Quality Competition in the Security Software Market

Debabrata Dey
Foster School of Business
University of Washington
ddey@uw.edu

Atanu Lahiri
Foster School of Business
University of Washington
lahiria@uw.edu

Guoying Zhang
Dillard College of Business
Midwestern State University
grace.zhang@mwsu.edu

Abstract
Recent years have witnessed an unprecedented growth in the security software market. This market is fiercely competitive with about seven dozen vendors; yet, the price is high and coverage low. Although current research has examined these idiosyncrasies and has found the existence of a negative network effect as a possible explanation, an important question still remains: what possibly discourages product differentiation in this competitive market? We develop a comprehensive quantitative model to answer this question. Our analyses reveal that the negative network effect makes quality differentiation less likely, as well. Hence, our contributions are two-fold: (i) we explain why quality differentiation is often suboptimal for vendors in this market, and (ii) we generalize prior work to include asymmetric equilibriums and find that the presence of the negative network effect still provides insights into the unique structure of this market, with important strategic implications for vendors.

Keywords: Security software, network effect, quality competition, market structure, vertical differentiation.

1. Introduction
The industry of security software, along with that of security hardware and services, has grown rapidly in response to a higher demand for the protection of an ever-increasing base of information technology (IT) infrastructure. According to the Gartner Group [12, 13], the worldwide security software revenue has increased from nearly US$6.4 billion in 2004 to about US$16.5 billion in 2010 (see Figure 1). Understanding the nature of this market and gaining insights on relevant competitive strategies are, therefore, of interest to academicians as much as they are to software vendors and consumers.

In general, security software can be classified into two main categories: (i) off-the-shelf third-party standalone tools, such as antivirus, anti-spyware, web filter, anti-spamware, and anti-phishing, for different operating systems, and (ii) system components, such as encryption software and firewalls that are often bundled with different operating systems. In this paper, we examine only the first category, which dominates the security software market and has a number of major players, including Symantec, Trend Micro, McAfee, Kaspersky, and several dozen others. A recent survey [22], for example, finds that there are 81 antivirus vendors (with 257 antivirus products) in North America and 87 vendors worldwide (with 367 products).

In the typical off-the-shelf software market, users enjoy a higher network utility from a larger market share, which is often referred to as the positive network effect [16]. This positive network effect primarily arises from users’ need for compatibility and often leads to a near-monopoly market condition. However, the market for off-the-shelf security software is quite different. First, it rarely has a single dominant player; Symantec, which once led this market with more than 50% of the industry sales, currently holds less than 20% of the market share [13]. In fact, the total market share of the top five antivirus software vendors is below 45%. Despite the presence of a large number of vendors [22], the price for this type of software has remained relatively high. For example,
Table 1. A Comparison of Antivirus Software Ratings

<table>
<thead>
<tr>
<th>Review Source</th>
<th>AVG</th>
<th>Avr</th>
<th>Avs</th>
<th>BD</th>
<th>BG</th>
<th>EN3</th>
<th>GD</th>
<th>Kky</th>
<th>Mct</th>
<th>Nrt</th>
<th>Pnd</th>
<th>TM</th>
</tr>
</thead>
<tbody>
<tr>
<td>TopTenREVIEWS</td>
<td>0.88</td>
<td>0.75</td>
<td>0.75</td>
<td>1.00</td>
<td>0.75</td>
<td>0.75</td>
<td>1.00</td>
<td>0.63</td>
<td>0.75</td>
<td>0.88</td>
<td>0.85</td>
<td>0.85</td>
</tr>
<tr>
<td>AV-Test.org</td>
<td>0.83</td>
<td>0.67</td>
<td>0.83</td>
<td>1.00</td>
<td>0.75</td>
<td>0.58</td>
<td>0.92</td>
<td>1.00</td>
<td>0.67</td>
<td>0.83</td>
<td>0.92</td>
<td>0.75</td>
</tr>
<tr>
<td>PC Antivirus Reviews</td>
<td>0.89</td>
<td>0.72</td>
<td>0.89</td>
<td>0.95</td>
<td>0.83</td>
<td>0.92</td>
<td>0.68</td>
<td>0.75</td>
<td>0.82</td>
<td>0.84</td>
<td>0.84</td>
<td>0.84</td>
</tr>
<tr>
<td>Best Free Antivirus</td>
<td>0.80</td>
<td>0.90</td>
<td>0.80</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antivirus Software Deals</td>
<td>0.40</td>
<td>0.70</td>
<td>1.00</td>
<td>0.80</td>
<td>0.80</td>
<td>0.60</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
</tr>
<tr>
<td>MaximumPC</td>
<td>1.00</td>
<td>0.96</td>
<td>0.95</td>
<td>0.99</td>
<td>0.93</td>
<td>0.94</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
<td>0.90</td>
</tr>
<tr>
<td>PC Magazine</td>
<td>0.80</td>
<td>0.70</td>
<td>0.80</td>
<td>0.60</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
</tr>
<tr>
<td>PC World</td>
<td>0.80</td>
<td>0.90</td>
<td>0.70</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Top Ten Antivirus</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>0.90</td>
<td>0.80</td>
<td>0.60</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
</tr>
<tr>
<td>AV Comparatives</td>
<td>0.59</td>
<td>0.43</td>
<td>0.54</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virus Bulletin</td>
<td>1.00</td>
<td>1.00</td>
<td>1.00</td>
<td>0.90</td>
<td>0.80</td>
<td>0.60</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
<td>0.40</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td>0.80</td>
<td>0.80</td>
<td>0.81</td>
<td>0.87</td>
<td>0.77</td>
<td>0.80</td>
<td>0.78</td>
<td>0.83</td>
<td>0.73</td>
<td>0.83</td>
<td>0.78</td>
<td>0.70</td>
</tr>
<tr>
<td><strong>Standard Deviation</strong></td>
<td>0.19</td>
<td>0.15</td>
<td>0.18</td>
<td>0.16</td>
<td>0.03</td>
<td>0.19</td>
<td>0.13</td>
<td>0.14</td>
<td>0.10</td>
<td>0.14</td>
<td>0.13</td>
<td>0.18</td>
</tr>
</tbody>
</table>

Avg=Avira; Avs=Avast; BD=BitDefender; BG=BullGuard; EN3=ESET NOD32; GD=G Data; Kky=Kaspersky; Mct=McAfee; Nrt=Norton; Pnd=Panda; TM=Trend Micro.

An annual subscription of Norton Internet Security 2012 can cost as much as US$80. At the same time, a three-year subscription can cost up to US$165, well above the price of Microsoft Word 2010, a product that enjoys greater monopoly power and also offers a perpetual license. Furthermore, in spite of so many choices in the marketplace, a significant percentage of individual computers are still lacking in basic protection [14, 18]. A recent study on online banking finds that as many as 47% of household finance managers (those who manage their household finances using online banking) do not use any antivirus software at all [10]. In an attempt to understand why this market behaves so differently, Dey et al. [8, 9] consider possible network effects in this market and find that the negative network effect provides an explanation for the observed market characteristics.

However, a notable characteristic of this market that has not been addressed in [8] is the lack of quality differentiation. A common measure of quality in this context is the set of security-related features a product offers. In this regard, we find that most vendors offer nearly identical products, despite being in a severely competitive market. Consider, for example, the list of top 12 antivirus software products shown in Table 1; the products shown in this table are the top 12 products as rated by TopTenREVIEWS [27]. A careful feature-by-feature comparison of these products readily reveals that they are quite similar with nearly identical feature content. For example, they all protect against different types of malware (such as virus, trojan horse, spyware, worm, and rootkit), provide internet security as well as in- and out-bound email protection, and offer different modes of scanning (such as on a real-time basis, at start up, on demand, and as per a schedule). Furthermore, all these products are of high quality and are certified by the leading assurance firm ICSA Labs. We have looked at many other products and have barely noticed any difference in the feature coverage.

It may be argued, however, that the feature content of a product does not fully reflect its effectiveness and may not be the appropriate indicator of quality. Hence, we also consider overall product ratings from well-known secondary sources. In order to facilitate easy comparison across these sources who employ different scales for ratings, we normalize all ratings on a 0-1 scale in Table 1. It is quite clear from this table that there is no broad consensus across these sources in terms of the perceived quality of these products. For example, Avira tops the rating chart provided by MaximumPC, but comes in 11th in the rating chart from AV-Test.org. Similarly, although BitDefender tops the rating charts from TopTenREVIEWS and AV-Test.org, it does not do as well on AV Comparatives’ chart. In order to see this variation more clearly, we also compute the average score for each product, along with the respective standard deviation. We find that, even though the average normalized score ranges from 0.70 for Trend Micro to 0.87 for BitDefender, because of significant variations that exist across these sources, the averages are not statistically different from one another—a one-way ANOVA returns a *p*-value of 0.761. In other words, Table 1 points to the fact that there is little quality differentiation in the market for antivirus software.

This lack of differentiation is somewhat unexpected and quite interesting. In practice, when market competition is fierce, vendors often resort to product differentiation, vertical or horizontal. As
a result, it is difficult to find an industry where dozens of firms compete with identical product or service offerings. In the security software market, given the nature of the product, horizontal differentiation apparently makes little practical sense. Naturally, one would expect this market to exhibit a significant level of vertical differentiation, a strategy often adopted by vendors to ease the level of competition when consumers differ in their willingness to pay for quality [15, 21]. Yet, as discussed above, vertical differentiation in this market is conspicuous in its absence. An important point of this paper is to understand this apparent anomaly, in addition to providing a comprehensive model of competition that can also explain other noticeable anomalies such as the unusually low market coverage.

As mentioned earlier, one of the factors capable of contributing to the idiosyncratic nature of the security software market is the negative network effect it experiences. Using a Cournot oligopoly model, Dey et al. [8, 9] have shown that the presence of this network effect furnishes possible explanations for some of the unique characteristics of this market. However, their model has a limited scope as it does not consider the quality decision at all. In this research, we generalize the model in [8] by endogenizing vendors' quality decisions. While this generalization leads to a more complex model, it also provides us with important economic tools necessary for addressing outstanding questions about the security software market. First, it allows us to corroborate their result concerning a low market coverage to settings that might not lead to a fully symmetric equilibrium with all firms offering identical products. Second, it helps us explore our primary research question regarding quality competition, which is critical to explaining why, despite severe competitive pressures, there is so little differentiation in this market.

The primary reason behind quality differentiation commonly observed in many other markets is that such differentiation allows manufacturers to relax competition. Some manufacturers target value-seeking consumers, while others quality-seeking ones, in effect reducing competition between vendors targeting different segments. This way, quality differentiation also expands the market coverage by providing cheaper alternatives to value-seeking consumers who are often reluctant to buy expensive high-end products. However, the negative network effect, which lowers consumers' willingness-to-pay with the market coverage, makes expansion of the market an unattractive proposition. In the end, it disincentivizes security software vendors from adopting quality differentiation. The net implication is that strategies that seek to segment the consumer market are often not as useful for security software vendors as they are for manufacturers of other products.

2. Literature
Researchers have long explored the role of the positive network effect and how it affects competitive outcomes in markets for software and other types of goods [11, 16]. Unlike traditional software markets, the positive network effect is not observed in the security software market. In fact, from the perspective of a consumer, security software is just a tool for preventing security exploitations, and there is hardly any benefit from the compatibility of user data. Hence, we focus on the negative network effect, which has received considerable attention from researchers in recent years. For example, Png and Wang [23] have shown that the negative network effect arising from strategic hacker behavior can provide a possible explanation for users' inertia in taking security precautions. As more users adopt security software, hackers find it less profitable to launch new attacks, which, in turn, makes the non-adopters less likely to adopt security solutions. Dey et al. [8] have argued that the negative network effect can also arise from indirect attacks, where a system is not a direct target but could become an eventual target from security exploitations of other systems. Typical examples of indirect attacks include Internet worms [5] and BOTNET agents [25], which could launch large-scale attacks with the ability to convert ordinary nodes into malicious agents. The larger the market coverage of security software, the less is the chance of getting infected from others and the willingness of a consumer to subscribe to a security solution. Thus, indirect attacks eventually lead to a negative network effect. Negative network effects have also been recognized by other researchers, for example, by August and Tunca [1, 2] as an important factor in changing the users' incentive to apply security patches.

Dey et al. [8] have also shown that, although different types of network effects can exist in the security software market, a model that captures the negative network effect from indirect attacks can be easily extended to capture all others. Hence, we too focus on this network effect. However, unlike them, we allow for the possibility that competing vendors may offer security products that are differentiated in quality. Our extended model provides us with the
novel insight that the presence of negative network effects can indeed explain the conspicuous lack of vertical differentiation in the security software market.

It is worth mentioning here that, despite some overlap, our model is quite different from the recent literature on application software. August and Tunca [1, 2] and Lahiri [19] also recognize the existence of a similar negative network effect and develop economic models in which a consumer’s valuation for an application software—or an operating system—depends on the number of unpatched vulnerable copies of that software in the user network.

In their models, the larger the number of vulnerable nodes, the lower is the valuation of the application product. What we have here is exactly the opposite: the larger the chance of an indirect infection, the higher is the value of a security software.

Also related to this work is the vast body of literature in economics and marketing, which examines the efficacy of vertical differentiation [3, 7, 21]. Often, the conclusion is that differentiation is optimal as it relaxes competition. While this stream of work is quite influential, it does not directly apply to our context, mainly because we are interested in a market where the marginal cost is negligible but product development costs are substantial [15, 26].

More importantly, we want to find out whether the negative network effect can influence quality differentiation, an issue that has not been examined previously.

3. Monopoly

In this section, we consider a profit-maximizing monopolist who serves a heterogeneous consumer market. Consumers (users) of security software are heterogeneous because the amount of benefit from thwarting an attack would vary from user to user. In order to capture this, consumers are indexed by a parameter \( u \) that indicates their relative expected benefit if an attack is thwarted. The absolute expected benefit to user \( u \) from thwarting an attack can then be expressed as \( Lu \), where \( L \) is a constant; \( Lu \) can also be viewed as a proxy for the potential loss to user \( u \) from an attack [8].

**Assumption 1.** The index \( u \) is uniformly distributed over the interval \([0, 1]\).

Hackers engage in two types of attacks: (i) mass attacks and (ii) targeted attacks [8, 23]. These types of attacks can be explained by the choice and chance models of hacker behavior [24]. Mass attacks essentially follow the path of chance—here, hackers create and distribute exploits with the objective of infecting as many computers as possible, and they do not choose specific targets. Targeted attacks, on the other hand, follow a path of choice, where hackers primarily preselect certain targets. In this paper, we develop the model only for mass attacks; extending our analysis to include targeted attacks is conceptually straightforward [8].

Mass attacks make use of generic exploits that are capable of breaching the security of a large variety of users [6, 24]. These attacks consist of: (i) direct attacks and (ii) indirect attacks. Accordingly, there are two types of benefits to be derived from adopting a security software—direct and indirect. A security software can be characterized by a quality parameter \( \theta \), \( 0 < \theta \leq 1 \), which can also be viewed as the effectiveness of the security software in providing the protection it is supposed to. In other words, a user, by installing the software, is able to thwart a fraction \( \theta \) of all the attacks—direct or indirect. Therefore, if \( \lambda \) represents the average rate of direct attacks, user \( u \) gets a direct mitigation benefit of \( \lambda \theta Lu \) per unit time by adopting a security software of quality \( \theta \).

Next, we consider the indirect benefit. Unprotected systems might replicate malicious codes and pass them to connected peers. At times, a hacker may attack a system indirectly, after first breaching the security of several other systems and using them as a launching pad. In other words, the existence of security software in one system can, indirectly, reduce attacks to others. Let \( x \) be the fraction of users who have adopted security software of quality \( \theta \). Then, a fraction \((1 - x)\) is completely vulnerable and would potentially serve as a launching pad of indirect attacks. The remaining fraction \( x \), though protected, may also be exploited for this purpose with a probability of \((1 - \theta)\). Therefore, the effective probability that a randomly selected node can be exploited as a launching pad is:

\[
1 - x + x(1 - \theta) = 1 - \theta x.
\]

Since an indirect attack ultimately originates from exploitations of intermediate vulnerable nodes through a direct attack, following [8], we assume the rate of indirect attacks to be \( g \lambda (1 - \theta x) \), where \( g \) is a model parameter representing the strength of the negative network effect from indirect attacks—the higher \( g \) is, the larger is the potential indirect benefit. It is now obvious that a larger market share (larger \( x \)) leads to a reduction in this indirect benefit. At the extreme, if all users are equipped with security software of perfect quality (i.e., \( \theta = 1 \)), no user derives any indirect benefit. A user adopting a
security software of quality \( \theta \), therefore, avoids indirect attacks from the unprotected users and derives an indirect benefit of \( \lambda \theta g Lu(1-\theta x) \).

The total benefit (per unit time) to user \( u \) from adopting a software of quality \( \theta \), in a market with coverage \( x \), can then be written as:

\[
B_u = \lambda \theta Lu + \lambda \theta g Lu(1-\theta x) = \lambda \theta Lu(1+g(1-\theta x)).
\] (1)

Security software products are usually licensed as a subscription for a fixed time period. Let \( P \) be the subscription price (per unit time). A user would adopt a security software if the total benefit from the software is larger than its subscription price: \( B_u \geq P \). The marginal user \( u \) who is indifferent between adopting and not adopting must then satisfy the following condition in equilibrium:

\[
\lambda \theta Lu(1+g(1-\theta x)) - P = 0.
\]

As shown in Figure 2, any user to the right of this marginal user adopts the software, whereas anyone to the left does not. Therefore, \( u = 1 - x \). Substituting this and letting \( p = \frac{\lambda \theta Lu}{1+g} \), we get:

\[
p = \theta (1+g(1-\theta x))(1-x).
\] (2)

Equation (2) represents the normalized price for a security software of quality \( \theta \) when the market coverage is \( x \).

**Assumption 2.** The normalized development cost of a product with quality level of \( \theta \) is \( c \theta^2 \), where \( c > 0 \) is a constant. The marginal cost of a subscription to the vendor is zero.

We now write the optimization problem of the monopolist:

\[
\begin{align*}
\text{Max } R &= px - c \theta^2 = \theta x(1+g(1-\theta x))(1-x) - c \theta^2 \\
\text{s.t. } 0 &\leq \theta \leq 1, \ 0 \leq x \leq 1.
\end{align*}
\] (3)

The first order condition, \( \frac{\partial R}{\partial x} = 0 \), results in two roots for \( x \). Since \( x \leq 1 \), we can discard one of the roots to get:

\[
x = \frac{1+g(1+\theta) - \sqrt{1+g(2+g-(1+g)\theta+g \theta^2)}}{3g \theta}.
\]

In order to verify that the second order condition is satisfied, we find:

\[
\frac{\partial^2 R}{\partial x^2} = -2\theta(1+g(1+\theta-3\theta x)),
\]

which, after some algebra, can be shown to be negative at the optimal \( x \). Substituting this \( x \) into \( R \), we find that \( R \) is a concave function of \( \theta \) and can be maximized to obtain the optimal quality level.

The final solution is shown in Figure 3, where the optimal \( \theta \) and \( x \) are plotted as a function of \( g \), for three different values of \( c \). As expected, the optimal quality decreases as the development cost increases. A decrease in quality, in effect, translates to a smaller negative network effect and lessens consumers’ free-riding behavior. This allows the monopolist to expand the market coverage. As a result, we find that the market coverage increases with \( c \); see Figure 3(b).

Figure 3(a) shows that the optimal quality level increases with \( g \). This is intuitive. As \( g \) increases, consumers’ willingness-to-pay (WTP) for quality goes up, and the vendor responds with a higher quality level. Interestingly, as shown in Figure 3(b), the monopolist drops the market coverage with \( g \), despite a higher WTP. This decline stems from two sources: First, even when the quality level remains the same, an increase in \( g \) makes the demand more inelastic and induces the monopolist to reduce coverage. Second, any increase in quality must be compensated by a commensurate decrease in the coverage to keep the free-riding behavior under control. As can be seen from Figure 3(b), the decline in the coverage is initially steeper since both sources contribute there. After the quality level saturates at one, only the first source matters; hence, the decline is more gradual, which is consistent with [8] where software quality is exogenous.

4. Duopoly

As mentioned in the introduction, the security software market is quite competitive with many different vendors. In order to obtain a more comprehensive picture of this market, it is necessary to
consider competitive scenarios, ideally with several firms. Here, we start this analysis with two vendors and, in the next section, show that many of the insights obtained in this duopoly setting are generalizable.

We apply the concept of fulfilled expectations Cournot equilibrium [16]. Cournot competition fits this context a lot better than Bertrand [8]. A large majority of subscriptions to security software happens through preloading contracts with computer manufacturers. Consumers get a free trial period for the preloaded software, but must purchase the subscription if they wish to continue using it beyond the trial period. Engaging in this kind of long-term preloading contracts means that a vendor plans how many subscriptions it intends to sell, since the price it is willing to pay for the preloading contract is contingent on the expected sales. Kreps and Scheinkman [17] show that, when vendors plan for a certain quantity in the first stage, a Bertrand-like price competition still leads to a Cournot equilibrium, even if the marginal production cost is zero. It is also instructive to see why the alternative, Bertrand competition, does not work in this context.

First, a pure Bertrand would drive the price down to zero—not something that is observed in practice. Second, a differentiated Bertrand—the circular or linear city models—would require a complete coverage of the market for real competition to set in. Of course, when the market is not fully covered, each firm essentially becomes a local monopoly, implying that our results in the previous section would be applicable to such a setting. On the other hand, assuming a complete coverage would be contrary to real-world observations.

Let us consider two vendors offering quality levels \( \theta_l \) and \( \theta_h \) at prices \( p_l \) and \( p_h \), respectively. Without loss of generality, we assume that \( \theta_l \leq \theta_h \). As shown in Figure 4, the overall market is segmented into three parts by the points \( u_h \) and \( u_l \), where \( 0 \leq u_l \leq u_h \leq 1 \). Consumers in \([u_h, 1]\) choose the superior product, those in \([u_l, u_h]\) choose the inferior one, and the rest in \([0, u_l]\) opts not to adopt either version. The respective market sizes for the superior and inferior products are \( x_h = 1 - u_h \) and \( x_l = u_h - u_l \). Of course, the marginal users, \( u_l \) and \( u_h \), must satisfy...
the following conditions:

\[ \theta_i (1 + g(1 - \theta_i x_i - \theta_i x_i)) u_i - p_i = 0, \quad \text{and} \]
\[ \theta_h (1 + g(1 - \theta_h x_h - \theta_h x_i)) u_h - p_h = \theta_i (1 + g(1 - \theta_i x_h - \theta_i x_i)) u_h - p_h. \]

Substituting \( u_h = 1 - x_h \) and \( u_i = 1 - x_h - x_i \) into the above conditions and solving for prices, we get:

\[ p_i = (1 + g(1 - \theta_i x_h - \theta_i x_i))(\theta_i (1 - x_h - x_i)), \quad \text{and} \]
\[ p_h = (1 + g(1 - \theta_h x_h - \theta_i x_i))(\theta_i (1 - x_h - \theta_i x_i)). \]

The high-quality provider then solves the following optimization problem:

\[
\begin{align*}
\text{Max } & R_h = p_h x_h - c\theta_h^2 \\
\text{s.t. } & \theta_i \leq \theta_h \leq 1, \quad 0 \leq x_h + x_i \leq 1, \tag{4}
\end{align*}
\]

while the low-quality provider solves:

\[
\begin{align*}
\text{Max } & R_i = p_i x_i - c\theta_i^2 \\
\text{s.t. } & 0 \leq \theta_i \leq \theta_h, \quad 0 \leq x_h + x_i \leq 1. \tag{5}
\end{align*}
\]

<table>
<thead>
<tr>
<th>Constraint ( \theta_i \leq 1 )</th>
<th>Region I</th>
<th>Region IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binding</td>
<td>( \theta_i = 1 )</td>
<td>( \theta_i = \theta_h )</td>
</tr>
<tr>
<td>Slack</td>
<td>( \theta_h &lt; 1 )</td>
<td>( \theta_h &lt; 1 )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Constraint ( \theta_i \leq \theta_h )</th>
<th>Region II</th>
<th>Region III</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binding</td>
<td>( \theta_i &lt; \theta_h )</td>
<td>( \theta_i &lt; \theta_h )</td>
</tr>
<tr>
<td>Slack</td>
<td>( \theta_h &lt; 1 )</td>
<td>( \theta_h &lt; 1 )</td>
</tr>
</tbody>
</table>

Figure 5. Four Feasible Regions for Equilibrium Outcome

In order to analyze this case in a more rigorous fashion, we decompose the feasible region of the equilibrium outcome into four regions, as shown in Figure 5.

**Proposition 1.** An equilibrium outcome cannot be in Region IV.

Proposition 1 implies that we need to examine only Regions I, II, and III in Figure 5. The actual outcome depends on \( g \) as follows. When \( g \) is high, both vendors choose the highest level of quality \( (\theta_i = \theta_h = 1) \)—there is no vertical differentiation, and the equilibrium is observed in Region I. However, as \( g \) decreases beyond a certain threshold, competition forces one of the vendors to lower its quality \( (\theta_i < 1) \), whereas the other vendor still maintains its own \( (\theta_h = 1) \). The equilibrium thus shifts to Region II, where product differentiation is optimal. As \( g \) decreases even further, beyond another threshold, the high-quality vendor is also forced to reduce the quality level \( (\theta_h < 1) \), but, as shown in Proposition 1, it continues to maintain a quality level higher than that of the other vendor \( (\theta_h > \theta_i) \); quality differentiation is now observed in Region III.

**Proposition 2.** Let \( \gamma(g) \) be the following monotonically increasing function:

\[ \gamma(g) = \frac{8g^3 + 52g^2 + 26g + 9 + (4g^2 - 8g - 3)\sqrt{4g^2 + 4g + 9}}{1024g^2}. \]

In the duopoly market, vertical differentiation would be observed if and only if \( g < \gamma^{-1}(c) \). Otherwise, the equilibrium outcome is symmetric and in Region I.

The result in Proposition 2 can be better visualized in Figure 6, where the \((g, c)\) space is partitioned into two regions by \( \gamma(g) \). It is clear from

Figure 6 that product differentiation decision in a duopoly depends critically on the negative network effect. Although product differentiation can be a valid strategy in this market, its feasible region shrinks significantly as \( g \) increases. Therefore, product differentiation is likely to be less predominant in this market when compared to a traditional market with no negative network effect \( (g = 0) \). This perhaps explains why the quality levels of competing
products are so close to one another in this market. We state this more formally:

**Proposition 3.** In the duopoly market, the negative network effect makes vertical differentiation less likely.

Another way to interpret Proposition 3 is as follows. The primary benefit from vertical differentiation is that it allows manufacturers to relax competition—some manufacturers can target value-seeking consumers and others quality-seeking ones. Such differentiation, however, expands the market coverage by providing value-seeking consumers with cheaper alternatives. Because the negative network effect makes market expansion unattractive, it also makes differentiation an unappealing proposition.

5. Oligopoly
We begin our analysis by discussing how a consumer would behave when multiple products with different quality levels are available to him. We assume that there are $n$ quality levels, the $i$-th level being denoted by $\theta_i$, $i = 1, 2, \ldots, n$. Without loss of generality, we assume the following ordering:

$$0 \leq \theta_1 \leq \theta_2 \leq \ldots \leq \theta_n \leq 1.$$ 

Let $p_i$ be the normalized price charged for $\theta_i$, $i = 1, 2, \ldots, n$.

As before, consumers self-select themselves into one of the $n+1$ classes. Let $u_i$ denote a consumer who is indifferent between class $i-1$ and class $i$, $i = 2, 3, \ldots, n$, and $u_1$ denote a consumer who is indifferent between buying $\theta_1$ and not buying at all. Setting $p_0 = \theta_0 = 0$, we can characterize the marginal consumer $u_i$, $i = 1, 2, \ldots, n$, as follows:

$$\theta_i \left(1 + g \left(1 - \sum_{j=1}^{n} \theta_j x_j\right)\right) u_i - p_i =$$

$$\theta_{i-1} \left(1 + g \left(1 - \sum_{j=1}^{n} \theta_j x_j\right)\right) u_i - p_{i-1}, \quad (6)$$

where $x_i$ is the individual market coverage of $\theta_i$. Solving the recursion in (6), we get:

$$p_i = \left(1 + g \left(1 - \sum_{j=1}^{n} \theta_j x_j\right)\right) \left(\theta_i \left(1 - \sum_{j=1}^{n} x_j\right) - \sum_{j=1}^{i-1} \theta_j x_j\right). \quad (7)$$

Assuming that each quality level is offered by a unique vendor, the optimization problem for the $i$-th vendor can be written as:

$$\begin{align*}
\text{Max} & \quad R_i = p_i x_i - c \theta_i^2 \\
\text{s.t.} & \quad \theta_{i-1} \leq \theta_i \leq \theta_{i+1}, \quad 0 \leq \sum_{i=1}^{n} x_i \leq 1.
\end{align*}$$

Characterizing the equilibrium analytically is a difficult task, and it continues to be a focus of our ongoing research. However, it is easier to obtain the equilibrium numerically. Figure 7 depicts the equilibrium for a market with five vendors: As $g$ increases, the asymmetry in the market progressively declines, with more and more vendors targeting the top end of the market, preferring to split the top end of the market instead of reaching toward the bottom. This is because leaving one end of the market uncovered significantly enhances the willingness-to-pay of the other, particularly when the negative network effect is large. Therefore, as shown in Figure 7(b), the market coverage also declines with $g$. It is important to note that these results are consistent with those from the duopoly case.

Our results have practical relevance. In Table 1, we have compared twelve leading antivirus products. As shown there, the average ratings of these products are quite close, indicating a lack of vertical differentiation. Our analysis suggests that a plausible reason for this market structure is the negative network effect. The main lesson for vendors, therefore, is that operating in the security software market requires moving away from the strategy of vertical differentiation and towards emulating quality leaders.

6. Conclusion
The motivation for this work is largely rooted in the unique structure of the market for off-the-shelf security software. One of the interesting characteristics of this market is that there are a large number of vendors who sell nearly identical products. We have examined offerings from several major players and found little evidence of product differentiation. Equally interesting is the observation that vendors in this market seem content leaving a large part of the market uncovered. All these characteristics are rather unusual for an oligopoly market with a large number of players.

There is a negative network effect in the case of security software, which is derived from the fact that, as the market coverage grows, the chance of an indirect attack from an unprotected computer decreases. Incorporating this negative network effect, we examine the strategy of vertical product differentiation in a competitive setting. We develop an economic model comprising all aspects that are relevant to this market. We consider different market structures—monopoly, duopoly, and oligopoly—and endogenize quality decisions of vendors. Additionally, we incorporate the fact that product development is costly.
for these information goods, although the cost of producing a marginal copy may be negligible.

The duopoly setting, though not entirely representative of the security software market, provides us with interesting insights about market competition. We find that there are three possible equilibrium configurations; see Figure 5. Only in two of these configurations, there is vertical differentiation. However, at higher levels of the negative network effect, the likely market configuration is the third one in which there is no differentiation. Proposition 2 shows that there is a threshold for the negative network effect parameter, $g$, beyond which the market becomes completely symmetric. We also find that this result extends to the oligopoly market. Figure 7(a) shows that, as $g$ increases, the asymmetry in the market progressively declines, with more and more vendors starting to concentrate at the very top end of the quality spectrum. This finding provides an economic explanation as to why there are so many vendors in this market offering nearly identical feature-rich products. We argue that controlling the free-riding behavior requires that vendors abandon the bottom end of the market in order to extract more revenues from the top end. This is corroborated by Figure 7(b), which shows that a higher $g$ leads to a lower equilibrium market coverage. This insight is valuable as it shows how vendors in this highly competitive market can respond to the negative network effect by suitably altering positioning of their products.

We have shown that the negative network effect reduces the likelihood of differentiation in the security software market. However, a few questions still remain. First, this result was obtained with the assumption that individual vendors do not version their products. Although prior literature has argued that, absent a marginal cost, versioning is not an optimal strategy for a monopolist [4], it is not clear whether it would continue to be so, especially given the extra competitive pressure in this oligopoly. Second and on a related note, vertical differentiation can still occur as a result of one or more vendors offering multiple versions. Therefore, to explain a lack of differentiation observed in practice, we need to analyze whether versioning could be optimal. Finally, several vendors have now started offering free antivirus software products [20]. Our analysis would remain incomplete until this aspect is carefully incorporated into the model. Of course, the model in its current form is quite complex already, so incorporating this new aspect may severely impact its analytical tractability. We are currently working on these issues.

References


