Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Concentration independent random number generation in tile self-assembly [☆]

Cameron T. Chalk [1], Bin Fu [2], Eric Martinez [1], Robert Schweller [*,1], Tim Wylie [*,1]

Department of Computer Science, The University of Texas – Rio Grande Valley, Edinburg, TX, 78539-2999, United States

ARTICLE INFO

Article history:
Received 2 February 2016
Received in revised form 20 November 2016
Accepted 19 December 2016
Available online xxxx
Communicated by S.P. Fekete

Keywords:
Tile self-assembly
aTAM
DNA computing
Biocomputing
Randomization

ABSTRACT

In this paper we introduce the *robust random number generation* problem where the goal is to design an abstract tile assembly system (aTAM system) whose terminal assemblies can be split into n partitions such that a resulting assembly of the system lies within each partition with probability $1/n$, regardless of the relative concentration assignment of the tile types in the system. First, we show this is possible for $n = 2$ (a *robust fair coin flip*) within the aTAM, and that such systems guarantee a worst case $\mathcal{O}(1)$ space usage. We accompany our primary construction with variants that show trade-offs in space complexity, initial seed size, temperature, tile complexity, bias, and extensibility, and also prove some negative results. As an application, we combine our coin-flip system with a result of Chandran, Gopalkrishnan, and Reif to show that for any positive integer n, there exists a $\mathcal{O}(\log n)$ tile system that assembles a constant-width linear assembly of expected length n for any concentration assignment. We then extend our robust fair coin flip result to solve the problem of robust random number generation in the aTAM for all n. Two variants of robust random bit generation solutions are presented: an unbounded space solution and a bounded space solution which incurs a small bias. Further, we consider the harder scenario where tile concentrations change arbitrarily at each assembly step and show that while this is not possible in the aTAM, the problem can be solved by exotic tile assembly models from the literature.

1. Introduction

Self-assembly is the process by which local interactivity among unorganized, autonomous units results in their amalgamation into more complex compounds. One of the premiere models for studying the theoretical possibilities of self-assembly is the *abstract tile assembly model* (aTAM) [2] in which system monomers are 4-sided tiles (inspired by Wang tiles [3]) that attach to a growing seed assembly when matching glues present a sufficient bonding strength. The motivation for studying the aTAM stems from the feasibility of a nanoscale DNA implementation [4], along with the universal computational power of the model [5], which permits many features including *algorithmic* self-assembly of general shapes [6], and more [7,8].

[☆] A preliminary version of this work appeared in [1].

[*] Corresponding authors.

E-mail addresses: cameron.chalk01@utrgv.edu (C.T. Chalk), bin.fu@utrgv.edu (B. Fu), eric.m.martinez02@utrgv.edu (E. Martinez), robert.schweller@utrgv.edu (R. Schweller), timothy.wylie@utrgv.edu (T. Wylie).

[1] Research supported in part by National Science Foundation Grants CCF-1117672 and CCF-1555626.

[2] Research supported in part by National Science Foundation Early Career Award 0845376.

http://dx.doi.org/10.1016/j.tcs.2016.12.021
0304-3975/© 2016 Published by Elsevier B.V.

Table 1

τ represents the temperature of the system, $|\sigma|$ is the number of tiles in the seed assembly, $|T|$ is the size of the tile system, and k-ext denotes the extensibility of the system. Given the largest disparity in relative tile concentration between any pair of tile types in the system for a given concentration distribution, p is the larger relative concentration of the two tiles. s is a space constraint, and n is the range of possible values or the length of the linear assembly.

Robust coin flip in the aTAM

Space	Bias	τ	$\lvert\sigma\rvert$	k-ext	Theorem
$\mathcal{O}(1)$	–	1	7	2	1
$\mathcal{O}(1)$	–	1	1	2	3
unbounded	–	2	1	1	10
s	$\leq p^{(s/10)}$	2	1	1	11

Unstable concentrations (Theorem 13)

Model	Space	τ	$\lvert\sigma\rvert$
neg-aTAM	$\mathcal{O}(1)$	1	2
neg-hTAM	$\mathcal{O}(1)$	1	1
polyTAM	$\mathcal{O}(1)$	2	3
GTAM	$\mathcal{O}(1)$	1	2

General random number generation

Space	Bias	τ	$\lvert\sigma\rvert$	k-ext	Theorem
unbounded	–	2	1	2	7
s	$\leq \frac{1}{2^{\Theta(s/\log n)}}$	2	1	2	8

Robust linear assemblies

$\lvert T\rvert$	Width	τ	$\lvert\sigma\rvert$	Theorem
$\mathcal{O}(\log n)$	4	2	1	Theorem 4, Corollary 1
$\mathcal{O}(\log n)$	6	1	1	Theorem 5, Corollary 2

A promising new direction in self-assembly is the consideration of *randomized* self-assembly systems. In randomized self-assembly (a.k.a. nondeterministic self-assembly), assembly growth is dictated by nondeterministic, competing assembly paths yielding a probability distribution on a set of final, terminal assemblies. Through careful design of tile-sets and the relative concentration distributions of these tiles, a number of new functionalities and efficiencies have been achieved that are provably impossible without this nondeterminism. For example, by precisely setting the concentration values of a generic set of tile species, arbitrarily complex strings of bits can be *programmed* into the system to achieve a specific shape with high probability [9,10]. Alternately, if the concentration of the system is assumed to be fixed at a uniform distribution, randomization still provides for efficient expected growth of linear assemblies [11] and low-error computation at temperature-1 [12]. Even in the case where concentrations are unknown, randomized self-assembly can build certain classes of shapes without error in a more efficient manner than without randomization [13].

Motivated by the power of randomized self-assembly, along with the potential for even greater future impact, we focus on the development of the most fundamental randomization primitive: the *robust* generation of a uniform random bit. In particular, we introduce the problem of self-assembling a uniformly random bit within $\mathcal{O}(1)$ space that is guaranteed to work for all possible concentration distributions. We define a tile system to be a *coin flip* system, with respect to some tile concentration distribution, if the terminal assemblies of the system can be partitioned such that each partition has exactly probability 1/2 of assembling one of its terminals. We say a system is a *robust coin flip* system if such a partition exists that guarantees 1/2 probability for all possible tile concentration distributions. Through designing systems that flip a fair coin for all possible (adversarially chosen) concentration distributions, we achieve an intrinsically fair coin-flipping system that is robust to the experimental realities of imprecise quantity measurements. Such fair systems may allow for increased scalability of randomized self-assembly systems in scenarios where exact concentrations of species are either unknown or intractable to predict at successive assembly stages.

Our results. Our primary result is an aTAM construction that constitutes a robust fair coin flip system which completes in a guaranteed $\mathcal{O}(1)$ space even at temperature one. We apply our robust coin-flip construction to the result of Chandran, Gopalkrishnan, and Reif [11] to show that for any positive integer n, there exists a $\mathcal{O}(\log n)$ tile system that assembles a constant width-4 linear assembly of expected length n that works for all concentration assignments. This result is for temperature two; at temperature one it must be a width-6 linear assembly. We accompany this result with a proof that such a concentration independent assembly of width-1 assemblies is not possible with fewer than n tile types. We further accompany our main coin-flip construction with variant constructions that provide trade-offs among standard aTAM metrics such as space, tile complexity, and temperature, as well as new metrics such as coin bias, and the *extensibility* of the system, which is the maximum number of distinct locations a tile can be added to a single producible assembly of the system.

We utilize the coin-flip construction as a fair random bit generator for implementation of some classical random number generation algorithms. We show that 1-extensible systems, while computationally universal, cannot robustly coin-flip in bounded space without incurring a bias, but can robustly coin-flip in bounded expected space. We also consider the more extreme model in which concentrations may change adversarially at each assembly step. We show that the aTAM cannot robustly coin flip in bounded space within this model, but a number of more exotic extensions of the aTAM from the literature are able to robustly coin flip in $\mathcal{O}(1)$ space. We summarize our results in Table 1. The problem of self-assembling random bits has been considered before [14], but their technique, and almost all randomized techniques to date, do not work when arbitrary concentrations are considered. Further, we utilize the self-assembly of uniform random bits to implement algorithms for uniform random number generation for any n, one construction achieving an unbiased generator with unbounded space and the other imposing a space constraint while incurring some bias.

Organization. Due to the many results in the paper, we briefly outline them here. Section 2 gives the definitions of the models and terms used throughout the paper as well as an overview of some related previous work. In Section 3 we cover

Please cite this article in press as: C.T. Chalk et al., Concentration independent random number generation in tile self-assembly, Theoret. Comput. Sci. (2016), http://dx.doi.org/10.1016/j.tcs.2016.12.021