

Analysis of Do-Not-Spam Registry

Eran Reshef* and Eilon Solan†

August 4, 2005

Abstract

We study how the launching of a do-not-spam registry will affect the internet's efficiency. We show that as long as the cost of sending spam messages is not high, having rich users (who have high-quality filters) join the registry has the desirable effect of lowering the number of spam messages sent to each user, while having poor users (who have low-quality filters) join the registry has the opposite undesirable effect.

We also show that the registry improves the total efficiency of the internet - as long as the cost of sending spam messages is not high; as more users join, the total number of spam messages sent to all users decreases.

1 Introduction

Bulk electronic mail, also known as spam mail, has become a major danger to the efficiency of the internet. Postini reports that spam activity has increased over 65% since January, 2002, and that roughly 80% of e-mail transportation is spam. The report states that “this increase causes e-mail systems to experience unexpected overload in bandwidth, server storage capacity, and loss of end-user productivity.”

The most popular way to defend oneself from spam mail is to use a filter, which is supposed to filter out spam messages. The effectiveness of this

*Blue Security Inc., www.bluesecurity.com

†School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel, and MEDS Department, Kellogg School of Management, Northwestern University, 2001 Sheridan Road, Evanston, IL 60208-2001. e-mail: eilons@post.tau.ac.il

method has been discussed in numerous articles, including [1], [2], [3], [4], [6]. In [13], we showed that unless the cost of sending a spam message is sufficiently high, improving filters has the undesirable effect of increasing the total number of spam messages spammers send.

Other methods of fighting spam mail that have been discussed in the literature include (see, e.g., [4], [12]) authentication and reputation services, counter attacks, channelling (e.g., [7], [8]), payments (e.g. [10], [14]), and regulatory actions (e.g. [9]).

In the present paper we concentrate on another solution to the spam problem, namely the do-not-spam registry. In this solution, users who opt not to receive spam mail join a do-not-spam registry, and spammers should not mail those users any spam mail.

The American Federal Trade Commission has studied the feasibility of such a registry, and concluded in June 2004 that “a National Do Not Email Registry, without a system in place to authenticate the origin of email messages, would fail to reduce the burden of spam and may even increase the amount of spam received by consumers.” Nevertheless, attempts at launching a registry are occasionally made (e.g., the Michigan registry for children in July 2005).

Whether or not current technology can support an effective registry is a crucial question for these attempts. However, another important question that was not asked during the debate on the desirability of a registry is what will be the effects of the registry on the amount of spam messages received by users who do *not* join the registry. That is, suppose there is an effective do-not-spam registry, and suppose that some portion of the population joins. Will other users, who do not join the registry, receive more or less spam messages? Will the total number of spam messages sent by spammers increase or decrease?¹

To answer these questions, we use the model studied in [13]. In that model, the population is divided to two groups, rich users who use more effective filters, and poor users who use less effective filters.

Our first main finding is that as long as the cost of mailing spam messages is not high, when poor users join to the registry, the total number of spam messages sent by spammers increases, whereas when rich users join the

¹Even if the number of messages each user receives increases, since there are fewer users who opt to receive spam mail, the total number of spam messages sent by spammers may decrease.

registry, the total number of spam messages sent by spammers decreases.

The intuition behind this result is the following. If poor users join the registry, the percentage of rich users in the population of those who opt to receive spam messages increases. Therefore, the average quality of filters increases as well, and spammers need to send more spam messages to bypass the filters.

Our second main finding concerns the efficiency of the internet. We show that as more poor users join the registry, the total number of spam messages sent to users decreases, so that having poor users join the registry improves the internet's efficiency.

When the cost of sending spam messages is low, the effect on the internet's efficiency of having rich users register is positive as well. Indeed, our first finding asserts that in this case the number of spam messages sent to each user decreases, and since the number of users who opt to receive spam mail decreases as well, the total number of spam messages decreases.

It is worthwhile to compare our findings with the effect of improving filters on the efficiency of the internet, as found in [13]. The main finding of [13] is that improving the quality of the filters has an ambiguous effect: users who use the improved filter receive less spam messages, but, if the cost of sending a spam message is not high, the total number of messages sent by spammers increases, and other users, who keep their old filters, receive more spam messages. Thus, whereas improving filters has the undesirable effect of harming the internet's efficiency, a registry has the opposite effect.

An important moral question is how to price the use of a registry. Since the use of a registry may increase the number of spam messages spammers send, the users who are potentially most harmed by this technology are poor users. If registering is costly, poor users will not be able to register, and they will suffer from a technology that helps rich users (as is the case nowadays with filters). Therefore, the socially responsible solution is to offer the registry free of charge to poor users. For rich users the registry serves as an improved substitute to filters: it completely eliminates the problem of spam mail, while improving the internet's efficiency.

We end the Introduction by mentioning that our results do not apply only to a do-not-spam registry. They apply to any technology that ensures its users do not receive spam messages.

The paper is arranged as follows. In section 2 we present the model of [13] adapted to the problem we study here, and we recall the results we need from [13]. In section 3 we describe our main results. The proofs appear in

section 4.

2 The Model

The population consists of $M_1 + M_2$ users and N spammers. Each spammer sends spam messages to the users. We assume that the spammers do not distinguish between users, so that each spammer sends the same number of messages to every user. However, spammers are not identical, so that each spammer may send a different number of messages.

The users are partitioned into two groups: there are M_1 poor users and M_2 rich users. There are two ways, two technologies, to fight spam mail: filters and a registry. We assume that all users have a spam filter. However, rich users have better filters than poor users. We measure the quality of a filter by the percentage of spam messages it allows to pass through. We denote by q and r the quality of the filter of poor and rich users respectively. Since rich users have better filters,

$$r < q. \tag{1}$$

We denote by s the percentage of users who purchase spam products. Those users are called *potential buyers*. We assume that those users are evenly distributed among poor and rich users.

For simplicity, we assume that each potential buyer makes at most one purchase of spam products every year. Moreover, we assume that a potential buyer who did not yet purchase a spam product this year, upon receiving a spam message has a probability p of deleting it, and a probability $1 - p$ of purchasing the spam product that is advertised in that message. We assume that the profit the spammer makes from each purchase is T dollars. Finally, we assume that users do not distinguish between spammers, so that if a potential buyer decides to purchase a spam product, the probability he will purchase a product from any specific spammer is equal to the proportion of spam messages that the spammer mailed to the user out of all spam messages the user received.

Spammers have two types of cost - a fixed cost and a per-message cost. The spammer's fixed cost is denoted by D dollars per year. The cost of each message is denoted by d dollars per message.

The goal of each spammer is to maximize his or her expected gain.

2.1 Spammers' Payoff

We now analyze the decision problem of a specific spammer. To this end, we calculate the spammer's expected gain.

Denote by x the number of messages per user per year that a specific spammer, say Spade, sends, and by y the total number of spam messages per user per year sent by all other spammers.

The total expected payoff of Spade is

$$W(x, y) = -D - x(M_1 + M_2)d + \frac{x}{x+y}Ts (M_1 (1 - p^{q(x+y)}) + M_2 (1 - p^{r(x+y)})) . \quad (2)$$

Indeed, Spade's total cost is $D + x(M_1 + M_2)d$. Each rich buyer receives $r(x + y)$ messages, so the probability he or she purchases a spam product is $1 - p^{r(x+y)}$. Similarly, the probability that a potential poor buyer purchases a product is $1 - p^{q(x+y)}$. Since there are M_1 poor users and M_2 rich users, and since potential buyers are evenly distributed among users, the expected number of users who purchase a spam product each year is $s (M_1 (1 - p^{q(x+y)}) + M_2 (1 - p^{r(x+y)}))$. Since the profit from each purchase is T dollars, and since $\frac{x}{x+y}$ of the purchases are made from Spade, the third term in (2) measures Spade's total gain.

If $W(x, y) < 0$, Spade has a negative payoff, and will go out of the market. Otherwise, Spade makes a profit.

For the mathematical analysis, it is more convenient to assume that the number of spam messages the spammer sends to each user is a non-negative real number, rather than a non-negative integer.

2.2 Stable configurations

A vector $\vec{x} = (x_1, \dots, x_N)$, which indicates the number of spam messages each spammer sends, is termed a spam configuration.

Definition 1 *A spam configuration is a vector $\vec{x} = (x_1, \dots, x_N)$, where x_i is the number of spam messages per user per year sent by spammer i , for each $1 \leq i \leq N$.*

A configuration is stable if no spammer has an incentive to deviate from it.

Definition 2 A spam configuration $\vec{x} = (x_1, \dots, x_N)$ is stable if for every spammer i

$$\frac{\partial W}{\partial x} \left(x_i, \sum_{j \neq i} x_j \right) = 0.^2$$

Since stable configurations are defined using local conditions (the directional derivatives are 0), at stable configurations no spammer can profit from *small* changes in the number of messages he or she mails. However, we do not rule out that the spammer can profit from large changes.

Note, though, that any configuration which is stable for large *and* small changes is in particular stable according to Definition 2.

2.3 Main Results of [13]

In this section we briefly recall some of the results of [13] we shall need here.

The following theorem contains two results. First, if the cost of sending a spam message is higher than some cut-off, there will be no spam, as at least one active spammer must have a loss, and will go out of the market. Second, if the cost of sending a spam message is below the cut-off, a stable configuration exists. Even though in principle there might exist several stable configurations, in all those configurations the total number of messages sent to users is the same, so that from the point of view of the users all those stable configurations are equivalent.

Theorem 3 [13] *If*

$$(M_1 + M_2)d > Ts(-\ln p)(M_1q + M_2r) \tag{3}$$

in every configuration the payoff of at least one spammer is negative.

If

$$(M_1 + M_2)d < Ts(-\ln p)(M_1q + M_2r) \tag{4}$$

a stable configuration exists. Moreover, in all stable configurations the total number of spam messages sent to each use is the same.

The left-hand side in (3) and (4) is the total cost of mailing a single spam message to all users, whereas the right-hand side in (3) and (4) is the

²Recall that $W(x, y)$ is a function of two variables, so that $\frac{\partial W}{\partial x}$ is its derivative relative to its first argument.

expected gain from the first spam message that is sent. Indeed, since p is in practice close to 1, $1 - p$ is close to $-\ln p$, so that $s(-\ln p)(M_1q + M_2r)$ is the expected number of users who purchase a spam product as a result of the first spam message they received.

We denote by $z(M_1, M_2)$ the total number of spam messages sent to each user in all stable configurations. By Theorem 3 this quantity is well defined.

3 Results

Our assumption that the registry is effective implies that each user who joins the registry stops receiving spam mail. This effectively means that that user is removed from the population: from the point of view of spammers, that user does not exist. Therefore, as more poor users join the registry, the number M_1 of poor users who opt to receive spam mail decreases. Similarly, as more rich users join the registry, the number M_2 of rich users who opt to receive spam mail decreases.

Our first result states that if having a rich user join the registry decreases the number of spam messages spammers send, then having a poor user register increases the number of spam messages spammers send. On the other hand, if having a rich user join the registry increases the number of spam messages spammers send, then having a poor user join decreases the number of spam messages spammers send.

Thus, if it is efficient that a rich user joins the registry, then it is inefficient that a poor user does so, whereas if it is efficient that a poor user joins the registry, it is inefficient that a rich user does so. This finding is stated in the following theorem.

Theorem 4

$$\frac{\partial z}{\partial M_1}(M_1, M_2) \frac{\partial z}{\partial M_2}(M_1, M_2) < 0, \quad \forall M_1, M_2.$$

In other words, the effect of rich users registering on the total number of spam messages sent is *always* opposite to the analog effect when poor users join the registry. This result is quite surprising, as it says that there is no win-win situation: in any given situation, either society as a whole prefers that a poor user joins the registry, or it prefers that a rich user does so, but not both.

The main force behind this result is that the behavior of spammers depends on M_1 and M_2 only through the ratio $\frac{M_1}{M_2}$. When poor users join the registry M_1 decreases and therefore the ratio decreases as well, whereas when rich users join M_2 decreases and therefore the ratio increases. Thus, the effect of having rich users join the registry on the ratio is opposite to the effect of having poor users join, so that the effect on the behavior of spammers is opposite as well.

It is interesting to note that this result is not particular to the model we study, but it is valid in any model in which the behavior of spammers depends on M_1 and M_2 only through the ratio $\frac{M_1}{M_2}$.

The following theorem states that when the cost of sending spam mail is not high, having poor users join the registry has a negative effect on the behavior of spammers: the number of spam messages they send to each non-registered user increases.

Theorem 5 *Provided N is large, if $r > \frac{N}{N-1} \frac{dN}{Ts(-\ln p)}$ then $\frac{\partial z}{\partial M_1}(M_1, M_2) < 0$.*

In practice $N \approx 200$, $d \approx \$0.000002$, $T \approx \$100$ and $s \approx 5\%$. Substituting $p \approx 99\%$ yields that the right-hand side is 0.8%. Presently for the best filters we have $r \approx 4\%$, so the condition in Theorem 5 holds. Thus, if these days a do-not-mail-me registry is launched, and spammers adhere to it, having poor users join the registry would increase the total number of spam messages sent by spammers.

Finally, we study the effect of the registry on the efficiency of the internet. We show that as more poor users join the registry, the total number of spam messages sent by spammers decreases. Thus, to increase efficiency one should encourage users to join the registry. Rich users have a similar effect, provided the cost of sending spam mail is not too high. This effect is summarized by the following two theorems.

Theorem 6 *The function $M_1 \mapsto (M_1 + M_2) \times z(M_1, M_2)$ is monotonic increasing: as M_1 , the number of poor users who do not join the registry, decreases, the total number of spam messages sent decreases as well.*

Theorem 7 *Provided N is large, if $r > \frac{N}{N-1} \frac{dN}{Ts(-\ln p)}$ the function $M_2 \mapsto (M_1 + M_2) \times z(M_1, M_2)$ is monotonic increasing: as M_2 , the number of rich users who do not join the registry, decreases, the total number of spam messages sent decreases as well.*

4 Proofs

Define

$$F(M_1, M_2, z) = (-\ln p) \left(\frac{M_1}{M_1 + M_2} qp^{qz} + \frac{M_2}{M_1 + M_2} rp^{rz} \right) + \frac{N-1}{z} \left(\frac{M_1}{M_1 + M_2} (1 - p^{qz}) + \frac{M_2}{M_1 + M_2} (1 - p^{rz}) \right).$$

The following result is proved in [13] (Lemma 10 and the proof of Theorem 5).

Theorem 8 *For every M_1, M_2 and z , $\frac{\partial F}{\partial z}(M_1, M_2, z) < 0$. Moreover,*

$$F(M_1, M_2, z(M_1, M_2)) = \frac{dN}{Ts}.$$

Theorem 8 implies that $z(M_1, M_2)$, the total number of spam messages sent by spammers, is the unique solution of a certain equation. Since $\frac{\partial F}{\partial z}$ is strictly positive, the implicit function theorem implies that $z(M_1, M_2)$ is differentiable.

We are now ready to prove Theorem 4.

Proof of Theorem 4. Define $\beta = \frac{M_1}{M_1 + M_2}$; it is the percentage of poor users in the population. Then $1 - \beta = \frac{M_2}{M_1 + M_2}$. Note that F depends on M_1 and M_2 only through β . Moreover, increasing M_1 while keeping M_2 fixed increases β , and increasing M_2 while keeping M_1 fixed decreases β .

Since the function $z(M_1, M_2)$ is differentiable, if increasing M_1 (increasing β) causes z to increase, then increasing M_2 (decreasing β) causes z to decrease, and vice versa. The result follows. ■

Proof of Theorem 5.

Step 1: $\frac{\partial z}{\partial M_1}(M_1, M_2) < 0$ if and only if $\frac{\partial F}{\partial M_1}(M_1, M_2, z(M_1, M_2)) < 0$.

Define $G(M_1) = F(M_1, M_2, z(M_1, M_2))$. By Theorem 8 $G(M_1) = \frac{dN}{Ts}$ for every M_1 , so that $G'(M_1) = 0$. Therefore, by the chain rule,

$$0 = G'(M_1) = \frac{\partial F}{\partial M_1}(M_1, M_2, z(M_1, M_2)) + \frac{\partial F}{\partial z}(M_1, M_2, z(M_1, M_2)) \frac{\partial z}{\partial M_1}(M_1, M_2).$$

By Theorem 8 we have $\frac{\partial F}{\partial z}(M_1, M_2, z) < 0$, so that

$$\frac{\partial z}{\partial M_1}(M_1, M_2) < 0 \quad \Leftrightarrow \quad \frac{\partial F}{\partial M_1}(M_1, M_2, z(M_1, M_2)) < 0. \quad (5)$$

Step 2: Conditions for $\frac{\partial F}{\partial M_1}(M_1, M_2, z(M_1, M_2)) < 0$.

We now calculate $\frac{\partial F}{\partial M_1}$.

$$\begin{aligned} \frac{\partial F}{\partial M_1}(M_1, M_2, z) &= \frac{M_2}{M_1 + M_2^2} \left((-\ln p)qp^{qz} + \frac{N-1}{z}(1-p^{qz}) \right) \\ &\quad - \frac{M_2}{M_1 + M_2^2} \left((-\ln p)rp^{rz} + \frac{N-1}{z}(1-p^{rz}) \right) \\ &= \frac{1}{z} \frac{M_2}{M_1 + M_2^2} \left((qz p^{qz}(-\ln p) - (N-1)p^{qz}) \right. \\ &\quad \left. - (rz p^{rz}(-\ln p) - (N-1)p^{rz}) \right). \end{aligned}$$

Thus,

$$\frac{\partial F}{\partial M_1}(M_1, M_2, z) < 0 \Leftrightarrow qz p^{qz}(-\ln p) - (N-1)p^{qz} < rz p^{rz}(-\ln p) - (N-1)p^{rz}.$$

Setting $\hat{q} = qz(-\ln p) - N + 1$ and $\hat{r} = rz(-\ln p) - N + 1$, multiplying both sides by $\exp(N-1)$, and using the equality $p^{1/(-\ln p)} = \exp(-1)$ we obtain

$$\frac{\partial F}{\partial M_1}(M_1, M_2, z) < 0 \Leftrightarrow \hat{q} \exp(-\hat{q}) < \hat{r} \exp(-\hat{r}). \quad (6)$$

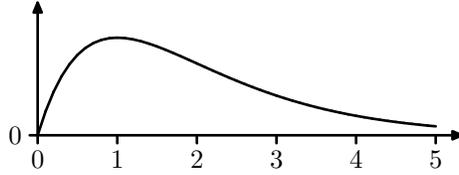


Figure 1: The graph of the function $x \exp(-x)$

One can use the Lambert function ([11], [5]) to solve Eq. (6), but the resulting equation involves the parameter z , and therefore we cannot derive an explicit necessary and sufficient condition for the inequality $\frac{\partial F}{\partial M_1}(M_1, M_2, z) < 0$. However, the function $x \exp(-x)$ is increasing in the interval $(0, 1]$ and decreasing in the interval $[1, \infty)$ (see Figure 1). Since $q > r$ we have $\hat{q} > \hat{r}$. Therefore we have

$$\hat{r} > 1 \implies \frac{\partial F}{\partial M_1}(M_1, M_2, z) < 0. \quad (7)$$

By the definition of \hat{r} , a sufficient condition for $\frac{\partial F}{\partial M_1}(M_1, M_2, z) < 0$ is

$$z(M_1, M_2) > \frac{N}{(-\ln p)r}.$$

Step 3: A condition for $z(M_1, M_2) > \frac{N}{(-\ln p)r}$.

Theorem 8 implies that $z(M_1, M_2) > \frac{N}{(-\ln p)r}$ if and only if $F(M_1, M_2, \frac{N}{(-\ln p)r}) > \frac{dN}{Ts}$.

$$\begin{aligned} F(M_1, M_2, \frac{N}{(-\ln p)r}) &= \\ &= (-\ln p) \left(\frac{M_1}{M_1 + M_2} qp^{qN/r(-\ln p)} + \frac{M_2}{M_1 + M_2} rp^{N/(-\ln p)} \right) \\ &+ \frac{N-1}{N} (-\ln p)r \left(\frac{M_1}{M_1 + M_2} (1 - p^{qN/r(-\ln p)}) + \frac{M_2}{M_1 + M_2} (1 - p^{N/(-\ln p)}) \right). \end{aligned} \quad (8)$$

We note that $p^{1/(-\ln p)} = \exp(-1)$. When N is large³ $\exp(-N) \approx 0$, so that using the inequality $q > r$ Eq. (8) becomes

$$F(M_1, M_2, \frac{N}{(-\ln p)r}) \approx \frac{N-1}{N} (-\ln p)r.$$

Thus, when N is large $z(M_1, M_2) > \frac{N}{(-\ln p)r}$ if and only if $\frac{N-1}{N} (-\ln p)r > \frac{dN}{Ts}$, or equivalently, if and only if

$$r > \frac{N}{N-1} \frac{dN}{Ts(-\ln p)}.$$

Step 4: Summary.

We now use the previous steps to conclude the proof. By step 1 $\frac{\partial z}{\partial M_1}(M_1, M_2) < 0$ if and only if $\frac{\partial F}{\partial M_1}(M_1, M_2, z(M_1, M_2)) < 0$. By Steps 2 and 3 a sufficient condition for $\frac{\partial F}{\partial M_1}(M_1, M_2, z(M_1, M_2)) < 0$ is $r > \frac{N}{N-1} \frac{dN}{Ts(-\ln p)}$. Therefore if $r > \frac{N}{N-1} \frac{dN}{Ts(-\ln p)}$ we also have $\frac{\partial z}{\partial M_1}(M_1, M_2) < 0$, as desired. ■

Proof of Theorem 6. Denote by $Z = (M_1 + M_2) \times z$ the total number of spam messages sent by each spammer. Define

$$\begin{aligned} G(M_1, M_2, Z) &= F(M_1, M_2, \frac{Z}{M_1 + M_2}) \\ &= (-\ln p) \left(\frac{M_1}{M_1 + M_2} qp^{qZ/(M_1+M_2)} + \frac{M_2}{M_1 + M_2} rp^{rZ/(M_1+M_2)} \right) \\ &+ \frac{N-1}{Z} (M_1 (1 - p^{qZ/(M_1+M_2)}) + M_2 (1 - p^{rZ/(M_1+M_2)})). \end{aligned}$$

³In practice $N \approx 200$.

Since the function $Z \mapsto p^{cZ}$ is monotonic decreasing for every $c > 0$, and since the function $Z \mapsto (1 - p^{cZ})/Z$ is monotonic decreasing for every $c > 0$ (see Lemma 12 in [13]), we have

$$\frac{\partial G}{\partial Z}(M_1, M_2, Z) < 0, \quad \forall M_1, M_2. \quad (9)$$

Set $H(M_1) = G(M_1, M_2, Z(M_1, M_2))$. By Theorem 8 we have $H(M_1) = \frac{dN}{Ts}$ for every M_1 , hence $H'(M_1) = 0$. By the chain rule

$$0 = H'(M_1) = \frac{\partial G}{\partial M_1}(M_1, M_2, Z(M_1, M_2)) + \frac{\partial G}{\partial Z}(M_1, M_2, Z(M_1, M_2)) \times \frac{\partial Z}{\partial M_1}(M_1, M_2).$$

By (9), to prove that $\frac{\partial Z}{\partial M_1}(M_1, M_2) > 0$ we need to show that $\frac{\partial G}{\partial M_1}(M_1, M_2, Z) > 0$.

The derivative of G w.r.t. M_1 is

$$\begin{aligned} \frac{\partial G}{\partial M_1}(M_1, M_2, Z) &= (-\ln p) \frac{M_2}{(M_1 + M_2)^2} (qp^{qZ/(M_1+M_2)} - rp^{rZ/(M_1+M_2)}) \\ &\quad + (-\ln p)^2 \frac{M_1 q^2 Z}{(M_1 + M_2)^3} p^{qZ/(M_1+M_2)} \\ &\quad + (-\ln p)^2 \frac{M_2 r^2 Z}{(M_1 + M_2)^3} p^{rZ/(M_1+M_2)} \\ &\quad + \frac{N-1}{Z} (1 - p^{qZ/(M_1+M_2)}) \\ &\quad - \frac{N-1}{Z} \frac{qZM_1}{(M_1 + M_2)^2} (-\ln p) p^{qZ/(M_1+M_2)} \\ &\quad - \frac{N-1}{Z} \frac{rZM_2}{(M_1 + M_2)^2} (-\ln p) p^{rZ/(M_1+M_2)}. \end{aligned} \quad (10)$$

Since $q > r$ we have $p^{-cq} > p^{-cr}$ for every $c > 0$, and therefore the fourth term can be split as follows.

$$\begin{aligned} \frac{N-1}{Z} (1 - p^{qZ/(M_1+M_2)}) &= \\ &= \frac{M_1}{M_1 + M_2} \frac{N-1}{Z} (1 - p^{qZ/(M_1+M_2)}) + \frac{M_2}{M_1 + M_2} \frac{N-1}{Z} (1 - p^{qZ/(M_1+M_2)}) \\ &\geq \frac{M_1}{M_1 + M_2} \frac{N-1}{Z} (1 - p^{qZ/(M_1+M_2)}) + \frac{M_2}{M_1 + M_2} \frac{N-1}{Z} (1 - p^{rZ/(M_1+M_2)}). \end{aligned} \quad (11)$$

Since $1 - p^x > x(-\ln p)p^x$ for every $x > 0$ and every $p \in (0, 1)$, the difference between the first term in Eq. (11) and the fifth term in Eq. (10) is positive. We will now show that the sum of all terms in (10) that contain the parameter r is non-negative. This will conclude the proof.

Indeed, the sum (as a function of r) is

$$\begin{aligned}
A(r) = & -(-\ln p) \frac{M_2}{(M_1 + M_2)^2} r p^{rZ/(M_1+M_2)} \\
& + (-\ln p) \frac{M_2}{M_1 + M_2} \frac{r^2 Z}{(M_1 + M_2)^2} (-\ln p) p^{rZ/(M_1+M_2)} \\
& - \frac{N-1}{Z} \frac{rZ M_2}{(M_1 + M_2)^2} (-\ln p) p^{rZ/(M_1+M_2)} \\
& + \frac{M_2}{M_1 + M_2} \frac{N-1}{Z} (1 - p^{rZ/(M_1+M_2)}).
\end{aligned}$$

Observe that $A(0) = 0$ and $A(\infty) = \frac{N-1}{Z} \frac{M_2}{M_1+M_2} > 0$. Therefore, to show that $A(r) \geq 0$ for every $r \geq 0$ it is sufficient to show that A is non-decreasing. The derivative of A , after dividing by $(-\ln p) \frac{M_2}{(M_1+M_2)^2} p^{rZ/(M_1+M_2)}$ is

$$-1 + (-\ln p)rZ + (N-1) + \frac{(N-1)rZ(-\ln p)}{M_1 + M_2} + 2 \frac{(-\ln p)rZ}{M_1 + M_2} - \frac{(-\ln p)r^2 Z^2}{(M_1 + M_2)^2}.$$

If $rZ \leq 1$ then, as soon as $N > 3$ this expression is positive.⁴ If $rZ \geq 1$ the last term is smaller than the penultimate term, so as soon as $N > 2$ this expression is positive. ■

Proof of Theorem 7. Assume that N is large, and that $r > \frac{N}{N-1} \frac{dN}{Ts(-\ln p)}$. By Theorem 5 we have $\frac{\partial z}{\partial M_1}(M_1, M_2) < 0$. By Theorem 4 we have $\frac{\partial z}{\partial M_2}(M_1, M_2) > 0$. In other words, the function $M_2 \mapsto z(M_1, M_2)$ is increasing. Therefore the function $M_2 \mapsto (M_1 + M_2) \times z(M_1, M_2)$, as a product of two increasing functions, is increasing as well. ■

References

- [1] I. Androutsopoulos, E.F. Magirou and D.K. Vassilakis (2005) A Game Theoretic Model of Spam E-Mailing. Forthcoming, CEAS 2005.

⁴Recall that $N \approx 200$ and that $M_1 + M_2$ is the total number of users, which is large.

- [2] I. Androutsopoulos, G. Paliouras, V. Karkaletsis, G. Sakkis, C.D. Spyropoulos and P. Stamatopoulos (2000) Learning to Filter Spam E-Mail: A Comparison of a Naive Bayesian and a Memory-Based Approach. In H. Zaragoza, P. Gallinari, and M. Rajman (Eds.), Proceedings of the Workshop on Machine Learning and Textual Information Access, 4th European Conference on Principles and Practice of Knowledge Discovery in Databases (PKDD 2000), Lyon, France, pp. 1-13.
- [3] X. Carreras and L. Marquez (2001) Boosting Trees for Anti-Spam Email Filtering. Proceedings of RANLP-01, 4th International Conference on Recent Advances in Natural Language Processing.
- [4] L.F. Cranor and B.A. LaMacchia (1998) Spam! Communications of the ACM, **41**, 74-83. <http://doi.acm.org/10.1145/280324.280336>
- [5] L. Euler (1783) De serie Lambertina Plurimisque eius insignibus proprietatibus. Acta Acad. Scient. Petropol., **2**, 29-51, 1783. Reprinted in L. Euler, Opera Omnia, Ser. 1, Vol. 6: Commentationes Algebraicae. Leipzig, Germany: Teubner, pp. 350-369, 1921.
- [6] F.D. Garcia, J.H. Hoepman and J. van Nieuwenhuizen Spam Filter Analysis (2004) Proceedings of 19th IFIP International Information Security Conference, WCC2004-SEC
- [7] R.J. Hall (1998) How to Avoid Unwanted Email. Communications of the ACM.
- [8] E. Gabber, M. Jakobsson, Y. Matias, and A. Mayer (1998) Curbing junk E-mail via secure classification. In Proceedings of Financial Cryptography '98, Anguilla, BWI.
- [9] D.W.K. Khong (2004) An Economic Analysis of Spam Law. Erasmus Law and Economics Review, **1**, 23-45.
- [10] R.E. Kraut, S. Sunder, R. Telang, and J. Morris (2005) Pricing Electronic Mail To Solve the Problem of Spam. Human-Computer Interaction Vol. 20, 195-223.
- [11] J.H. Lambert (1758) Observations variae in Mathesin Puram. Acta Helvetica, physico-mathematico-anatomico-botanico-medica, **3**, 128-168.

- [12] B. Leiba and N. Borenstein (2004) A Multifaceted Approach to Spam Reduction. Proceedings of the 1st Conference on Email and Anti-Spam (CEAS 2004), Mountain View, CA, USA.
- [13] E. Reshef and E. Solan (2005) The Effect of Filters on Spam Mail. CMS-EMS Discussion paper #1402. www.kellogg.northwestern.edu/research/math/papers/1402.pdf
- [14] T. Van Zandt (2004) Information Overload in a Network of Targeted Communication. RAND Journal of Economics, **35**, 542-560.