Group Representation Theory for Knowledge Graph Embedding

Chen Cai
Department of Computer Science
Ohio State University
cai.507@osu.edu

Abstract

Knowledge graph embedding has recently become a popular way to model relations and infer missing links. In this paper, we present a group theoretical perspective of knowledge graph embedding, connecting previous methods with different group actions. Furthermore, by utilizing Schur's lemma from group representation theory, we show that the state of the art embedding method RotatE has the capacity to model relations from any finite Abelian group.

1 Introduction

Knowledge graphs are collections of factual triples, where each triple (h, r, t) represents a relation r between a head entity h and a tail entity t. Examples of real-world knowledge graphs include Freebase, Yago [13], and WordNet [9]. Knowledge graphs are potentially useful for a variety of applications such as question-answering [6], information retrieval [18], recommender systems [22], and natural language processing [20]. Research on knowledge graphs is attracting growing interests in both academia and industry communities.

Since knowledge graphs are usually incomplete, a fundamental problem for knowledge graph is predicting the missing links. Recently, extensive studies have been done on learning low-dimensional representations of entities and relations for missing link prediction (a.k.a., knowledge graph embedding). These methods have been shown to be scalable and effective compared to previous methods [2, 8, 10, 12, 15, 17]. The general intuition of these methods is to model and infer the connectivity patterns in knowledge graphs according to observed knowledge facts. For example, some relations are symmetric (e.g., marriage) while others are antisymmetric (e.g., filiation); some relations are the inverse of other relations (e.g., hypernym and hyponym); and some relations may be composed by others (e.g., my mother's husband is my father). It is critical to find ways to model and infer these patterns, i.e., **symmetry/antisymmetry**, **inversion**, and **composition**, from observed facts in order to predict missing links.

We argue that symmetry/antisymmetry, inversion and composition have natural correspondence to notions in group theory. Under this perspective, many existing embedding models can be interpreted as modeling relations as elements of the group acting on a properly chosen space. However, as a step to understand the power and limitation of knowledge graph embedding, we believe this perspective is still interesting and worth investigation. Our algebraic (group) perspective of knowledge graph embedding can also complement existing statistical approaches [11, 24] and deepen our understanding of knowledge graph embedding. Specifically, our main contributions are

- We bring a group theoretical perspective to knowledge graph embedding. To the best of our knowledge, this connection has not been made explicitly before.
- We provide a self-contained introduction of concepts and examples from group theory and group representation theory.

- We characterize the representation power of a recent embedding method RotatE. By utilizing tools from group representation theory, we showed that RotatE has the capacity to represent **any** finite Abelian groups.

2 Background

The general methodology of Knowledge Graph Embedding(KGE) is to define a score function for the triples. Formally, let $\mathcal{E}$ denote the set of entities and $\mathcal{R}$ denote the set of relations, then a knowledge graph is a collection of factual triples (h, r, t), where $h, t \in \mathcal{E}$ and $r \in \mathcal{R}$. Since entity embeddings are usually represented as vectors, the score function usually takes the form $f(h, r, t)$, where h and t are head and tail entity embeddings. We listed the score functions for a few popular embedding methods.

- TransE [1]: $f(h, r, t) = -\|h + r - t\|, h, r, t \in \mathbb{R}^k$
- TorusE [4]: $f(h, r, t) = -\|h + r - t\|, h, r, t \in \mathbb{T}^k$ where $\mathbb{T}^k$ is a k-dimensional torus.
- DistMul [21]: $f(h, r, t) = h^T diag(r)t, h, r, t \in \mathbb{R}^k$.
- ComplEx [16]: $f(h, r, t) = Re(h^T diag(r)\bar{t}), h, r, t \in \mathbb{C}^k$
- RotatE [14]: $f(h, r, t) = -\|h \circ r - t\|, h, r, t \in \mathbb{C}^d, \|r_i\| = 1$ where $\circ$ denotes Hadmard product.

Most models can capture only a portion of the relation patterns. For example, TransE represents each relation as a translation from source entities and target entities, and thus implicitly models inversion and composition of relations, but it can not model symmetric relations; ComplEx [7] extends DistMult by introducing complex embeddings so as to better model asymmetric relations, but it can not infer the composition pattern. RotatE is the first model that is able to model all the relation patterns and is the main focus of this paper.

2.1 Relation Pattern

We formally define common relation patterns that many embedding methods try to model in knowledge graph.

Definition 2.1. A relation clause r is symmetric if $\forall x, y, \ r(y, x) \implies r(y, x)$. A clause with such form is a symmetry pattern.

Definition 2.2. A relation clause r is anti-symmetric if $\forall x, y, r(x, y) \implies \neg r(y, x)$. A clause with such form is an anti-symmetry pattern.

Definition 2.3. A relation r_1 is inverse to r_2 if $\forall x, y, r_2(x, y) \implies r_1(y, x)$. A clause with such form is an inversion pattern.

Definition 2.4. A relation r_1 is composed of relation r_2 and relation r_3 if $\forall x, y, z, r_1(x, y) \wedge r_2(y, z) \implies r_3(x, z)$. A clause with such form is a composition pattern.

Definition 2.5. A relation r_1 the subrelation of r_2 if $\forall x, y, r_1(x, y) \implies r_2(x, y)$. A clause with such form is a subrelation pattern.

3 Group and Relation Modeling

Due to space limitation, we only provide the definition of group here. Readers who are not familiar with group theory are encouraged to read the appendix where a self-contained introduction of group theory is given.

Definition 3.1. Group. Let G be a set. We say that G is a group with law of composition $\star$ if the following axioms hold:

(G_1, closure of $\star$): the assignment $(g, h) \to g \star h \in G$, defines a function $G \times G \to G$. We call $g \star h$ the product of G and h.

(G_2, existence of identity): there exists $e_G \in G$ such that for every $g \in G$ we have $g \star e_G = G = e_G \star g$. We call e_G an identity of G.

(G_3, existence of inverse): for every $g \in G$ there exists some $h \in G$ such that $h \star G = e_G = g \star h$. We call such h an inverse of G.

(G_4, associativity): for any $g, h, k \in G$ we have $(g \star h) \star k = g \star (h \star k)$.

As we can see, the definitions of inversion and composition pattern of the relation are similar to G_1 and G_3 in the definition of the group. A symmetry pattern can be modeled as a group element of order 2. (In the case of RotatE, it corresponds to the rotation of magnitude π.) We summarize the correspondence in Table 1.

For embedding models like TransE, TorusE, RotatE, and DihEdral [19], relations are modeled as elements of the group acting on certain spaces. In particular, TransE model relations are elements of the translation group acting on $\mathbb{R}^n$. TorusE model relations as elements of translation group acting on the high dimensional torus $\mathbb{T}^n$. RotatE model relations as elements of the group of diagonal complex matrices (where each entry is of length 1) acting on the $\mathbb{C}^n$. DihEdral model relations as elements of Dihedral group acting on $\mathbb{R}^n$.

Table 1: The correspondence between relation modeling and group theory.

	Relation	Group	Example
Symmetry	$r(x, y) \implies r(y, x)$	$g_r = g_r^{-1}$	Marriage
Antisymmetry	$r(x, y) \implies \neg r(y, x)$	$g_r \neq g_r^{-1}$	Filiation
Inverse	$r_1(x, y) \implies r_2(y, x)$	$g_{r_1} = g_{r_2}^{-1}$	Hypernym and hyponym
Composition	$r_1(x, y) \wedge r_2(y, z) \implies r_3(x, z)$	$g_{r_1} \star g_{r_2} = g_{r_3}$	Mother's husband is father
Subrelation	$r_1(x, y) \implies r_2(x, y)$	-	Father of and parent of

Limitation: Combining composition and subrelation patterns, cases like $r_1(x, y) \wedge r_1(y, z) \implies r_1(x, z)$ would happen. An example of this type of relation pattern can be *sibling of* or *coworker with*. However, in the group formulation, $g_{r_1} \star g_{r_1} = g_{r_1}$. Therefore, g_{r_1} is modeled as the identity in the group. Due to the uniqueness of identity, all relations that exhibit the above pattern will be modeled as the same element in the group. This certainly limits the modeling capacity and is shared by all models that can be formulated under the group action perspective.

4 Main Theorem

Assuming that readers are familiar with concepts defined in the appendix, we are now ready to present two lemmas and the main theorem.

Lemma 4.1. Schur's Lemma. The only self-isomomorphisms of a finite dimensional irreducible representation of a group G on the complex vector space are given by scalar multiplication.

Proof. Fix an isomorphism $\phi : V \to V$ of complex representations of G. The linear map ϕ must have an eigenvalue λ over $\mathbb{C}$, and also some non-zero eigenvector v. But then the G-linear map (because both $\phi(x)$ and λx are both linear maps)

$$V \to V$$
$$x \to \phi(x) - \lambda x$$

has the vector v in its kernel, which is again a representation of G. Since V is irreducible, the kernel must be all of V. In other words, we have $\phi(x) = \lambda x, \forall x \in V$, which means ϕ is multiplication by λ. $\square$

Lemma 4.2. If V is a finite dimensional irreducible representation of an abelian group G, the action of G on V induces a homomorphism of $G-$representations.

Proof. By the definition of homomorphism of G-representations, the map ϕ ($V \to V; v \to g \cdot v$) induced by action of G must satisfy $h \cdot \phi(v) = \phi(h \cdot v)$ for all $v \in V$ and all $h \in G$, i.e., $h \cdot (g \cdot v) = g \cdot (h \cdot v)$ holds for all $v \in V, g, h \in G$. Indeed,

$$h \cdot (g \cdot v) = (h \star g) \cdot v = (g \star h) \cdot v = g \cdot (h \cdot v)$$

The second equation holds because G is abelian. The other two equations hold by the definition of group action. $\square$

Combining two lemmas above leads to our main theorem.

Theorem 4.3. Every finite dimensional irreducible complex representation of an abelian (both finite and infinite) group is one-dimensional.

Proof. By Lemma 5.2, the action of G on V is G-linear (does not hold for non-abelian groups). By Schur's lemma, the action of G on V is simply multiplication by some scalar, $\lambda(g)$, which of course, can depend on the element G. In any case, every subspace is invariant under scalar multiplication, so every subspace is a sub-representation. So since V is irreducible, it must have dimension one. $\qquad\square$

This does not mean that the representation theory of abelian groups over $\mathbb{C}$ is completely trivial. An irreducible representation of an abelian group is a group homomorphism

$$G \to GL_1(\mathbb{C}) = \mathbb{C}^*$$

where $\mathbb{C}^*$ denotes the multiplicative group of nonzero complex numbers. There can be many different homomorphisms of such form. Furthermore, it may not be obvious, given a representation of an abelian group, how to decompose it into one-dimensional sub-representations. Schur's Lemma guarantees that there is a choice of basis for V so that the action of an abelian group G is given by multiplication by

$$\begin{pmatrix} \lambda_1(g) & 0 & 0 & ... & 0 \\ 0 & \lambda_2(g) & 0 & ... & 0 \\ ... & & & & ... \\ 0 & 0 & ... & 0 & \lambda_n(g) \end{pmatrix}$$

where the diagonal entries $\lambda_i : G \to \mathbb{C}^*$ are group homomorphisms. But it does not tell us how to find this basis or the functions λ_i.

Connection to RotatE: Note the theorem applies to both finite and infinite abelian groups. For finite abelian groups, we can actually get stronger result. Since every irreducible representation of G is a homomorphism $\lambda_i : G \to \mathbb{C}^*$. Since each element of G has finite order (because G is finite), the values of $\lambda_i(g)$ are roots of unity. In particular, we have $|\lambda_i(g)| = 1$ for any i and $g \in G$. This is exactly the form of RotatE. In other words, *RotatE has the capacity to represent any finite abelian group.* [1]

5   Conclusion

In this paper, we present a group theoretical perspective of relation modeling in knowledge graph. We provide a self-contained introduction of group theory and representation theory to computer scientists. By utilizing the Schur's lemma from group representation theory, we find that existing embedding methods RotatE can model relations from any finite Abelian group.

We would like to point out a few directions. First, composition of relations in the real world is not communicative (son's wife $\neq$ wife's son), a straightforward way to model relations from non-abelian group is extending $\mathbb{C}$ to quaternion field $\mathbb{H}$, which is done by [23]. Understanding how much extra power this approach brings in from group representation theory is interesting. Second, it is important to chart the limitations of group theoretical perspective. Specifically, not being able to model uncertainty, sub relations and 1-N/N-1/N-N is posing restriction on this group theoretical perspective of relation modelings. Third, importing more sophisticated tools from group representation theory to extend the representation of finite groups to infinite groups (say, compact lie groups) and draw a connection with existing knowledge graph embedding methods. Fourth, designing more powerful knowledge graph embedding from this new perspective for real-world datasets.

---

[1]For computer scientists, the question of interest might be the what is the smallest dimension of a faithful representation so that any two different elements in the group are represented differently (minimal embedding dimension)? In the case of a finite abelian group with minimal generating set of size d, the smallest dimension of a faithful representation is d.

References

[1] BORDES, A., USUNIER, N., GARCIA-DURAN, A., WESTON, J., AND YAKHNENKO, O. Translating embeddings for modeling multi-relational data. In *Advances in neural information processing systems* (2013), pp. 2787–2795.

[2] DING, B., WANG, Q., WANG, B., AND GUO, L. Improving knowledge graph embedding using simple constraints. *arXiv preprint arXiv:1805.02408* (2018).

[3] DUMMIT, D. S., AND FOOTE, R. M. *Abstract algebra*, vol. 3. Wiley Hoboken, 2004.

[4] EBISU, T., AND ICHISE, R. Toruse: Knowledge graph embedding on a lie group. In *Thirty-Second AAAI Conference on Artificial Intelligence* (2018).

[5] FRALEIGH, J. B. *A first course in abstract algebra.* Pearson Education India, 2003.

[6] HAO, Y., ZHANG, Y., LIU, K., HE, S., LIU, Z., WU, H., AND ZHAO, J. An end-to-end model for question answering over knowledge base with cross-attention combining global knowledge. In *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)* (2017), pp. 221–231.

[7] HAYASHI, K., AND SHIMBO, M. On the equivalence of holographic and complex embeddings for link prediction. *arXiv preprint arXiv:1702.05563* (2017).

[8] KERSTING, K., AND DE RAEDT, L. Towards combining inductive logic programming with bayesian networks. In *International Conference on Inductive Logic Programming* (2001), Springer, pp. 118–131.

[9] MILLER, G. A. Wordnet: a lexical database for english. *Communications of the ACM 38*, 11 (1995), 39–41.

[10] POOLE, D. Probabilistic horn abduction and bayesian networks. *Artificial intelligence 64*, 1 (1993), 81–129.

[11] QU, M., AND TANG, J. Probabilistic logic neural networks for reasoning. *arXiv preprint arXiv:1906.08495* (2019).

[12] SINGLA, P., AND DOMINGOS, P. Discriminative training of markov logic networks. In *AAAI* (2005), vol. 5, pp. 868–873.

[13] SUCHANEK, F. M., KASNECI, G., AND WEIKUM, G. Yago: a core of semantic knowledge. In *Proceedings of the 16th international conference on World Wide Web* (2007), ACM, pp. 697–706.

[14] SUN, Z., DENG, Z.-H., NIE, J.-Y., AND TANG, J. Rotate: Knowledge graph embedding by relational rotation in complex space. *arXiv preprint arXiv:1902.10197* (2019).

[15] TASKAR, B., ABBEEL, P., WONG, M.-F., AND KOLLER, D. Relational markov networks. *Introduction to statistical relational learning* (2007), 175–200.

[16] TROUILLON, T., WELBL, J., RIEDEL, S., GAUSSIER, É., AND BOUCHARD, G. Complex embeddings for simple link prediction. In *International Conference on Machine Learning* (2016), pp. 2071–2080.

[17] WELLMAN, M. P., BREESE, J. S., AND GOLDMAN, R. P. From knowledge bases to decision models. *The Knowledge Engineering Review 7*, 1 (1992), 35–53.

[18] XIONG, C., POWER, R., AND CALLAN, J. Explicit semantic ranking for academic search via knowledge graph embedding. In *Proceedings of the 26th international conference on world wide web* (2017), International World Wide Web Conferences Steering Committee, pp. 1271–1279.

[19] XU, C., AND LI, R. Relation embedding with dihedral group in knowledge graph. *arXiv preprint arXiv:1906.00687* (2019).

[20] YANG, B., AND MITCHELL, T. Leveraging knowledge bases in lstms for improving machine reading. *arXiv preprint arXiv:1902.09091* (2019).

[21] YANG, B., YIH, W.-T., HE, X., GAO, J., AND DENG, L. Embedding entities and relations for learning and inference in knowledge bases. *arXiv preprint arXiv:1412.6575* (2014).

[22] ZHANG, F., YUAN, N. J., LIAN, D., XIE, X., AND MA, W.-Y. Collaborative knowledge base embedding for recommender systems. In *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining* (2016), ACM, pp. 353–362.

[23] ZHANG, S., TAY, Y., YAO, L., AND LIU, Q. Quaternion knowledge graph embedding. *arXiv preprint arXiv:1904.10281* (2019).

[24] ZHANG, Y., CHEN, X., YANG, Y., RAMAMURTHY, A., LI, B., QI, Y., AND SONG, L. Can graph neural networks help logic reasoning? *arXiv preprint arXiv:1906.02111* (2019).

A   Appendix

In this appendix, we provide a self-contained introduction of groups and their representations. We divide the contents into three parts. In the First part, we introduce the concept of group and give some elementary examples for developing intuitions. In the Second part, we introduce the notion of group action that can be used to unify several previous knowledge graph embedding methods. In the Third part, we introduce group representation and related concepts that are needed to understand the proof of the main theorem in the paper.

B   Basic concepts and examples

We sketch some elementary group theory that is needed for the paper. We refer readers to [3,5] for a more comprehensive overview of group theory.

Definition B.1. Group. Let G be a set. We say that G is a group with law of composition $\star$ if the following axioms hold:

(G_1, closure of $\star$): the assignment $(g, h) \rightarrow g \star h \in G$, defines a function $G \times G \rightarrow G$. We call $g \star h$ the product of G and h.

(G_2, existence of identity): there exists $e_G \in G$ such that for every $g \in G$ we have $g \star e_G = G = e_G \star g$. We call e_G an identity of G.

(G_3, existence of inverse): for every $g \in G$ there exists some $h \in G$ such that $h \star G = e_G = g \star h$. We call such an h an inverse of G.

(G_4, associativity): for any $g, h, k \in G$ we have $(g \star h) \star k = g \star (h \star k)$.

We will often denote a group $(G, \star)$ to emphasize the law of composition $\star$, or simply G when $\star$ is understood.

A group is called commutative or abelian if for every $g, h \in G$, we have $g \star h = h \star g$; finite if G is a finite set; infinite if G is an infinite set. The **order of group** is simply the cardinality of the group. The **order of element** $g \in G$ is smallest positive integer m such that $g^m = e_G$.

To make the reader familiar with the concept of the group, we introduce a few examples of groups.

- **Cyclic group C_n.** A group G is cyclic if there exists $x \in G$ such that $G =< x >= \{..., x^{-1}, e_G, x, x^2, ...\}$. We call such x a generator of G, and say that G is generated by x. In this paper we focus on finite cyclic group of order n, denoted by C_n, which is isomorphic (defined below) to the additive group of $\mathbb{Z}/n\mathbb{Z}$. $(\mathbb{Z}/n\mathbb{Z}, \star)$ is set $\{0, 1, 2, ..., n-1\}$ with modular arithmetic operation where $\bar{i} \star \bar{j} = \bar{i} + \bar{j}$ defines a group with identity $e_G = \bar{0}$. The inverse of $\bar{i} \in G$ is $\overline{-i}$.

- **Dihedral group D_{2n}.** Let $n > 2$ be an integer. Then, the dihedral group of order $2n$, D_{2n}, is the group of symmetries of the regular n-gon. In particular, we can write the elements of this group as $D_{2n} = \{e, a, ..., a^{n-1}, b, ba, ..., ba^{n-1}\}$, where b is the rotate by $2\pi/n$ counterclockwise rotation of the n-gon, and a is a reflection of the plane preserving the n-gon. We have
  $$a^i \star a^j = a^{i+j}, b \star a = a^{-1} \star b, a^n = e, b^2 = e.$$
  We say that $a, b \in D_{2n}$ are generators of D_{2n} subject to the above relations. Illustration of D_{2n} when $n = 4$ is shown in the Figure 1.

- **Automorphism group $AutX$.** A transformation of set X is a bijective map $f : X \rightarrow X$. It's easy to verify that all transformations of X form a group under composition. The identity element is the identity transformation e that fix every element in X. We denote this group by $AutX = \{f : X \rightarrow X | f \text{ is bijective}\}$. Depending on what X is, $AutX$ can have different realizations. We give two examples below.
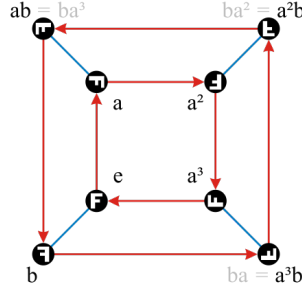
Figure 1: A visualization (Cayley graph) of dihedral group D_8. Both inner square and outer square correspond to cyclic group C_4. The figure is taken from wikipedia.

- **Symmetric group** S_n**.**When X is a finite set of cardinality n, the Aut X is called symmetric group S_n. For example, S_3 denotes the group of all permutations of set $\{1, 2, 3\}$. There are six elements in S_3 (S_n has $n!$ elements in in general). For the ease of presentation, we use cycle notation. (12) means send 1 to 2 and 2 to 1; (132) means send 1 to 3, 3 to 2, 2 to 1. Under the cycle notation, the six elements in S_3 are:
    * e: the identity permutation, fixing every element

    three transpositions: namely
    * (23) τ_1 : fixing 1 and switching 2 and 3
    * (13) τ_2 : fixing 2 and switching 1 and 3
    * (12) τ_3 : fixing 3 and switching 1 and 2

    and two 3-cycles: specifically
    * (123) σ : sending $1 \to 2, 2 \to 3, 3 \to 1$
    * (132) σ^{-1} : sending $1 \to 3, 3 \to 2, 2 \to 1$

- **Groups of linear transformation** $GL(V)$**.** When X is a vector space V, we are interested in the bijective self maps $f : X \to X$ that preserve the vector space structure (a.k.a., linear transformations). The set of all linear transformations of V form a group, which we denote by $GL(V)$. Of course, a linear transformation is a very special kind of bijective self-map, so $GL(V)$ is a subgroup (defined below) of $AutX$ in general. For the computer scientist, the vector space we are most comfortable with is the Euclidean space $\mathbb{R}^n$ or Complex space $\mathbb{C}^n$. The corresponding group $GL(\mathbb{R}^n)$ and its close cousin $GL(\mathbb{C}^n)$ are among the most important groups in mathematics and physics. Without loss of generality[2], we can think of them as $n \times n$ invertible real/complex matrices.

Definition B.2. Subgroup. A subset $H \subset G$ of a group $(G, \star)$ is a subgroup if H also forms a group under $\star$.

A simple example is that C_n is a subgroup of D_{2n}, as illustrated for the case of $n = 4$ in the Figure 1.

Definition B.3. Generator(s) of group. A set of generators is a set of group elements such that possibly repeated application of the generators on themselves and each other is capable of producing all the elements in the group.

For example, finite cyclic groups can be generated as powers of a single generator. Dihedral group D_{2n} is generated by two elements, reflection and rotation by $\frac{2\pi}{n}$.

Definition B.4. Group homomorphism. Let G and H be groups. A group homomorphism is a map $\psi : G \to H$ which preserves the multiplication: $\psi(g_1 \star g_2) = \psi(g_1) \star \psi(g_2)$.

- An isomorphism is the simplest example of a homomorphism. Indeed, an isomorphism can be defined as a bijective homomorphism. Isomorphism is the formal way of saying two groups are the "same".

---

[2]It can be shown that the group of linear transformations of $\mathbb{R}^n$, $GL(\mathbb{R}^n)$, is isomorphic to the group of invertible real $n \times n$ matrices. The similar results can also be shown in other fields.

- The inclusion of a subgroup H in a group G is an example of an injective but not surjective homomorphism. The projection of a product group $G \times H$ onto either factor is an example of a surjective but not injective homomorphism. That is, $\pi : G \times H \to G$ sending (g, h) to g is a homomorphism.

C Group Action

Definition C.1. Let G be a group, S an arbitrary (nonempty) set. A (left) group action of G on S is a function.
$$a : G \times S \to S;$$
$$(g, x) \to a(g, x) = g \cdot x$$
satisfying the following properties 1) $e \cdot x = x, \forall x \in S$. 2) $g \cdot (h \cdot x) = (g \star h) \cdot x, \forall g, h \in G, x \in S$.

When there exists a (left) group action of G on S via the function a, we will say that G **acts on** S.

Example. An relevant example of group action is RotatE. RotatE models relations as rotation in the complex vector space. Formally, it is equivalent to group $G_{RotatE} \overset{\text{def}}{=\!=} \{M | M \in diag\{r_1, r_2, ..., r_d\}, \forall i, r_i \in \mathbb{C}, \|r_i\| = 1 \}$ acting on the space $\mathbb{C}^d$. G_{RotatE} is a subgroup of matrix group over field $\mathbb{C}$.

D Group Representation

We will present some notions in group representation theory that are needed to understand the proof of the main theorem.

Definition D.1. Linear Representation. A linear representation of a group G on a vector space V is a group homomorphism
$$G \to GL(V).$$

We will usually omit the word "linear" and just speak of a representation of a group on a vector space unless there is a chance of confusion. We sometimes also say V is a "G-representation". A representation has dimension d if the dimension of vector space V is d.

For computer scientists, we can think of group representation as a way to embed group G into a space of linear transformations of V. We give a few examples below.

- Trivial representation. The trivial representation of G on V is the group homomorphism $G \to GL(V)$ sending every element of G to the identity transformation. That is, the elements of G all act on V trivially by doing nothing.

- The tautological representation of D_n on $\mathbb{R}^2$. We describe explicitly map $D_n \to GL(\mathbb{R}^2)$ when $n = 4$. Since there are two generators of D_n it is suffice to give the representation of two generators a and b.
$$a \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, b \to \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

- Alternating representation. Let σ be any permutation of n objects. Write σ as a composition of transpositions $\sigma = \tau_1 \circ ...\tau_t$; where each i just interchanges two elements, fixing the others. Of course, there may be many ways to do this (for example, the identity is (12)(12)) but one can check that the parity of t is well-defined. We say the sign of is 1 or -1 depending on whether is a product of an even or an odd number of transpositions. That is, there is a well-defined map
$$sign : S_n :\to \{1, -1\}$$
$$\sigma = \tau \circ ... \circ \tau_t \to (-1)^t$$

- Permutation representation of S_3. We can represent (embed) the symmetric group S_3 into $GL(\mathbb{R}^3)$ by sending, for example,
$$(12) \to \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} ; (13) \to \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} ; (123) \to \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Remark: Not all groups can be represented as a linear group acting on a vector space V. Some examples of nonlinear groups are infinite abelian 2-group $(\mathbb{Z}/2\mathbb{Z})^N$, Thompson's group, Higman's group. Those groups are rather exotic and are not discussed here.

The good thing is that **all** finite group can be represented on the Euclidean space $\mathbb{R}^{|G|}$. This is implied by the Cayley's theorem. We state the theorem without proof.

Theorem D.1. (Cayley's Theorem). Every group $(G, \star)$ is a transformation group. Specifically, G is isomorphic to a subgroup of Aut G.

Therefore as a corollary, Cayley's theorem implies that every group of finite order n is isomorphic to a subgroup of S_n.

Combining Cayley's theorem with permutation representation, we can represent any finite group on a space of dimension at most $|G|$. The representation of any finite group G over the field $\mathbb{F}$ is given by the group homomorphism.

$$G \to GL(\mathbb{F}^{|G|}).$$

$$g \mapsto \left[g : \mathbb{F}^{|G|} \to \mathbb{F}^{|G|}; e_h \mapsto e_{gh} \right].$$

Definition D.2. Subrepresentation. Let V be a linear representation of a group G. A subspace W of V is a subrepresentation if W is invariant under g—that is, if $g \star w \in W$ $\forall g \in G$ and $\forall w \in W$.

For example, every subspace is a sub-representation of the trivial representation on any vector space, since the trivial G action obviously takes every subspace back to itself. At the other extreme, the tautological representation of D_4 on $\mathbb{R}^2$ has no proper non-zero subrepresentations: there is no line taken back to itself under every symmetry of the square, that is, there is no line left invariant by D_4 .

Definition D.3. Irreducible representation. A representation of a group on a vector space is irreducible if it has no proper non-trivial subrepresentations.

As is shown above, there is no 1-dimensional subspace of $\mathbb{R}^2$ that is fixed by D_4, therefore the tautological representation T of D_4 on $\mathbb{R}^2$ is irreducible. In contrast, the permutation representation of S_3 on $\mathbb{R}^3(\mathbb{C}^3)$ is not irreducible: all permutation matrices preserve $(1, 1, 1)$.

The study of irreducible representation is justified by the following theorem.

Theorem D.2. (Maschke's Theorem) Given a finite group G, every representation of G on a nonzero, finite-dimensional complex vector space is a direct sum of irreducible representations.

Maschke's theorem allows one to make general conclusions about representations of a finite group G without actually computing them. It reduces the task of classifying all representations to a more manageable task of classifying irreducible representations since when the theorem applies, any representation is a direct sum of irreducible pieces.

We need one more concept before delving into the main theorem.

Definition D.4. A homomorphism of G-representations is a map $\phi : V \to W$ which preserves both the vector space structure and the G-action. That is, it is a linear map ϕ of the vector spaces (over the same field) satisfying $h \cdot \phi(v) = \phi(h \cdot v)$ for all $v \in V$ and all $h \in G$.

We also use "G-linear mapping" to refer a homomorphism of G-representations.