DIMACS Technical Report 97-24
June 1997

Symmetrization of Binary Random Variables[2]

by

Abram Kagan University of Maryland, College Park, MD
Colin Mallows AT&T Laboratories, Floram Park, NJ
Larry Shepp Rutgers University, New Brunswick, NJ[1]
Robert J. Vanderbei Princeton University, Princeton, NJ[1]
Yehuda Vardi Rutgers University, New Brunswick, NJ

[1]Permanent Member

[2]Research of the fourth author supported by the NSF through grant CCR-9403789 and by AFOSR through grant F49620-95-1-0351. Research of the fifth author supported by the NSA through grant DMA 96-1-0034.

DIMACS is a partnership of Rutgers University, Princeton University, AT&T Labs, Bellcore, and Bell Labs.
DIMACS is an NSF Science and Technology Center, funded under contract STC–91–19999; and also receives support from the New Jersey Commission on Science and Technology.

Abstract

A random variable Y is called an *independent symmetrizer* of a given random variable X if (a) it is independent of X and (b) the distribution of $X + Y$ is symmetric about 0. In cases where the distribution of X is symmetric about its mean, it is easy to see that the constant random variable $Y = -\mathbb{E}X$ is a minimum-variance independent symmetrizer. Taking Y to have the same distribution as $-X$ clearly produces a symmetric sum but it may not be of minimum variance. We say that a random variable X is *symmetry resistant* if the variance of any symmetrizer, Y, is never smaller than the variance of X. Let X be a binary random variable: $\mathbb{P}\{X = a\} = p$ and $\mathbb{P}\{X = b\} = q$ where $a \neq b$, $0 < p < 1$, and $q = 1 - p$. We prove that such a binary random variable is symmetry resistant if (and only if) $p \neq 1/2$. Note that the minimum variance as a function of p is discontinuous at $p = 1/2$. Dropping the independence assumption, we show that the minimum-variance reduces to $pq - \min(p, q)/2$, which is a continuous function of p.

1. Introduction

Let X be a given random variable. Given the special place of the Gaussian distribution, it is of interest to find out what random variable Y that is independent of X makes the distribution of the sum $X+Y$ close to Gaussian. With no further restriction on Y, the problem does not make sense, since a Gaussian Y with large variance will make the distribution of $X+Y$ arbitrarily close to Gaussian in any reasonable sense. However, if the perturbations Y are subject to

$$\operatorname{var}(Y) \leq \sigma^2, \tag{1}$$

σ^2 being a given (small) constant, the problem makes sense once the distance from $X+Y$ to the class of Gaussian random variables is chosen. An easier version of the problem would be this: find Y independent of X with minimum variance such that $X+Y$ is Gaussian. However, the classical decomposition theorem due to Cramér (see, e.g., [2]) states that unless X is itself Gaussian no Y makes $X+Y$ Gaussian. Rather than asking for $X+Y$ to be Gaussian, one could stipulate that $X+Y$ be within a certain distance of the class of Gaussian random variables and again the problem makes sense. However, we have not been able to obtain any concrete results along these lines.

Looking for weaker properties than being Gaussian leads to meaningful and nontrivial problems. We say that a random variable Y is a *symmetrizer* of a given random variable X if the distribution of $X+Y$ is symmetric about 0. It is called an *independent symmetrizer* if, in addition, it is independent of X. A symmetrizer (or independent symmetrizer) is called *minimum-variance* if among all such symmetrizers it has minimum variance.

When the distribution of X is symmetric about its mean, it is easy to see that the constant random variable $Y=-\mathbb{E}X$ is a minimum-variance independent symmetrizer, the minimum variance being zero. In general, taking Y to have the same distribution as $-X$ clearly produces a symmetric sum but it may not be of minimum variance. Such a Y provides an upper bound on the variance of a symmetrizer. We say that a random variable X is *symmetry resistant* if such a Y is indeed the minimum-variance independent symmetrizer.

It is interesting to determine which random variables are symmetry resistant. In this paper, we solve the problem in the case where X is a *binary random variable*; that is, $\mathbb{P}\{X=a\}=p$ and $\mathbb{P}\{X=b\}=q$ where $a\neq b$, $0<p<1$, and $q=1-p$. In Section 2, we show that X is symmetry resistant when $p\neq 1/2$. Hence, the minimum variance for $p\neq 1/2$ is pq whereas for $p=1/2$ it is 0. It seems interesting that there is this discontinuity as p varies.

In Section 3, we drop the independence assumption and exhibit a minimum-variance symmetrizer of a binary random variable having variance $pq-\min(p,q)/2$, which is a continuous function of p.

Section 4 explores the relationship between symmetry-resistance and decomposability. We show that the absense of a symmetric component is not sufficient to guarantee symmetry resistance. In a related vein, we show that binomial random variables with parameters n and p are not symmetry resistant when $n\geq 4$ and p is close to $1/2$. We also show that an independent symmetrizer need not be unique.

The problem of symmetrizing X by an independent random variable Y can be formulated within the framework of the arithmetic of characteristic functions. Let

$$f(t)=\mathbb{E}\exp(itX), \qquad g(t)=\mathbb{E}\exp(itY).$$

The condition that Y is an independent symmetrizer of X is equivalent to the condition that

$$f(t)g(t) \text{ is real for } t \in \mathbb{R}. \tag{2}$$

Finding a minimum variance symmetrizer Y is then equivalent to finding a characteristic function g subject to (2) with minimum value of

$$-\left(g''(0) + (g'(0))^2\right). \tag{3}$$

Though the arithmetic of characteristic functions is a well-developed chapter of probability (see, e.g., [1]) it seems that its methods are not fit for the problem under study and instead one needs duality theory of linear programming to obtain sharp bounds. This is seen most clearly in the example of Section 4.

2. Independent Symmetrizers

In this section, we prove the following result.

Theorem 1. *A binary random variable is symmetry resistant if and only if it is not symmetric about its mean (i.e., $p \neq 1/2$).*

Proof. Applying translation and scaling operations, it is easy to reduce the problem to the case where X is a Bernoulli random variable. That is, $\mathbb{P}\{X = 1\} = p$ and $\mathbb{P}\{X = 0\} = q$.

Since the mean value of $X + Y$ must, by symmetry, be zero, it follows that $\mathbb{E}Y = -p$. Thus minimizing the variance of Y is equivalent to minimizing the second moment, $\mathbb{E}Y^2$, which is a linear functional on the space of distributions for Y. Also, the constraints that Y is independent of X and that $X + Y$ is symmetric about zero are linear constraints on the space of distributions for Y. Hence, the problem is an infinite dimensional linear programming problem.

We have already mentioned that a random variable Y whose distribution is the same as that of $-X$ symmetrizes X. This random variable has second moment p. To prove that it minimizes the second moment, we need to show that every symmetrizer has second moment at least p. In the language of linear programming, we need to exhibit the optimal solution to the dual problem (see, e.g., [4]) and then use the weak duality theorem to derive the desired inequality. Suppose we can find a function ρ defined on $\mathbb{R}$ that has the following properties:

1. ρ is an odd function: $\rho(-y) = -\rho(y), \quad -\infty < y < \infty$.
2. $q\rho(y) + p\rho(1 + y) \leq y^2 - p, \quad -\infty < y < \infty$.

Then, for any independent symmetrizer Y of X, we compute as follows:

$$\begin{aligned} 0 &= \mathbb{E}\rho(X+Y) \\ &= q\mathbb{E}\rho(Y) + p\mathbb{E}\rho(1+Y) \\ &= \mathbb{E}(q\rho(Y) + p\rho(1+Y)) \\ &\leq \mathbb{E}Y^2 - p, \end{aligned}$$

where the first equality follows from the facts that ρ is odd and $X+Y$ is symmetric and the second from the independence of X and Y. The inequality follows from property (2) of ρ.

When $p = 1/2$, we know that there can be no function ρ with the properties given above because we have already given a Y which has zero variance and therefore violates the inequality derived above. But, for every $p \neq 1/2$, we can exhibit such a function. It is defined as follows. First, let h be a saw-tooth function defined on $\mathbb{R}$ by setting

$$h(y) = y, \qquad -1/2 \le y \le 1/2,$$

and then extending to all reals by setting

$$h(y+1) = -h(y), \qquad -\infty \le y \le \infty.$$

The function h is odd. Furthermore, h agrees with the parabolic function $y(y+1)$ at $y = 0$ and $y = -1$ and each curve has the same derivative at these points as well. It therefore follows from convexity that $h(y) \le y(y+1)$ for all $y \in \mathbb{R}$. The function ρ is defined by:

$$\rho(y) = \frac{h(y)}{q-p} - y.$$

Clearly, ρ is odd. It also satisfies the second requisite condition as the following calculations show:

$$\begin{aligned} q\rho(y) + p\rho(1+y) &= q\left(\frac{h(y)}{q-p} - y\right) + p\left(\frac{h(1+y)}{q-p} - (1+y)\right) \\ &= h(y) - y - p \\ &\le y(y+1) - y - p \\ &= y^2 - p. \end{aligned}$$

This finishes the proof. $\square$

The reader may be wondering how we thought of the correct choice of ρ. The answer is that we discretized an interval of the real line and thereby formulated a finite dimensional linear program as an approximation to the problem. We then used the fourth author's software, called LOQO (see [3]), to solve these discrete approximations and eventually were able to guess at the correct functional form for ρ. It is interesting to note that ρ is far from unique, since we needed only the properties $h(y) = -h(y+1)$ and the inequality $h(y) \le y(y-1)$ of the odd function h. There are many such examples; the one given may be the simplest. A standard algorithm for solving finite dimensional linear programming problems is the simplex method. This method proved of no use to solve this problem since among the myriad possible solutions it gives an essentially random one. Hence, we were unable to see the form of ρ from such solutions. LOQO, on the other hand, implements an interior-point method and consequently converges to the (uniquely defined) analytic center of the set of optimal solutions (see [4] for details). From such a "regular" (smooth) solution it was fairly easy to discover the function ρ.

The reader may also feel that a simpler proof should exist given that X is assumed to take on only two values. In particular, one might expect that it would be possible to restrict the search to random variables Y that only take on a finite number of values (by invoking, say, Carathéodory's theorem—see e.g. [4]). This, of course, would simplify the problem, but we were unable to justify such a restricted search.

Finally, we note that as p tends to $1/2$, ρ has no limit.

3. Dependent Symmetrizers

In this section, we find the minimum-variance symmetrizer when Y is allowed to depend on X. One could take $Y = -X$ noting this symmetrizes X since $X+Y = 0$, but this Y again has variance pq. The following theorem asserts that there is a dependent symmetrizer whose variance is less than pq.

Theorem 2. *Allowing dependence between a binary random variable and its symmetrizer, the minimum-variance symmetrizer has variance* $pq - \min(p, q)/2$.

Note that in this dependent case, the minimizing variance is continuous in p. Why it should be continuous in the dependent case but discontinuous in the independent one seems a bit mysterious.

Proof. We assume without loss of generality that $p \geq q$, and consider a three point sample space, $\Omega = \{\omega_1, \omega_2, \omega_3\}$, with the following assigned probabilities:

$$P(\omega_1) = P(\omega_2) = q, \quad P(\omega_3) = p - q = 1 - 2q.$$

On this space we define random variables X and Y as follows:

$$\begin{array}{llll} X(\omega_1) & = 1, & Y(\omega_1) & = -1/2, \\ X(\omega_2) & = 0, & Y(\omega_2) & = -1/2, \\ X(\omega_3) & = 1, & Y(\omega_3) & = -1. \end{array}$$

It is easy to check that X takes values 1 and 0 with probabilities p and q, respectively, and that $Z = X + Y$ is symmetric. Indeed,

$$\begin{array}{ll} Z(\omega_1) & = 1/2 \\ Z(\omega_2) & = -1/2 \\ Z(\omega_3) & = 0. \end{array}$$

Also, the variance of Y is easily seen to be $pq - \min(p, q)/2$. All that remains is to show that any symmetrizer must have a variance at least this large.

To show one can't do better, we will use a linear programming argument similar to the one before. We start by assuming the existence of an odd function, ρ, satisfying the following two inequalities:

$$\rho(z) \leq z^2 + 1/2 \quad \text{and} \quad \rho(z) \leq (z-1)^2 - 1.$$

Using these inequalities, we see that

$$\begin{array}{rcl} \rho(X+Y) & = & \rho(Y)1_{X=0} + \rho(1+Y)1_{X=1} \\ & \leq & (Y^2 + 1/2)1_{X=0} + (Y^2 - 1)1_{X=1} \\ & = & Y^2 - 1_{X=1} + 1/2\ 1_{X=0}. \end{array}$$

Taking expectations we see that

$$0 = \mathbb{E}\rho(X+Y) \leq \mathbb{E}Y^2 - p + q/2,$$

where as before the equality follows from the symmetry of $X + Y$ and the oddness of ρ. Hence, the second moment of Y is at least $p - q/2$ from which it follows that

$$\mathrm{var}(Y) \geq p - q/2 - p^2 = pq - q/2 = pq - \min(p, q)/2.$$

To complete the proof, we only need to exhibit a function ρ with the desired properties. It is easy to check that the following function works:

$$\rho(z) = z(|z| - 2).$$

$\square$

4. Decomposition

Let $\text{var}(X) < \infty$. A simple necessary condition for X to be symmetry resistant is that X has no symmetric component, i.e. X cannot be represented as

$$X = U + V,$$

with U and V independent and U symmetric about 0 since in that case $-V$ would be a symmetrizer. Note that V is allowed to be degenerate; in this respect our notion of decomposability differs from the usual one that does not allow degenerate random variables. A binary random variable X with $p \neq 1/2$ has no symmetric component. If, on the other hand, it takes values a and b with equal probability then X has a symmetric component $U = X - (a+b)/2$.

Looking for symmetric components of X falls within the framework of the arithmetic of characteristic functions. Unfortunately, the absence of a symmetric component in X is not sufficient for its being symmetry resistant:

Theorem 3. *There exist symmetry-nonresistant random variables that have no symmetric components.*

Proof. The proof is by construction of an example. Suppose that X has the following distribution:

$$\begin{aligned} \mathbb{P}\{X=0\} &= 4/9, \\ \mathbb{P}\{X=1\} &= 0, \\ \mathbb{P}\{X=2\} &= 3/9, \\ \mathbb{P}\{X=3\} &= 2/9. \end{aligned}$$

If Y is independent of X and takes values -1 and -2 with probability $2/3$ and $1/3$, respectively, then

$$\begin{aligned} \mathbb{P}\{X+Y=-2\} = \mathbb{P}\{X+Y=2\} &= 4/27 \\ \mathbb{P}\{X+Y=-1\} = \mathbb{P}\{X+Y=1\} &= 8/27 \\ \mathbb{P}\{X+Y=0\} &= 3/27 \end{aligned}$$

so that $X+Y$ is symmetric. As one can see, $\text{var}(Y) < \text{var}(X)$ which implies that X is not symmetry resistant.

To see that X is not decomposable, note that the probability generating function of X is $(4+3z^2+2z^3)/9$ and has the unique real factorization $(1+2z)/3 \cdot (2 - z + 2z^2)/3$. But the second factor is not the probability generating function of a proper random variable. $\square$

A similar construction shows that the sum of four independent replicas of a binary random variable with $0.4889752 < p < 0.5$ is not symmetry-resistant, even though it has no symmetric component. Indeed, let Z have a six-point improper distribution with negative "variance", with "probabilities" proportional to $(p^2q, -4p^3, 16p^2q - 6q^3, 16p^2q - 6q^3, -4p^3, p^2q)$. Then for the stated range of p, $X+Z$ is proper, and has variance less than the variance of X. The corresponding random variable is a symmetrizer of $-X$. The lower extreme of the range of p is a root of the cubic $71p^3 - 23p^2 - 18p + 6$.

This result implies that for all $n \geq 4$, for p in a neighborhood of $1/2$, a sum of n independent binary random variables is not symmetry-resistant. We conjecture that this is not true for $n = 2, 3$.

Finally, we ask the question: is a minimum-variance symmetrizer unique? The answer is no:

Theorem 4. *There exists a random variable for which the minimum-variance independent symmetrizer is not unique.*

Proof. We shall show that there is a nonsymmetric random variable X with at least two different minimum-variance symmetrizers, one of which may be symmetric. First, we construct a non-symmetric distribution such that a sum $X_1 + X_2$ of two independent random variables with this non-symmetric distribution is symmetric. Let ψ be a real characteristic function that vanishes for all $|t| \geq 1/2$, for example the characteristic function corresponding to the density

$$f(x) = A\left(\frac{\sin(x/8)}{x/8}\right)^4,$$

where $A = 3/4\pi$ is a normalizing constant so that f integrates to unity. Let

$$\phi(t) = \psi(t) + (i/2)(\psi(t-1) - \psi(t+1)).$$

Clearly, ϕ^2 is real, so that $X_1 + X_2$ is symmetric. The density corresponding to ϕ is

$$g(x) = A(1 - \sin x)\left(\frac{\sin(x/8)}{x/8}\right)^4,$$

which has finite variance. We do not know whether or not this X is resistant. (we suspect not.) If it is, then both X and $-X$ are minimum-variance symmetrizers of X. If not, let Y be a minimum-variance symmetrizer of X. Then the characteristic function χ of Y must be real (or zero) where ϕ is real, and purely imaginary (or zero) where ϕ is purely imaginary. If Y is not symmetric, then both Y and $-Y$ are minimum-variance symmetrizers of X. If Y is symmetric, then $\chi(t)$ must vanish for $1/2 < |t| < 3/2$, and $\chi(t) + i(\chi(t+1) - \chi(t-1))/2$ is the characteristic function of a non-symmetric symmetrizer of X, with the same variance as Y. $\square$

References

[1] Yu.V. Linnik and I.V. Ostrovskii. *Decomposition of Random Variables and Vectors.* Amer. Math. Soc., Providence RI, 1977.

[2] E. Lukacs. *Characteristic Functions.* Griffin, London, 2 edition, 1970.

[3] R.J. Vanderbei. LOQO: An interior point code for quadratic programming. Technical Report SOR 94-15, Princeton University, 1994.

[4] R.J. Vanderbei. *Linear Programming: Foundations and Extensions.* Kluwer Academic Publishers, 1996.