Exploring Multi-Banking Customer-to-Customer Relations in AML Context with Poincaré Embeddings

Lucia Larise Stavarache\textsuperscript{1}, Donatas Narbutis\textsuperscript{2}, Toyotaro Suzumura\textsuperscript{3}, Ray Harishankar\textsuperscript{1}, and Augustas Žaltauskas\textsuperscript{2}

\textsuperscript{1}IBM Global Business Services
\textsuperscript{2}IBM Lithuania, Client Innovation Center Baltic
\textsuperscript{3}IBM T.J. Watson Research Center

Abstract

In the recent years money laundering schemes have grown in complexity and speed of realization, affecting financial institutions and millions of customers globally. Strengthened privacy policies, along with in-country regulations, make it hard for banks to inner- and cross-share, and report suspicious activities for the AML (Anti-Money Laundering) measures. Existing topologies and models for AML analysis and information sharing are subject to major limitations, such as compliance with regulatory constraints, extended infrastructure to run high-computation algorithms, data quality and span, proving cumbersome and costly to execute, federate, and interpret. This paper proposes a new topology for exploring multi-banking customer social relations in AML context – customer-to-customer, customer-to-transaction, and transaction-to-transaction – using a 3D modeling topological algebra formulated through Poincaré embeddings.

1 Introduction

AML (Anti-Money Laundering) exploration can take different pathways for each financial or related institution and there are multiple factors which contribute, e.g., institution type, segment, region, language, country regulations. Absence of a unified strategy alongside with known technical limitations present main vulnerability and expose such fragmented financial domain to continuously evolving fraud schema risks. KYC (Know Your Customer) and AML requirements represent old problems for the financial domain, however, in the recent years the increased strength of the rules for data privacy and security boosted them as the focus of each financial player with major impact and massive financial fines.

The impact of GDPR (General Data Protection Regulation) \cite{1} in the financial field made it almost impossible for financial institutions to share malicious customer activity reports due to personal information constraints. The emphasized data privacy measures that had to be implemented to protect genuine customers also allow for the wicked ones to thrive – situation in many aspects resembles the “chicken and egg” paradigm \cite{2}. Groups of malicious customers usually operate as networks across multiple banks, therefore, analysis of their connectivity has to be performed.

Current technology solutions explore various topological structures, e.g., matrices \cite{3}, graphs \cite{4}, and various variants of neural networks \cite{5} with known limitations: the amount of data that can be analyzed, its quality and duplication, possibility to discover logical and cross-referenced relationships that can point to SAR (Suspicious Activity Reports). Given the current topologies, the complexity of each structure can reach $O(n^2)$ limiting the scaling, while transaction-to-transaction scenarios or correlating customer-to-transactions in billion-row data volumes becomes impossible to explore.
Recent year breakthroughs shifted the perspective from relational matrix analysis on big data systems (e.g., Hadoop) to applications of homogeneous graphs and neural networks, which enhance discovery of customer relationships and their interaction patterns. However, scalability of these models is limited by a large memory use, slow learning rate, difficulty to transfer them to new datasets, and low capability for distributed architectures. In banking ecosystems, restricted access to information and business flows makes the real-time processing difficult. Therefore, capturing SAR patterns and transferring them to an exhaustive topology that can learn, share, and express features in a federated multi-banking manner, as proposed by this paper, addresses a major industry problem.

The KYC/AML ecosystem involves multiple parties and steps for the detection of SARs, implying that analysts and regulators must have the ability to validate, explore, make corrections, feed new findings/patterns into the system, and have historical explainability of the results. Reporting back to the mentioned constraints, this paper proposes a new approach and topology for expressing the customer relationships, allowing to visualize and explore the data in a spherical 3D Poincaré space. The approach accounts for transformation from a sparse matrix 2D into a finite condensed 3D space, i.e., matrices are \( O(n^2) \) and high-graphs \( O(n \log(n)) \). Replacing the Euclidean distances with Poincaré allows the 3D sphere to be limited to a finite radius and create a natural taxonomy classifier of the customer relationships.

## 2 Data and Approach

The dataset was designed by the Financial Conduct Authority (UK) for their annual “2019 Global AML and Financial Crime TechSprint” \(^6\) in collaboration with SYNTHETICR, considering real world scenarios and AML/KYC patterns, i.e., laundromat, layered, dispersal, and collecting networks, among others. The explored dataset is based on a simulated multi-banking transaction scenario, comprising of six individual financial institutions with the characteristics provided in Table 1.

### Table 1: Data corpora characteristics of six banks.

| Corpora component | Volumetric |
|-------------------|------------|
| Accounts per bank | 1. 273k – large  
2. 177k – medium  
3. 154k – medium  
4. 147k – medium  
5. 95k – small  
6. 74k – small |
| Account holders | 396k – female  
316k – male  
58k – company |
| Unique individuals | ~200k after entity resolution  
typo corrections and deduplication |
| Customer nationality | 750k UK  
11k Poland  
5k Romania  
4k India  
others |

The total amount of data provided in CSV format was \( \sim 250 \text{ GB} \), containing \( \sim 0.9 \) million accounts and \( \sim 1 \) billion transactions over period of 24 months distributed across six banks. The CSV files were converted into HDF5 format using Vaex \(^7\) for real-time scanning, e.g., selecting all transactions of a target account and displaying transaction money amount as a function of time. The analyzed corpora contained only \( \sim 10\% \) (108k) transactions in the dataset, which were provided with “source-origin” and “destination-origin” account numbers, i.e., not cash, contact-less, or open-ended operations. For fast interactive exploratory analysis and visualization TOPCAT tool \(^8\) was used.

The dataset contained mappings of the following relationships: customer-to-bank, bank-to-account, account-to-transaction, customer-to-customer, customer-to-related-party, related-party-to-risk-intelligence. Data tables used for analysis and their aliases are presented in Table 2; columns doc_id, entity_id, and relation_duration_months were created. The financial crime activity for a specific customer was marked in RISK table, column fincrime_risk_exit was used as main indicator, while columns black_list and aml_flag were used as secondary indicators of suspicious activities.

Two money laundering schemes “collecting network” and “layered network” were investigated on the dataset in preparation for the Poincaré embedding of customer-to-customer relationship mapping to visualize fraudulent relationships in 3D space. The “collecting network” describes customers that act as an entry point for distinct networks of criminal customers (individuals or companies). Accounts that were opened and closed within the time span of 8 months were considered, correlating them with customers associated to the accounts with fincrime_risk_exit = true. The list of customers that most likely belong to this scheme was produced, identifying 124 account with accuracy of 90%.
Table 2: Data table schemas used for analysis.

| Alias: CUSTOMERS | LINK | PARTIES | RISK |
|------------------|------|---------|------|
| bank_id          | bank_id | bank_id | bank_id |
| bank_name        | bank_name | bank_name | bank_name |
| customer_id      | customer_id | customer_id | customer_id |
| company_registration_id | id_doc_number | ... | ... |
| doc_id           | ... | ... | ... |
| related_party_id | related_party_id | related_party_id | related_party_id |
| relation_start_date | ... | ... | ... |
| relation_end_date | ... | ... | ... |
| entity_id        | ... | ... | fincrime_risk_exit |

CUSTOMERS and RISK: 923,622 rows. fincrime_risk_exit for 2,785 banned customers.
id_doc_number: 90% (individuals). company_registration_id: 10% (companies).

The “layered network” activities are focused on the accounts that are connected to criminals. Any account that had any transfer with a confirmed criminal account identified in “collecting network” was considered. All the transactions per such account were binned into weeks with the underlying idea that this should be enough time to transfer money to and from the account. For each account every week the number of transactions and accumulated sum for inbound and outbound transfers was calculated. To take into consideration the low balance at the end of the week, all the accounts that had a balance larger than 20% of the accumulated sum of inbound transactions were filtered. This resulted in 288 identified fraudulent accounts with an accuracy of 90% on confirmed results.

However, the main analyzed relationship of this study was a customer-to-customer relation, comprising of social interactions, their duration time, activity, and risk criteria. It was considered to be the central relationship to explore under the following hypothesis: a customer (person identified by id_doc_number, i.e., passport, or company identified by company_registration_id, i.e., number given by common registry) can have numerous accounts in different banks and the linkage via customer-to-bank, bank-to-account, and account-to-transaction relations interconnects customers into a relation graph.

The graph can be imagined as arranged in three homogeneous planes (individuals, accounts, transactions) with the following properties: a) individuals can have 1:M accounts over multiple banks, b) some of individuals have associated risk intelligence records across different banks, c) account has 1:M transactions that identify behavior patterns by time, frequency, amount or operation. The above proposed 3D model of the customer relation graph extends enormously in Euclidean space. However, once embedded in n-dimensional Poincaré space (in subsequent analysis 3D is used), it is limited to a finite radius, allowing visualization, and has customer relationships classified by taxonomy. There is a possibility to extend the analysis in transaction time domain, since AML fraud schemes have patterns in time. From the provided data, a social relation graph of ~200,000 unique individuals within a simulated multi-banking dataset using Poincaré embeddings was explored. Two types of customers were considered: individuals and companies. Links between customers based on their social relations and their duration time was considered.

Note 1. Using existing approaches this large graph could be represented as a sparse square matrix, which would require 200 x 200 typical computer screens arranged as a grid to display it. Visual inspection of relationship matrix was performed without obtaining insight on the sparsity pattern in representation of the data, except that the connection structure on the large scale view looks random.

Note 2. There is a significant interest in banking data analysis to tackle the anti-money laundering problem via transaction analysis. A graph learning approach has been introduced [5] and was based on simulations within a single bank. Evolving graph convolutional networks have been proposed for node and edge classification, and link prediction [9].

Note 3. Big data manipulation exposes common “knowns” as incompleteness, redundancy, inconsistency and incorrectness, therefore entity resolution curation is a necessary step before starting the actual data analysis.
3 Experiments

Embeddings are a widely used approach to create a low-dimension representation of a given graph [10]. Comprehensive surveys have been provided for graph [11] and network [12] embeddings. Poincaré embeddings have shown a good performance in learning the representations of graphs in n-dimensional Poincaré ball by capturing context and hierarchy of related entities [13]. Taking as reference point the approach developed developed by [14] (see for the detailed description of the method and its application on various graphs), this paper explores the customer-to-customer relationship in a 3D Poincaré space, extending the approach into a banking domain with the purpose to identify potential suspicious/criminal activities across the banking operations.

3.1 Customer links

The linkages for the customer-to-customer relationship analysis were mapped using the data schema and table aliases described in Table 2. Columns of the tables are referenced by table’s name as a prefix, e.g., CUSTOMERS:bank_id. To define the Poincaré sphere space, the customer-to-customer relationship from table PARTIES was modelled with the following data observations: PARTIES:entity_id contains only individuals, not companies. To identify unique customers an internal match (i.e. group by) on PARTIES:id_doc_number was performed, resulting in 63,912 unique entities with sparse relationships links in range from 0 to 32 with various PARTIES:related_party_id entities.

To measure relationship duration table LINK was used to extract relationship start-end information. Relationship duration time (LINK:relation_duration_months) is an attribute of the link and is used as a weight of the graph edge between the nodes (entities) when performing the Poincaré embedding. The longest relation duration was \( \sim 600 \) months.

To identify entities in CUSTOMERS and PARTIES tables, id_doc_number was used for individuals and company_registration_id for companies. An entity is either an individual or a company, but no companies were found in PARTIES as noted above. A new doc_id column was created in these tables from id_doc_number with prefix “individual_” or from company_registration_id with prefix “company_”. Finally, internal match was performed on CUSTOMERS:doc_id and PARTIES:doc_id columns separately to count unique entities and to create CUSTOMERS:entity_id and PARTIES:entity_id columns. Entity cross-identification was realized through the following cross-joins:

\[
\begin{align*}
\text{PL} &= \text{merge}(
\text{PARTIES, LINK}, \\
& \quad \text{left_on}=[\text{PARTIES:bank_id, PARTIES:related_party_id}], \\
& \quad \text{right_on}=[\text{LINK:bank_id, LINK:related_party_id}]) \\
\text{PLC} &= \text{merge}(\text{PL, CUSTOMERS}, \\
& \quad \text{left_on}=[\text{LINK:bank_id, LINK:customer_id}], \\
& \quad \text{right_on}=[\text{CUSTOMERS:bank_id, CUSTOMERS:customer_id}]) \\
\text{PLCR} &= \text{merge}(\text{PLC, RISK}, \\
& \quad \text{left_on}=[\text{CUSTOMERS:bank_id, CUSTOMERS:customer_id}], \\
& \quad \text{right_on}=[\text{RISK:bank_id, RISK:customer_id}, \text{how}='left'])
\end{align*}
\]

Further analysis of the resulting table PLCR showed that the customer relation graph contains links from individuals to companies. To create a data structure suitable for Poincaré embeddings with [14] program, a list of tuples, consisting of (ID1, ID2, weight) must be provided. Since PARTIES:entity_id can be linked to CUSTOMERS:entity_id via several banks (up to six) with different relation duration times, it was decided to treat these relations separately. Finally, the data created for Poincaré embeddings contained these columns: ID1 = PARTIES:entity_id, ID2 = CUSTOMERS:bank_id + CUSTOMERS:entity_id, weight = LINK:relation_duration_months. There are 205,207 edges (relation links) in the graph and 151,044 nodes – unique entities, i.e., individuals and companies, which are treated as separate entities if have accounts in different banks.

3.2 Poincaré relationship mapping

A entity-to-entity relation graph was constructed from the list of (entity, entity, weight) tuples, which is passed as input to the algorithm to perform Poincaré embedding. The embedded entity (individual or a company) is represented as a 3D vector of float numbers within ranges \(-1 \) to 1. The entity representation vectors are moved in the Poincaré space using the following transformation sequence: a) initially the vectors are assigned random values close to zero (Gaussian with zero mean and standard deviation of 0.001), b) in each step a random pairing of entities is performed, c) for linked entities their vectors are brought closer together and not linked entities the vectors are moved further.
Figure 1: 3D Poincaré embeddings of the customer-to-customer relations are projected onto a plane. Dots show entity vectors with origin at the center, color-coded corresponding to number of connections they have, from 2 (yellow/green) to more than 10 (dark blue). Grey shaded circle is a Poincaré sphere of radius 1. Panels show progress of embedding iterations 30, 40, 60, and 80. Three groupings of customers emerge in panel b).

apart by computing the objective function as a sum of Poincaré distances between the vectors as described in [14].

Fig. 1 shows sequence of embeddings representations during the progress of model training; number of training iterations was limited due to data access policy set by the “2019 Global AML and Financial Crime TechSprint” [6] and additional iterations could have improved the results.

As can be seen in Fig. 1, it takes 80 iterations for some entity embedding vectors to asymptotically approach length of $\sim 1$ in Euclidean space, which corresponds to infinite distance in Poincaré space.

A useful feature of Poincaré representation is that the maximum length of embedding vector is 1, and since it is a non-linear space, entity vector representations are approaching 1 asymptotically. If the entities were not connected, they would be embedded on the surface of radius = 1 sphere and with maximum separation along great circle lines connecting them. If entities are highly connected, they are brought closer together.

As can be seen in Fig. 1, Poincaré embeddings of customer-to-customer relationship revealed interesting groupings of entities. Entities with low and high connectivity are initially separated into two clusters (Fig. 1b). Low connectivity entities are pushed towards the boundary of the lower left half of the sphere. Upper right is occupied by $\sim 28,000$ high connectivity entities. As training progresses, an intermediate elongated group appears (Fig. 1c–d), containing $\sim 6,000$ entities.
Figure 2: Same as Fig. 1d) after 80 iterations of Poincaré embedding, but color-coded in gray. Each panel shows a single entity marked by positive \texttt{fincrime\_risk\_exit} and magenta lines linking it to its related parties. Number of links is indicated in top left corner of each panel.

Although the initial embedding vector values and the training process is random, by running the embeddings with different initial conditions it was verified that the clusters finally obtained are stable and can be reliably distinguished from a random chance. Only the 3D rotation of the whole system is arbitrary.

4 Results and Discussion

Fig. 2 shows that entities marked with positive \texttt{fincrime\_risk\_exit}, i.e., have been banned from banks due to financial crimes, are highly-connected and belong to the grouping of other highly-connected entities. Each panel shows the “suspicious” entity with magenta lines indicating links to its related parties. Majority of the “suspicious” entities reside in the upper right compact grouping and have connections mostly within this grouping or intermediate elongated grouping below. Note, that connections are displayed as lines assuming Euclidean space for simplicity.

In Fig. 3 entities with highest number of connections are shown, starting with 32 and continuing to 20. Highly connected entities reside in the outer part of embeddings and are linked with upper right grouping of entities. Comparing Fig. 2 and Fig. 3 entities with positive \texttt{fincrime\_risk\_exit} coincide with grouping of highly connected ones.

There are 2,785 entities with positive \texttt{fincrime\_risk\_exit} and highly connected group contains ~28,000 entities, 90% of remaining ones could be suspects for further investigation. The 3D embeddings space was chosen to give additional degree of freedom, scalability, dimensionality reduction and new pattern approach perspective (shapes) in respect to other studies using 2D embeddings, but
still providing us with comprehensible insights. Entities that are “proxies”, connecting two or more clusters of highly connected entities, in many scenarios tie together a suspicious cluster with a cluster that at the first sight looks clean. Isolated entities have less than two connections which either stand by themselves (they are flagged as initial “unknowns”, as these do not exhibit any character or linkage for being classified as suspicious or clean), or are in the extended radius of a cluster, meaning that they will most-likely join that cluster in time and start forming relationships.

Using Poincaré embeddings it was possible to visualize and naturally classify a large interconnected datasets that would have been impossible to plot in a graph and clearly see the connections. A cluster identification technique, suitable for Poincaré distances, should be used to identify entity groupings of interest.

5 Conclusions

This paper demonstrated that 3D Poincaré embeddings can represent complex multi-banking customer social relations and allow identification of similarities among customers. Entities tagged by financial crime exit flag are highly connected and belong to the grouping of other highly connected entities.

The general construction of a relation high-graph is complicated and entity resolution is a major source of noise since same individuals or companies are present in registries of different banks. Working with simulated data partly addressed the problem, because individuals were uniquely iden-
tified via passport number and companies via company registration number, which simplified finding links between customers and embedding them in 3D Poincaré space.

The simulated data by SYNTHETICR aimed to follow real world financial interaction and crime scenarios to provide a global view of customer relations in multi-banking scenario. Nevertheless, consolidating the experiment in a real-bank scenario is necessary with the pursuit of entity resolution and deduplication before relationship embeddings to avoid noise and accuracy loss. The approach proposed in this paper could be extended to transaction data, potentially share-able as encrypted account numbers among banks, and applicable to the real world.

6 Future work

Going further the aim is to explore the capabilities of Poincaré embeddings in transactional relationships and to expand them by the federated learning concept using descriptive features, which are clear of personal information and can be shared between multiple banks. Analysis of known complex patterns, e.g., laundromat, and search for new patterns has to be performed. Clustering and discovery in a naturally and hierarchically embedded customer relation data is a key feature missing in current existing approaches based on matrix and graph analysis, which is needed to identify malicious networks. Carving this experiment to the financial industry domain, this paper opens the stage for near- and real-time SAR processing and data exploration, defining an architecture and topology for secure federated learning and insights sharing in a close to opaque industry.

Acknowledgments

We thank the organizers of “2019 Global AML and Financial Crime TechSprint”, “Looming Threats” team for discussions, Orestas Miskivas and Karolis Matuliauskas for their help with computing environment, and SYNTHETICR for providing the simulated data.

References

[1] General Data Protection Regulation. https://eugdpr.org.
[2] Chicken and egg situation. https://www.collinsdictionary.com/us/dictionary/english/a-chicken-and-egg-situation.
[3] Anti-Money Laundering Solution Deep Dive. https://s3.amazonaws.com/cdn.ayasdi.com/wp-content/uploads/2018/04/22170635/AML_Solutions_Deep_Dive_WP_051617v01.pdf.
[4] Nhien-An Le-Khac, Sammer Markos, Michael O’Neill, Anthony Brabazon, and M. Tahar Kechadi. An efficient customer search tool within an Anti-Money Laundering application implemented on an international bank’s dataset. CoRR, abs/1609.02031, 2016.
[5] Mark Weber, Jie Chen, Toyotaro Suzumura, Aldo Pareja, Tengfei Ma, Hiroki Kanezashi, Tim Kaler, Charles E. Leiserson, and Tao B. Schardl. Scalable Graph Learning for Anti-Money Laundering: A First Look. CoRR, abs/1812.00076, 2018.
[6] 2019 Global AML and Financial Crime TechSprint. https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint.
[7] Vaex. https://vaex.io.
[8] TOPCAT. http://www.star.bris.ac.uk/~mbt/topcat/
[9] Aldo Pareja, Giacomo Domeniconi, Jie Chen, Tengfei Ma, Toyotaro Suzumura, Hiroki Kanezashi, Tim Kaler, and Charles E. Leiserson. EvolveGCN: Evolving Graph Convolutional Networks for Dynamic Graphs. CoRR, abs/1902.10191, 2019.
[10] Stephen Bonner, Ibad Kureshi, John Brennan, Georgios Theodoropoulos, Andrew Stephen McGough, and Boguslaw Obara. Exploring the Semantic Content of Unsupervised Graph Embeddings: An Empirical Study. CoRR, abs/1806.07464, 2018.
[11] HongYun Cui, Vincent W. Zheng, and Kevin Chen-Chuan Chang. A Comprehensive Survey of Graph Embedding: Problems, Techniques and Applications. CoRR, abs/1709.07604, 2017.
[12] Peng Cui, Xiao Wang, Jian Pei, and Wenwu Zhu. A Survey on Network Embedding. CoRR, abs/1711.08752, 2017.
[13] Ivana Balazevic, Carl Allen, and Timothy M. Hospedales. Multi-relational Poincaré Graph Embeddings. CoRR, abs/1905.09791, 2019.
[14] Maximilian Nickel and Douwe Kiela. Poincaré Embeddings for Learning Hierarchical Representations. CoRR, abs/1705.08039, 2017.