Supplemental Material: A Practical Implementation of the Bernoulli Factory

Anonymous Author 1
Unknown Institution 1

Anonymous Author 2
Unknown Institution 2

Theoretical Justification

Proposition 3 of Nacu and Peres [2005] provides a set of theoretical requirements for a set of factory functions, known as the compatibility equations, under which a Bernoulli Factory exists: (i) the approximation functions are between 0 and 1; (ii) the functions can yield integer counts equal to a count of possible (n, k) bit strings; (iii) the sequences converge to the target function as the number of bits goes to infinity, and (iv) all members of the terminating set $|A_{m_i}|$ have all their possible $2^{m_{i+1}-m_i}$ descendants in $|A_{m_i+1}|$, and similarly for B_{m_i}.

Conditions (i) and (ii) are guaranteed by the design of the method. To prove condition (iii), we show that there exists a sequence of envelopes that converges to the factory function as the number of bits increases. Consider the case of a concave factory function, so that the "difficult" envelopes come from above.

- For any fixed envelope $b^n(p)$ and Bernstein polynomial $b_n^n(p)$, for any $\delta > 0$ there exists some n such that $b^n(p) - b_n^n(p) < \delta$ for all $0 < p < 1$, by the convergence properties of Bernstein polynomials. In the concave case, it is immediate that all $m > n$ also satisfy the condition.
- There exists a point on the descent function that is equidistant from any chosen envelope and the factory function. If the previous envelope's Bernstein expansion is less than this, choose instead the point where the Bernstein expansion and the descent function intersect. Choose a new envelope $k(p)$ that intersects this point, and set the previous n such that $f(p) < k(p) < b_n^n(p) < b^n(p)$ for all $0 < p < 1$. Choose a bit count n_2 such that $f(p) < k_{n_2}(p) < k(p)$ for all $0 < p < 1$.
- With every successive iteration, the envelope sequence covers at least half the distance to the target factory function. Since we explicitly choose the choice of the envelopes to be geometrically compatible with the target function $f(p)$, the fact that each of the envelope parameters converges to the target function's parameters ensures that there must therefore exist a sequence of functions such that $\lim_{k\to\infty} h_{n_k}^{n_k}(p) - f(p) = 0$ for all $p \in [0, 1]$.

The existence of an asymptotically "fast" algorithm for this target function is similarly easy to prove:

- By Nacu and Peres [2005], there exists a series of lower and upper envelopes $(g^n(p), h^n(p))$ for which $Pr(N > n) \leq Ce^{-cn}$ for some (C, c). [1]
- For any Cascade envelope $b^n(p)$, define $b^m(p) = b^n(p)$ for all $m > n$. If there exists an m such that $h^m(p)$ that is less than $b^m(p)$ for all $0 < p < 1$, then there must be some $m' > m$ for all $0 < p < 1$ such that

$$f(p) < h^{m'}(p) < b_{m'}^{m'}(p) < b^{m'}(p)$$

  as $h^{m'}(p) \to f(p)$ and $b_{m'}^{m'}(p) \to b^{m'}(p)$ as $m' \to \infty$.

We show that these conditions are satisfied for the Nacu-Peres upper envelope and the cascade. The cascade has greater slope than the former at $p = 0$ where the curves meet, so that for small values of p the cascade is guaranteed to be greater; for the remainder of the domain, we simply need a value of n at which the chosen upper cascade is greater than the Nacu-Peres upper envelope, which is checked at a finite number of points; the only catch is that the number of input

[1] The upper envelope functions proposed by Nacu and Peres [2005] for the elbow function take the form $h^n(p) = \min(cp, 1-\varepsilon) + C_1\sqrt{\frac{2}{n}}\max\left(p - \left(\frac{1}{2} - 3\varepsilon\right), 0\right) + C_2\exp\left(-2\varepsilon^2 n\right)\max\left(p - \frac{1}{9}, 0\right)$ and are constructed to converge to the target function from above at exponential rates for small p and polynomial rates for other p; C_1 and C_2 are constants required to be large enough so that the function produces valid envelopes. This also requires a very large number of bits for the first acceptable envelope – 2^{16} is often quoted for $c = 2$ and $\varepsilon = 0.2$, which is still overly burdensome for current hardware.

bits required will be extremely large. For the example in the above table, four envelopes were produced with cascading envelopes. To produce a fifth under the Nacu-Peres criteria, a startlingly high value of $n_5 = 2^{37}$ is required for the envelope $h_{n_5}(p)$ to first fits between $f(p)$ and the fourth upper envelope $b^{1223}_{1223}(p)$; from this point on, additional envelopes h_{n_i} can be produced that fit below the previous envelope and the target function by doubling each successive n. With over 100 *billion* bits required, this would not be at all feasible in practice, but as we have already passed the point of feasibility of executing the original factory operation on existing hardware, this is immaterial. We seek only to establish that there is a choice of envelopes for which the method has a "fast" convergence rate.

Condition (iv) applies to the lower envelope automatically, due to the concavity of the target function. Consider the change from n to $n+1$ bits. By definition,

$$|A_{n+1,k+1}| = \lfloor \binom{n+1}{k+1} f\left(\frac{k+1}{n+1}\right) \rfloor,$$

and for its antecedents,

$$|A_{n,k}| = \lfloor \binom{n}{k} f\left(\frac{k}{n}\right) \rfloor;$$

$$|A_{n,k+1}| = \lfloor \binom{n}{k+1} f\left(\frac{k+1}{n}\right) \rfloor.$$

The concavity of $f(x)$ guarantees that for $a < x < b$, $f(x) > pf(a) + (1-p)f(b)$ for all $p \in [0,1]$; downward rounding gives us $\lfloor f(x) \rfloor \geq \lfloor pf(a) + (1-p)f(b) \rfloor \geq \lfloor pf(a) \rfloor + \lfloor (1-p)f(b) \rfloor$. For $p = \frac{\binom{n}{k}}{\binom{n+1}{k+1}}$, Pascal's rule means $1-p = \frac{\binom{n}{k+1}}{\binom{n+1}{k+1}}$, guaranteeing that $|A_{n+1,k+1}| > |A_{n,k}| + |A_{n,k+1}|$.

To show condition (iv) for the upper envelope series, consider an existing envelope $b^m(p)$, its Bernstein expansion $b^m_m(p)$, and its identical polynomial augmentation $(p+(1-p))^{l-m} b^m_m(p)$. We identify a piecewise linear function $g^l(p)$ whose Bernstein expansion of degree l is identical to the $l-m$-polynomial augmentation; it is sufficient to define g on a set of points and complete the rest of the function as being piecewise linear. The function is defined explicitly as the combination of terms from the expansion,

$$\binom{l}{k} g_l\left(\frac{k}{l}\right) = \sum_{i=0}^{l-m} \binom{l-m}{i} \binom{n}{k-i} f\left(\frac{k-i}{n}\right).$$

From this definition it is clear that on the relevant set of points, $g^l(p)$ is concave, as the sum of a series of terms that are concave on the same domain. $g^l(p)$ must then yield a Bernstein expansion that is less than or equal to itself on the domain $[0,1]$, so it must be that $g^l(p) \geq b^m_m(p)$.

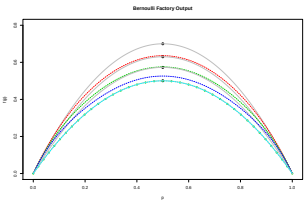

Figure 1: An envelope cascade for the factory function $f(p) = c(1 - 4(p-0.5)^2)$ for $c = 0.5$; the target function is the thick green dotted line, while thinner dashed lines are the envelopes (top only shown). The cascade is formed starting with $c_1 = 0.75$, with each successive c_i set where the previous Bernstein expansion intersected the line $x = 0.5$. The convexity argument for the piecewise linear case does not apply here, meaning that the envelope condition must be checked manually.

Now, the method chooses the next envelope $b^l(p)$ to be less than or equal to the previous Bernstein expansion. Since $g^l(p) \geq b^m_m(p) > b^l(p)$, we also have $1 - g^l(p) \leq 1 - b^l(p)$, so that it is immediate that all terms in the former's Bernstein expansion will be nested in the latter, and hence that the cardinality rule is respected; B_l may then include all strings in B_m appended with all combinations of zeroes and ones, plus whatever new additions may be added at this step.

Parabolic Factory Function

Consider a parabolic factory function

$$f(p) = c\left(1 - 4\left(p - 0.5\right)^2\right), 0 < c < 1$$

which is concave and bounded on the interval $(0,1)$. Because of this concavity, the only supplemental envelopes that are required are above the function.

Figure 1 demonstrates an envelope scheme for the parabolic target in which the envelopes are formed by taking values of c_i that approach the target c from above, by setting the next c_i to be where the previous Bernstein expansion crosses the line $x = 0.5$. Manual checking of each set size, with a finite number of elements, guarantees that the envelope condition is satisfied. Because we do not have a piecewise linear target function, we cannot easily determine whether or not the upper envelope's Bernstein approximation is greater than or equal to the target function across the entire interval $[0,1]$ and must check the condition manually.

References

Nacu, S. and Peres, Y. (2005). Fast Simulation of New Coins from Old. *Annals of Applied Probability*, **15** 93–115.