Aplikasi Teorema Bayes dalam Penyaringan Email

Dyah Diwasasri Ratnaningtyas (18209005)
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
dyah.diwasasri@students.itb.ac.id

***Abstrak*—Email adalah salah satu media penyebaran komunikasi yang mudah dan praktis digunakan oleh sebagian besar masyarakat dan komunitas saat ini. Kegunaan email sebagai media komunikasi tidak terlepas dari dampak positif dan negatif dari email itu sendiri. Dampak negatif yang dihasilkan salah satunya dapat berupa spam mail atau biasa disebut junk mail yakni penyalahgunaan sistem pesan elektronik untuk mengirim berita iklan dan keperluan lain secara massal dan tidak dikehendaki penerimanya. Hingga saat ini permasalahan spam mail masih terus berkembang seiring dengan berkembangnya sistem penyaringan email (email filtering) yang menggunakan berbagai metode penerapan. Salah satu metode penerapan dari email filtering yang cukup efektif yakni menggunakan metode probabilistik dengan pengaplikasian teorema Bayes yang difokuskan pada klasifilasi Naive Bayesian untuk mengidentifikasi spam mail sehingga pada akhirnya akan dihasilkan ffilter anti spam yang akurat dengan sesedikit mungkin tingkat false positif dan false negatif.**

***Kata Kunci*—spam mail, email filtering, teorema bayes, bayesian filtering, naive bayesian**

I. PENDAHULUAN

1.1 Latar Belakang

Email (Electronic Mail) adalah salah satu media komunikasi dengan metode bertukar informasi secara digital melalui internet atau jaringan komputer lain. Informasi dapat berupa pesan, file (attachment), atau berupa media iklan dan promosi dari suatu perusahaan atau produk tertentu. Dari segi penggunaannya sendiri, email adalah alat komunikasi yang mudah digunakan oleh seluruh kalangan masyarakat baik untuk kepentingan personal maupun kepentingan suatu instansi atau komunitas. Selain itu fasilitas email terhitung murah dan tidak terpatok pada jarak tujuan pengiriman. Penggunaan email juga memiliki dampak positif dan negatif. Dampak positifnya seperti yang telah dijabarkan tadi yaitu mudah digunakan, murah, dan jangkauan tempat luas sedangkan dampak negatif yang ditimbulkan salah satunya adalah spam mail. Spam mail atau biasa disebut junk mail itu sendiri adalah penyalahgunaan sistem pesan elektronik untuk mengirim berita iklan dan keperluan lain secara massal dan tidak dikehendaki penerimanya. Isi dari spam email biasanya berupa iklan produk barang atau jasa, virus, pornografi, dan content – content tidak penting lainnya.

Kerugian yang didapat dari penerimaan spam mail antara lain inbox email akan penuh dengan spam mail yang nantinya menutup email lain yang sekiranya lebih penting. Selain itu untuk menghapus spam mail tersebut satu persatu akan membuang waktu secara percuma. Hal ini belum termasuk apabila pengguna tidak sengaja membuka spam email yang berisi content virus di dalamnya sehingga merusak sistem komputer pengguna itu sendiri.

Langkah antisipasi dari spam mail ini sendiri sudah ada yaitu dengan cara penyaringan email (email filtering) melalui perangkat lunak khusus email filtering atau fasilitas email filtering yang saat ini telah disediakan oleh beberapa host mail. Ada beberapa metode dari email filtering, salah satu metode email filtering yang cukup efektif yaitu naive bayesian filtering. Merode ini merupakan pengaplikasian dari teorema probabilitas yaitu teorema bayes dan klasifikasi naive bayesian. Pengaplikasian kedua teorema tersebut menghasiklan sebuah sistem email filtering yang cukup efektif, memiliki tingkat akurasi cukup tinggi, dan menghasilkan galat minimum sehingga mudah untuk dikembangkan.

1.2 Tujuan Penulisan

Tujuan penulisan makalah adalah sebagai berikut :

1.2.1 Memotivasi mahasiswa agar memiliki kemampuan menulis untuk menuangkan ide-ide atau hasil risetnya;

1.2.2 Melakukan eksplorasi terhadap isu, metode, dan masalah yang dipelajari dalam pengembangan serta menyebarkan aplikasi yang mendukung teknologi informasi;

1.2.3 Sebagai media untuk berbagi informasi hasil-hasil pemikiran dan penelitian.

1.3 Ruang Lingkup

Ruang lingkup penulisan makalah ini adalah aplikasi teori peluang dan statistika dalam bidang sistem dan teknologi informasi. Dalam makalah ini

adalah pengaplikasian teorema bayes yakni naive bayesian dalam metode penyaringan email (email filtering).

II. PEMBAHASAN

2.1 Email Filtering

Dalam penggunaan layanan email tentu saja tidak terlepas dari spam mail yang dari hari ke hari jumlah spam mail yang diterima oleh sebagian besar pengguna email semakin banyak dan tentunya sangat mengganggu. Hal ini belum termasuk kemungkinan dalam spam mail tersebut mengandung virus atau hal – hal yang tentunya tidak diinginkan. Pengguna email biasanya mengalami masalah dalam menghapus spam mail satu persatu sehingga banyak waktu yang tebuang percuma.

Salah satu cara yang dapat digunakan yaitu email filtering dimana mengaplikasikan proses pemilahan email untuk menentukan apakah email tersebut adalah email spam atau bukan spam. Kebutuhan dari email filtering adalah sebagai berikut :

- *Binary Class* – Email filtering hanya mengklasifikasikan email ke dalam kelas spam mail dan legitimate mail
- *Easy Computation* – Melakukan komputasi terhadap sifat data email yang memiiki dimensi tinggi
- Prediksi – Mampu memprediksi kelas dari suatu email
- Learning – Mampu melakukan learning (menyimpan memori) dari email – email yang sudah ada sebelumnya
- Kinerja – Memiliki akurasi tinggi, meminimalisir nilai false positif dan mentolerir nilai false negatif yang cukup tinggi

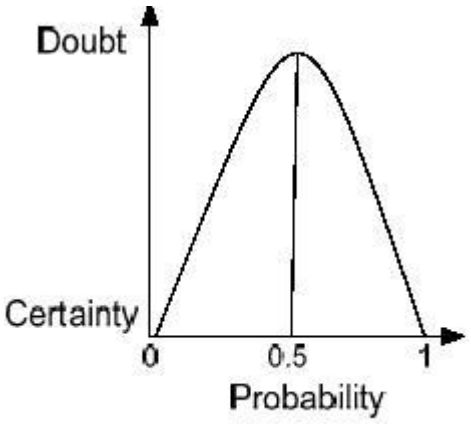
Beberapa metode yang dapat digunakan untuk email filtering antara lain *Black listing* dan *White listing, Signature-Based Filtering, Naive Bayesian (Statistical) Filtering, Keyword filtering, Rule-based filtering, dan Challenge-response filtering.* Pada kali ini metode yang disorot adalah Naive Bayesian Filtering.

2.2 Teorema Bayes

Nama teorema Bayes diambil dari nama penemu teorema tersebut yaitu Thomas Bayes (1702 – 1761). Teorema Bayes dalam probabilitas dan statistika menunjukkan hubungan antara dua probabilitas kondisional dimana kedua kondisi tersebut saling bertolak belakang dan memperhitungkan bahwa probabilitas suatu kejadian (hipotesis) bergantung pada keadaan lain (bukti). Ringkasnya yaitu teorema tersebut menyatakan bahwa suatu kejadian yang terjadi di masa depan atau yang belum terjadi dapat diprediksi sebelumnya dengan syarat kejadian sebelumnya telah terjadi.

Probabilitas itu sendiri dapat dideffinisikan sebagai ukuran kuantitatif dari suatu ketidakpastikan informasi atau peristiwa. Probabilitas memiliki indeks nilai yang berkisr antara 0 sampai 1. Hal ini juga dipengaruhi oleh jumlah total kejadian selama percobaan. Apabila probabilitas suatu keadaan adalah 0 (nol), maka keadaan tersebut dapat diyakinkan pasti tidak akan terjadi. Namun, apabila probabilitas suatu keadaan adalah 1, maka keadaan tersebut dapat diyakinkan pasti akan terjadi. Sedangkan misalkan suatu kejadian memiliki probabilitas 0,5 maka kejadian tersebut memiliki tingkat keraguan yang maksimum.

Keadaan probabilitas dapat digambarkan seperti di bawah ini :



Gambar 1 Grafik Probabilitas

Dalam Teorema Bayes sering disebut istilah probabilitas bersyarat. Probabilitas bersyarat adalah suatu kejadian yang mungkin atau tidak tergantung pada terjadinya peristiwa lain. Ketergantungan ini dapat ditulis dalam bentuk probabilitas bersyarat sebagai berikut :

$$P(A \mid B)$$

Maksudnya adalah probabilitas bahwa kejadian A akan terjadi apabila kejadian B terjadi atau bisa disebut sebagai probabilitas gabungan kejadian A dan B. Dari kondisi tersebut dapat dirumuskan suatu hubungan sebagai berikut :

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)}$$

$$P(B \mid A) = \frac{P(A \cap B)}{P(A)}$$

$$P(A \cap B) = P(B \mid A)P(A) = P(A \mid B)P(B)$$

Dengan penjelasan sebagai berikut :

- P(A) adalah probabilitas sebelum (tanpa syarat atau probabilitas marjinal) kejadian A. Maksudnya ini adalah kejadian A sebelum memperhitungkan segala informasi tentang kejadian B.
- P(B) adalah probabilitas atau marjinal sebelum kejadian B dan bertindak sebagai konstanta normalisasi.
- P(A|B) adalah probabilitas bersyarat dari kejadian A apabila kejadian B telah terjadi.
- P(B|A) adalah probabilitas bersyarat dari kejadian B apabila kejadian A telah terjadi.

Misalkan kejadian A adalah independen atau saling bebas terhadap kejadian B, maka teorema Bayes dapat dituliskan sebagai berikut :

$$P(A \mid B) = P(A)$$
$$P(B \mid A) = P(B)$$

Secara Umum teorema Bayes dapat dituliskan dalam bentuk :

$$P(A_i \cap B) = \frac{P(B \mid A_i)P(A_i)}{\sum P(B \mid A_i)P(A_i)}$$

Jika(A_i) membentuk partisi dari ruang kejadian untuk setiap (A_i) dalam partisi.

Teorema Bayes dalam hal ini memberikan representasi secara matematis tentang bagaimana probabilitas bersyarat kejadian A dan B yang diberikan adalah saling berkaitan dengan probabilitas bersyarat B karena A.

2.3 Naive Bayesian

Variasi lain dari teorema Bayes yang digunakan untuk metode email filtering adalah Naive Bayesian Filtering. Naive bayesian klasifikasi adalah suatu klasifikasi berpeluang sederhana berdasarkan aplikasi teorema Bayes dengan asumsi antar variabel penjelas saling bebas (independen). Dalam hal ini, diasumsikan bahwa kehadiran atau ketiadaan dari suatu kejadian tertentu dari suatu kelompok tidak berhubungan dengan kehadiran atau ketiadaan dari kejadian lainnya.

Naive Bayesian dapat digunakan untuk berbagai macam keperluan antara lain untuk klasifikasi dokumen, deteksi spam atau filtering spam, dan masalah klasifikasi lainnya. Dalm hal ini lebih disorot mengenai penggunaan teorema Naive Bayesian untuk spam filtering

Teorema Naive Bayesian memiliki beberapa kelebihan dan kekurangan yaitu sebagai berikut :

Keuntungan Naive Bayesian :

- Menangani kuantitatif dan data diskrit
- Kokoh untuk titik noise yang diisolasi, misalkan titik yang dirata – ratakan ketika mengestimasi peluang bersyarat data.
- Hanya memerlukan sejumlah kecil data pelatihan untuk mengestimasi parameter (rata – rata dan variansi dari variabel) yang dibutuhkan untuk klasifikasi.
- Menangani nilai yang hilang dengan mengabaikan instansi selama perhitungan estimasi peluang
- Cepat dan efisiensi ruang
- Kokoh terhadap atribut yang tidak relevan

Kekurangan Naive Bayesian :

- Tidak berlaku jika probabilitas kondisionalnya adalah nol, apabila nol maka probabilitas prediksi akan bernilai nol juga
- Mengasumsikan variabel bebas

Naive Bayesian dapat dirumuskan sebagai berikut :

$$P(X \mid C_i) = \prod_{k=1}^{n} P(x_k \mid C_i)$$

Dengan tiap set atribut $X = \{X_1, X_2, \ldots, X_d\}$terdiri dari *n* atribut.

Atau dapat dituliskan sebagai berikut :

$$P(X \mid C_i, \ldots\ldots, C_n) = \frac{1}{Z} P(X) \prod_{k=1}^{n} P(C_k \mid X\ )$$

2.4 Aplikasi Naive Bayesian Filtering dalam Email Filtering

Bayesian Filtering memudahkan kita untuk memprediksi kemungkinan apakah suatu email adalah spam dari hasil tes kata yaitu keadaan dari kata – kata tertentu yang telah ditentukan sebelumnya. Misalnya, kata – kata seperti "viagra" memiliki peluang lebih besar untuk muncul dalam spam mail dibanding email normal.

Spam filtering berdasarkan sistem blacklist adalah kurang direkomendasikan karena metode tersebut terlalu ketat dan kemungkinan false positif cukup tinggi. Tetapi, Bayesian filtering memberikan jalan tengah karena konsep yang digunakan adalah probabilitas.

Pada saat menganalisa kata – kata dalam sebuah email maka dapat dihitung peluang bahwa email tersebut adalah spam, bukan langsung merujuk pada keputusan ya atau tidak dalam pengidentifikasian awal. Apabila email tersebut memiliki 99% peluang email spam, maka kemungkinan besar email tersebut adalah email spam. Semakin berkembangnya filter makan akan semakin diperbaharui probabilitas kata – kata tertentu yang merujuk pada email spam. Kata – kata tertentu telah ditentukan pada awal. Bayesian filter dapat memeriksa beberapa kata dalam satu baris sebagai jalur data.

Aplikasi dari Teorema Bayes dalam Email filtering secara mudahnya adalah sebagai berikut :

- Kejadian A : Email adalah spam
- Tes X : Email mengandung kata – kata tertentu (X)

$$P(A|X) = \frac{P(X|A)P(A)}{P(X)}$$

Dalam aplikasi nyata, email filtering menekankan pada konsep Naive Bayesian dengan kasus sebagai berikut :

Misalkan seorang pengguna mendapat sebuah email. Dengan metode Naive Bayesian filtering hal yang dilakukan pertama kali yaitu membagi email tersebut per kata secara independen. Tiap kata tersebut dinyatakan dalam notasi $W_{i.}$ Untuk mengetahui peluang bahwa email tersebut adalah spam mail maka dapat dinyatakan dalam sebuah pernyataan sebagai berikut :

$$P(spam|W_i)$$

Pada langkah ini diaplikasikan Teorema Bayes berdasarkan pengamatan pada kata tersebut :

$$P(spam|W_i) = \frac{P(W_i|spam)P(spam)}{\sum_{i=1}^{n} P(W_i|spam)P(spam\ )}$$

Berdasarkan persamaan tersebut maka dapat diasumsikan bahwa :

- Total *n* kata yang muncul di spam mail maupun non-spam mail telah didata dalam sebuah list
- Peluang independen dari setiap kata yang muncul apabila email telah dinyatakan spam didata dalam list
- Kata W_i terdapat dalam list
- Diketahui jumlah total dari spam mail dan non-spam mail

Cara untuk mendeteksi apakah email tersebut adalah spam maka dilakukan dua langkah yaitu sebagai berikut :

a. Mengidentifikasi jumlah dari setiap kata yang muncul apakah termasuk spam atau non-spam mail, ini mengarahkan kita untuk mendefinisikan $P(W_{|i}|spam)$ dan $P(W_{|i}|non-spam)$ berdasarkan probabilitas kondisional yang tidak terdapat dalam persamaan diatas. Bagaimanapun juga, ini akan muncul dalam perhitungan $P(non-spam|W_{|i})$
b. Menghitung jumlah total spam dan non-spam mal, ini mengarahkan kita untuk mendefinisikan $P(spam)$ dan $P(non-spam)$

Sampai tahap ini, kita telah menyatakan peluang bahwa email tersebut adalah spam mail berdasarkan pengamatan dari setiap kata yang terdapat dalam email tersebut. Ini merupakan pendekatan sub-optimal dimana merupakan pendekatan yang lebih baik dapat di komputasikan sehingga dapat dinyatakan bahwa email tersebut adalah spam mail berdasarkan seluruh data yang tersedia (seluruh kata yang terdapat dalam email tersebut).

Ada banyak cara untuk menyelesaikan permasalahan ini, salah satu pendekatan yang mungkin dapat dipertimbangkan yaitu melalui bukti yang disediakan oleh seluruh kata dalam email tersebut kemudian dikomputasi dengan peluang kombinasi dari seluruh kata tersebut. Pendekatan ini diprediksi dengan asumsi bahwa kondisi dari seluruh kata dalam email tersebut adalah independen (bebas) terhadap satu sama lain. Misalkan asumsi saling bebas itu benar adanya maka kita dapat merumuskan kombinasi peluang sebagai berikut :

$$P(spam) = \frac{\prod_{k=1}^{K} P_k}{\prod_{k-1}^{K} P_k + \prod_{k=1}^{K} (1-P_k)}$$

Dimana *K* adalah jumlah kata yang terdapat dalam email, dan P_k didefinisikan sebagai berikut :

$$P_k = P(spam|W_k)$$

$$P_k = \frac{P(W_k|spam)P(spam)}{P(W_1|spam)P(spam) + P(W_2|spam)P(spam) + .. + P(W_{N1}|spam)P(spam)}$$

Dari persamaan diatas dapat dihitung peluang bahwa email yang masuk adalah spam dengan mengombinasikan peluang independen dari email yang diidentifikasi sebagai spam berdasarkan kemunculan kata dalam email tersebut. Misalkan ada sedikitnya dua implementasi yang berbeda dari persamaan di atas, dalam satu kasus, kita dapat mempertimbangkan *hanya* kata – kata unik yang terdapat dalam email. Alternatif lain, kita dapat mempertimbangkan *setiap* kata dalam email tersebut walaupun dipakai secara berulang kali.

Dari pernyataan diatas dapat disimpulkan bahwa kemungkinan email yang masuk ke inbox pengguna adalah spam, tetapi ini hanya sebuah kemungkinan, belum pernyataan akhir.

Hal yang dapat disimpulkan secara jelas adalah apabila peluang spam email bernilai lebih dari 0,5 maka dapat dipastikan email tersebut adalah spam, apabila peluang bernilai kurang dari 0,5 maka dapat dideklarasikan bahwa email itu bukan spam. Namun, apabila ternyata peluangnyatepat sebesar 0,5 maka nantinya akan diserahkan kepada pengguna email apakah nantinya pengguna mendeteksi dan menolak email tersebut atau tidak.

2.5 Kenggulan Naive Bayesian dalam Email Filtering

Naive bayesian filtering memiliki kelebihan dibandingkan dengan metoda *filtering* yang lain, diantaranya adalah:

1. Komputasi yang mudah dan praktis
2. Dapat memeriksa *email* secara keseluruhan yaitu memeriksa token di *database spam* maupun *legitimate*.
3. *Supervised learning* yaitu secara otomatis akan melakukan proses *learning* dari *email* yang masuk.
4. Cocok diterapkan di level aplikasi *client*/*individual user*.
5. Cocok diterapkan pada *binary class* yaitu klasifikasi ke dalam dua kelas.
6. Metode ini *multilingual* dan internasional. *Bayesian filtering* meng*generate* token dengan pengenalan karakter sehingga mampu diimplementasikan pada *email* dengan bahasa apapun.

III. KESIMPULAN

Kesimpulan yang dapat ditarik adalah sebagai berikut :

1. Teorema Bayes adalah dasar dari probabilitas sebagai sumber dari pengaplikasian berbagai hal dalam dunia nyata dengan klasifikasi Naive Bayesian adalah adalah kasus spesifik dari kategori ini
2. Bayesian spam filtering adalah aplikasi dari klasifikasi Naive Bayesian dalam hal email filtering yang berhubungan dengan peluang yang dapat didapat dari beberapa percobaan
3. Bayesian spam filter merupakan salah satu aplikasi dari teori probabilitas dan statistik dalam bidang Sistem dan Teknologi Informasi yaitu email filtering.

IV. UCAPAN TERIMA KASIH

Dalam pembuatan makalah ini terjadi banyak hal yang tentunya mempengaruhi pembuatan makalah ini. Oleh karena itu, penyusun menyampaikan ucapan terima kasih kepada :

1. Allah SWT, atas rahmat-Nya sehingga makalah ini dapat selesai tanpa halangan suatu apapun
2. Orang Tua, atas dukungan dan doanya sehingga makalah ini dapat terselesaikan
3. Pak Rinaldi Munir, atas bimbingan selama ini dalam mata kuliah Probabilitas dan Statistik
4. Teman – teman, atas dukungannya selama ini

DAFTAR PUSTAKA

[1] http://en.wikipedia.org/wiki/Bayesian_spam_filtering
(Tanggal akses : 15 Desember 2010)
[2] http://en.wikipedia.org/wiki/Bayes'_theorem
[3] (Tanggal akses : 15 Desember 2010)
[4] http://betterexplained.com/articles/an-intuitive-and-short-explanation-of-bayes-theorem/
(Tanggal akses : 15 Desember 2010)
[5] http://id.wikipedia.org/wiki/Spam
[6] (Tanggal akses : 15 Desember 2010)
[7] http://nayyeri.net/an-introduction-to-bayesian-spam-filtering
(Tanggal akses : 15 Desember 2010)
[8] http://raza-rizvi.blogspot.com/2010/03/creating-spam-filter-using-naive-bayes.html
(Tanggal akses : 15 Desember 2010)
[9] http://www.sharewareconnection.com/antispam-marisuite.htm
(Tanggal akses : 16 Desember 2010)
[10] http://www.vjs.org/spam/bayesian-analysis.html
(Tanggal akses : 16 Desember 2010)
[11] http://www.codeproject.com/KB/recipes/Naive_Bayes
(Tanggal akses : 16 Desember 2010)
[12] http://www.green-baby.co.cc/2010/12/konsep-naive-bayes.html
(Tanggal akses : 16 Desember 2010)

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 17 Desember 2010

Dyah Diwasasri 18209005