Sattolo's algorithm

Mark C. Wilson

University of Auckland

INRIA Rocquencourt, 28 June 2004

The algorithm

```
algorithm sattolo
    Input: positive integer n
begin
{initialize to identity permutation}
array a[1..n]
for k from 1 to n do
    a[k] ← k
end for
{now the main part}
for i from n to 2 step -1 do
    {uniformly random element of [i − 1]}
    j ← rand(i − 1)
swap(a, i, j) {exchange a[i] with a[j]}
end for
return a
end
```

Recursive formulation

Starting with integer array $a[1..n]$, call the following.

algorithm `sattolo-rec`

Input: positive integer t

begin

if $t = 1$ **then** break

$j \leftarrow \text{rand}(t-1)$

$\texttt{swap}(a, t, j)$

$\texttt{sattolo-rec}(a,\ t-1)$

return

end

Sample execution

1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
1 5 3 4 2	1 2 3 5 4	5 2 3 4 1
4 5 3 1 2	1 2 5 3 4	4 2 3 5 1
3 5 4 1 2	1 5 2 3 4	3 2 4 5 1
5 3 4 1 2	5 1 2 3 4	2 3 4 5 1

At each stage, green denotes “will not move again”, red denotes “current value of i”, cyan denotes “chosen randomly as j”.

The results in cycle notation are (15234), (15432), (12345).

Notation for permutations

- $\mathcal{S}_n$ permutations of $[n] := \{1, \ldots, n\}$, $\mathcal{S} = \bigcup_n \mathcal{S}_n$.
- $\mathcal{C}_n$ cyclic permutations of $[n]$, $\mathcal{C} = \bigcup_n \mathcal{C}_n$.
- For $\pi \in \mathcal{S}_n$, if π fixes n we let $\pi_\downarrow$ denote the restriction to $[n-1]$, an element of $\mathcal{S}_n$.
- For $\pi \in \mathcal{S}_{n-1}$, let $\pi^\uparrow$ be the extension to an element of $\mathcal{S}_n$ (it must fix n). Note $^\uparrow$ and $_\downarrow$ are inverses.
- For $\pi \in \mathcal{S}$, let $n(\pi)$ denote the value of n above, and let $q(\pi) = \pi^{-1}(n)$.
- Above, $n = 5$, $q = 1, 1, 4$, $\sigma_\downarrow = (1234), (1432), (1234)$.

Proof of correctness

- Claim: in either case a now represents a uniform sample from the set $\mathcal{C}_n$ of cyclic permutations of a.
- For each $\sigma \in \mathcal{C}$, let τ be the transposition swapping $n(\sigma)$ and $q(\sigma)$. Then $\tau\sigma$ fixes n.
- For $n \geq 2$, $\mathcal{C}_n \cong \mathcal{C}_{n-1} \times [n-1]$ via the map $\sigma \mapsto ((\tau\sigma)_{\downarrow}, q(\sigma))$ with inverse $(\sigma, q) \mapsto \tau\sigma^{\uparrow}$.
- Thus the Sattolo measure on $\mathcal{C}_n$ is the product of uniform measures on $[1] \times [2] \times \cdots \times [n-1]$, hence uniform.

Quantities of interest

- Number of swaps is always $n-1$. Others: number of moves by a given element, distance moved by a given element, total distance moved.
- Examples: $j=i$ for each i yields $(n\,n-1\cdots 1)$; $j=1$ for each i yields $(12\ldots n)$. The first maximizes the number of moves of digit n, the second minimizes it.
- Let $\chi(\sigma,p)$ be either number of moves or distance moved by p when σ is the output of the algorithm.

GFs

Introduce generating functions

$$F(u,t,x) = \sum_{\sigma\in\mathcal{C}} \sum_{p\le n(\sigma)} u^{\chi(\sigma,p)} t^p \frac{x^{n(\sigma)}}{(n(\sigma)-1)!}$$

$$= \sum_n x^n \sum_p t^p \phi_{np}(u)$$

where $\phi_{np}(u)$ is the PGF for χ for fixed n, p, with respect to the uniform measure on $\mathcal{C}_n$. Also we need the "diagonal" with $p = n$,

$$G(u,x) = \sum_{\sigma\in\mathcal{C}} \frac{x^{n(\sigma)}}{(n(\sigma)-1)!} u^{\chi(\sigma,n(\sigma))}.$$

Number of moves

- It is convenient to work with $f = F/x, g = G/x$.
- The decomposition of $\mathcal{C}$ yields, via the symbolic method, the equations

$$(1-x)f'(u,t,x) = t^2 g'(u,tx) + s'(u,t,x);$$
$$g'(u,x) = uf(u,1,x);$$
$$s(u,t,x) = \frac{ut}{1-t}[\log(1-tx) - \log(1-x)].$$

- Put $t = 1$, eliminate g', solve for $f'(u,1,x)$, then ge $g'(u,x)$, then $f'(u,t,x)$. All first order linear. Explicit integration of last step seems hard.

Formula - number of moves of given element

$$(1-x)f'(u,t,x) = ut^2\frac{u}{2-u}\frac{1}{(1-tx)^2} + \frac{2(1-u)}{2-u}(1-tx)^{-u} + \frac{ut}{1-t}\left(\frac{1}{1-x} - \frac{t}{1-tx}\right).$$

$$\phi_{np}(u) = \frac{n-p}{n-1}u + \frac{p-1}{n-1}\frac{u^2}{2-u}\left(1 - 2\frac{\Gamma(u+p-2)}{u\Gamma(u-1)\Gamma(p)}\right).$$

Simpler when $p = n$.

Distance moved by a given element

- This time we obtain equations

$$\begin{aligned}(1-x)f'(u,t,x) &= t^2 g'(u,tx) + s'(u,t,x);\\ g'(u,x) &= u^2 f(u,u^{-1},ux);\\ s(u,t,x) &= \frac{ut}{1-t}[\log(1-tx) - \log(1-x)].\end{aligned}$$

- Put $t = u^{-1}$, eliminate g' from second equation, solve for $f'(u,u^{-1},ux)$, then for g', then f'.

Formula - distance moved by an element

$$
\begin{aligned}
&(1-x)f'(u,t,x)\\
&= t^2u^2\left(\frac{u^3}{1-u^2}\frac{\log(1-u^2tx)-\log(1-tx)}{1-utx}+\frac{u}{1-utx}\right)\\
&\qquad +\frac{ut}{u-t}\left(\frac{u}{1-ux}-\frac{t}{1-tx}\right).
\end{aligned}
$$

$$
\begin{aligned}
\phi_{np}(u) &= \frac{u}{n-1}\frac{1-u^{n-p}}{1-u}\\
&\quad + \frac{1-\delta_{p1}}{n-1}\left(u^{p-1}+\frac{u^{p+1}}{1-u^2}\sum_{i=1}^{p-2}\frac{u^{-i}-u^{i}}{i}\right).
\end{aligned}
$$

Probabilistic discussion

- Mean and expectation (Prodinger) for number of moves, distance moved by a given element are readily extracted.
- Mahmoud interprets the limit distribution for number of moves as a mixture of 1 and 1+Geom(1/2), where the mixing probability is the limiting ratio of p/n.
- The distance moved by an element must be scaled by dividing by n: it then converges to a mixture of a uniform and a shifted product of a pair of independent uniforms.

- Total distance moved is the sum

$$D_n = \sum_{i=2}^{n} 2(i - U_i).$$

  where U_i is uniform on $[i-1]$. They are independent and satisfy (for example) the Lindeberg-Feller condition, since each individual variance is $O(n^2)$ and the total variance is $\Theta(n^3)$. Hence the central limit theorem applies.

- It is desirable to prove the Gaussian law directly from the grand PGF.

Recurrences

For number of moves, then distance moved.

$$\chi(\sigma, p) = \begin{cases} \chi(\sigma_\downarrow, p) & \text{if } p \neq n, p \neq q; \\ 1 + \chi(\sigma_\downarrow, q) & \text{if } p = n, p \neq q; \\ 1 & \text{if } p \neq n, p = q; \\ 0 & \text{if } p = n, p = q. \end{cases}$$

$$\chi(\sigma, p) = \begin{cases} \chi(\sigma_\downarrow, p) & \text{if } p \neq n, p \neq q; \\ n - q + \chi(\sigma_\downarrow, q) & \text{if } p = n, p \neq q; \\ n - q & \text{if } p \neq n, p = q; \\ 0 & \text{if } p = n, p = q. \end{cases}$$

Total distance moved

have not yet been able to translate the obvious ecurrence

$$d(\sigma) = d(\sigma_{\downarrow}) + 2(n(\sigma) - q(\sigma))$$

nto useful generating function equations.

Any ideas?

Other questions

- Are there other quantities associated with (cyclic) permutations that can be easily analysed in this way?
- Suppose we generate n randomly and then apply Sattolo's algorithm. What can we say about the distribution of the various quantities?
- Derive asymptotics for various quantities directly from the grand GF.
- Extend to non-uniform generation.