

Real, Tight Frames with Maximal Robustness to Erasures

Markus Püschel¹ and Jelena Kovačević^{2,1}

Departments of ¹ECE and ²BME

Carnegie Mellon University

Pittsburgh, PA

pueschel@ece.cmu.edu, jelenak@cmu.edu

Abstract

Motivated by the use of frames for robust transmission over the Internet, we present a first systematic construction of real tight frames with maximum robustness to erasures. We approach the problem in steps: we first construct maximally robust frames by using polynomial transforms. We then add tightness as additional property with the help of orthogonal polynomials. Finally, we impose the last requirement of equal norm on the frame and construct, to our best knowledge, the first real, tight, equal norm frames that are maximally robust to erasures.

1 Introduction and Motivation

As the field of applications using various linear transforms exploded in the past couple of decades, the focus has been shifting to exploring the use of redundant representations. These redundant representations, termed *frames*, were originally introduced by Duffin and Schaeffer [1], and are the topic of much research both from the mathematical standpoint and that of diverse applications (see [2, 3, 4] and references therein). Simply stated, in finite dimensions, frames are linearly dependent sets which span the space of interest. As such, there is much less restriction posed upon them when compared to bases. This freedom is what allows frames to be robust to noise, quantization, losses, and also allows frames to capture significant signal characteristics. Of course, these improvements do not come for free and the price is usually the increase in the number of bits needed to code the frame coefficients.

Of particular interest are *tight frames* which can be seen as generalizations of orthonormal bases [5]. As such, a fair amount of work has gone in trying to characterize finite-dimensional tight frames. Benedetto and Fickus do the job beautifully for unit-norm tight frames and show that tight frames and orthonormal bases arise as minima of the same minimization problem under different conditions [5]. In [6], the same is done for tight frames with elements having different norms. All tight frames are projections of orthonormal bases

from a larger space, a result attributed to Naimark [7]. This fact motivates constructions we present in this paper.

Tight frames were introduced as a tool to provide robustness to transmission errors in [4]; this will be our application of choice. The problem is to provide robustness to erasures on a network such as the Internet, by expanding the original data in a redundant signal representation—frame. As the frame operation can be modeled as a rectangular matrix operating on the input data, the problem can be mathematically stated as looking for rectangular matrices which are subject to row erasures. In [4], some justification was provided as to why tight frames in particular should be used. Starting from that assumption, we will look for an even more restricted class of frames; those which are maximally robust to erasures, that is, those which can withstand the maximum possible number of losses. This can be restated as looking for $m \times n$ ($m \geq n$) matrices, which remain full rank after deletion of any subset of $m - n$ rows. Previous work in this area is described in [4, 8, 9, 10]. To the best of our knowledge, we present the first systematic construction of a large number of maximally robust frames using concepts from the theory of from polynomial algebras and orthogonal polynomials. Then we use our approach to construct *real* frames, for all choices of m and n , that combine the properties of equal norm, tightness, and maximal robustness to erasures. To the best of our knowledge, to date only one class of *complex* frames with these properties have been found.

We start with a brief overview of finite-dimensional frames in the next section. We then introduce polynomial transforms and show how they naturally lead to maximum robustness. We then add another requirement, that of tightness, and introduce orthogonal polynomials as a vehicle for ensuring tightness. Finally, we complete our task by constructing real, tight frames maximally robust to erasures where all the elements have equal norm.

2 Background on Frames

In this section we provide the necessary background on frames. We consider the finite-dimensional Hilbert spaces \mathbb{R}^n and \mathbb{C}^n endowed with the usual scalar product. We will jointly denote these spaces with \mathcal{H}_n , where n is the dimension.

Definitions. We start with some basic definitions.

Definition 1 (Frame) A frame is a generating system $\{\phi_0, \dots, \phi_{m-1}\}$ of \mathcal{H}_n . Necessarily, $m \geq n$. We represent the frame as an $m \times n$ matrix with rows ϕ_k^T :

$$F = \begin{bmatrix} \phi_0^T \\ \phi_1^T \\ \vdots \\ \phi_{m-1}^T \end{bmatrix}.$$

The definition implies $\text{rank}(F) = n$.

In the following, when we speak of a frame, we always mean the matrix F . Likewise, we define all frame properties in terms of F .

As a convention, all index sets used in this paper (e.g., for matrix entries) start with 0, i.e., are of the form $\{0, \dots, n-1\}$. Further, we denote with A^* the hermitian (transpose-conjugate) of the matrix A , and with I_n the $n \times n$ identity matrix.

Definition 2 (Frame Properties) A frame F is called *tight*, if the columns of F are of equal norm and form an orthogonal set:

$$F^*F = aI_n, \quad a \neq 0.$$

A frame is called *unit-norm tight*, if $a = 1$.

A frame F is called *equal-norm (EN)*, if all rows have equal norm, i.e., if the main diagonal of FF^* is constant.

We call a frame *maximally robust to erasures (MR)*, if every $n \times n$ submatrix (obtained by deleting $m-n$ rows) of F is invertible.

Seeding. In this paper, we construct frames F from suitable invertible matrices M by deleting a suitable set of columns¹. We call this process *seeding*, and call F a *seed* of M . This construction does not impose any restriction, since every frame F can be completed to an invertible matrix M by adding a suitable set of columns. In other words, every frame can be obtained by seeding. If M is an $m \times m$ matrix, and F is constructed by keeping all columns with indices in the set $I \subset \{i_0, \dots, i_{n-1}\}$, then we write

$$F = M[I].$$

As an example, we consider the discrete Fourier transform, defined by

$$\text{DFT}_m = [\omega_m^{k\ell}]_{0 \leq k, \ell < m}, \quad \omega_m = e^{-2\pi i/m}.$$

Its unitary version is given by $\text{DFT}'_m = \frac{1}{\sqrt{m}} \text{DFT}_m$.

The only known class of tight ENMR frames is seeded by the DFT [4].

Lemma 1 Let $n \leq m$. Then

$$F = \text{DFT}_m[0, \dots, n-1], \quad \text{and} \quad F' = \text{DFT}'_m[0, \dots, n-1] \quad (1)$$

is a tight ENMR and unit-norm tight MR frame, respectively.

Proof Tightness and EN is straightforward. We show MR later as a special case of a more general class of MR frames.

In this paper we provide a large class of tight MR frames and also a new class of tight ENMR frames with real entries.

Invariances of Frame Properties. Let a frame F be given satisfying one (or several) of the properties in Definition 2. We ask under what conditions a product AFB is again a frame satisfying the same properties.

Lemma 2 (Invariance of Frame Properties) Let F be a frame. In all matrix products below, we assume the sizes to be compatible.

¹In the orthogonal case, this fact is known as the Naimark Theorem [7].

- (i) AFB is a frame for any invertible matrices A, B .
- (ii) If F is tight (unit-norm tight), then $aUFV$ (UFV) is tight (unit-norm tight) for any unitary matrices U, V and $a \neq 0$.
- (iii) If F is EN, then $aDFU$ is EN for any diagonal unitary matrix D , unitary matrix U , and $a \neq 0$.
- (iv) If F is MR, then $DF A$ is MR for any invertible diagonal matrix D and any invertible matrix A .
- (v) If F is unit-norm tight MR, then DFU is unit-norm tight MR for any unitary diagonal matrix D and any unitary matrix U .

Proof The proof is straightforward from the definition of the properties in each case. We show only (iv). Let F be an $m \times n$ MR frame, D an $m \times m$ invertible diagonal matrix, and A an $n \times n$ invertible matrix. Let M be any $n \times n$ submatrix of $DF A$, then $M = D' M' A$, where D' is a diagonal matrix that contains a suitable subset of the diagonal elements of D , and M' is an $n \times n$ submatrix of F . By assumption, M' is invertible and so is D' and A , which implies that also M is invertible as desired.

3 Polynomial Transforms and MR Frames

In this section we construct a large class of MR frames from so-called polynomial transforms.

Polynomial Algebras and Transforms. We denote with $\mathbb{C}[x]$ the algebra of polynomials with complex coefficients. For a given polynomial $p(x) \in \mathbb{C}[x]$ we denote with $\mathbb{C}[x]/p(x)$ the algebra of polynomials of degree less than $\deg(p)$ with addition and multiplication modulo p ; the dimension of $\mathbb{C}[x]/p(x)$ is $\deg(p)$. We call $\mathbb{C}[x]/p(x)$ a *polynomial algebra*. We call p separable, if p has pairwise distinct zeros $\alpha = (\alpha_0, \dots, \alpha_{m-1})$, where $m = \deg(p)$. Then, by the Chinese remainder theorem (CRT),

$$\mathbb{C}[x]/p(x) \cong \mathbb{C}[x]/(x - \alpha_0) \oplus \dots \oplus \mathbb{C}[x]/(x - \alpha_{m-1}) \quad (2)$$

as algebras. In particular, (2) is an isomorphism of vector spaces and can thus be represented by a matrix. To do so, we choose a basis $b = (p_0, \dots, p_{m-1})$ with the property $\deg(p_\ell) = \ell$ of $\mathbb{C}[x]/p(x)$ and the basis (x^0) in each of the one-dimensional summands $\mathbb{C}[x]/(x - \alpha_k)$. With respect to these bases, (2) is represented by the matrix

$$\mathcal{P}_{b,\alpha} = [p_\ell(\alpha_k)]_{0 \leq k, \ell < m} = \begin{bmatrix} p_0(\alpha_0) & \dots & p_{m-1}(\alpha_0) \\ \vdots & \vdots & \vdots \\ p_0(\alpha_{m-1}) & \dots & p_{m-1}(\alpha_{m-1}) \end{bmatrix},$$

which we call the *polynomial transform* for $\mathbb{C}[x]/p(x)$ with basis b . As a consequence of the CRT, $\mathcal{P}_{b,\alpha}$ is invertible, which we restate in the following lemma.

Lemma 3 Let $\alpha = (\alpha_0, \dots, \alpha_{m-1})$ be a list of pairwise different complex numbers, and set $p(x) = \prod_{0 \leq k < n} (x - \alpha_k)$. Further let $b = (p_0, \dots, p_{m-1})$ be a list of linearly independent polynomials with degree $\deg(p_\ell) = \ell$, $0 \leq \ell < m$. Then $\mathcal{P}_{b,\alpha}$ is a polynomial transform and invertible.

Seeded MR Frames. We now show how polynomial transforms can be used to seed MR frames.

Lemma 4 Let $\mathcal{P}_{b,\alpha}$ be a polynomial transform and let $n \leq m$. Then

$$F = \mathcal{P}_{b,\alpha}[0, \dots, n-1]$$

is an MR frame.

Proof Since $\mathcal{P}_{b,\alpha}$ is invertible, F is a frame. Further, every $n \times n$ submatrix of F is again a polynomial transform, since $\deg(p_\ell) = \ell$ for $p_\ell \in b$, and thus invertible. This implies that F is MR.

Lemma 4 provides a large class of structured MR frames including the frames seeded by the DFT, which thus completes the proof of Lemma 1. The DFT seeded frames were also tight and EN, whereas in general, the frames in Lemma 4 are neither EN, nor tight. EN can simply be achieved by multiplying F from the left by a suitable diagonal matrix D (using Lemma 2, (iv)). The problem is that by doing that, tightness is usually destroyed, a problem which we consider next.

4 Orthogonal Polynomial Transforms and Real Tight MR Frames

In this section we consider a subclass of polynomial transforms that seed real, tight MR frames. It is clear that in order to achieve tightness we have to seed from an orthogonal matrix (a result known as Naimark Theorem [7]), as we mentioned before). The basic idea is to construct polynomial transforms from orthogonal polynomials. These transforms are orthogonal after a suitable scaling, which does not destroy the MR property because of Lemma 2, (iv).

We start with introducing orthogonal polynomials.

Orthogonal Polynomials. Let $I \subset \mathbb{R}$ be an interval, and $w(x)$ a function on I , called weight function. Then $(p_\ell | \ell \geq 0)$, with $\deg(p_\ell) = \ell$, is called a series of orthogonal polynomials on I with respect to $w(x)$, if

$$\int_I p_k(x)p_\ell(x)w(x)dx = \mu_\ell \delta_{k\ell}, \quad \mu_\ell > 0. \quad (3)$$

where δ denotes the Kronecker delta function and the μ_ℓ are constants.

Orthogonal polynomials have many interesting properties and applications. A good overview is provided for example in [11].

In this paper, we will use the following properties of orthogonal polynomials:

Lemma 5 Let $(p_\ell \mid \ell \geq 0)$ be a sequence of orthogonal polynomials. The following properties hold:

1. p_ℓ is separable for any $\ell \geq 0$.
2. p_ℓ and $p_{\ell-1}$ have no common zeros.

The key ingredient to obtaining orthogonal polynomial transforms is the following Christoffel-Darboux formula [11]:

Theorem 1 (Christoffel-Darboux Formula) Let $(p_\ell \mid \ell \geq 0)$ be a sequence of orthogonal polynomials on I with respect to some weight function $w(x)$, and let μ_ℓ be defined as in (3).

Further, we denote with β_ℓ the leading coefficient of p_ℓ , choose an $m \geq 0$, and define $c_m = \beta_{m-1}/(\beta_m \mu_{m-1})$. Then the following equation holds.

$$\sum_{0 \leq \ell < m} \frac{1}{\mu_\ell} p_\ell(x) p_\ell(y) = \begin{cases} c_m \frac{p_{m-1}(y) p_m(x) - p_m(y) p_{m-1}(x)}{x - y}, & x \neq y, \\ c_m (p_{m-1}(x) p'_m(x) - p_m(x) p'_{m-1}(x)), & x = y, \end{cases}$$

where p'_ℓ denotes the derivative of p_ℓ .

Orthogonal Polynomial Transforms. We can now construct orthogonal polynomial transforms, by constructing a polynomial algebra and its basis from orthogonal polynomials. This construction was introduced into signal processing by [12], where it was called Gauss-Jacobi procedure.

Theorem 2 Under the assumptions of Theorem 1, consider $\mathbb{C}[x]/p_m(x)$ with basis $b = (p_0, \dots, p_{m-1})$, and let $\alpha = (\alpha_0, \dots, \alpha_{m-1})$ denote the zeros of p_m , which are necessarily distinct (see Lemma 5, 1). Then, $\mathcal{P}_{b,\alpha}$ is a polynomial transform (by Lemma 3) and

$$\mathcal{P}_{b,\alpha}^{-1} = E \mathcal{P}_{b,\alpha}^T D,$$

with

$$\begin{aligned} D &= c_m^{-1} \text{diag}_{0 \leq k < m} ((p_{m-1}(\alpha_k) p'_m(\alpha_k))^{-1}) \\ E &= \text{diag}_{0 \leq k < m} (\mu_k^{-1}). \end{aligned}$$

In particular, the matrix

$$P'_{b,\alpha} = \sqrt{D} \mathcal{P}_{b,\alpha} \sqrt{E} \tag{4}$$

is orthogonal and will be called the *orthogonal polynomial transform*² for $\mathbb{C}[x]/p_m(x)$ with basis b .

Proof We apply Theorem 1 to the special case of two zeros α_i, α_j of $p_m(x)$ and get

$$\sum_{0 \leq \ell < m} \frac{1}{\mu_\ell} p_\ell(\alpha_i) p_\ell(\alpha_j) = \begin{cases} 0, & i \neq j, \\ c_m p_{m-1}(\alpha_i) p'_m(\alpha_i), & i = j. \end{cases}$$

Then, it can be easily checked that $\mathcal{P}_{b,\alpha}^{-1} \mathcal{P}_{b,\alpha} = I$, as desired. Note that $p_{m-1}(\alpha_i) p'_m(\alpha_i) \neq 0$ because of Lemma 5.

²Note that this definition is a slight abuse of terminology, since an orthogonal polynomial transform is, in general, not a polynomial transform. Scaling from left by a diagonal matrix destroys this property.

Seeded Tight MR Frames. The orthogonal polynomial transform constructed in Theorem 2 can be used to construct real, tight MR frames.

Theorem 3 Let $\mathcal{P}'_{b,\alpha}$ be the orthogonal polynomial transform constructed in Theorem 2, and let $n \leq m$. Then

$$F = \mathcal{P}'_{b,\alpha}[0, \dots, n-1]$$

is a real, tight MR frame.

Theorem 3 provides a large class of real, tight MR frames corresponding to the many different classes of orthogonal polynomials [11]. In particular, the 16 DTTs are orthogonal polynomial transforms [13], and thus their seeded frames have cosine entries. In the general case, the entries of the seeded frames will not be cosines or numbers that can be expressed in a closed form.

The remaining question we address is how, in addition to constructing frames which are tight and are maximally robust to erasures, we make them equal-norm as well. By scaling the rows of a frame constructed with Theorem 3, we can establish EN, but will lose tightness. To achieve all these properties together, in the next section, we use a construction method somewhat different from the ones above.

5 Real, Tight ENMR Frames

In this section, we finally construct real frames that have all the introduced properties, i.e., they are tight ENMR. We start with complex tight ENMR frames seeded by the DFT and then use Lemma 2, (v), to construct real counterparts with the same properties.

We start by extending the class of tight ENMR frames seeded by the DFT as in Lemma 1, by using the first $(n - k)$ and the last k columns of the DFT_m .

Lemma 6 Let $n \leq m$. Then

$$F = \text{DFT}_m[0, \dots, n-k-1, m-k, \dots, m-1]$$

is a tight ENMR frame. The same construction with DFT'_m yields unit-norm tight ENMR frames.

Proof We use that DFT_m diagonalizes the cyclic shift

$$Z_m = \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ 1 & & & 0 \end{bmatrix},$$

namely $\text{DFT}_m Z_m \text{DFT}_m^{-1} = D_m = \text{diag}(1, \omega_m^{-1}, \dots, \omega_m^{-(m-1)})$. This implies

$$\begin{aligned} F &= (\text{DFT}_m Z_m^k)[0, \dots, n-1] \\ &= (D_m^k \text{DFT}_m)[0, \dots, n-1], \end{aligned}$$

which is a tight ENMR frame using Lemma 1 and Lemma 2, (v).

Real Tight Frames for Odd n . If we choose $n = 2k + 1$ in Lemma 6, then the resulting frame F consists of pairs of conjugated column at positions $i, m - i$, for $1 \leq i \leq k$. (The first column of F is real.) The idea is to replace the conjugate pairs by their real and imaginary parts, respectively, to construct real frames. Recall that, if $x, \bar{x} \in \mathbb{C}^m$ are conjugates, then

$$[x \ \bar{x}] \cdot \frac{1}{2} \begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix} = \left[\frac{1}{2}(x + \bar{x}) \quad -\frac{i}{2}(x - \bar{x}) \right] = [\operatorname{Re}(x) \ \operatorname{Im}(x)].$$

With this as a motivation, we define, for odd $n = 2k + 1$,

$$U_n = \begin{bmatrix} 1 & & \\ & \mathbf{I}_k & -i \mathbf{J}_k \\ & \mathbf{J}_k & i \mathbf{I}_k \end{bmatrix}.$$

Here, \mathbf{J}_k is \mathbf{I}_k with the columns in reversed order. Clearly, U_n is unitary.

Theorem 4 Let $0 \leq k < (m - 1)/2$ and $n = 2k + 1$. Then

$$\begin{aligned} F &= \operatorname{DFT}_m[0, \dots, k, m - k, \dots, m - 1]U_n \\ &= \left[[\cos \frac{2j\ell\pi}{n}]_{0 \leq j < m, 0 \leq \ell \leq k} \quad [-\sin \frac{2j\ell\pi}{n}]_{0 \leq j < m, k \geq \ell \geq 1} \right] \end{aligned}$$

is a real, tight ENMR frame, and

$$F' = \frac{1}{\sqrt{n}}F$$

is a real, unit-norm tight ENMR frame. Each row of F' has norm $\sqrt{k + 1}$.

Proof Follows from Lemma 6 and Lemma 2, (v). The actual row norm is obtained using the identity $\cos^2 \alpha + \sin^2 \alpha = 1$.

Real Tight Frames for Even n . Theorem 4 provides real, tight ENMR frames F of sizes $m \times n$ for odd n . To also cover even n , we need to start with another seed matrix. Namely, we consider polynomial transform for $\mathbb{C}[x]/(x^n + 1)$ with basis $b = (1, x, \dots, x^{n-1})$, which is given by

$$\widetilde{\operatorname{DFT}}_m = [\omega_m^{(k+1/2)\ell}]_{0 \leq k, \ell < m} = \operatorname{DFT}_m \operatorname{diag}_{0 \leq \ell < m}(\omega_n^{\ell/2}). \quad (5)$$

It follows that the corresponding orthogonal version is given by $\widetilde{\operatorname{DFT}}_m' = \frac{1}{\sqrt{m}}\widetilde{\operatorname{DFT}}_m$.

The matrix $\widetilde{\operatorname{DFT}}_m$ has no real columns and has conjugate pairs of columns at indices $i, n - i - 1$, $0 \leq i < m$, which allows us to solve the even case. We define, for even $n = 2k$, the unitary matrix

$$V_n = \begin{bmatrix} \mathbf{I}_k & -i \mathbf{J}_k \\ \mathbf{J}_k & i \mathbf{I}_k \end{bmatrix}.$$

Theorem 5 Let $1 \leq k \leq m/2$, and let $n = 2k$. Then

$$\begin{aligned} F &= \widetilde{\text{DFT}}_m[0, \dots, k-1, m-k, \dots, m-1]V_n \\ &= \left[\left[\cos \frac{2(j+1/2)\ell\pi}{n} \right]_{0 \leq j < m, 0 \leq \ell < k} \left[-\sin \frac{2(j+1/2)\ell\pi}{n} \right]_{0 \leq j < m, k \leq \ell \leq 1} \right] \end{aligned}$$

is a real, tight ENMR frame, and

$$F' = \frac{1}{\sqrt{n}}F$$

is a real, unit-norm tight ENMR frame. Each row of F' has norm \sqrt{k} .

Proof Because of (5)

$$\widetilde{\text{DFT}}_m[0, \dots, k-1, m-k, \dots, m-1] = \text{DFT}_m[0, \dots, k-1, m-k, \dots, m-1]D$$

with a suitable diagonal, unitary matrix D . Using Lemma 6 and Lemma 2, (v), we see that $\widetilde{\text{DFT}}_m[0, \dots, k-1, m-k, \dots, m-1]$ is a tight ENMR frame. Since V_n is unitary, the result follows from Lemma 2, (v).

6 Acknowledgement

This work was supported in part by by NSF through award 0310941, and in part by the PA State Tobacco Settlement, Kamlet-Smith Bioinformatics Grant.

References

- [1] R. J. Duffin and A. C. Schaeffer. A class of nonharmonic Fourier series. *Trans. Amer. Math. Soc.*, 72:341–366, 1952.
- [2] O. Christensen. *Introduction to Frames and Riesz Bases*. Birkhäuser, 2002.
- [3] C. Heil and D. Walnut. Continuous and discrete wavelet transforms. *SIAM Rev.*, 31:628–666, 1989.
- [4] V. K Goyal, J. Kovačević, and J. A. Kelner. Quantized frame expansions with erasures. *Journal of Appl. and Comput. Harmonic Analysis*, 10(3):203–233, May 2001.
- [5] J. J. Benedetto and M. Fickus. Finite normalized tight frames. *Advances in Computational Mathematics, special issue on Frames*, 2002.
- [6] P. G. Casazza, M. Fickus, J. Kovačević, M. Leon, and J. Tremain. *Harmonic Analysis and Applications*, chapter A Physical Interpretation for Finite Tight Frames. Birkhäuser, Boston, MA, 2004.
- [7] N. I. Akhiezer and I. M. Glazman. *Theory of Linear Operators in Hilbert Spaces*, volume 1. Frederick Ungar Publisher, 1966.

- [8] P. G. Casazza and J. Kovačević. Equal-norm tight frames with erasures. *Advances in Computational Mathematics, special issue on Frames*, 18:387–430, 2002. Invited paper.
- [9] R. B. Holmes and V. I. Paulsen. Optimal frames for erasures. *Linear Algebra and Its Appl.*, 377:31–51, 2004.
- [10] B. G. Bodmann and V. I. Paulsen. Frames, graphs and erasures. *Linear Algebra and Its Appl.*, 2004. Submitted.
- [11] G. Szegő. *Orthogonal Polynomials*. Amer. Math. Soc. Colloq. Publ., 3rd edition, 1967.
- [12] Y. Yemini and J. Pearl. Asymptotic properties of discrete unitary transforms. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, PAMI-1(4):366–371, 1979.
- [13] M. Püschel and J. M. F. Moura. The algebraic approach to the discrete cosine and sine transforms and their fast algorithms. *SIAM Journal of Computing*, 32(5):1280–1316, 2003.