Count-Wheels

Steven H. Weintraub*

Louisiana State University
Baton Rouge LA 70803-4918

Abstract. We define a sequence of positive integers $A = (a_1, \ldots, a_n)$ to be a count-wheel of length n and weight $w = a_1 + \cdots + a_n$ if it has the following property: Let $\overline{A}$ be the infinite sequence $(\overline{a}_i) = (a_1, \ldots a_n, a_1, \ldots, a_n, \ldots)$. Then there is a sequence $0 = i(0) < i(1) < i(2) < \ldots$ such that for every positive integer k, $\overline{a}_{i(k-1)+1} + \cdots + \overline{a}_{i(k)} = k$. There are obvious notions of when a count-wheel is reduced or primitive. We show that for every positive integer w, there is a unique reduced count-wheel of weight w, denoted $[w]$. Also, $[w]$ is primitive if and only if w is odd. Further, we give several algorithms for constructing $[w]$, and a formula for its length. (Remark: The count-wheel $[15] = (1,2,3,4,3,2)$ was discovered by medieval clock-makers.)

Apparently because of the difficulty of cutting notched and toothed wheels precisely enough, clock-makers in the 14th through 16th centuries used the following method to have their clocks strike the hours: They used a count-wheel with 6 positions on it, causing the hour to be struck the following number of times: $1,2,3,4,3,2$. Beginning the day positioned at the number 1, the wheel could strike the hours as follows: $1,2,3,4,3+2,1+2+3,4+3,2+1+2+3,\ldots$. At that time it was common to strike the hours $1,2,\ldots,24$, for a total of 300 strikes, so in a day this wheel would have made 20 complete revolutions, and hence at the end of the day the wheel was properly positioned for the next day, ad infinitum[1]. In fact, such a count-wheel can not only count the integers from 1 through 24, but can count all positive integers. This raises some interesting mathematical questions. First we make the notion of a count-wheel precise.

Definition 1. *A sequence $A = (a_1, \ldots, a_n)$ of positive integers is a count-wheel of length n and weight $w = a_1 + \cdots + a_n$ if it has the following property: Let $\overline{A}$ be the infinite sequence $(\overline{a}_i)_{i=1,\ldots} = (a_1, \ldots, a_n, a_1, \ldots, a_n, \ldots)$. Then there exists a sequence $0 = i(0) < i(1) < i(2) < \ldots$ such that for every positive integer k,*

$$\sum_{i=i(k-1)+1}^{i(k)} \overline{a}_i = k \qquad (*)$$

Thus $(1,2,3,4,3,2)$ is a count-wheel of length 6 and weight 15. Given this, we see that $(1,2,3,2,2,3,2)$ is also a count-wheel of weight 15, and indeed for any w there is a count-wheel of weight w, namely $(1,1,1,\ldots,1)$. Hence, instead of simply looking for count-wheels, we should look for reduced count-wheels, where reduced is defined as follows:

* Partially supported by the National Science Foundation

[1] This information is taken from an exhibit in the clock room of the British Museum.

Definition 2. *A count-wheel* $B = (b_1, \ldots, b_m)$ *is an amalgam of a count-wheel* $A = (a_1, \ldots, a_n)$ *if* $B \neq A$ *and for some* $j(2), j(3), \ldots$

$$b_1 = a_1 = 1$$
$$b_2 = a_2 + \cdots + a_{j(2)}$$
$$b_3 = a_{j(2)+1} + \cdots + a_{j(3)}$$
$$b_m = a_{j(m-1)+1} + \cdots + a_{j(m)}$$

A count-wheel A is called reduced if it has no amalgams.

Our first result is:

Theorem 3. *For every positive integer* w*, there is a unique reduced count-wheel of weight* w*, denoted* $[w]$*. Also,* $[w]$ *is an amalgam of any other count-wheel of weight* w*.*

If $A = (a_1, \ldots, a_m)$ and $B = (b_1, \ldots, b_n)$ are sequences, we define their sum $A + B$ to be the sequence $(a_1, \ldots a_m, b_1, \ldots, b_n)$ and we let tA be the sequence $A + \cdots + A$ (t summands). If A and B are count-wheels, there is no reason to expect that $A + B$ will be one, and usually it is not. Of course, if A is a count-wheel, so is tA for any t, but if A is reduced tA need not be. What we are really looking for are primitive count-wheels, where primitive is defined as follows:

Definition 4. *A count-wheel A is primitive if the equation* $A = tB$ *only has the solution* $t = 1, B = A$.

Our second result is:

Theorem 5.

(a) *The reduced count-wheel* $[w]$ *is primitive if* w *is odd.*
(b) *If* $w = 2^t v, t > 0$, *then* $[w] = 2^t[v]$.

(From part (b) we see that we in fact have if and only if in part (a), and that if $w = 2^t$ the only count-wheel of weight w is $(1, 1, 1, \ldots, 1)$.)

We now proceed to the proofs of these results.

We adopt the convention here that the residue classes mod w are $1, \ldots, w$ (rather than the usual $0, \ldots, w - 1$).

Proposition 6. *The following algorithm produces a reduced count-wheel of weight* w*:*

Index the positions on a wheel $1, \ldots, w$ *clockwise and place a* 1 *in each position. Begin with a pointer between positions* w *and* 1.

Step 1: For $k = 1, \ldots, w - 1$ *for* w *odd and for* $k = 1, \ldots, 2w - 1$ *for* w *even, successively rotate the pointer* k *positions clockwise and place a bar at the point where the pointer stops, if there is not one there already.*

Step 2: Begin with the empty sequence and the pointer positioned between positions w and 1. Rotate the pointer clockwise until a bar is reached, and let the next term of the sequence be the number of 1's the pointer has passed in doing so. Do this until the pointer has returned to its original position.

Proof: We first show that the resulting sequence A is a count-wheel, and then that it is reduced. Set $x = w - 1$ for w odd and $x = 2w - 1$ for w even.

Clearly A satisfies $(*)$ for $k = 1, \ldots, x$. We must show it satisfies $(*)$ for all positive integers. Note that at the end of step 1 the pointer has returned to its original position as $x(x+1)/2$ is divisible by w.

Observe that step 1 would yield identical results (i.e., bars in the same places) if instead of k we used any $k' \equiv k \pmod{w}$, as rotating k' positions would be rotating through k positions followed by $(k' - k)/w$ complete revolutions.

Now performing the procedure of step 1 for $k = x + 1$ simply rotates the wheel through 1 or 2 complete revolutions, so does nothing, and then by the above observation doing it for $k = (x+1)+1, (x+1)+2, (x+1)+3, \ldots$ yields no new bars, so A satisfies $(*)$ for all positive integers and so is a count-wheel.

Let us refer to the procedure of step 2 as decoding, and its inverse as encoding.

Note that if any bar were removed before decoding, the resulting sequence would not be a count-wheel. We may view the procedure of amalgamation as beginning with a count-wheel A, encoding it, removing one or more bars, and decoding the result to obtain a new sequence B. Since such a B cannot be a count-wheel, A is reduced.

Proof of Theorem 3: Denote the reduced count-wheel constructed in Proposition 6 by $[w]$. Encode it. Then, as observed above, any count-wheel A, when encoded, must have bars in the same places as $[w]$, and perhaps others as well. If there are no others, then $A = [w]$, while if there are others they may be removed and the result decoded, yielding an amalgamation from A to $[w]$.

We now give an alternate algorithm for producing $[w]$ which will also lead to an improvement in the algorithm of Proposition 6.

Proposition 7. *The following algorithm produces a reduced count-wheel of weight w:*

Let $E = \{k(k+1)/2 \text{ reduced } \bmod w | k = 0, \ldots, v\}$ where $v = (w-1)/2$ for w odd and $2w - 2$ for w even.

Arrange the elements of E in ascending order:

$$1 = e_1 < e_2 < \cdots < e_n = w.$$

If $a_1 = e_1$, $a_i = e_i - e_{i-1}$, $i = 2, \ldots, n$, then $A = (a_1, \ldots, a_n)$ is a reduced count-wheel of weight w.

Proof: By comparison with Proposition 6, we see that the following three statements are equivalent:

(a) for $1 \leq e \leq w, e \in E$.

(b) $k(k+1)/2 \equiv e \pmod{w}$ for some k.

(c) Step 1 of the algorithm of Proposition 6 puts a bar following position e.

Note also that the second part of the algorithm of Proposition 7 is just another description of decoding.

Thus the only difference between the results of these two algorithms arises from the fact that the ranges of k differ. For w even, we note that taking $k = 0$ here produces a bar at position w, as did taking $k = 2w - 1$ there. For w odd, we note that $k(k+1)/2 \equiv ((w-1)-k)((w-1)-k+1)/2 \pmod{w}$, so again $k = 0$ here gives the same position w as $k = w - 1$ there, and taking $k = (w+1)/2, \ldots, w-2$ just repeats the values of $e \in E$ obtained from $k = 1, \ldots, (w-1)/2$, so is superfluous.

Corollary 8. *For w odd, the algorithm of Proposition 6 remains valid if it is modified as follows:*

At the beginning of step 1 put a bar at the current pointer location (i.e., between positions w and 1) and perform the construction of step 1 for $k = 1, \ldots, (w-1)/2$.

Lemma 9. *Let A be a reduced count-wheel. Then $2A$ is also reduced, but kA is not reduced for any odd $k > 1$.*

Proof: Let A have weight v.

If the encoding of A has bars following positions $e_1, \ldots, e_n$, then the encoding of $2A$ has bars following positions $e_1, \ldots, e_n, e_{n+1}, \ldots, e_{2n}$ with $e_{n+i} = v + e_i$, $i = 1, \ldots, n$. In view of Proposition 7, to show $2A$ is reduced we must find integers $k_1, \ldots, k_{2n}$ with $k_i(k_i+1)/2 \equiv e_i \pmod{2v}$. Now again by Proposition 7, as A is reduced, there are integers j_i with $j_i(j_i+1)/2 \equiv e_i \pmod{v}$, i.e., with $j_i(j_i+1) \equiv \epsilon_i v + e_i \pmod{2v}$, with $\epsilon_i = 0$ or 1. Since, for any j, $(2v-j-1)(2v-j)/2 \equiv v + j(j+1)/2 \pmod{2v}$, we may take $\{k_i, k_{n+i}\} = \{j_i, 2v - j_i - 1\}$.

Now suppose that $t > 1$ is odd. By the same logic, to show that tA is not reduced it suffices to find integers e and s such that $k(k+1)/2 \equiv e \pmod{tv}$ has a solution but $k(k+1)/2 \equiv e + sv \pmod{tv}$ does not. To this end, let p be an odd prime factor of t, p^a the highest power of p dividing t and p^b the highest power of p dividing v. Set

$$e = \frac{(p^{2(a+b)} - 1)}{8} = \left(\frac{p^{a+b} - 1}{2}\right)\left(\frac{p^{a+b} - 1}{2} + 1\right)/2.$$

Then $k(k+1)/2 \equiv e + sv \pmod{tv}$ yields the congruence

$$(2k+1)^2 \equiv p^{2(a+b)} + 8sv \pmod{tv}$$

which reduced mod p^{a+b} is the congruence

$$(2k+1)^2 \equiv (8v'p^b)s \pmod{p^{a+b}}$$

where $v' = v/p^b$ is prime to p, and if s is chosen so that $8v's$ is not a square mod p, this congruence will have no solution.

Proof of Theorem 5: Let w be odd. Suppose $[w] = t[v]$. Then $w = tv$, so t is odd. But then $[w]$ is reduced, by assumption, so $t[v]$ must be reduced, so $t = 1$ and $[w]$ is primitive. Now let w be even, $w = 2w'$. Then $2[w']$ is a reduced count-wheel of weight of w, so by uniqueness $[w] = 2[w']$. The theorem then follows.

We now give a method of constructing new count-wheels from old. For any two sequences A and B of the same weight, it is clear that their longest common amalgam (lca) should be: the longest sequence C which is an amalgam of both A and B. For two sequences A and B of weights v and w respectively, we define their product AB to be the sequence $C = lca(wA, vB)$.

Proposition 10. *If v and w are relatively prime,*

$$[v][w] = [vw].$$

Proof: Let $A = w[v] = (a_1, \ldots, a_n)$ and $B = v[w] = (b_1, \ldots, b_m)$. It is clear that their lca, of length r, say, is formed as follows: Take all pairs (n_i, m_i), $i = 1, \ldots, r$, with $a_1 + \cdots + a_{n_i} = b_1 + \cdots + b_{m_i}$, and let C be the amalgam $(a_1, a_2 + \cdots + a_{n_2}, a_{n_2+1} + \cdots + a_{n_3}, \ldots) = (b_1, b_2 + \cdots + b_{m_2}, b_{m_2+1} + \cdots + b_{m_3}, \ldots) = (c_1, \ldots, c_r)$. (Of course, $a_1 = b_1 = 1$, so $m_1 = n_1 = 1$.)

Now, as in Proposition 7, we see that the c_i are precisely the integers, reduced mod vw, such that the equations $k(k+1) \equiv c_1 + \cdots + c_i \pmod{v}$ and $\pmod{w}$ both have a solution. But these two congruences are equivalent to the congruence

$$k(k+1)/2 \equiv c_1 + \cdots + c_i \pmod{vw},$$

as we are assuming v and w relatively prime, and by the same logic we see that $C = (c_1, \ldots, c_r) = [vw]$, as claimed.

We present one more algorithm for finding $[w]$, for w odd.

Proposition 11. *Let z be an integer with $8z \equiv -1 \pmod{w}$. Then the set E of Proposition 7 is given by*

$$E = \{2j + z \pmod{w} \mid j = 0 \text{ or } j \text{ a quadratic residue } \bmod w\}.$$

Proof: Immediate from the equation

$$k(k+1)/2 = 2((2k+1)/4)^2 - 1/8.$$

We now dispose of the question of the length of reduced count-wheels. We let $\lambda(w)$ denote the length of $[w]$.

Proposition 12.

(a) $\lambda(2^t) = 2^t$ *for all* $t \geq 0$.

(b) *If* w *is odd,* $\lambda(w) \leq (w+1)/2$, *with equality if and only if* w *is prime.*

(c) *If* v *and* w *are relatively prime,* $\lambda(vw) = \lambda(v)\lambda(w)$.

(d) *For an odd prime* p, *and any* $t \geq 1$,

$$\lambda(p^{2t-1}) = \frac{p^{2t}-1}{2(p+1)} + 1,$$

$$\lambda(p^{2t}) = \frac{p(p^{2t}-1)}{2(p+1)} + 1.$$

Proof: As $[2^t v] = 2^t[v]$ and $[1] = (1)$, a) is obvious and c) is true if $\lambda(vw) = \lambda(v)\lambda(w)$ when v and w are both odd and relatively prime.

From Proposition 7 we see that $\lambda(w) \leq (w+1)/2$ for w odd, with equality if $j(j+1)/2 \equiv k(k+1)/2 \pmod{w}$ has no solution for $0 \leq j < k \leq (w-1)/2$, and it is easy to check this holds exactly when w is prime. Indeed, by Proposition 7 we see that $\lambda(w) = \#\{e \mid 1 \leq e \leq w \text{ and } k(k+1)/2 \equiv e \pmod{w} \text{ for some } k\}$ and so by the Chinese remainder theorem, $\lambda(vw) = \lambda(v)\lambda(w)$ if v and w are relatively prime.

Finally, we see that for w odd, $\lambda(w) = 1 + q(w)$, where $q(w)$ is the number of non-zero quadratic residues mod w. Then $q(1) = 0$, $q(p) = (p-1)/2$, and for $s \geq 2$, $q(p^s) = \varphi(p^s)/2 + q(p^{s-2})$ with φ Euler's function, $\varphi(p^s) = (p^{s-1})(p-1)$. (The term $\varphi(p^s)/2$ counts those quadratic residues prime to p, and the term $q(p^{s-2})$ counts those divisible by p and hence by p^2.) The proposition follows.

From Theorem 5 and Proposition 10 we see that it is only necessary to apply the algorithm of Corollary 8 to calculate $[w]$ for w an odd prime power. For the edification of the reader, we give the values of $[w]$ for various w below. To explain our notation, given that $[5] = (1,2,2)$, and that $[25] = (1,2,2,1,4,1,4,1,4,1,4)$, we shall write $[25] = ([5],4(1,4))$. We then have

$[3] = (1,2)$
$[5] = (1,2,2)$
$[7] = (1,2,3,1)$
$[9] = ([3],2(3))$
$[11] = (1,2,1,2,4,1)$
$[13] = (1,1,1,3,2,2,3)$
$[15] = (1,2,3,4,3,2)$
$[17] = (1,1,1,1,2,4,1,4,2)$
$[19] = (1,1,1,3,1,2,1,5,2,2)$
$[21] = (1,2,3,1,3,3,2,6)$
$[23] = (1,2,2,1,3,1,3,2,5,1,1,1)$
$[25] = ([5],4(1,4))$
$[27] = (2[9],3(3))$
$[45] = (1,2,3,4,5,3,3,7,2,3,3,9)$
$[49] = ([7],6(1,2,4))$
$[81] = ([27],2([9],6(3)))$
$[121] = (1,2,3,4,1,[11],9(1,2,3,4,1))$
$[125] = ([25],2([25],5(1,4)))$

Remark 13. Clearly a count-wheel $[w]$ must begin either $(1,2,\ldots)$ or $(1,1,1,\cdots)$. It is easy to check that the second case occurs if and only if 17 is a square mod v, where v is defined by $w = 2^t v$, v odd. It is also easy to check that the number of times 1 appears in $[w]$ is equal to $2^t m$, where

$$m = \#\{j | 0 < j \leq v \text{ and } j \text{ and } j+8 \text{ are both squares } \pmod{v}\}.$$

Remark 14. If $[w] = (a_1, \ldots, a_n)$, define the height $h(w) = \max\{a_1, \ldots, a_n\}$. Clearly we may keep $h(w)$ small, as $h(2^t) = 1$. Also, we may make $h(w)$ large, for if w is the product of k distinct primes, $\lambda(w)/w$ is approximately $1/2^k$, so $h(w)$ is at least approximately 2^k. Since for any w the set E of Proposition 7 contains all the triangular numbers less than or equal to w, we readily obtain the bound $h(w) < \sqrt{2w}$. Numerical evidence seems to indicate that as w ranges over primes, $h(w)$ grows more slowly than this bound.

Remark 15. Let f be any function from the positive integers to the positive integers. Then we may define a count-wheel for the function f by Definition 1 with equation $(*)$ replaced by

$$\sum_{i=1(k-1)+1}^{i(k)} \overline{a}_i = f(k).$$

(Thus our count-wheels above are count-wheels for the function $f(k) = k$.) It is easy to check that Theorem 3 holds in this more general case, giving a unique reduced count-wheel $[w]_f$. If we let $\lambda_f(w)$ be the length of $[w]_f$ then by an argument analogous to that in the case of $\lambda(w)$ (cf Proposition 7) it is easy to see that

$$\lambda_f(w) = \{j | 0 < j \leq w \text{ and } F(k) \equiv j \pmod{w} \text{ for some } k \geq 0\}$$

where $F(k)$ is defined by $F(0) = 0$ and $F(k) = \Sigma_{i=1}^{k} f(i)$ for $k > 0$.