Probabilistic Voting with Three Ballots*

Sergiu Hart†

November 5, 2022

You want to vote for party A with probability p and party B with probability $q = 1 - p$. You are alone in the voting booth, where there are paper ballots marked A and B, exactly one of which you must put in the given voting envelope. You want to do this with *zero knowledge* about your actual vote, i.e., such that you will only know that you have voted with probabilites p, q and nothing else (formally, the posterior probabilities must always be p, q). Finally, you are not allowed to deform the ballots or mark them in any way (as it will disqualify the vote).

For $p = 2/3$, you can easily do it with two A-ballots and one B-ballot: turn them upside down, mix them, choose one at random (i.e., uniformly) and put it in the envelope, and finally dispose of the other two (in such a way that you won't see what they are).

QUESTION. Can one do it for an arbitrary p with two A-ballots and one B-ballot only ?

ANSWER. Yes, for every rational p.

PROOF. The ballots are kept throughout upside down, i.e., with the non-marked side up (where they are all identical), except when checking the marking of a ballot, after which it is returned to be upside down.

One of the ballots, call it X, is put aside; the X ballot at the end of the procedure will be the actual vote. It is convenient to work with odds rather than probabilities; thus, $\mathbb{P}[X = \mathrm{A}] / \mathbb{P}[X = \mathrm{B}]$ are the *odds* (of X), which we

*Proposed and solved by Ariel Brand (see `https://arielbranda.com/?p=1`), and communicated by Oded Margalit. We present here a slightly simpler solution.

†The Hebrew University of Jerusalem (Federmann Center for the Study of Rationality, Institute of Mathematics, and Department of Economics). *E-mail*: `hart@huji.ac.il` *Web site*: `http://www.ma.huji.ac.il/hart`

write as $a : b$ (and so $\mathbb{P}[X = \mathrm{A}] = a/(a+b)$, $\mathbb{P}[X = \mathrm{B}] = b/(a+b)$, and $a : b$ and $\lambda a : \lambda b$ are the same for any $\lambda > 0$).

We will use two operations, ADD and SWAP, that, if successful, change the odds as follows:

ADD	$a : b \to (a+b) : b$
SWAP	$a : b \to b : a$

;

they both include a basic operation, CHECK. These operations are defined as follows:

- CHECK: Choose randomly one of the two non-X ballots, call it Y, and check its marking. If $Y =$ B then we restart the entire procedure. If $Y =$ A, which we call a *success*, then we continue; in this case the odds change from $a : b$ to $a : 2b$, because

$$\frac{\mathbb{P}[X = \mathrm{A} | Y = \mathrm{A}]}{\mathbb{P}[X = \mathrm{B} | Y = \mathrm{A}]} = \frac{\mathbb{P}[Y = \mathrm{A} | X = \mathrm{A}] \cdot \mathbb{P}[X = \mathrm{A}]}{\mathbb{P}[Y = \mathrm{A} | X = \mathrm{B}] \cdot \mathbb{P}[X = \mathrm{B}]} = \frac{\frac{1}{2} \cdot a}{1 \cdot b} = \frac{a}{2b}.$$

  Since at least one of the two non-X ballots is an A, the probability of success is at least $1/2$.

- ADD: First, a CHECK operation; if successful (i.e., $Y =$ A) then mix the X and Y ballots and choose one of them randomly to be the new X ballot. In this case the odds change as follows: $a : b \to a : 2b \to (a+b) : b$, because, letting X' denote the new X, we have

$$\frac{\mathbb{P}[X' = \mathrm{A}]}{\mathbb{P}[X' = \mathrm{B}]} = \frac{\frac{1}{2} \cdot \mathbb{P}[X = \mathrm{A}] + \frac{1}{2} \cdot \mathbb{P}[Y = \mathrm{A}]}{\frac{1}{2} \cdot \mathbb{P}[X = \mathrm{B}] + \frac{1}{2} \cdot \mathbb{P}[Y = \mathrm{B}]} = \frac{\frac{a}{a+2b} + 1}{\frac{2b}{a+2b} + 0} = \frac{a+b}{b}.$$

- SWAP: First, a CHECK operation; if successful then interchange the X ballot with the third ballot, Z (i.e., the ballot that is neither X nor Y); finally, another CHECK operation (to clarify, this means choosing again, given the *current* X ballot, a random non-X ballot and checking it). If successful (i.e., the two CHECK operations were both successful) then the odds change as follows: $a : b \to a : 2b \to 2b : a \to 2b : 2a \equiv b : a$ (the second $\to$ because given that $Y =$ A the marking of Z is the opposite of that of X).

The procedure starts with X being randomly chosen from an A-ballot and a B-ballot; the starting odds are therefore $1 : 1$. We claim that for any odds

$a : b$ with a and b positive integers (the cases $p = 0$ and $p = 1$ are trivial) there is a finite sequence of ADD and SWAP steps such that, if all steps are successful—otherwise we restart the entire procedure—then the odds of the final X ballot are indeed $a : b$. The probability of success of the procedure is positive (because there are finitely many CHECK operations, and each one succeeds with probability at least 1/2), and so it succeeds eventually (i.e., after finitely many trials) almost surely (i.e., with probability one).

To construct the sequence of steps, take without loss of generality a and b to be relatively prime, and apply the (long) Euclidean algorithm, which substracts the smaller number from the larger number repeatedly, until it gets to 1 (which is the greatest common divisor of a and b). Reversing the algorithm corresponds to a sequence that starts from $1 : 1$ and gets to $a : b$ by applying ADD steps (the inverse of subtraction) and SWAP steps (when we need to invert the odds so that $a < b$).

For example, take $p = 3/10$, i.e., odds $3 : 7$. The Euclidean algorithm gives the sequence $(3, 7) = (7, 3) \to (4, 3) \to (1, 3) = (3, 1) \to (2, 1) \to (1, 1)$, which translates to the following procedure:

START	$1 : 1$
ADD	$1 : 1 \to 2 : 1$
ADD	$2 : 1 \to 3 : 1$
SWAP	$3 : 1 \to 1 : 3$
ADD	$1 : 3 \to 4 : 3$
ADD	$4 : 3 \to 7 : 3$
SWAP	$7 : 3 \to 3 : 7$

.

The final X is the chosen ballot, with odds $3 : 7$ as required.

Remarks. *(a)* We have shown that a p-procedure exists, and have not attempted to minimize its length.

(b) The posterior probabilities after any finite number of operations must be rational numbers, and so to obtain an irrational p would require infinitely many steps.