, where $A = \{O^{\rho}_1, \ldots, O^{\rho}_t\}$ and $A' = \{O^{\rho}_1, \ldots, O^{\rho}_t, \text{the position of } \times\}$. We shall prove that $(A, A') \in \mathcal{M}_{f_{\mathsf{mod}}(\rho)}$. By the definition of $\mathcal{M}_{f_{\mathsf{mod}}(\rho)}$, it reduces to proving that the single element in $A' - A$ is the y-th largest one in $[v] - A$, where $y = (\Sigma A + f_{\mathsf{mod}}(\rho)) \bmod (t+1)$ $(y \in [t+1])$. Namely, the unique $\times$ has rank y when enumerating all $\triangle$'s or $\times$ in ρ in CCW; i.e., $\mathsf{rank}^{\circlearrowright}_{\triangle}(\rho) = y \bmod (t+1)$. This holds since $y = \Sigma A + f_{\mathsf{mod}}(\rho) = \Sigma^t_{j=1} O^{\rho}_j + \mathsf{rank}^{\circlearrowright}_{\triangle}(\rho) - \Sigma^t_{j=1} O^{\rho}_j \bmod (t+1)$. □

Next, recall the variation laws of f_{mod} and f_{MOD} in Lemma 9. Notice that (3) and (5) are equivalent to (2) and (4) respectively. We now prove (2) and (4).

Proof (of (2)). We only need to prove $f_{\mathsf{MOD}}(\rho^{\times \to \triangle}) = f_{\mathsf{MOD}}(\rho) - 1(\bmod t+1)$. The other equation $f_{\mathsf{MOD}}(\rho^{\bigcirc \leftarrow \times}) = f_{\mathsf{MOD}}(\rho) - 1(\bmod t+1)$ in (2) is symmetric.

See Fig. 7. Denote by a the number of $\bigcirc$'s between $\times$ and its CW next $\triangle$ in ρ. Recall that $f_{\mathsf{MOD}}(\rho)$ denotes the number of $(\times, \bigcirc, \triangle)$-tuples which are located in CW order within ρ (and then modulo $t+1$). So, $f_{\mathsf{MOD}}(\rho^{\times \to \triangle}) - f_{\mathsf{MOD}}(\rho) = (t - a) \cdot 1 - a \cdot t \bmod (t+1)$, which implies that $f_{\mathsf{MOD}}(\rho^{\times \to \triangle}) = f_{\mathsf{MOD}}(\rho) - 1 \bmod (t+1)$. In calculating the difference between $f_{\mathsf{MOD}}(\rho^{\times \to \triangle})$ and $f_{\mathsf{MOD}}(\rho)$, observe that (i) for the $\bigcirc$'s located CW between the $\triangle$ being swapped and $\times$, the number of $(\times, \bigcirc, \triangle)$-tuples related to each of them increases by 1; and (ii) for the other $\bigcirc$'s, the number of $(\times, \bigcirc, \triangle)$-tuples related to each of them decreases by t. □

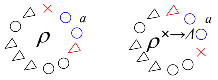


Fig. 7. Illustration of the proof the variation law of f_{MOD} function..

Proof (of (4)). By swapping $\times$ with its CW next $\triangle$, $\mathsf{rank}^{\circlearrowright}_{\triangle}(\rho)$ decreases by 1. Further by (7), $f_{\mathsf{mod}}(\rho) = \mathsf{rank}^{\circlearrowright}_{\triangle}(\rho) - \Sigma^t_{j=1} O^{\rho}_j(\bmod t+1)$ decreases by 1. Similarly, by swapping $\times$ with its CCW next $\bigcirc$, $\mathsf{rank}^{\circlearrowright}_{\bigcirc}(\rho)$ increases by 1. Further by (8), $f_{\mathsf{mod}}(\rho) = 1 + \Sigma^t_{j=1} T^{\rho}_j - \mathsf{rank}^{\circlearrowright}_{\bigcirc}(\rho)(\bmod t+1)$ decreases by 1. □

D Explicit 1-factors of the bipartite Kneser graph

Although, most explicit 1-factorizations of the bipartite Kneser graph $H(v,t)$ have not been found, especially for $v > 2t+1$, two explicit 1-factors of $H(v,t)$ are known for a long time. To make the paper more self-contained, in this appendix we briefly review the literature of these 1-factors and give their new definitions.

Definition 7. *Assume $A \subset [v]$ and $|A| \leq v/2$. By the following two steps, we can obtain a subset A' which has equal size as A and is disjoint with A, and we define it to be $\circlearrowleft(A)$.*

Step 1. Write down all the numbers in $[v]$ to a cycle from 1 to v in CW order.

Step 2. Enumerate each number a in A, find the CCW first number from a that is not contained in $A \cup A'$ yet and add it to A'.

Note: The order of the enumeration in Step 2 does not matter. Take $v = 10$ and $A = \{1, 3, 8, 9\}$ for example. In order $1, 3, 8, 9$, the numbers added to A' would be $10, 2, 7, 6$. In order $3, 9, 8, 1$, the numbers added to A' would be $2, 7, 6, 10$.)

We define $\circlearrowright(A)$ symmetrically (by changing CCW to CW in Step 2).

Recall that $\mathcal{P}_t$ denotes the t-th level of the subset lattice of $[v]$, i.e., it contains all subsets of $[v]$ with t elements. For $t < v/2$ and $A \subset \mathcal{P}_t$, define

$$\gamma_t^v(A) := [v] - \circlearrowleft(A) \text{ and } {\gamma'}_t^v(A) := [v] - \circlearrowright(A). \tag{9}$$

Obviously, γ_t^v and ${\gamma'}_t^v$ are two 1-factors of $H(v,t)$, and they are disjoint.

Lemma 11. *When $v = 2t+1$, we have $\gamma_t^v = \mathcal{L}_{t+1}$ and ${\gamma'}_t^v = \mathcal{L}_t$.*

Proof. We only show that $\gamma_t^v = \mathcal{L}_{t+1}$. The other equation is similar. Consider a subset $A \subset \mathcal{P}_t$. Replace all elements in A by $\bigcirc$ and all the elements in $\circlearrowleft(A)$ by $\triangle$ and the remaining element by $\times$. Clearly, this permutation is mapped to $t+1$ under f_{LEX}, because no $\bigcirc$ is positive. This means A is mapped to $[v] - \circlearrowleft(A)$ in $\mathcal{L}_{t+1}$. Also, A is mapped to $[v] - \circlearrowleft(A)$ in γ_t^v. □

In the following, we review a 1-factor β_t^v of $H(v,t)$ and prove that $\beta_t^v = \alpha_t^v$.

D.1 Definition of β_t^v introduced in [13]

First, we review the chain-decomposition of the subset lattice given in [13]. Recall the parenthesis representation introduced in subsection 3.2. The sequence of parentheses can be parenthesized uniquely in the usual way, and there may remain several parenthesis unpaired. For example, in $)_1, (_2,)_3,)_4, (_5, (_6, (_7,)_8,)_9, (_{10}$, "$(_2$" is paired with "$)_3$", "$(_6$" is paired with "$)_9$", and "$(_7$" is paired with "$)_8$". All the others are unpaired. Note that all the unpaired right parentheses always occur to the left of the unpaired left parentheses.

Chain-decomposition of the subset lattice via parenthesizing[13]. Two subsets of $[v]$ are in the same chain, if and only if their associated parenthesis sequences contain the same paired parenthesis. Equivalently, suppose $A \subset [v]$ is associated with sequence S. Replace the leftmost unpaired '(' in S by ')' and assume that the new sequence corresponds to subset A'. Then, A' is the next member in the chain containing A. For the above example, the leftmost unpaired '(' is $(_5$, so $A' = \{1,3,4,5,8,9\}$. The entire chain in this example is $\{3,8,9\} \to \{1,3,8,9\} \to \{1,3,4,8,9\} \to \{1,3,4,5,8,9\} \to \{1,3,4,5,8,9,10\}$.

Clearly, all chains in this decomposition are *symmetric* – if a chain contains a member A, it must contain a member with size $v - |A|$. So, this chain-decomposition implicitly defines an antipodal matching β^v_t between the antipodal layers $\mathcal{P}_t$ and $\mathcal{P}_{v-t}$ for each $t < v/2$.

D.2 The equivalence between β^v_t and γ^v_t.

Lemma 12. *Assume $t < v/2$. We have $\beta^v_t(A) = \gamma^v_t(A)$ for any $A \in \mathcal{P}_t$.*

Proof. We shall prove that $\beta^v_t(A) = [v] - \circlearrowleft(A)$. We first prove it by an example and then give the formal proof. Let $\mathsf{PS}(A)$ denote the *parenthesis sequence* associated with A.

Example 2. $v = 11, A = \{1,3,4,8,9\}$. The sequence of parentheses associated with A is:

$$\mathsf{PS}(A) = \boxed{)}_1\ (_2\ )_3\ \boxed{)}_4\ \boxed{(}_5\ (_6\ (_7\ )_8\ )_9\ \boxed{(}_{10}\ \boxed{(}_{11}.$$

The unpaired parentheses are boxed for ease of distinction.

There are two unmatched right parentheses and three unmatched left parentheses. According to the definition of the chain-decomposition, in its symmetric member $\beta^{11}_5(A)$ we should replace the first unmatched left parenthesis by a right parenthesis. So,

$$\mathsf{PS}(\beta^{11}_5(A)) = \boxed{)}_1\ (_2\ )_3\ \boxed{)}_4\ \boxed{)}_5\ (_6\ (_7\ )_8\ )_9\ \boxed{(}_{10}\ \boxed{(}_{11}.$$

Then, let us also compute $\circlearrowleft(A)$ and $[v] - \circlearrowleft(A)$. (In the following, the positions of boxes stay the same as above; they do not indicate the unpaired parentheses.)

$$\mathsf{PS}(\circlearrowleft(A)) = \boxed{(}_1\ )_2\ (_3\ \boxed{(}_4\ \boxed{(}_5\ )_6\ )_7\ (_8\ (_9\ \boxed{)}_{10}\ \boxed{)}_{11}.$$

$$\mathsf{PS}([v] - \circlearrowleft(A)) = \boxed{)}_1\ (_2\ )_3\ \boxed{)}_4\ \boxed{)}_5\ (_6\ (_7\ )_8\ )_9\ \boxed{(}_{10}\ \boxed{(}_{11}.$$

We see $\mathsf{PS}(\beta^{11}_5(A)) = \mathsf{PS}([v] - \circlearrowleft(A))$. Therefore, $\beta^{11}_5(A) = [v] - \circlearrowleft(A)$.

For any $i \in [v]$, we shall prove that (X) $i \in \beta^v_t(A)$ if and only if $i \in [v] - \circlearrowleft(A)$. We discuss two cases distinguished by whether i belongs to U, where U is the set of unpaired positions of $\mathsf{PS}(A)$ (the positions are indexed by $1, \ldots, v$).

Case 1: $i \notin U$. Then, the i-th parenthesis of $\mathsf{PS}(A)$ is paired. It will not change within the chain containing A and $\beta^v_t(A)$. Therefore, (I) $i \in \beta^v_t(A)$ if and only if $i \in A$. On the other hand, by the definition of $\circlearrowleft(A)$, it easily follows that $i \in \circlearrowleft(A)$ if and only if $i \notin A$. (In the example above, the paired number

3 in A will go to 2 in $\circlearrowleft(A)$, the paired numbers 8 and 9 will go to 6 and 7 in $\circlearrowleft(A)$. So $i \in \circlearrowleft(A)$ if and only if $i \notin A$.) Therefore, (II) $i \in [v] - \circlearrowleft(A)$ if and only if $i \in A$. Combine (I) and (II), we get statement (X).

Case 2: $i \in U$. Assume $\mathsf{PS}(A)$ has r unpaired right parentheses and l unpaired left parentheses. For any sequence S with length v, let $S^{(U)}$ denote the subsequence of S that are located at U. We state the following arguments about the parentheses locating at U.

1. $\mathsf{PS}(A)^{(U)}$ starts by r ')'s and is followed by l '('s.
2. $\mathsf{PS}(\beta_t^v(A))^{(U)}$ starts by l ')'s and is followed by r '('s.
3. $\mathsf{PS}(\circlearrowleft(A))^{(U)}$ starts by l '('s and is followed by r ')'s.
4. $\mathsf{PS}([v] - \circlearrowleft(A))^{(U)}$ starts by l ')'s and is followed by r '('s.

The first argument is according to the assumption of l and r. The second follows by 1 and the fact that $\beta_t^v(A)$ is the symmetric member of A in the chain containing them. The third follows by 1 and the definition of the CCW-rotating-subset. The last follows by the third. According to 2 and 4, we obtain (X) for those i in U altogether. □

D.3 Remarks and related work

Remark 3. According to Lemma 12, our definition of γ_t^v essentially gives an **explicit** definition of the antipodal matching β_t^v, which was previously defined implicitly from the chain-decomposition.

In fact, [25] presented an even more explicit definition of β_t^v using Cycle Lemma [9]. Based on their definition, they further showed that $\beta_t^v(A)$ can be computed in $O(v)$ time and $O(\log v)$ space. We do not review their work in depth in this appendix. (Note: we believe that [25] in fact discusses the other 1-factor γ'^v_t rather than γ_t^v, but it is straightforward to extend their result to the symmetric 1-factor $\gamma_t^v = \beta_t^v$.)

An equivalent definition of the chain-decomposition A few years earlier than [13], Aigner [2] proposed a greedy algorithm which can produce a matching λ_t between two consecutive layers $\mathcal{P}_t, \mathcal{P}_{t+1}$. The v matchings $\lambda_0, \ldots, \lambda_{v-1}$ together describe a chain-decomposition of the subset lattice. Interestingly, [29] pointed out that this decomposition is the same as the above one introduced in [13] via parenthesizing. This was not mentioned in [13].

Yet Another definition of the chain-decomposition. Recently, another alternative definition for the above chain-decomposition was proposed in [12]. However, their definition looks extremely complicated. We do not introduce it in this manuscript.

Remark 4. The bipartite graph $H(v,t)$ admits two disjoint 1-factors according to the fact that it is Hamiltonian [23]. Recently, Spink [27] found out three orthogonal chain decompositions of the subset lattice, which implies three disjoint 1-factors of $H(v,t)$. More recently, four orthogonal chain decompositions can be found for $v \geq 60$ [8].

E Application: unique-supply hat-guessing games

Hat-guessing games have been studied extensively in a broad area due to their relations to graph entropy, circuit complexity, network coding, and auctions [1,4,6,11,16,20]. In this appendix we show applications of the 1-factorization of the bipartite Kneser graphs in the following variant of hat-guessing game:

♠ **Unique-supply hat-guessing game [16].** There are v hats, each with a different color in $[v] = \{1, \dots, v\}$ (so for each color there is only one hat supplied). The *hat guessing game* is played by m players and one dealer (who is the nature).

- The dealer randomly places t hats to each player (assume $v - mt = d > 0$).
- Each player can observe those hats placed to any other player, but cannot see and has to guess the t colors of hats placed to himself or herself.
- The guess is private between one player and the dealer – players are forbidden to communicate during the whole game. Yet it is permissible for the players to discuss a strategy before the game starts.
- Player i ($i \in [m]$) is allowed to guess g_i times. A guess is correct if all the t colors are correct. If any guess of any player is correct, all players (as a team) win the game. All the parameters are given before the game starts.

Q. How can we design a strategy to achieve the optimal chance of winning?

Example 3. $v = 3, m = 2, t = d = g_1 = g_2 = 1$. *If Player 1 observes* b*, she guesses* b *mod* $3 + 1$. *If Player 2 observes* a*, he guesses* a *mod* $3 + 1$. Then, exactly one player guesses right. This strategy wins always and is optimal.

The answer for the two players case (i.e. $m = 2$) is as follows.

Graph Model. Let A, B respectively denote the set of colors placed to Player 1 and Player 2. Let $A' = [v] - B$. The state of the game can be represented as edge (A, A') in $H(v, t)$. Each player knows one node of the edge; Player 1 knows A' and Player 2 knows A.

Upper bound. The uncertainty for each player is $\binom{t+d}{d}$. This is the degree of each node. By one guess, a player has $1/\binom{t+d}{d}$ chance to win. Therefore, the maximum winning probability is no larger than $p = \max\{1, (g_1 + g_2)/\binom{t+d}{d}\}$.

Lower bound. Suppose a 1-factorization of $H(v, t)$ labels each edge by a number in $[\binom{t+d}{d}]$. In the $g_1 + g_2$ guesses, by respectively choosing the edges with labels $1, \dots, g_1 + g_2$, the players win if the label of the edge (state) is in $[g_1 + g_2]$, which occurs with probability p.

Remark 5. To play this game, both players wish to have a simple and realistic strategy that is easy to remember. This gives us a motivation to design an explicit 1-factorization of $H(v, t)$. We also point out that our algorithm for solving P1 and P2 in section 3 find applications in this game, because the following task arises in playing the game: Given A (or A') and a number $l \in [\binom{t+d}{d}]$, find the unique A' (or A) such that (A, A') is labeled with l in the factorization.