Constructing $O(n \log n)$ Size Monotone Formulae for the $k$-th Elementary Symmetric Polynomial of $n$ Boolean Variables

J. Friedman
Harvard University
Cambridge, MA 02138

Abstract: In this paper, we construct formulae for the $k$-th elementary symmetry polynomial of $n$ Boolean variables, using only conjunction and disjunction, which for fixed $k$ are of size $O(n \log n)$, with the construction taking time polynomial in $n$. We also prove theorems involving $n \log n$ (polynomial in $k$) upper bounds on such formulae. Our methods involve solving the following combinatorial problem: for fixed $k$ and any $n$ construct a collection of $r=O(\log n)$ functions $f_1,...,f_r$ from $\{1,...,n\}$ to $\{1,...,k\}$ such that any subset of $\{1,...,n\}$ of order $k$ is mapped 1-1 to $\{1,...,k\}$ by at least one $f_i$.

0. INTRODUCTION

For Boolean variables $x_1,...,x_n$ we define the "threshold $k$" function

$$Th_k(x_1,...,x_n)$$

$$= \begin{cases} 1 & \text{if at least } k \text{ of the } x_1,...,x_n \text{ are 1} \\ 0 & \text{otherwise} \end{cases}$$

In [Kr] Krichevskii proved that any monotone Boolean formula, i.e., formula using only conjunction and disjunction, for $Th_2(x_1,...,x_n)$ must be of size (i.e., number of occurrences of variables) $\Omega(n \log n)$, and hence so does $Th_k(x_1,...,x_n)$, $k>2$. In [K] Khasin proves the existence of formulae for $Th_k(x_1,...,x_n)$ of size $O(n \log n)$ for fixed $k$; unfortunately, the proof is not constructive (an exhaustive search for such a formula would take time exponential in $n$). Kleiman and Pippenger, in [K,P], have constructed formulae for $Th_k(x_1,...,x_n)$ of size $O(n \log n)$ for fixed $k$. In this paper, we construct monotone formulae for $Th_k(x_1,...,x_n)$ of size $O(n \log n)$ in time polynomial in $n$ for fixed $k$. In addition, we prove the existence of monotone formulae of size $O(k^{12.6}\log n)$. We also prove constructions for formulae of size $O(k^{k.74}\log n)$ which also use negation.

As a byproduct of our construction, we solve the following combinatorial problem. It is well known that for fixed $k$ and any $n$, there exists a collection of $r=O(\log n)$ functions $f_1,...,f_r$ from $\{1,...,n\}$ to $\{1,...,k\}$, such that any subset of $\{1,...,n\}$ of order $k$ is mapped 1-1 to $\{1,...,k\}$ by at least one $f_i$. Previous proofs are nonconstructive. We give a construction for such a collection of functions.

In Section 1, we give a simple construction for $Th_k(x_1,...,x_n)$ which, for fixed $k$, is of size $O(n \log n)$ and requires polynomial time in $n$. The construction makes use of certain sets, which, to coding theorists, are certain types of error-correcting codes. In Section 2, we explain those more thoroughly, and derive more general results using these codes, including the $O(k^{12.6}\log n)$ existence theorem. The rest of the paper is devoted to quicker constructions of these codes, using well-known coding techniques. Section 3 gives a randomized algorithm for construction, simplified by using linear codes. Section 4 uses the idea of concatenating codes and Reed-Solomon codes, which greatly improve the construction at the cost of lengthening.
the code somewhat. Section 5 uses BCH codes and a Justesen code to give explicit codes; these codes are much longer than those of Sections 3 and 4 (giving threshold function formulae for size $c \cdot n \log n$ for fixed $k$ with a much larger constant $c$).

The $T(h, x_1, \ldots, x_n)$ construction problem was posed to the author by L. G. Valiant; the author would like to thank him, as well as P. Elias and M. O. Rabin, for several helpful conversations and suggestions.

1. THE BASIC CONSTRUCTION

We construct formulae of the form

$$T(h, x_1, \ldots, x_n) = \bigvee_{i=1}^{r} F_i$$

where each $F_i$ is of the form

$$\left( \bigvee_{i \in \Lambda_i^1} x_i \right) \wedge \left( \bigvee_{i \in \Lambda_i^2} x_i \right) \wedge \ldots \wedge \left( \bigvee_{i \in \Lambda_i^k} x_i \right)$$

where $\Lambda_i^1, \ldots, \Lambda_i^k$ are disjoint subsets of $\{1, \ldots, n\}$. We shall call each $\Lambda_i^1, \ldots, \Lambda_i^k$ a partition of $\{1, \ldots, n\}$, though we do not require $\Lambda_i^1 \cup \ldots \cup \Lambda_i^k$ to be all of $\{1, \ldots, n\}$.

The formula (1.1) is valid iff the $r$ partitions have the property that each subset $\{i_1, \ldots, i_k\}$ of $\{1, \ldots, n\}$ is separated by at least one of the partitions, i.e., for some $j$ the sets $\Lambda_i^j, \ldots, \Lambda_k^j$ each contain exactly one element of $\{i_1, \ldots, i_k\}$. Such a collection of partitions will be called an $n, k$ scheme of size $r$. The formula (1.1) has length $\leq r n$. In what follows, we construct $n, k$ schemes of size $O(\log n)$ for fixed $k$.

For $k=2$, and any $m$, we construct a $2^m, 2$ scheme size $m$ as follows. For positive integers $i$ and $j$, let $\text{Bin}_j(i)$ be the $j$-th digit (from the right) of the binary representation of $i$ (i.e., $i = \text{Bin}_1(i) + 2 \cdot \text{Bin}_2(i) + 4 \cdot \text{Bin}_3(i) + \ldots$). For $j=1, \ldots, m$, we define the partition of $\{1, \ldots, 2^m\}$

$$\Lambda_0^j = \{i: \text{Bin}_j(i) = 0, \quad 1 \leq i \leq 2^m\}$$

$$\Lambda_1^j = \{i: \text{Bin}_j(i) = 1, \quad 1 \leq i \leq 2^m\}$$

Since any two distinct integers of $\{1, \ldots, 2^m\}$ differ at the $j$-th digit of their binary representations for some $j$, $1 \leq j \leq m$, the above collection of partitions separates $\{1, \ldots, 2^m\}$. Thus, they define a $2^m, 2$ scheme of size $m$.

This method does not directly generalize to $k > 2$. For example, one might try to use base 3 representations to construct $3^m, 3$ schemes for size $m$. Unfortunately, there are triples such as $(222, 122, 221)$ of distinct base 3 integers with no digit on which they all differ. Our idea is to consider, for some base $b$, a subset $S$ of $\{1, \ldots, b^m\}$ such that any two distinct elements of $S$, expressed in base $b$, differ on more than $2/3$ of their (first) $m$ digits. For such $S$, any triple $(x, y, z)$ of distinct elements of $S$ all differ on at least one of the first $m$ digits, because each of the three pairs $(x, y), (y, z)$, and $(x, z)$ coincide on less than $1/3$ of these digits. Partitioning by digits as before we get a $|S|, 3$ scheme of size linear in $m$ (where $|S|$ denotes the cardinality of $S$). If $b$ is chosen large enough, we find an $S$ of size exponential in $m$.

On $\{1, \ldots, b\}^m$, the set of $m$-tuples of integers from 1 to $b$, we define the "Hamming distance,"

$$\rho((x_1, \ldots, x_m), (y_1, \ldots, y_m)) = \left| \{i: x_i \neq y_i\} \right|$$

For $x \in \{1, \ldots, b\}^m$ we define the ball of radius $r$ about $x$,

$$B_r(x) \equiv \{y: \rho(x, y) \leq r\}$$

For positive integer $r$ clearly

$$|B_r(x)| \leq \left( \frac{b^m}{r} \right)^r$$
where
\[
\binom{m}{r} = \frac{m!}{r!(m-r)!}.
\]

For a subset \(S \subseteq \{1, \ldots, b\}^m\) we define its minimum distance to be \(\min\{\rho(x,y): x,y \in S, x \neq y\}\).

**Lemma 1.1.** Let \(\ell\) be an integer \(\geq 1\). Then for \(b = 2^{2\ell}, c = 2\ell\) we have that for any positive integer \(m\) there exists a subset \(S\) of \(\{1, \ldots, b\}^m\) with \(|S| = b^m\) and with minimum distance \(> (1-1/\ell)m^c\).

**Proof.** Let \(\theta = 1-1/\ell\). For any \(x \in \{1, \ldots, b\}^m\) we have
\[
|B^\theta_{\text{me}}(x)| \leq \binom{mc}{\theta \text{me}} b^{\theta \text{me}} < 2^{mc} b^{mc} = b^{(\theta+\log b^2)mc} = b^{(1-1/\ell + 1/2\ell)mc} = b^{(1-1/2\ell)mc} = \frac{1}{b^{mc/2\ell}}.
\]

\[
= \frac{mc}{b^m} = \frac{1}{b^m}.
\]

Since \(\log_b 2 = 1/2\ell\). To construct \(S\) we choose any \(x_1 \in \{1, \ldots, b\}^m\) as our first element and subsequently choose \(x_i\) from
\[
[1, \ldots, b]^m - B^\theta_{\text{me}}(x_1) - \cdots - B^\theta_{\text{me}}(x_{i-1}).
\]

Since this set has at least \(|\{1, \ldots, b\}^m| - (1 - 1/2^\ell) b^m\) elements, we can keep choosing \(x_i\)'s for \(1 \leq i \leq b^m\).

The above construction of \(S\) takes polynomial time in \(b^m\), since we can go through the set \([1, \ldots, b]^m\) in some order to find points for \(S\); each time we add a point \(x\) to \(S\) we "mark off" the points in \(B^\theta_{\text{me}}(x)\).

**Theorem 1.2.** For fixed \(k\) we can construct \(n,k\) schemes of size \(O(\log n)\) in time polynomial in \(n\).

**Proof.** In the above lemma, let \(\ell = \binom{k}{2}\), let \(m\) be fixed, and let \(S = \{x_1, \ldots, x_{n^k}\}\). Let \(y_1, \ldots, y_k\) be distinct points in \(S\). Since each of the \(\binom{k}{2}\) pairs of these points differ at a fraction \(> 1 - \binom{k}{2}\) of their components, there must be one component at which all pairs differ, i.e., for some \(u\) the \(u\)-th component of \(y_1, \ldots, y_k\) are all distinct. We therefore construct a \(b^{mc}, k\) scheme as follows: for each integer \(j, 1 \leq j \leq cm\), and integers \(t_1, \ldots, t_k\) with \(1 \leq t_1 < t_2 < \ldots < t_k \leq b^m\) we define the partition whose \(u\)-th subset is
\[
\Lambda_u^{t_1, \ldots, t_k}
\]

\(u = 1, \ldots, k\). Since any \(k\) \(x_i\)'s are separated by some \(j\)-th component, the above collection of partitions separates any \(k\) points of \([1, \ldots, b^m]\). This scheme is of size
\[
mc\binom{b}{k} = mk(k-1)\binom{2^{k(k-1)}}{k} = O(m).
\]

Hence for any \(n\), we can take \(m = \lceil \log_2 n \rceil \) (\(\lceil a \rceil\) denoting the smallest integer \(\geq a\)) to get an \(n,k\) scheme of size \(O(\log n)\). Furthermore, the construction of \(S\) is done in polynomial time of \(b^{mc} = O(n^k)\).

We can significantly improve on Lemma 1 by using Stirling's formula
\[
n! = \sqrt{2\pi n} \left( \frac{n}{e} \right)^n e^{r_{n}}
\]
where
\[
\frac{1}{12n+1} < r_n < \frac{1}{12n}.
\]
Then we have
\[
\frac{mc}{\theta mc} < \frac{1}{\sqrt{2\pi\theta(1-\theta)mc}}
\]
\[
\left[\theta^\frac{(1-\theta)}{1-\theta} \right]^{-\frac{mc}{2/12mc}}
\]
\[
< \left[\theta^\frac{(1-\theta)}{1-\theta} \right]^{-\frac{mc}{2}}
\]
or
\[
\frac{mc}{\theta mc} < h^{mc}
\]
where
\[
h = \left[\theta^\frac{(1-\theta)}{1-\theta} \right]^{-1}.
\] (1.2)

Using this bound, instead of \( \frac{mc}{\theta mc} < 2^{mc} \) which we used before, we get

**Lemma 1.3.** Lemma 1.1 holds for any \( c \) and \( b = h^\theta \) with
\[
\frac{1}{c} + \frac{1}{b} \leq \frac{1}{\ell}.
\] (1.3)

**Proof.** Details omitted.

**Corollary 1.4.** Lemma 1.1 holds with \( c = 2\ell \) and any \( b \geq e^2 \ell^2 = (7.389 \ldots)^2 \) or \( c = \ell^2 \) and \( b \geq 8\ell \).

**Proof.** For \( c = 2\ell \) we need \( b \geq 2\ell \) and thus
\[
b \geq h^{2\ell} = \left[\ell^\frac{1/2}{(\ell-1)} \right]^{(\ell-1)/\ell} 2^{2\ell}
\]
\[
= \ell^2 \left[\left(1 + \frac{1}{\ell-1}\right)^{\ell-1}\right]^2
\]
\[
< \ell^2 e^2
\]
since \( (1+1/n)^n < e \) for all \( n \). Also, using \( (1+1/n)^{n+1} < 4 \) and \( n^{\ell/(n-1)} \leq 2 \) for all \( n \geq 2 \), we see that for \( c = \ell^2 \) it suffices to choose

\[
b \geq \frac{\ell^2}{h^{(\ell-1)}} = \ell^{1/(\ell-1)} \left(1 + \frac{1}{\ell-1}\right)^\ell
\]
\[
= \ell^{1/(\ell-1)} \left(1 + \frac{\ell}{\ell-1}\right)^\ell
\]
\[
< \ell + 2 + 4 = 8\ell.
\]

Thus in Theorem 1.2 we can take \( c = k(k-1) \) and \( b = 2k^2(k-1)^2 \) or \( c = 1/4 k^2(k-1)^2 \) and \( b = 4k(k-1) \).

## 2. THE GENERAL THEORY

In this section, we generalize on the basic construction of Theorem 1.2 and describe how the theory of error-correcting codes ties into our construction.

By a \( b,m,c,\theta \) set we shall mean a subset of \( S \) of \( \{1, \ldots, b\}^m \) of minimal distance \( > \theta mc \) and with \( |S| = b^m \). In Sections 2 and 3, we shall always take \( m \) to be an integer. Of course, \( b, cm, \) and \( b^m \) must always be integers.

Let us examine the role played then the \( b,m,c,\theta \) set, \( S = \{x_1, \ldots, x_{b^m}\} \), in the proof of Theorem 1.2.

We constructed our \( b^m,k \) scheme by separating \( x_1, \ldots, x_{b^m} \) by their components. For each \( j, 1 \leq j \leq cm \) we associated \( \theta \) partitions to the \( j \)-th component;
we point out that the \( j \)-th component of \( k \) points in \( S \) represent \( k \) points of \( \{1, \ldots, b\} \), and so the \( \theta \) partitions associated to the \( j \)-th component simply represent a \( b,k \) scheme. We observe that a better \( b,k \) scheme, of size \( r \), would lead to a construction of a \( b^m,k \) scheme of size \( cm+r \).

**Theorem 2.1.** Let \( \{A_1, \ldots, A_k\}_{j=1, \ldots, r} \) be a \( b,k \) scheme of size \( r \). Then from this scheme, and from a \( b,m,c,\theta \) set \( S = \{x_1, \ldots, x_{b^m}\} \) with \( \theta = 1 - \frac{1}{\theta} \) we can construct a \( b^m,k \) scheme of size \( cm+r \).

**Proof.** For integers \( i_1, i_2 \) with \( 1 \leq i_1 \leq mc \) and \( 1 \leq i_2 \leq r \) we define the partition whose \( u \)-th subset is
of $x_i$ is contained in $A_i^{\{j\}}$. Clearly these $m \cdot r$ partitions separate any $k$ distinct points of $\{1, \ldots, b^m\}$ and thus form a $b^m, k$ scheme of size $c m \cdot r$.

Theorem 2.1 tells us that the role of the $b, m, c, \theta$ set was to combine with a $b, k$ scheme to form a $b^m, k$ scheme. Next, we show how to combine a $b, m, c, \theta$ set directly with a formula for $Th_k(z_1, \ldots, z_n)$ to get a formula for $Th_k(y_1, \ldots, y_{b^m})$:

**Theorem 2.2.** Let there exist a (monotone) formula for $Th_k(z_1, \ldots, z_n)$ of size $r$ (i.e., total number of occurrences of variables). From this formula, and from a $b, m, c, \theta$ set $S = \{x_1, \ldots, x_{b^m}\}$ with $\theta = 1 - \left(\frac{b^m}{b}\right)^{-1}$, we can construct a (monotone) formula for $Th_k(y_1, \ldots, y_{b^m})$ of size $rcmb^{m-1}$.

**Proof.** For each $j, 1 \leq j \leq cm$ we define the partition $\{1, \ldots, b^m\}$ into $b$ subsets, $A_1^j, \ldots, A_b^j$, where

$$A_i^j = \{i: \text{the } j\text{-th component of } x_i \text{ is } u_i\}.$$  

Then

$$Th_k(y_1, \ldots, y_{b^m}) = \bigvee_{j=1}^{cm} Th_k(V_{i \in A_1^j} y_i, V_{i \in A_2^j} y_i, V_{i \in A_b^j} y_i) \quad (2.1)$$

because a subset $R$ of $\{1, \ldots, b^m\}$ satisfies $|R| \geq k$ iff there is some $j$ for which $R$ has members in at least $k$ of $A_1^j, \ldots, A_b^j$. On the right hand side of (2.1) we have a disjunction of $cm$ threshold-k functions of $b$ arguments. Consider one of these functions

$$Th_k(V_{i \in A_1^j} y_i, V_{i \in A_2^j} y_i, V_{i \in A_b^j} y_i) \quad (2.2)$$

for some fixed $j$. The $b$ arguments of this threshold-k function contain a total of $b^m$ occurrences of variables (in fact, each variable $y_1, \ldots, y_{b^m}$ occurs once). If, in our formula for $Th_k(z_1, \ldots, z_n)$, each variable $z_i$ appears the same number of times, i.e., $r/b$ times, then the formula constructed for (2.2) will be of size $r/b \cdot b^m$. If some of the variables $z_1, \ldots, z_n$ occur less often then others, then by matching these ones up with the larger sets among $A_1^j, \ldots, A_b^j$ we will do no worse than $r/b \cdot b^m$. Thus, using (2.1) we can construct a (monotone) formula for $Th_k(y_1, \ldots, y_{b^m})$ of size $cm \cdot r/b \cdot b^m$.

The construction of $b, m, c, \theta$ sets is a central problem of the theory of error-correcting codes: Assume that the characters of a transmitted message each have a certain probability of being received incorrectly. If we only transmit from a subset, $S$, of all possible messages, having minimum distance $\geq 2t+1$, then we can correct the errors in the received message as long as no more than $t$ characters are in error. Lemma 1.4 tells us that for $\theta = 1 - \frac{1}{r}$, there are $8r, m, f^2, \theta$ sets for integers $m$, constructable in polynomial time in $(8f^2)m^2$.

Actually, there are more sophisticated error-correcting codes which, for fixed $\theta$, yield explicit $b, m, c, \theta$ for all $m$ and some fixed $b$ and $c$. We will devote Sections 3-5 to explaining some of these techniques. Before doing so, we shall discuss the implications of Theorems 2.1 and 2.2.

According to Corollary 1.4, for $\theta(k) = 1 - \left(\frac{k}{2}\right)^{-1}$ we can construct $b, m, c, \theta$ sets for any $m$ and for $b(k)=4k(k-1)$, $c(k) = 1/4 k^2(k-1)^2$.

By Theorem 2.1, if we can construct a $b(k), k$ scheme of size $r(k)$ then we can construct $b^m, k$ schemes of size $cmr(k) = O(k^2m \ln(k))$. Thus constructing $Th_k(x_1, \ldots, x_n)$ formulae of size $n \log n$ times a polynomial in $k$ would follow from a construction of $4k^2, k$ schemes of polynomial size in $k$.

Unfortunately, $4k^2, k$ schemes are of size $\Omega(k^6)$; more generally, on $n, k$ scheme is necessarily of size $(\frac{n}{k})^{(\frac{n}{k})^k}$, since a partition of $\{1, \ldots, n\}$ into $k$
subsets of size \( p_1, \ldots, p_k \) accounts for 
\( p_1 p_2 \cdots p_k \binom{\sum p_i}{k} \), (using the 
arithmetic-geometric mean inequality) \( k \)-tuples 
separated.

However, recently L. G. Valiant has demonstrated 
polynomial bounds for the size of monotone 
formulae for \( Th_k(x_1, \ldots, x_{4k^2}) \):

**Lemma 2.3.** There exist monotone Boolean formulae for 
\( Th_k(x_1, \ldots, x_n) \) for any \( k \) of size \( O(n^{3.3}) \).

**Proof.** See [V].

**Theorem 2.4.** There exist monotone Boolean formulae for 
\( Th_k(x_1, \ldots, x_n) \) of size \( O(k^{12.6} n \log n) \).

**Proof.** By Lemma 2.3, there exist monotone 
formulae for \( Th_k(x_1, \ldots, x_{4k^2}) \) of size \( O(k^{10.6}) \). Combining this with Theorem 3.2 in which we take 
b=4k^2, \( c=k^4 \) yields formulae for \( Th_k(x_1, \ldots, x_n) \) of size

\[
O(k^{12.6} n \log n).
\]

For any \( n \) set \( m=\lceil \log_b n \rceil = \lceil \log n \rceil / \log b \) and 
construct \( Th_k(y_1, \ldots, y_n) \) out of our \( Th_k(x_1, \ldots, x_n) \) 
formula, by choosing the \( n \) variables of \( x_1, \ldots, x_n \) 
which occur with the least frequency in our formula 
(and setting the others to 0). This yields a formula 
for \( Th_k(y_1, \ldots, y_n) \) no more than \( n/b^m \) times the size 
of our \( Th_k(x_1, \ldots, x_n) \) formula, i.e., a formula for 
\( Th_k(y_1, \ldots, y_n) \) of size

\[
O(k^{12.6} n \log n).
\]

Since Valiant’s proof of Lemma 2.3 is 
nonconstructive, so is Theorem 2.4. Works of 
Pippenger [P], Paterson [Pa], and Peterson [Pe] have led to constructions of formulae for \( Th_k(x_1, \ldots, x_n) \) of 
size \( O(n^{3.3}) \) (for all \( k \)) in which negation is allowed 
as well. Also, a result of Ajtai, Komlos, and 
Szemeredi [AKS] on comparator sorting networks 
of depth \( O(\log n) \) implies a construction for 
monotone formulae for \( Th_k(x_1, \ldots, x_n) \) (for all \( k \)) 
of size polynomial in \( n \) (but the degree of the 
polynomial is very large). Using Theorem 2.2, these 
results yield constructions for formulae for 
\( Th_k(x_1, \ldots, x_n) \) of size \( O(k^{7.4} n \log n) \) using negation, 
conjunction, and disjunction, and monotone 
formulae of size \( n \log n \)-polynomial (of large degree) 
of \( k \).

3. A RANDOMIZED LINEAR CONSTRUCTION

In Theorem 1.2, we constructed \( n, k, \theta \) schemes of 
size \( O(\log n) \) in time polynomial in \( n^{k(k-1)} \). In what 
follows, we give a random algorithm which will 
construct \( b, m, c, \theta \) sets, \( S \), in space \( O(m^2) \) bits and 
expected time \( O(m^2) \) with time measured as number 
of bit operations. We require that \( b \) be prime and 
that \( b, m, c, \theta \) satisfy (1.3).

Let \( b, m, c, \theta \) satisfy (1.3). Our first attempt at a 
random algorithm to construct \( S \) would be to pick 
\( x_1, \ldots, x_n \) at random and to see if \( (\rho(x_i, x_j) > \theta m) \) for all 
\( i, j \), \( i \neq j \). We would have \( b^m (b^m-1)/2 \) pairs 
\( x_i, x_j \) to check, and each check would require \( O(m) \) bit 
operations since the \( x_i \)'s are of length \( O(m) \) bits. 
Thus, this check would require \( O(m^2) \) bit 
operations, as well as \( O(m^2) \) bits of storage for the 
\( x_i \)'s. So even if our first guess is correct, we need a 
fair amount of time and a lot of storage. To 
improve on this, we use the idea of linear codes.

Let us further assume that \( b \) is a prime number, 
which we will henceforth denote \( p \). Then \( \mathbb{Z}/p\mathbb{Z} \), the 
integers modulo \( p \), form a field and \( (\mathbb{Z}/p\mathbb{Z})^m \) 
forms a vector space over \( \mathbb{Z}/p\mathbb{Z} \). We can identify
Theorem 3.2. We can construct an $S$ with minimum distance $> \theta mc$ and $|S| = p^m$ via a random algorithm in space $O(m^2)$ bits and in expected time $O(mp^m)$ bit operations.

Proof. Choose $v_1, \ldots, v_m$ at random from $(\mathbb{Z}/p\mathbb{Z})^{mc}$ and consider $S = \text{span}(v_1, \ldots, v_m)$. By the above proposition, if $\rho(v_i, 0) \geq d$ and for each $i > 1$, $\rho(v_i, \text{span}(v_1, \ldots, v_{i-1})) \geq d$, then an easy induction argument shows $\text{span}(v_1, \ldots, v_m)$ has minimum distance $\geq d$. Since the probability that $\rho(v_i, \text{span}(v_1, \ldots, v_{i-1})) > \theta mc$ is

$$\geq 1 - \frac{p^i - 1}{p^{mc}} \left( \frac{1}{p^m} \right) \left( \frac{1}{p^m} \right) \cdots \left( \frac{1}{p^m} \right) \geq 1 - \frac{1}{p^m \cdots p^m} \geq 1 - \frac{1}{p - 1} \geq 1 - \frac{2}{p - 1},$$

we have that $S$ has minimum distance $> \theta mc$ with probability

$$\geq 1 - \frac{2}{p - 1}.$$ 

Rest of proof omitted.

Corollary 3.3. Using the above random algorithm, for fixed $k$ we can construct monotone formulae for $\text{Th}_k(x_1, \ldots, x_n)$ of size $O(n \log n)$, explicit up to a construction of a set, $S$, taking space $O((\log n)^2)$ bits and expected time $O(n \log n)$ bit operations.

4. A CONCATENATION CONSTRUCTION

In Section 2, we demonstrated ways of constructing new $\text{Th}_k(x_1, \ldots, x_n)$ formulae and $n,k$ schemes from ones with smaller $n$ by combining
them with a b,m,c,θ set. In this section, we show a way of combining two b,m,c,θ sets to get a new one, and apply this technique.

From now on, we no longer require m to be an integer in a b,m,c,θ set (only that b,bm, and cni be integers). Note that for any b,m,c,θ set S, S is also a b,m,c,θ' set for θ'<θ, and any subset of S of size b,m' is a b,m',c,m/m',θ set, for any m'<m with b,m' an integer.

Let S₁ be a b₁,m₁,c₁,θ₁ set and S₂ a b₂,c₂,m₂,θ₂ set with b₂ = |S₁| = b₁m₁. Then we can identify S₂ with S₁ and think of each element of S₂ as a c₂m₂-tuple of elements of S₁. More precisely, let the points of S₁ be ordered x₁,...,b₁m₁ and let i(1,...,b₁) = i₁(1,...,b₁m₁) = i₁(1,...,b₁m₁), for each point y = (y₁,...,y₁m₁) in S₁, let i(y) = (i₁(y₁),...,i₁(y₁m₁)). Then i:S₂±S₁\×S₂^m₂ which we can identify with i(1,...,b₁)^m₂ \times S₁\times S₂^m₂. We define S₁\circ S₂, the concatenation of S₂ with S₁ (with respect to a given order of S₁), as the image i(S₂). Note that |S₁\circ S₂| = |S₁|, and further that S₁\circ S₂ is a b₁,m₁,m₂,c,c₁,θ₁,θ₂ set.

The above construction also works for b₂<|S₁|, but then

|S₁\circ S₂| = |S₂| = b₂m₂ = b₁m₁

where

μ = \frac{\log b₂}{\log b₁}

and so S₁\circ S₂ is a b₁,μm₂, m₁/μ c₁,c₂,θ,θ₂ set.

The following set is known to coding theorists as a Reed-Solomon code: for any prime p and integer d<p we define

S(p,d) = \{ f(0), f(1),..., f(p-1) \} \times (\mathbb{Z}/p\mathbb{Z})^p;

f is a polynomial of degree \leq d-1 (over a field) has at most d-1 roots,

S(p,d) is a p,d,p/d,(1 - \frac{d}{p}) set.

While S(p,d) is simple and explicit, it only gives b,m,c,θ sets for m<b. However, concatenating S(p,d) sets with other sets is a very powerful technique.

Theorem 4.1. For fixed b,c,θ=1-1/2, let Sₘ, M=1,2,..., be a sequence of b,M,c,θ sets. Then for each sufficiently large m, we can construct a b,m,c',1-1/θ set for some c'<4b²c(2d+1), by concatenating an S(p,d) set with an S₀(log m), for primes p between b⁻¹ and b⁻¹ for some M with b⁻¹M<m.

Proof. Details omitted.

For integer k≥1 let logᵏx denote the kth iteration of log x, and define log₀x=x.

Repeated application of theorem 4.1 yields

Theorem 4.2. Let k be a fixed positive integer. Then for θ=1-1/ℓ there exists constants b,c polynomial in ℓ such that for each sufficiently large m (larger than some polynomial in ℓ), a b,m,c,θ set with c'<c can be constructed, explicit up to a set, S, constructible in time polynomial in log⁻¹ m, and k appropriately chosen primes <m.

Note that one can find all primes <m in time polynomial in m. Thus

Corollary 4.3. For fixed k we can construct monotone formulae for Tₖ₁(x₁,...,xₙ) of size O(n log n) in polynomial time in n, where the degree of the polynomial does not depend on k.

5. AN EXPLICIT CONSTRUCTION

In the previous sections, our constructions for b,m,c,θ sets have always involved, at some point, the
choosing of points in \([1, \ldots, b]\) which are a large
distance apart. Such points were not explicitly
specified. Using a Justesen code, it is possible to
specify sets explicitly (for \(m=1, 2, \ldots\), fixed \(b, c, \theta\)), in
terms of finite fields.

Here, we shall briefly describe these Justesen
codes, assuming a familiarity with finite fields. For
a more detailed discussion and background on finite
fields, see [vLI] or [B].

Let us generalize the notion of a concatenated
set. Let \(T\) be a \(b_2, m_2, c_2, \theta\) set and let \(S_i\) be
\(b_i, m_i, c_i, \theta_i\) sets for \(i=1, \ldots, c_2, \theta\), with \(b_2 = b_1^{m_1}\).
Then we define the concatenation for \(T\) with
\(\{S_i\}\), denoted \(\{S_i\} \circ T\), as \(c(T)\) where
\[i: T \times S_1 \times S_2 \times \cdots \times S_{c_2, \theta}\]
is given by

\[\tilde{y} \in \{y_1, \ldots, y_{c_2, \theta}\}\]

where \(i_1(y_1, \ldots, y_{c_2, \theta})\) is

\[= (\tilde{i}(y_1, \ldots, y_{c_2, \theta}))\]

where \(i_1\) are any bijections from \([1, \ldots, b_2]\) to \(S_i\). In
the construction of Section 4, we constructed
\(\{S_i\} \circ S(p, d)\) with \(S_1 = S_2 = \cdots = S_{c_2, \theta}\).

Unfortunately, we do not have an explicit
description of \(S\). However, there are explicit
descriptions of collections \(\mathcal{A}\) of \(b_i, m_i, c_i, \theta\) sets with
fixed \(b_i, m_i, c_i\) and with almost all of the \(\theta\)'s close to
1. The idea behind a Justesen code is to take such
collections \(\mathcal{A}\) and construct \(\{S_i\} \circ T\) with the \(S_i\)
distinct elements of \(\mathcal{A}\).

Proposition 5.1. Let \(T\) be a \(b_2, m_2, c_2, \theta\) set, \(S_i\) be
\(b_i, m_i, c_i, \theta_i\) sets for \(i=1, \ldots, c_2, \theta\) with \(b_2 = b_1^{m_1}\). Of
\(\theta, \ldots, \theta_{c_2, \theta}\), let no more than \(\epsilon m_2, c_2\) of them be \(\theta\) for
some \(\epsilon < 1\) and \(\theta\). Then \(\{S_i\} \circ T\) is a

\[b_1, m_1, c_1, c_2, \theta (\theta - \epsilon) \] set.

Next, we demonstrate collections \(\mathcal{A}\) mentioned
previously.

Let \(c\), \(q\), and \(m\) be fixed. For any
\(a_1, \ldots, a_{c-1} \in GF(q^m)\) consider the set

\[S_{a_1, \ldots, a_{c-1}} = \{(\beta, \beta a_1, \ldots, \beta a_{c-1}) : \beta \in GF(q^m)\}\]

c \(GF(q^m)^c\).

Viewing \(GF(q^m)\) as \((GF(q))^m\), we view each
\(S_{a_1, \ldots, a_{c-1}}\) as \(q, m, c, \theta\) set for some \(\theta\). Each element of
\((GF(q))^m\) of nonzero weight can belong to at most
one \(S_{a_1, \ldots, a_{c-1}}\). Thus, of the \(q^m(c-1)\) sets \(S_{a_1, \ldots, a_{c-1}}\), at
most \(|B_{\theta, 0}(0)|\) have nonzero element of weight
\(\theta\). The proof of Lemma 1.3 also proves:

Proposition 5.2. Let \(q = h^3\) where \(h = [\theta^3(1-\theta)(1-\theta)]^{-1}\), and let

\[\frac{q}{\theta} + \frac{1}{\beta} \leq \frac{1}{\theta}\]

where \(1/\theta = 1/\theta\). Then \(|B_{\theta, 0}(0)| \leq q^{m(\theta-2)}\)

Corollary 5.3. Let \(q\), \(c\), and \(\theta\) be as in Proposition 5.2.
Then less than \(1/q^m\) of the \(S_{a_1, \ldots, a_{c-1}}\)'s are not \(q, m, c, \theta\)
sets.

Next, we specify the set \(T\) which we
concatenate with \(\{S_{a_1, \ldots, a_{c-1}}\}\). \(T\) will be taken to a
"primitive BCH code." For background on BCH
codes, see [vLI] Chapter 6 and [B] Chapter 12, for
example.

Let a prime power \(q\) and positive integer \(n\) be
relatively prime. Let \(e\) be the multiplicative order of
\(q\) in \(n\). Then there exist primitive \(n\)-th roots of
unity in \(GF(q^e)\): let \(\beta\) be one of them. For any \(d < n\)

\[BCH(q, n, d) = \{a(x) \in R : a(\beta) = a(\beta^d) = \cdots = a(\beta^{d-1}) = 0\}\]

Lemma 5.4. \(BCH(q, n, d)\) has minimum distance \(\geq d\).

Now consider the case \(n = q^{e-1}\) (note that the
multiplicative order of \(q\) in \(q^{e-1}\) is \(e\)). BCH codes
with such \(n\) are called primitive.
Lemma 5.5. Let \( d = (q - a)a^{c-1} \) for some integer \( a \).
Then \(|\text{BCH}(q,n,d)| = q^c\). Also this BCH has minimum distance \( >d \).

If in Lemma 5.5 we replace \( q \) by \( q^m \) and by \( aq^{m-1} \) then we see that the BCH set has size \((q^c)^a q^{mc-c}\) and minimum distance \( > (q-a)q^m \).
Hence we have

Corollary 5.6. \( \text{BCH}(q^m,q^{mc-1},(q-a)q^{me-1}) \) is an \( a \)

Let \( T \) be the BCH set in Corollary 5.6 with \( c \) replaced by \( c-1 \). Let
\[
\mathcal{A} = \{ S_{y_1,\ldots,y_{c-1}} \} - S_{0,0,\ldots,0}
\]
and consider \( \mathcal{A} \circ T \). Applying Proposition 5.1 and

Theorem 5.7. The above construction gives for each integer \( n \) a \( q,n,c',1-1/\ell \) set for fixed \( q \leq 15\ell^2 \) and some \( c' \leq \ell(\ell + 1)4^{4\ell-1} \).
Proofs omitted.

Although finite fields can be constructed quickly (see [R]), one can modify the above to avoid
the need for field construction. Rather than using \( T=\text{BCH}(q^m,a) \) with \( m=1,2,\ldots \), we can take
\( T=\text{BCH}(p_m,a) \) with \( p_m \) being the largest prime \( \leq q^m \)
and use \( U \circ T \circ \mathcal{A} \) with \( U=\{1,\ldots,q\}^m \).

REFERENCES


