On the Approximate Communal Fraud Scoring of Credit Applications

Clifton Phua
PhD Candidate
clifton.phua@infotech.monash.edu.au
http://www.bsys.monash.edu.au/people/cphua
2005

Other contributors:
Dr. Ross Gayler
Assoc. Prof. Vincent Lee
Assoc. Prof. Kate Smith

Overview

- Credit applications, fraud detection, and existing techniques
- Pair-wise matching, approximation of pair-wise communal score, smoothed *k*-wise score, and temporal and spatial weights
- Experiments: synthetic data, training and scoring phases, and results
- Discussion: directed graph, types of subgraphs, prediction scores, and related work

Importance of credit application fraud detection

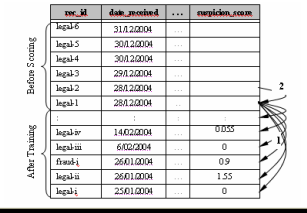
- Each credit application contains identity and non-identity information
- Credit bureaux collect millions of enquiries related to credit applications
- Identity crime
- First stage of credit life cycle

Existing techniques

- Attribute validation / verification rules
- Credit history matching
- Black lists
- Classification

Pair-wise matching (Part 1)

- Better timeliness, sensitivity, and specificity
- Pair-wise matching with application / time window, training and scoring phases



Pair-wise matching (Part 2)

- Pair-wise relationship with case-sensitive exact / fuzzy and cross matching
- Permanent, stable, and transient identity attributes

date_ received	given_ name	surname	street_ number	current_ address	previous_ address	suburb	postcode	state	home_ phone
31/12/2004	junwei	pan	3	jean avenue	marsh avenue	clayton	6000	vic	85777756
7/01/2004	chun wei	pin	2	sven jean	marsh ave	cleyton	3168	vic	85777756
6/01/2004	chun wei	pin	2	sven jean	marsh ave	cleyton	3168	vic	85777756
5/01/2004	junyu	pen	3	jean ave	marsh avenue	clayton	3168	vic	85777756
4/01/2004	junge	pin	3	jean avenue	marsh ave	clayton	3168	vic	85777756
3/01/2004	junwei	pan	3	jean avenue	marsh avenue	clayton	3168	vic	85777756
2/01/2004	junwei	pan	3	jean avenue	marsh avenue	clayton	3168	vic	85777756

Approximation of the pair-wise communal score (Part 1)

- Black list
  - Outlinks to known fraud applications
  - Outlinks to applications with excessive inlinks
- White list
  - Legitimate relationships
- Anomalous relationships
- No relationships

Approximation of the pair-wise communal score (Part 2)

- Score range, advantage, disadvantage, and secondary use

Application-Pairs	**Black List**	**White List**	**Anomalous Links**	**Unlinked**
Score range	Highest	Lowest	Medium to high	None
Main advantage	Reasonably accurate	Filters normal relations	Finds irregular relations	Contains weak or no relations
Main disadvantage	Time delay	Prone to manipulation	Reliant on attribute weights	Unlinked (once-off) fraud
Secondary use other than real-time fraud detection	Update attribute, normal, temporal, spatial weights	Viral marketing	Error detection	-

Smoothed *k*-wise scoring function

$$S(v_i) = \sum_{v_j \in M(v_i)} \left[(1-\alpha) * w_{ij} + \alpha * \frac{S(v_j)}{E_O(v_j)} \right]$$

- v_i refers to the current application which is being scored; v_j refers to the previous application which has been scored
- High suspicion score roughly captures the strong connection between v_i and v_j (high link weight), and/or the quality of v_j (high average suspicion scores), and/or the quantity of v_j (large number of connected applications); and vice versa
- α controls the contribution of previous scores of v_j

Communal, temporal, and spatial weights

$$\tilde{w}_{ij} = w_{communal\ ij} * w_{temporal\ ij} * w_{spatial\ ij}$$

- $\tilde{w}_{ij}$ roughly captures the relative strength of the communal links over time and space
- $w_{temporal}$ is the link weight derived from pair-wise time difference of *date_received*, $w_{spatial}$ is the link weight derived from pair-wise geographical distance of *postcode*
- High link weight roughly indicates strong connection, and/or no time difference, and/or maximum geographic distance between v_i and v_j; and vice versa

Experiments - synthetic data

- External concerns: Privacy, confidentiality, ethical, and competitive; Technical reasons: Data set size, population drift, concept drift, adversarial countermeasures, and data entry error rates
- Original records, duplicate records (uniform and poisson distributions), error rates
- 52,750 applications, 19 attributes which span the entire year 2004. ~10% are fraudulent (regular frauds, occasional frauds, seasonal frauds, and once-off frauds). ~90% are legal applications and 50 are hand-crafted applications with both fraudulent and legal examples

Experiments - training & scoring phases

- All attributes are included except *rec_id* (all unique), *date_received* (for calculating $w_{temporal}$), *postcode* (for calculating $w_{spatial}$) *street_number*, *suburb*, and *state* (too dense). Also, three additional attributes are created to store *suspicion_score*, *outlinks*, and *inlinks*
- Train 10,000 applications (01/01/2004 to 10/03/2004); score 42,750 applications from (10/03/2004 to 31/12/2005). The scoring phase retains trained applications which have non-zero scores

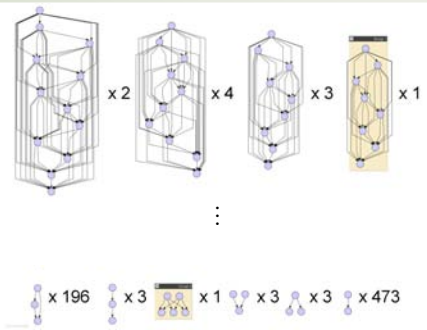
Experiments - results

- Parameter tuning and scalability issues
- Significant change of link activity in the scoring phase over the training phase which is probably due to seasonal frauds

	Training	Scoring
g	10,000	44,238
w	10,000	10,000
$T_{similarity}$	0.8	0.8
$T_{\overline{d}}$	10	10
$T_{fraud} = T_{anomalies}$	3	3
$\mathfrak{R}_W$	1.26	1.26
α	0.8	0.8
h	2,917	17,868
$computation_{time}$	2.7 secs/app 4.52 mins	6.5 secs/app 4,688 mins
$\overline{d}_I = \overline{d}_O = \frac{h}{g}$	0.292	0.418
$\Delta = \frac{h}{g(g-1)}$	0.0000029	0.00001
$\frac{\sum_{i=1}^{H} S(v_i)}{g}$	0.116	0.197

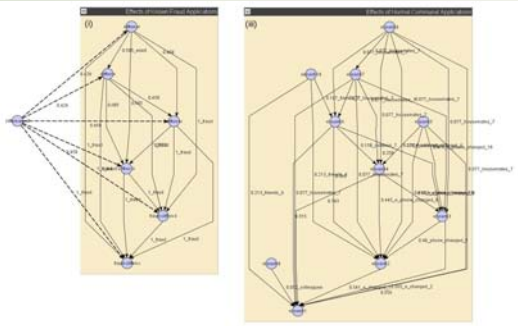
Discussion - directed graph

- The descriptive directed graph allow the analyst to visually inspect / explore the subgraphs
- The following slide presents the compressed hierarchical subgraph structures of linked applications after training.
- The synthetic data generation process causes all the 27 different types of subgraphs to be disconnected although this is unlikely with real applications



Discussion - types of directed subgraphs

- Subgraph (i) consists of known fraud applications and the subsequent linked applications.
- Subgraph (ii) is made up of linked applications which have frequent address changes by the same identity.
- In addition to subgraph (ii), subgraph (iii) includes linked applications submitted by an identity's social network.
- Subgraph (iv) consists of linked applications with data entry errors which may also turn out to be frauds.
- Subgraph (v) illustrates synthetic applications which "mix and match" attributes from some other previous applications.
- Subgraph (vi) have all exact applications to demonstrate the effects of temporal and spatial weights.
- Subgraph (vii) shows the effects of exponential smoothing.



Discussion - prediction scores

- The predictive suspicion scores allow the analyst to rank the most recent applications and investigate the most suspicious applications
- The decision thresholds can be defined as:
  If $0 < S(v_i) \leq T_{lower}$, then current application v_i is unusual
  If $T_{lower} < S(v_i) < T_{upper}$, then v_i is suspicious
  If $S(v_i) \geq T_{upper}$, then v_i should be investigated
  If the investigated v_i is fraudulent, feedback should be provided to the fraud detection system
- If T_{lower} = 0.8 and T_{upper} = 1, then out of 50 applications, thirteen are be investigated (strong fraud symptoms) and three are considered suspicious (some fraud symptoms)

Related work

- There is no academic research, to the best of our knowledge, into the scoring of dynamic credit applications which accounts for its sparse-identifiers, communal, temporal, and spatial aspects
- However, there are other related and established application fields in multi-attribute pair-wise matching (for example, record linkage/de-duplication detection), and single-attribute communal scoring/directed graphs with explicit links (for example, telecommunications fraud detection, terrorist detection, social network analysis, and webpage ranking)

The End of Presentation ☺

Questions?