Versatile Coins

István Szalkai and Dan Velleman

Suppose you had a coin which, when flipped, came up heads with probability

$$p = \frac{3 + \sqrt{3}}{6}$$

and tails with probability

$$1 - p = \frac{3 - \sqrt{3}}{6}.$$

If you flipped the coin three times, the probability of getting either three heads or three tails would be

$$p^3 + (1 - p)^3 = \frac{9 + 5\sqrt{3}}{36} + \frac{9 - 5\sqrt{3}}{36} = \frac{1}{2}.$$

Thus, by flipping this coin three times you could simulate the behavior of a fair coin, and thus make a random choice between two alternatives, with each alternative being chosen with probability $1/2$. But note that if you flipped the coin twice, the probability of getting one head and one tail (in either order) would be $2p(1 - p) = 1/3$, so you could also use this coin to make a random choice between two alternatives, with one alternative being chosen with probability $1/3$, and the other with probability $2/3$. In a sense, this coin is more versatile than either a fair coin or a coin which comes up heads with probability $1/3$.

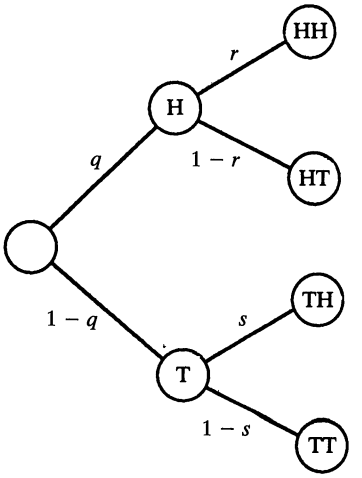
We will say that $(3 + \sqrt{3})/6$ *simulates* both $1/2$ and $1/3$. In general, if p and q are any two numbers between 0 and 1, we will say that p *simulates* q if, given a coin which comes up heads with probability p, we can, in a finite number of flips, simulate the behavior of a coin which comes up heads with probability q. More precisely, p simulates q if there is some positive integer n and some subset E of the 2^n possible outcomes of flipping a coin n times such that, if a coin which comes up heads with probability p is flipped n times, the probability that the resulting sequence of heads and tails is in the set E is q. Now the probability $P(E)$ that the sequence of heads and tails is in the set E is given by the formula

$$P(E) = \sum_{i=0}^{n} a_i p^i (1 - p)^{n-i},$$

where for each i, a_i is the number of elements of E which contain i heads and $n - i$ tails. Clearly we have $0 \le a_i \le \binom{n}{i}$, and any sequence of integers $\{a_i\}_{i=0}^{n}$ satisfying these inequalities will correspond to some set E. Thus, p simulates q iff there is a positive integer n, and integers a_i satisfying $0 \le a_i \le \binom{n}{i}$, such that

$$q = \sum_{i=0}^{n} a_i p^i (1 - p)^{n-i}.$$

There are a number of observations that we can make right away. Clearly the "simulates" relation is reflexive, and it is not hard to see that it is also transitive. In other words, it is a preorder. Every number between 0 and 1 simulates both 0 and 1, since any coin can be used to simulate the behavior of a coin which either always comes up heads or always comes up tails. It is also clear that in general p and $1 - p$ simulate each other, and it follows by transitivity that if p simulates q then both p and $1 - p$ simulate both q and $1 - q$. It is not hard to see that if p simulates q and r, then it simulates their product qr. More generally, if p simulates q, r, and s, then it simulates $qr + (1 - q)s$ (see FIGURE 1). In fact, the reader might want to verify that the set of numbers simulated by p is precisely the closure of the set $\{0, 1\}$ under the function $f(x, y) = px + (1 - p)y$.



P(HH or TH) = $qr + (1 - q)s$

Figure 1. If we flip three coins, whose probabilities of coming up heads are q, r, and s, then we can find an event with probability $qr + (1 - q)s$. Thus, if p simulates q, r, and s, then it also simulates $qr + (1 - q)s$.

What else can we say about the "simulates" relation? One interesting way to investigate this relation is to try to design versatile coins, like the one described in the first paragraph of this paper. In that example we found that $(3 + \sqrt{3})/6$ simulates both $1/2$ and $1/3$. The reader may have been surprised that we used such a complicated number to simulate both $1/2$ and $1/3$. Couldn't we have found a rational number that would do it?

The answer, it turns out, is no. The reason is that $1/2$ doesn't simulate $1/3$, and no rational number other than $1/2$ simulates $1/2$. The first of these facts can be seen by noting that $1/2$ only simulates rational numbers with denominators of the form 2^n, for some natural number n. To prove the second, suppose $p = j/k$ is a rational number, with j and k relatively prime, and p simulates $1/2$. Then we can choose a positive integer n and integers a_i, $0 \le a_i \le \binom{n}{i}$, such that

$$\sum_{i=0}^{n} a_i p^i (1 - p)^{n-i} = \frac{1}{2}.$$

Now let $b_i = \binom{n}{i} - a_i$, and note that by the binomial theorem we have

$$\sum_{i=0}^{n} b_i p^i (1-p)^{n-i} = 1 - \frac{1}{2} = \frac{1}{2}.$$

Since $a_0 + b_0 = \binom{n}{0} = 1$, we have either $a_0 = 0$ or $b_0 = 0$. Without loss of generality, assume $a_0 = 0$. Then

$$\frac{1}{2} = \sum_{i=1}^{n} a_i p^i (1-p)^{n-i} = p \sum_{i=1}^{n} a_i p^{i-1} (1-p)^{n-i} = \frac{j}{k} \cdot \frac{\sum_{i=1}^{n} a_i j^{i-1} (k-j)^{n-i}}{k^{n-1}}.$$

Thus we have $k^n = 2j \cdot \sum_{i=1}^{n} a_i j^{i-1} (k-j)^{n-i}$, so $j | k^n$. Since j and k were assumed to be relatively prime, it follows that $j = 1$. But now note that $1 - p = (k-j)/k = (k-1)/k$ also simulates $1/2$, so by the same reasoning we have $k - 1 = 1$. Therefore $k = 2$, so $p = 1/2$. A similar, although slightly more complicated, proof can be used to show that the only rational numbers that simulate $1/3$ are $1/3$ and $2/3$. In fact, the proof can be generalized to show that for any square-free integer $N > 1$, the only rational numbers that simulate $1/N$ are $1/N$ and $(N-1)/N$.

Thus, we see that there are strict limits to the versatility of coins whose probability of coming up heads is rational. However, as the following theorem shows, coins with an irrational probability of coming up heads can sometimes be quite versatile.

Theorem 1. *Suppose F is a finite set of rational numbers and $F \subseteq [0, 1]$. Then there is a number $p \in [0, 1]$ such that p simulates every element of F.*

In the proof of the theorem, we will need the following lemmas:

Lemma 2. *For every integer $n > 1$,*

$$\left(1 - \frac{1}{n}\right)^{n-1} > \frac{1}{e}.$$

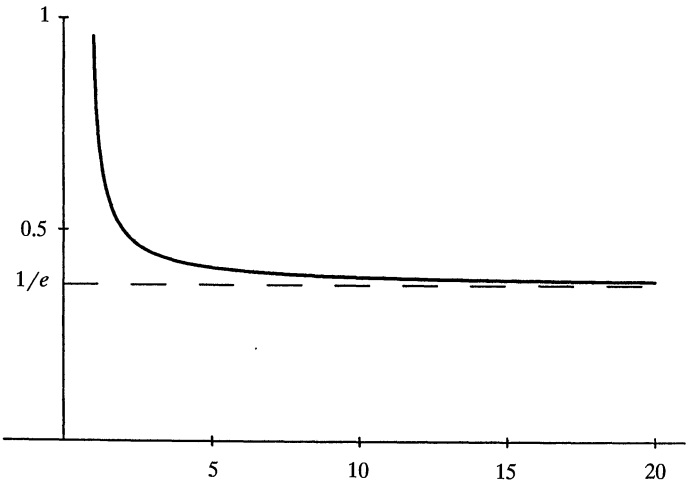


Figure 2. The Graph of the Function $f(x) = (1 - 1/x)^{x-1}$.

Proof: Let $f(x) = (1 - 1/x)^{x-1}$ for $x > 1$. It is clear that $\lim_{x \to \infty} f(x) = 1/e$, so to prove the lemma it will suffice to show that f is decreasing. We will let the reader check that

$$f'(x) = f(x)\left[\frac{1}{x} + \ln\left(1 - \frac{1}{x}\right)\right].$$

Since $\ln x < x - 1$ for all $x \in (0, 1)$, we have $\ln(1 - 1/x) < -1/x$ for all $x > 1$. Thus $f'(x) < 0$, so f is decreasing. □

Lemma 3. *For every real number $z \in [0, 1/e]$ and positive integer n, there is a number $p \in [0, 1]$ such that*

$$np(1 - p)^{n-1} = z.$$

(Note that this equation says that if a coin which comes up heads with probability p is flipped n times, then the probability of getting exactly one head is z.)

Proof: If $n = 1$ then we simply let $p = z$. Now suppose $n > 1$. If $p = 0$ then the left side of the equation above is $0 \le z$. If $p = 1/n$ then by Lemma 2 the left side is $(1 - 1/n)^{n-1} > 1/e \ge z$. Thus there is some $p \in [0, 1/n)$ such that $np(1 - p)^{n-1} = z$. □

Proof of Theorem 1. Let N be the maximum of the denominators of the elements of F. We assume w.l.o.g. that $N \ge 4$. Let $n = N!/3$. By Lemma 3, let p be a solution to the equation $np(1 - p)^{n-1} = 1/3$. Then according to the analysis of the "simulates" relation above, p will simulate every number of the form

$$ap(1 - p)^{n-1} = \frac{a}{3n} = \frac{a}{N!},$$

for $0 \le a \le \binom{n}{1} = n = N!/3$. It follows that p simulates $1/3, 1/4, \ldots, 1/N$.

As we observed above, if p simulates q then it also simulates $1 - q$, and if p simulates both q and r then it simulates their product qr. Thus, p simulates $2/3, 3/4, \ldots, (N - 1)/N$. Since p simulates both $2/3$ and $3/4$, it also simulates $2/3 \cdot 3/4 = 1/2$. (This is where we use the assumption $N \ge 4$.) Now for any rational number j/k, with $1 \le j < k \le N$, we have

$$\frac{j}{k} = \frac{j}{j+1} \cdot \frac{j+1}{j+2} \cdot \cdots \cdot \frac{k-1}{k}.$$

Since we have already shown that p simulates every factor on the right side, it follows that p simulates j/k. Thus p simulates every rational number between 0 and 1 with denominator at most N, and therefore in particular it simulates every element of F. □

The same method of proof can also handle some sets of non-rational probabilities. Let F be a finite subset of $[0, 1/e]$ such that the ratio of any two nonzero elements of F is rational. Let z be the largest element of F. Then every other element of F can be written as a rational multiple of z, and by finding a common denominator for these rational multiples we may write F as

$$F = \left\{z, \frac{zj_1}{n}, \frac{zj_2}{n}, \ldots, \frac{zj_m}{n}\right\},$$

for some integers $j_1, j_2, \ldots, j_m$ and n with $0 \le j_i < n$ for $1 \le i \le m$. Since $z \le 1/e$, by Lemma 3 there is a number $p \in [0, 1]$ such that $np(1 - p)^{n-1} = z$. Then as

above p simulates every number of the form $ap(1-p)^{n-1} = za/n$, for $0 \le a \le n$. Since every element of F has this form, p simulates every element of F.

We can eliminate the upper bound $1/e$ in this result by using a somewhat more complicated proof. Instead of considering only sequences of coin flips in which there is *exactly* one head, we consider sequences which have *at least* one head.

Theorem 4. *Suppose $F \subseteq [0,1]$, F is finite, and the ratio of any two nonzero elements of F is rational. Then there is a number $p \in [0,1]$ such that p simulates every element of F.*

Proof: Since every number between 0 and 1 simulates 1, we may assume w.l.o.g. that $1 \notin F$. As before, we let z be the largest element of F, and then write F as

$$F = \left\{ z, \frac{zj_1}{N}, \frac{zj_2}{N}, \ldots, \frac{zj_m}{N} \right\},$$

for some integers $j_1, j_2, \ldots, j_m$ and N with $0 \le j_i < N$ for $1 \le i \le m$. Since $z < 1$, we can choose an integer n large enough so that

$$1 - \frac{1 + nN}{2^n} > z.$$

For each integer i, $1 \le i \le n$, let q_i be the quotient when $\binom{n}{i}$ is divided by N, and let r_i be the remainder. Thus q_i and r_i are nonnegative integers, $r_i < N$, and

$$\binom{n}{i} = Nq_i + r_i.$$

We now claim that we can choose $p \in [0,1]$ so that p is a solution to the equation

$$(*) \qquad \sum_{i=1}^{n} Nq_i p^i (1-p)^{n-i} = z.$$

Once we have such a p, we can conclude that for every integer a, $0 \le a \le N$, p simulates

$$\sum_{i=1}^{n} aq_i p^i (1-p)^{n-i} = \frac{za}{N}.$$

Since every element of F has this form, it follows that p simulates every element of F.

To see that we can choose $p \in [0,1]$ satisfying $(*)$, first note that when $p = 0$, the left side of $(*)$ is $0 \le z$. But when $p = 1/2$, the left side is

$$\sum_{i=1}^{n} \frac{Nq_i}{2^n} = \frac{1}{2^n} \sum_{i=1}^{n} \left[\binom{n}{i} - r_i \right] = \frac{1}{2^n} \left[2^n - 1 - \sum_{i=1}^{n} r_i \right]$$

$$> \frac{1}{2^n} [2^n - 1 - nN] = 1 - \frac{1 + nN}{2^n} > z.$$

Thus, there is a value of p between 0 and $1/2$ which satisfies $(*)$. □

Note that in the proof of Theorem 1 above, p was chosen as a root of a polynomial with rational coefficients, so p was algebraic. In fact, in hindsight it is easy to see that this had to be true. If p simulates $q \in (0,1)$, then by our characterization of the "simulates" relation there is a nonconstant polynomial $f(x)$ with integer coefficients such that $f(p) = q$. Thus if either p or q is algebraic then the other must be as well. More generally, we can say that $\mathbb{Q}[p] = \mathbb{Q}[q]$,

where for any real number a, $\mathbb{Q}[a] = \{r \in \mathbb{R} | r$ is algebraic over $\mathbb{Q}(a)\}$. This shows that if p simulates every element of some set $F \subseteq [0,1]$, then for every $q \in F \setminus \{0,1\}, \mathbb{Q}[q] = \mathbb{Q}[p]$. Thus, if $F \subseteq [0,1]$ then there cannot be a number p which simulates every element of F unless for every q, $r \in F \setminus \{0,1\}, \mathbb{Q}[q] = \mathbb{Q}[r]$.

For which sets $F \subseteq [0,1]$ is there a number $p \in [0,1]$ such that p simulates every element of F? Our theorems so far do not completely settle this question. Although we do not know the complete answer, we can give the answer for the case $F \subseteq \mathbb{Q}$. We will need the following notation. For every positive integer N, let $\mathbb{Q}_N$ be the set

$$\mathbb{Q}_N = \left\{ \frac{j}{N^k} \middle| j, k \in \mathbb{Z} \right\}.$$

Our characterization of those sets $F \subseteq \mathbb{Q} \cap [0,1]$ such that some number $p \in [0,1]$ simulates all elements of F will be a consequence of the next two theorems.

Theorem 5. *Suppose $p \in [0,1]$. Then there is some positive integer N such that $\{q \in \mathbb{Q} \cap [0,1] | p$ simulates $q\} \subseteq \mathbb{Q}_N$.*

Proof: This proof is a modified version of a proof suggested to us by Martin Goldstern.

If p is not algebraic then, as we observed above, $\{q \in \mathbb{Q} \cap [0,1] | p$ simulates $q\} = \{0,1\}$, so the conclusion clearly holds. Now suppose p is algebraic. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a minimal degree nonconstant polynomial with integer coefficients such that $f(p) = 0$. By multiplying through by -1 if necessary, we may assume that $a_n > 0$. We will show that $\{q \in \mathbb{Q} \cap [0,1] | p$ simulates $q\} \subseteq \mathbb{Q}_{a_n}$.

Clearly $0, 1 \in \mathbb{Q}_{a_n}$. Now suppose $q \in \mathbb{Q} \cap (0,1)$ and p simulates q. Then there is a nonconstant polynomial $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ with integer coefficients such that $g(p) = q$. Thus $g(p) - q = 0$, so by the minimality of the degree of $f(x)$, $f(x)$ must divide $g(x) - q$. In other words, $g(x) - q = f(x) \cdot h(x)$ for some polynomial $h(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0$ with rational coefficients. Multiplying out the product $f(x) \cdot h(x)$ and equating the coefficients with the coefficients of $g(x) - q$, we get the following equations:

$$\begin{aligned}
m &= n + k \\
b_m &= a_n \cdot c_k \\
b_{m-1} &= a_n \cdot c_{k-1} + a_{n-1} \cdot c_k \\
b_{m-2} &= a_n \cdot c_{k-2} + a_{n-1} \cdot c_{k-1} + a_{n-2} \cdot c_k \\
&\cdots \\
b_1 &= a_1 \cdot c_0 + a_0 \cdot c_1 \\
b_0 - q &= a_0 \cdot c_0.
\end{aligned}$$

Claim. For $i = 0, 1, \ldots, k$, $(a_n)^{i+1} \cdot c_{k-i}$ is an integer.

Proof: By induction on i. The case $i = 0$ is taken care of by the second equation above, since b_m is an integer. For the general case we use the equation

$$b_{m-i} = a_n \cdot c_{k-i} + a_{n-1} \cdot c_{k-i+1} + \cdots.$$

Multiplying both sides by $(a_n)^i$ we get:

$$(a_n)^i \cdot b_{m-i} = (a_n)^{i+1} \cdot c_{k-i} + a_{n-1} \cdot (a_n)^i \cdot c_{k-i+1} + \cdots.$$

Clearly the left side of this equation is an integer, and by inductive hypothesis all

terms on the right side except the first are integers. Thus the first term must be an integer too. This proves the claim.

Applying the claim in the case $i = k$ we find that $(a_n)^{k+1} \cdot c_0$ is an integer. Let $j = (a_n)^{k+1} \cdot c_0$, so $c_0 = j/(a_n)^{k+1}$. Substituting this into the equation $b_0 - q = a_0 \cdot c_0$ we find that $q = b_0 - a_0 \cdot j/(a_n)^{k+1} \in \mathbb{Q}_{a_n}$, as required. □

Theorem 6. *For every positive integer N there is a number $p \in [0, 1]$ such that p simulates every element of $\mathbb{Q}_N \cap [0, 1]$.*

Proof: Let N be any positive integer, and by Theorem 1 choose $p \in [0, 1]$ such that p simulates $1/2, 1/3, \ldots, 1/N, 2/N, \ldots, (N-1)/N$. To complete the proof we will show that for all positive integers j and k with $j < N^k$, p simulates j/N^k.

We proceed by induction on k. The case $k = 1$ is clear, by the choice of p. For the induction step, suppose that for every positive integer $j < N^k$, p simulates j/N^k, and let j be any positive integer less than N^{k+1}. We must show that p simulates j/N^{k+1}.

Let q and r be the quotient and remainder when j is divided by N^k. Then $j = qN^k + r$, $0 \le q < N$, and $0 \le r < N^k$. By the choice of p, p simulates q/N and $1/(N-q)$, and by inductive hypothesis p simulates r/N^k. Now we apply the fact, observed above, that if p simulates x, y, and z, then it simulates $xy + (1-x)z$. Taking $x = q/N$, $y = 1$, and $z = 1/(N-q) \cdot r/N^k$, we see that p simulates

$$\frac{q}{N} + \left[1 - \frac{q}{N}\right] \frac{r}{(N-q)N^k} = \frac{q}{N} + \frac{r}{N^{k+1}} = \frac{qN^k + r}{N^{k+1}} = \frac{j}{N^{k+1}},$$

as required. □

Combining Theorems 5 and 6, we get the following characterization of those sets of rational probabilities which can be simulated by a single number.

Corollary 7. *Suppose $F \subseteq \mathbb{Q} \cap [0, 1]$. Then there is a number $p \in [0, 1]$ such that p simulates every element of F iff for some positive integer N, $F \subseteq \mathbb{Q}_N$.* □

By examining the proofs of some of the theorems above, we can actually determine precisely what rational probabilities are simulated by the numbers used in some of our proofs. Suppose N is an integer, $N \ge 4$, and let p be a solution to the equation $np(1-p)^{n-1} = 1/3$, where $n = N!/3$. As we showed in the proof of Theorem 1, p simulates all rational probabilities with denominator at most N. In fact, this also holds if $N = 3$, as the example in the first paragraph of this paper shows. The proof of Theorem 6 now shows that p also simulates all elements of $\mathbb{Q}_N \cap [0, 1]$. In fact, we can improve on the argument in that proof to show that p simulates all elements of $\mathbb{Q}_{N!} \cap [0, 1]$. This is easily seen to follow from the following proposition.

Proposition 8. *Let p and N be as described above. Suppose M and k are positive integers, $2 \le k \le N$, and p simulates all rational numbers of the form j/M, for $0 < j < M$. Then p simulates all rational numbers of the form $j/(M\kappa)$, for $0 < j < Mk$.*

Proof: Suppose $0 < j < Mk$. Let q and r be the quotient and remainder when j is divided by M. Then $j = Mq + r$, $0 \le q < k$, and $0 \le r < M$. Thus p simulates

q/k, $1/(k-q)$, and r/M. As in the proof of Theorem 6, it follows that p simulates

$$\frac{q}{k} + \left[1 - \frac{q}{k}\right] \cdot \frac{1}{k-q} \cdot \frac{r}{M} = \frac{Mq + r}{Mk} = \frac{j}{Mk}. \qquad \square$$

We can learn more about the rational numbers simulated by p by examining the proof of Theorem 5. Clearly p is algebraic, since it was chosen to be a root of the polynomial $g(x) = 3nx(1-x)^{n-1} - 1 = (N!)x(1-x)^{n-1} - 1$. Let $f(x)$ be a minimal degree nonconstant polynomial with integer coefficients such that $f(p) = 0$, and let a be the coefficient of the highest power of x in $f(x)$. The proof of Theorem 5 shows that every rational probability simulated by p must be in the set $\mathbb{Q}_a$. What can we say about the value of a?

Recall that the *content* of a polynomial with integer coefficients is defined to be the greatest common divisor of its coefficients. A polynomial is called *primitive* if its content is 1, and Gauss' Lemma says that the product of two primitive polynomials is also primitive. Note that $g(x)$ is primitive, since its constant term is -1, and w.l.o.g. we may assume that $f(x)$ is primitive as well.

By the minimality of the degree of $f(x)$, $g(x)$ is divisible by $f(x)$, so $g(x) = f(x) \cdot h(x)$, for some polynomial $h(x)$ with rational coefficients. By finding a common denominator for the coefficients of $h(x)$, and then factoring out the greatest common divisor of their numerators, we may write $h(x) = (j/k) \cdot h'(x)$, for some primitive polynomial $h'(x)$. Thus $k \cdot g(x) = j \cdot f(x) \cdot h'(x)$. But now the content of the left side of this equation is k, and by Gauss' Lemma the content of the right is j, so $j = k$, and therefore $h(x) = h'(x)$, so $h(x)$ is primitive.

Since the coefficient of the highest power of x in $g(x)$ is $\pm N!$ and $g(x) = f(x) \cdot h(x)$, it follows that $a | N!$, and therefore $\mathbb{Q}_a \subseteq \mathbb{Q}_{N!}$. Combining this with our earlier conclusions that p simulates all elements of $\mathbb{Q}_{N!} \cap [0,1]$, and that all rational probabilities simulated by p are in $\mathbb{Q}_a$, we see that

$$\{q \in \mathbb{Q} \cap [0,1] \mid p \text{ simulates } q\} = \mathbb{Q}_{N!} \cap [0,1].$$

For example, in the case $N = 3$ we can conclude that the set of rational probabilities simulated by the number $(3 + \sqrt{3})/6$ is precisely $\mathbb{Q}_6 \cap [0,1]$.

There are still many unanswered questions about the simulation of irrational probabilities. One of the simplest is this: If q and r are algebraic numbers between 0 and 1, must there be a number $p \in [0,1]$ such that p simulates both q and r?

Department of Mathematics
University of Veszprém
H 8201 Veszprém
Hungary
h2109sza@ella.hu

Dept. of Mathematics and Computer Science
Amherst College
Amherst, MA 01002
djvelleman@amherst.edu