and

$$\begin{aligned} \text{perm } A(4;1) &= \text{perm} \begin{bmatrix} 1 & -1 & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ &= 1 \cdot \frac{1}{2} \cdot 1 - 1 \cdot \frac{1}{2} \cdot 1 \\ &= 0 \,. \end{aligned}$$

The full adjacency matrix B with submatrices A corresponding to these four-node widgets counts 1 for each good cycle cover in H and 0 for each bad cycle cover, thus its permanent is equal to $(k!)^2$ times the number of vertex covers in G.

We have argued that computing the permanent of a matrix containing elements in $\{-1, 0, \frac{1}{2}, 1\}$ is $\#P$-hard, but there is still a ways to go. The next step is to note that

$$\text{perm } 2B = 2^n \cdot \text{perm } B \,,$$

and this implies that computing the permanent of a matrix with elements in $\{-2, 0, 1, 2\}$ is hard for $\#P$. We now show that this problem reduces to computing the permanents of polynomially many matrices over $\{0, 1\}$. The reduction we use here is somewhat weaker than the one we have been using in that it will require several instances of the $\{0, 1\}$ permanent problem to encode a given instance of the $\{-2, 0, 1, 2\}$ permanent problem, but the reduction still has the property that any fast algorithm for the $\{0, 1\}$ problem would give a fast algorithm for the $\{-2, 0, 1, 2\}$ problem.

Let B be an $n \times n$ matrix over $\{-2, 0, 1, 2\}$. A bound on the absolute value of perm B is given by the case in which each entry of B is 2; then

$$|\text{perm } B| \leq 2^n n! \,.$$

It thus suffices to compute perm B modulo any $N > 2^{n+1}n!$, and from this we will be able to recover the value of perm B.

Let $p_1, p_2, \ldots, p_k$ be the first k primes, where k is the least number such that

$$N = \prod_{i=1}^{k} p_i > 2^{n+1} n! \,.$$

It is not hard to show that $k \leq n + 1$. Moreover, since p_m is $\Theta(m \log m)$ (see [49, p. 10]), we can generate the first k primes in polynomial time using the sieve of Eratosthenes. Before proceeding further, we need the following theorem.

Theorem 27.2 (Chinese Remainder Theorem) *Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime positive integers, and let $m = \prod_{i=1}^{k} m_i$. Let $\mathcal{Z}_n$*

denote the ring of integers modulo n. The ring $\mathcal{Z}_m$ *and the direct product of rings*

$$\mathcal{Z}_{m_1} \times \mathcal{Z}_{m_2} \times \cdots \times \mathcal{Z}_{m_k}$$

are isomorphic under the function

$$f : \mathcal{Z}_m \rightarrow \mathcal{Z}_{m_1} \times \mathcal{Z}_{m_2} \times \cdots \times \mathcal{Z}_{m_k}$$

given by

$$f(x) = (x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_k) .$$

This just says that the numbers mod m and the k-tuples of numbers mod m_i, $1 \leq i \leq k$, are in one-to-one correspondence, and that arithmetic is preserved under the map f. For example, in the following table, we have compared $\mathcal{Z}_{15}$ to $\mathcal{Z}_3 \times \mathcal{Z}_5$.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x mod 3	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
x mod 5	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4

Note that each pair in $\mathcal{Z}_3 \times \mathcal{Z}_5$ occurs exactly once. This is because 3 and 5 are relatively prime. Arithmetic is preserved as well: for example, 4 and 7 correspond to the pairs $(1,4)$ and $(1,2)$, respectively; multiplying these pairwise gives the pair $(1,3)$ (mod 3 and 5, respectively), which occurs under 13; and $4 \times 7 = 28 = 13 \pmod{15}$.

Also, f and f^{-1} are computable in polynomial time. To compute $f(x)$, we just reduce x modulo $m_1, \ldots, m_k$. To compute $f^{-1}(x_1, \ldots, x_k)$, we first compute, for each $1 \leq i \leq k$, integers s and t such that

$$sm_i + t \prod_{\substack{1 \leq j \leq k \\ j \neq i}} m_j = 1$$

and take

$$u_i = t \prod_{\substack{1 \leq j \leq k \\ j \neq i}} m_j .$$

The numbers s and t are available as a byproduct of the Euclidean algorithm. For each $1 \leq i, j \leq k$, $u_i \equiv 1 \bmod m_i$ and $u_i \equiv 0 \bmod m_j$, $i \neq j$. Take

$$f^{-1}(x_1, \ldots, x_k) = x_1 u_1 + \cdots + x_k u_k \bmod m .$$

For further details and a proof of the Chinese Remainder Theorem see [3, pp. 289ff.].